

Lab 3

CST8912\_011

Yuntian Du

du000086

February 19, 2025

Submitted to :

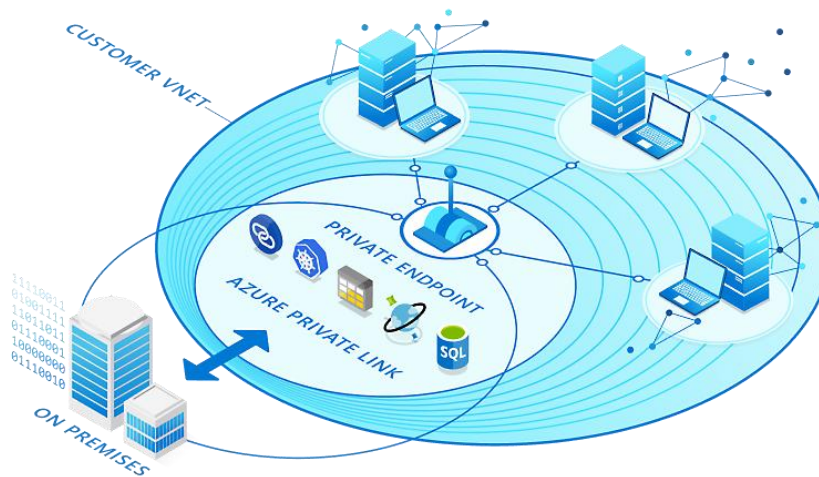
**Prof. Ragini Madaan**

# Practice generate shared access signatures for Azure Cloud and manage lifecycle of cloud storage

## Introduction & Purpose

### Introduction:

Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public internet.



Private Endpoint is the key technology behind Private Link. Private Endpoint is a network interface that enables a private and secure connection between your virtual network and an Azure service. In other words, Private Endpoint is the network interface that replaces the resource's public endpoint.

Private Link gives you private access from your Azure virtual network to PaaS services and Microsoft Partner services in Azure. However, what if your company has created its own Azure services for your company's customers to consume? Is it possible to offer those customers a private connection to your company's services?

Yes, by using Azure Private Link Service. This service lets you offer Private Link connections to your custom Azure services. Consumers of your custom services can then access those services privately—that is, without using the internet—from their own Azure virtual networks.

When to use Private Link?

You know what Private Link is and how it works. Now you need some criteria to help you evaluate whether Private Link is a suitable choice for your company. To help you make a decision, let's consider the following goals:

- Bringing Azure PaaS services into your virtual network
- Securing traffic between your company network and the Azure cloud
- Eliminating internet exposure for PaaS services
- Accessing Azure PaaS resources across networks
- Lowering the risk of data exfiltration
- Offering customers private access to company-created Azure services

#### **Purpose:**

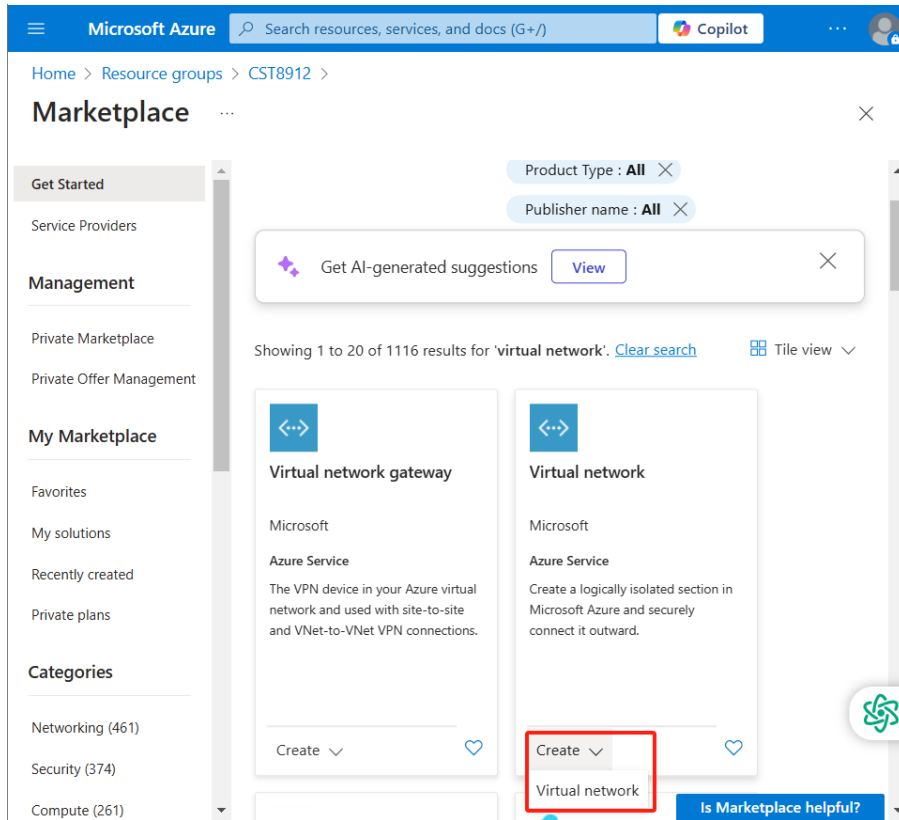
Upon completion of this lab, you will be able to create, configure and test the private link for any CSP

Azure Private endpoint is the fundamental building block for Private Link in Azure. It enables Azure resources, like virtual machines (VMs), to privately and securely communicate with Private Link resources such as Azure Storage.

#### **Steps covered in the lab**

##### **Create a Virtual network and Bastion Host**

1. In the portal, search for and select Virtual networks.



2. On the Virtual networks page, select + Create.
3. On the Basics tab of Create virtual network, enter or select the following information:

Setting	Value
Subscription	Azure for students
Resource Group	CST8912demo
Name	8912-vnet1
Region	Canada Central

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Resource groups > CST8912 > Marketplace >

## Create virtual network

Basics Security IP addresses Tags Review + create

**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 \* (New) CST8912demo [Create new](#)

**Instance details**

Virtual network name \* 8912-vnet1

Region \* (Canada) Canada Central [Deploy to an Azure Extended Zone](#)

Previous Next Review + create Give feedback

4. Select Next to proceed to the Security tab.
5. Select Enable Bastion in the Azure Bastion section of the Security tab.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Resource groups > CST8912 > Marketplace >

## Create virtual network

Basics Security IP addresses Tags Review + create

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more.](#)

Virtual network encryption ☐

**Azure Bastion**

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more.](#)

Enable Azure Bastion ☒

Azure Bastion host name Bastion8912

Azure Bastion public IP address \* (New) 8912-vnet1-bastion [Create a public IP address](#)

Previous Next Review + create Give feedback

Azure Bastion uses your browser to connect to VMs in your virtual network over secure shell (SSH) or remote desktop protocol (RDP) by using their private IP

addresses. The VMs don't need public IP addresses, client software, or special configuration

6. Enter or select the following information in Azure Bastion:

Setting	Value
Azure Bastion host name	Enter Bastion8912
Azure Bastion public IP address	Select <b>Create a public IP address</b> . Enter <b>public-ip</b> in Name. Select <b>OK</b> .

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'Security' tab is selected, showing options for virtual network encryption and Azure Bastion. The 'Azure Bastion' section is expanded, showing the 'Enable Azure Bastion' checkbox checked, the 'Azure Bastion host name' set to 'Bastion8912', and the 'Azure Bastion public IP address' set to '(New) public-ip'. A red circle with the number 11 is around the 'Next' button at the bottom of the wizard.

7. Select Next to proceed to the IP Addresses tab.
8. In the address space box in Subnets, select the default subnet.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

[Home](#) > [Resource groups](#) > [CST8912](#) > [Marketplace](#) >

## Create virtual network

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

+

Add a subnet

10.0.0.0/16

10.0.0.0

/16

10.0.0.0 - 10.0.255.255

65,536 addresses

Delete address space

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
AzureBastionSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)	-

Add IPv4 address space

Previous

Next

Review + create

Give feedback

9. In Edit subnet, enter or select the following information:

Setting	Value
Subnet template	Leave the default <b>Default</b> .
Name	Subnet-1-8912
IPv4 address range	Leave 10.0.0.0/16.
Starting address	Leave the default of 10.0.0.0.
Subnet size	Leave the default of /24(256 addresses).

Microsoft Azure Search resources, services, and docs (G+/) Copilot

## Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ⓘ Default

Name \* ⓘ Subnet-1-8912

**IPv4**

Include an IPv4 address space ☒

IPv4 address range ⓘ 10.0.0.0/16  
10.0.0.0 - 10.0.255.255

Starting address \* ⓘ 10.0.0.0

Size ⓘ /24 (256 addresses)

Subnet address range ⓘ 10.0.0.0 - 10.0.255

**IPv6**

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

**Private subnet**  
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual

[Save](#) [Cancel](#) [Give feedback](#)

10. Select save

11. Create and review when the validation passes

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Resource groups > CST8912 > Marketplace >

## Create virtual network

Basics Security IP addresses Tags Review + create

**Basics**

Subscription	Azure for Students
Resource Group	CST8912demo
Name	8912-vnet1
Region	Canada Central

**Security**

Azure Bastion	Enabled
- Name	(New) Bastion8912
- Public IP Address	(New) public-ip
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

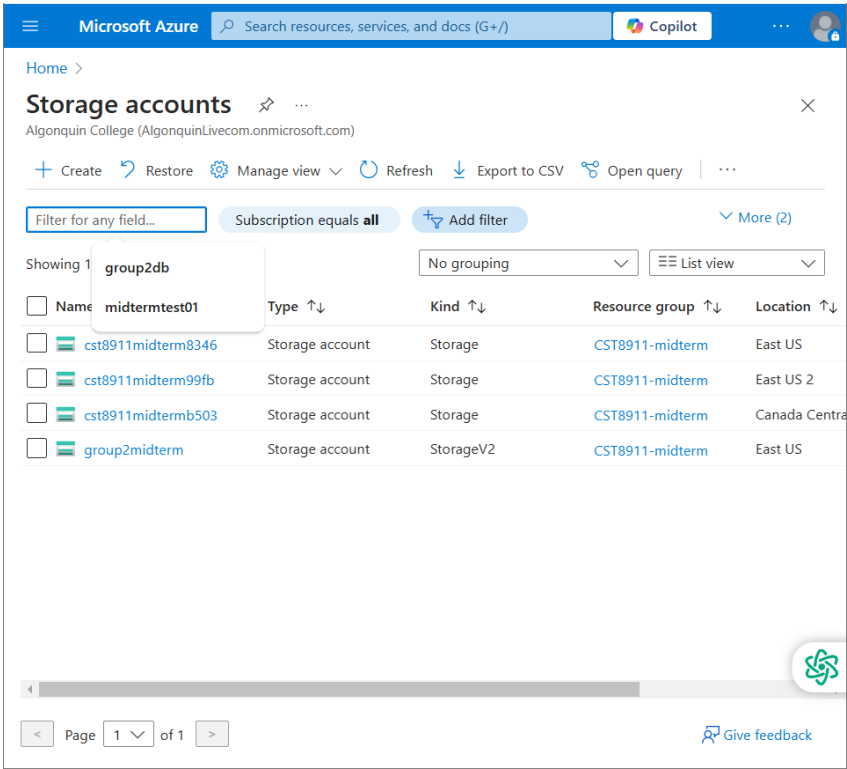
**IP addresses**

[Previous](#) [Next](#) [Create](#) [Give feedback](#)



Create a Storage Account

- 1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.



- 2. Select + Create.
- 3. In the Basics tab of Create a storage account enter or select the following information:

Setting	Value
Subscription	Azure for students
Resource Group	CST8912demo
Storage Account Name	Storage1-8912
Location	Canada Central
Performance	Standard
Redundancy	Local Redundant Storage (LRS)

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Storage accounts >

## Create a storage account

and manage your storage account together with other resources.

Subscription \* Azure for Students

Resource group \* CST8912demo  
[Create new](#)

### Instance details

Storage account name \* ① storage018912

Region \* ① (Canada) Canada Central  
[Deploy to an Azure Extended Zone](#)

Primary service ① Select a primary service

Performance \* ① ☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)  
☐ **Premium:** Recommended for scenarios that require low latency.

Redundancy \* ① Locally-redundant storage (LRS)

[Previous](#) [Next](#) [Review + create](#) [Give feedback](#)

#### 4. Select review

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Storage accounts >

## Create a storage account

Basics Advanced Networking Data protection Encryption **Review + create** ...

[View automation template](#)

### Basics

Subscription	Azure for Students
Resource group	CST8912demo
Location	Canada Central
Storage account name	storage018912
Primary service	
Performance	Standard
Replication	Locally-redundant storage (LRS)

### Advanced

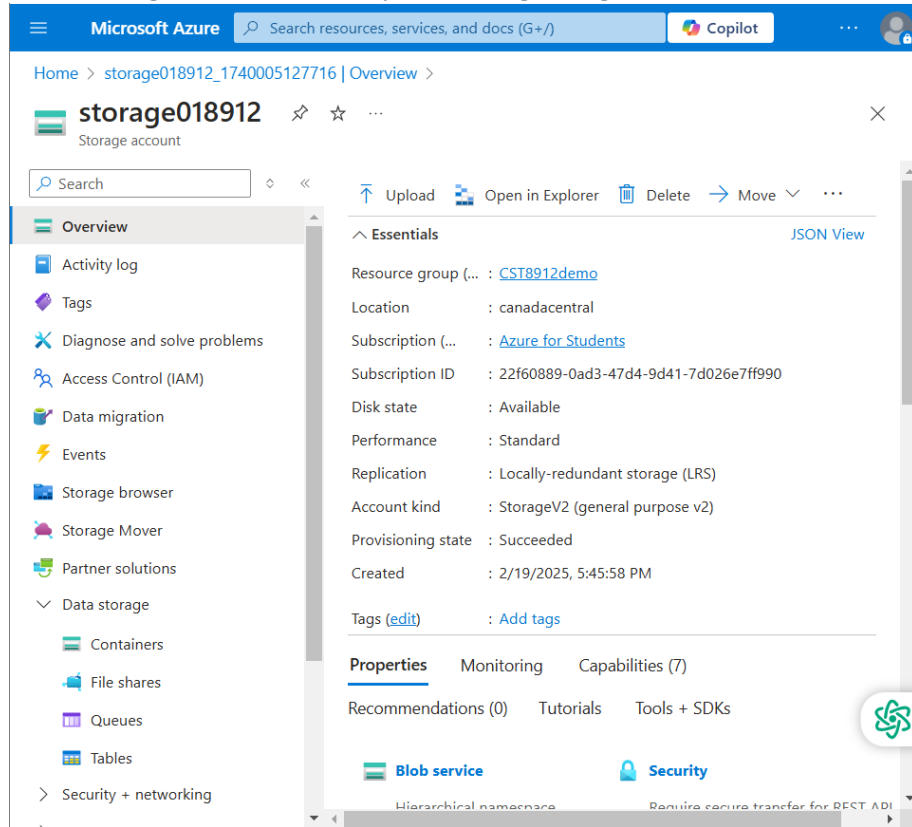
Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled

[Previous](#) [Next](#) [Create](#) [Give feedback](#)

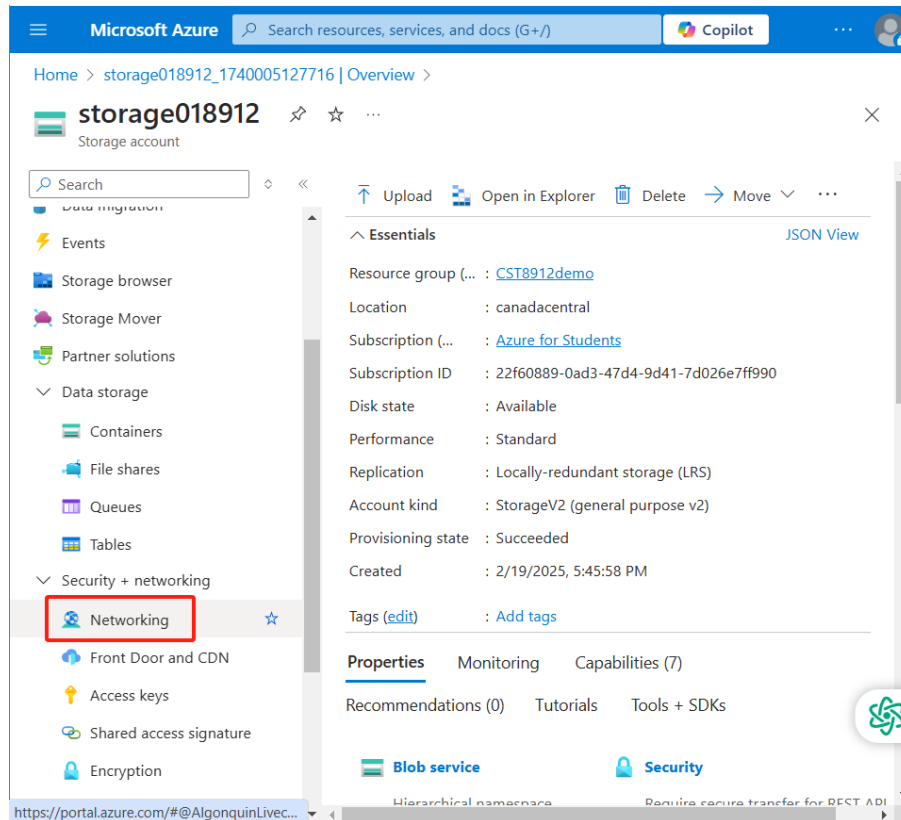
#### 5. Select create

## Disable public access to storage account

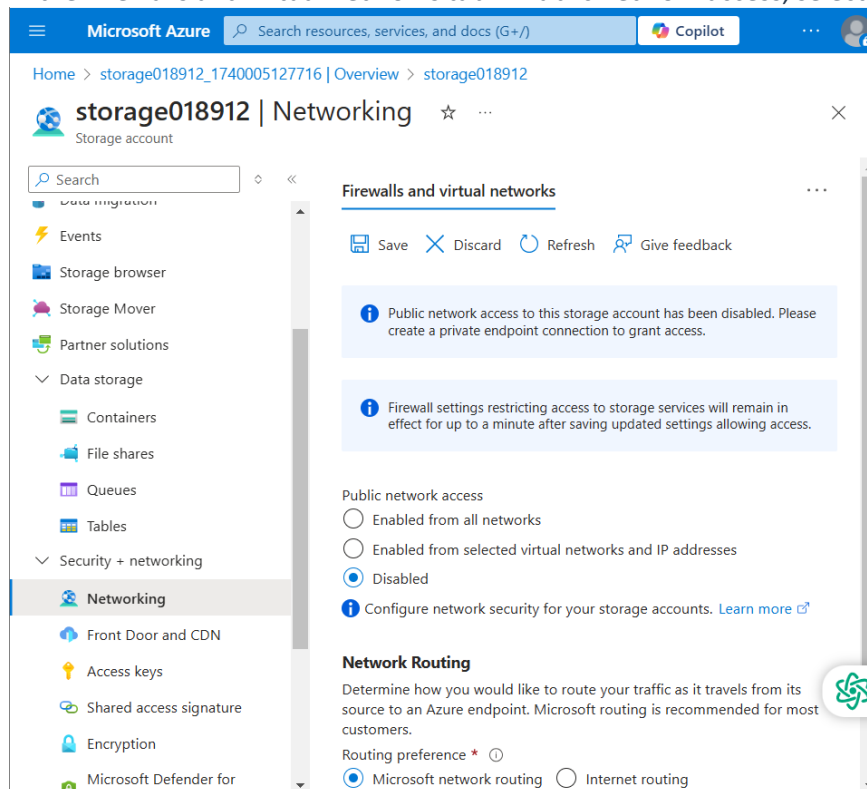
1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select storage1 or the name of your existing storage account.



3. In Security + networking, select Networking.



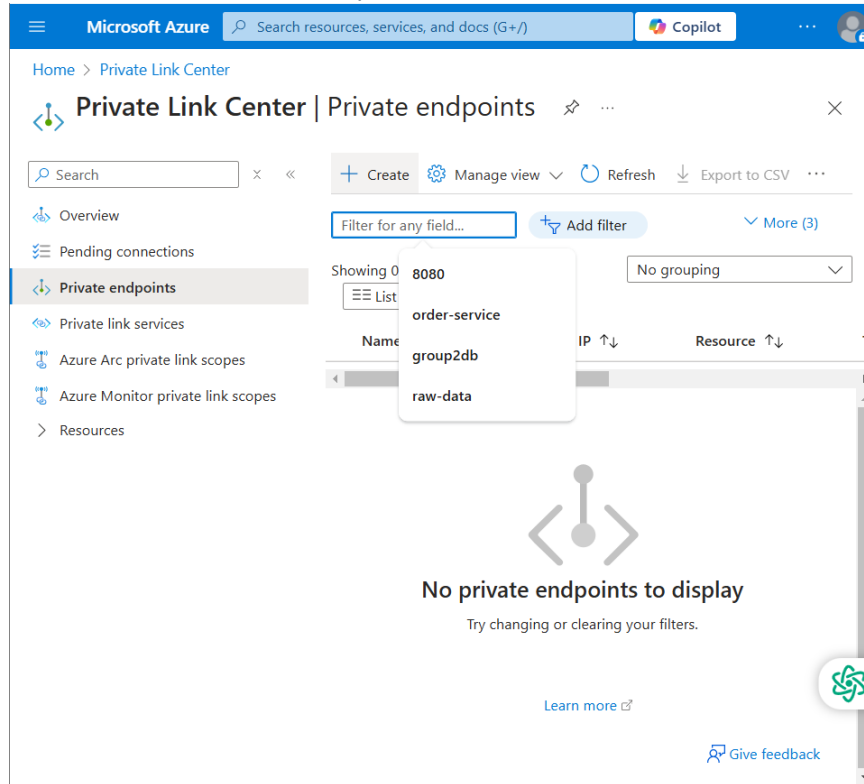
4. In the Firewalls and virtual networks tab in Public network access, select Disabled.



5. Select Save.

## Create private endpoint

1. In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.
2. Select + Create in Private endpoints.



3. In the Basics tab of Create a private endpoint, enter or select the following information.

Setting	Value
Subscription	Azure for students
Resource Group	CST8912demo
Name	Privateendpoint-8912
Network Interface Name	Leave the default of <b>private-endpoint-nic</b> .
Region	Canada Central

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

[Home](#) > [Private Link Center](#) | [Private endpoints](#) >

## Create a private endpoint

1 Basics

2 Resource

3 Virtual Network

4 DNS

5 Tags

6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \*

Azure for Students

Resource group \*

CST8912demo

[Create new](#)

**Instance details**

Name \*

Privateendpoint-8912

Network Interface Name \*

Privateendpoint-8912-nic

Region \*

Canada Central

< Previous

Next : Resource >

4. Select Next:Resource
5. In the Resource pane, enter or select the following information.

Setting	Value
Connection method	Leave the default of Connect to an Azure resource in my directory.
Subscription	Select your subscription.
Resource type	Select Microsoft.Storage/storageAccounts.
Resource	Select Storage1-8912 or your storage account.
Target subresource	Select blob.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Private Link Center | Private endpoints >

## Create a private endpoint

✓ Basics **2 Resource** ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method

☒ Connect to an Azure resource in my directory.  
☐ Connect to an Azure resource by resource ID or alias.

Subscription \* Azure for Students

Resource type \* Microsoft.Storage/storageAccounts

Resource \* storage018912

Target sub-resource \* blob

< Previous Next : Virtual Network >

6. Select Next: Virtual Network.
7. In Virtual Network, enter or select the following information.

Setting	Value
Virtual network	Select 8912-vnet (CST8912demo).
Subnet	Select Subnet-1-8912.
Network policy for private endpoints	<p>Select edit to apply Network policy for private endpoints.</p> <p>In Edit subnet network policy, select the checkbox next to Network security groups and Route Tables in the Network policies setting for all private endpoints in this subnet pull-down.</p> <p>Select Save.</p>
Private IP configuration	Select Dynamically allocate IP address.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot


## Edit subnet network policy

To apply network security groups (NSGs) and user defined routes (UDRs) to a private endpoint, network policies must be enabled on the subnet. All private endpoints within the subnet are affected. [Learn more](#)

Virtual network 8912-vnet1 (CST8912demo)

Subnet Subnet-1-8912 (10.0.0.0/24)

Network policies setting for all private endpoints in this subnet. Enabled

 This change will affect all private endpoints associated to this subnet. [Learn more](#)

### Existing private endpoints

Name	Private IP	Resource	Sub-resource
------	------------	----------	--------------

Save

Discard

Microsoft Azure

Search resources, services, and docs (G+)


Copilot


[Home](#) > [Private Link Center](#) | [Private endpoints](#) >

## Create a private endpoint

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network  8912-vnet1 (CST8912demo)

Subnet \*  Subnet-1-8912

Network policy for private endpoints Enabled ([edit](#))

### Private IP configuration

☒ Dynamically allocate IP address

☐ Statically allocate IP address

### Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule [Learn more](#)

[+ Create](#)

Application security group

< Previous

Next : DNS >

<https://portal.azure.com/#>

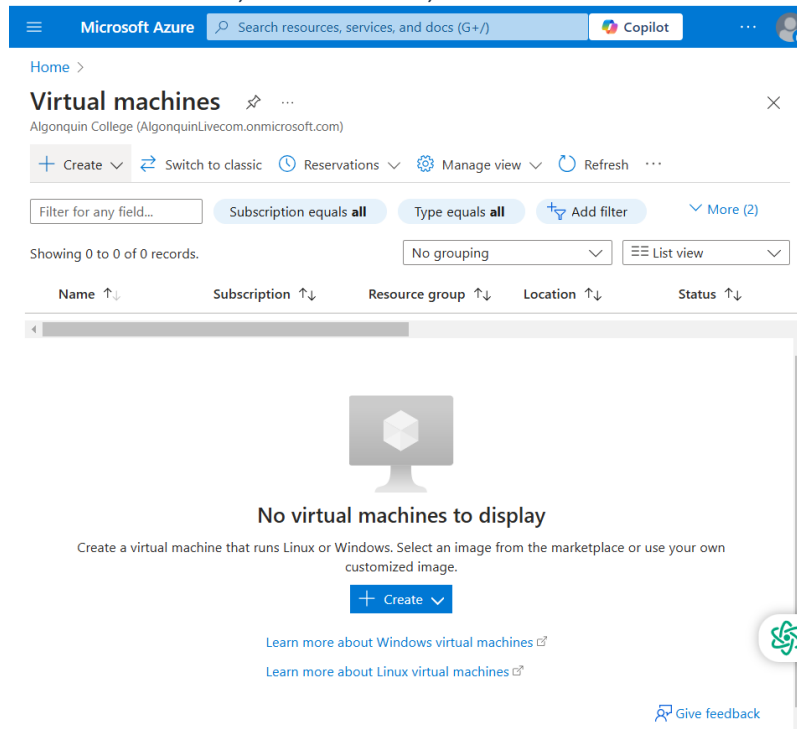
8. Select Next: DNS.





## Create test virtual machine

1. In the portal, search for and select Virtual machines.
2. In Virtual machines, select + Create, then Azure virtual machine.



3. On the Basics tab of Create a virtual machine, enter or select the following information:

Setting	Value
Subscription	Azure for students
Resource Group	CST8912demo
Virtual Machine name	8912-VM1
Region	Canada central
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Select Windows Server 2022 Datacenter - x64 Gen2.
VM architecture	Leave the default of x64.
Size	Select size (B1)
Authentication	Choose username and password
Public inbound ports	Select None

Microsoft Azure

Search resources, services, and docs (G+/J)

Copilot

...

Home > Virtual machines >

Create a virtual machine ...

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Subscription \*

Azure for Students

Resource group \*

CST8912demo

Create new

Instance details

Virtual machine name \*

8912-VM1

Region \*

(Canada) Canada Central

Availability options

No infrastructure redundancy required

Security type

Standard

Trusted launch virtual machine is required when using 1P Gallery images.

Image \*

Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

< Previous

Next : Disks >

Review + create

Give feedback

Microsoft Azure

Search resources, services, and docs (G+/J)

Copilot

...

Home > Virtual machines >

Create a virtual machine ...

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Size \*

Standard\_B1s - 1 vcpu, 1 GiB memory (\$11.39/month) (free services eligib...

See all sizes

Enable Hibernation

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

Administrator account

Username \*

yuntiandu

Password \*

.....

Confirm password \*

.....

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granu...

< Previous

Next : Disks >

Review + create

Give feedback

Microsoft Azure Search resources, services, and docs (G+/I) Copilot

Home > Virtual machines >

## Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

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

**10** Previous Next : Disks > Review + create Give feedback

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

4. Select the Networking tab at the top of the page.
5. Enter or select the following information in the Networking tab:

Setting	Value
Virtual Network	Select 8912-vnet (CST8912demo).
Subnet	Select Subnet-1-8912.
Public IP	Select None
NIC network security group	Select Advanced
Configure network security group	Select Create new.  Enter nsg-1 for the name.  Leave the rest at the defaults and select OK.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Virtual machines >

## Create network security group

Name \*

nsg-1 ✓

Inbound rules ⓘ

1000: default-allow-rdp  
Any  
RDP (TCP/3389) ✓

+ Add an inbound rule

Outbound rules ⓘ

No results.

+ Add an outbound rule

OK

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Virtual machines >

## Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability  
Help me choose the right VM size for my workload

Subnet \* ⓘ Subnet-1-8912 (10.0.0.0/24) Manage subnet configuration

Public IP ⓘ None Create new

NIC network security group ⓘ ☐ None ☐ Basic ☒ Advanced

Configure network security group \* (new) nsg-1 Create new

Delete NIC when VM is deleted ⓘ ☒

Enable accelerated networking ⓘ ☐

The selected VM size does not support accelerated networking

Load balancing

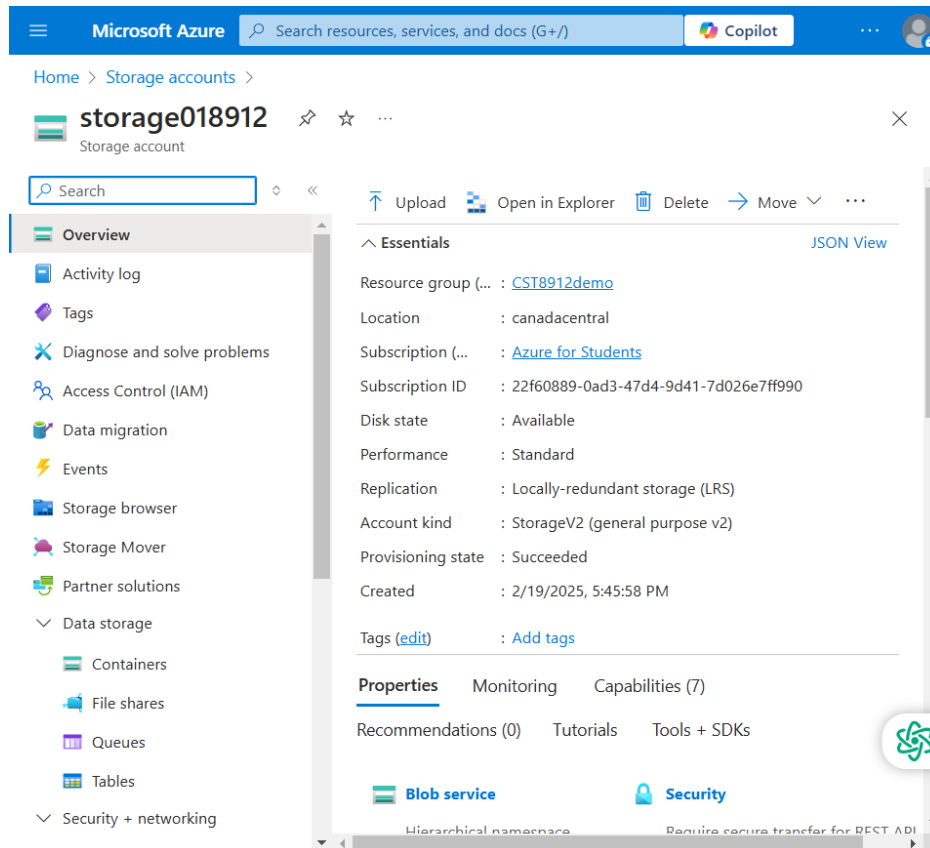
< Previous Next : Management > Review + create Give feedback

https://portal.azure.com/#

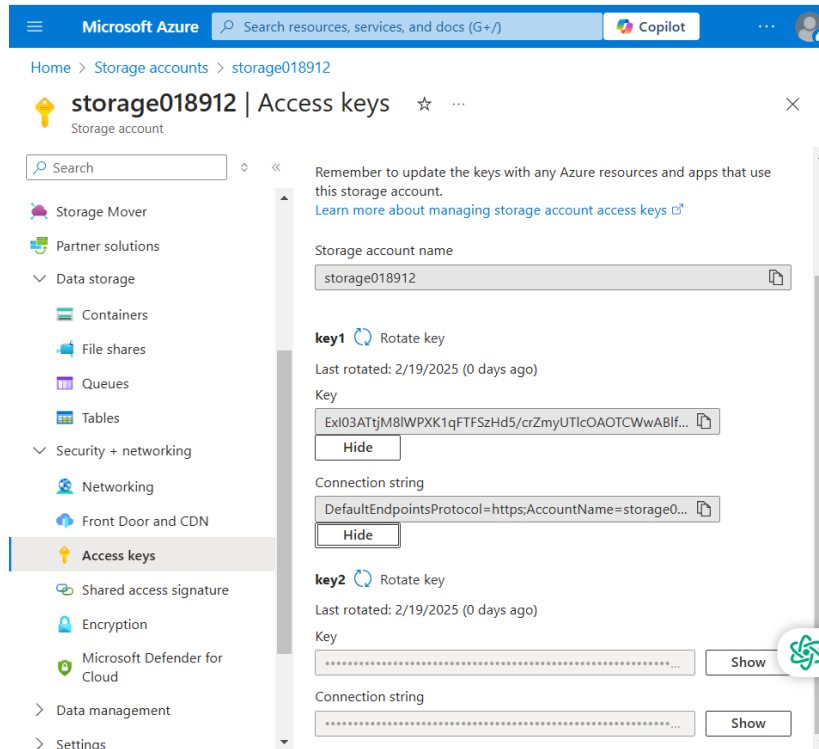
6. Leave the rest of the settings at the defaults and select Review + create.
7. Review the settings and select Create.

## Storage access key

1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select the storage account you created in the previous steps or your existing storage account.



3. In the Security + networking section of the storage account, select Access keys.
4. Select Show, then select copy on the Connection string for key1.



## Add a blob container

1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select the storage account you created in the previous steps.
3. In the Data storage section, select Containers.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Storage accounts > storage018912

### storage018912 | Containers

Storage account

Search

+ Container Change access level Restore containers

Search containers by prefix

Show deleted containers

Name	Last modified	Anonymous access l.
<input type="checkbox"/> \$logs	2/19/2025, 5:46:18 PM	Private

Overview  
Activity log  
Tags  
Diagnose and solve problems  
Access Control (IAM)  
Data migration  
Events  
Storage browser  
Storage Mover  
Partner solutions  
Data storage  
Containers  
File shares  
Queues  
Tables  
Security + networking

4. Select + Container to create a new container.
5. Enter container in Name and select Private (no anonymous access) under Public access level.



Microsoft Azure Search resources, services, and docs (G+ /) Copilot

Home > Storage accounts > storage018912

**storage018912 | Containers**  
Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Storage Mover
- Partner solutions
- ▼ Data storage
- Containers**
- File shares
- Queues
- Tables
- ▼ Security + networking

**New container**

Name \*  
container8912demo ✓

Anonymous access level ⓘ  
Private (no anonymous access) ▼

**i** The access level is set to private because anonymous access is disabled on this storage account.

▼ Advanced

**Create** Give feedback ⓘ

6. Select Create.

### Test connectivity to private endpoint

1. In the search box at the top of the portal, enter Virtual machine. Select Virtual machines in the search results.
2. Select 8912-VM1.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > CST8912demo >

## 8912-VM1

Virtual machine

Search Help me copy this VM in any region

**Overview**

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

**Essentials** [JSON View](#)

Resource group [\(move\)](#)  
[CST8912demo](#)

Status  
**Running**

Location  
Canada Central

Subscription [\(move\)](#)  
[Azure for Students](#)

Subscription ID  
22f60889-0ad3-47d4-9d41-7d026e7ff990

Operating system  
Windows (Windows Server 2022 Datacenter Azure Edition)

Size  
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address  
-

Virtual network/subnet  
[8912-vnet1/Subnet-1-8912](#)

DNS name

3. In Operations, select Bastion.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > CST8912demo > 8912-VM1

## 8912-VM1 | Bastion

Virtual machine

Search

**Overview**

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Bastion**
- Windows Admin Center
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Auto-shutdown

Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)

Using Bastion: **Bastion8912**

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

**Connection Settings**

Keyboard Language ⓘ  
English (US)

Authentication Type ⓘ  
VM Password

Username ⓘ

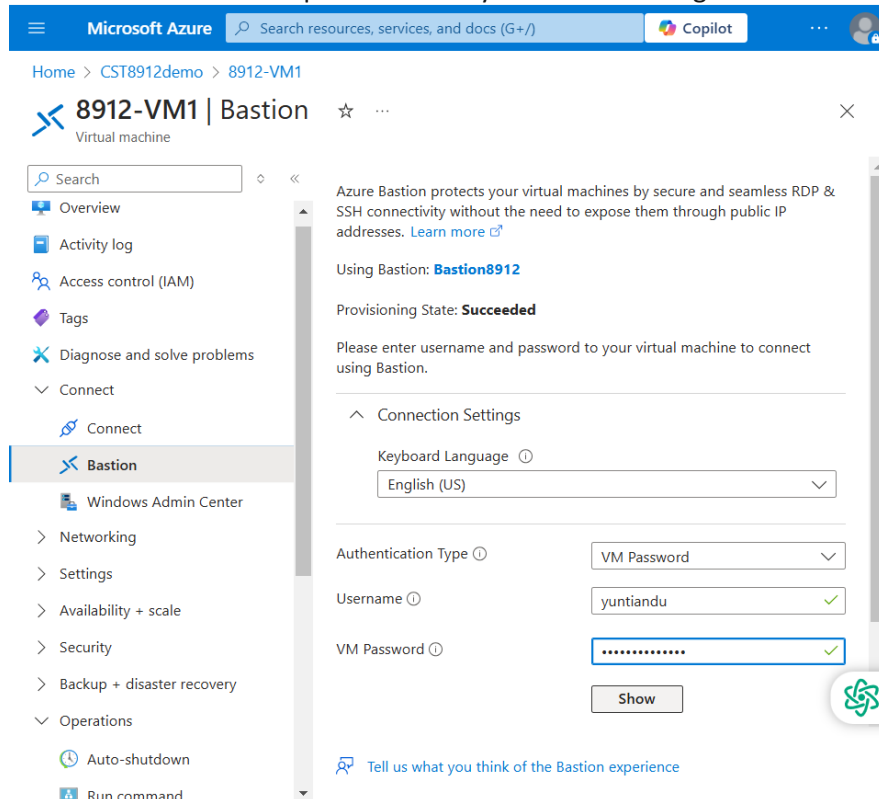
VM Password ⓘ

Show

[Tell us what you think of the Bastion experience](#)

<https://go.microsoft.com/fwlink/p/?linkid=2206313>

4. Enter the username and password that you entered during the virtual machine creation.

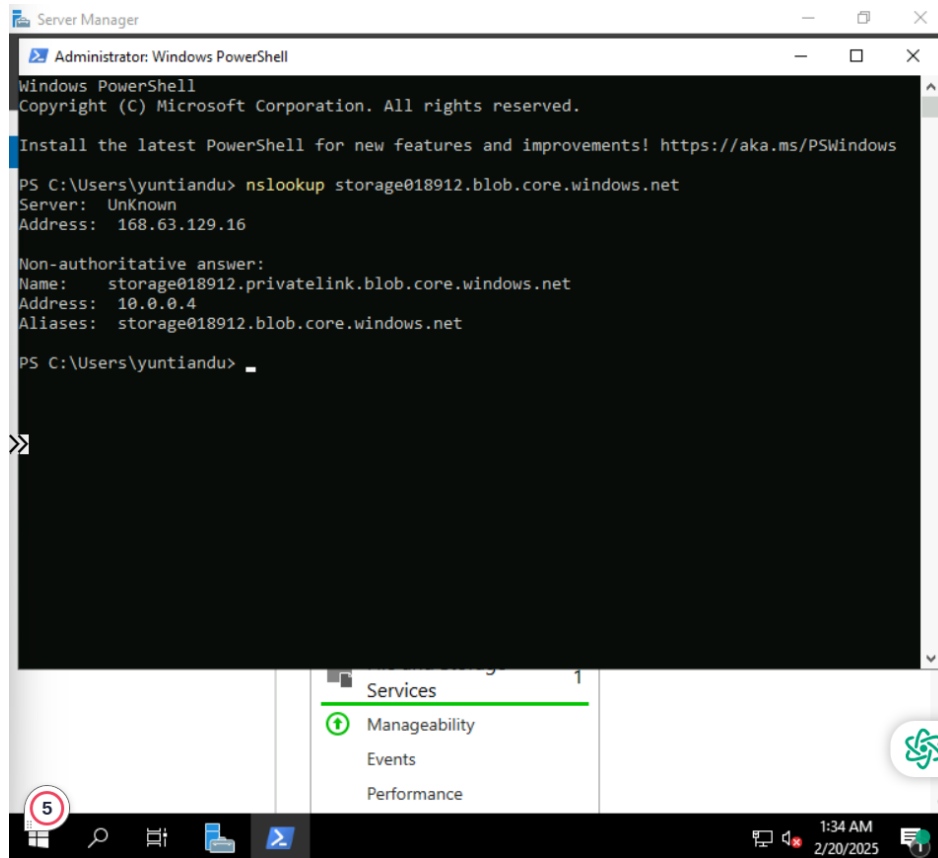


5. Select Connect.
6. Open Windows PowerShell on the server after you connect.
7. Enter nslookup <storage-account-name>.blob.core.windows.net. Replace <storage-account-name> with the name of the storage account you created in the previous steps. The following example shows the output of the command.

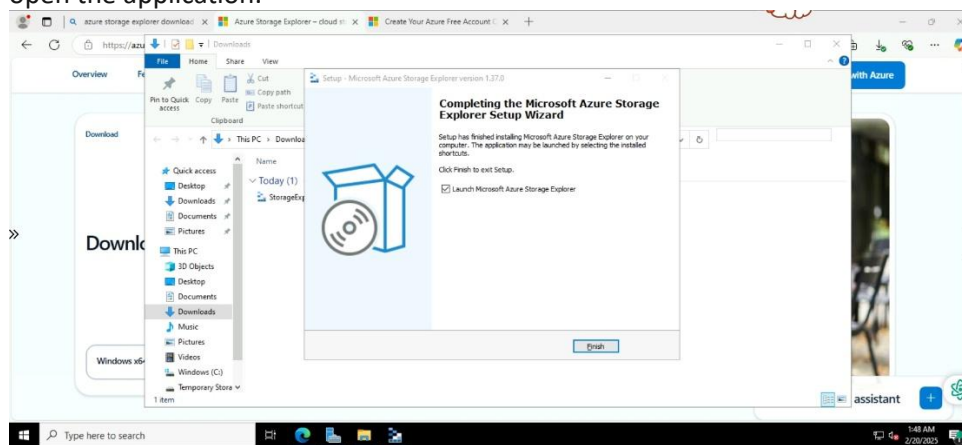
Server: UnKnown  
Address: 168.63.129.16

Non-authoritative answer:  
Name: storage1.privatelink.blob.core.windows.net  
Address: 10.0.0.10  
Aliases: mystorageaccount.blob.core.windows.net

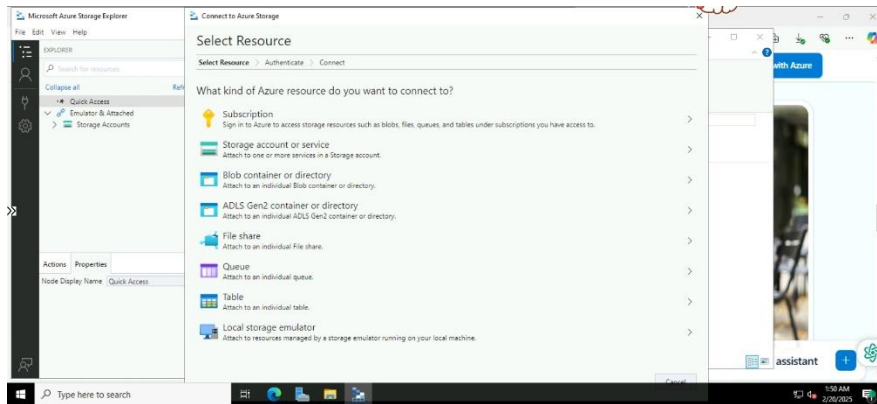
A private IP address of 10.0.0.10 is returned for the storage account name. This address is in Subnet-1-8912 subnet of 8912-vnet virtual network you created previously.



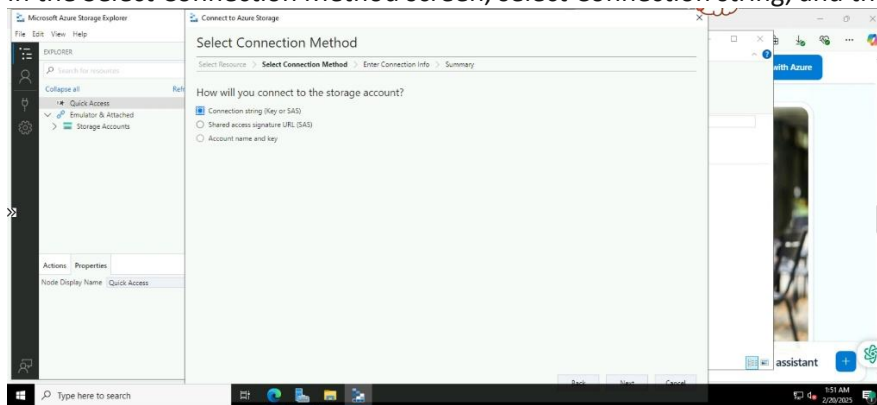
8. Install Microsoft Azure Storage Explorer on the virtual machine.
9. Select Finish after the Microsoft Azure Storage Explorer is installed. Leave the box checked to open the application.



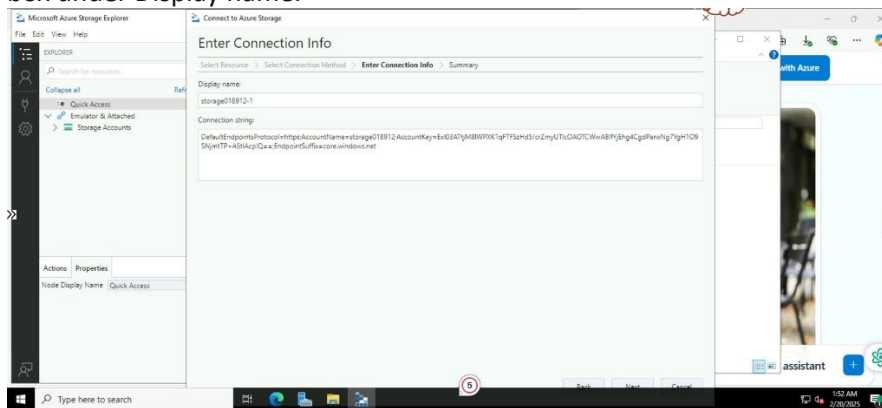
10. Select the Power plug symbol to open the Select Resource dialog box in the left-hand toolbar.



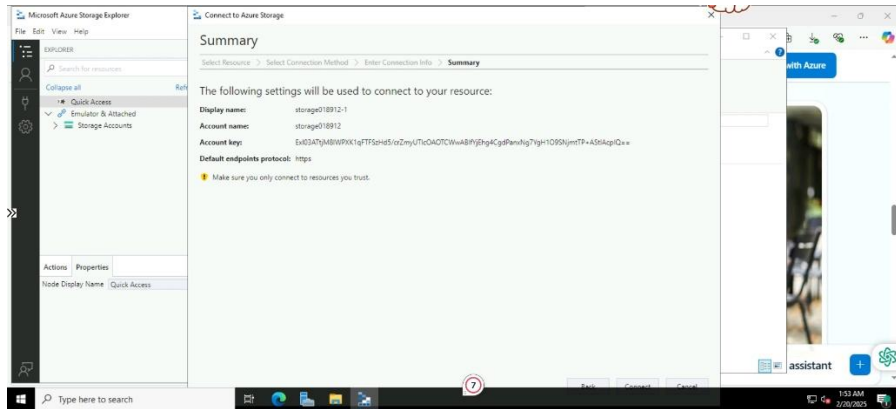
11. In Select Resource , select Storage account or service to add a connection in Microsoft Azure Storage Explorer to your storage account that you created in the previous steps.
12. In the Select Connection Method screen, select Connection string, and then Next.



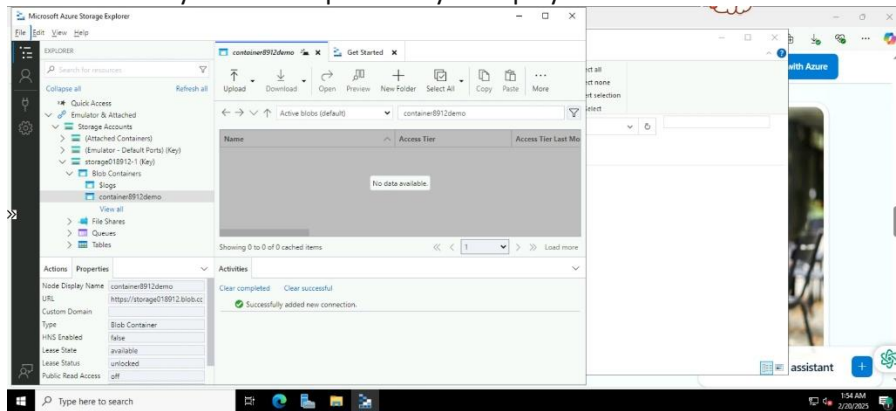
13. In the box under Connection String, paste the connection string from the storage account you copied in the previous steps. The storage account name automatically populates in the box under Display name.



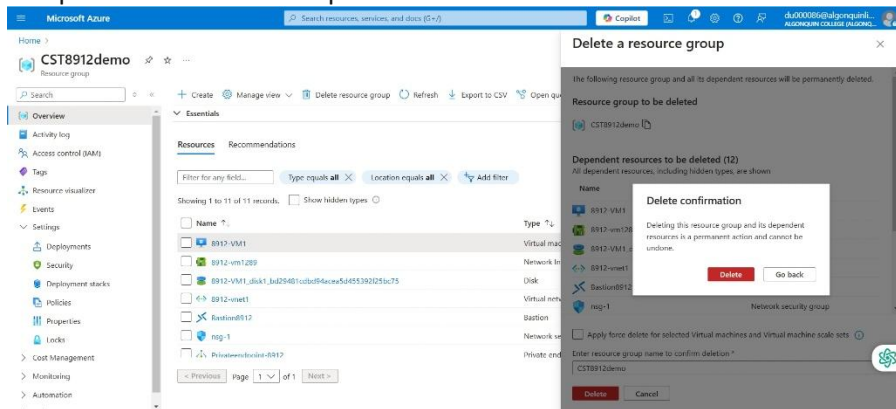
14. Select Next.
15. Verify the settings are correct in Summary.
16. Select Connect



17. Select your storage account from the Storage Accounts in the explorer menu.
18. Expand the storage account and then Blob Containers.
19. The container you created previously is displayed.



- 20.
21. Close the connection to 8912-VM1.
22. Clean all the resources created during the lab and document all the steps using screenshots and paste that in the lab report.



## References

None.