CST8912 – Cloud Solution Architecture

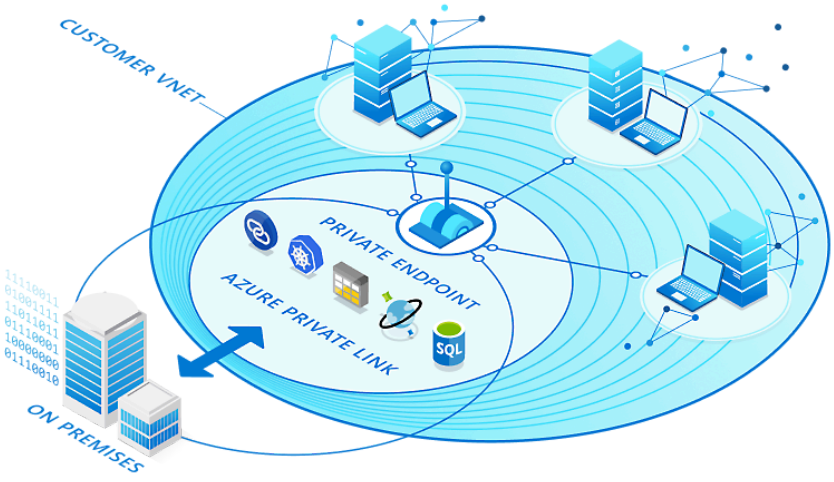
Graded Lab Activity #6

1. Distinguish between public-cloud, private-cloud, hybrid-cloud and multi-cloud solution design patterns. (2,5,6,7)

   - Classify and describe the type of clouds available in the marketplace
   - Identify the pros, cons, use cases, and pricing of each cloud computing service
   - Examine the risks associated with each type of cloud computing service
   - Assess security compliance requirements as part of the decision-making process

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

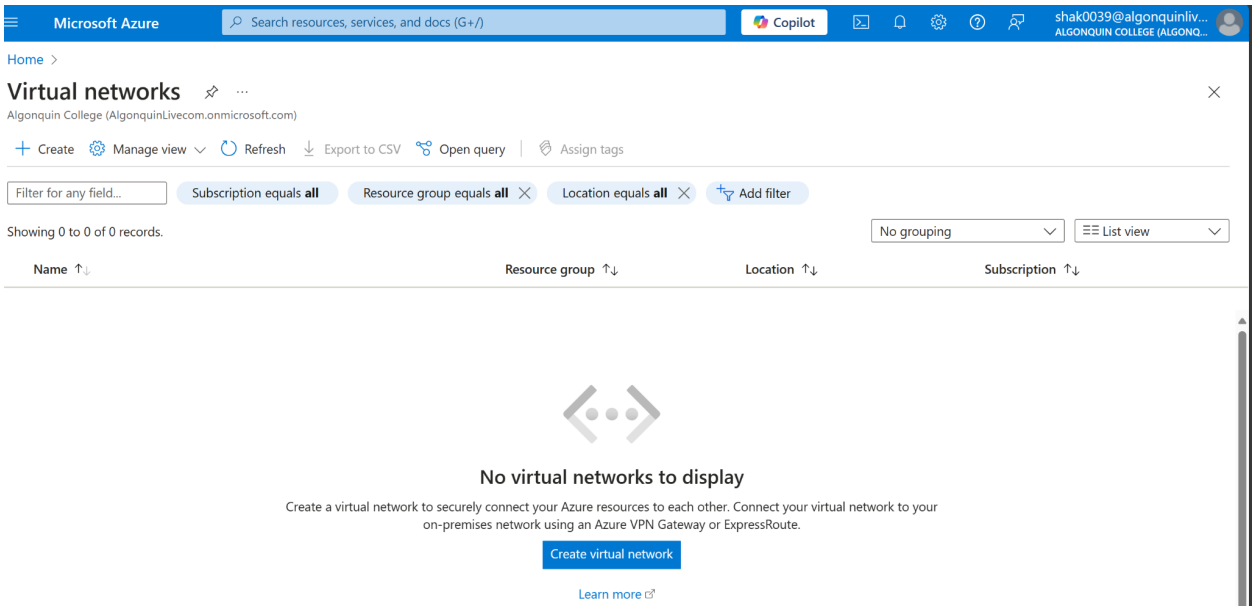
Purpose of this hands-on-lab that can be simulated for any CSP:

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

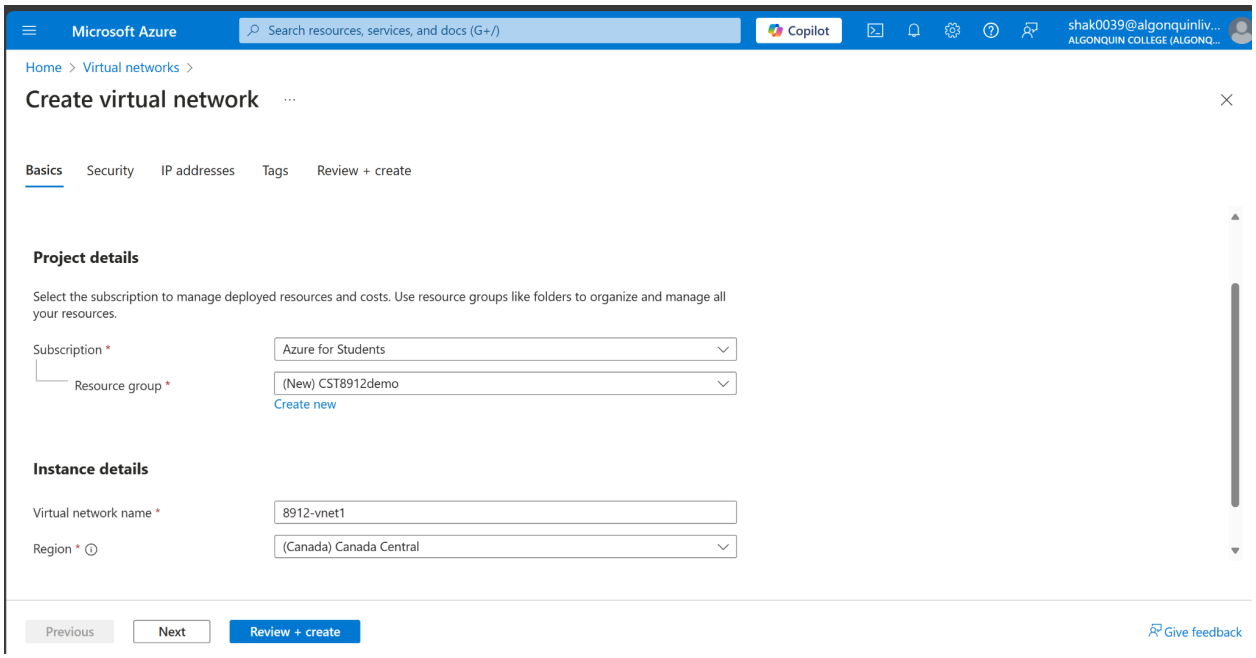
Azure Private endpoint is the fundamental building block for Private Link in Azure. It enables Azure resources, like virtual machines (VMs), to privately and securely communicate with Private Link resources such as Azure Storage.

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

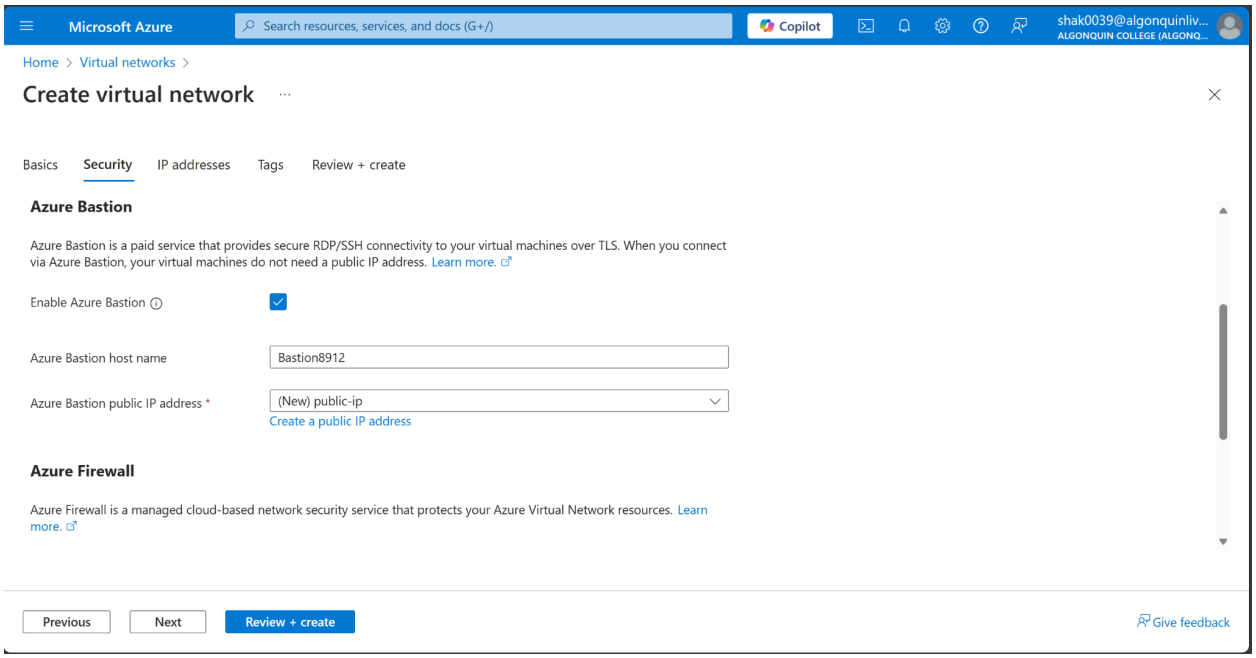
Subscription	Azure for students
Resource Group	CST8912demo
Name	8912-vnet1
Region	Canada Central

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

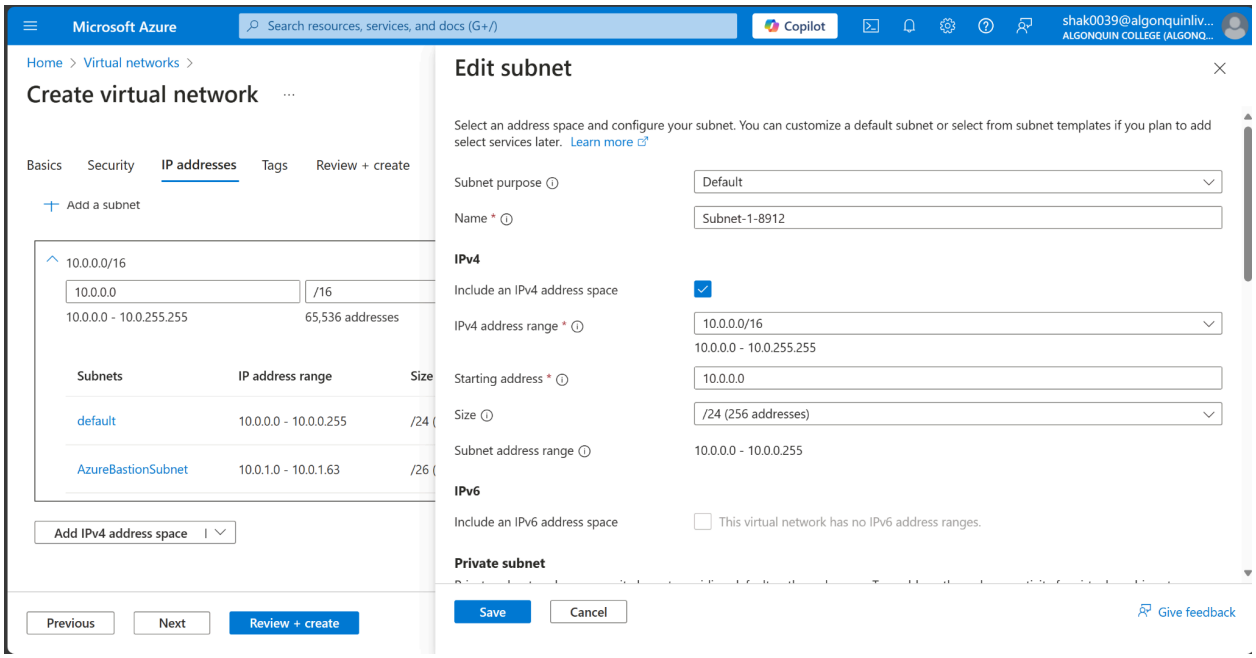
6. Enter or select the following information in Azure Bastion:

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**.

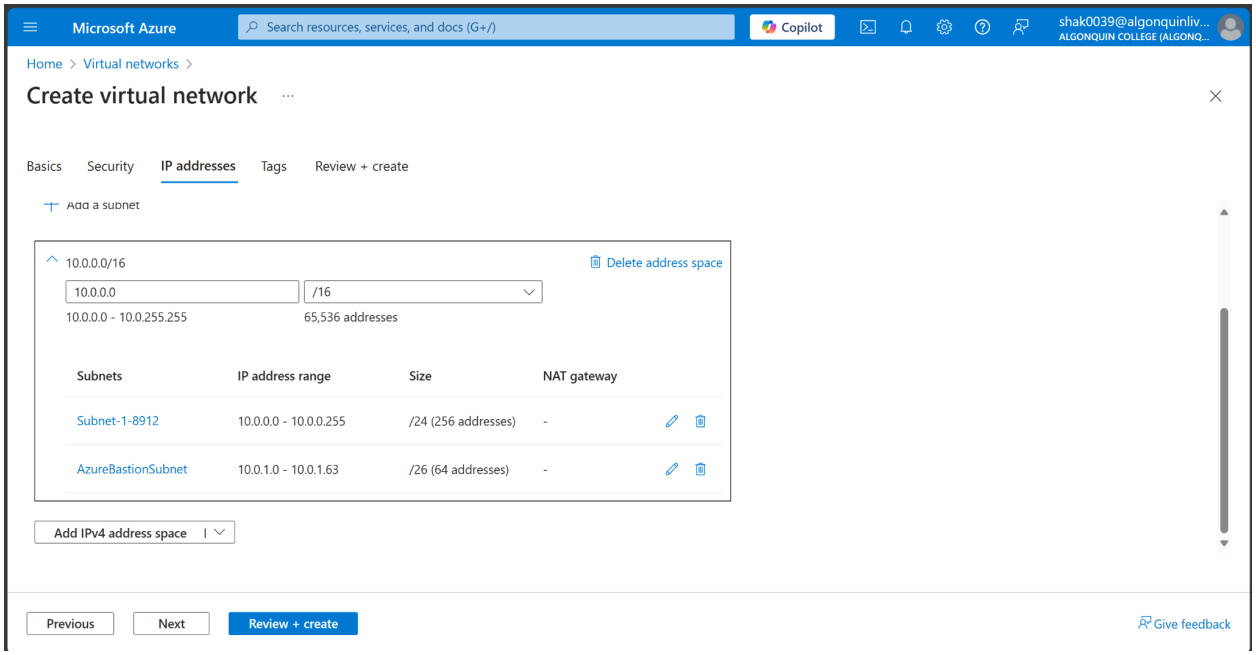


7. Select Next to proceed to the IP Addresses tab.
8. In the address space box in Subnets, select the default subnet.
9. In Edit subnet, enter or select the following information:

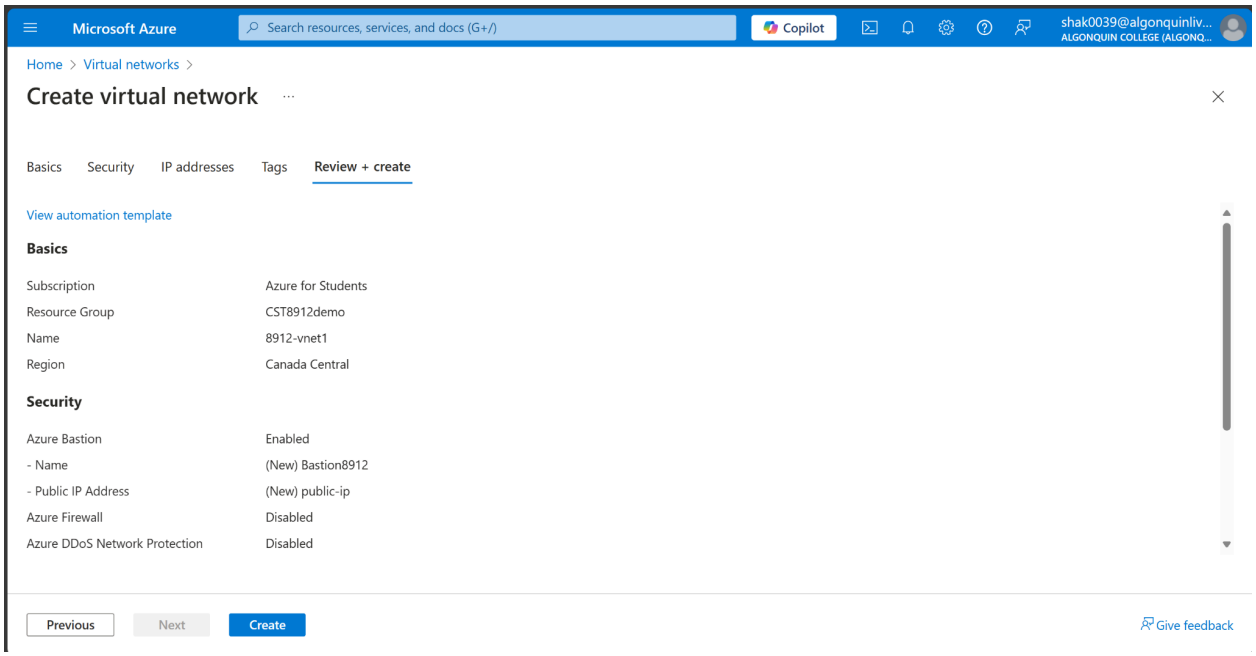
Setting	**Value**
Subnet template	Leave the default **Default**.
Name	Subnet-1-8912
IPv4 address range	Leave 10.0.0.0/16.
Starting address	Leave the default of 10.0.0.0.
Subnet size	Leave the default of /24(256 addresses).

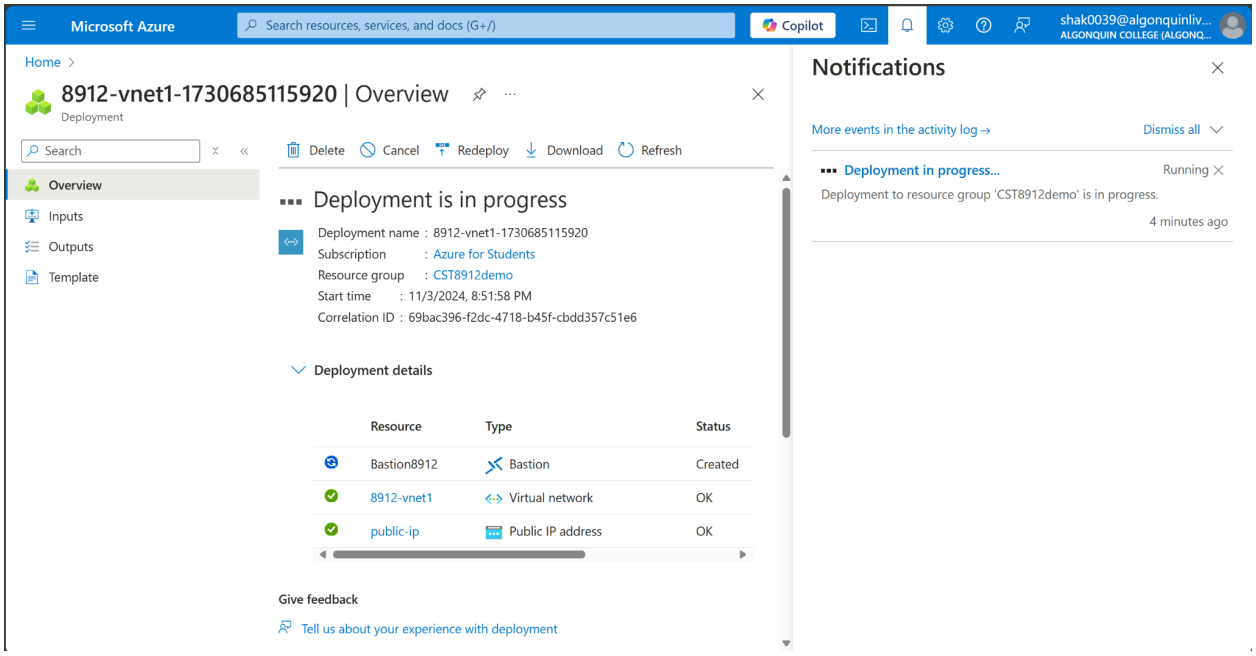


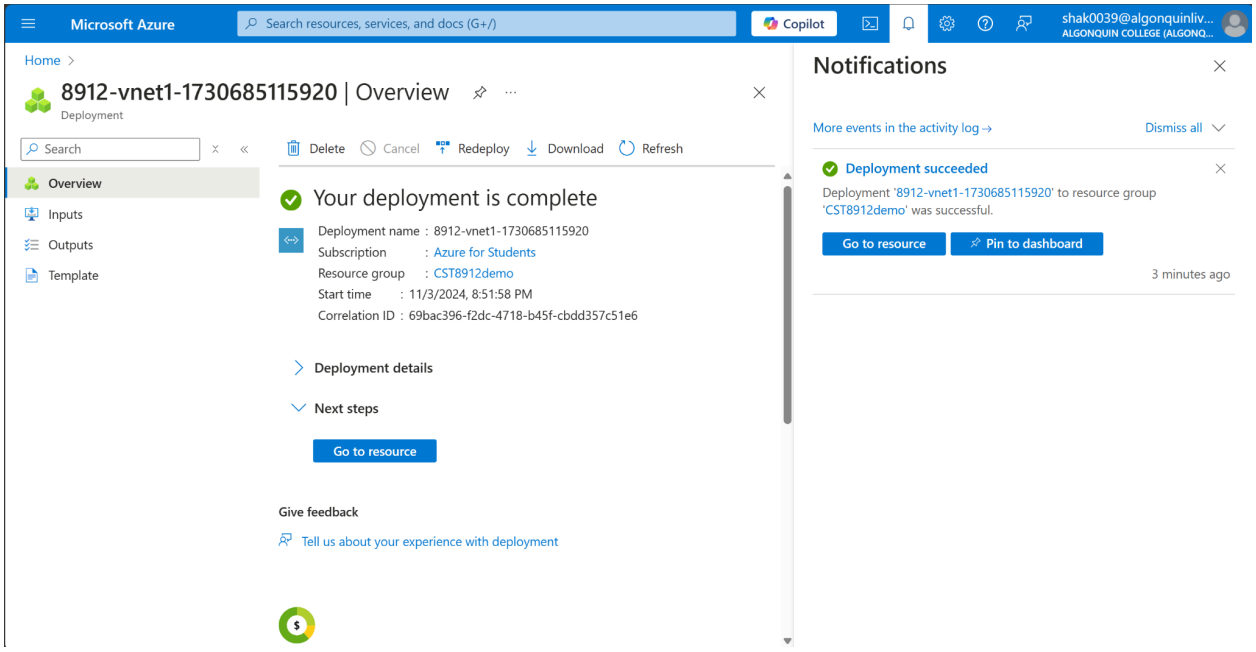
10. Select save

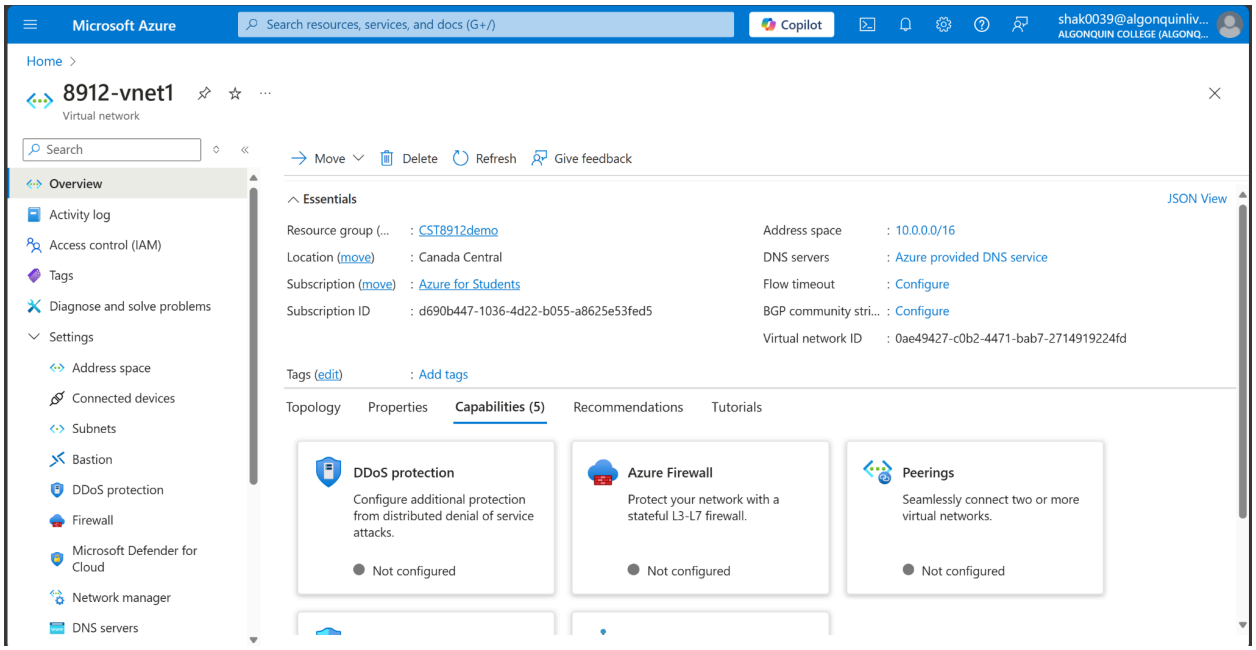


11. Create and review when the validation passes


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Virtual networks >
Create virtual network
Basics
Security
IP addresses
Tags
Review + create
View automation template
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
Previous
Next
Create
Give feedback

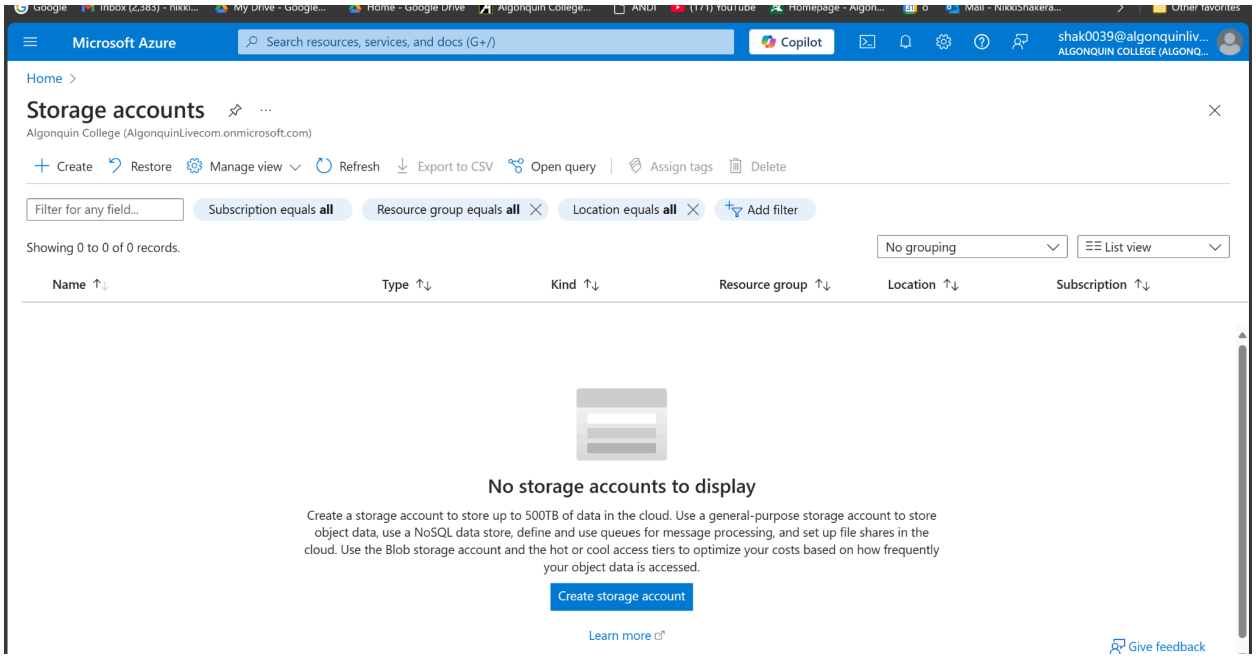

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home >
8912-vnet1-1730685115920 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name : 8912-vnet1-1730685115920
Subscription : Azure for Students
Resource group : CST8912demo
Start time : 11/3/2024, 8:51:58 PM
Correlation ID : 69bac396-f2dc-4718-b45f-cbdd357c51e6
Deployment details
Resource
Type
Status
Bastion8912
Bastion
Created
8912-vnet1
Virtual network
OK
public-ip
Public IP address
OK
Give feedback
Tell us about your experience with deployment
Notifications
More events in the activity log →
Dismiss all
Deployment in progress...
Running
Deployment to resource group 'CST8912demo' is in progress.
4 minutes ago





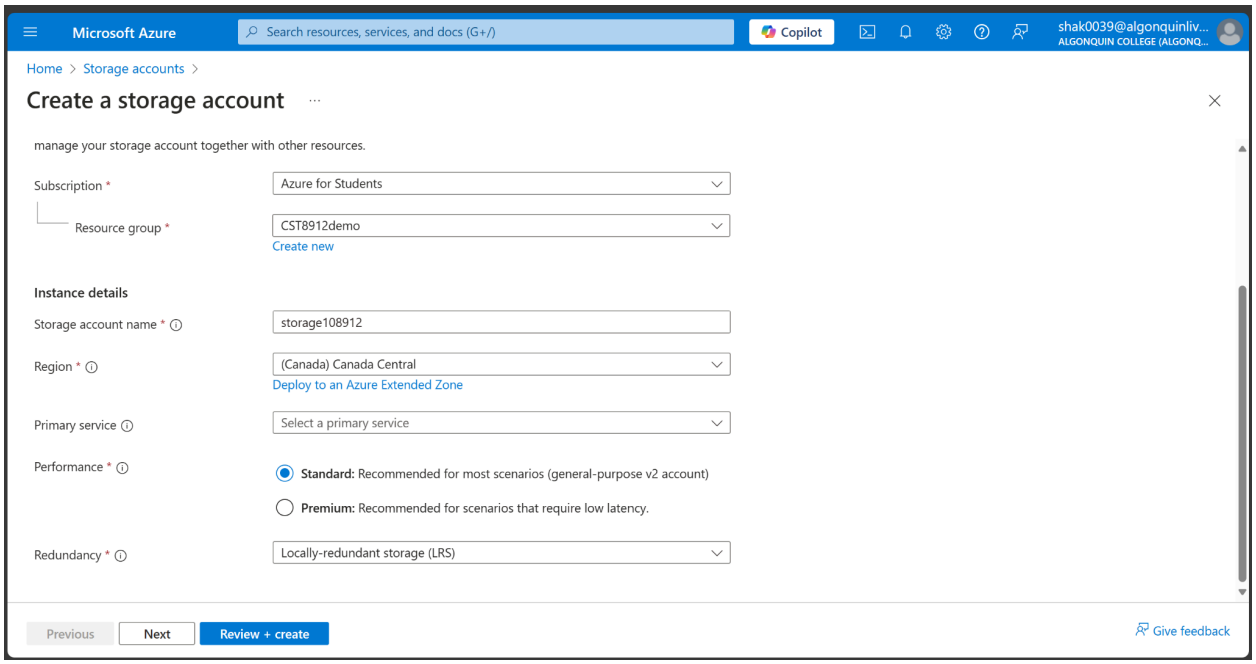
Create a Storage Account

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

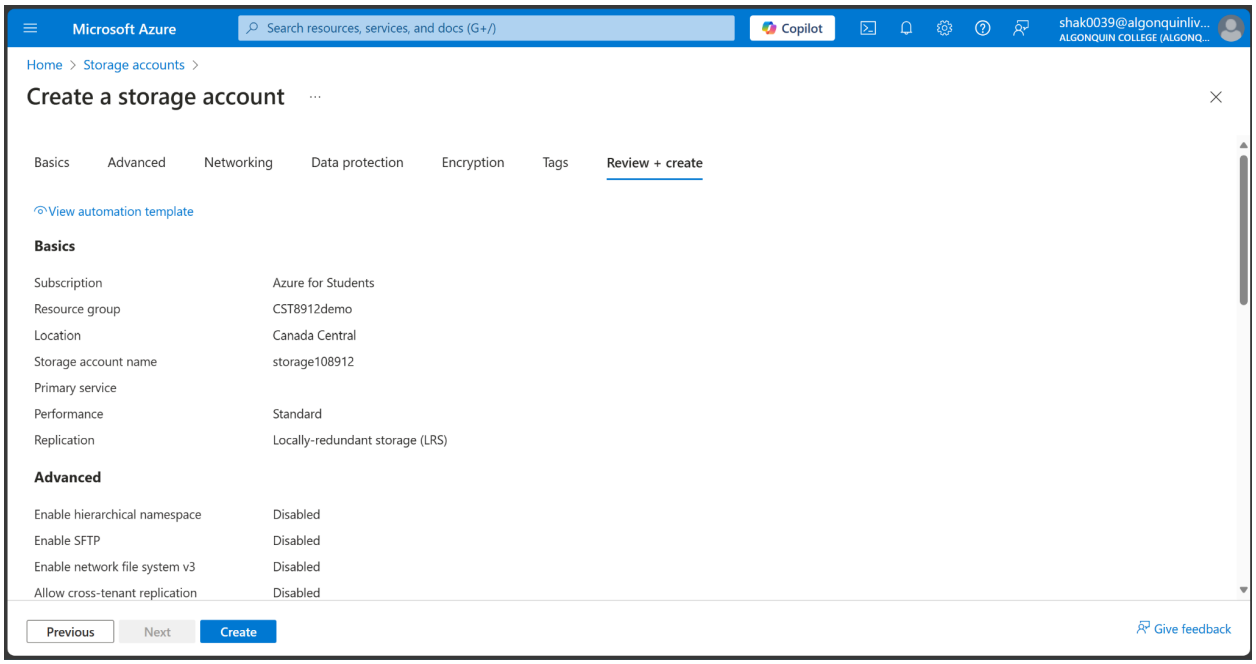


2. Select + Create.
3. In the Basics tab of Create a storage account enter or select the following information:

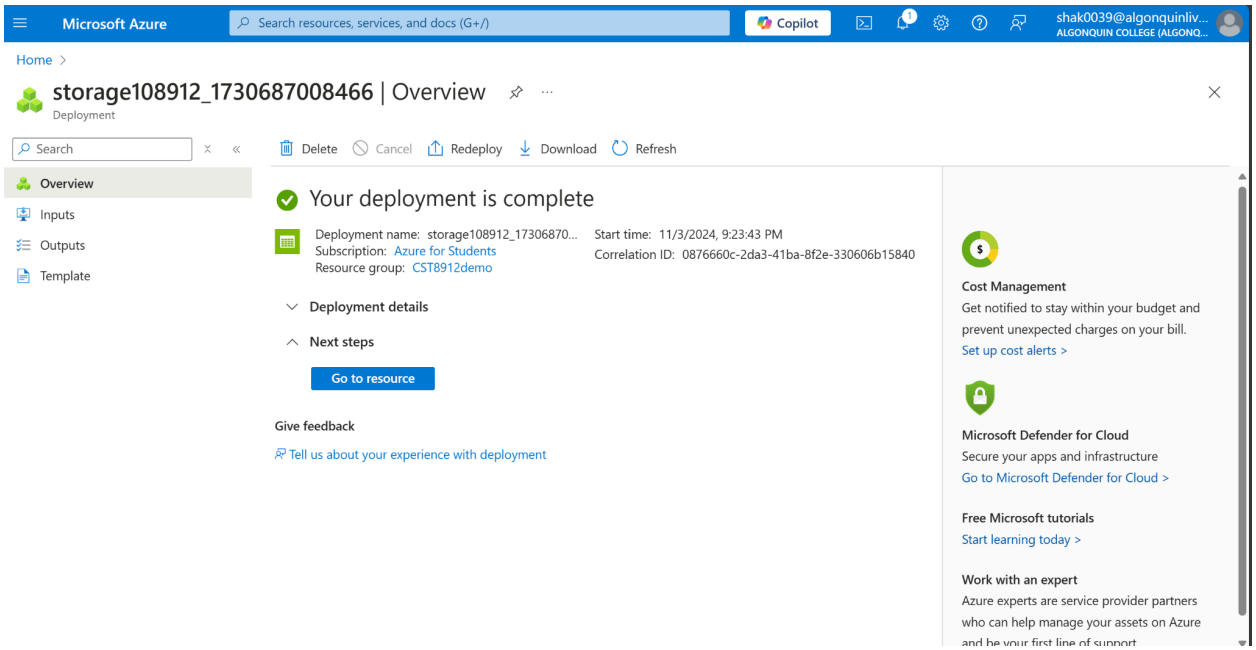
Setting	**Value**
Subscription	Azure for students
Resource Group	CST8912demo
Storage Account Name	Storage1-8912
Location	Canada Central
Performance	Standard
Redundancy	Local Redundant Storage (LRS)

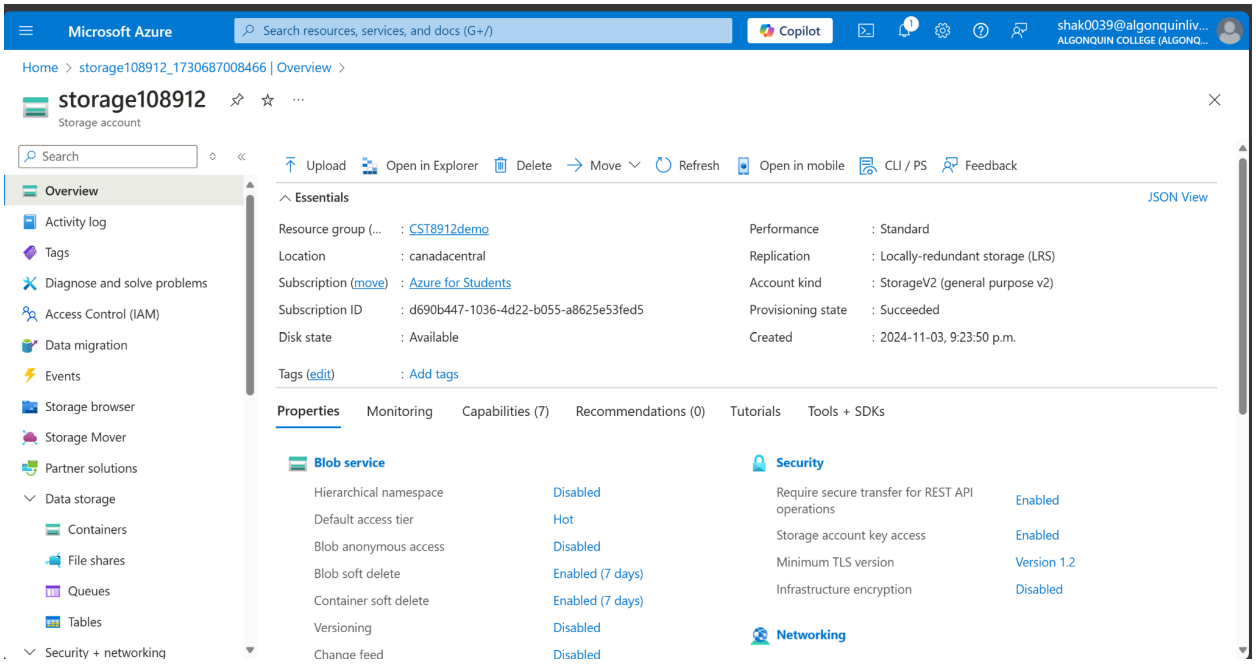


4. Select review



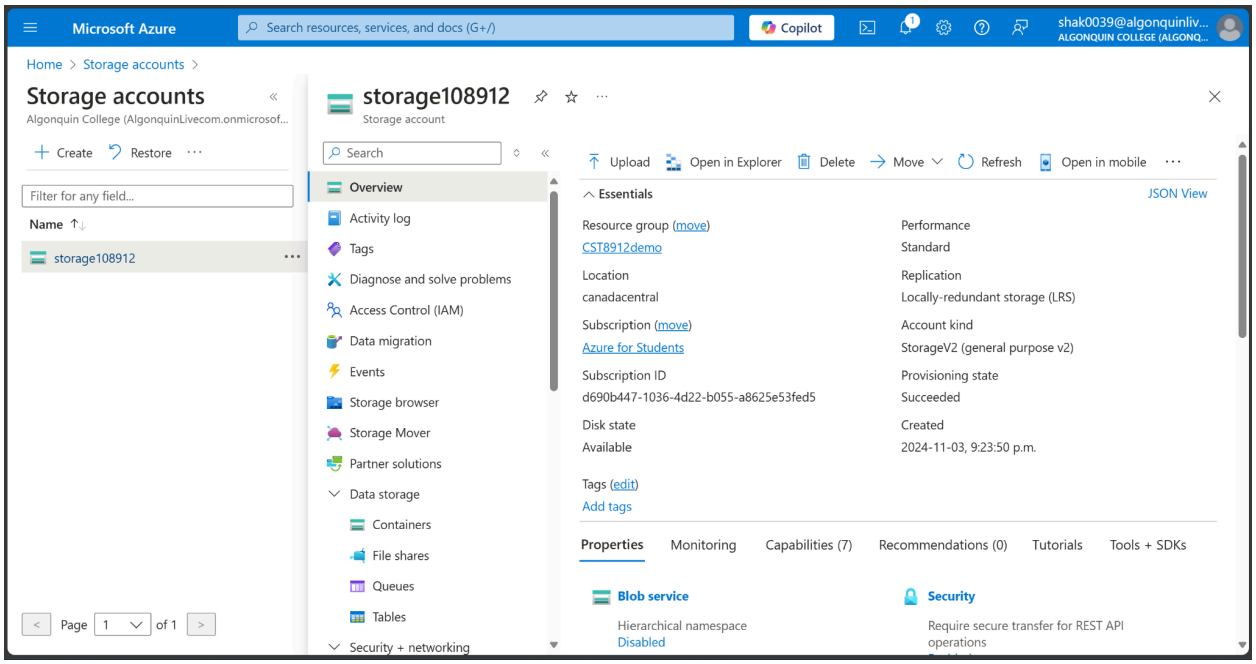
5. Select create



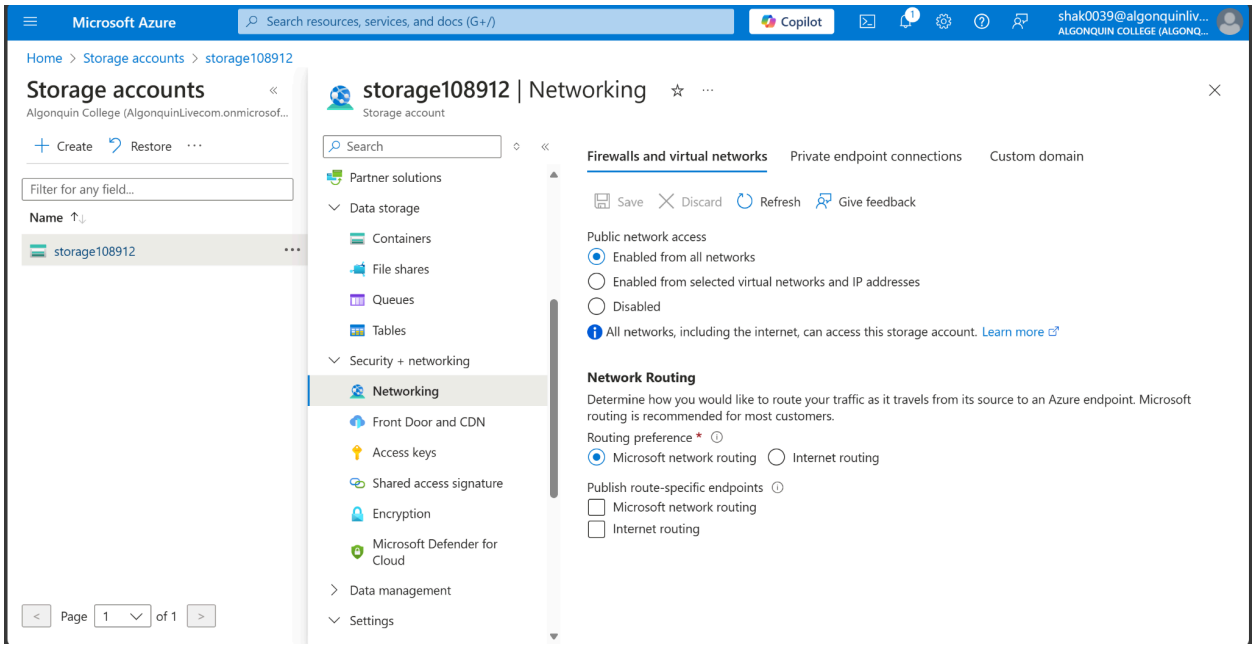


Disable public access to storage account

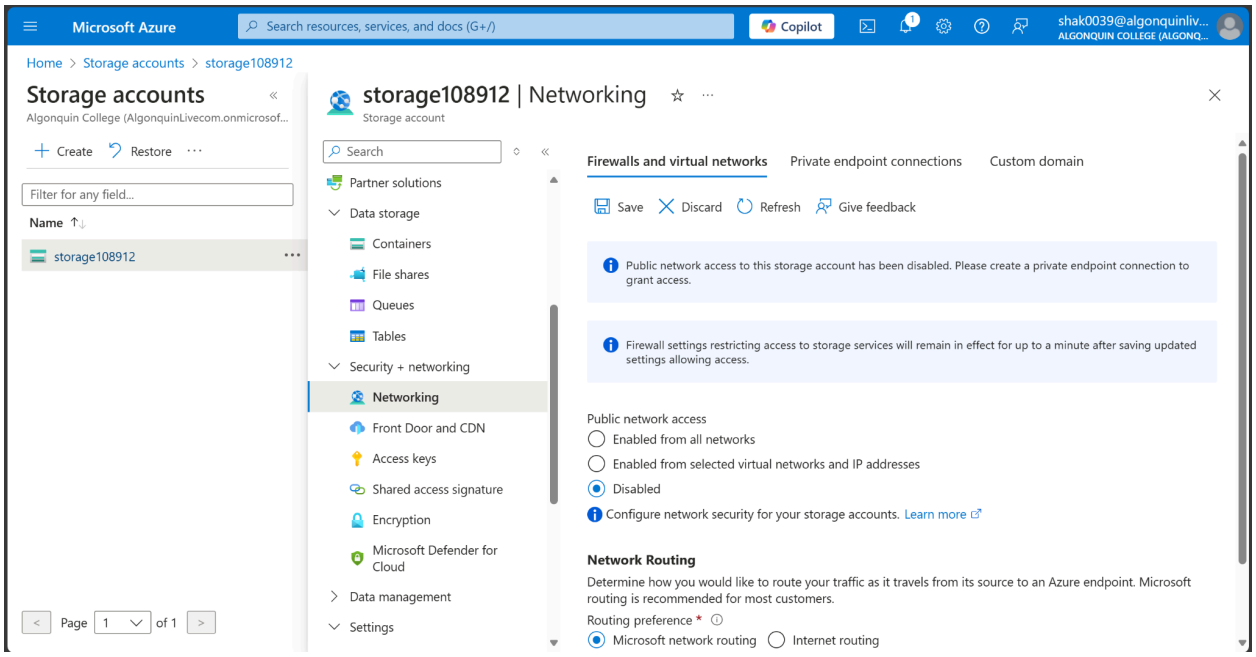
1. In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.
2. Select storage1 or the name of your existing storage account.



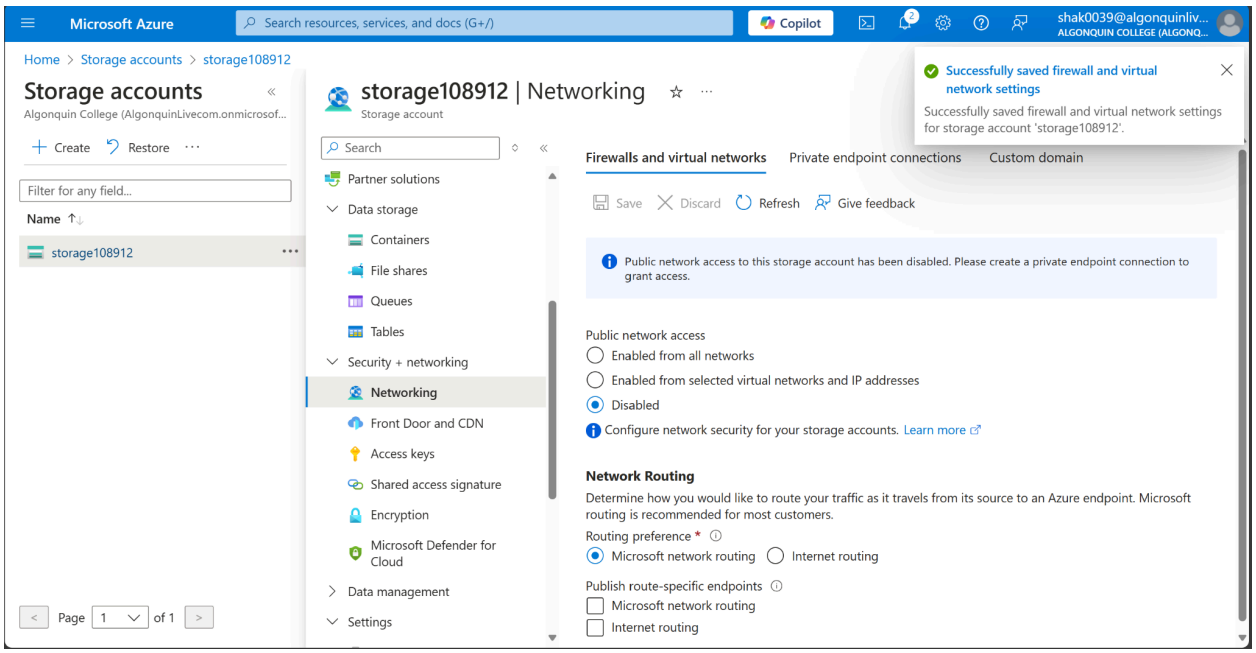
3. In Security + networking, select Networking.



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

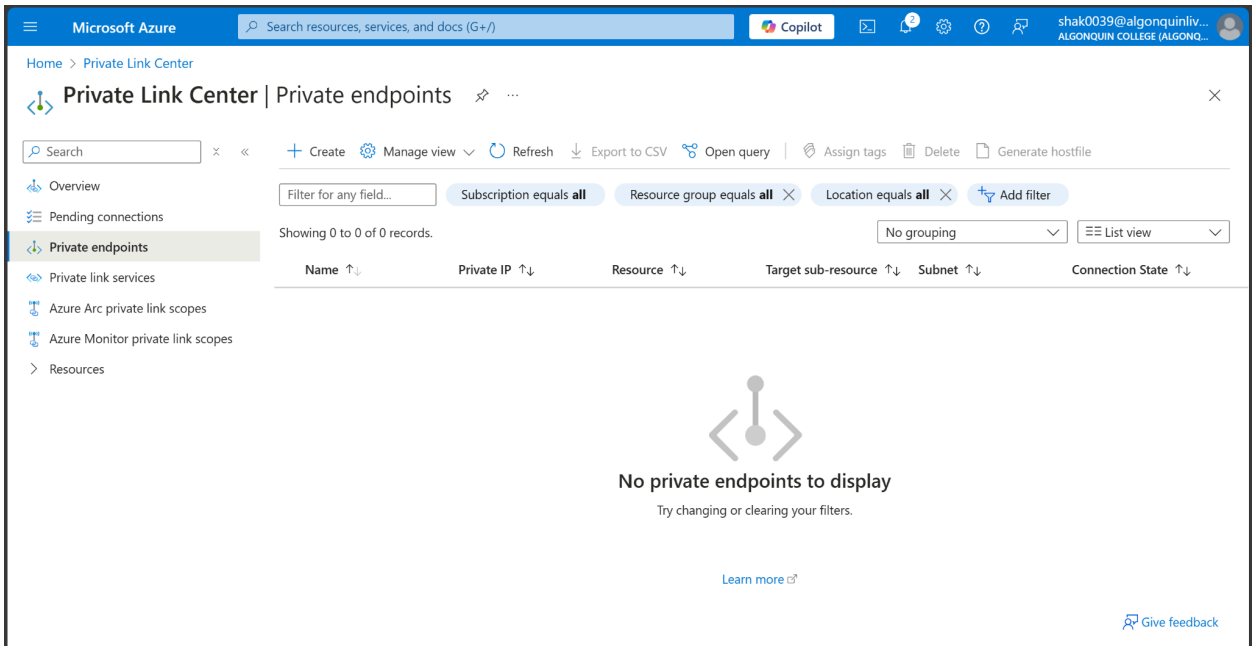


5. Select Save.



Create private endpoint

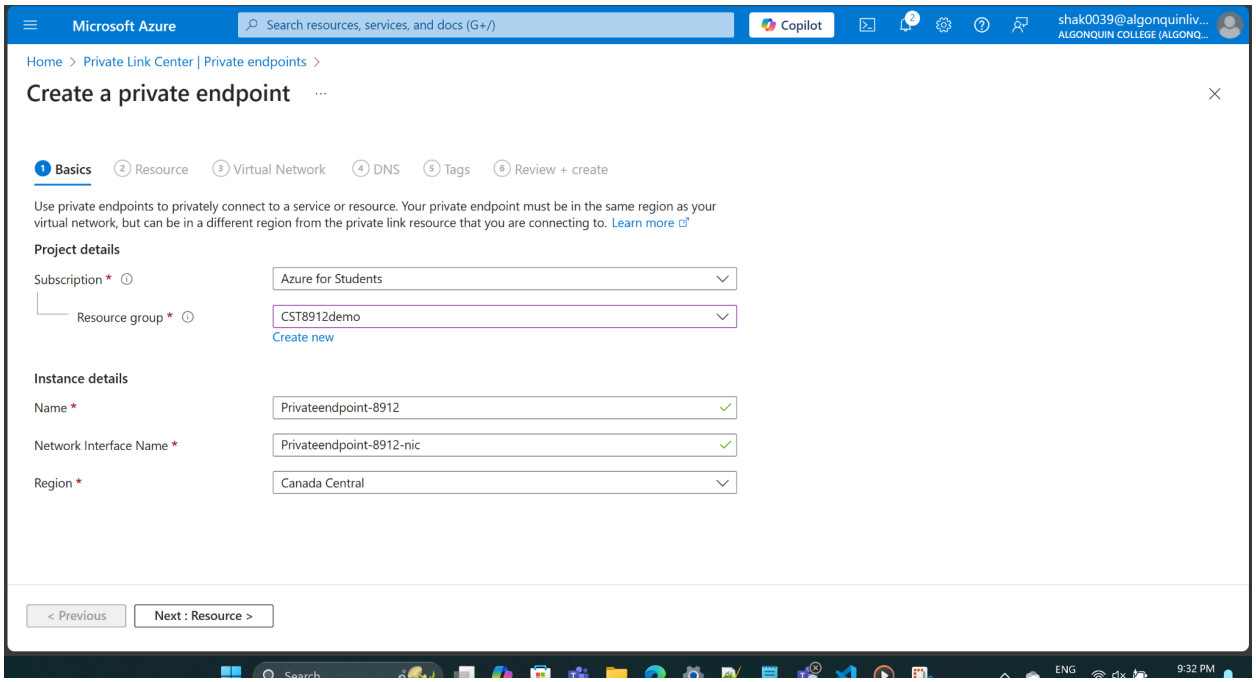
1. In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.



2. Select + Create in Private endpoints.

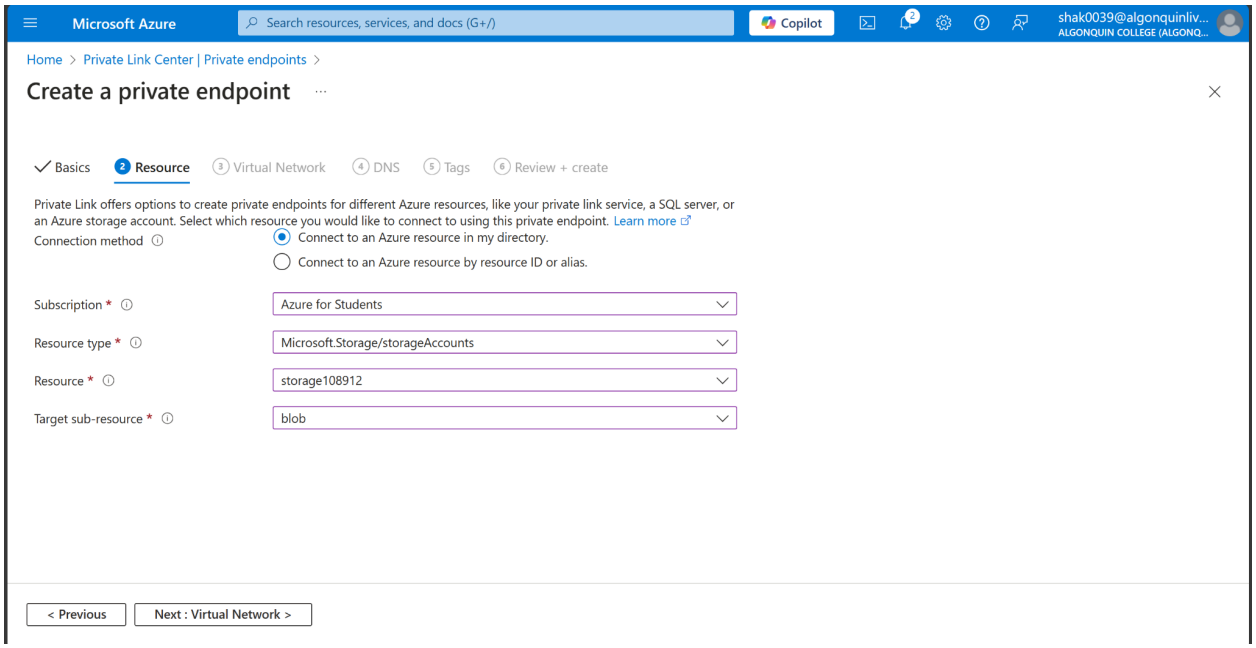
3. In the Basics tab of Create a private endpoint, enter or select the following information.

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



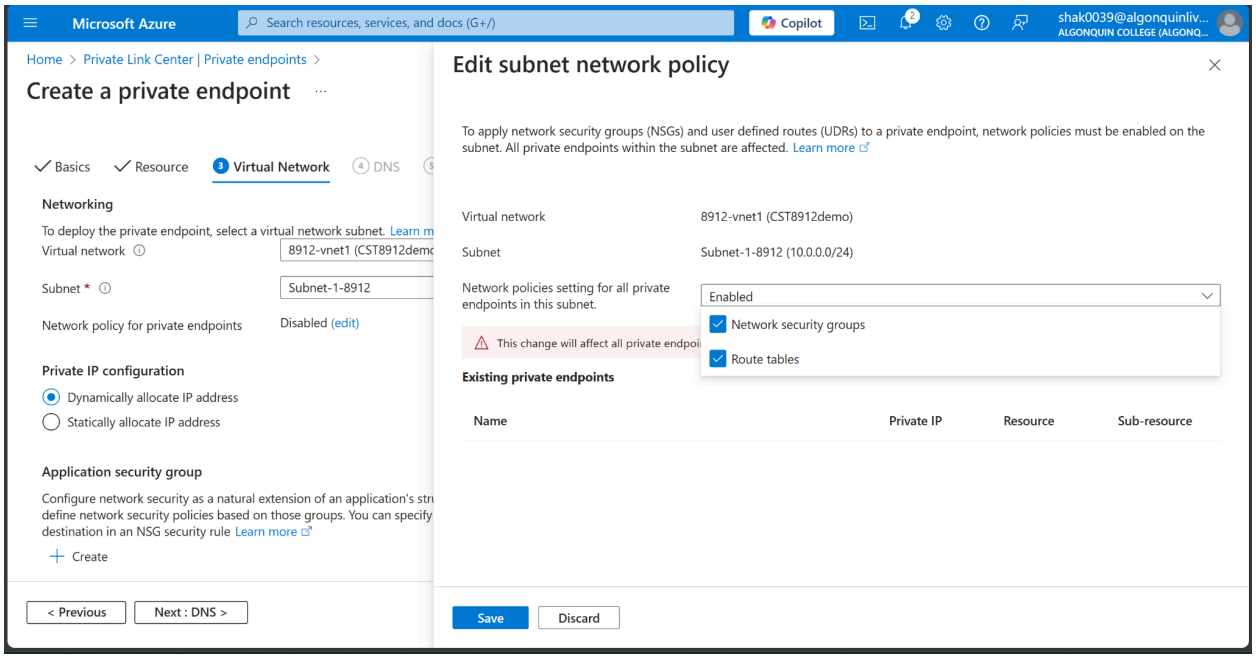
4. Select Next:Resource
5. In the Resource pane, enter or select the following information.

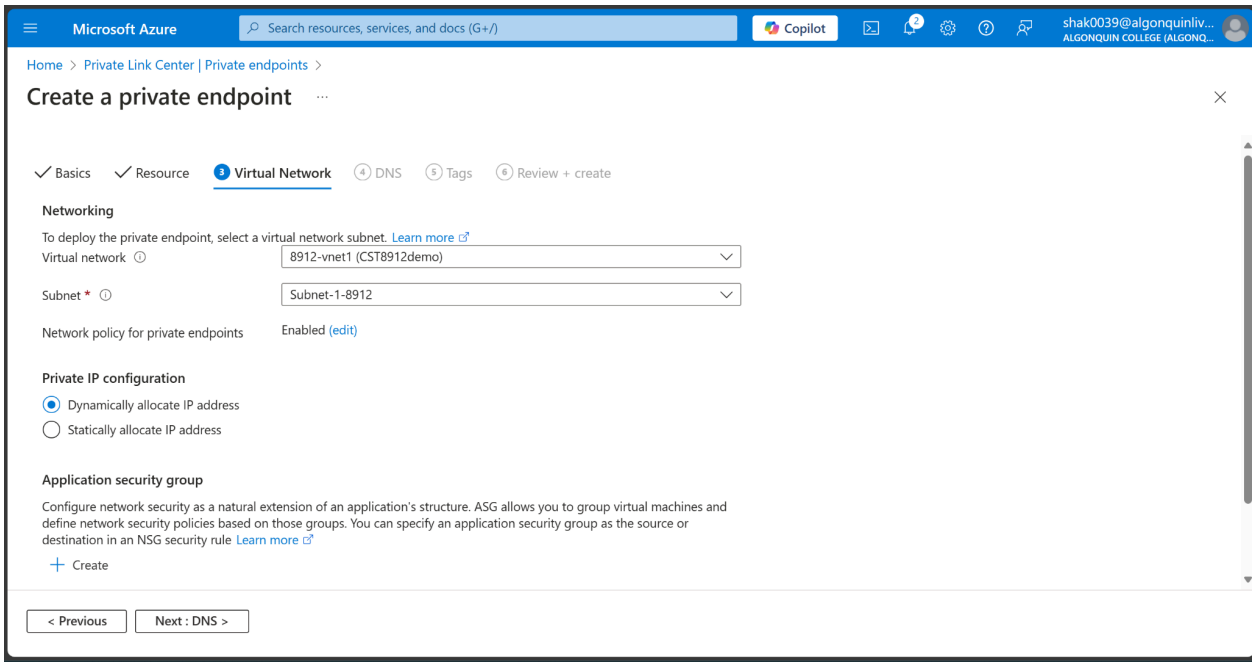
Setting	Value
Connection method	Leave the default of Connect to an Azure resource in my directory.
Subscription	Select your subscription.
Resource type	Select Microsoft.Storage/storageAccounts.
Resource	Select Storage1-8912 or your storage account.
Target subresource	Select blob.



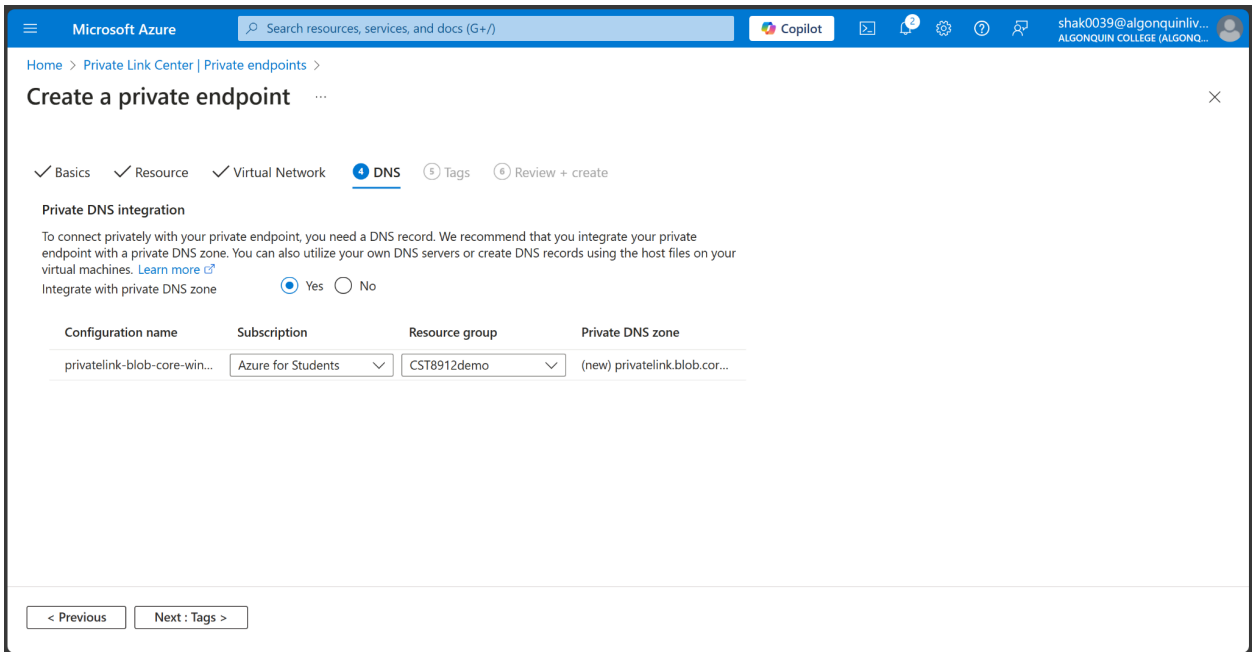
6. Select Next: Virtual Network.
7. In Virtual Network, enter or select the following information.

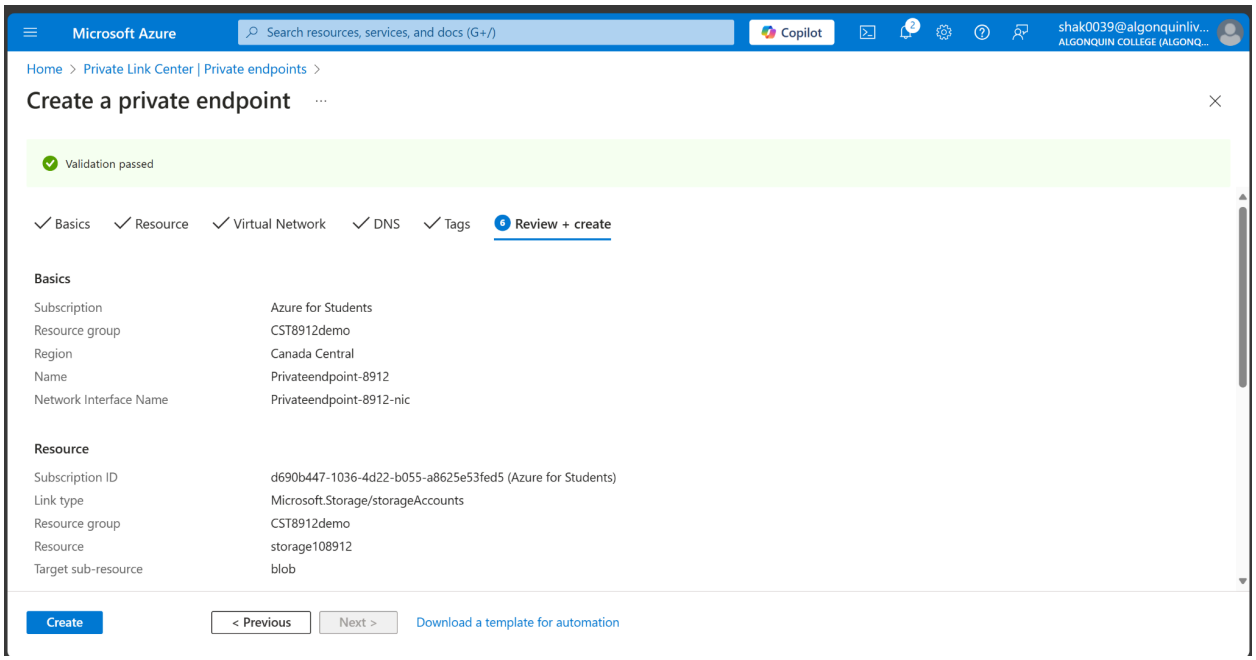
Setting	Value
Virtual network	Select 8912-vnet (CST8912demo).
Subnet	Select Subnet-1-8912.
Network policy for private endpoints	Select edit to apply Network policy for private endpoints. In Edit subnet network policy, select the checkbox next to Network security groups and Route Tables in the Network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

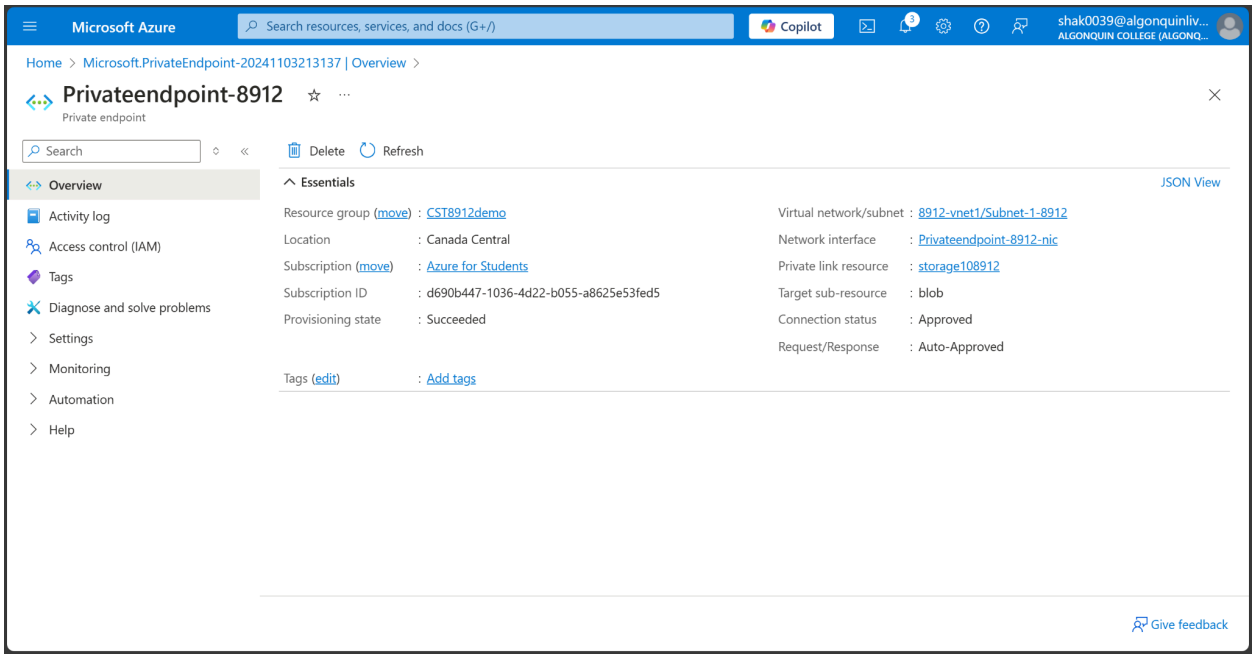




8. Select Next: DNS.
9. Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.
10. Select Create.

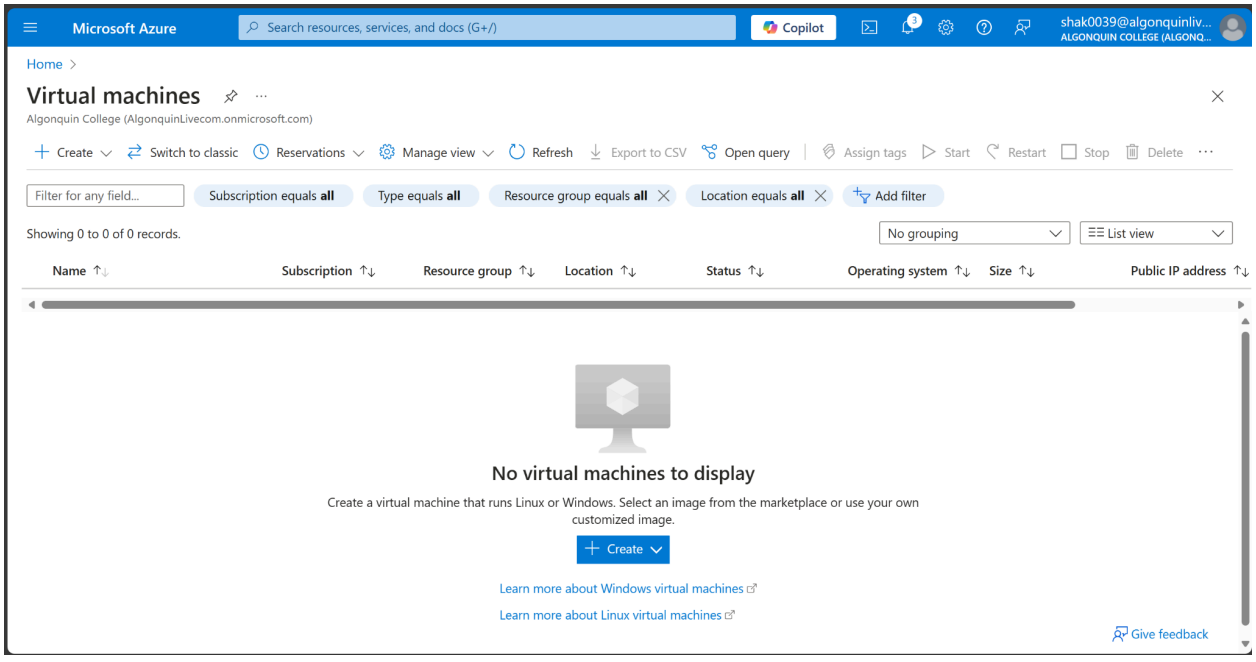

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Private Link Center | Private endpoints >
Create a private endpoint
Basics
Resource
Virtual Network
4 DNS
5 Tags
6 Review + create
Private DNS integration
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more
Integrate with private DNS zone
Yes
No
Configuration name
Subscription
Resource group
Private DNS zone
privatelink-blob-core-win...
Azure for Students
CST8912demo
(new) privatelink.blob.cor...
< Previous
Next : Tags >


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Private Link Center | Private endpoints >
Create a private endpoint
Validation passed
Basics
Resource
Virtual Network
DNS
Tags
6 Review + create
Basics
Subscription
Azure for Students
Resource group
CST8912demo
Region
Canada Central
Name
Privateendpoint-8912
Network Interface Name
Privateendpoint-8912-nic
Resource
Subscription ID
d690b447-1036-4d22-b055-a8625e53fed5 (Azure for Students)
Link type
Microsoft.Storage/storageAccounts
Resource group
CST8912demo
Resource
storage108912
Target sub-resource
blob
Create
< Previous
Next >
Download a template for automation



Create test virtual machine

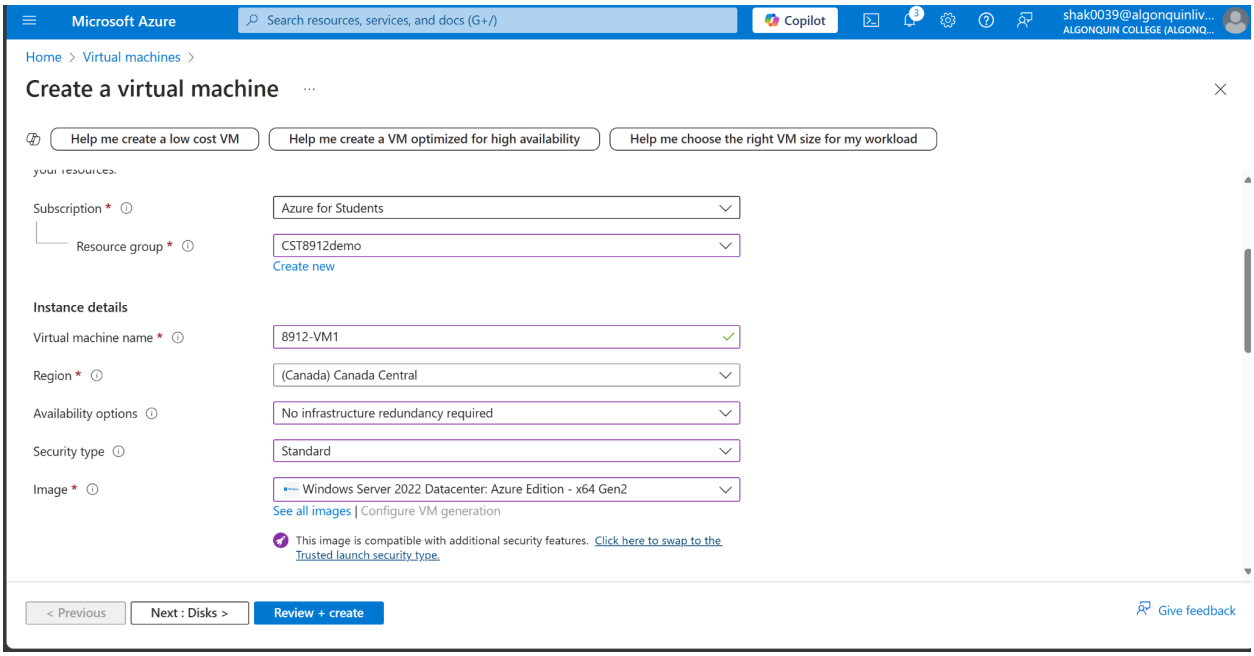
1. In the portal, search for and select Virtual machines.

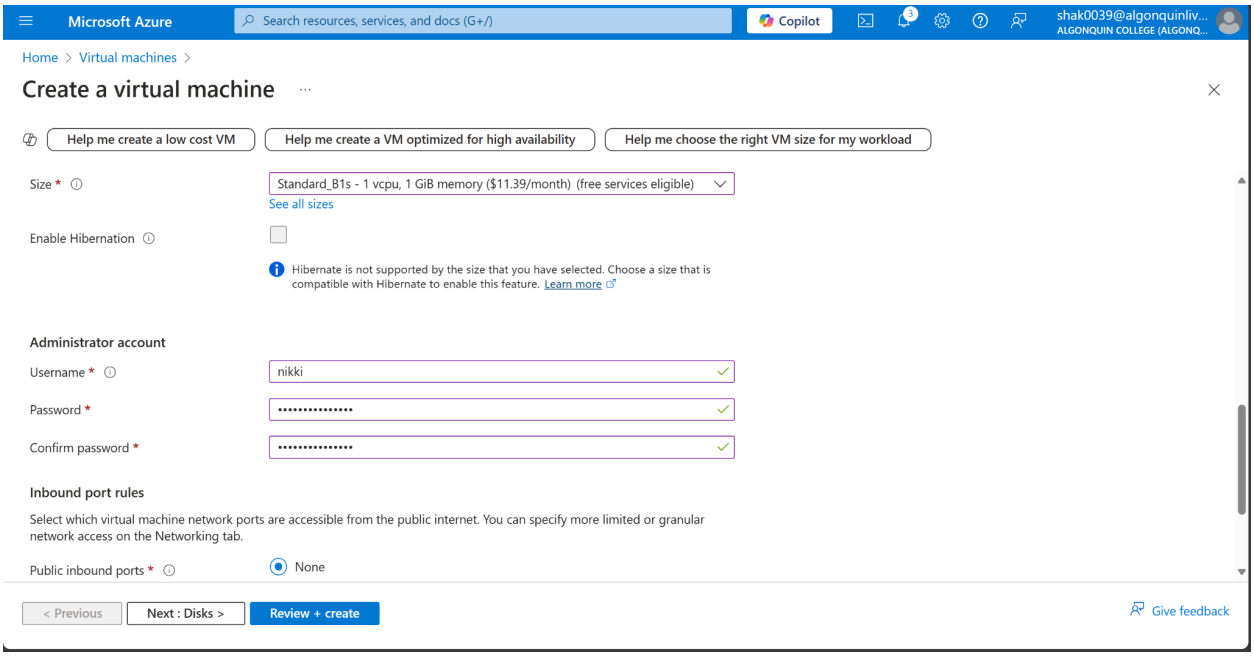


2. In Virtual machines, select + Create, then Azure virtual machine.

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

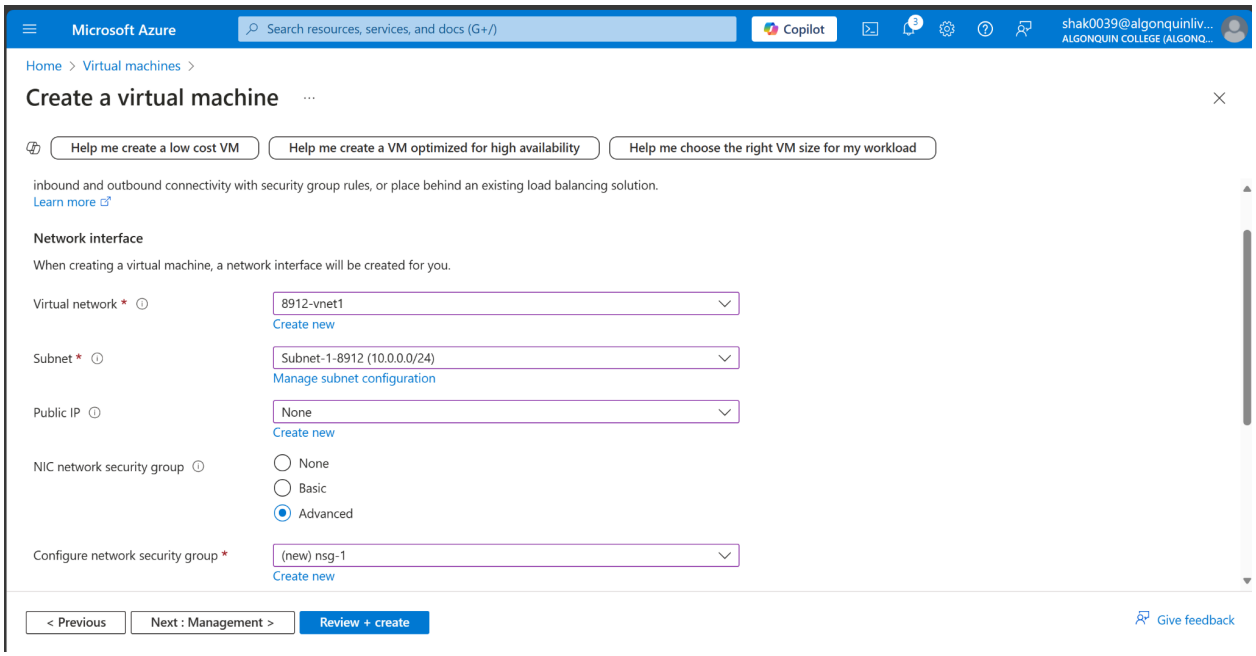


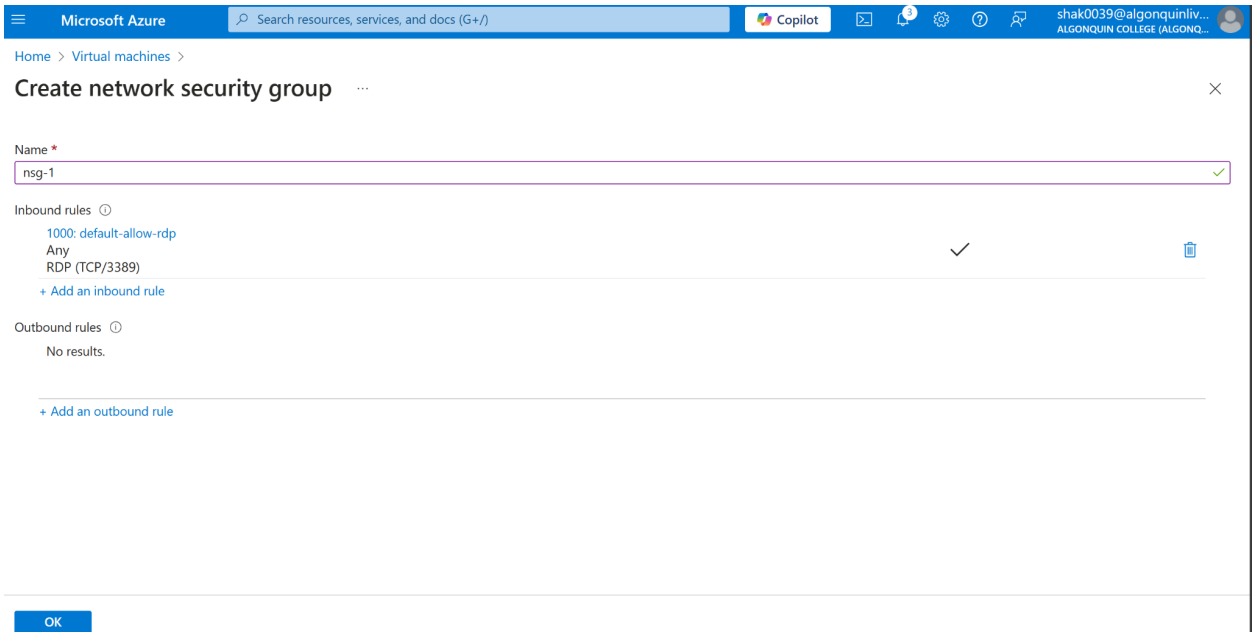


4. Select the Networking tab at the top of the page.
5. Enter or select the following information in the Networking tab:

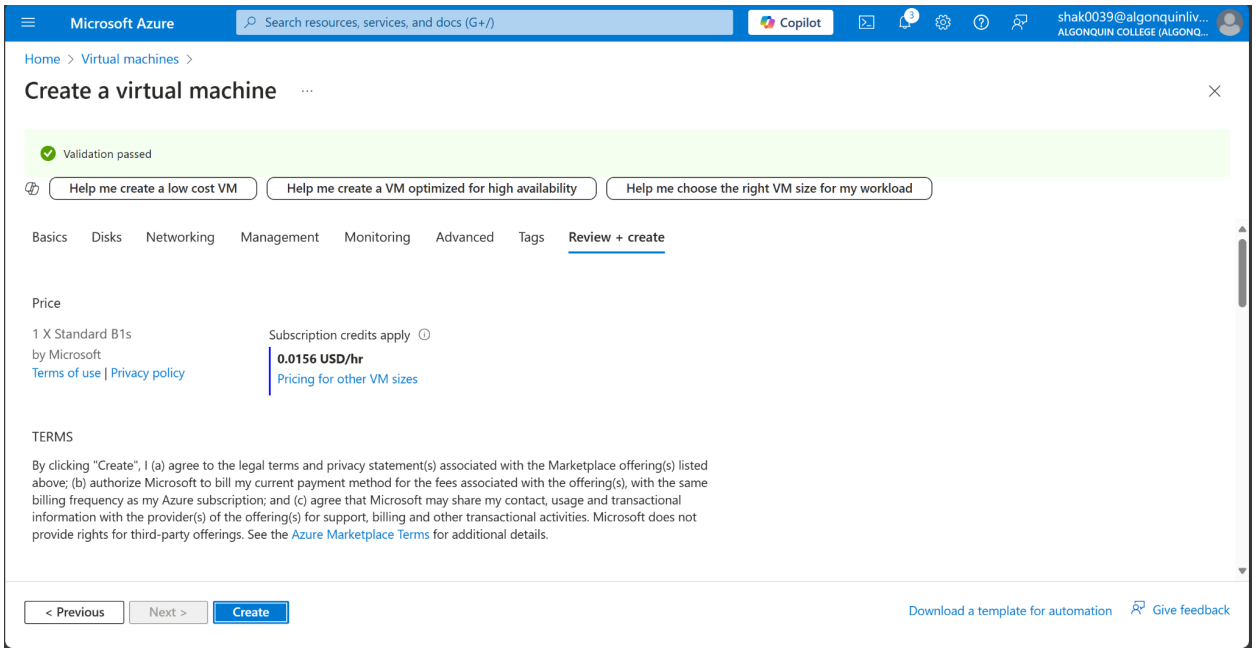
Setting	Value
Virtual Network	Select 8912-vnet (CST8912demo).
Subnet	Select Subnet-1-8912.

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.

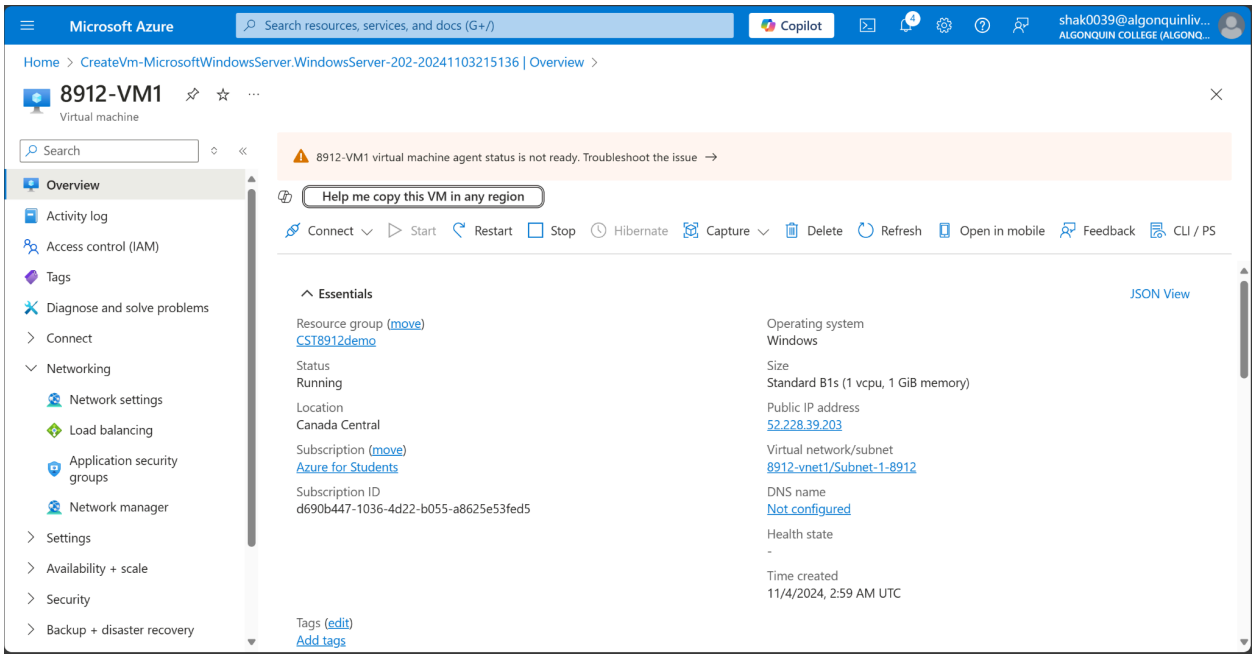




6. Leave the rest of the settings at the defaults and select Review + create.

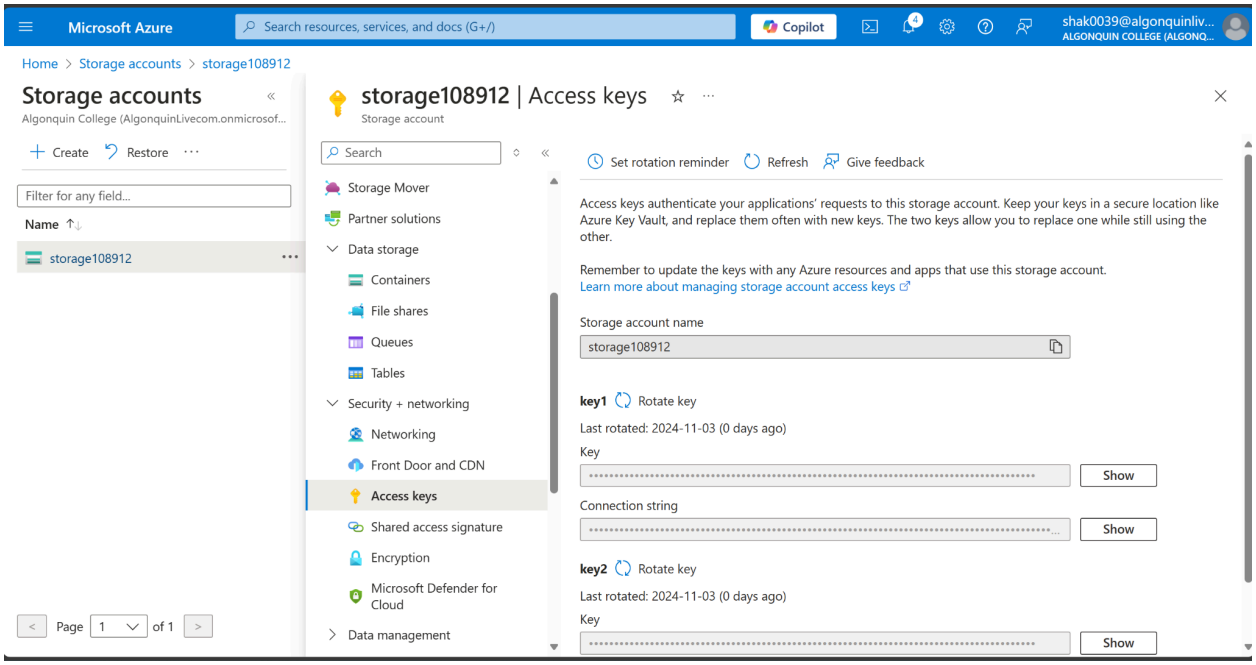


7. Review the settings and select Create.



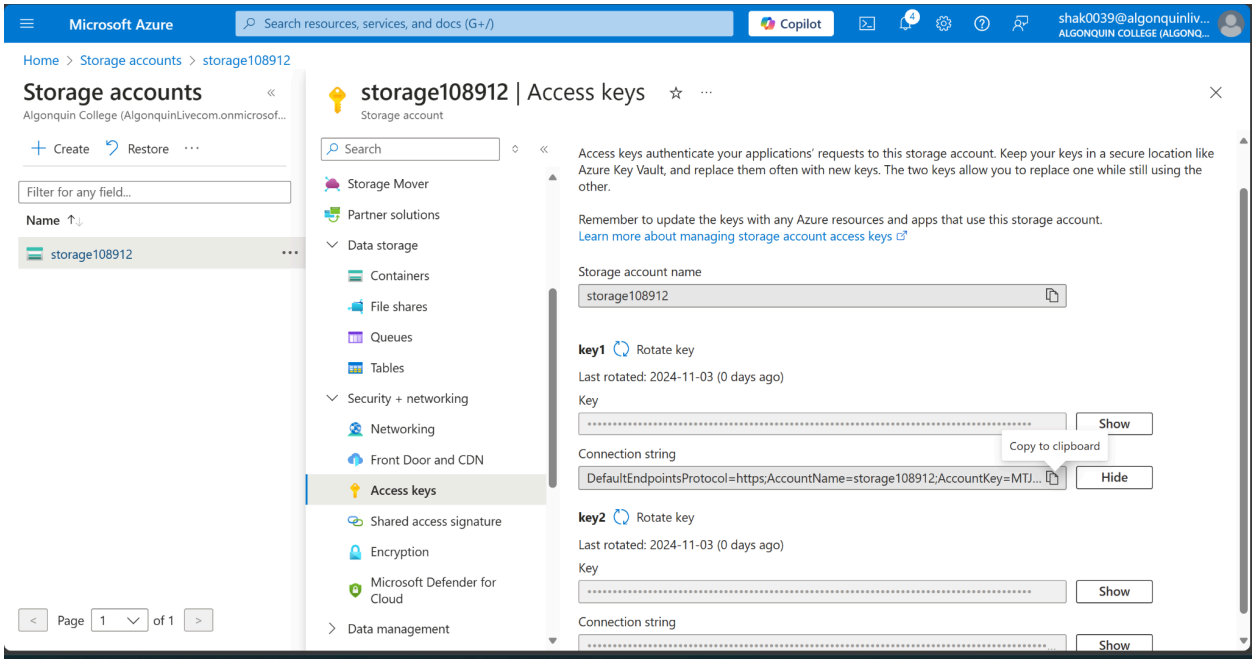
Storage access key

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.



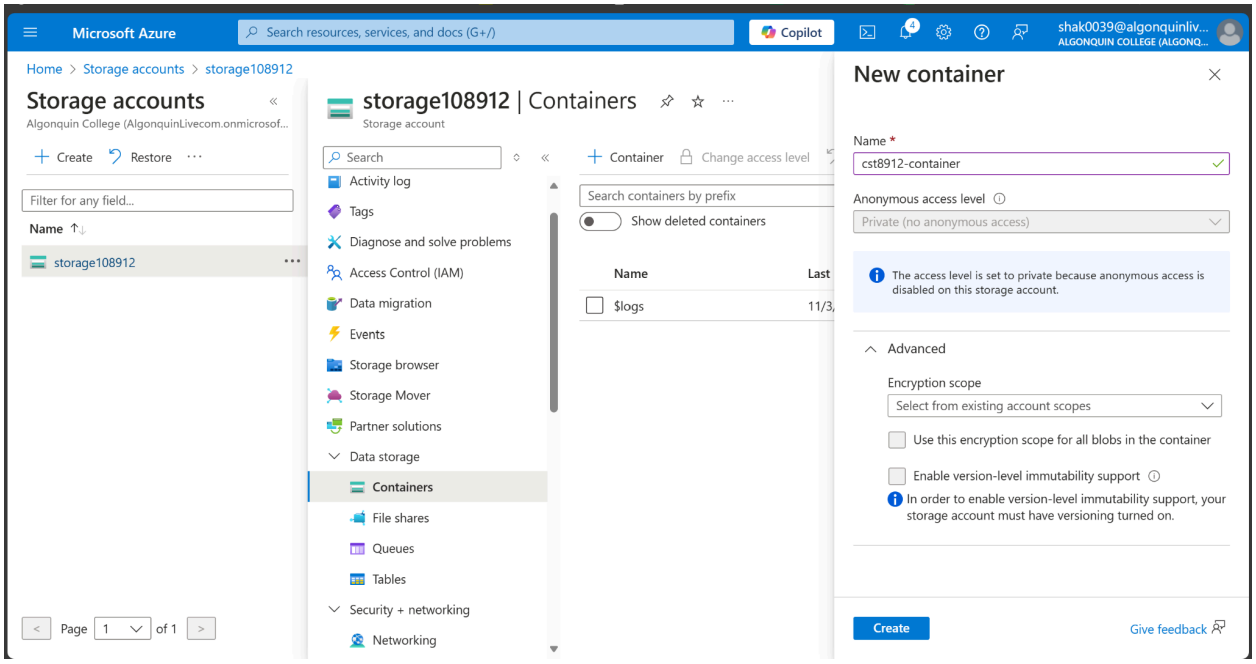
4. Select Show, then select copy on the Connection string for key1.

MTJcdVk8shCVOic74js3eUiHJ/7wb4UWKPUw6WtdfRpMSoBir3vuNXVgkb8bSHV8O0dOW+SYpIVI+AStvDWOhg==

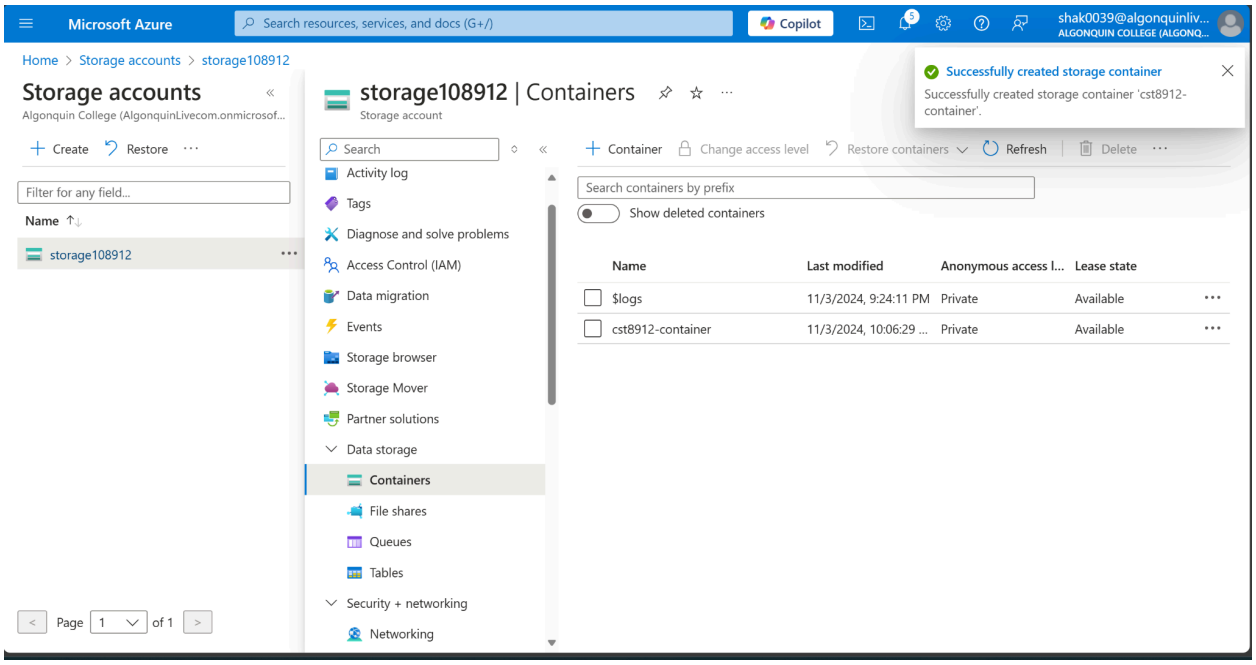


Add a blob container

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.

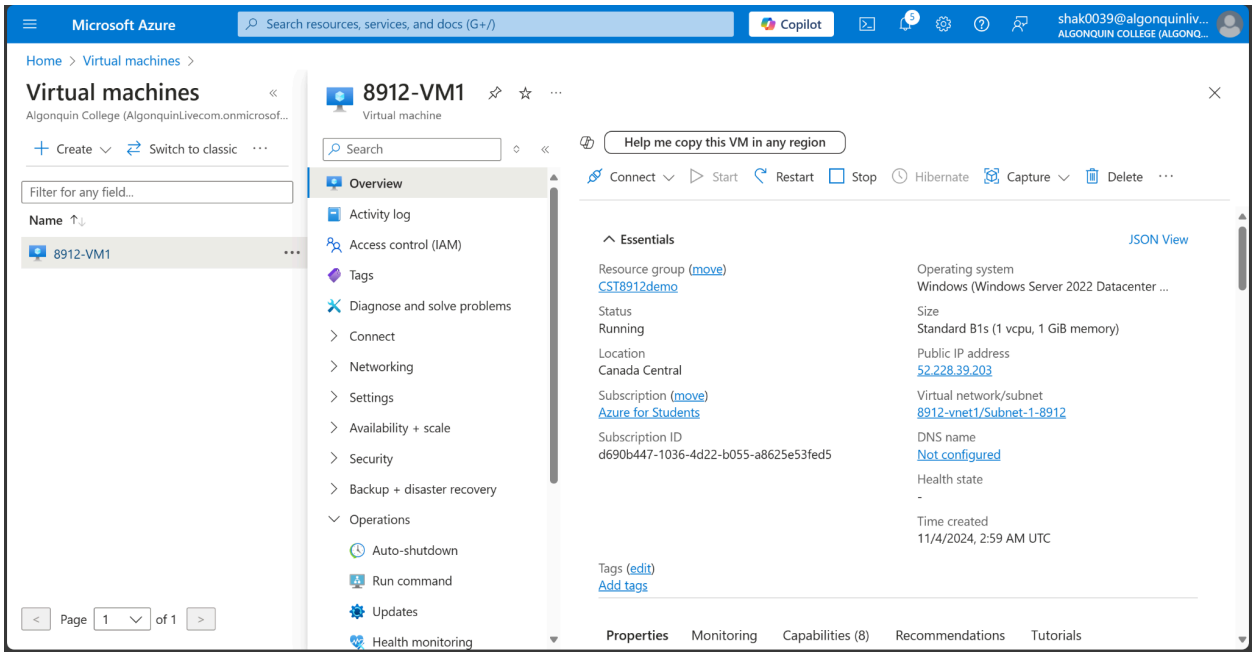


6. Select Create.



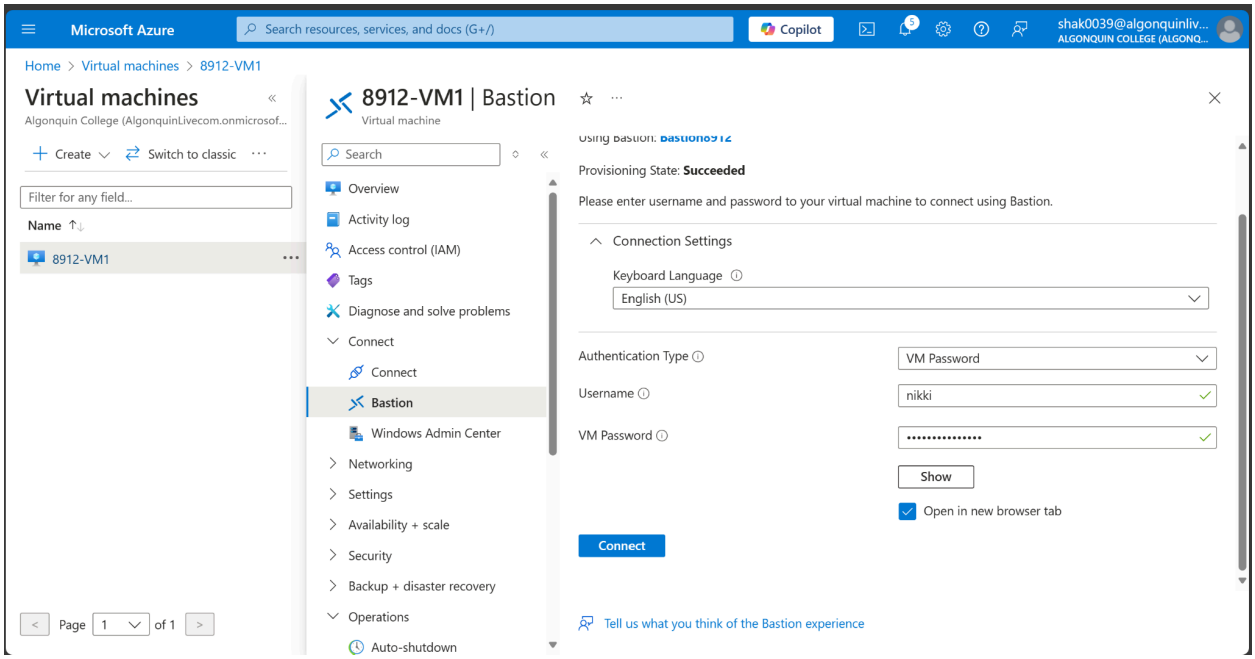
Test connectivity to private endpoint

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.

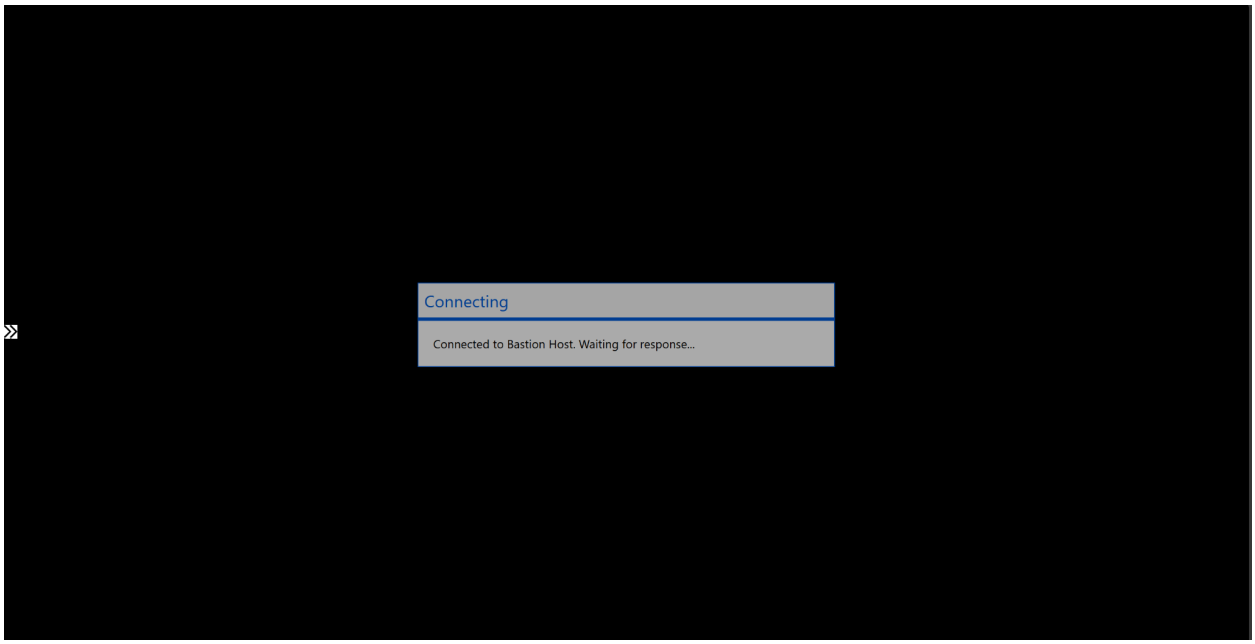


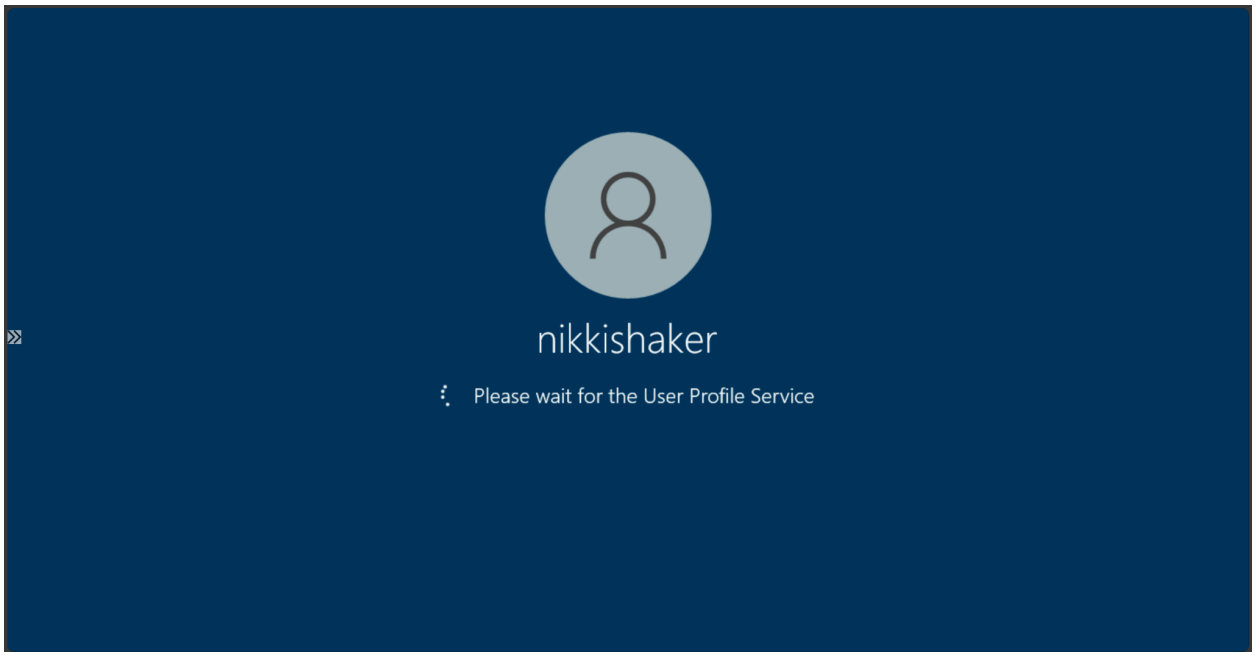
3. In Operations, select Bastion.

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



5. Select Connect.



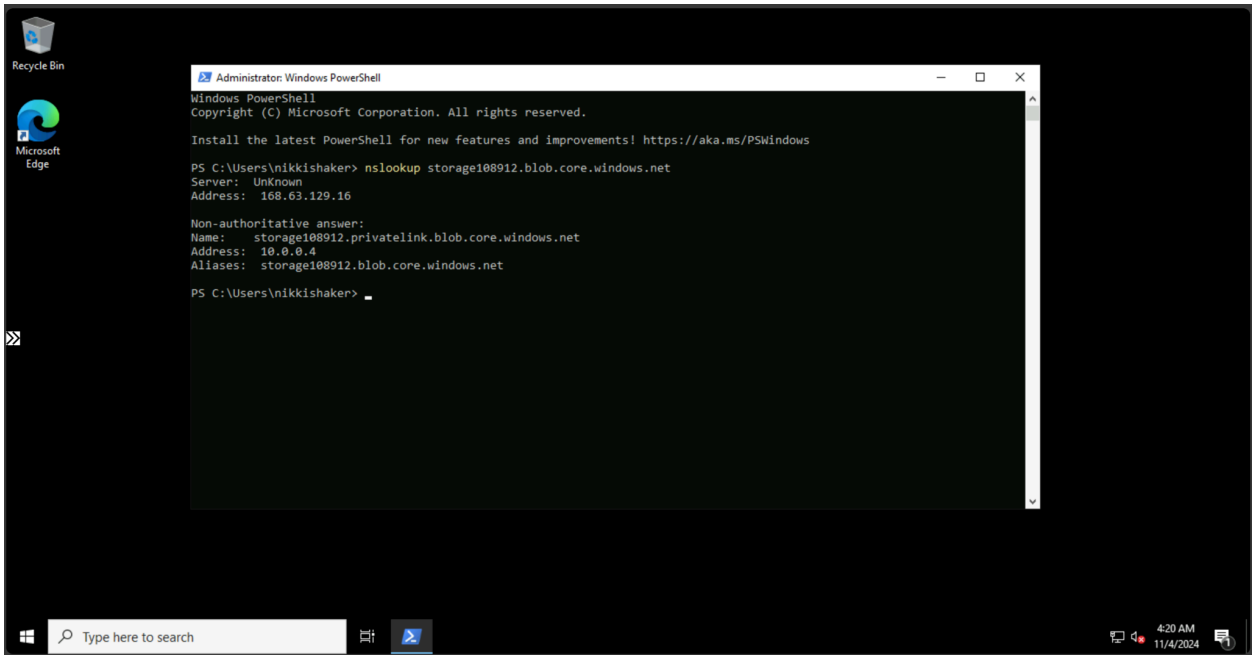


6. Open Windows PowerShell on the server after you connect.
7. Enter nslookup <storage-account-name>.blob.core.windows.net. Replace <storage-account-name> with the name of the storage account you created in the previous steps. The following example shows the output of the command.

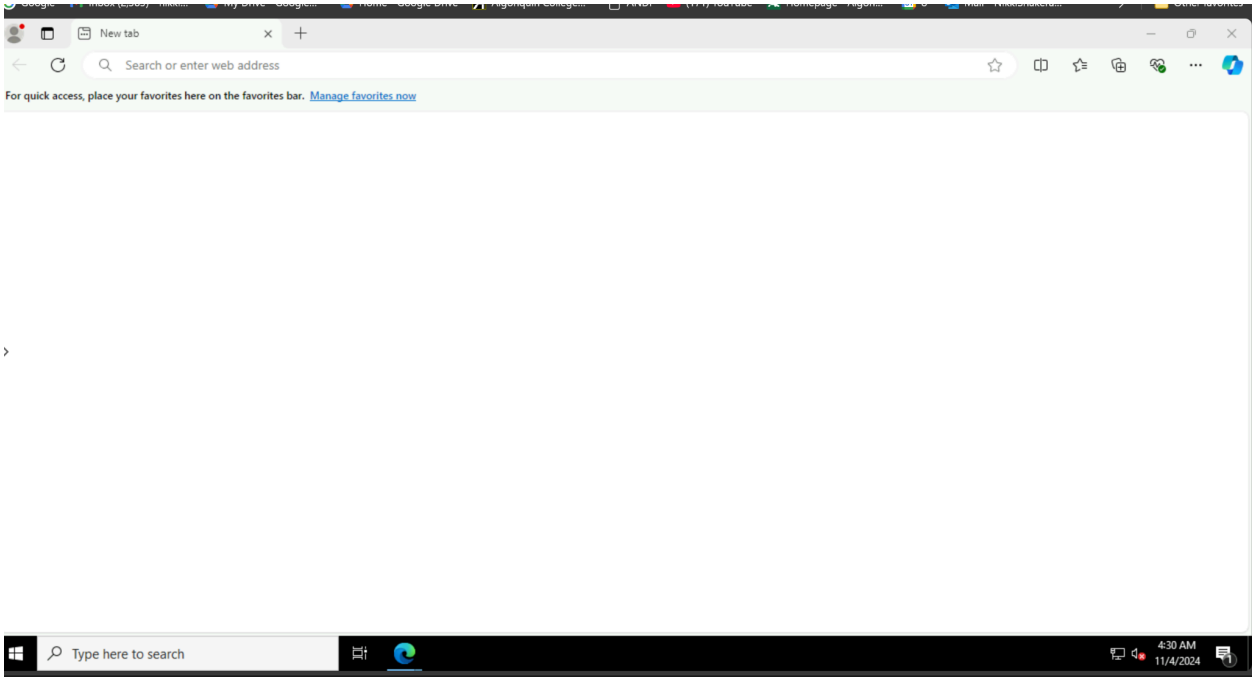
   Server: UnKnown
   Address: 168.63.129.16

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

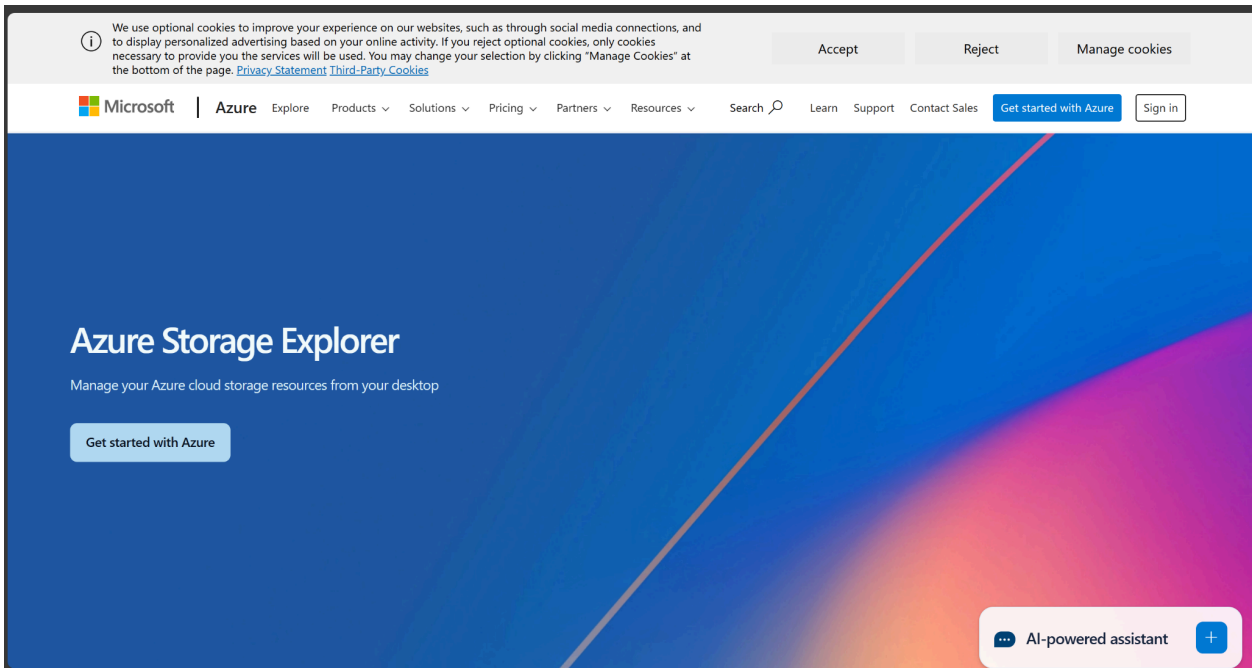
   A private IP address of 10.0.0.10 is returned for the storage account name. This address is in Subnet-1-8912 subnet of 8912-vnet virtual network you created previously.



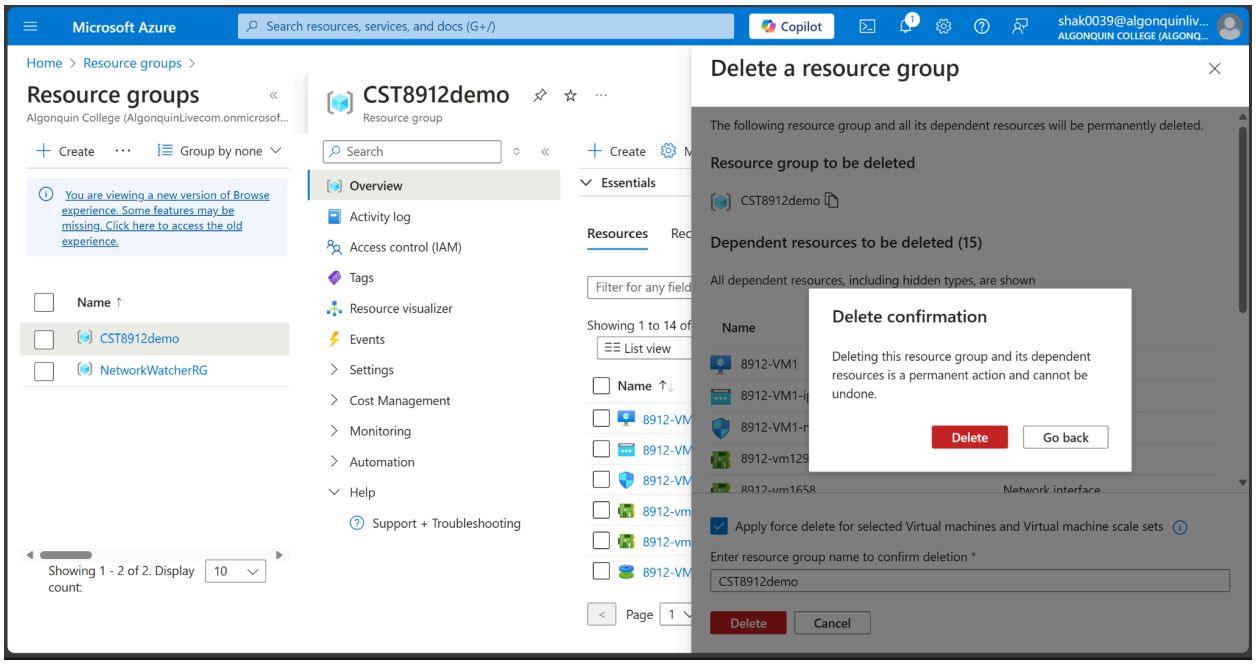
8. Install Microsoft Azure Storage Explorer on the virtual machine.

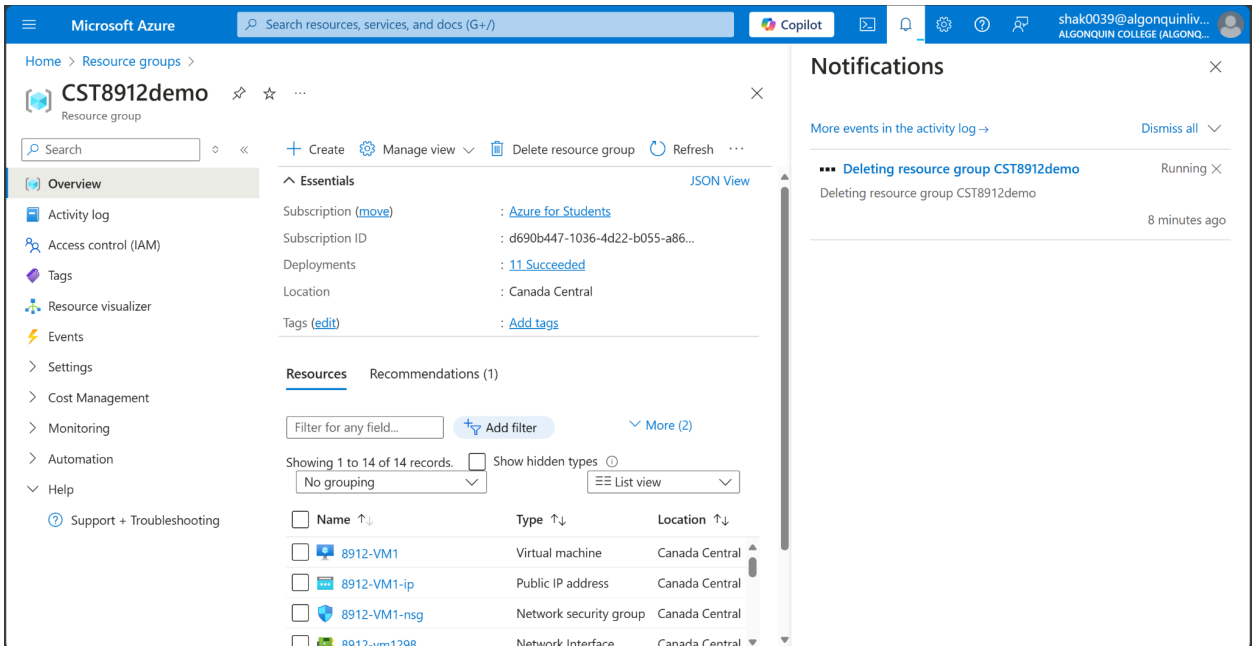


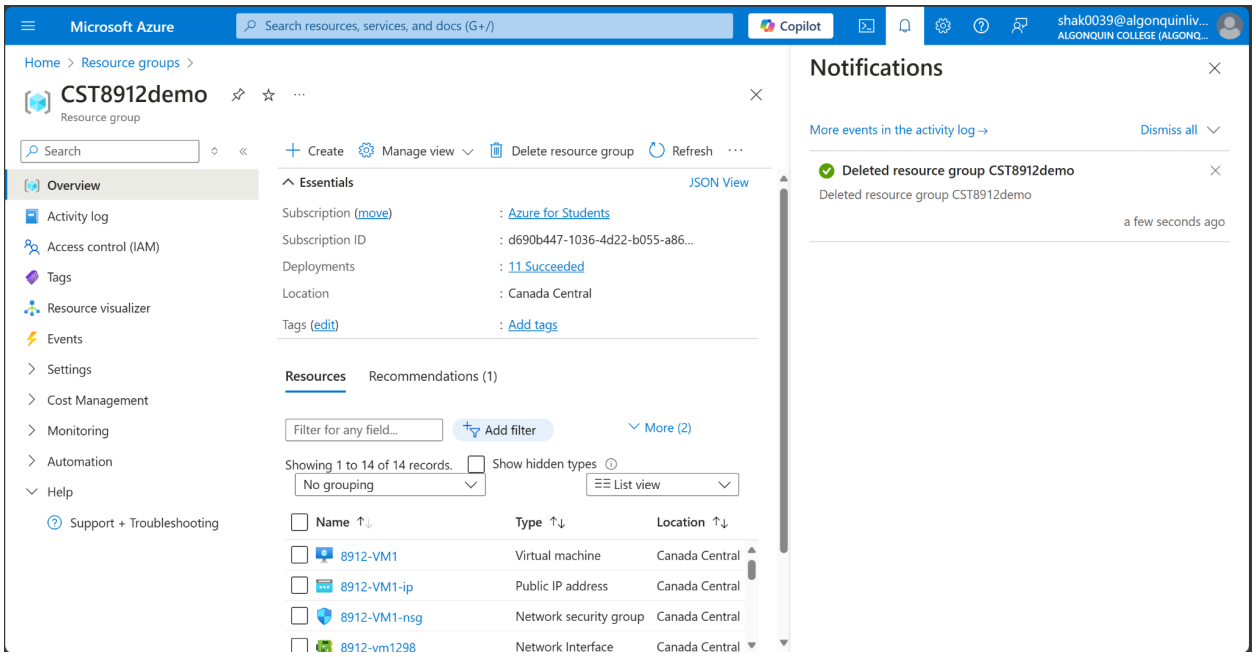
9. Select Finish after the Microsoft Azure Storage Explorer is installed. Leave the box checked to open the application.

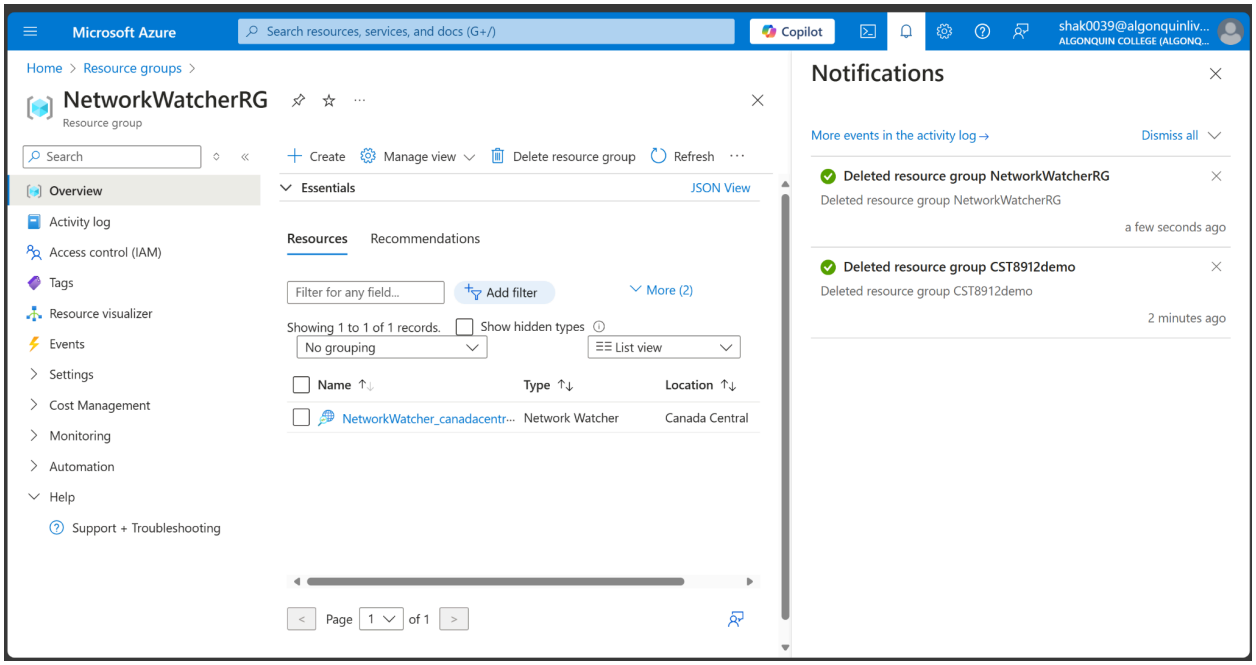


10. Select the Power plug symbol to open the Select Resource dialog box in the left-hand toolbar.
11. In Select Resource , select Storage account or service to add a connection in Microsoft Azure Storage Explorer to your storage account that you created in the previous steps.
12. In the Select Connection 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. 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.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Resource groups >
Resource groups
Algonquin College (AlgonquinLivecom.onmicrosof...
Create
Group by none
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
CST8912demo
NetworkWatcherRG
Showing 1 - 2 of 2. Display count: 10
CST8912demo
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Support + Troubleshooting
Create
Essentials
Resources
Filter for any field
Showing 1 to 14 of
List view
Name
Page 1
Delete a resource group
The following resource group and all its dependent resources will be permanently deleted.
Resource group to be deleted
CST8912demo
Dependent resources to be deleted (15)
All dependent resources, including hidden types, are shown
Name
8912-VM1
Delete confirmation
Deleting this resource group and its dependent resources is a permanent action and cannot be undone.
Delete
Go back
Apply force delete for selected Virtual machines and Virtual machine scale sets
Enter resource group name to confirm deletion *
CST8912demo
Delete
Cancel


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Resource groups >
CST8912demo
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Support + Troubleshooting
Create
Manage view
Delete resource group
Refresh
Essentials
JSON View
Subscription (move) : Azure for Students
Subscription ID : d690b447-1036-4d22-b055-a86...
Deployments : 11 Succeeded
Location : Canada Central
Tags (edit) : Add tags
Resources
Recommendations (1)
Filter for any field...
Add filter
More (2)
Showing 1 to 14 of 14 records.
Show hidden types
No grouping
List view
Name
Type
Location
8912-VM1
Virtual machine
Canada Central
8912-VM1-ip
Public IP address
Canada Central
8912-VM1-nsg
Network security group
Canada Central
Notifications
More events in the activity log →
Dismiss all
Deleting resource group CST8912demo
Running
Deleting resource group CST8912demo
8 minutes ago


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Resource groups >
CST8912demo
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Support + Troubleshooting
Create
Manage view
Delete resource group
Refresh
Essentials
JSON View
Subscription (move) : Azure for Students
Subscription ID : d690b447-1036-4d22-b055-a86...
Deployments : 11 Succeeded
Location : Canada Central
Tags (edit) : Add tags
Resources
Recommendations (1)
Filter for any field...
Add filter
More (2)
Showing 1 to 14 of 14 records.
Show hidden types
No grouping
List view
Name
Type
Location
8912-VM1
Virtual machine
Canada Central
8912-VM1-ip
Public IP address
Canada Central
8912-VM1-nsg
Network security group
Canada Central
8912-vm1298
Network Interface
Canada Central
Notifications
More events in the activity log →
Dismiss all
Deleted resource group CST8912demo
Deleted resource group CST8912demo
a few seconds ago


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shak0039@algonquinliv...
ALGONQUIN COLLEGE (ALGONQ...
Home > Resource groups >
NetworkWatcherRG
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Support + Troubleshooting
Create
Manage view
Delete resource group
Refresh
Essentials
JSON View
Resources
Recommendations
Filter for any field...
Add filter
More (2)
Showing 1 to 1 of 1 records.
Show hidden types
No grouping
List view
Name
Type
Location
NetworkWatcher_canadacentr...
Network Watcher
Canada Central
Page 1 of 1
Notifications
More events in the activity log →
Dismiss all
Deleted resource group NetworkWatcherRG
Deleted resource group NetworkWatcherRG
a few seconds ago
Deleted resource group CST8912demo
Deleted resource group CST8912demo
2 minutes ago

Lab Report

This lab focused on configuring and testing Azure Private Link to securely connect virtual networks to Azure resources without exposing data to the internet. First, I created a virtual network, Bastion Host, and storage account. Then, I disabled public access to the storage account, and set up a private endpoint to establish private connectivity. A test virtual machine was created and connected using Azure Bastion; however, I had connectivity issues, because of a popup blocker that caused a login failure error, which I was able to fix by making changes to the popup blocker. A test virtual machine was created and connected using Azure Bastion, and in order to verify secure access to the storage account, I used a private IP using PowerShell. I also used Microsoft Azure Storage Explorer to confirm blob storage connectivity through the private endpoint. Finally, I cleaned up resources to avoid costs, which shows how the Azure Private Link enhances security and network architecture by facilitating secure, private access to Azure PaaS services.