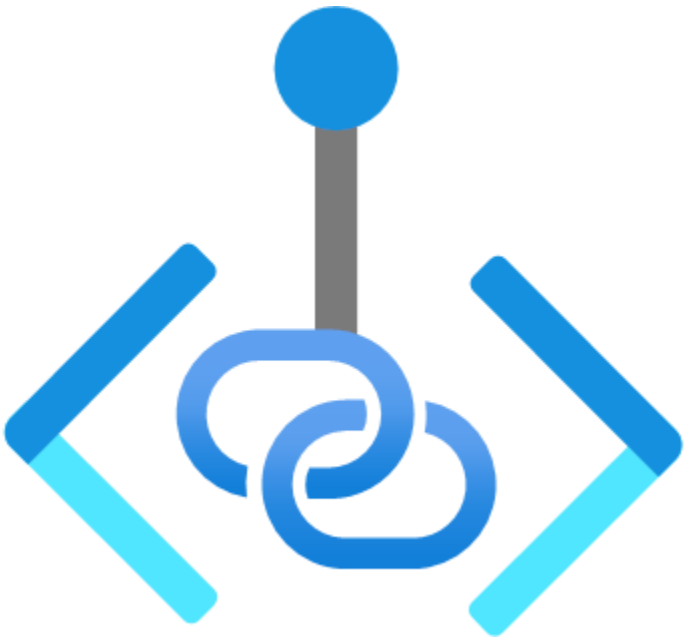
Exploring Azure Private Links and Private Endpoints



(*Pricing - Azure Private Link | Microsoft Azure*, n.d.)

Donna Ha
041174159
CST8912
Lab Activity 6

Abstract

This lab report explores the usage of Private Links and Private Endpoints to establish a secure and simple connection between a Virtual Network and Azure resources. The lab involved setting up a virtual network with Azure Bastion, a storage account, a Private Endpoint that the storage account uses for connection purposes, and a virtual machine for testing purposes. Azure is used in this lab but can be replicated in any cloud provider, such as AWS or GCP. The results of this lab demonstrate successful communication between the storage account and the virtual machine through the Private Endpoint, ensuring enhanced security and isolation from public networks.

Introduction

Azure Private Links simplify network architectures and offer secure connections between private endpoints. This is done by removing the risk of data exposure to the public internet. Only clients with private endpoints can obtain connectivity from a virtual network to Azure services, which include PaaS, customer-owned, or Microsoft partner services.

A private endpoint is a network interface that offers a safe and secure connection between the virtual network and the Azure service; Private endpoints replace the resource's public endpoint. By removing public access, we are eliminating or minimizing threats and attacks that can occur with public access. In this scenario, public access is not required, so private endpoints can be used to establish connections safely and securely.

The objective of this lab is to explore the usage and benefits of Private Links and Private Endpoints; this will be done by using Azure.

Background Research (Literature Review)

Azure Private Link enables employees, vendors, and customers to securely access Azure resources through a network interface, called a private endpoint.

A typical method for connectivity is to use a public endpoint. The resource is assigned a public IP address, which means the connection between them takes place over the Internet. The exposure to the Internet introduces multiple security risks, such as DNS attacks, IP spoofing Attacks, the Man-in-the-middle attack, etc (Sudha et al., 2013). DNS attacks take advantage of vulnerabilities in the domain name system, manipulating it for malicious purposes. Some types of DNS attacks include Zero-day attacks, Cache poisoning, Denial of service (DoS), Distributed denial of service (DDoS), DNS amplification, DNS tunneling, etc. DNS attacks are very common and can lead to data breaches, loss of customer confidence, decrease in sales and revenue, legal action, and regulatory punishments (Awati, 2024).

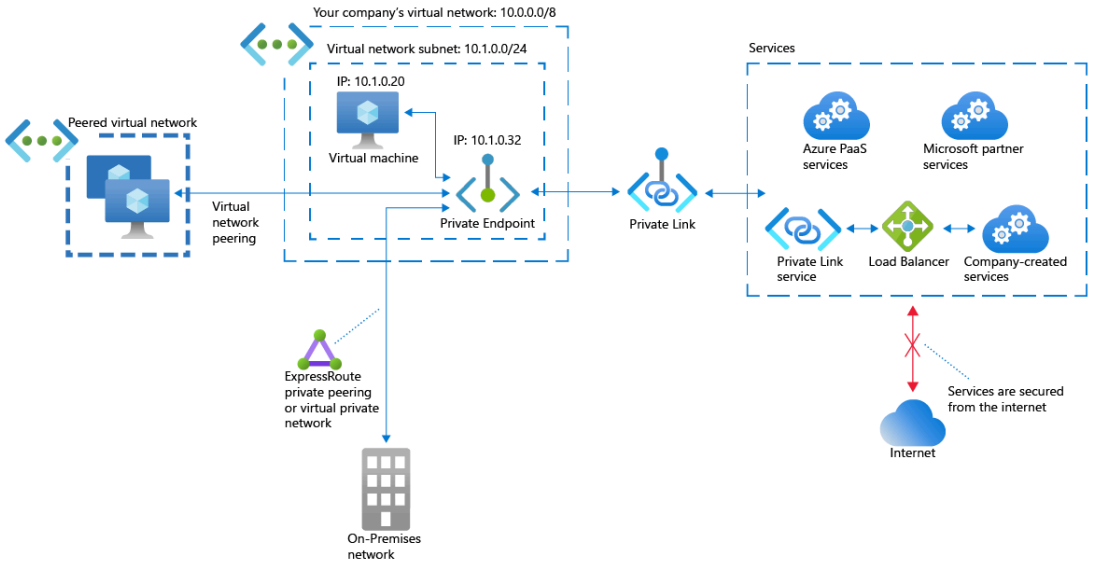
Replacing the public endpoint with a private network interface reduces and prevents those security risks. “Private Endpoint is the key technology behind Private Link. Private Endpoint is a network interface that enables a private and secure connection between your virtual network and an Azure service” (*What is Azure private link?*).

By changing the connectivity method from public endpoint to private endpoint, traffic to and from the resource completely bypasses the public internet; the connection uses the Microsoft Azure backbone network instead. However, the public endpoint of the resource still exists and is also a security concern. Thus, it is good practice to disable the Azure resource’s public endpoint to eliminate these potential risks.

Azure Private Endpoints are created and added to the network configuration. “Private Endpoint takes an unused private IP address from the address space of a specified subnet in your virtual network” (*How Azure Private Link Works*).

Azure Private Link provides private access to PaaS services and Microsoft Partner services on Azure, private access to Azure services in any region, nonpublic routes to Azure services, disable function for public endpoint, protection against data exfiltration, and private access to your own Azure services (*What is Azure private link?*).

Below is a diagram that shows how Private Link and Private Endpoint work.



(*How Azure Private Link Works*, n.d.)

Methodology

(From given lab specs)

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.

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.

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 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.

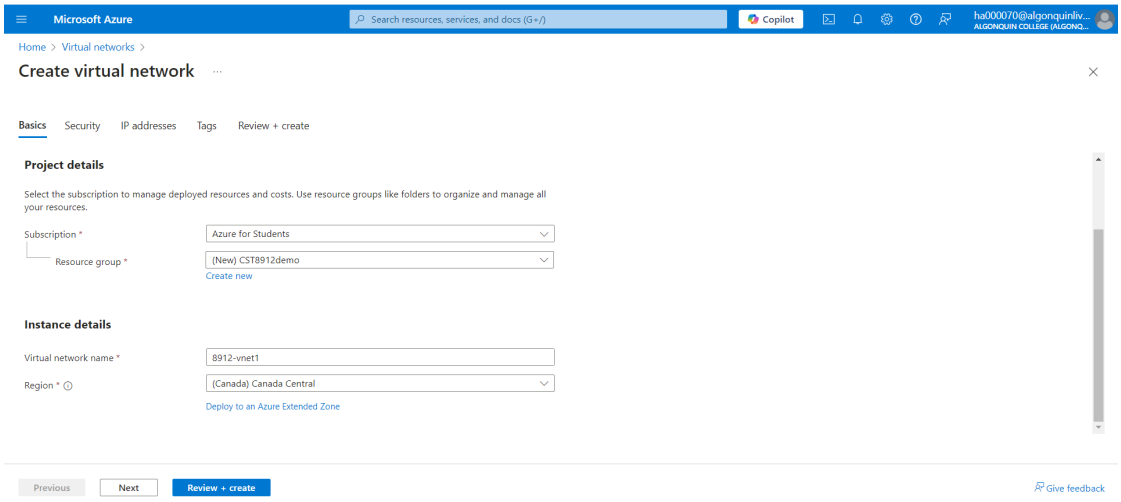
21. Clean all the resources created during the lab and document all the steps using screenshots and paste that in the lab report.

Results

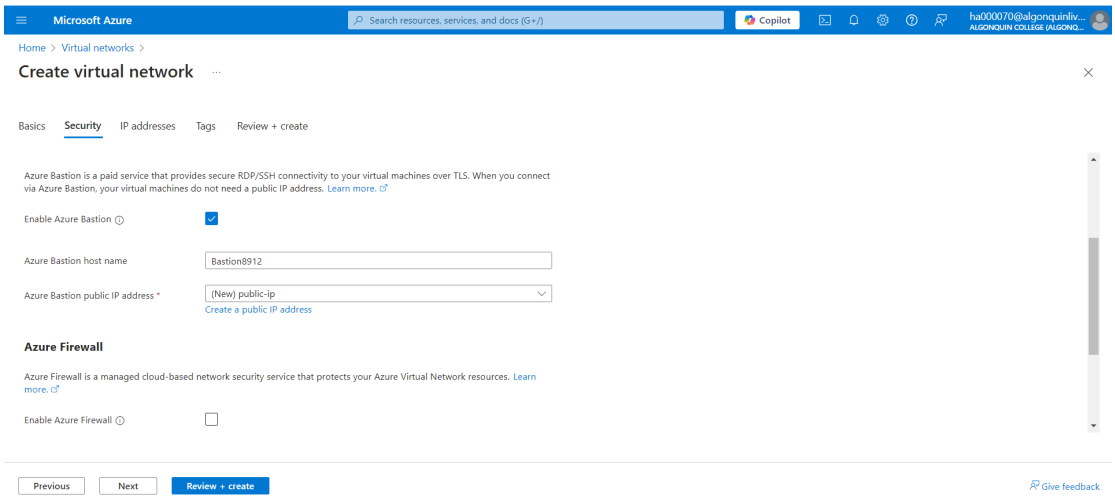
Note: All resources will be in the resource group: CST8912demo

1. Create a virtual network and Bastion host

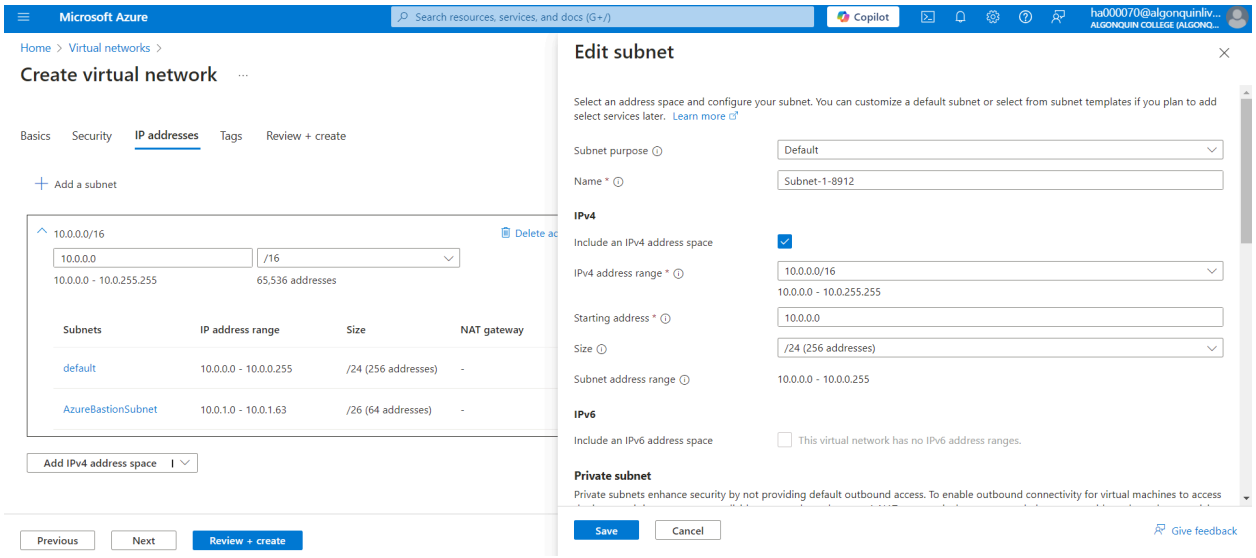
Create a virtual network named 8912-vnet1, in the Canada Central region.
Canada Central is chosen as the region for low latency as it is close to our location.



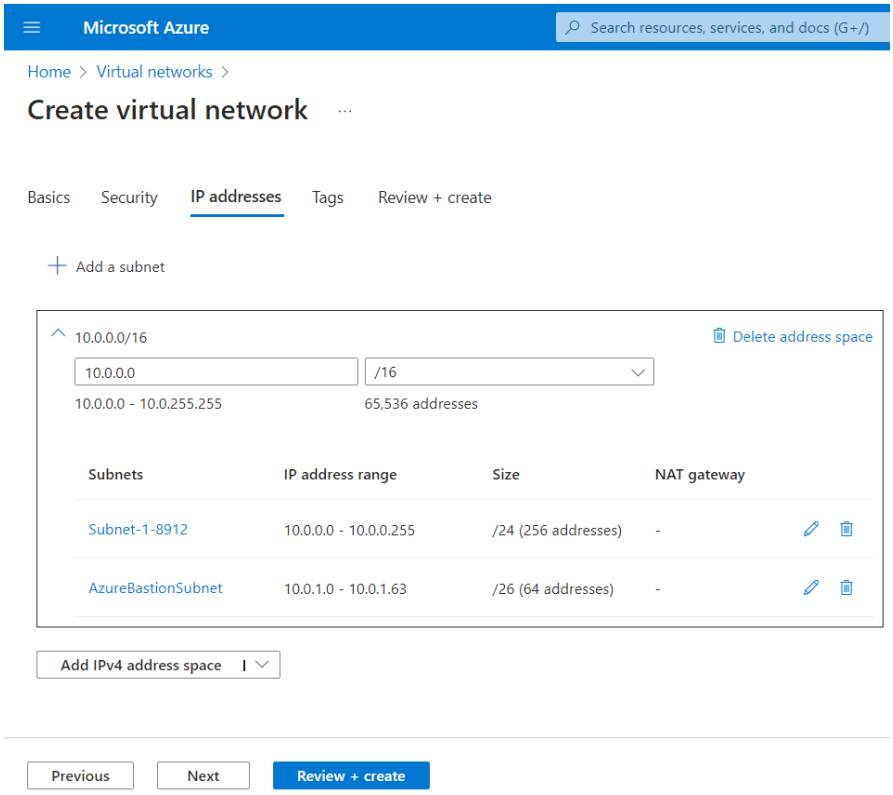
Azure Bastion is enabled in the security tab to allow SSH or RDP connection to the VMs that are in this virtual network. VMs will use private IP addresses, enhancing security.



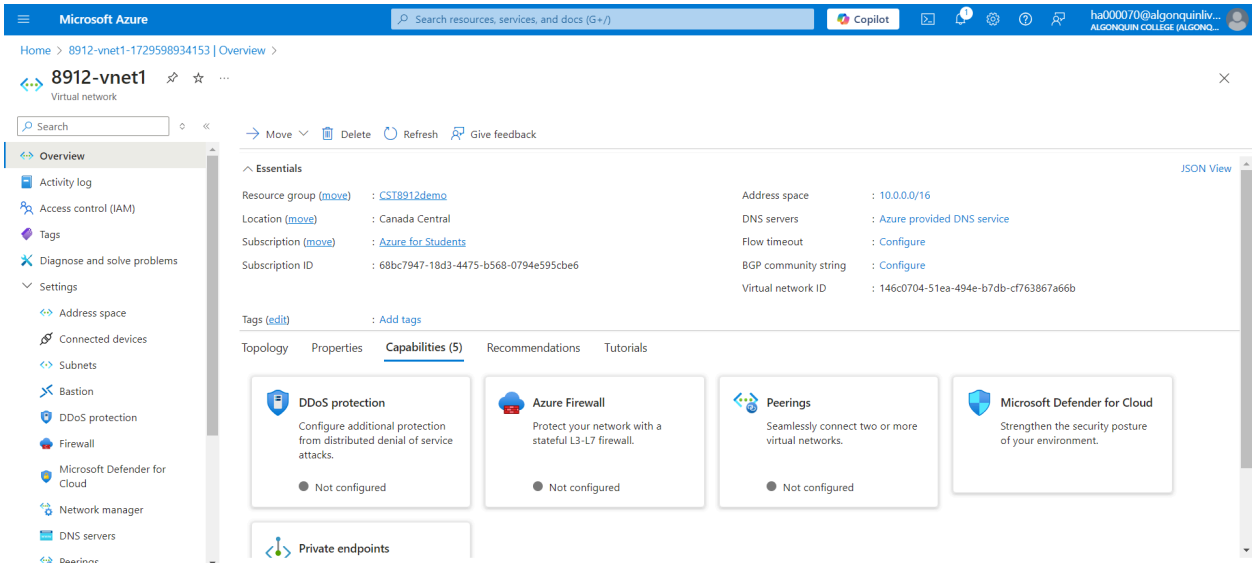
In the IP Addresses tab, the default subnet is edited to have the name **Subnet-1-8912** for easier readability and organization. The rest is left default.



Subnet-1-8912 saved.

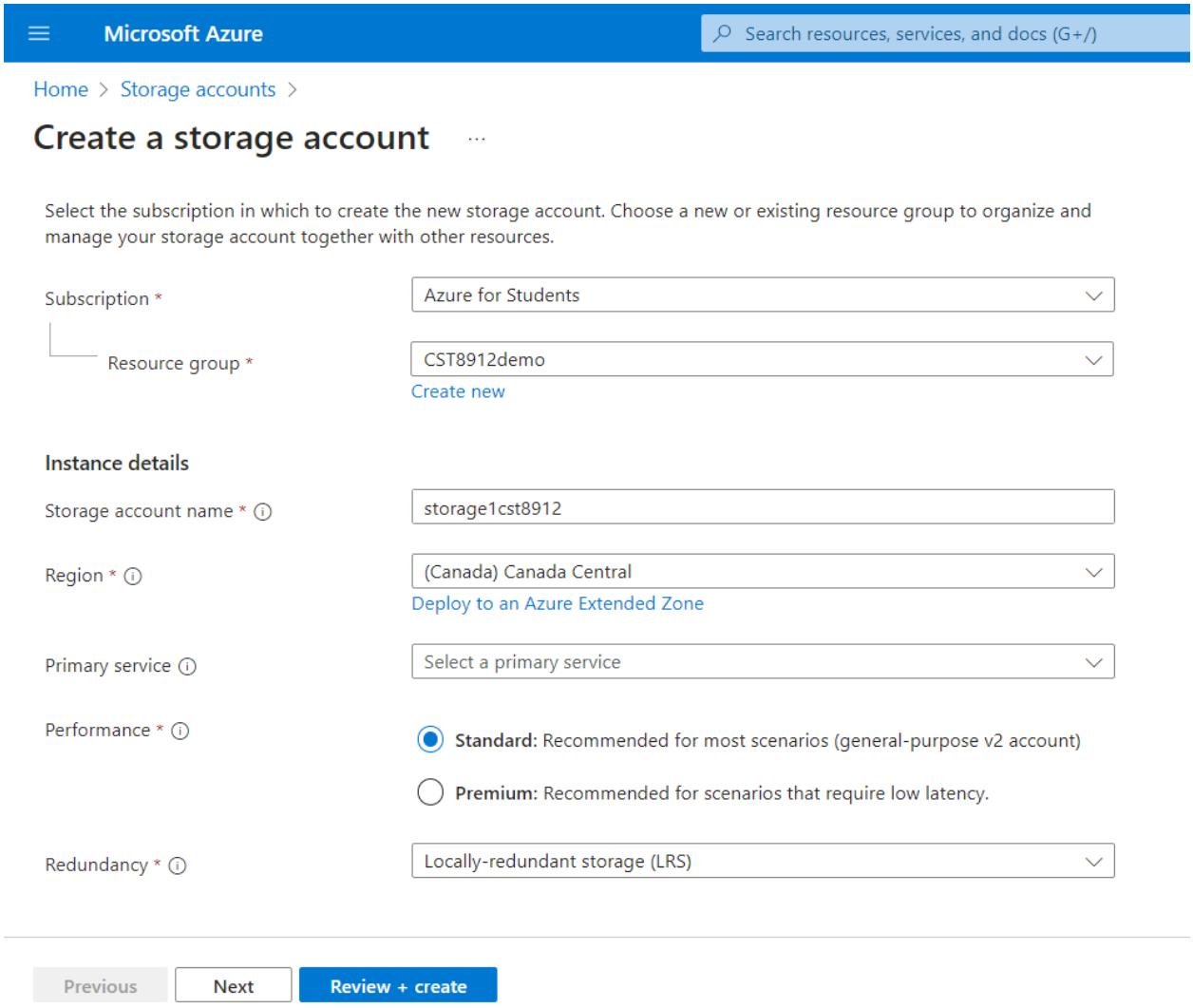


Virtual Network (8912-vnet1) overview

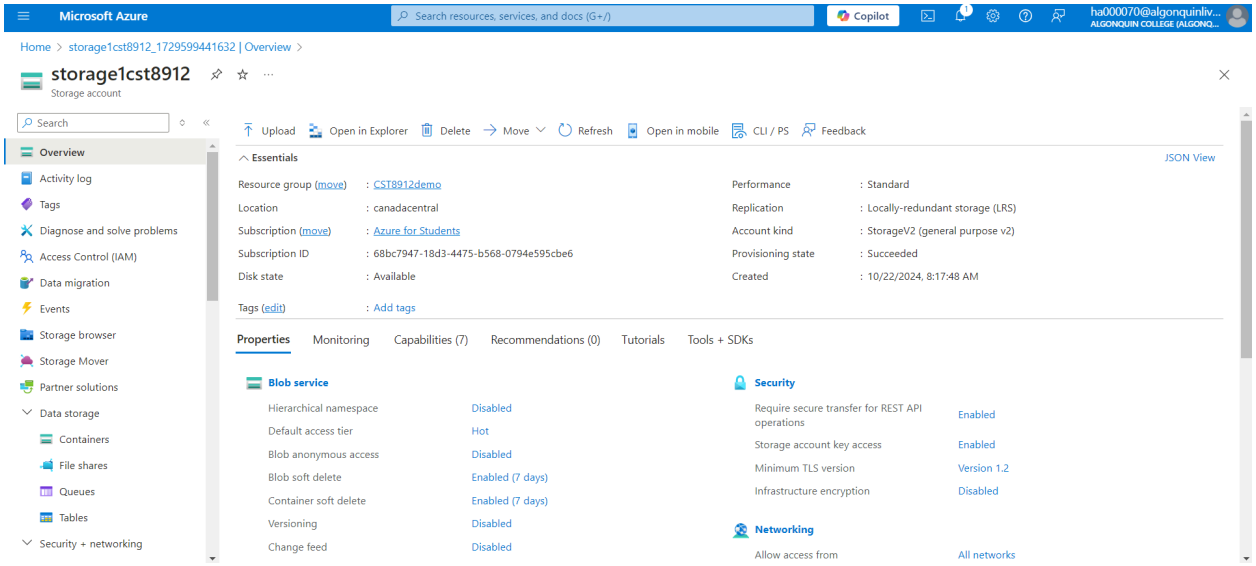


2. Create a Storage Account

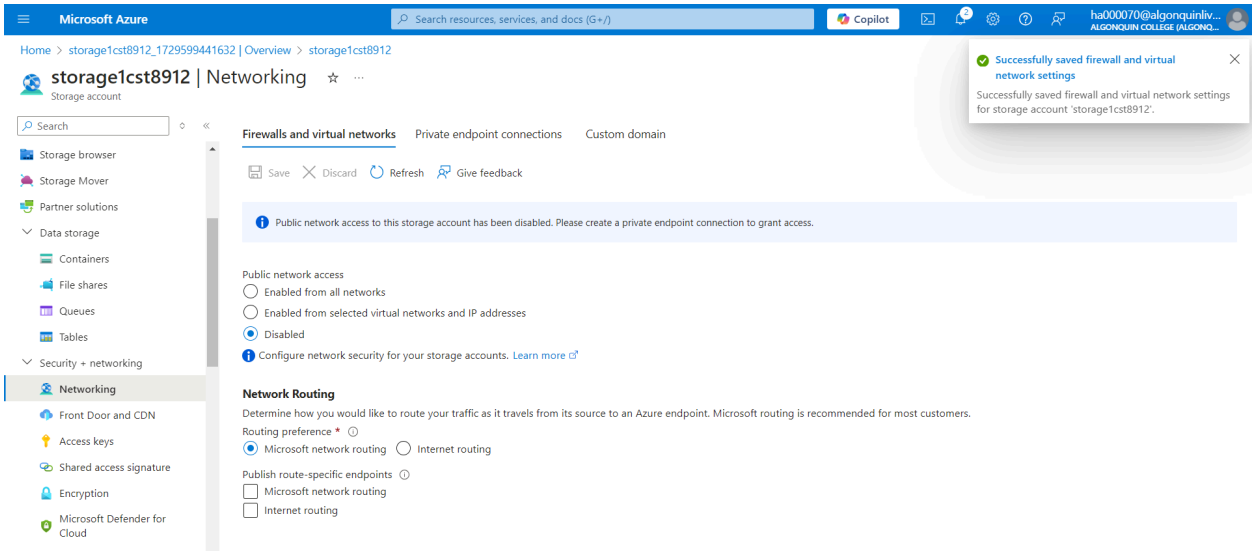
Storage account is created with the name **storage1cst8912** (the name provided in the lab instructions does not work as it must only contain lowercase letters and numbers).
Canada Central is chosen as the location to match the other resources for low latency.
Standard performance is chosen because it satisfies the general criteria, and reduces costs.
Locally-redundant storage is also chosen to reduce costs.



Storage account (storage1cst8912) overview

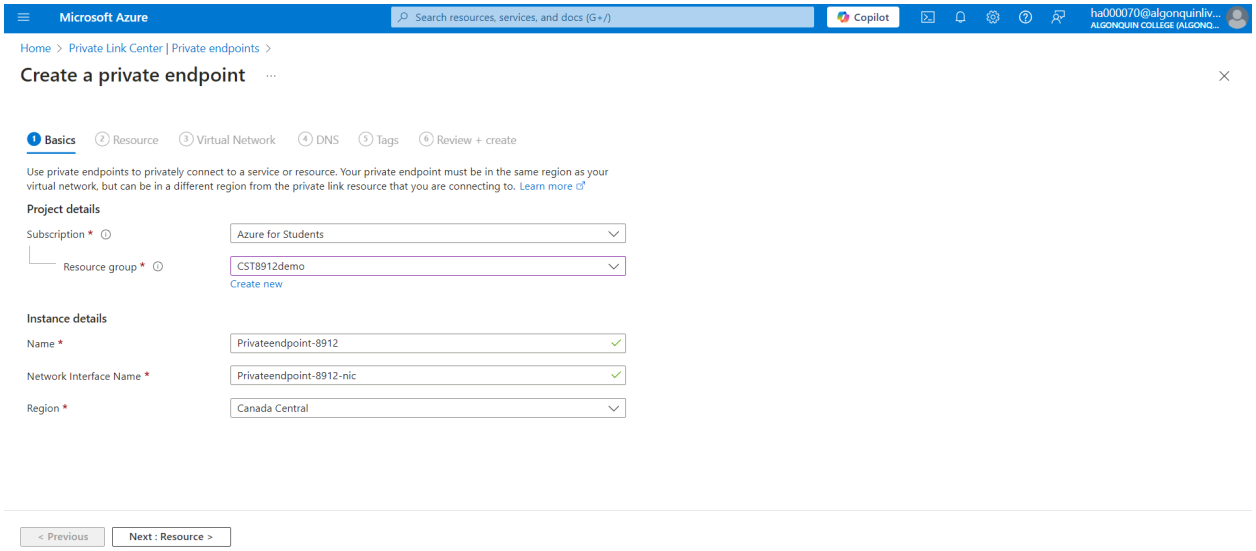


Under the security > networking tab of the storage1cst8912 account, public network access is disabled. This enhances security and data protection by limiting access to the storage account; cannot be accessed via the public internet.

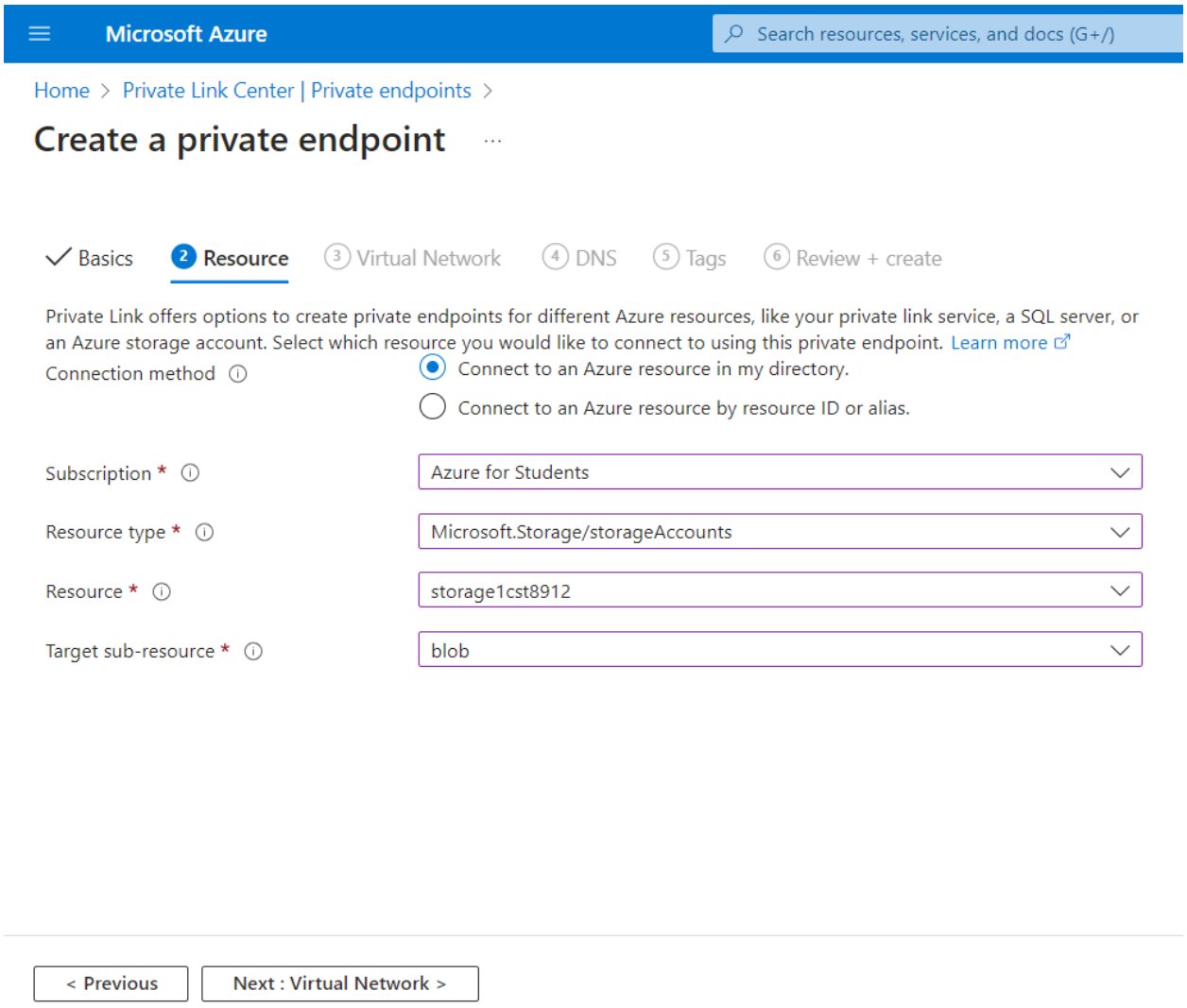


3. Create a Private Endpoint

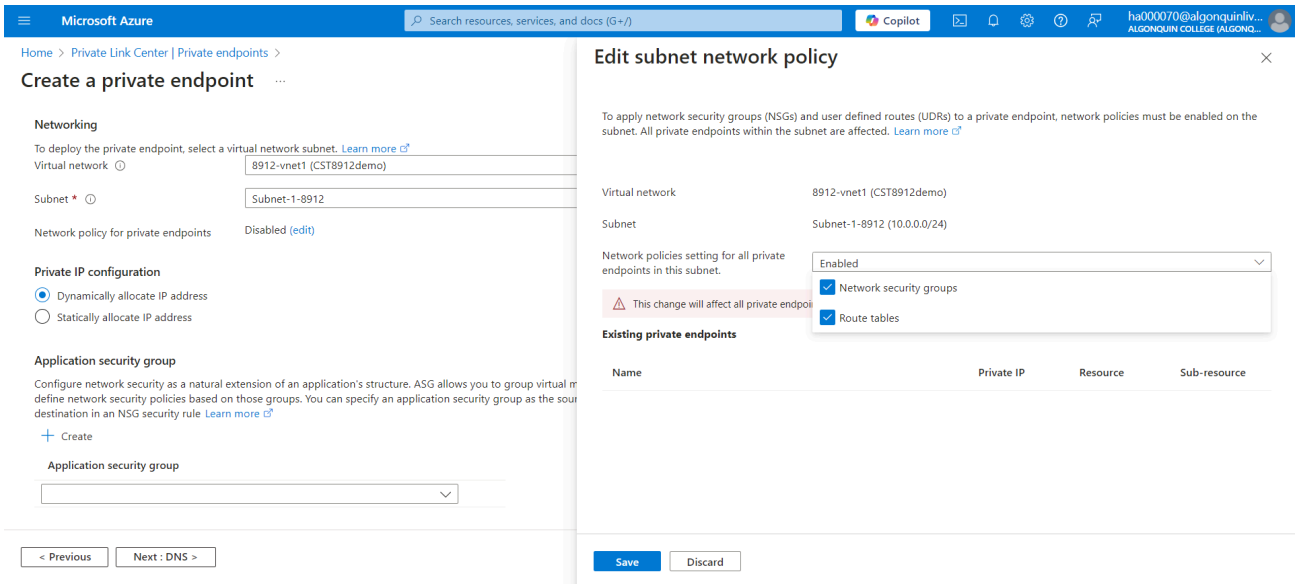
Created a private endpoint within the same resource group, with the same region of Canada Central (again, for low latency).



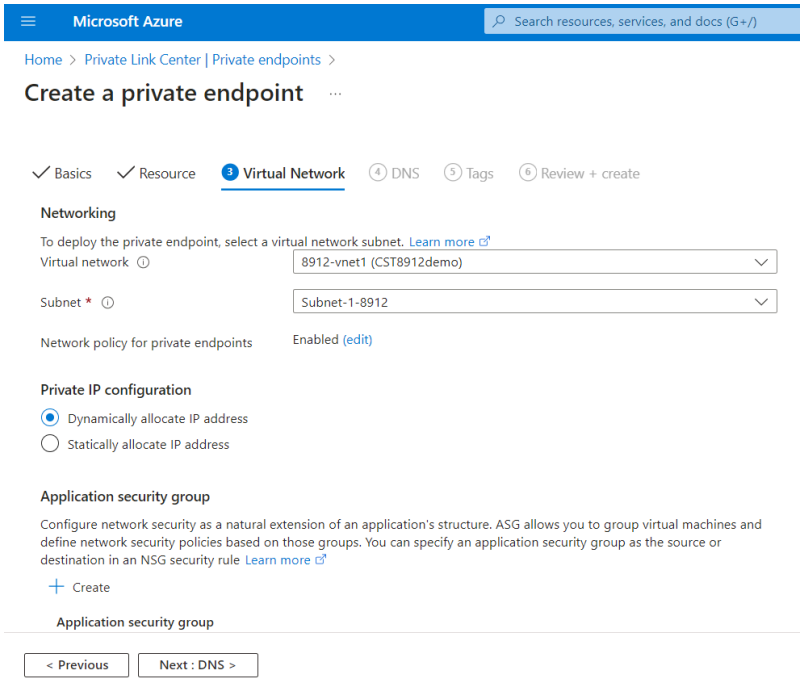
Connect the private endpoint to the Azure storage account created previously (storage1cst8912). The type is blob.



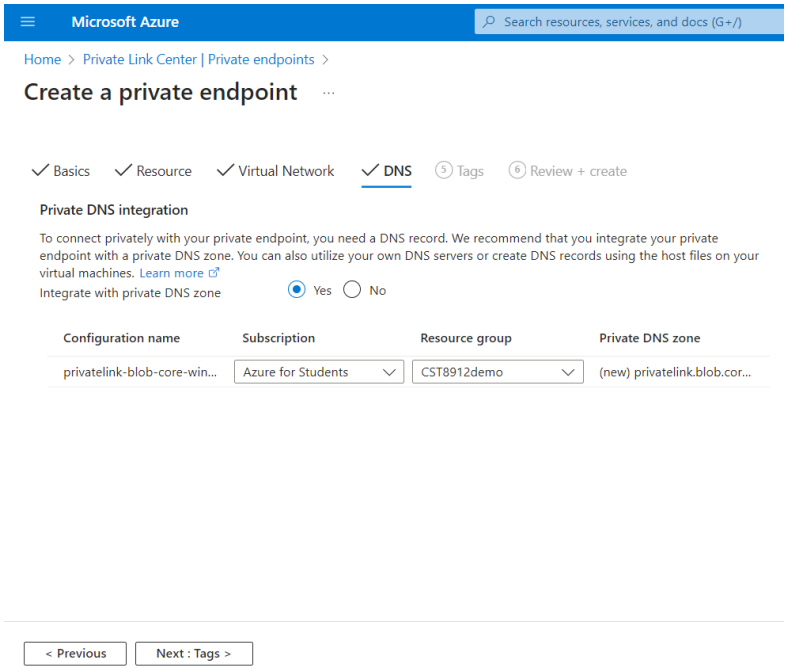
In the private endpoint's virtual network tab, the virtual network created previously (8912-vnet1) is selected, and the subnet (Subnet-1-8912) is selected. (This endpoint will use the selected subnet).
In "Network policy", **network security groups** and **route tables** are selected.
Network security groups contain security rules that define what traffic is allowed in and out. Route tables define how traffic is directed. These two options allow for performance optimization and flexibility while also ensuring good security.



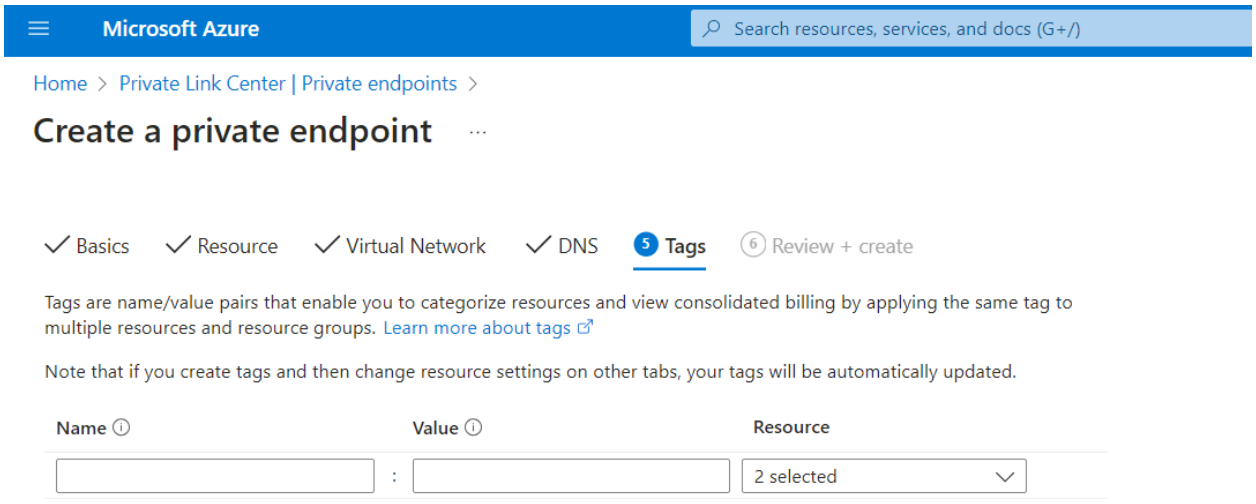
Finished editing subnet network policy



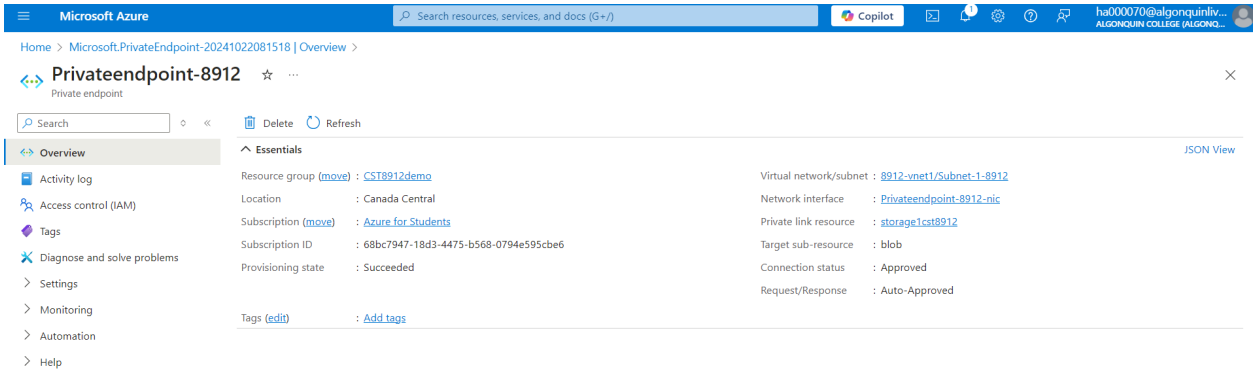
DNS is left default.



Tags is left default.

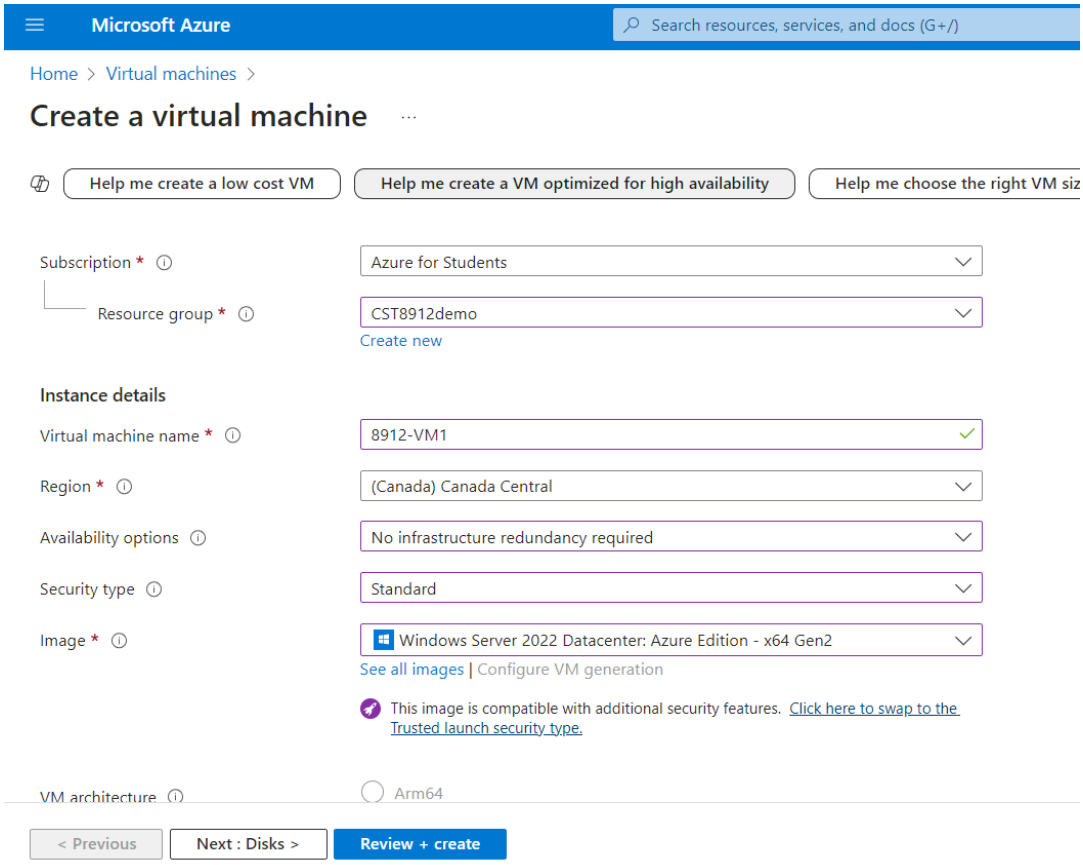


Private endpoint overview

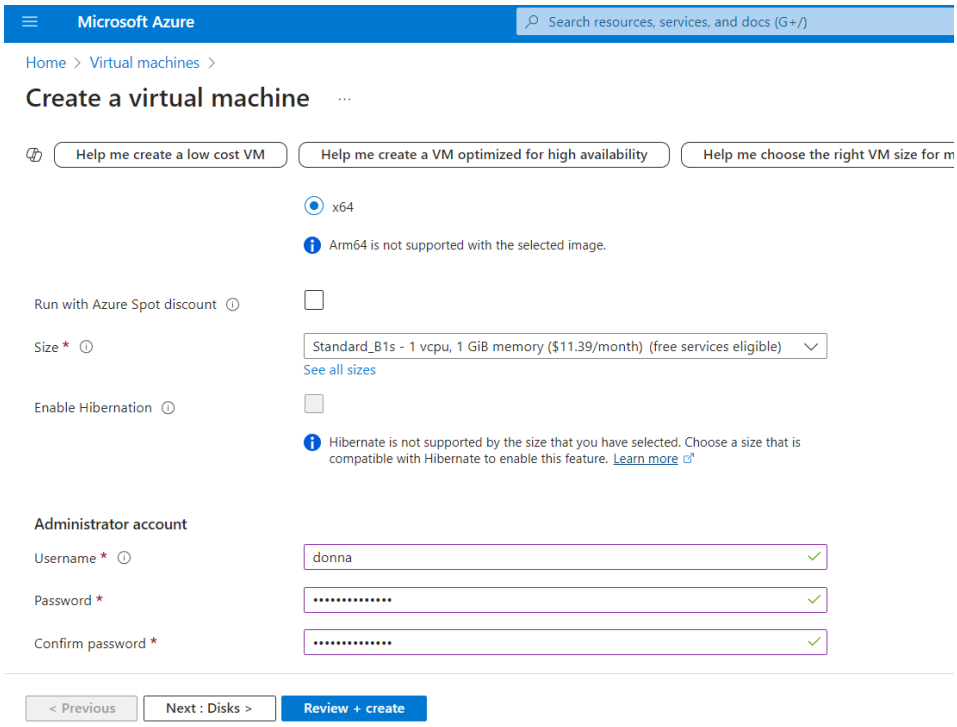


4. Create a test Virtual Machine

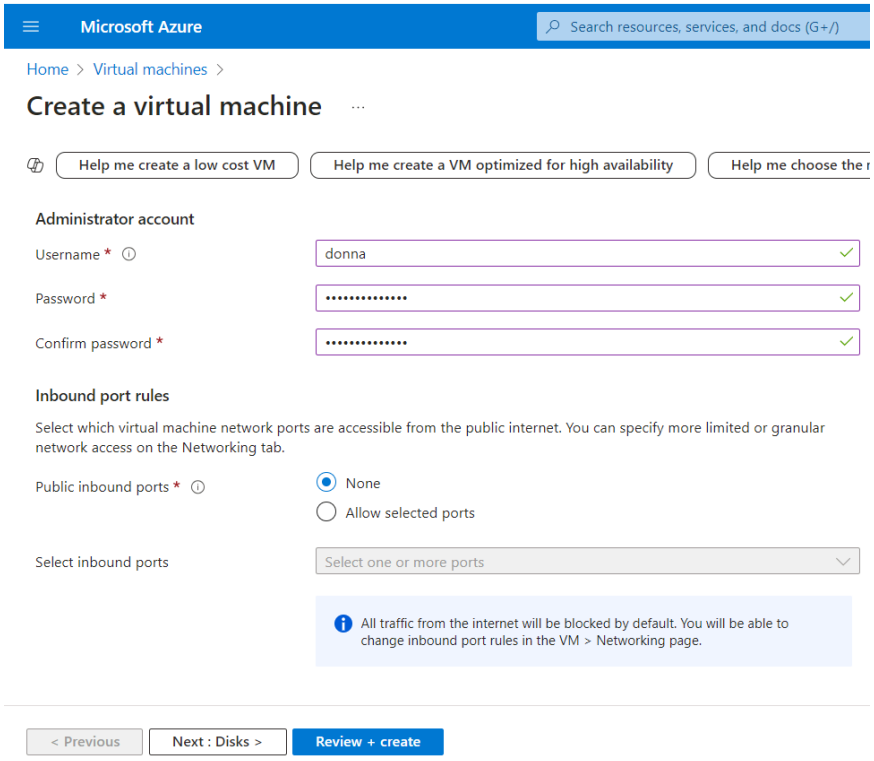
Created a virtual machine to test the connection with the storage account.
The virtual machine is named 8912-VM1, and is placed in the same resource group and region as the other resources (for low latency). The availability options are set to “No infrastructure redundancy required”, and standard for security to reduce costs.
The image is set to “Windows Server 2022 Datacenter -x64 Gen2”, because it is a popular OS and it supports what we want to do (use Bastion to connect to VM, then download Microsoft Azure Storage Explorer to access the storage account)



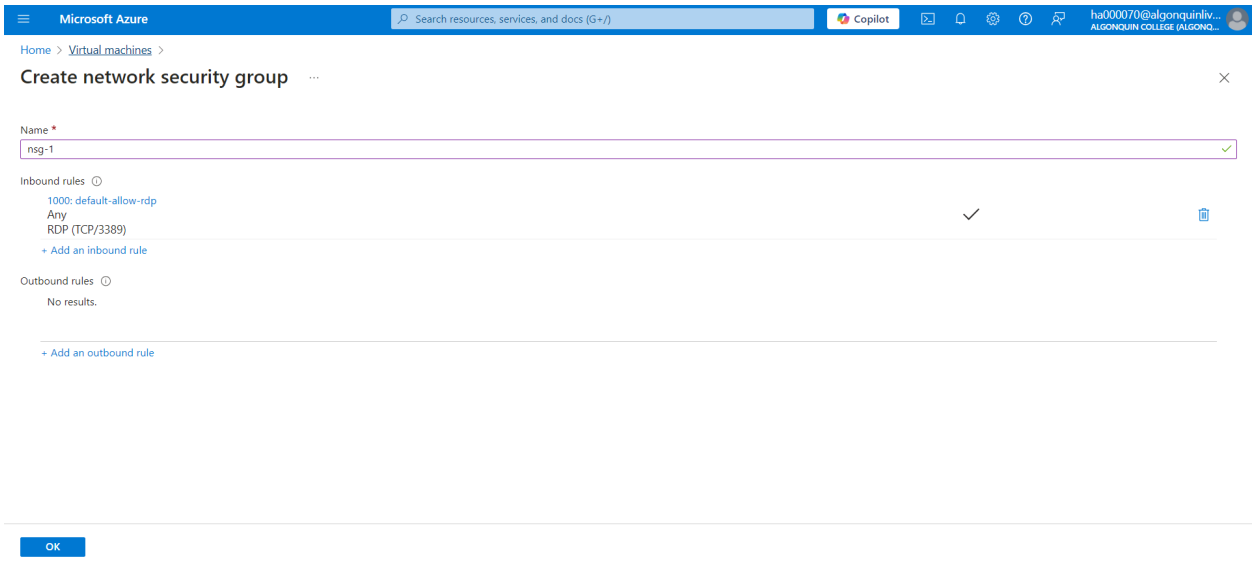
Standard_B1s is selected for the size as it is the smallest size; minimizes cost. (Later changed to B2 for proper operations)



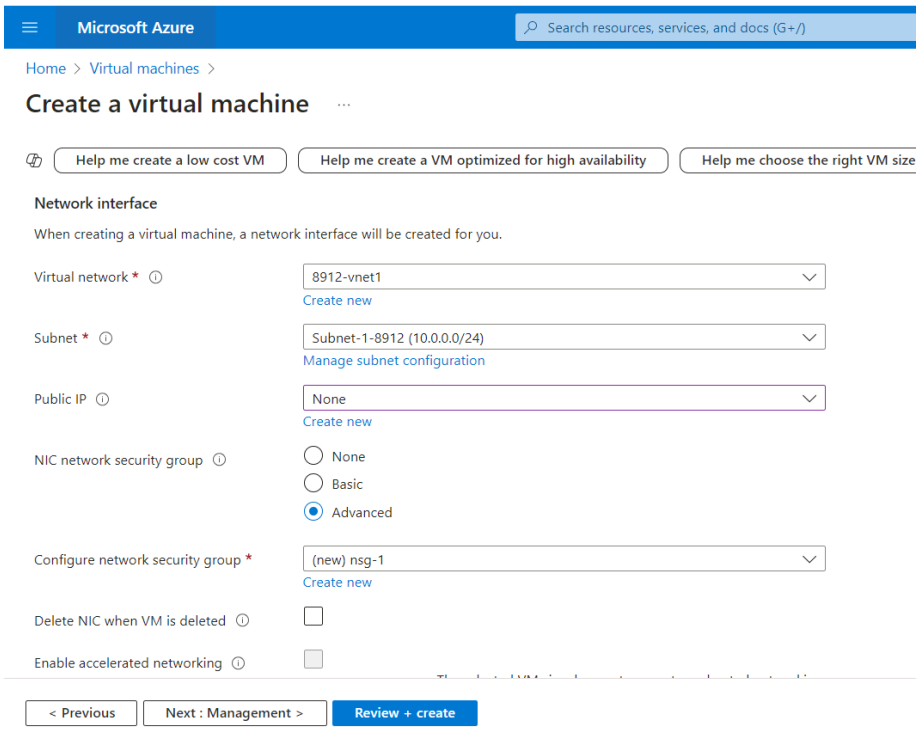
Administrator account is created using username and password. No ports are accessible from the public internet to enhance security.



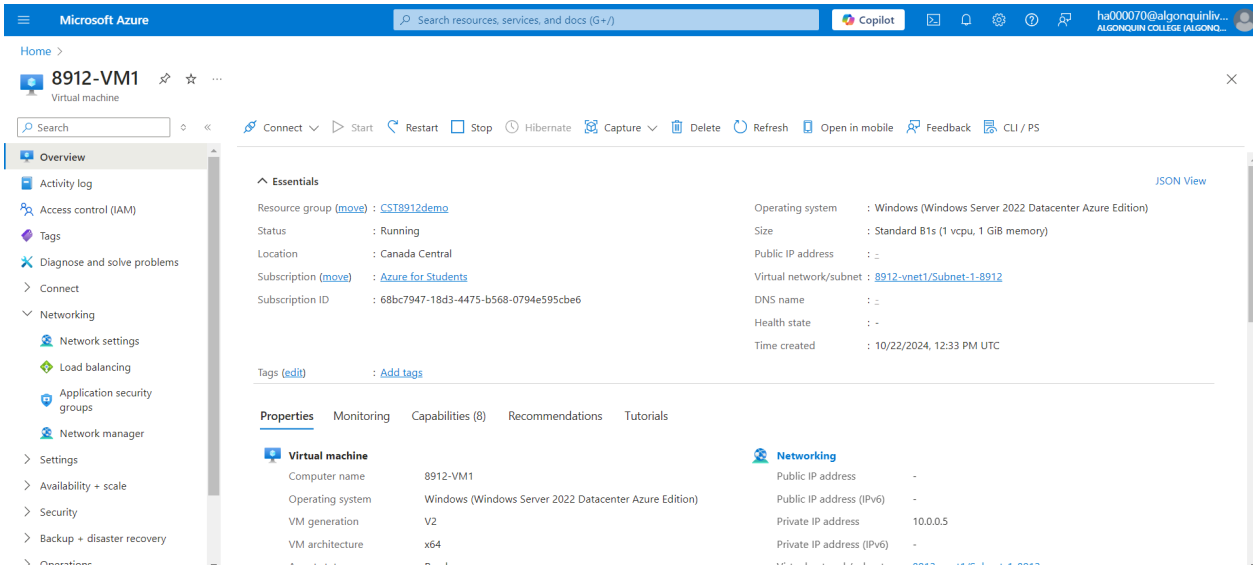
In the networking tab of creating a VM, a network security group is created, named **nsg-1**, with default settings as that is enough for the purpose of this lab.



In the networking tab, the same virtual network (8912-vnet1) and subnet (Subnet-1-8912) and the NSG just created are set to this Virtual Machine to allow for communication between the resources of 8912-vnet1.

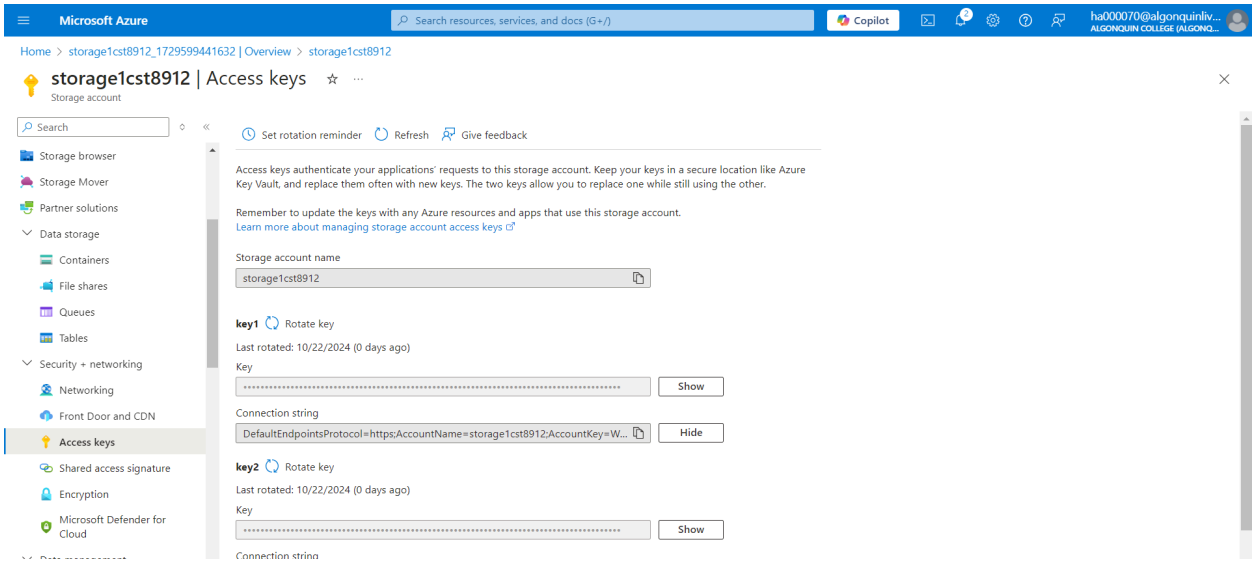


Overview of the created virtual machine.



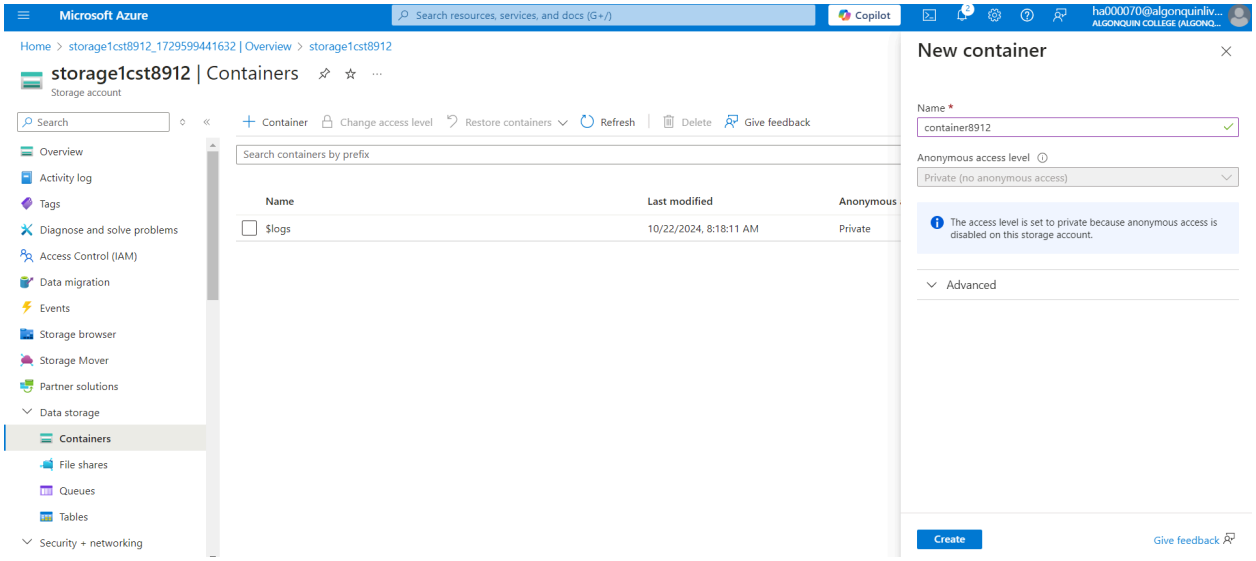
5. Storage Access Key

The storage account's (storage1cst8912) connection string for key1 (under access keys) is copied. This will be used to connect to this storage account later.

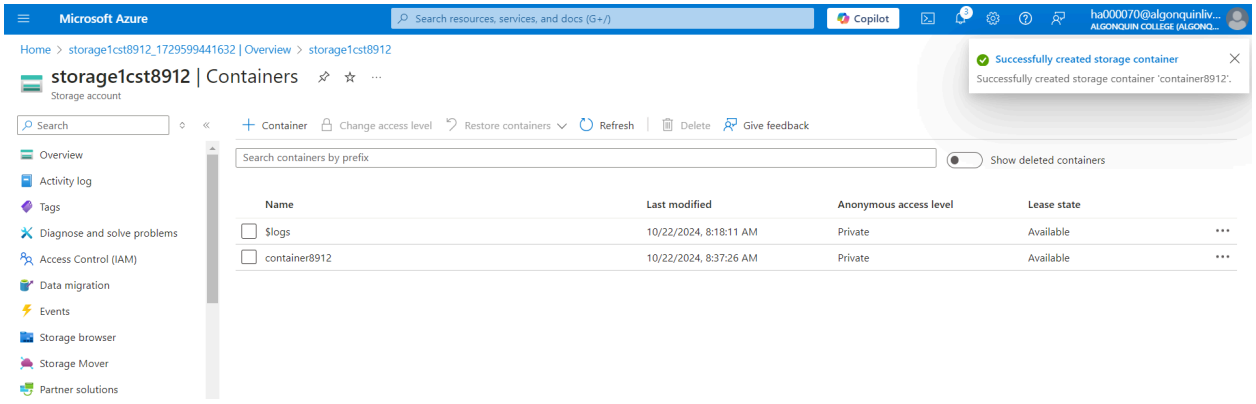


6. Adding a Blob Container

A blob container is created in the storage account (storage1cst8912). The container is named **container8912**.

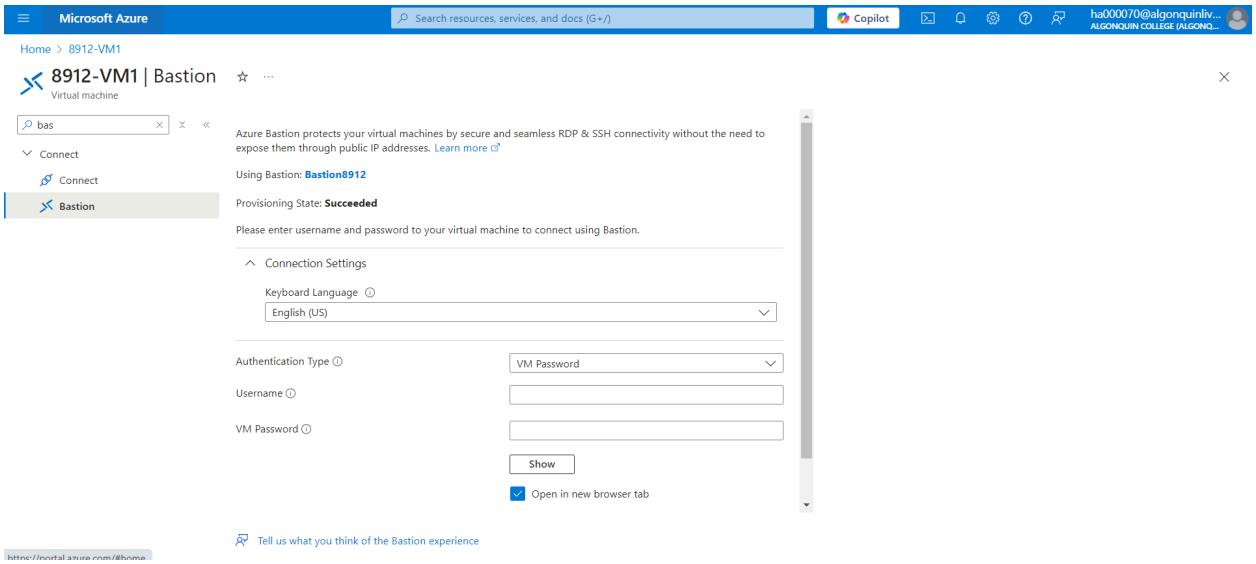


container8912 is successfully created.

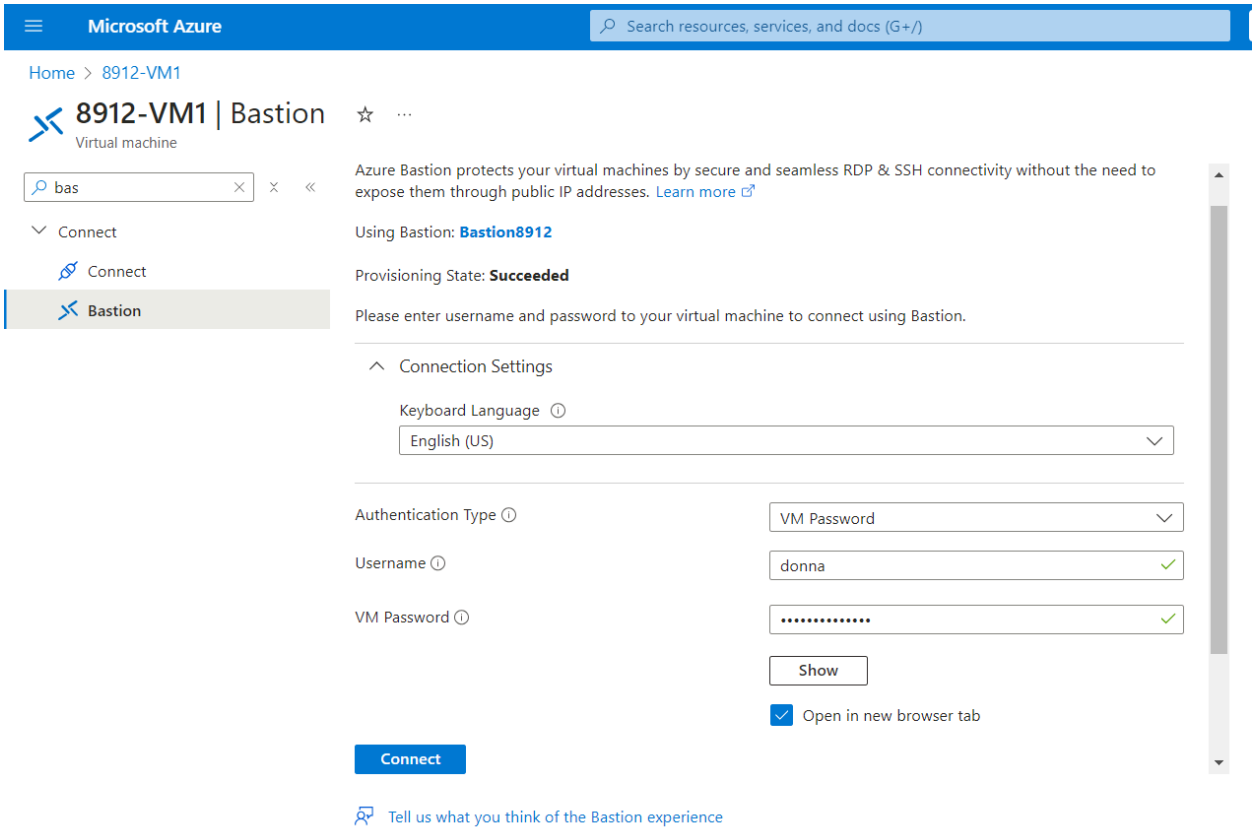


7. Testing Connectivity to Private Endpoint

In the virtual machine (8912-VM1), Bastion is selected to start connecting to the VM through RDP and SSH connectivity.

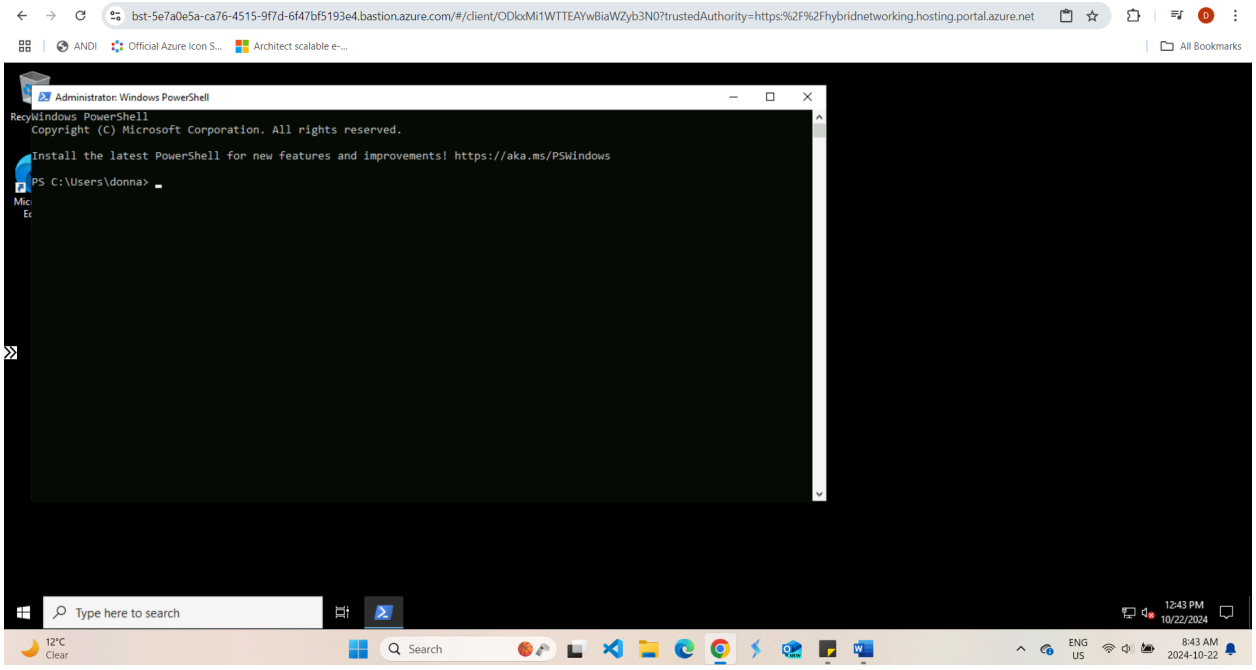


Username and password is entered to log in.

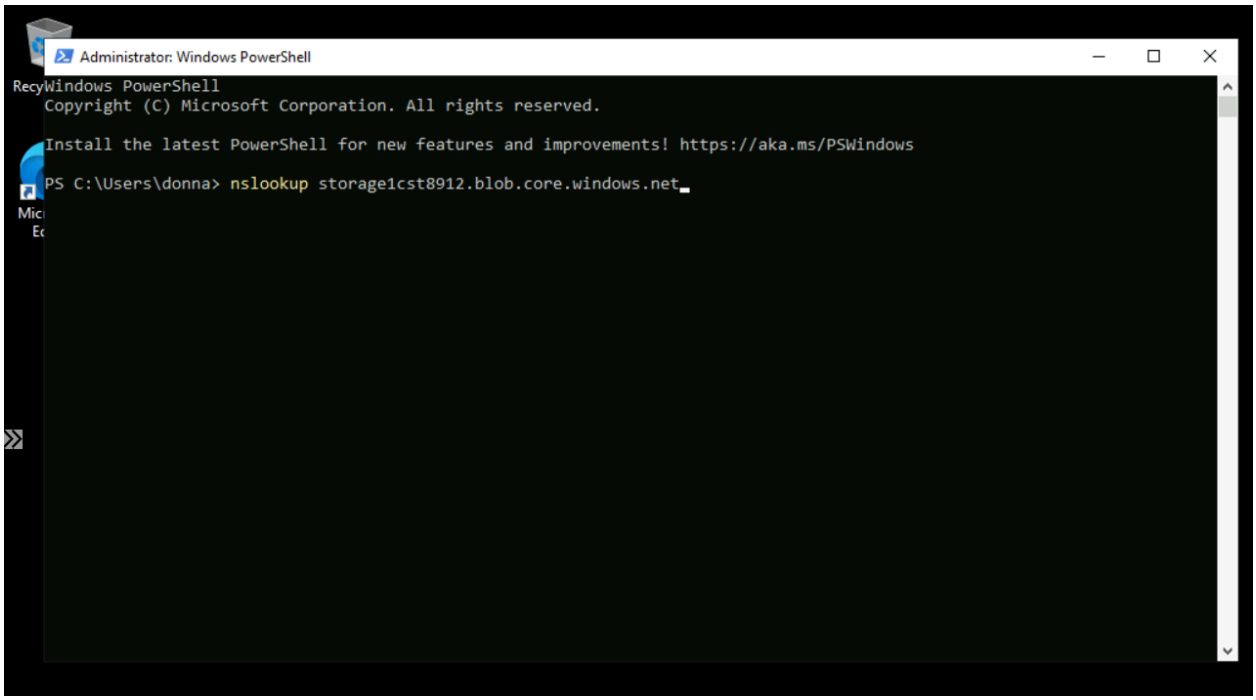


Connection completed, the virtual machine server is opened in a new tab

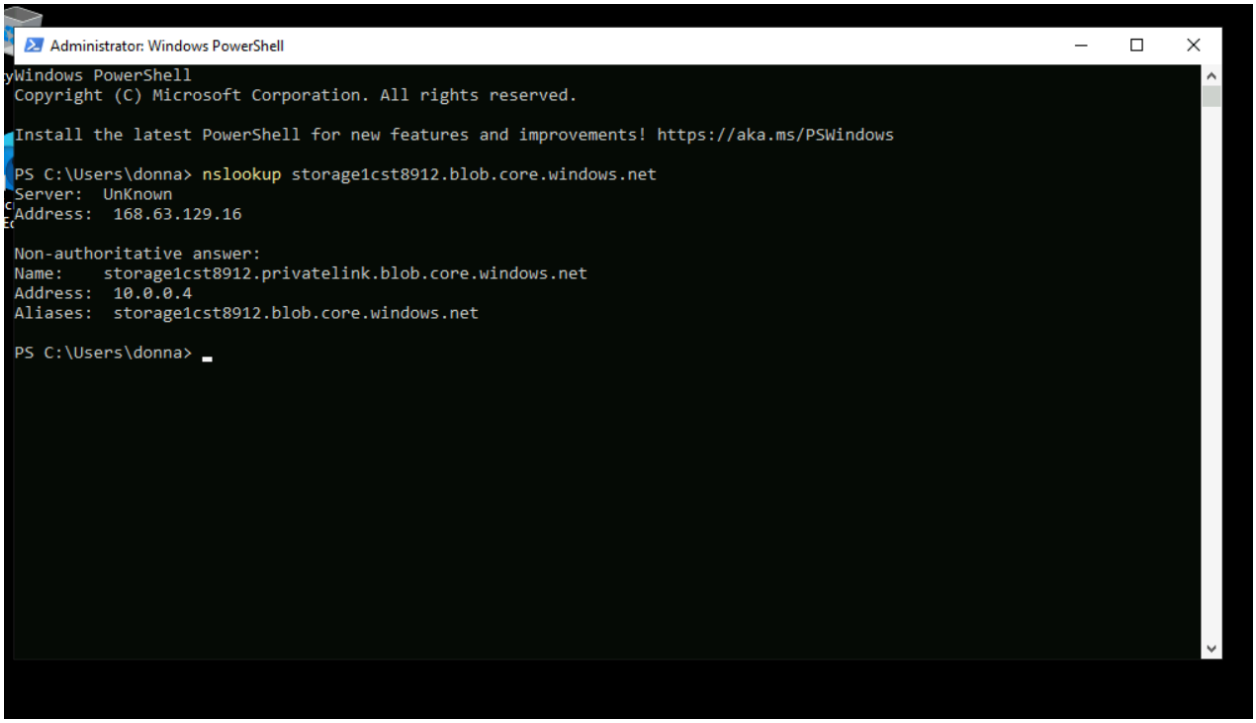
Powershell is opened on the server.



The following command is entered in the powershell:
nslookup storage1cst8912.blob.core.windows.net



The command gives the following output:
Explanation of output: The server DNS is unknown. The address 168.63.129.16 is the IP address of the server.
“Non-authoritative answer” indicates that this response is not coming directly from the storage account itself.
The address 10.0.04 is the address of the storage account, and is most likely the subnet we set above (Subnet-1-8912).



Text Output:
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

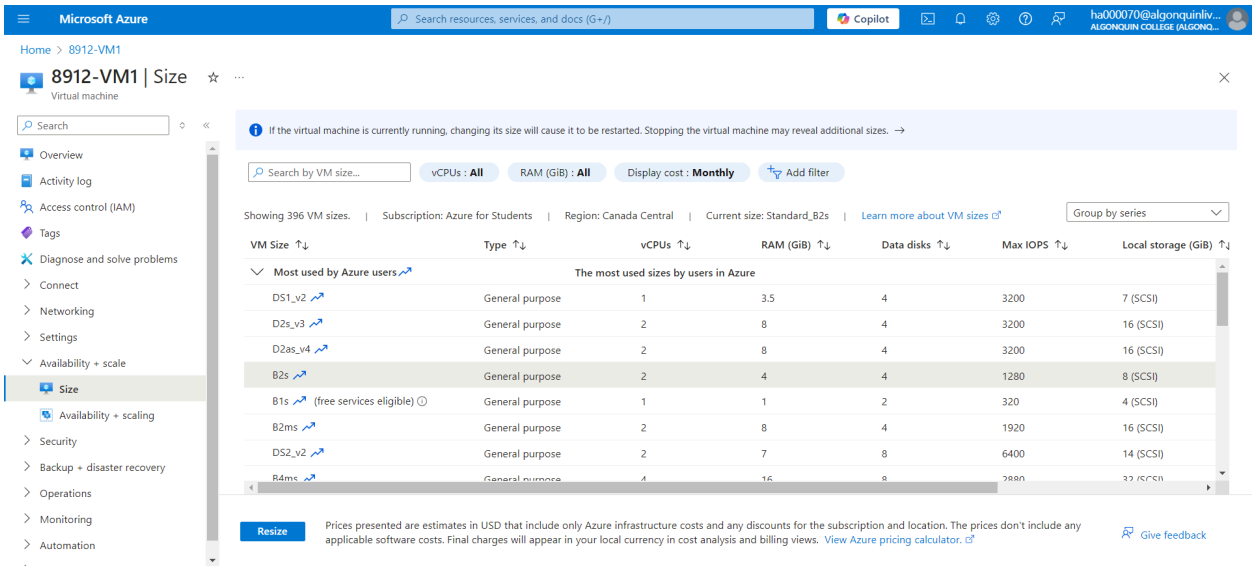
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\donna> nslookup storage1cst8912.blob.core.windows.net
Server: UnKnown
Address: 168.63.129.16

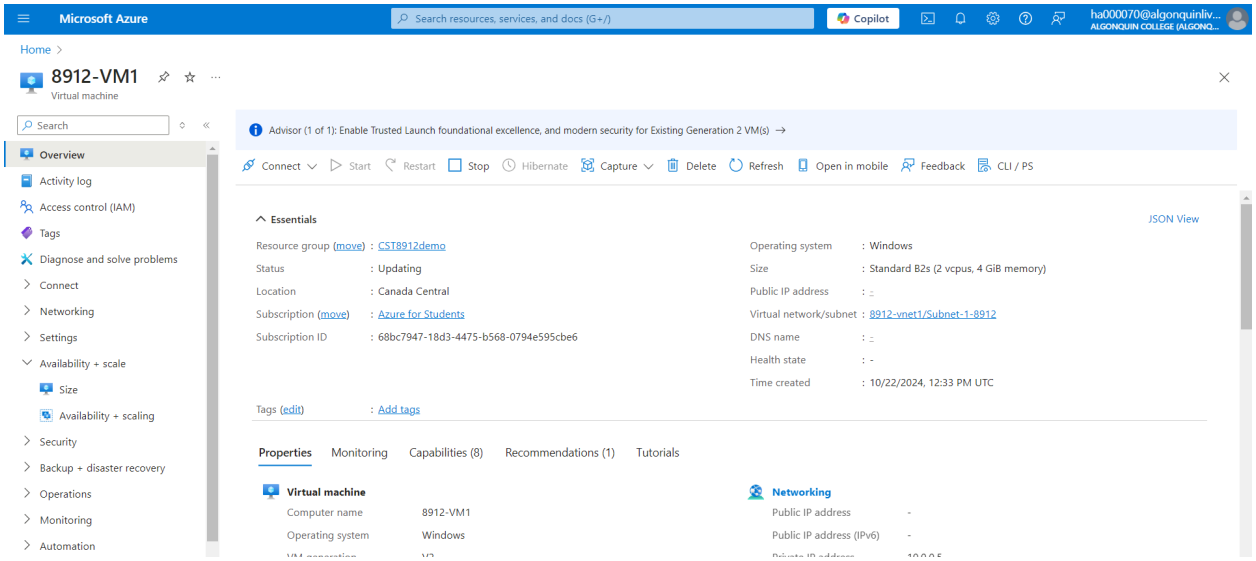
Non-authoritative answer:
Name: storage1cst8912.privatelink.blob.core.windows.net
Address: 10.0.0.4
Aliases: storage1cst8912.blob.core.windows.net

PS C:\Users\donna>

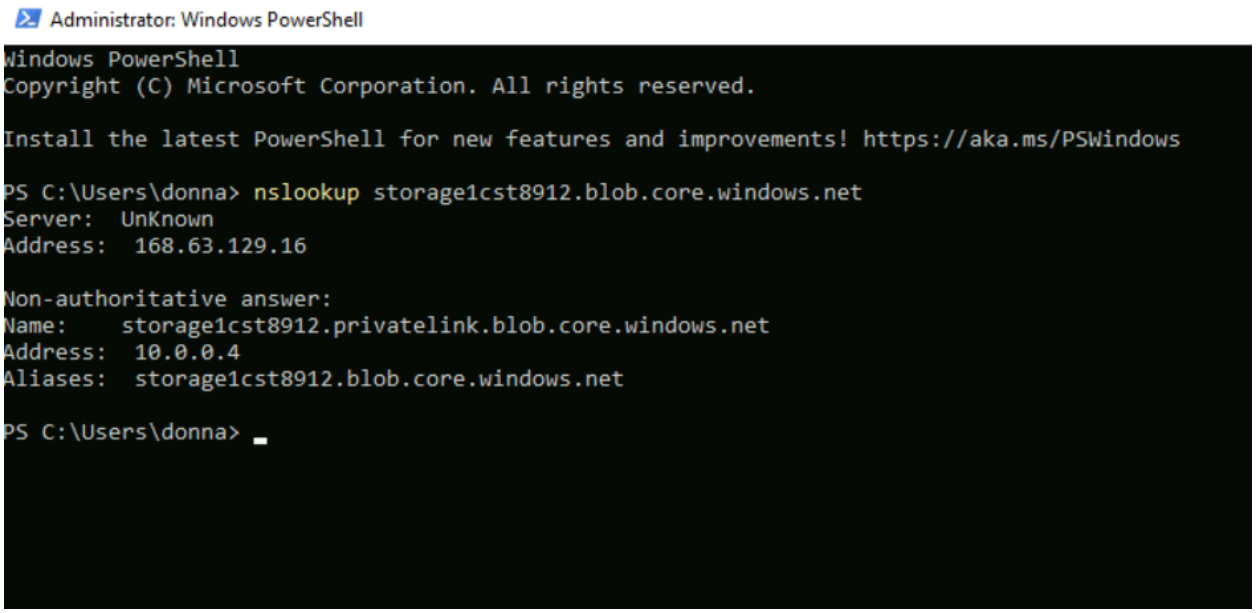
Changing the VM (8912-VM1) size to B2 because B1 was too small to download the required software (Microsoft Azure Storage Explorer)



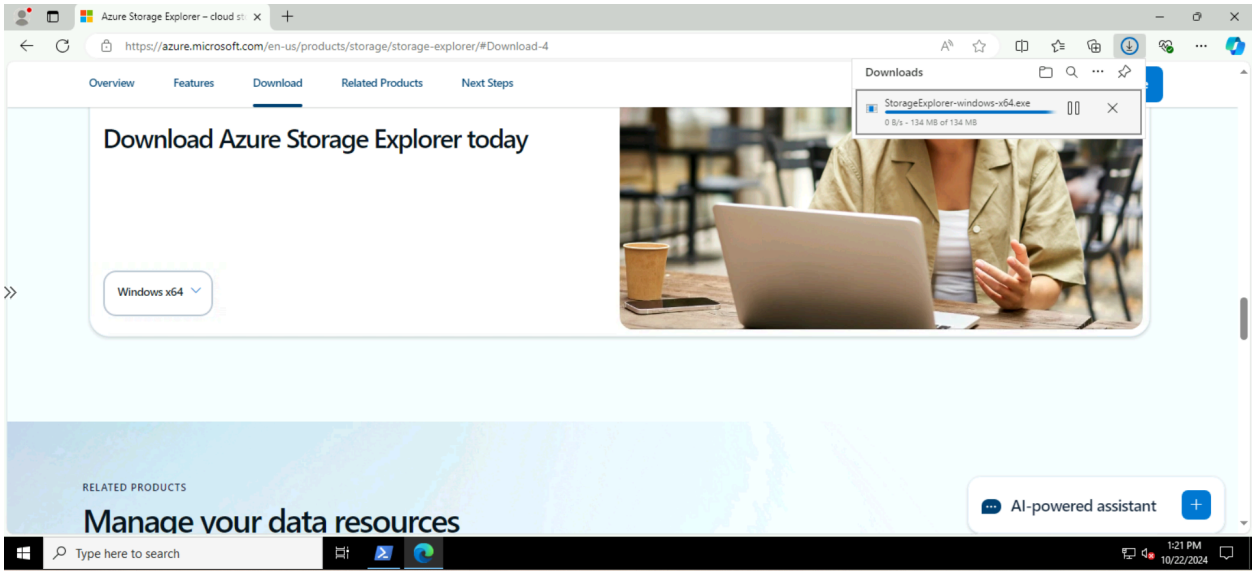
New Vm size of B2 successfully changes; this is the new overview of the VM.



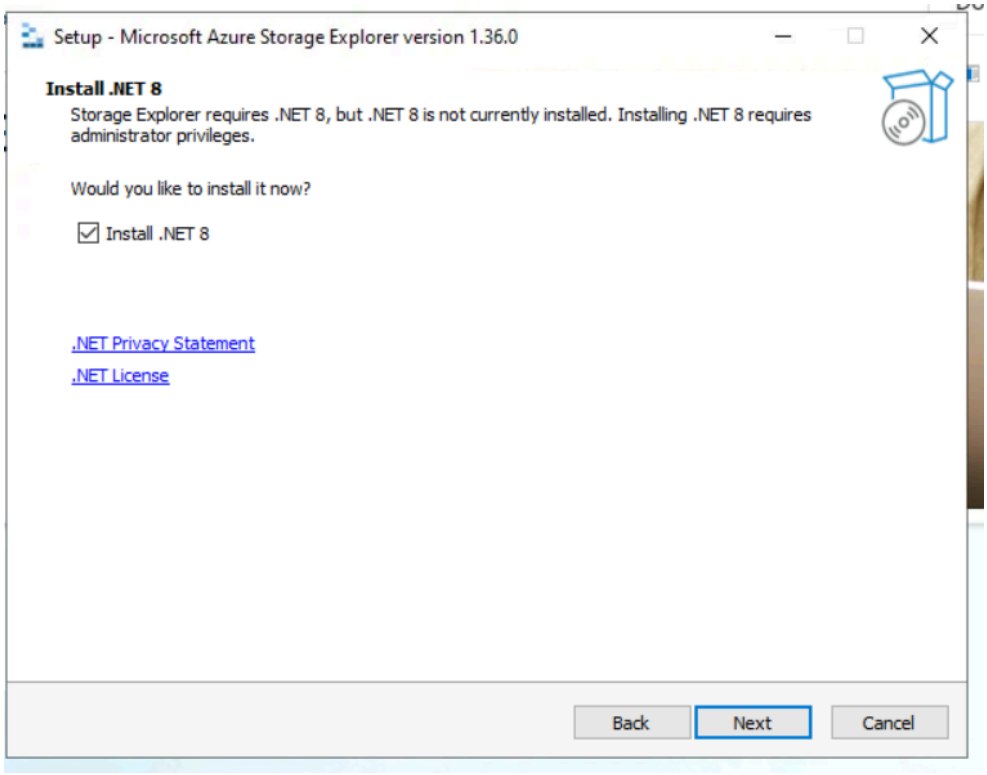
Restarted the VM server connection via Bastion, and did the command in powershell again.



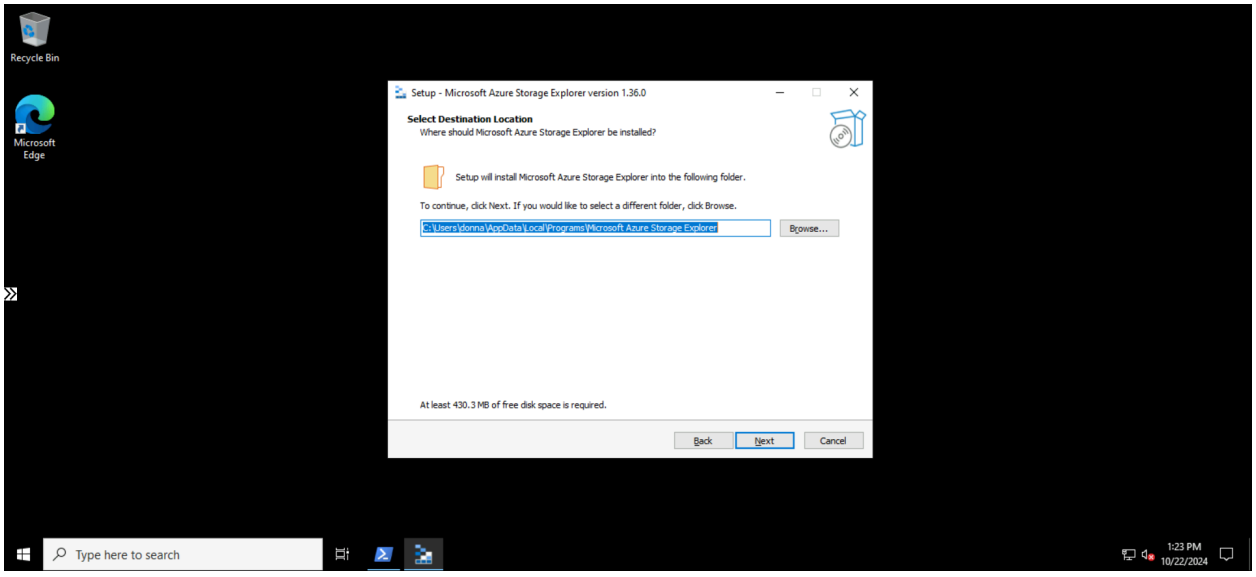
Use Microsoft Edge to download the Microsoft Azure Storage Explorer.



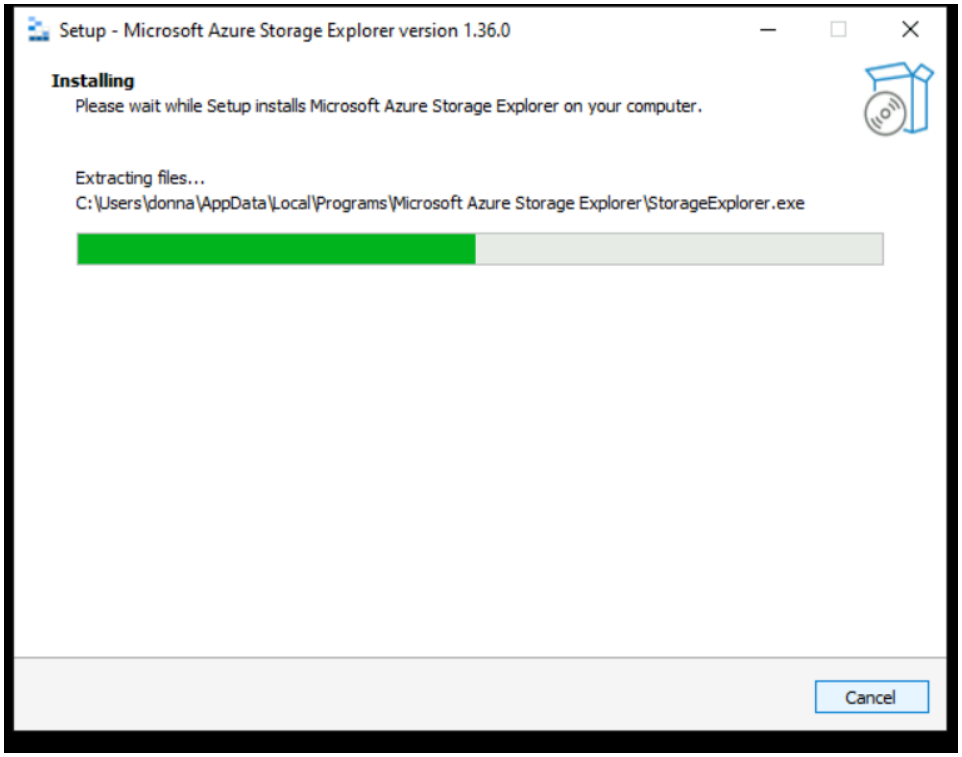
Installing Microsoft Azure Storage Explorer



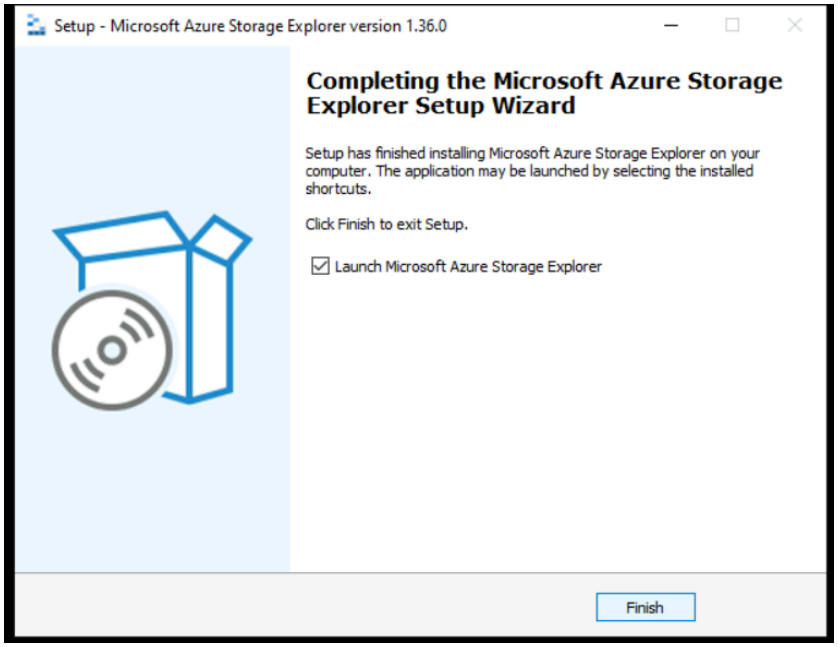
Installing Microsoft Azure Storage Explorer in file location.



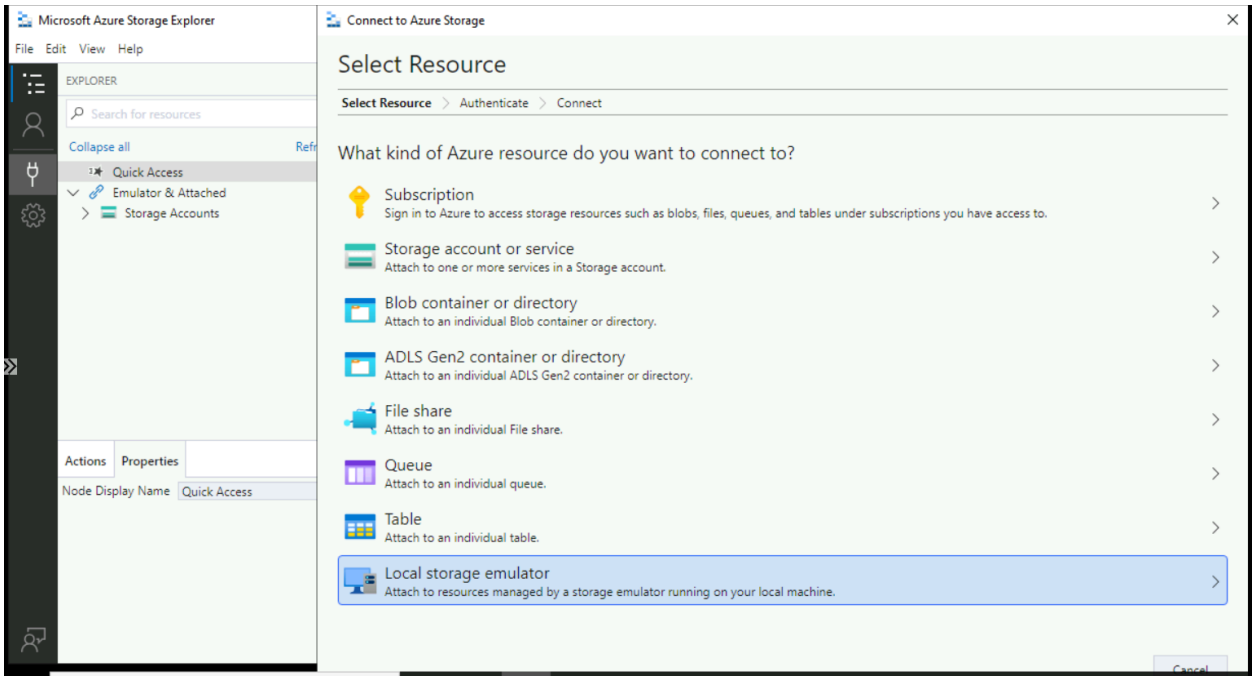
Installing Microsoft Azure Storage Explorer, loading.



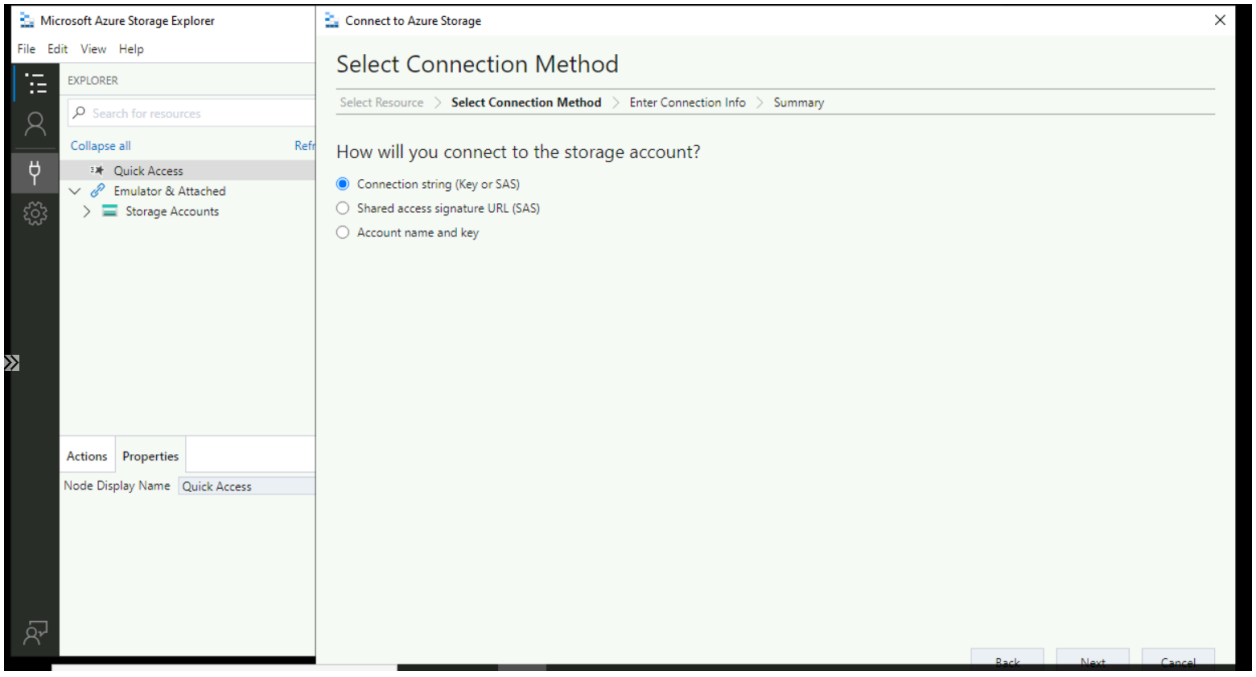
Installing Microsoft Azure Storage Explorer, completed.
Launched is left checked to launch the application right away.



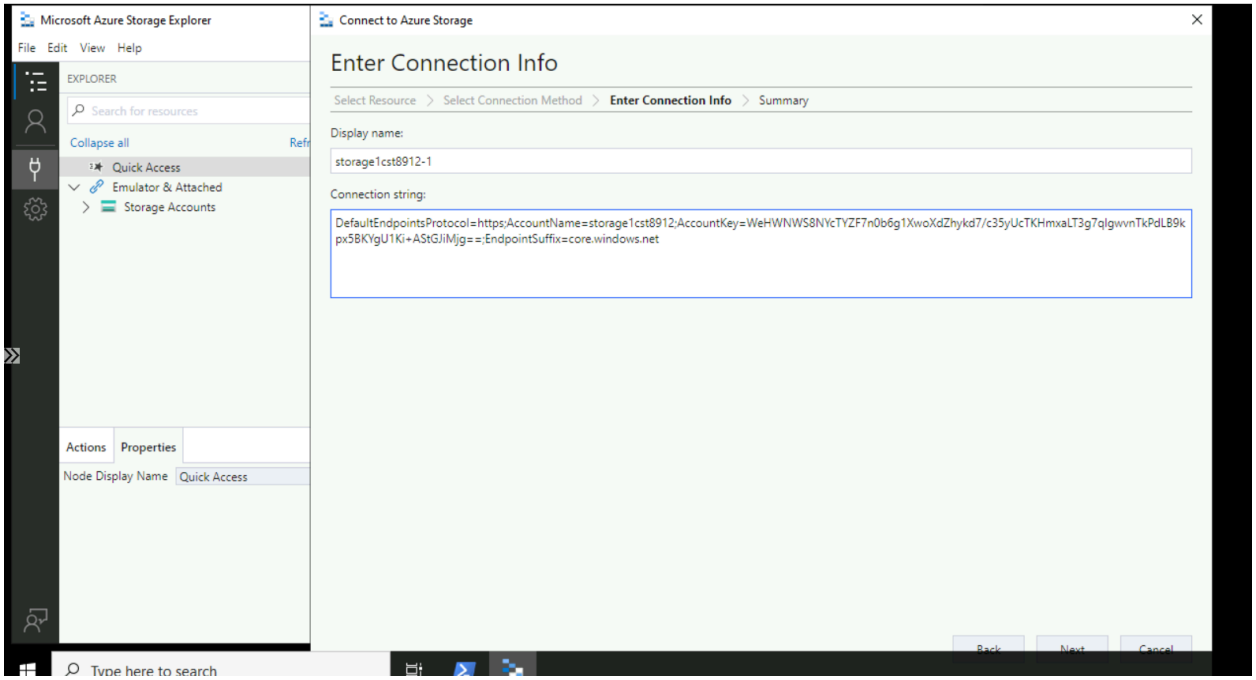
Accessed the “Select resource” by selecting the power plug button.
Select “Local storage emulator” to connect to the storage account created previously.



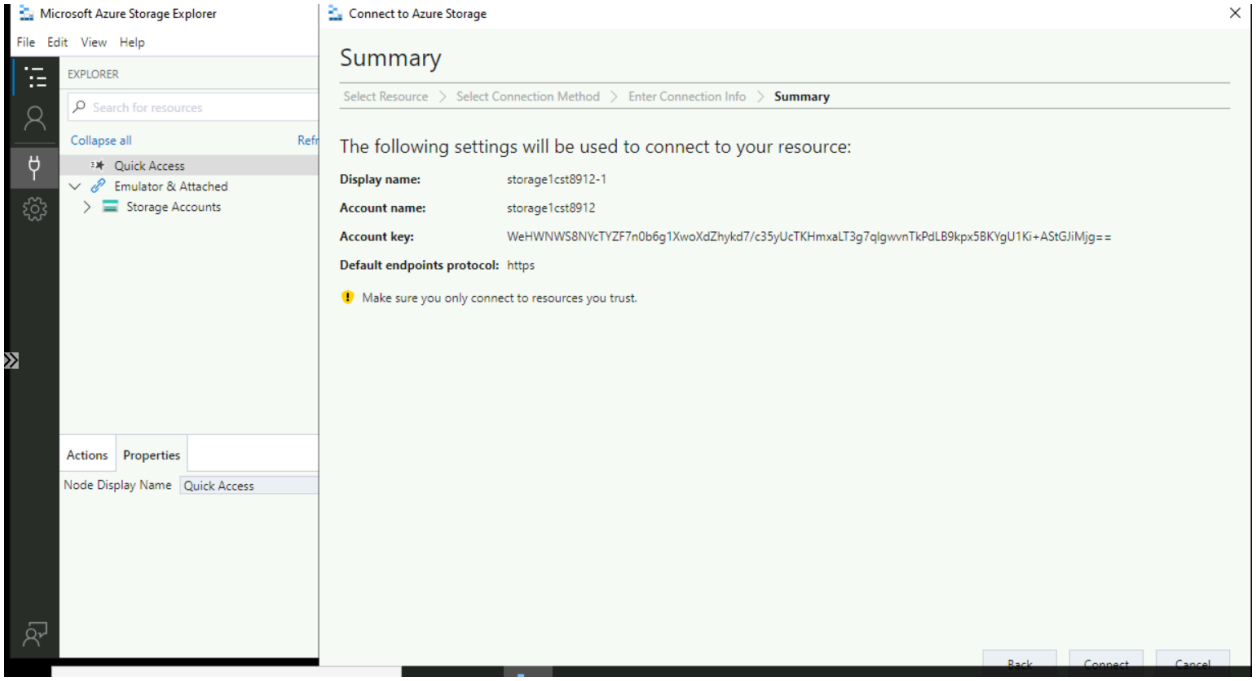
Select connection string as the method to connect to the storage account.



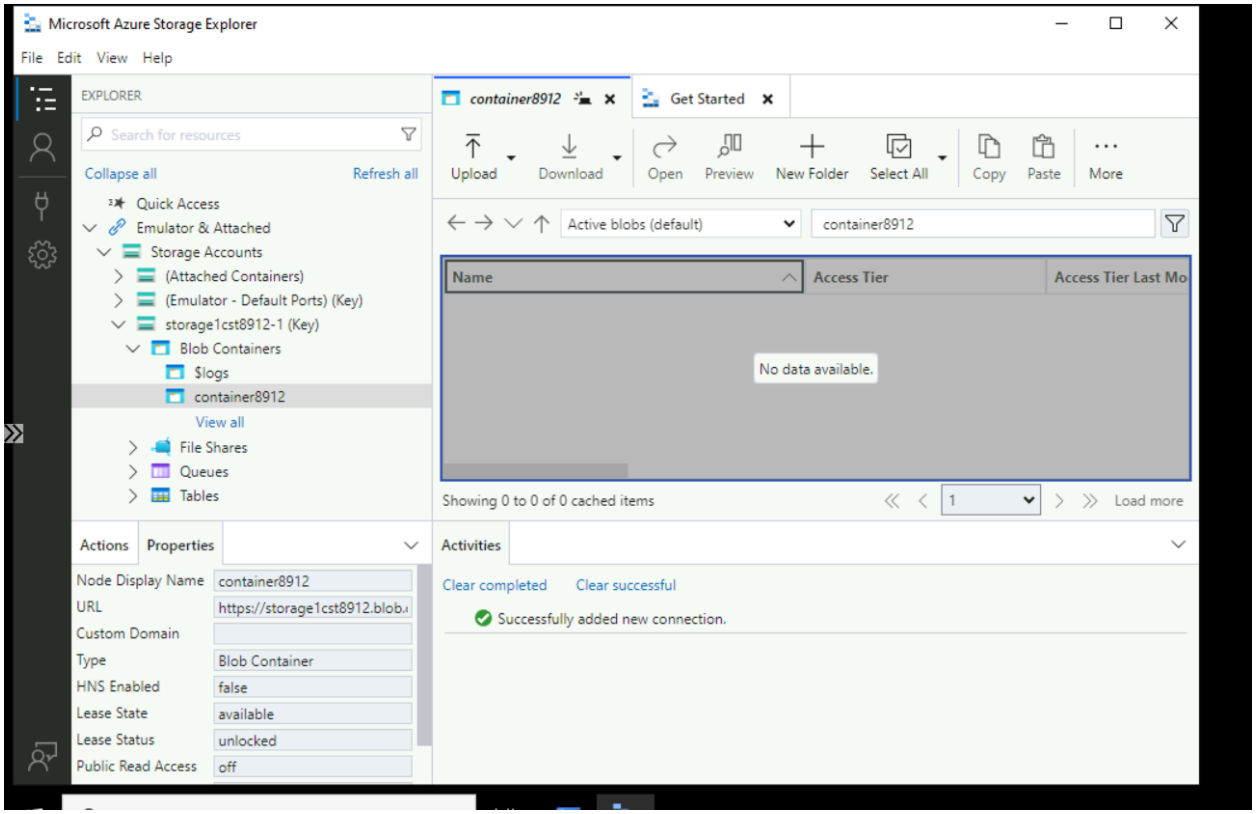
The connection string for key1 previously copied is pasted in the connection string input box. The display name is automatically generated.



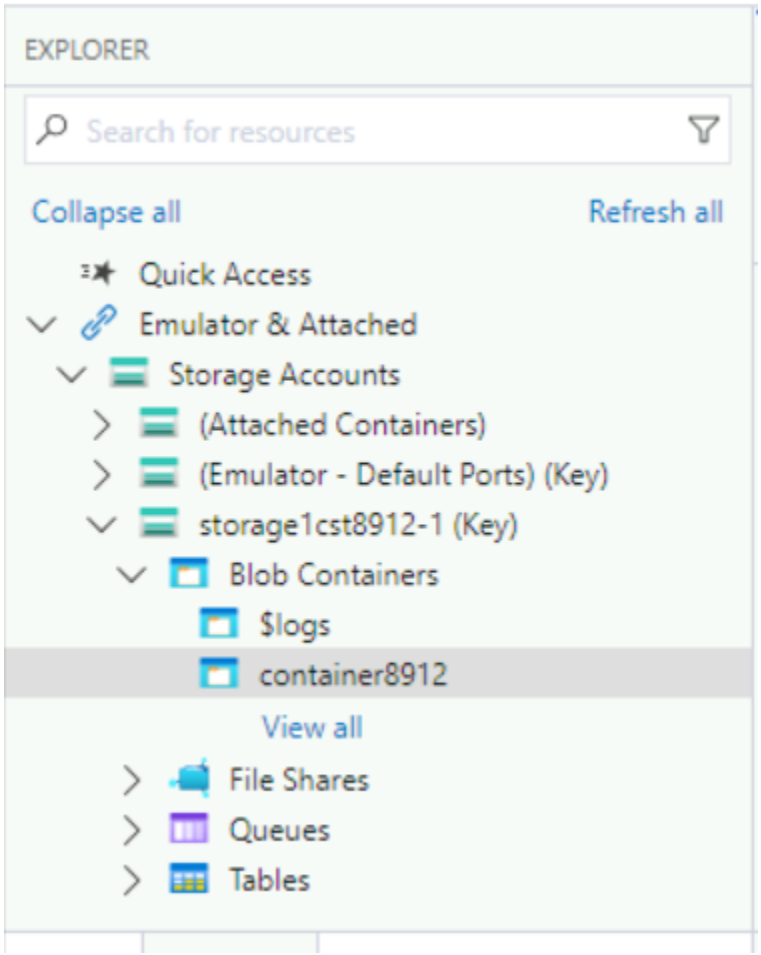
The connection settings are reviewed in the Summary tab, and then connect is selected.



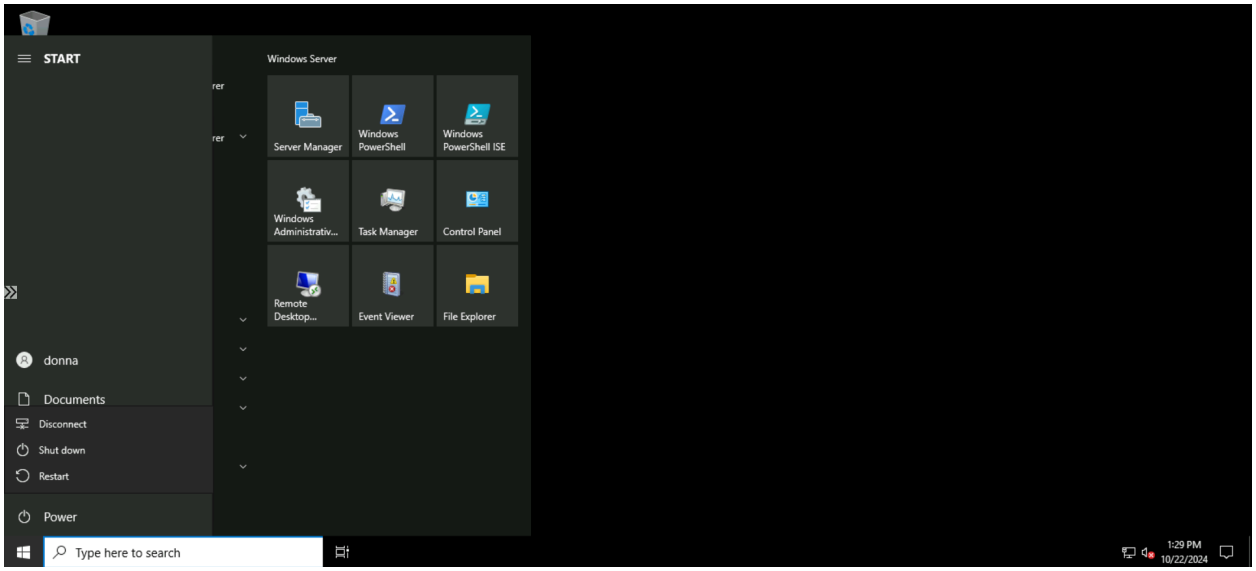
The storage account (storage1cst8912) is connected and expanded to show the container (container 8912) that was created. The connection is successful.



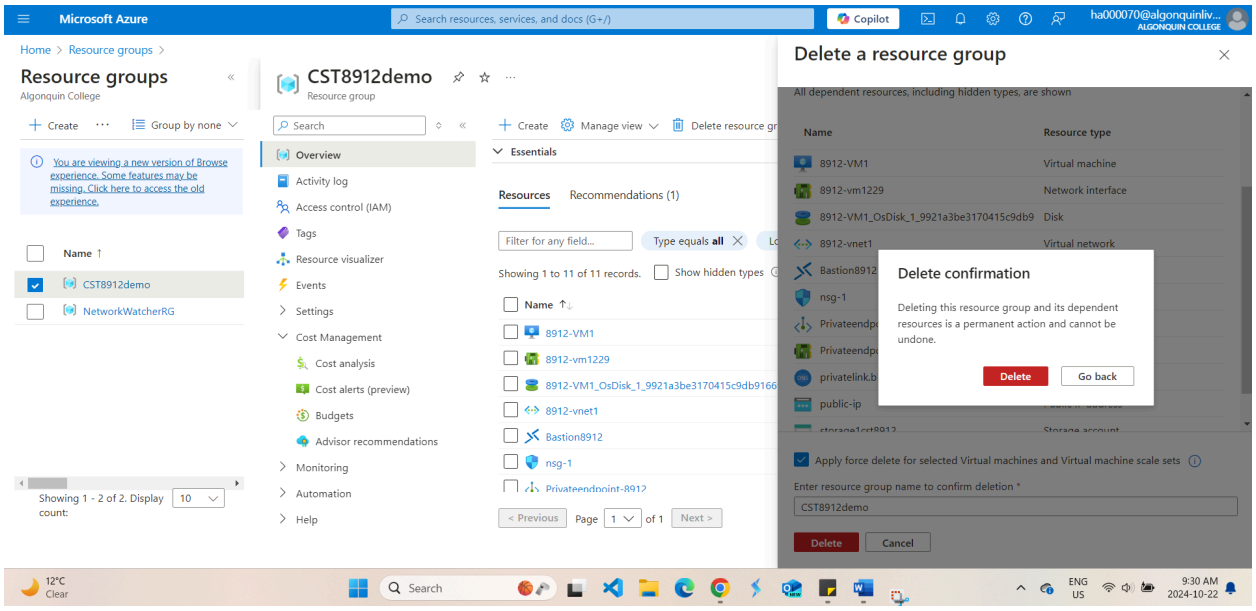
Close up of the quick access. The storage account, and blob container is correctly displayed.



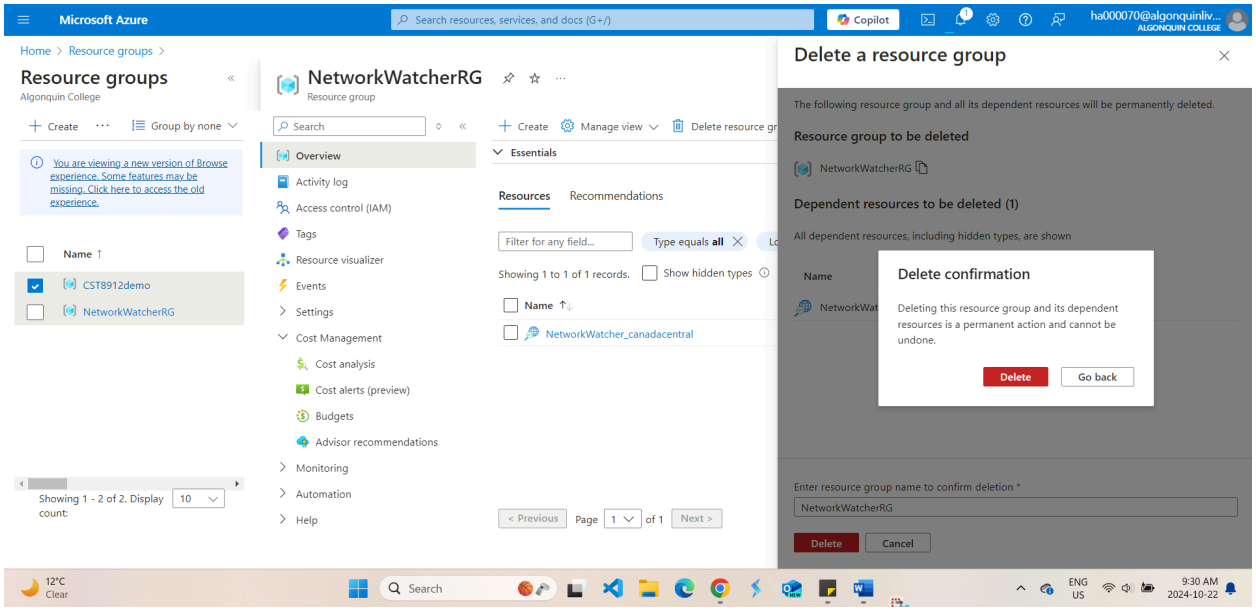
The server is powered off/logged out.



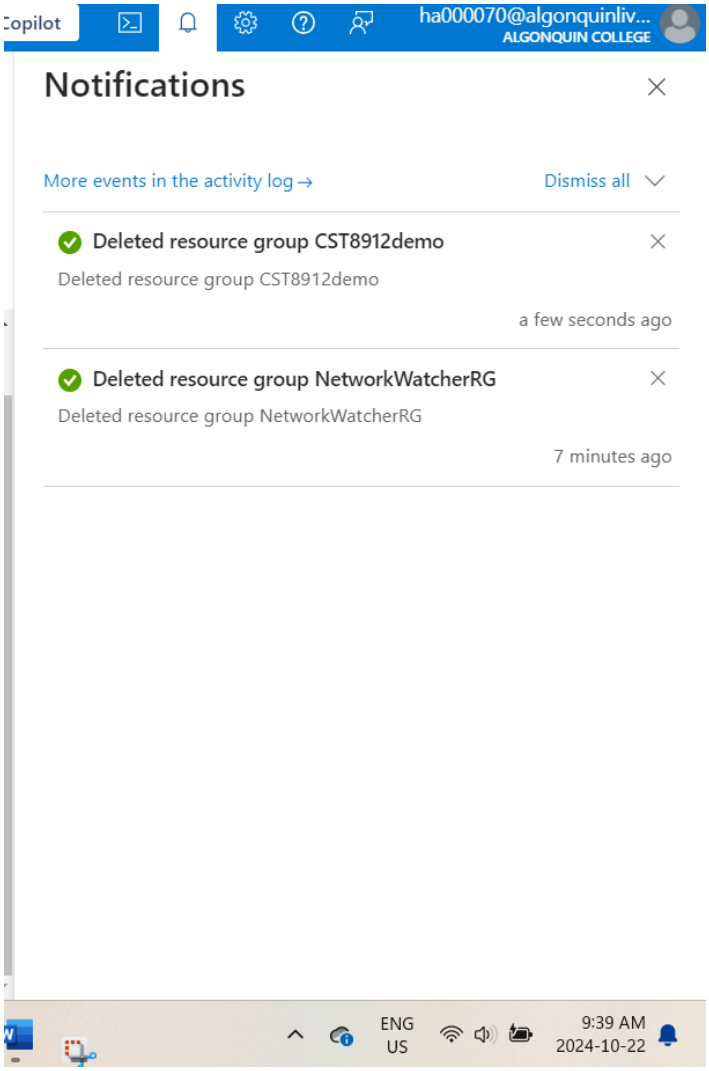
All resources (Vnets, VM, Storage Account, Private Endpoint, etc) are deleted via the resource group (CST8912demo).



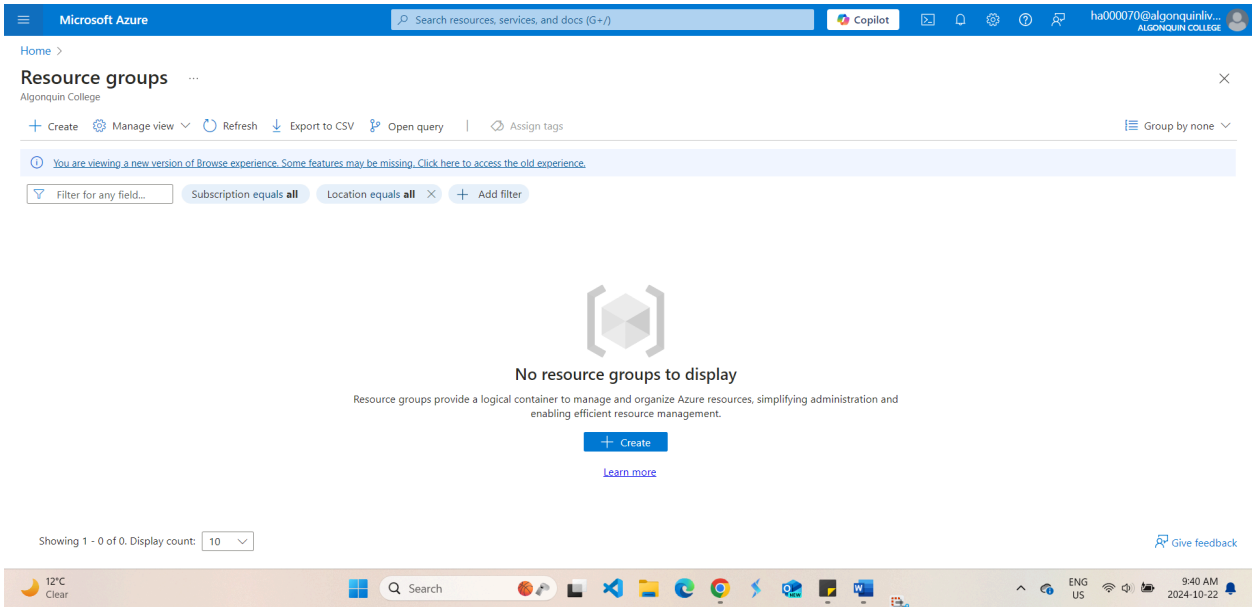
The automatic resource group NetworkWatcherRG is deleted.



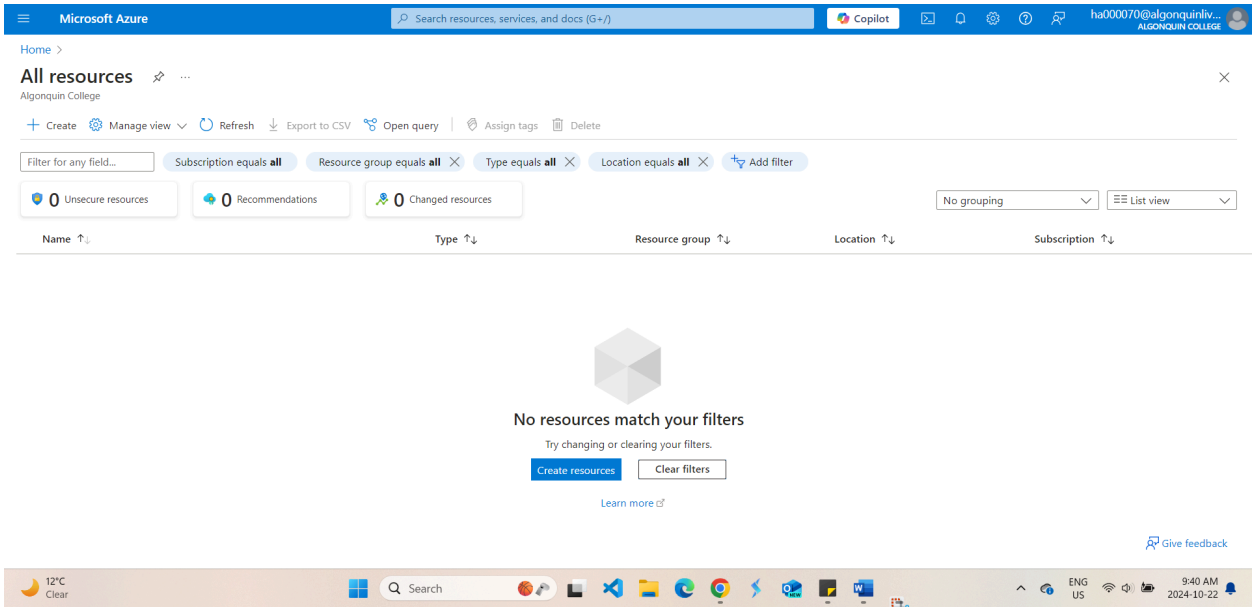
Both resource groups are successfully deleted.



There are no more resource groups; all resource groups are successfully deleted.



There are no more resources; all resources are successfully deleted.



Discussion

This lab focuses on implementing Azure Private Link using Azure Private Endpoint to provide a more secure way to connect to Azure resources from a virtual network.

First, a virtual network was created with the setup of Bastion Host. Bastion Host was used to connect to the Virtual Machine created within the virtual network for testing. Bastion Host offered secure access, simple browser connectivity, and enhanced security without needing a public IP address.

In this lab, a storage account was used as the Azure resource to be accessed. To further reduce security risks, the public network access in the storage account was disabled, ensuring we were only connecting via a private endpoint. A private endpoint was created and linked to the virtual network and storage account. The virtual machine was then created with the smallest size (B1), and configured to be within the same virtual network and subnet.

A blob container is created within the storage account for testing purposes. This was a simple and inexpensive way to test the connection. To test the connectivity, the VM was connected via Bastion Host, which showed some information in the PowerShell (with the command **nslookup storage1cst8912.blob.core.windows.net**). The explanation is included in the results section. In general, the output showed us that the private endpoint was configured correctly as it returned a private IP address.

Next, we used Microsoft Azure Storage Explore and the provided connection string (copied from the storage account) to successfully connect to the Azure storage account. The connection was fast and secure.

The only issue that was run into was the VM size. The chosen B1 size, which was chosen for cost efficiency, was not big enough to perform the tasks. In these cases, we can set up automatic size changes or scaling for a more cost-effective and time-saving solution.

Conclusion

Successful private endpoint configuration completed in this lab demonstrates the ability to create a secure way to connect to Azure resources without the need for public endpoints. As more and more companies are migrating to the cloud, it is important to focus on enhancing security. Private endpoints offer security because it eliminates the need for public endpoints and IP addresses that are more prone to security risks and attacks. Sometimes public endpoints are required, but in cases that they are not, another option should be used for best practice. Some goal-oriented scenarios where Private Links are suitable are:

- 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

In general, if a resource or service needs to be accessed securely without exposure to the public internet, then Private Links are a good candidate. To enhance security even further the next steps could include a deeper exploration of NSGs and Azure Firewall configurations.

References

Awati, R. (2024, June 18). *DNS attack*. TechTarget. https://www.techtarget.com/searchsecurity/definition/DNS-attack

How Azure Private Link Works. Training | Microsoft Learn. (n.d.-a). https://learn.microsoft.com/en-us/training/modules/introduction-azure-private-link/3-how-azure-private-link-works

Microsoft. (n.d.). *Pricing - azure private link: Microsoft Azure*. Pricing - Azure Private Link | Microsoft Azure. https://azure.microsoft.com/en-us/pricing/details/private-link/

Sudha, S., & Viswanatham, V. M. (2013). Addressing Security and Privacy Issues in Cloud Computing. *Journal of Theoretical and Applied Information Technology*, *48*(2), 708–719.

What is Azure private link? Training | Microsoft Learn. (n.d.). https://learn.microsoft.com/en-us/training/modules/introduction-azure-private-link/2-what-is-azure-private-link