

CST8912 – Cloud Solution Architecture

Graded Lab Activity #6

Lab 6

CST8912_011

Satyam Panseriya

ID :- 41128392

Feb 23, 2025

Submitted to : Prof. Tanishq Bansal

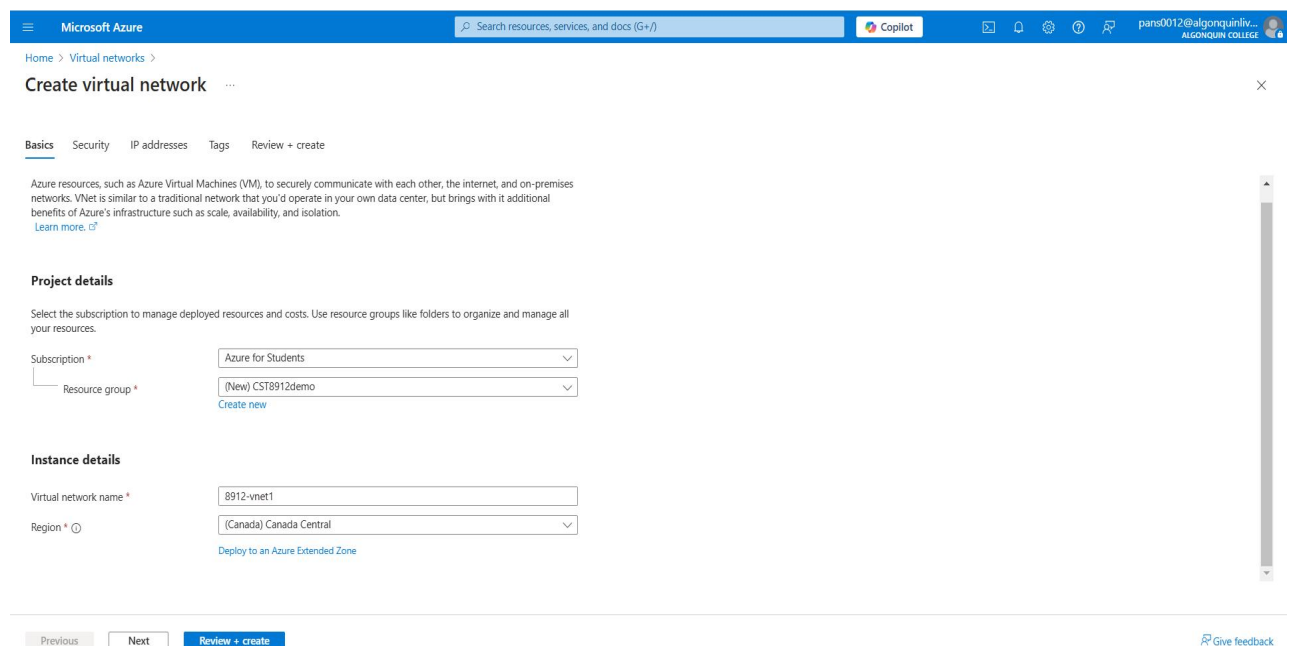
Introduction:

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.

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



The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal, specifically the 'Basics' tab. The page header includes the Microsoft Azure logo, a search bar, and the user's profile (pans0012@algonquinliv...). The main heading is 'Create virtual network'. Below this, there are tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'Basics' tab is active, showing a description of VNet and a 'Project details' section. The 'Project details' section includes a 'Subscription' dropdown set to 'Azure for Students' and a 'Resource group' dropdown set to '(New) CST8912demo'. Below these is a 'Create new' link. The 'Instance details' section includes a 'Virtual network name' text box with '8912-vnet1' and a 'Region' dropdown set to '(Canada) Canada Central'. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

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](#)

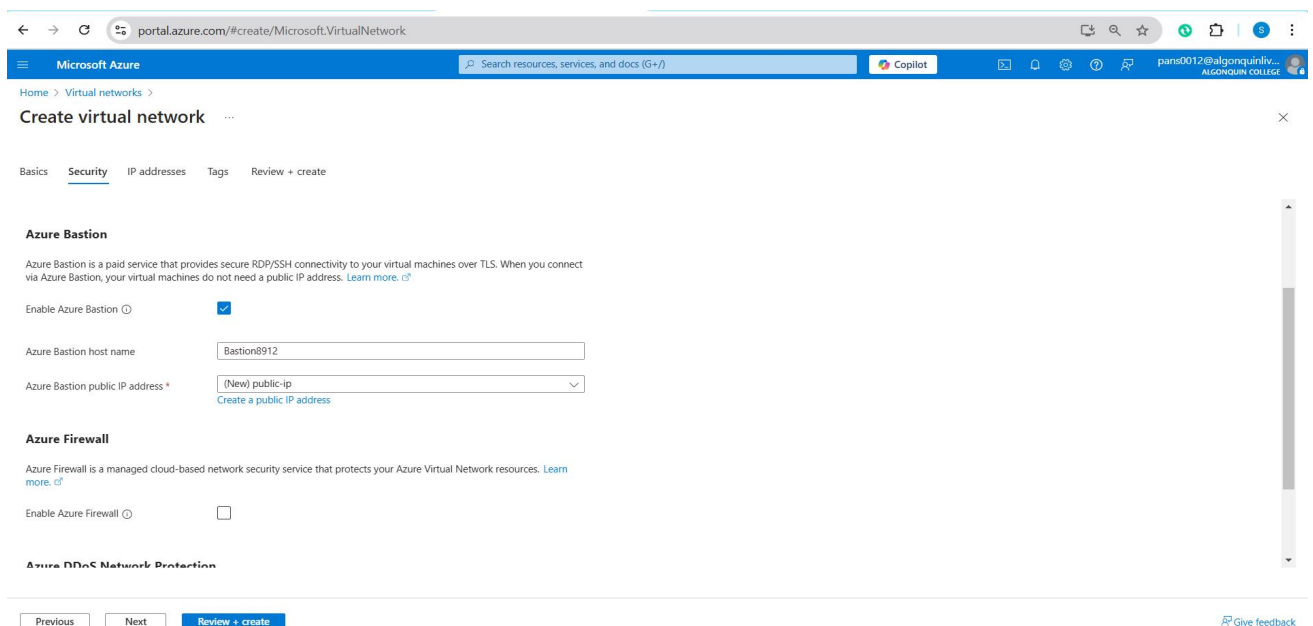
[Give feedback](#)

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

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 Create a public IP address . Enter public-ip in Name. Select OK .



The screenshot shows the 'Create virtual network' page in the Azure portal, specifically the 'Security' tab. The 'Azure Bastion' section is expanded, showing the following configuration:

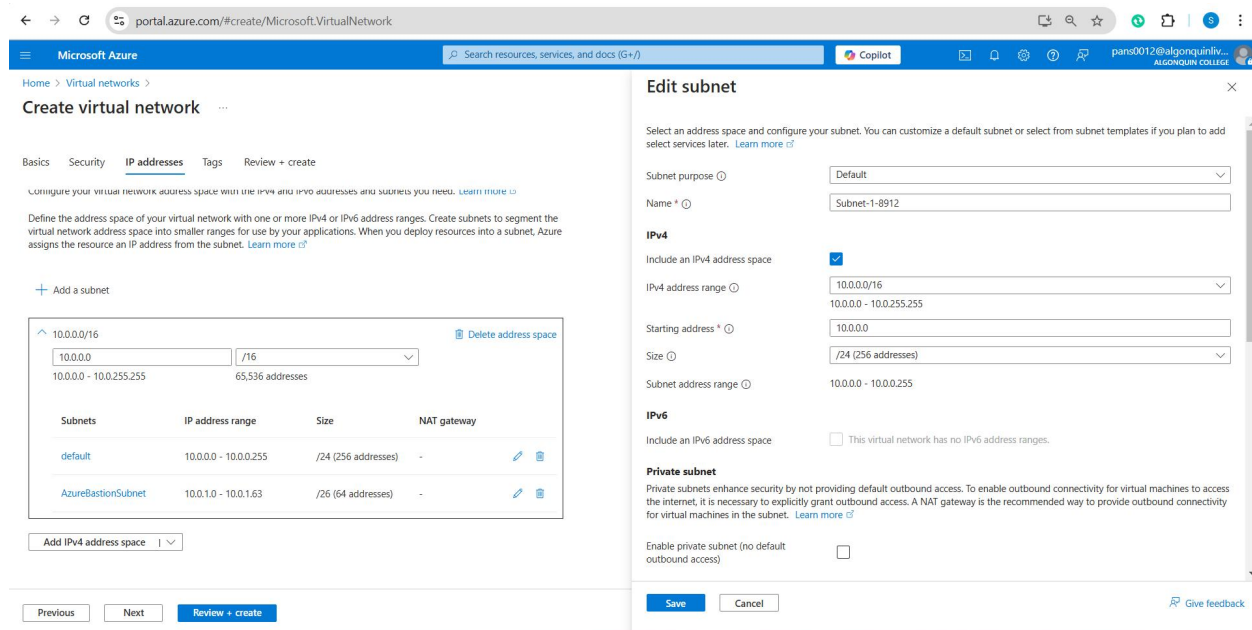
- Enable Azure Bastion:** Checked (checkbox).
- Azure Bastion host name:** Bastion8912
- Azure Bastion public IP address:** (New) public-ip (with a link to 'Create a public IP address').

The 'Azure Firewall' section is also visible, with 'Enable Azure Firewall' unchecked. At the bottom, there are navigation buttons: 'Previous', 'Next', and 'Review + create'.

7. Select Next to proceed to the IP Addresses tab.
8. In the address space box in Subnets, select the default subnet.
9. In Edit subnet, enter or select the following information:

Setting	Value
Subnet template	Leave the default Default .

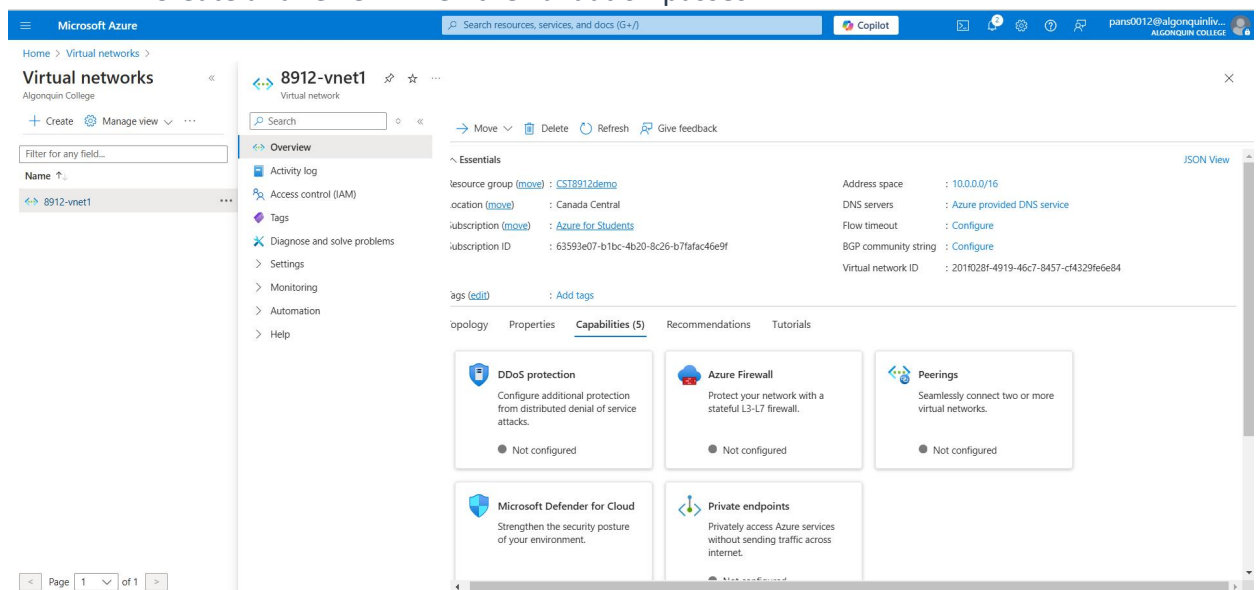
Name	Subnet-1-8912
IPv4 address range	Leave 10.0.0.0/16.
Starting address	Leave the default of 10.0.0.0.
Subnet size	Leave the default of /24(256 addresses).



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Create virtual network' wizard is visible, with the 'IP addresses' tab selected. It shows a table of subnets with columns for Name, IP address range, Size, and NAT gateway. The 'default' subnet is highlighted. On the right, the 'Edit subnet' dialog is open, showing the configuration for 'Subnet-1-8912'. The 'IPv4' section is expanded, showing the 'Include an IPv4 address space' checkbox checked, and the 'IPv4 address range' set to '10.0.0.0/16'. The 'Starting address' is '10.0.0.0' and the 'Size' is '/24 (256 addresses)'. The 'IPv6' section is collapsed, and the 'Private subnet' checkbox is unchecked.

10. Select save

11. Create and review when the validation passes

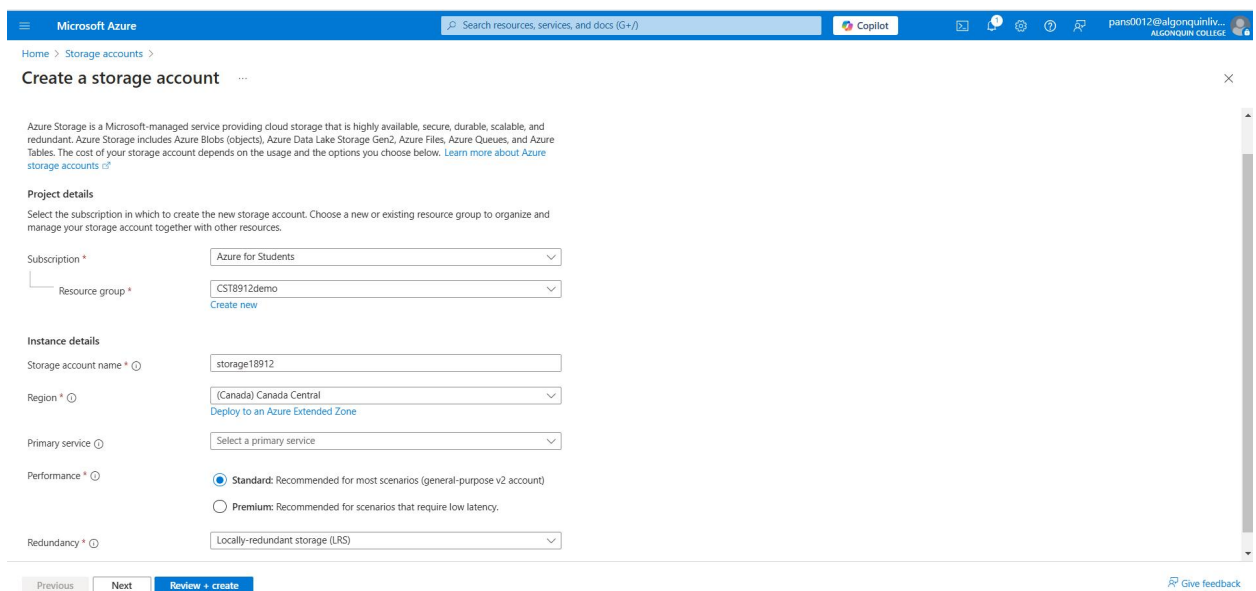


The screenshot shows the Microsoft Azure portal interface for the '8912-vnet1' virtual network. The 'Overview' tab is selected, showing the 'Essentials' section with details about the resource group, location, subscription, and address space. The 'Capabilities' section is expanded, showing five capabilities: 'DDoS protection', 'Azure Firewall', 'Peering', 'Microsoft Defender for Cloud', and 'Private endpoints'. Each capability has a 'Not configured' status.

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

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure for Students

Resource group * CST8912demo [Create new](#)

Instance details

Storage account name * storage18912

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

Primary service * Select a primary service

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

Redundancy * Locally-redundant storage (LRS)

Previous Next Review + create

[Give feedback](#)

4. Select review
5. Select create

Microsoft Azure

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

Copilot

Home >

storage18912_1739994573610 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name: storage18912_1739994573610
Subscription: Azure for Students
Resource group: CST8912demo

Start time: 19/2/2025, 2:50:02 pm
Correlation ID: 78086270-c7a7-4abc-9411-f9b3fd160a

Deployment details

Resource	Type	Status	Operation details
storage18912/default	Microsoft.Storage/storageAccounts/filese...	OK	Operation details
storage18912/default	Microsoft.Storage/storageAccounts/blob...	OK	Operation details
storage18912	Microsoft.Storage/storageAccounts	OK	Operation details

Next steps

[Go to resource](#)

Give feedback

Tell us about your experience with deployment

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 >](#)

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.

Microsoft Azure

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

Copilot

Home > Storage accounts > storage18912

Storage accounts

Algonquin College

+ Create Restore ...

Filter for any field...

Name ↑

storage18912

storage18912 | Networking

Storage account

Search

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

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Firewalls and virtual networks

Private endpoint connections

Custom domain

Save Discard Refresh Give feedback

Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

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](#)

Network Routing

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.

Routing preference *

☒ Microsoft network routing ☐ Internet routing

Publish route-specific endpoints

☐ Microsoft network routing

☐ Internet routing

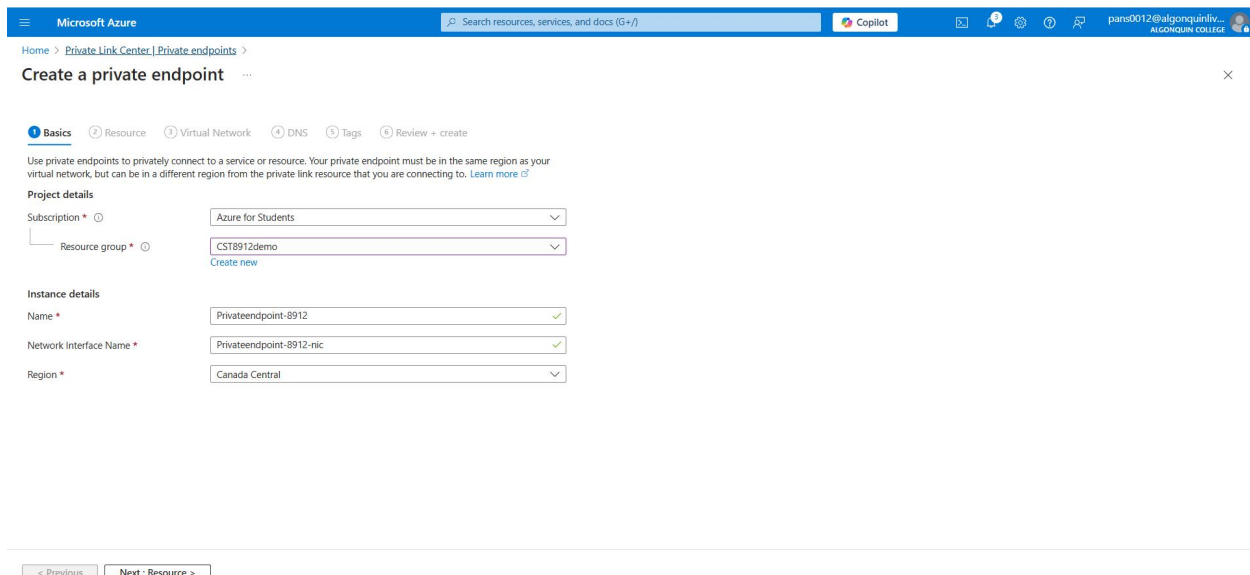
Page 1 of 1

Step 3

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 private-endpoint-nic .
Region	Canada Central

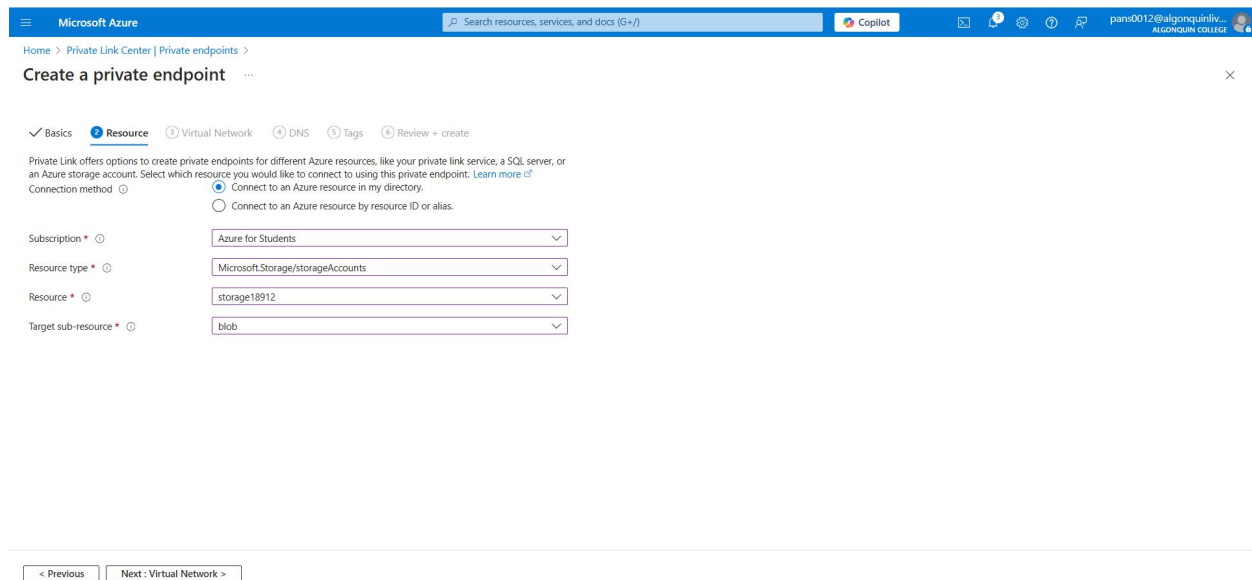


The screenshot shows the 'Create a private endpoint' page in the Microsoft Azure portal, specifically the 'Basics' tab. The page header includes the Microsoft Azure logo, a search bar, and the user's profile. The breadcrumb trail is 'Home > Private Link Center > Private endpoints >'. The page title is 'Create a private endpoint'. Below the title is a progress bar with five steps: 1. Basics (selected), 2. Resource, 3. Virtual Network, 4. DNS, and 5. Tags. A description states: '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](#)'. The 'Project details' section contains two dropdown menus: 'Subscription *' (set to 'Azure for Students') and 'Resource group *' (set to 'CST8912demo'). Below this is a 'Create new' link. The 'Instance details' section contains three dropdown menus: 'Name *' (set to 'Privateendpoint-8912'), 'Network interface Name *' (set to 'Privateendpoint-8912-nic'), and 'Region *' (set to 'Canada Central'). At the bottom of the page are two buttons: '< Previous' and 'Next: Resource >'. The 'Next: Resource >' button is highlighted.

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 **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 ①

☒ Connect to an Azure resource in my directory.

☐ Connect to an Azure resource by resource ID or alias.

Subscription * ② Azure for Students

Resource type * ② Microsoft.Storage/storageAccounts

Resource * ② storage18912

Target sub-resource * ② blob

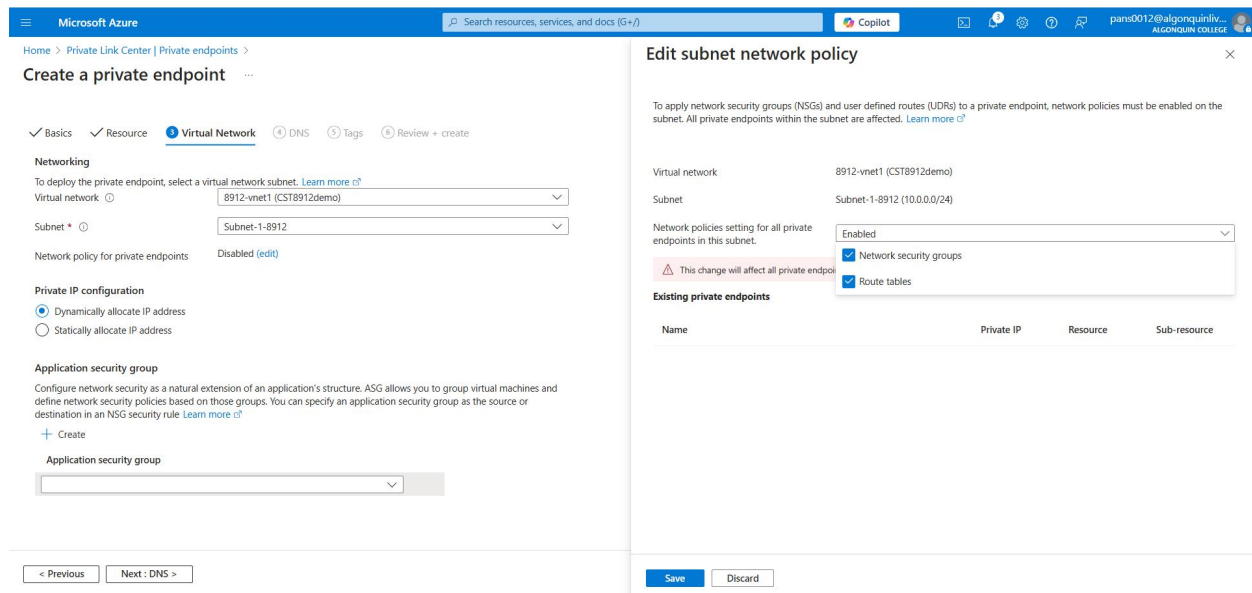
< Previous Next: Virtual Network >

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</p>

	in this subnet pull-down. Select Save.
Private IP configuration	Select Dynamically allocate IP address.



Microsoft Azure

Home > Private Link Center | Private endpoints >

Create a private endpoint

✓ Basics ✓ Resource **Virtual Network** DNS Tags Review + create

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: Disabled (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 >

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

☒ Network security groups

☒ Route tables

Existing private endpoints

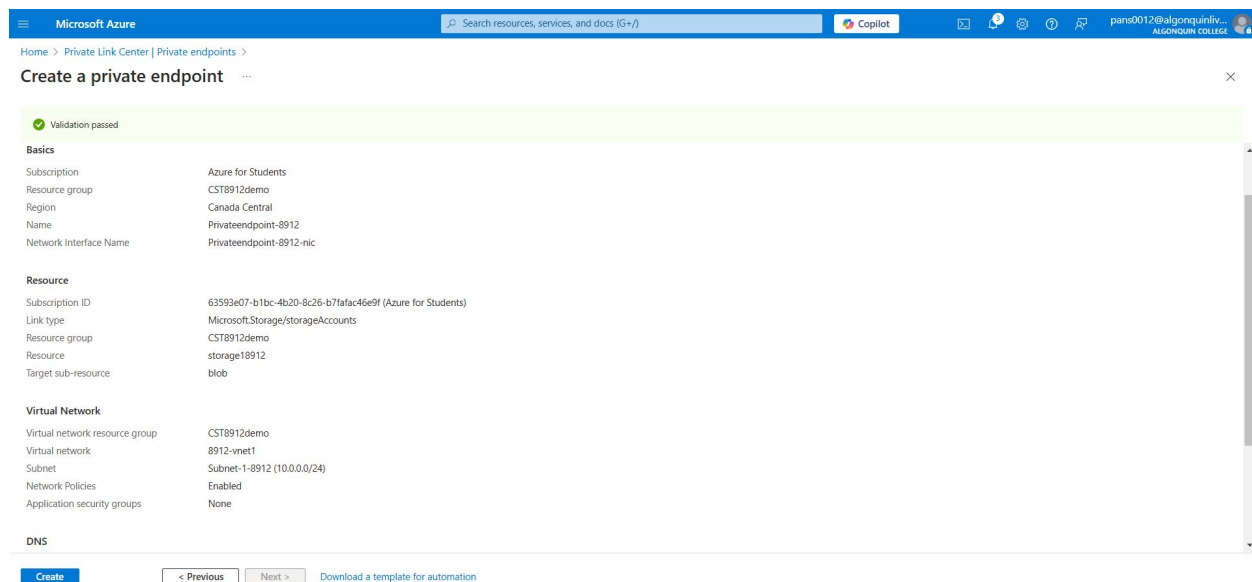
Name	Private IP	Resource	Sub-resource
------	------------	----------	--------------

Save Discard

8. Select Next: DNS.

9. Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

10. Select Create.



Microsoft Azure

Home > Private Link Center | Private endpoints >

Create a private endpoint

✓ Validation passed

Basics

Subscription: Azure for Students

Resource group: CST8912demo

Region: Canada Central

Name: Privateendpoint-8912

Network Interface Name: Privateendpoint-8912-nic

Resource

Subscription ID: 63593e07-b1bc-4b20-8c26-b7afac46e9f (Azure for Students)

Link type: Microsoft.Storage/storageAccounts

Resource group: CST8912demo

Resource: storage18912

Target sub-resource: blob

Virtual Network

Virtual network resource group: CST8912demo

Virtual network: 8912-vnet1

Subnet: Subnet-1-8912 (10.0.0.0/24)

Network Policies: Enabled

Application security groups: None

DNS

Create < Previous Next > Download a template for automation

Step 4

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+/)

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

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 * CST8912demo

Create new

Instance details

Virtual machine name * 8912-VM1

Region * (Canada) Canada Central

Availability options No infrastructure redundancy required

Security type Standard

Image * Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

See all images | Configure VM generation

This image is compatible with additional security features. Click here to swap to the trusted launch security type.

VM architecture

Arm64

x64

< Previous Next : Disks > Review + create

Give feedback

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+/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

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

Virtual network * 8912-vnet1
[Create new](#)

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
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options ☐ None

< Previous | Next: Management > | **Review + create**

[Give feedback](#)

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

Microsoft Azure

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

Copilot

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20250219150858 | Overview

8912-VM1

Virtual machine

Search

Overview | Activity log | Access control (IAM) | Tags | Diagnose and solve problems

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback | CLI / PS

Help me copy this VM in any region

8912-VM1 virtual machine agent status is not ready. Troubleshoot the issue

Virtual machine

Computer name	8912-VM1
Operating system	Windows
VM generation	V2
VM architecture	x64
Agent status	Not Ready
Agent version	Unknown
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Azure Spot

Azure Spot	-
Azure Spot eviction policy	-

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	8912-vnet1/Subnet-1-8912
DNS name	-

Size

Size	Standard B1s
vCPUs	1
RAM	1 GiB

Source image details

Source image publisher	MicrosoftWindowsServer
Source image offer	WindowsServer
Source image plan	2022-datacenter-azure-edition

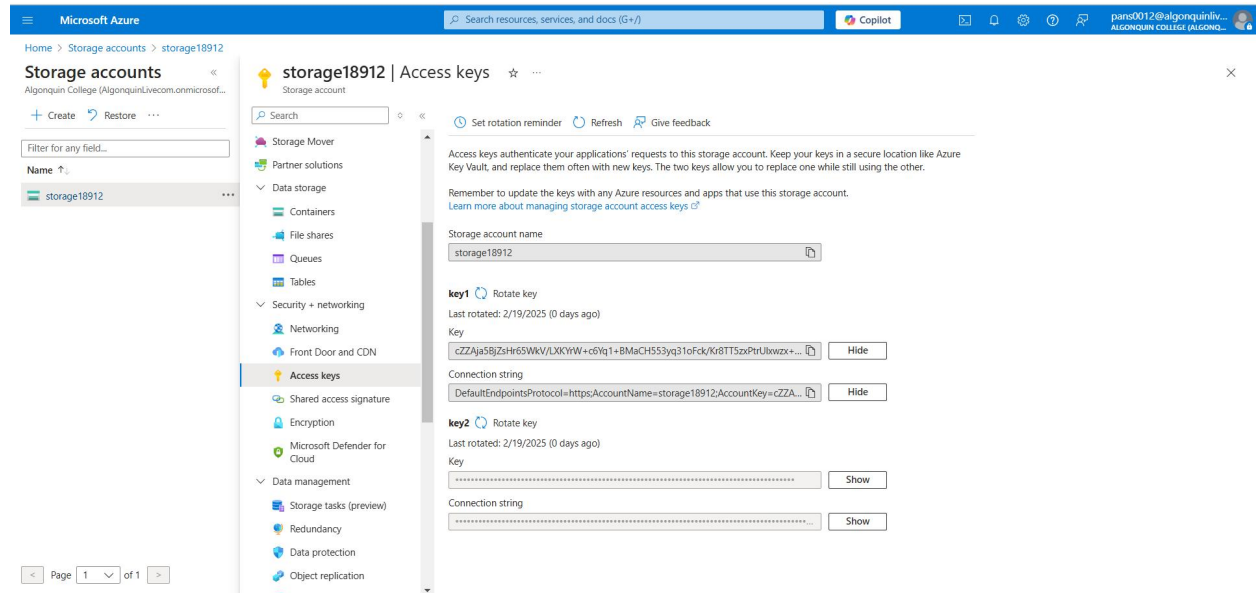
Disk

OS disk	8912-VM1_disk1_0ec79c50d3214dd9ad01448a374fd9e
---------	--

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.

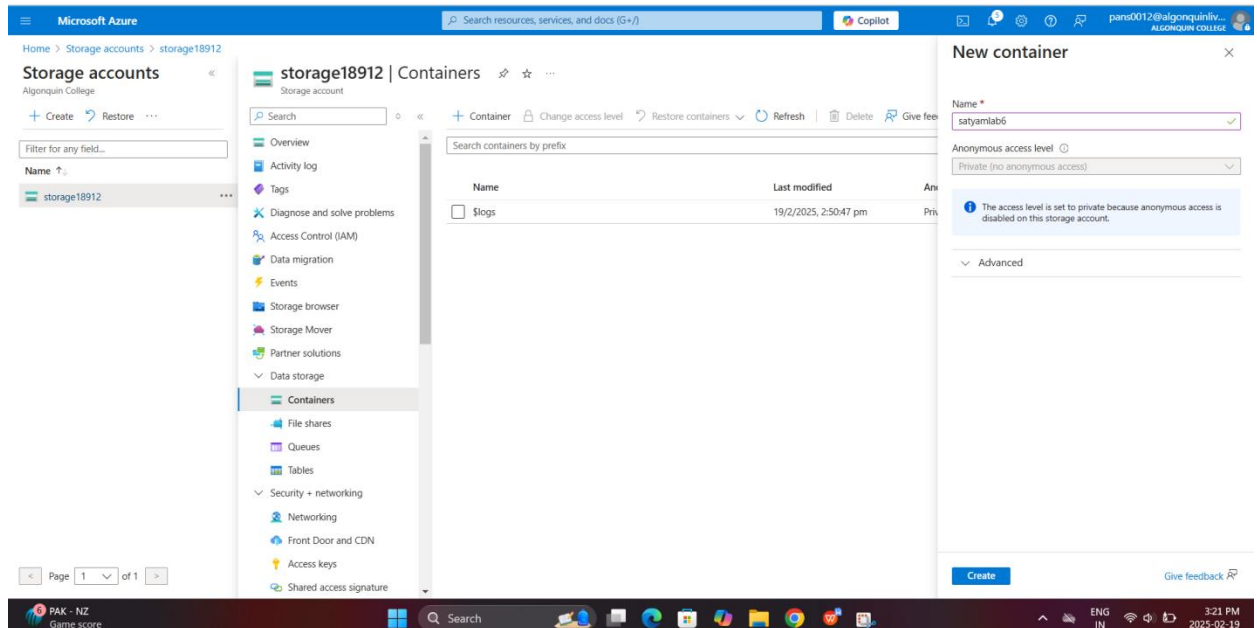
3. In the Security + networking section of the storage account, select Access keys.



4. Select Show, then select copy on the Connection string for key1.

Add a blob container

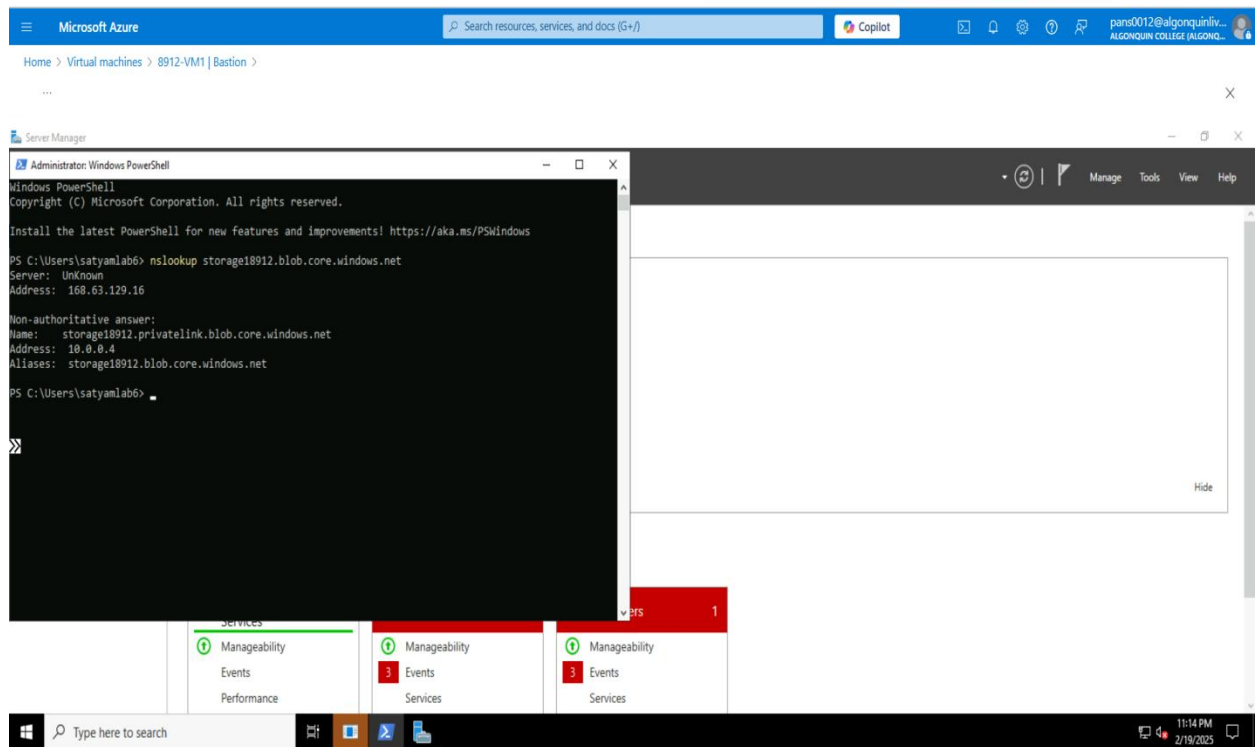
1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select the storage account you created in the previous steps.
3. In the Data storage section, select Containers.
4. Select + Container to create a new container.
5. Enter container in Name and select Private (no anonymous access) under Public access level.
6. Select Create.



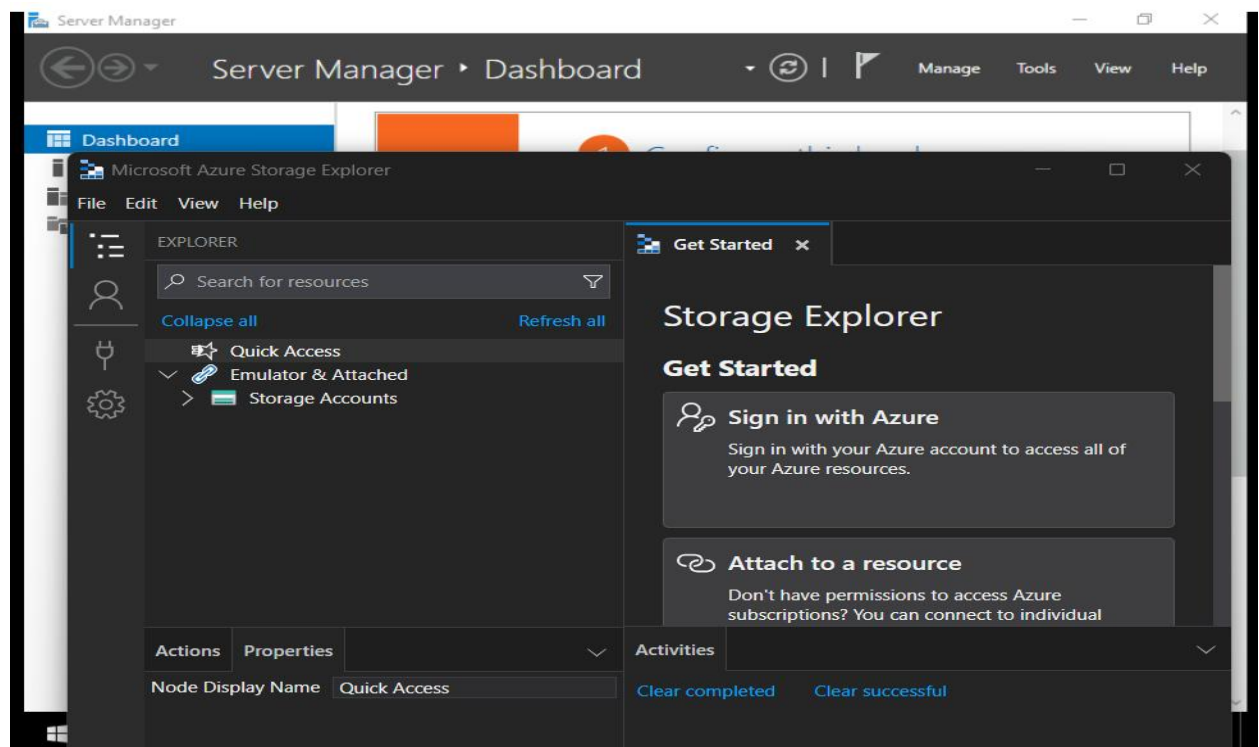
Test connectivity to private endpoint

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.
3. In Operations, select Bastion.
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

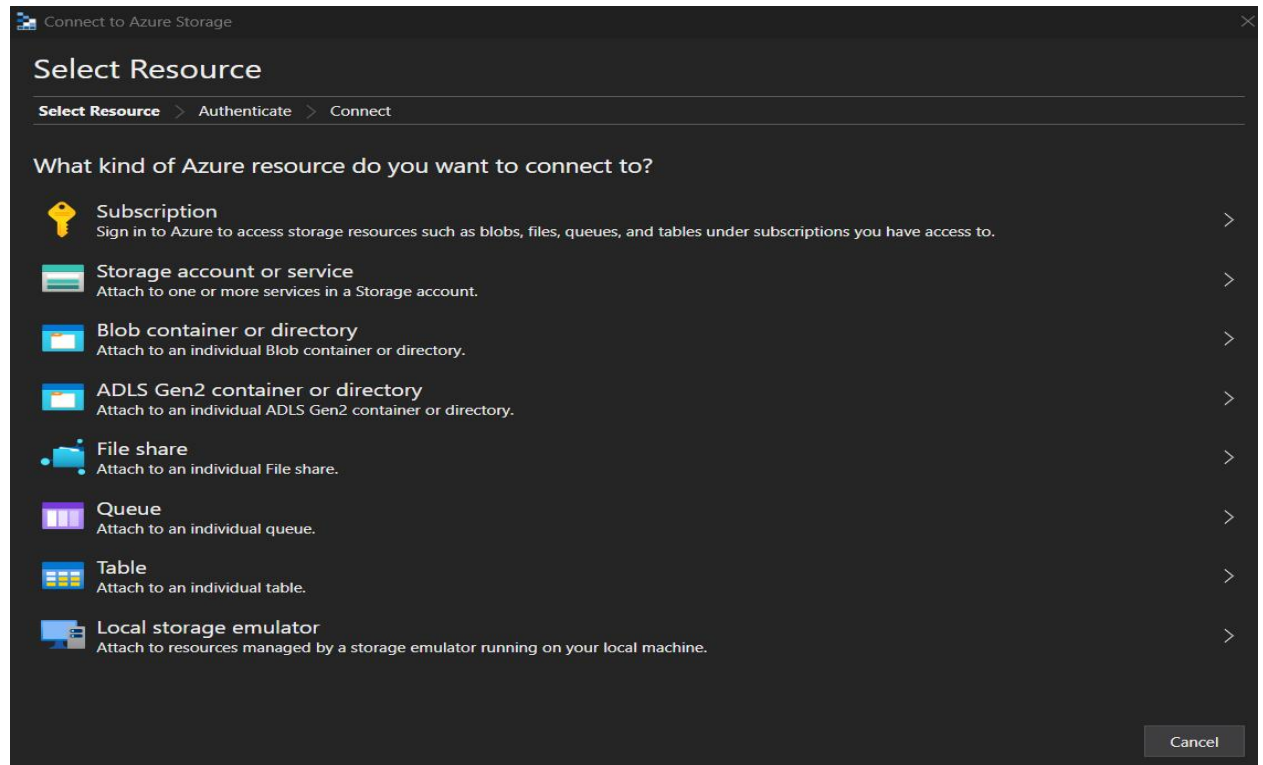
A private IP address of 10.0.0.10 is returned for the storage account name. This address is in Subnet-1-8912 subnet of 8912-vnet virtual network you created previously.



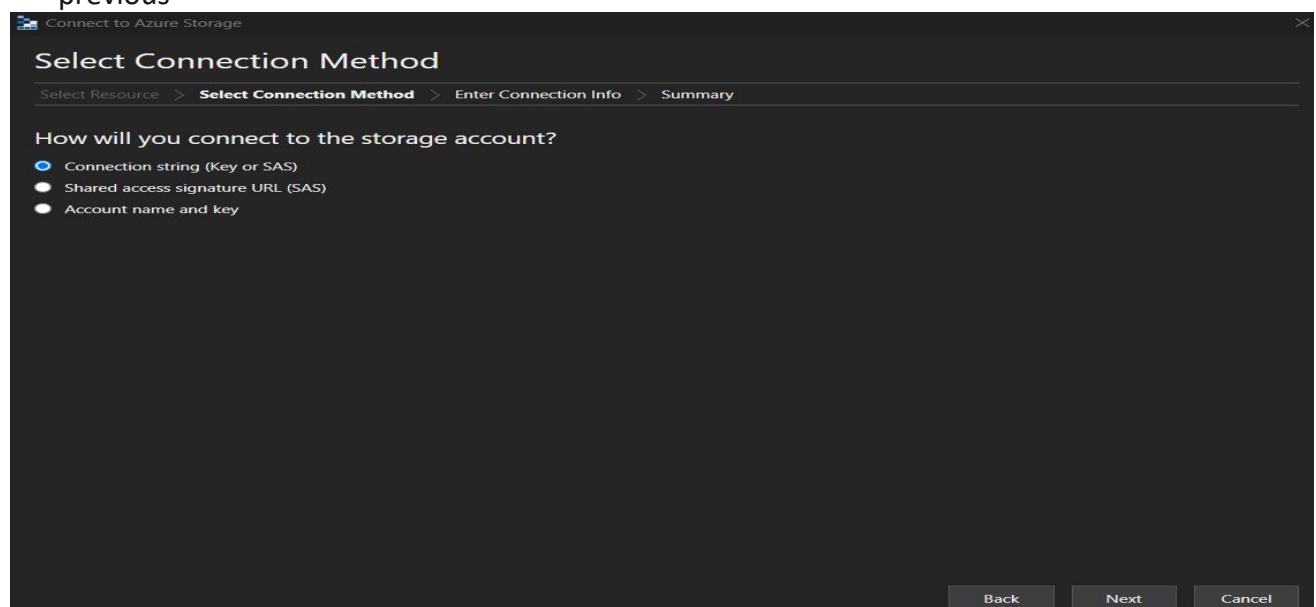
8. Install Microsoft Azure Storage Explorer on the virtual machine.
9. Select Finish after the Microsoft Azure Storage Explorer is installed. Leave the box checked to open the application.



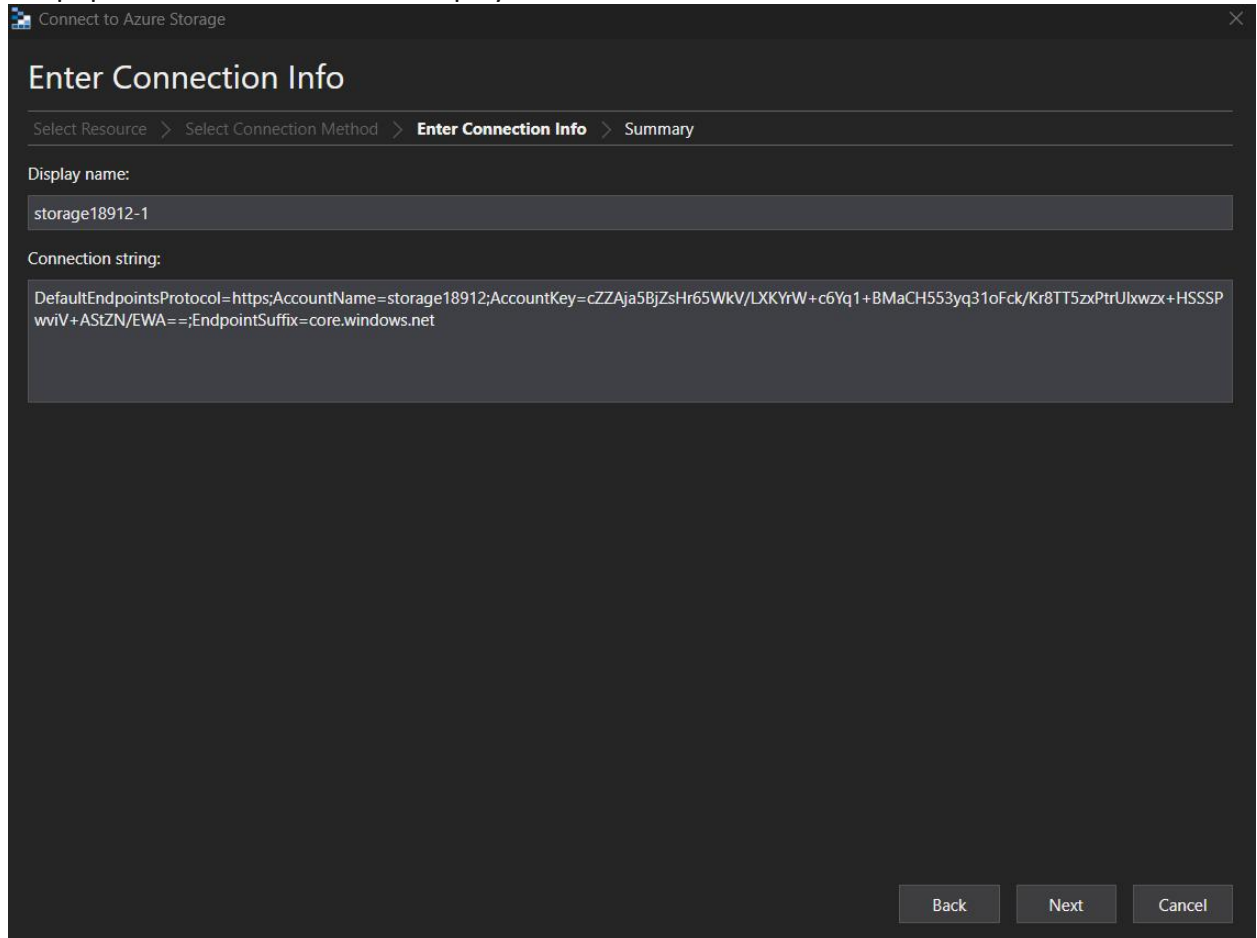
10. Select the Power plug symbol to open the Select Resource dialog box in the left-hand toolbar.



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



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.



The screenshot shows a dark-themed dialog box titled "Connect to Azure Storage". The main heading is "Enter Connection Info". Below the heading is a breadcrumb trail: "Select Resource > Select Connection Method > Enter Connection Info > Summary". The "Enter Connection Info" step is currently active. There are two input fields: "Display name:" with the value "storage18912-1" and "Connection string:" with a long, complex string. At the bottom right are three buttons: "Back", "Next", and "Cancel".

Connect to Azure Storage

Enter Connection Info

Select Resource > Select Connection Method > **Enter Connection Info** > Summary

Display name:

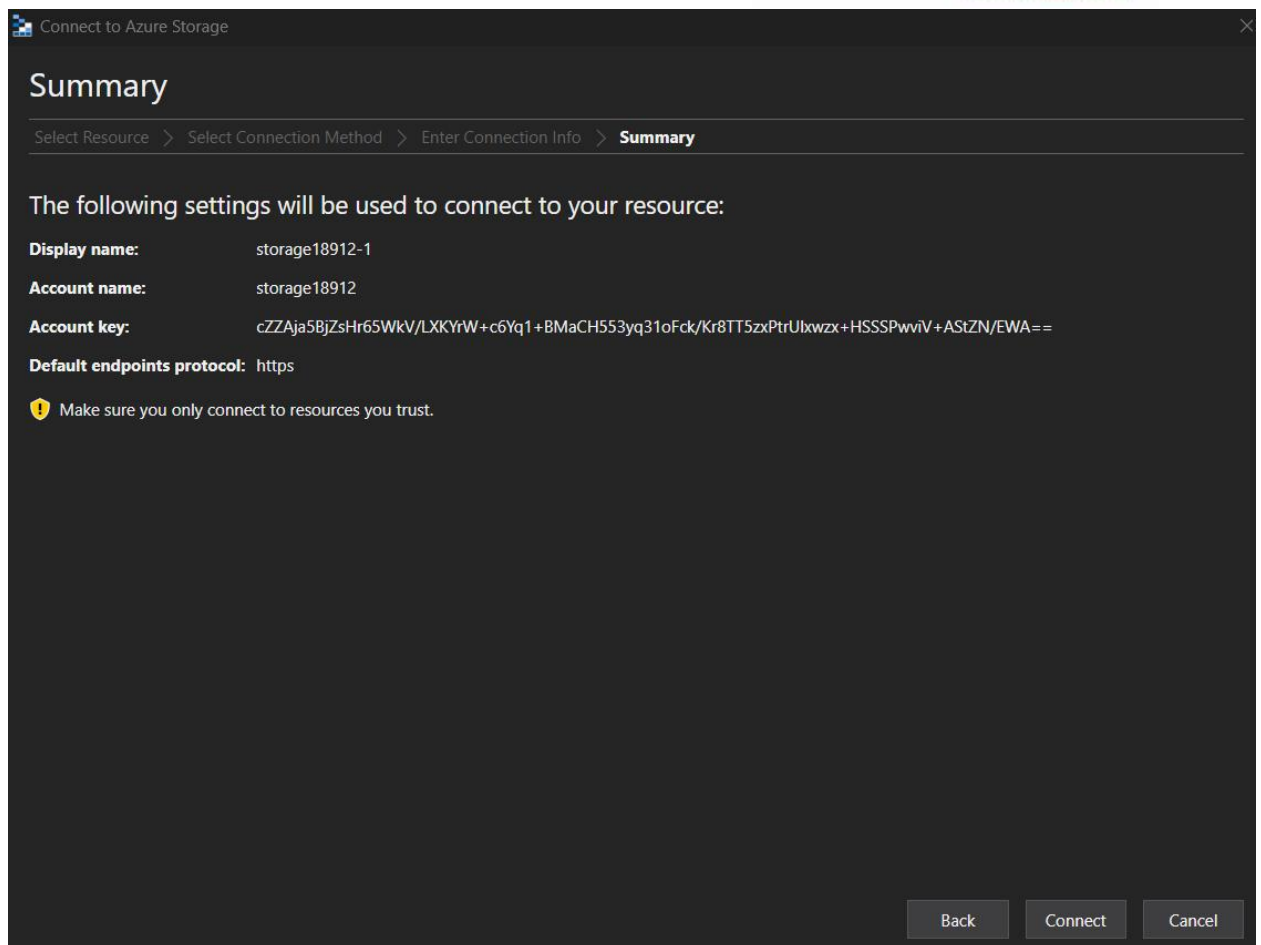
storage18912-1

Connection string:

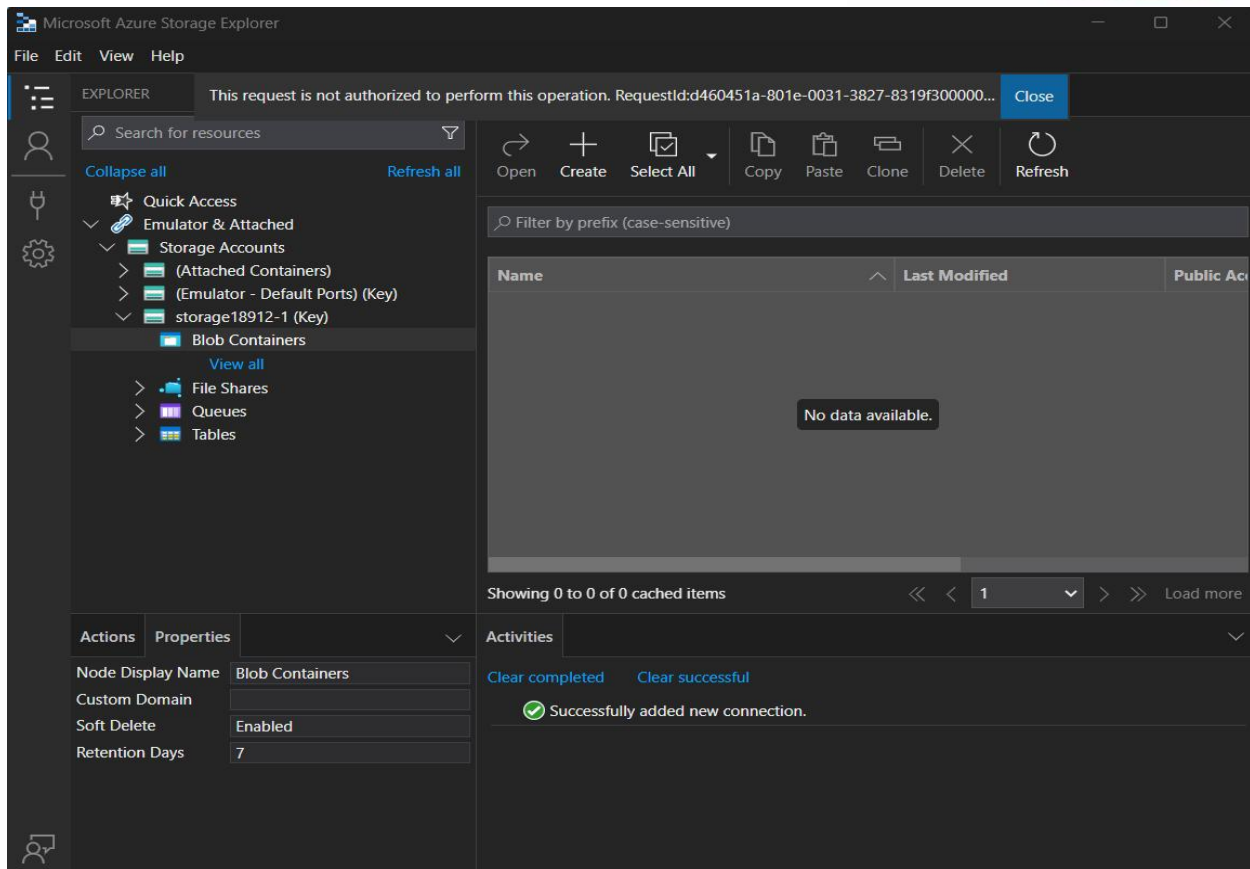
DefaultEndpointsProtocol=https;AccountName=storage18912;AccountKey=cZZAja5BjZsHr65WkV/LXKYrW+c6Yq1+BMaCH553yq31oFck/Kr8TT5zxPtrUlxwzx+HSSSPwviV+AStZN/EWA==;EndpointSuffix=core.windows.net

Back Next Cancel

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

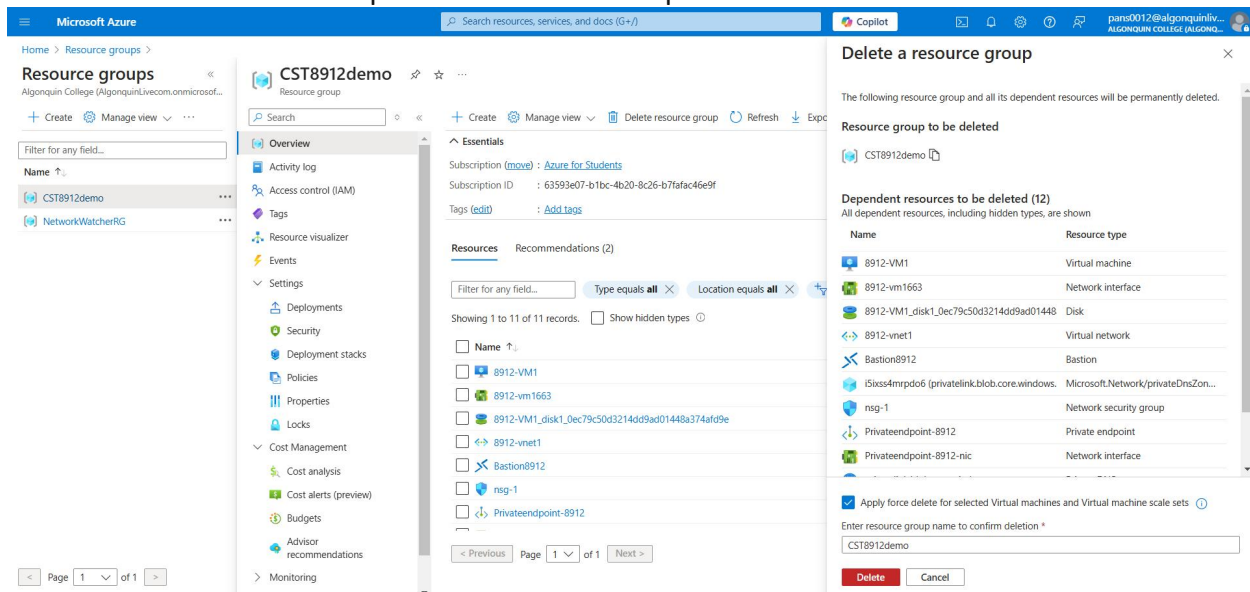


16. Select Connect
17. Select your storage account from the Storage Accounts in the explorer menu.
18. Expand the storage account and then Blob Containers.
19. The container you created previously is displayed.



20. Close the connection to 8912-VM1.

21. Clean all the resources created during the lab and document all the steps using screenshots and paste that in the lab report.



Conclusion of the Lab

We completed the setting of the Azure Private Link to allow the safe and private sharing of data between an Azure Virtual Network and Azure PaaS (Azure Storage). The lab discussed Private Endpoints, Virtual Network Configuration, Bastion Host Deployment, and Storage Account Security Enhancements as the main contents.

Challenges Faced & Solutions:

Bastion Connection Error: Finally, I checked Bastion deployment, VM status, NSG rules, and private endpoint configuration, and once everything was okay, the problem got resolved.

Storage Access Issues: I made sure that public access was disabled and also confirmed the private DNS resolution.