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.

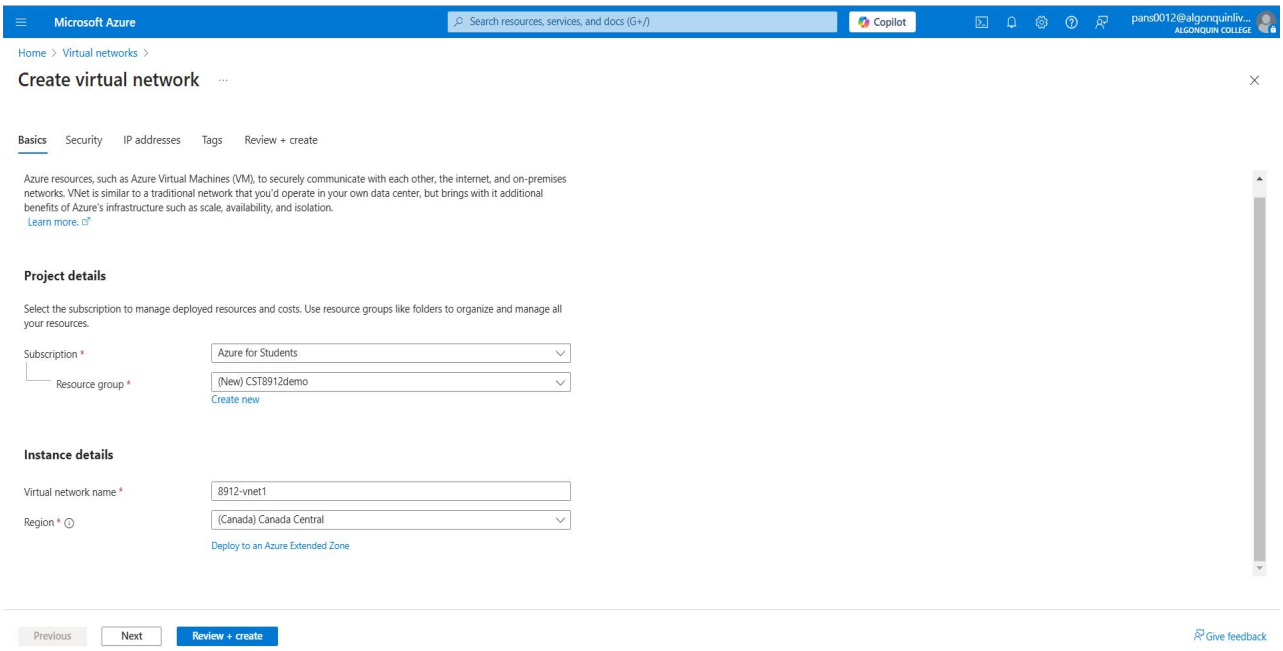
Create a Virtual network and Bastion Host

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

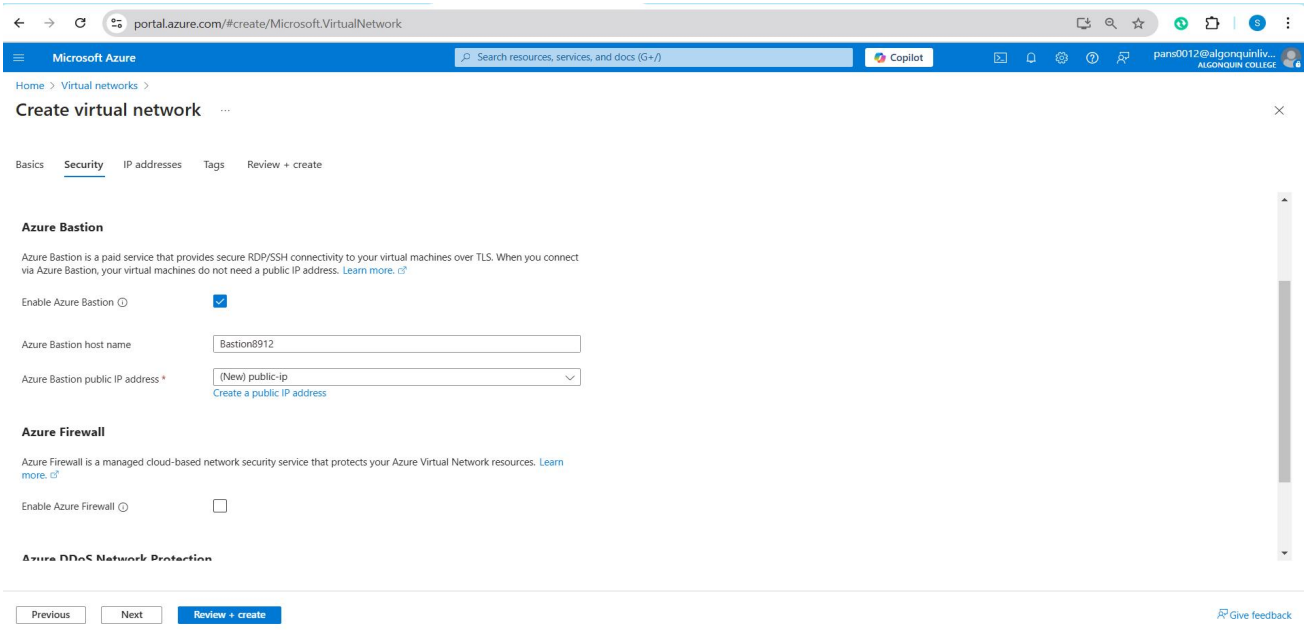


4. Select Next to proceed to the Security tab.
5. Select Enable Bastion in the Azure Bastion section of the Security tab.

   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:

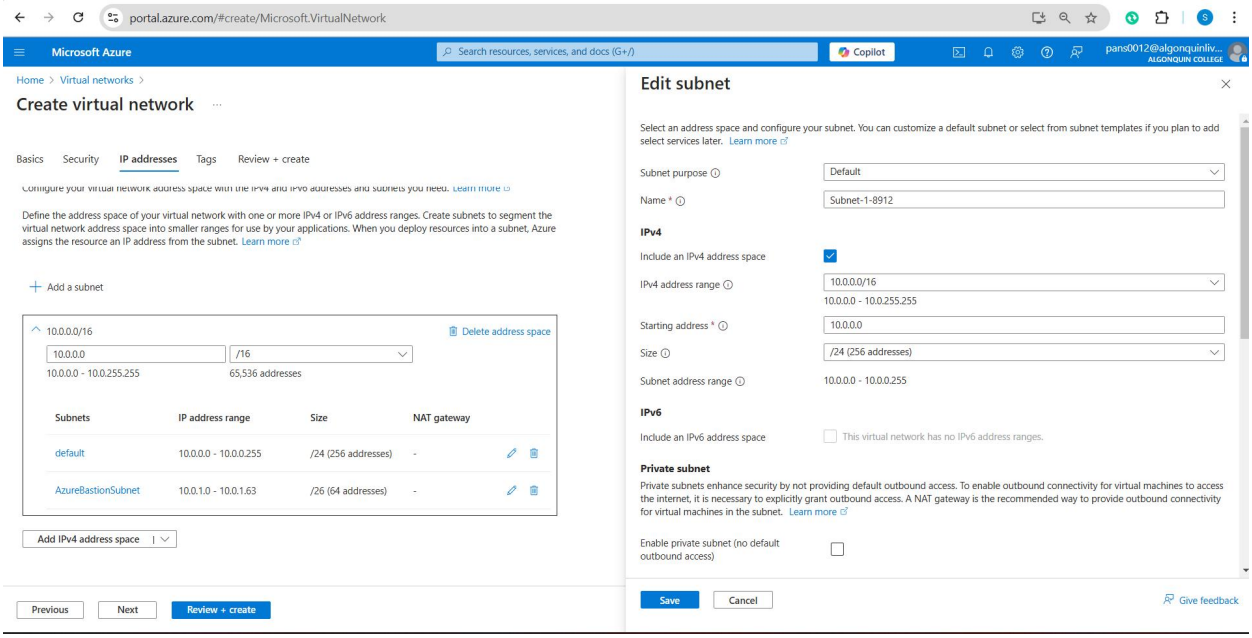
Setting	Value
Azure Bastion host name	Enter Bastion8912
Azure Bastion public IP address	Select **Create a public IP address**. Enter **public-ip** in Name. Select **OK**.



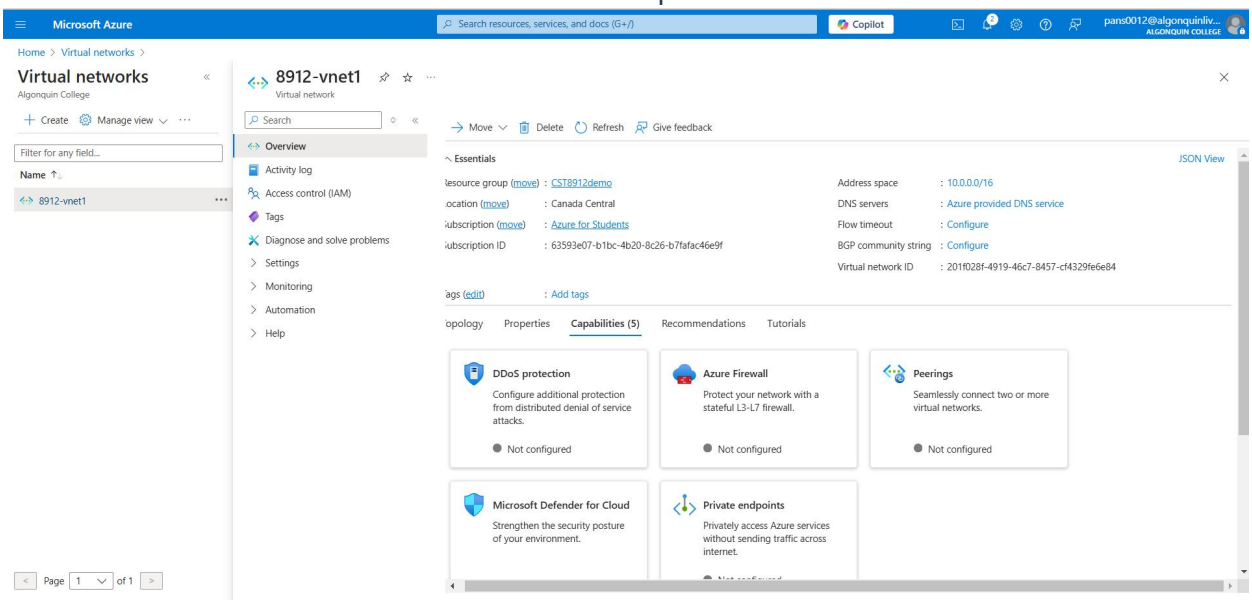
7. Select Next to proceed to the IP Addresses tab.
8. In the address space box in Subnets, select the default subnet.
9. In Edit subnet, enter or select the following information:

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).



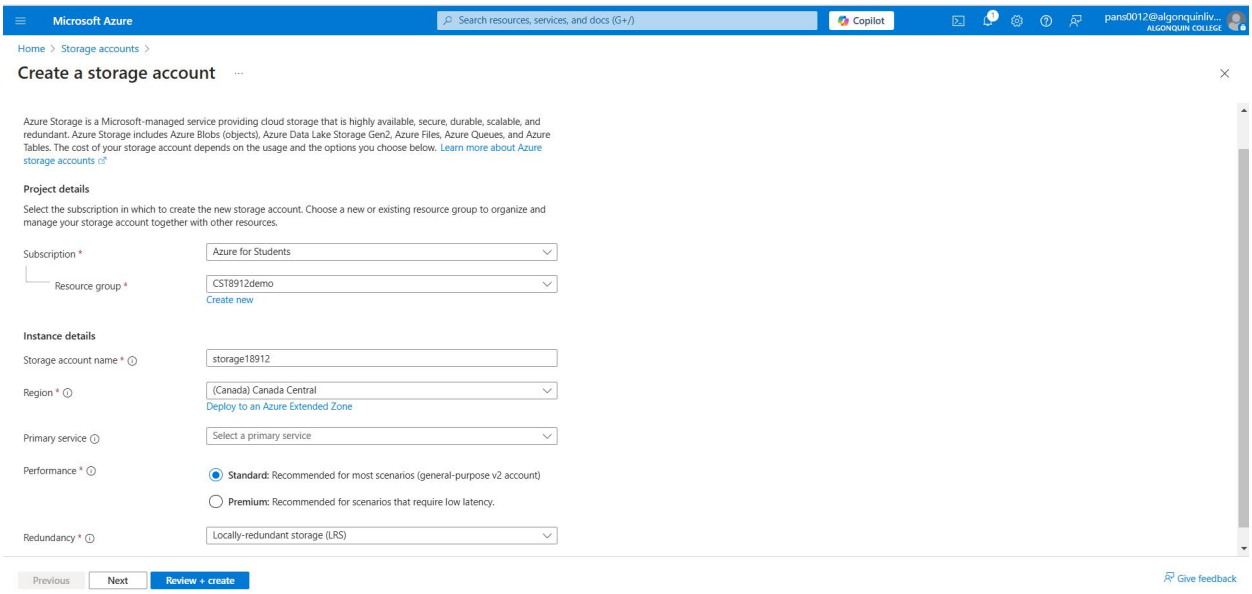
10. Select save
11. Create and review when the validation passes



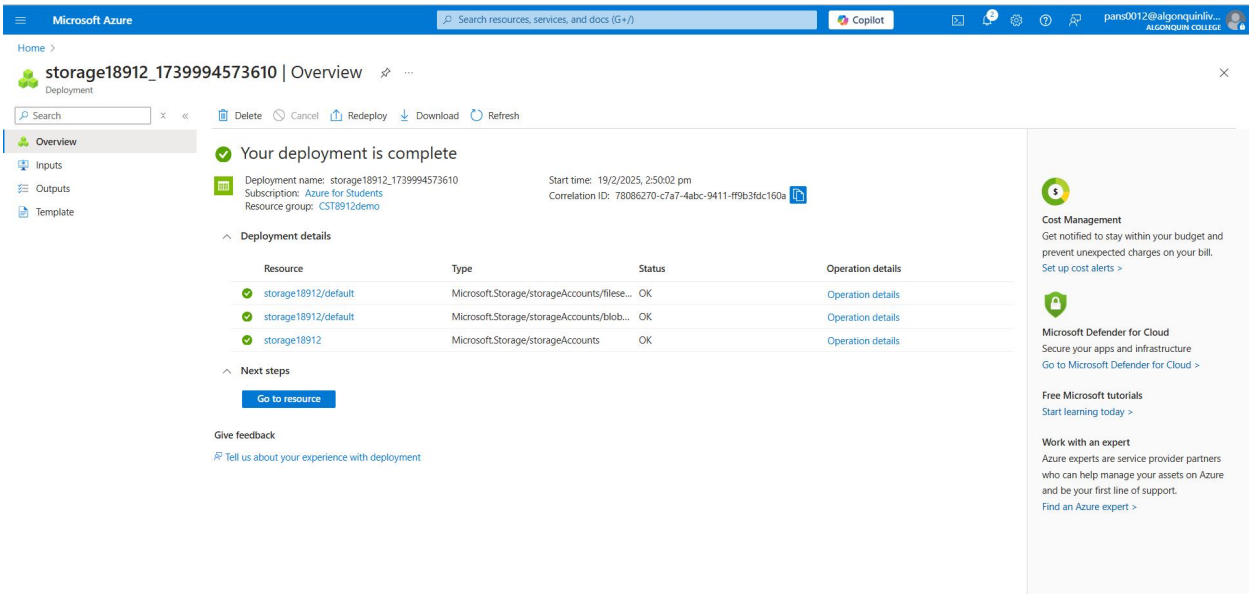
Create a Storage Account

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)

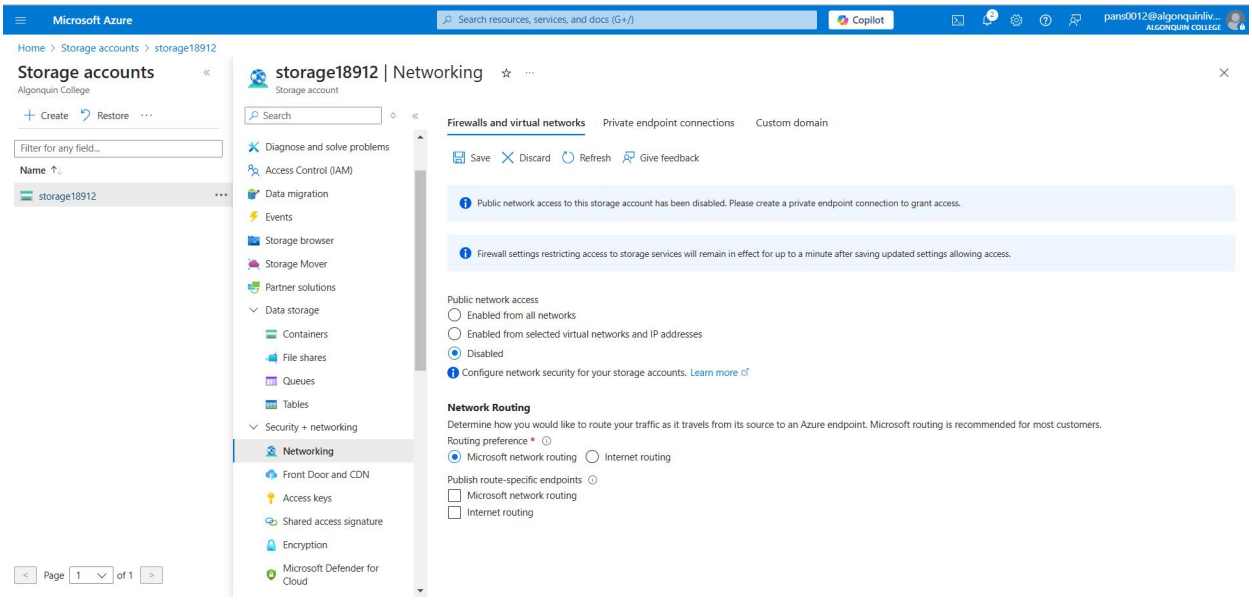


4. Select review
5. Select create



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.

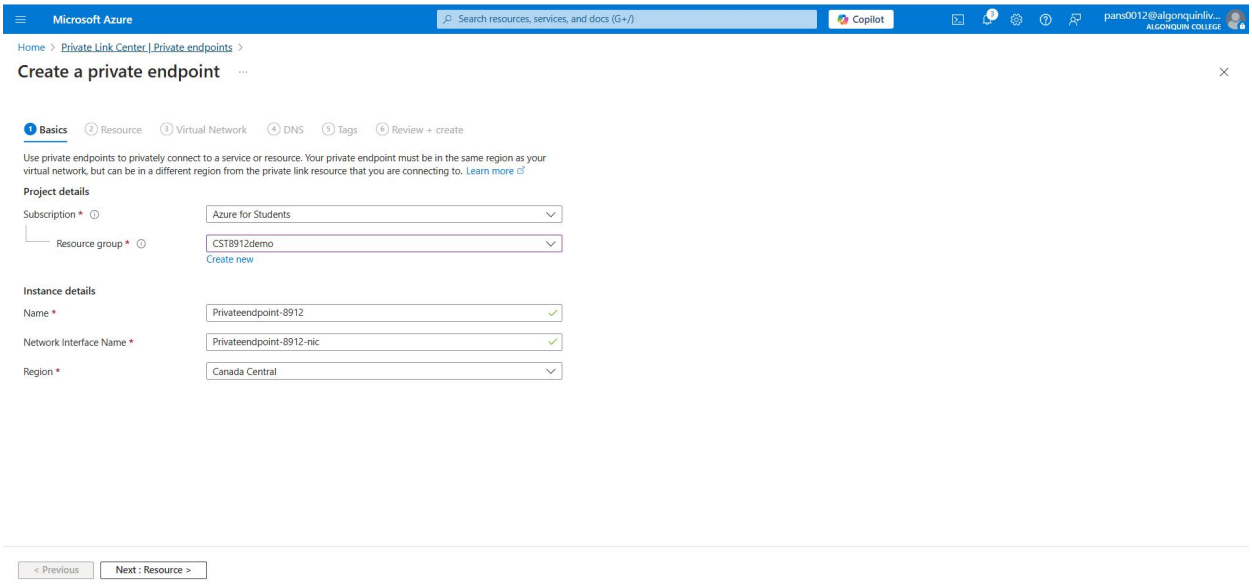


Step 3

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.

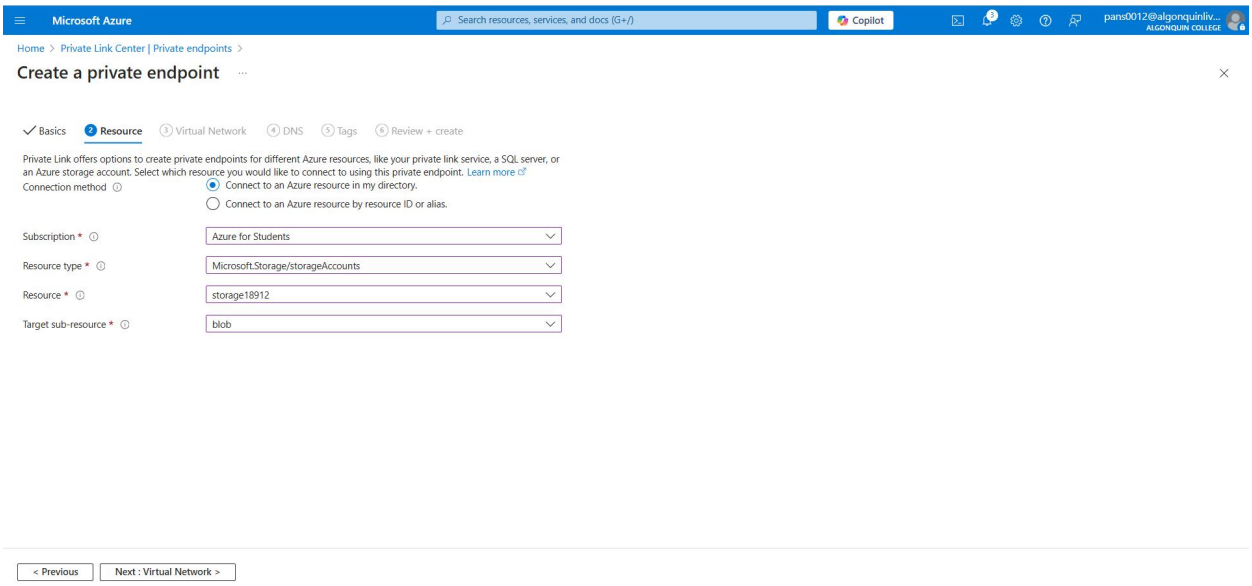
Setting	Value
Subscription	Azure for students
Resource Group	CST8912demo
Name	Privateendpoint-8912
Network Interface Name	Leave the default of **private-endpoint-nic**.
Region	Canada Central



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

Setting	Value

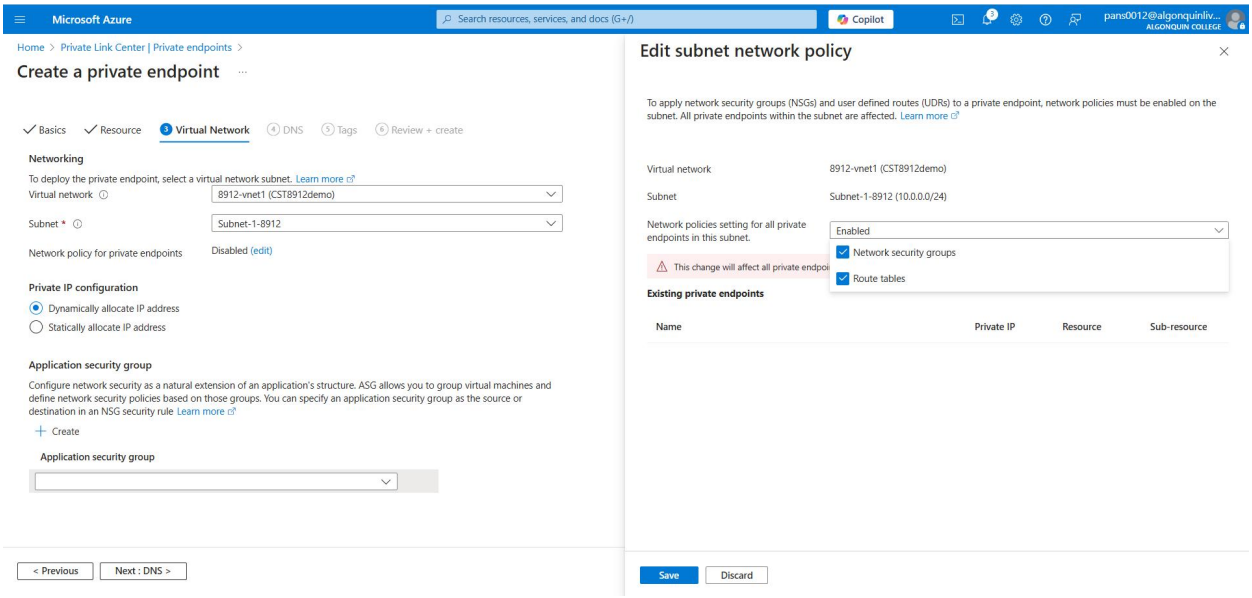
Connection method	Leave the default of Connect to an Azure resource in my directory.
Subscription	Select your subscription.
Resource type	Select Microsoft.Storage/storageAccounts.
Resource	Select Storage1-8912 or your storage account.
Target subresource	Select blob.



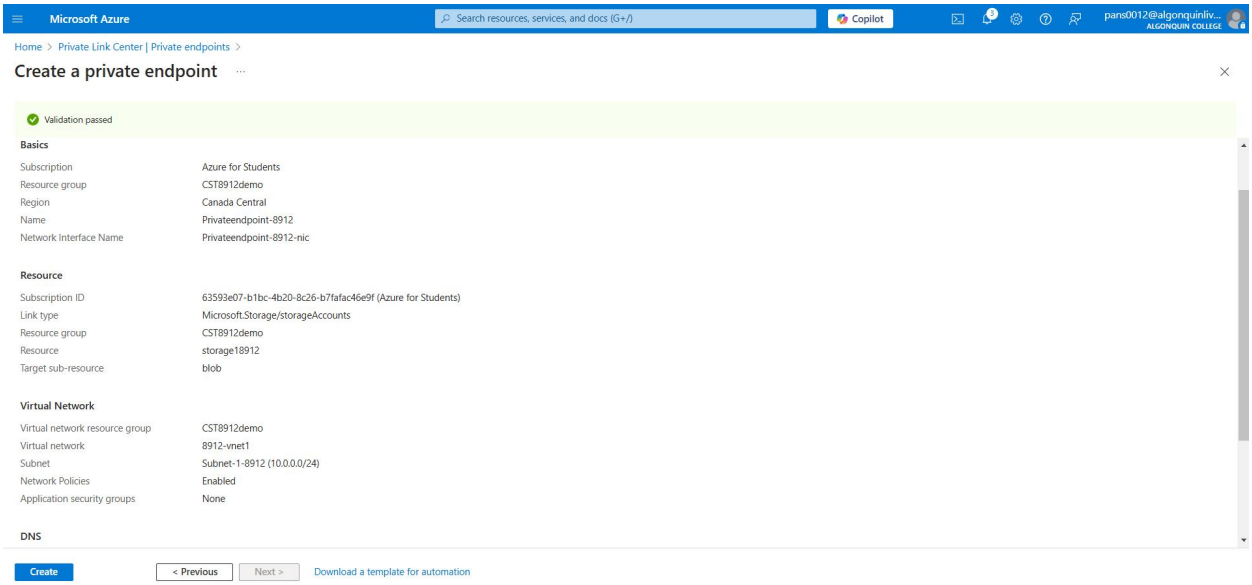
6. Select Next: Virtual Network.
7. In Virtual Network, enter or select the following information.

Setting	**Value**
Virtual network	Select 8912-vnet (CST8912demo).
Subnet	Select Subnet-1-8912.
Network policy for private endpoints	Select edit to apply Network policy for private endpoints. 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. Select Save.
Private IP configuration	Select Dynamically allocate IP address.



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

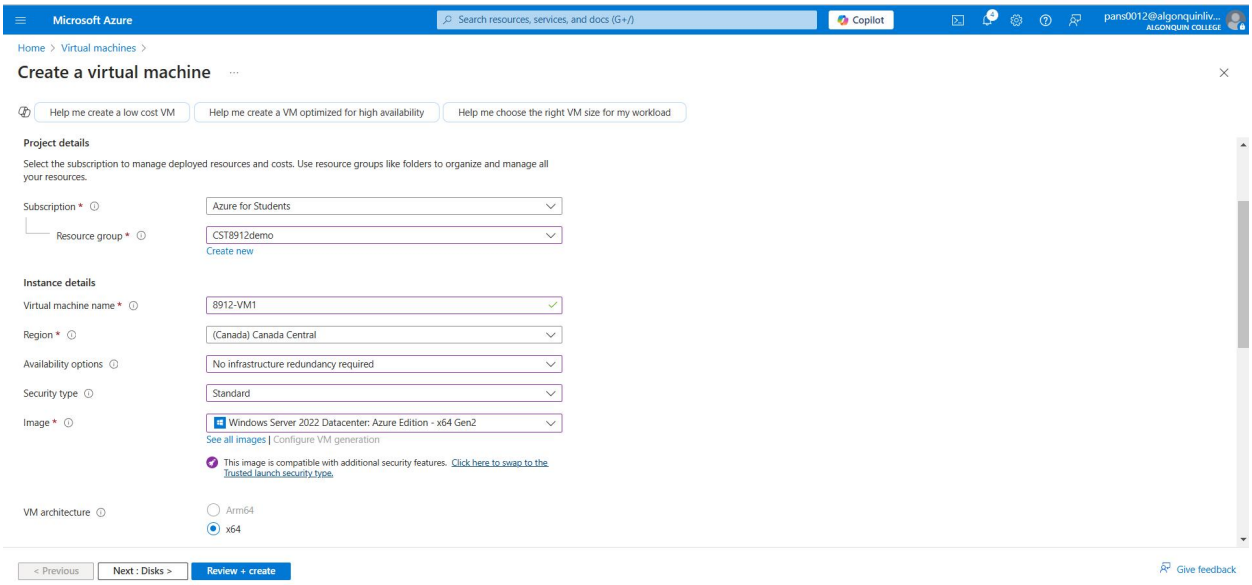


Step 4

Create test virtual machine

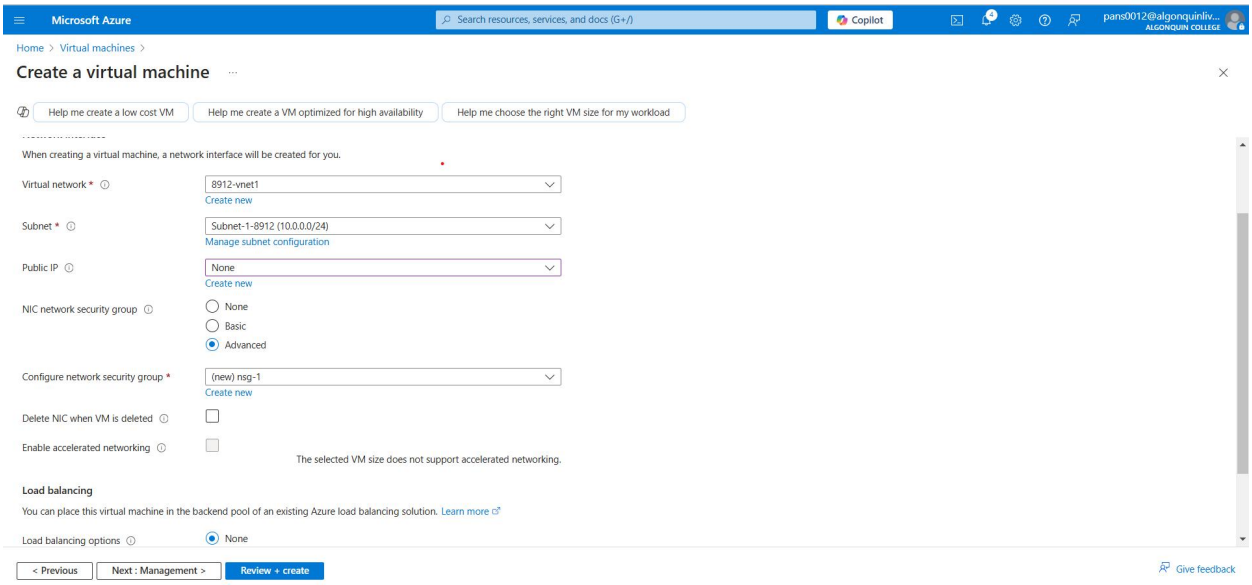
1. In the portal, search for and select Virtual machines.
2. In Virtual machines, select + Create, then Azure virtual machine.
3. On the Basics tab of Create a virtual machine, enter or select the following information:

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

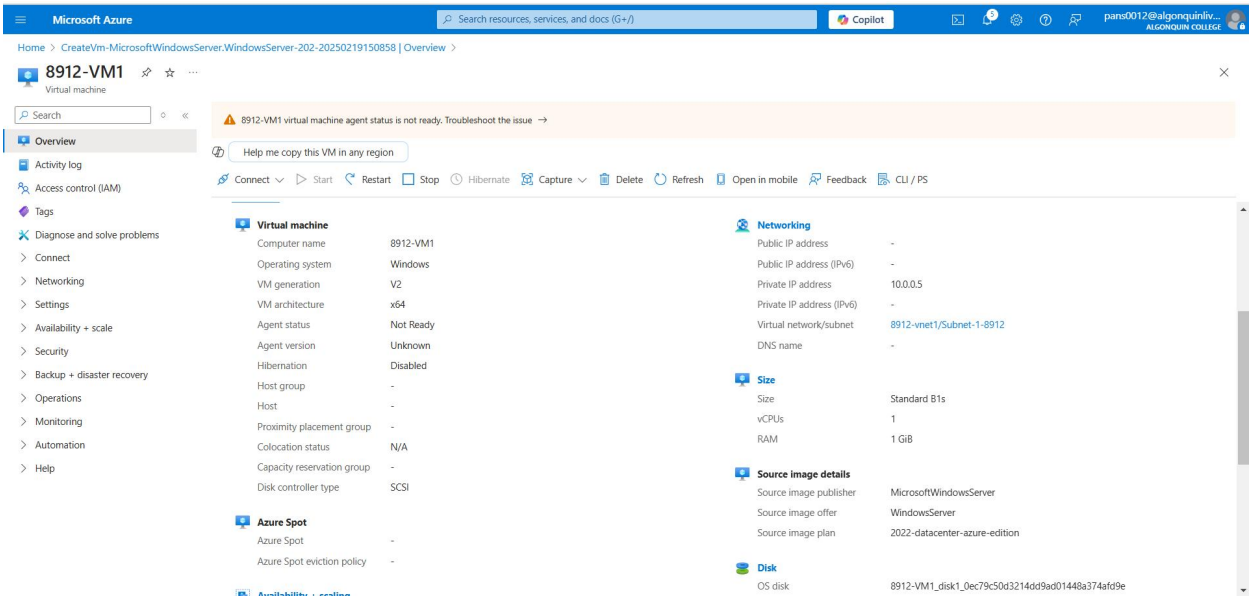


4. Select the Networking tab at the top of the page.
5. Enter or select the following information in the Networking tab:

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.



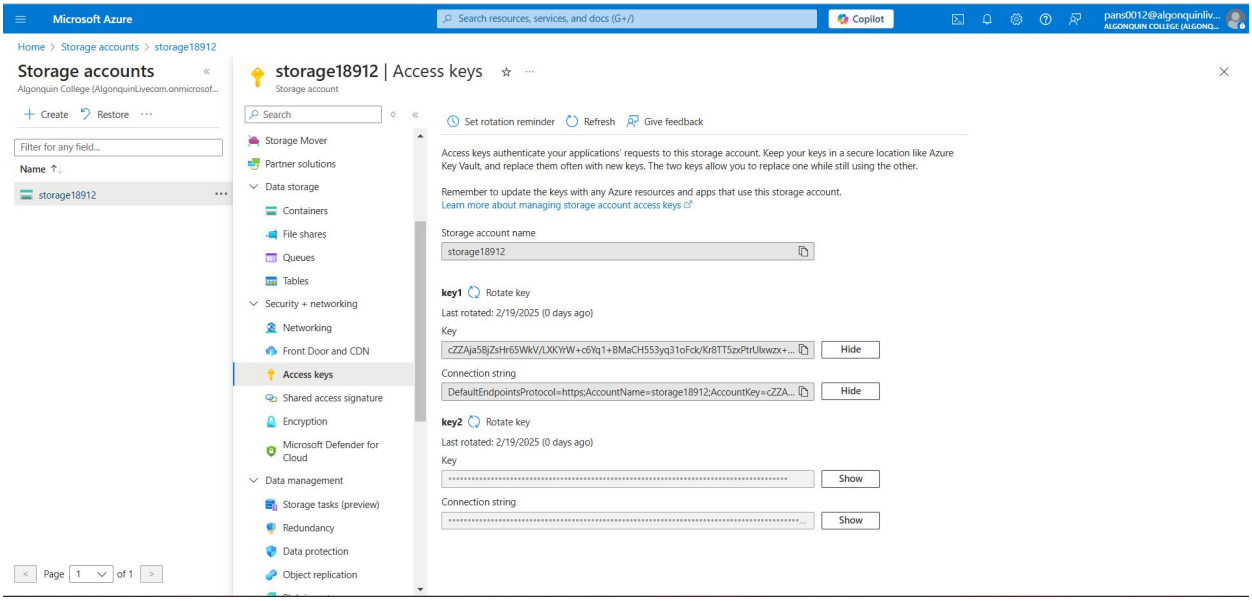
6. Leave the rest of the settings at the defaults and select Review + create.
7. Review the settings and select Create.



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.

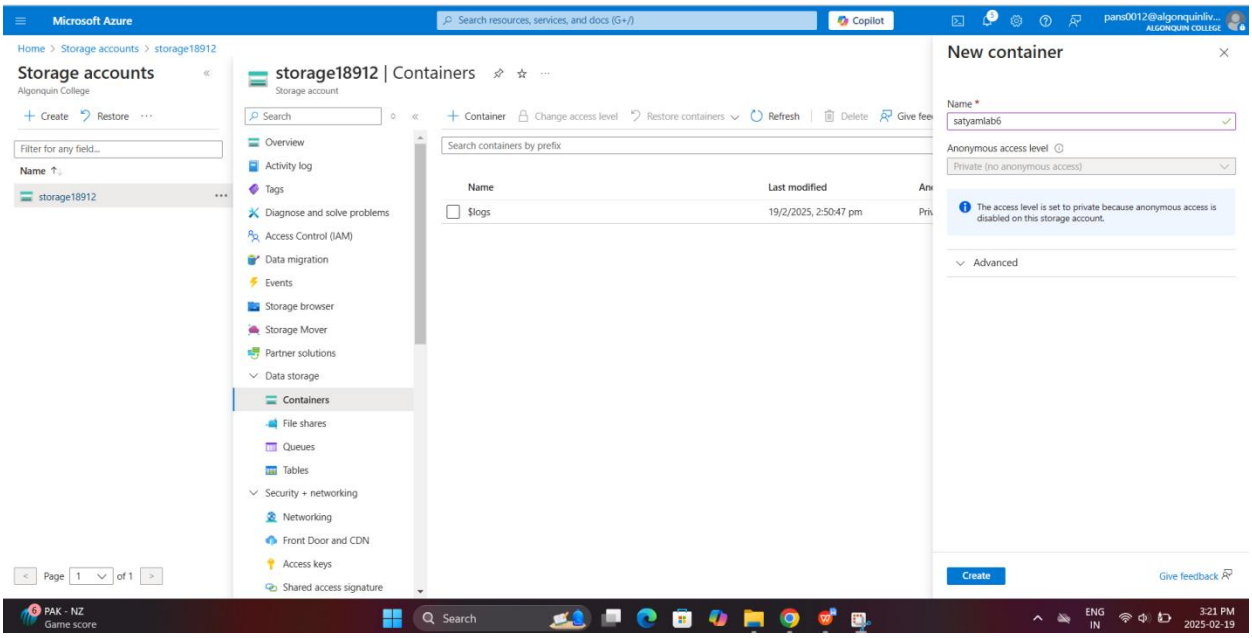
3. In the Security + networking section of the storage account, select Access keys.



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

Add a blob container

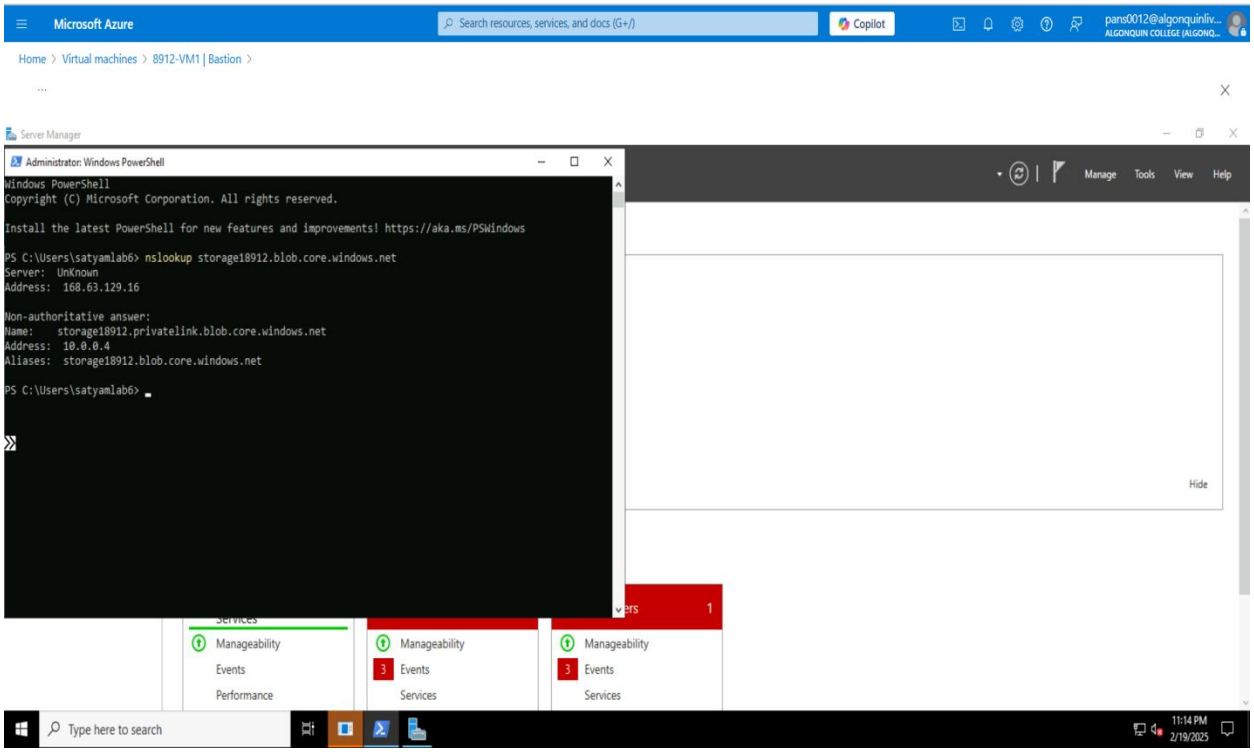
1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select the storage account you created in the previous steps.
3. In the Data storage section, select Containers.
4. Select + Container to create a new container.
5. Enter container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



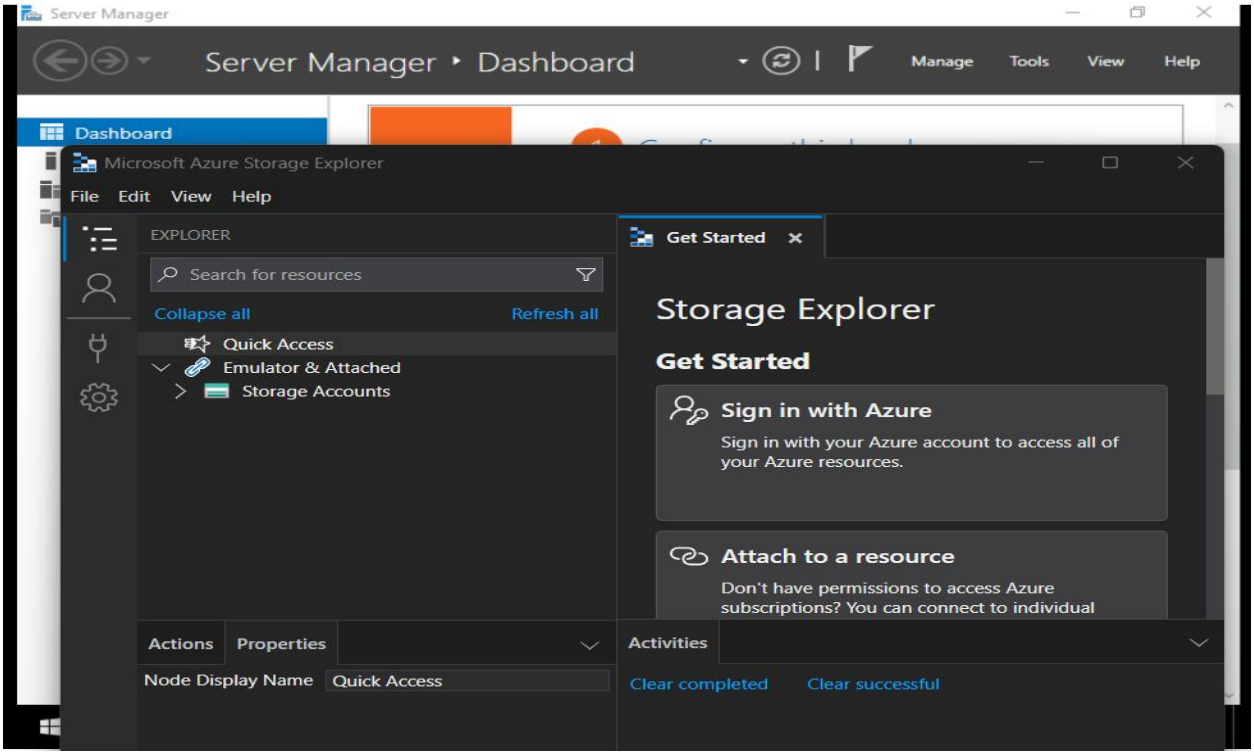
Test connectivity to private endpoint

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

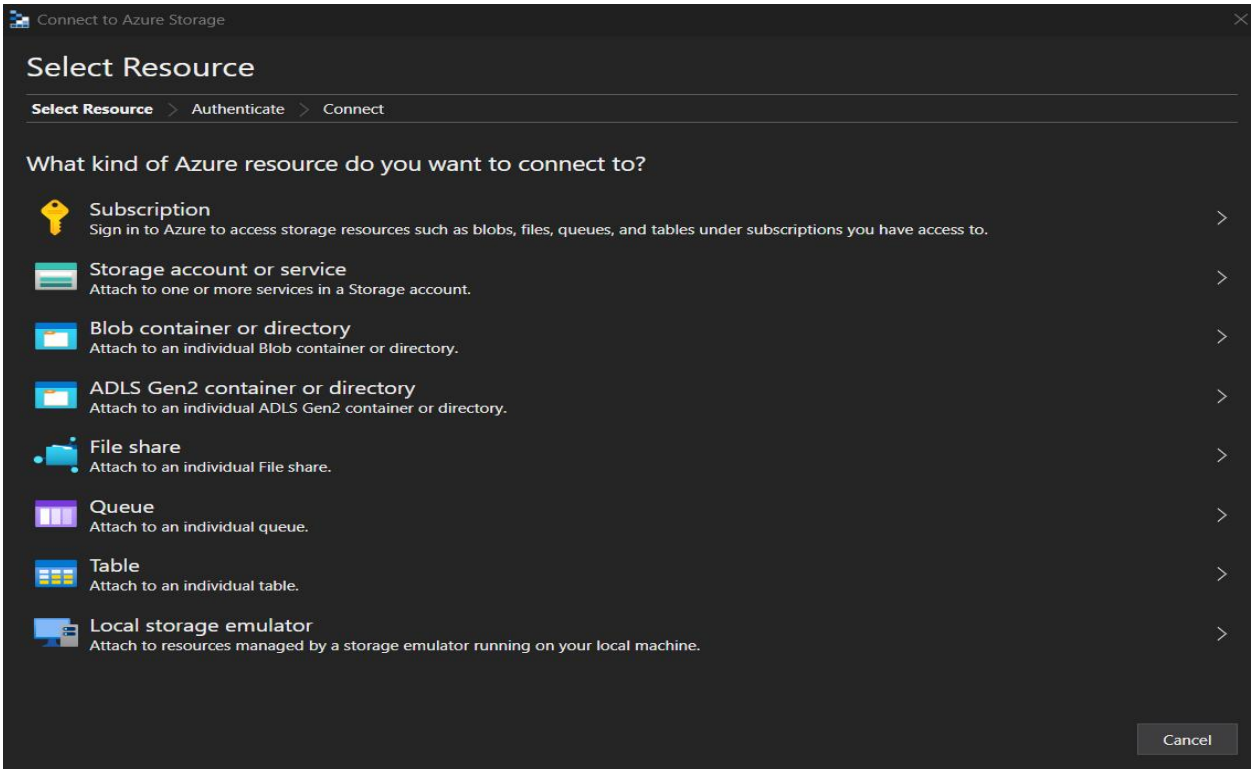
   A private IP address of 10.0.0.10 is returned for the storage account name. This address is in Subnet-1-8912 subnet of 8912-vnet virtual network you created previously.



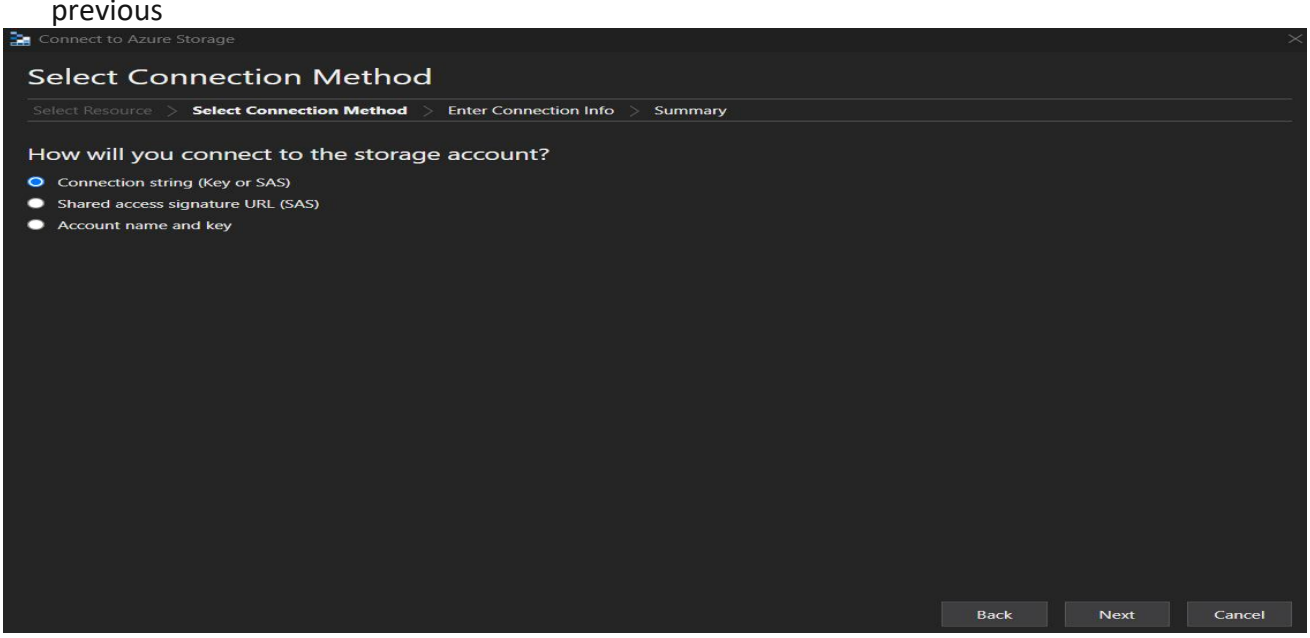
8. Install Microsoft Azure Storage Explorer on the virtual machine.
9. Select Finish after the Microsoft Azure Storage Explorer is installed. Leave the box checked to open the application.



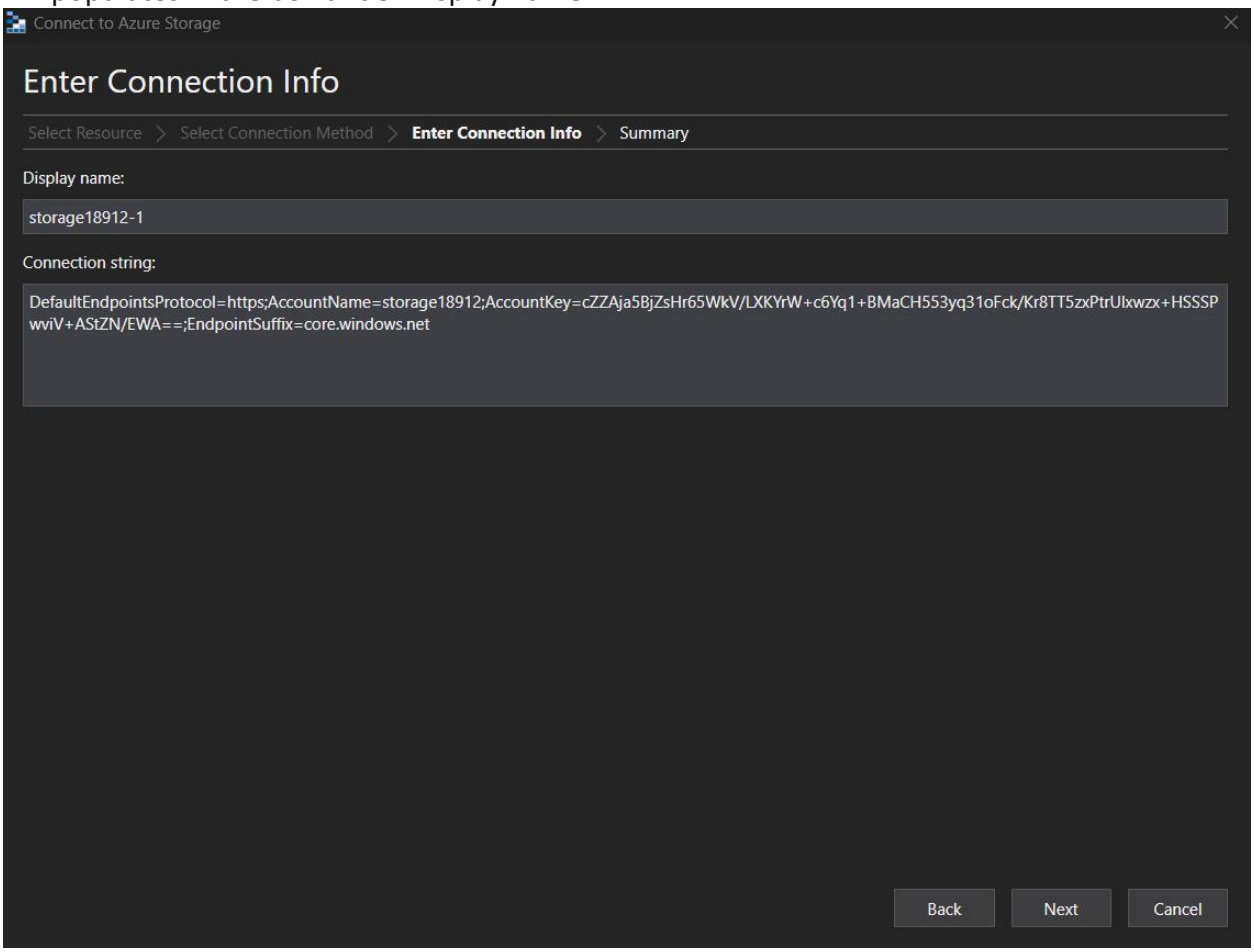
10. Select the Power plug symbol to open the Select Resource dialog box in the left-hand toolbar.



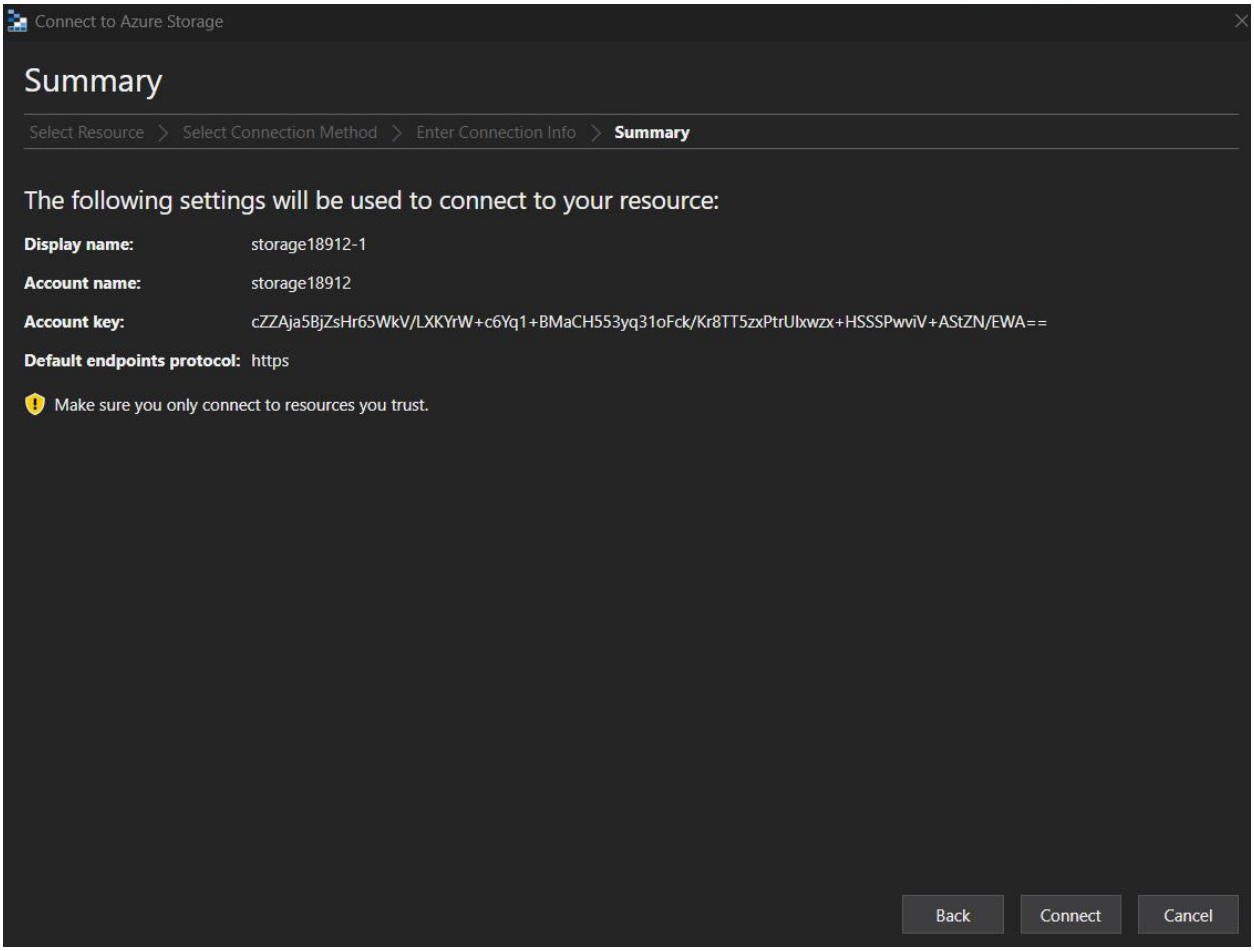
11. In Select Resource , select Storage account or service to add a connection in Microsoft Azure Storage Explorer to your storage account that you created in the previous



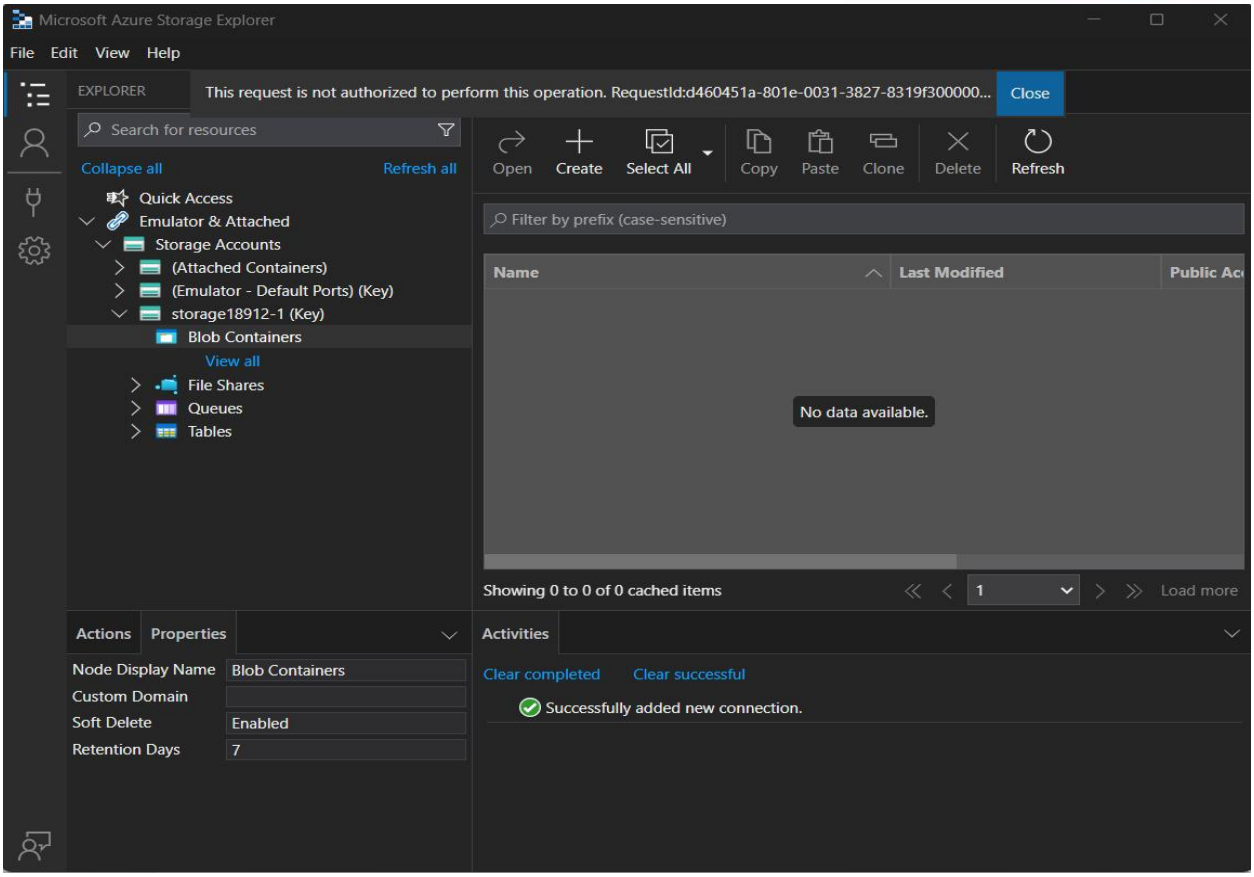
12. In the Select Connection Method screen, select Connection string, and then Next.
13. In the box under Connection String, paste the connection string from the storage account you copied in the previous steps. The storage account name automatically populates in the box under Display name.



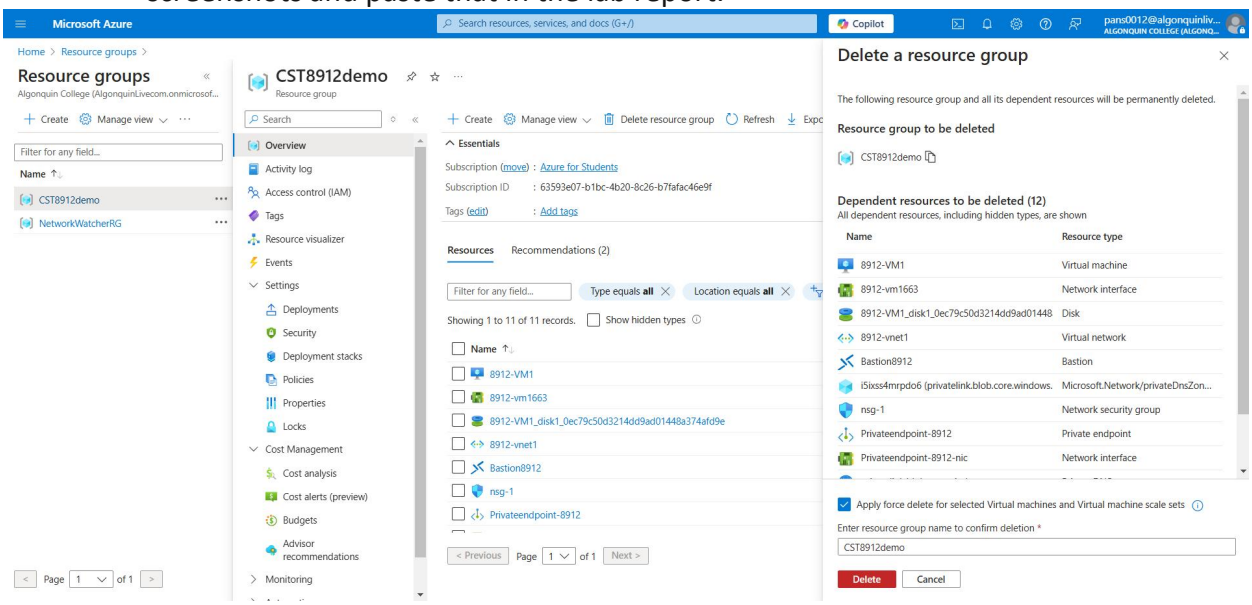
14. Select Next.
15. Verify the settings are correct in Summary.



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.