

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).

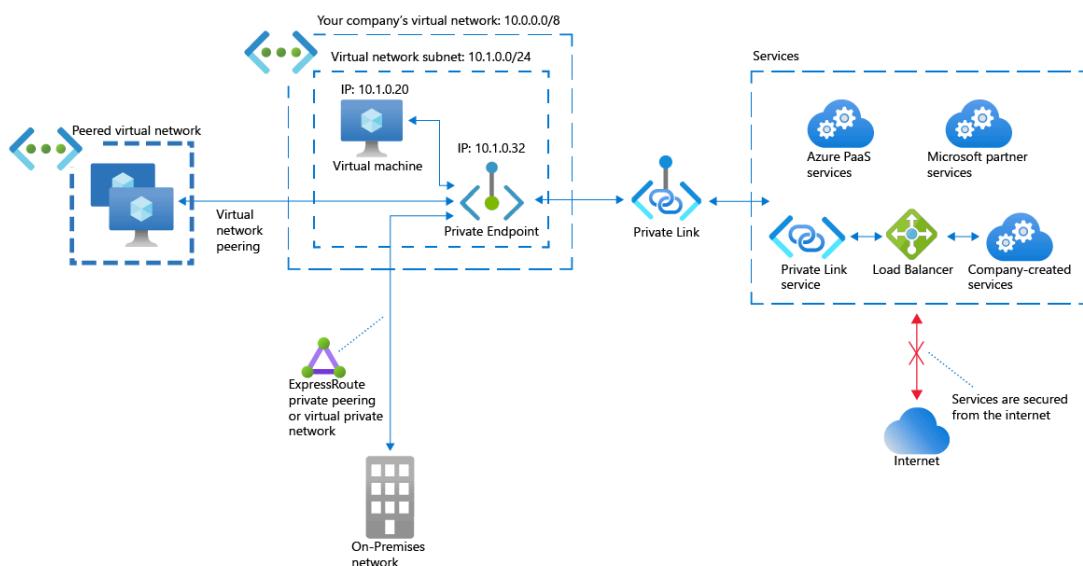
Replacing the public endpoint with a private network interface reduces and prevents those security risks. “Private Endpoint is the key technology behind Private Link. Private Endpoint is a network interface that enables a private and secure connection between your virtual network and an Azure service” (*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	<p>Select edit to apply Network policy for private endpoints.</p> <p>In Edit subnet network policy, select the checkbox next to Network security groups and Route Tables in the Network policies setting for all private endpoints in this subnet pull-down.</p> <p>Select Save.</p>

Private IP configuration	Select Dynamically allocate IP address.
--------------------------	--

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.

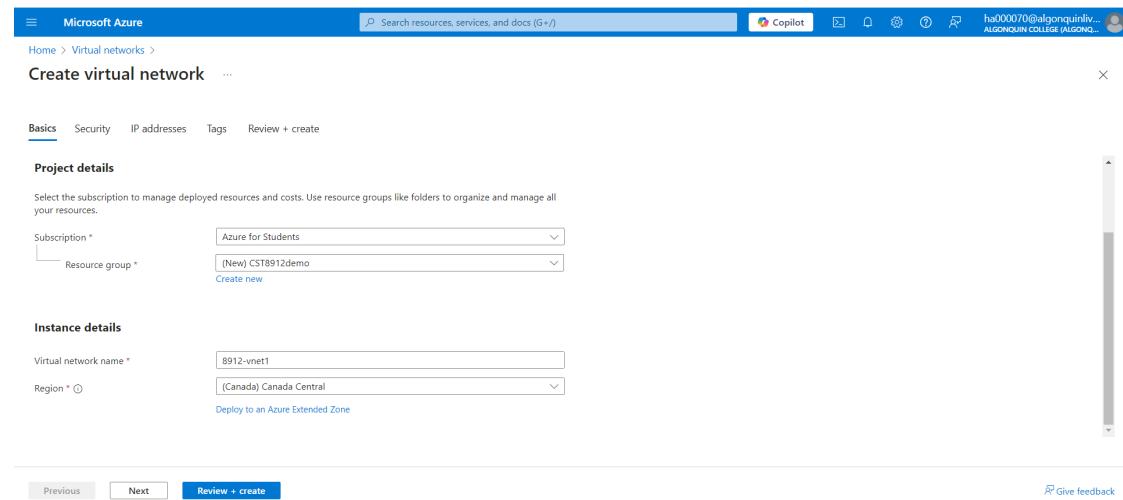
21. Clean all the resources created during the lab and document all the steps using screenshots and paste that in the lab report.

Results

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

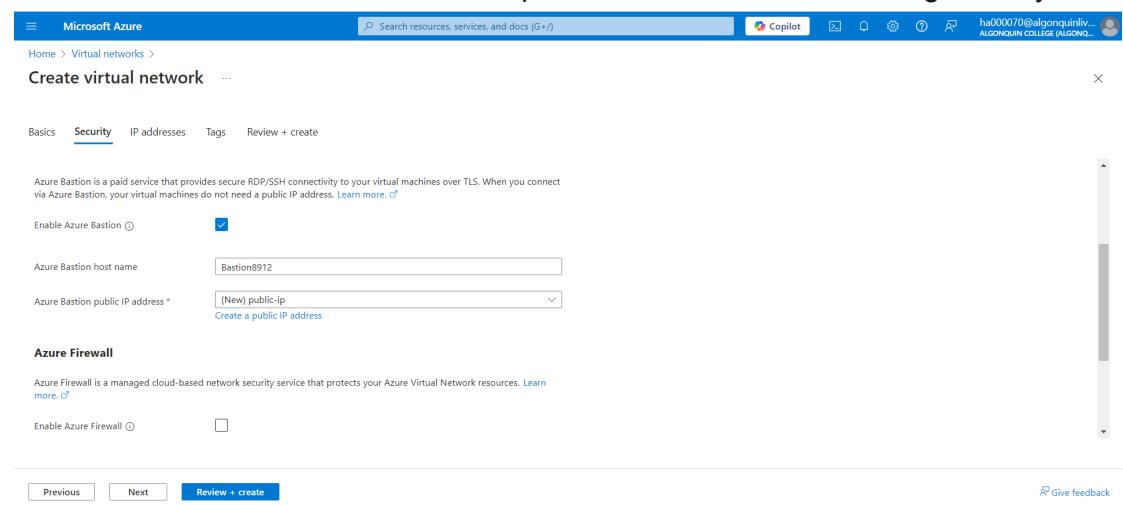
1. Create a virtual network and Bastion host

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.



The screenshot shows the 'Create virtual network' wizard on the 'Basics' tab. In the 'Project details' section, the subscription is set to 'Azure for Students' and the resource group is '(New) CST8912demo'. In the 'Instance details' section, the virtual network name is '8912-vnet1' and the region is '(Canada) Canada Central'. At the bottom, there are 'Previous' and 'Next' buttons, and a 'Review + create' button which is highlighted in blue.

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.



The screenshot shows the 'Create virtual network' wizard on the 'Security' tab. It includes sections for 'Azure Bastion' (with a checked checkbox), 'Azure Bastion host name' (set to 'Bastion8912'), 'Azure Bastion public IP address' (set to '(New) public-ip'), and 'Azure Firewall' (with an unchecked checkbox). At the bottom, there are 'Previous' and 'Next' buttons, and a 'Review + create' button which is highlighted in blue.

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.

The screenshot shows the 'Edit subnet' dialog in the Microsoft Azure portal. The 'Name' field is set to 'Subnet-1-8912'. Under 'IPv4', the 'Starting address' is '10.0.0.0' and the 'Size' is '/24 (256 addresses)'. The 'Subnet address range' is '10.0.0.0 - 10.0.0.255'. The 'IPV6' section has a note: 'This virtual network has no IPv6 address ranges.' The 'Private subnet' note states: 'Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, you must assign a public IP address to the subnet or enable a NAT gateway.' Buttons for 'Save' and 'Cancel' are at the bottom.

Subnet-1-8912 saved.

The screenshot shows the 'Create virtual network' dialog in the Microsoft Azure portal, specifically the 'IP addresses' tab. A new subnet named 'Subnet-1-8912' has been added to the list. The table shows:

Subnets	IP address range	Size	NAT gateway
Subnet-1-8912	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
AzureBastionSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)	-

Buttons for 'Previous', 'Next', and 'Review + create' are at the bottom.

Virtual Network (8912-vnet1) overview

The screenshot shows the Azure portal interface for a virtual network named "8912-vnet1". The left sidebar contains navigation links for Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Queues), and Queues. The main content area has tabs for Overview, Essentials, Properties, Capabilities (5), Recommendations, and Tutorials. The Capabilities tab is selected, showing five cards: DDoS protection (Not configured), Azure Firewall (Not configured), Peerings (Not configured), Private endpoints (Not configured), and Microsoft Defender for Cloud (Not configured). The top right corner shows user information: ha000070@algonquinlive.onmicrosoft.com and ALGONQUIN COLLEGE (ALGONQ...).

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

ha000070@algonquinlive.onmicrosoft.com ALGONQUIN COLLEGE (ALGONQ...

Home > 8912-vnet1-1729598934153 | Overview >

8912-vnet1 Virtual network

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS servers

Queues

Move Delete Refresh Give feedback

Essentials

Resource group (move) : CST8912demo

Location (move) : Canada Central

Subscription (move) : Azure for Students

Subscription ID : 68bc7947-18d3-4475-b568-0794e595cbe6

Address space : 10.0.0.0/16

DNS servers : Azure provided DNS service

Flow timeout : Configure

BGP community string : Configure

Virtual network ID : 146c0704-51ea-494e-b7db-cf763867a66b

Tags (edit) : Add tags

Topology Properties Capabilities (5) Recommendations Tutorials

DDoS protection

Configure additional protection from distributed denial of service attacks.

Not configured

Azure Firewall

Protect your network with a stateful L3-L7 firewall.

Not configured

Peerings

Seamlessly connect two or more virtual networks.

Not configured

Microsoft Defender for Cloud

Strengthen the security posture of your environment.

Private endpoints

JSON View

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.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Home > Storage accounts >' breadcrumb. The main title is 'Create a storage account'. A descriptive text box says: '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.' Below this, there are two dropdown menus: 'Subscription *' set to 'Azure for Students' and 'Resource group *' set to 'CST8912demo' with a 'Create new' link. The 'Instance details' section contains fields for 'Storage account name *' (set to 'storage1cst8912'), 'Region *' (set to '(Canada) Canada Central' with a 'Deploy to an Azure Extended Zone' link), 'Primary service' (set to 'Select a primary service'), and 'Performance *' (radio button selected for 'Standard: Recommended for most scenarios (general-purpose v2 account)'). The 'Redundancy' field is set to 'Locally-redundant storage (LRS)'. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Review + create' button.

Storage account (storage1cst8912) overview

The screenshot shows the Azure Storage account overview page for 'storage1cst8912'. The left sidebar includes links for Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Data storage (Containers, File shares, Queues, Tables), and Security + networking. The main content area has tabs for Overview, Properties (selected), Monitoring, Capabilities (7), Recommendations (0), Tutorials, and Tools + SDKs. Under the Properties tab, the 'Essentials' section displays resource group (CST8912demo), location (canadacentral), subscription (Azure for Students), disk state (Available), and tags (Add tags). The 'Blob service' section shows settings like Hierarchical namespace (Disabled), Default access tier (Hot), Blob anonymous access (Disabled), Blob soft delete (Enabled (7 days)), Container soft delete (Enabled (7 days)), Versioning (Disabled), and Change feed (Disabled). The 'Security' section includes Require secure transfer for REST API operations (Enabled), Storage account key access (Enabled), Minimum TLS version (Version 1.2), and Infrastructure encryption (Disabled). The 'Networking' section shows Allow access from (All networks). A JSON View link is located in the top right corner.

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.

The screenshot shows the Azure Storage account Networking page for 'storage1cst8912'. The left sidebar includes links for Storage browser, Storage Mover, Partner solutions, Data storage (Containers, File shares, Queues, Tables), and Security + networking (Networking selected). The main content area has tabs for Firewalls and virtual networks (selected), Private endpoint connections, and Custom domain. It features Save, Discard, Refresh, and Give feedback buttons. A message states: 'Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.' Below this, the 'Network Routing' section asks how to route traffic from source to endpoint, with Microsoft network routing selected. The 'Publish route-specific endpoints' section has options for Microsoft network routing and Internet routing, both unchecked. A success message in the top right corner says: 'Successfully saved firewall and virtual network settings' and 'Successfully saved firewall and virtual network settings for storage account 'storage1cst8912''. A tooltip for 'Configure network security for your storage accounts' points to 'Learn more'.

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).

The screenshot shows the 'Create a private endpoint' wizard in the Microsoft Azure portal. The current step is 'Basics'. The page title is 'Create a private endpoint'.

Project details:

- Subscription: Azure for Students
- Resource group: CST8912demo (selected)
- Create new

Instance details:

- Name: Privateendpoint-8912
- Network Interface Name: Privateendpoint-8912-nic
- Region: Canada Central

At the bottom, there are navigation buttons: '< Previous' and 'Next : Resource >'.

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

Microsoft Azure

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

Home > Private Link Center | Private endpoints >

Create a private endpoint ...

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

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

Connection method (1)

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

Subscription * (1)

Azure for Students

Resource type * (1)

Microsoft.Storage/storageAccounts

Resource * (1)

storage1cst8912

Target sub-resource * (1)

blob

< Previous Next : Virtual Network >

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

ha000070@algonquinliv... ALGONQUIN COLLEGE (ALGON...)

Home > Private Link Center | Private endpoints >

Create a private endpoint ...

Networking

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

Virtual network ① 8912-vnet1 (CST8912demo)

Subnet * ① 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

This change will affect all private endpoints

Existing private endpoints

Name	Private IP	Resource	Sub-resource

Save Discard

Finished editing subnet network policy

Microsoft Azure

Search resources, services, and docs (G+)

Home > Private Link Center | Private endpoints >

Create a private endpoint ...

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

Networking

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

Virtual network ① 8912-vnet1 (CST8912demo)

Subnet * ① Subnet-1-8912

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

Private IP configuration

Dynamically allocate IP address

Statically allocate IP address

Application security group

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

+ Create

Application security group

< Previous Next : DNS >

DNS is left default.

The screenshot shows the Microsoft Azure 'Create a private endpoint' wizard at the 'DNS' step. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Create a private endpoint' button. Below the navigation, a breadcrumb trail shows 'Home > Private Link Center | Private endpoints > Create a private endpoint'. The main content area has tabs for 'Basics', 'Resource', 'Virtual Network', 'DNS' (which is selected), 'Tags', and 'Review + create'. A sub-section titled 'Private DNS integration' explains that connecting privately requires a DNS record. It includes a note about utilizing private DNS zones or host files, a 'Learn more' link, and a radio button selection between 'Yes' (selected) and 'No'. Configuration fields for 'Configuration name' (privatelink-blob-core-win...), 'Subscription' (Azure for Students), 'Resource group' (CST8912demo), and 'Private DNS zone' ((new) privatelink.blob.cor...) are shown. At the bottom are 'Next : Tags >' and '< Previous' buttons.

Tags is left default.

The screenshot shows the Microsoft Azure 'Create a private endpoint' wizard at the 'Tags' step. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Create a private endpoint' button. Below the navigation, a breadcrumb trail shows 'Home > Private Link Center | Private endpoints > Create a private endpoint'. The main content area has tabs for 'Basics', 'Resource', 'Virtual Network', 'DNS', 'Tags' (which is selected), and 'Review + create'. A sub-section explains that tags are name/value pairs for categorization and billing. It includes a note about tag synchronization across resource settings and a 'Learn more about tags' link. A note also states that tags will automatically update if changed. A table for adding tags is shown with columns for 'Name', 'Value', and 'Resource'. The first row has empty input fields. The second row shows '2 selected' in the 'Resource' dropdown. At the bottom are 'Next : Review + create >' and '< Previous' buttons.

Private endpoint overview

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

Home > Microsoft.PrivateEndpoint-20241022081518 | Overview > Privateendpoint-8912

Private endpoint

Search Delete Refresh

Overview Essentials JSON View

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

Resource group : CST8912demo

Location : Canada Central

Subscription : Azure for Students

Subscription ID : 68bc7947-18d3-4475-b568-0794e595cbe6

Provisioning state : Succeeded

Virtual network/subnet : 8912-vnet1/Subnet-1-8912

Network interface : Privateendpoint-8912-nic

Private link resource : storage1cts8912

Target sub-resource : blob

Connection status : Approved

Request/Response : Auto-Approved

Tags (edit) : Add tags

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)

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Help me choose the right VM size' button. Below the navigation, the breadcrumb trail shows 'Home > Virtual machines > Create a virtual machine'. The main form is titled 'Create a virtual machine' with a '... more' link. It contains several input fields:

- Subscription:** Azure for Students (selected)
- Resource group:** CST8912demo (selected)
- Virtual machine name:** 8912-VM1 (highlighted with a green checkmark)
- Region:** (Canada) Canada Central
- Availability options:** No infrastructure redundancy required
- Security type:** Standard
- Image:** Windows Server 2022 Datacenter: Azure Edition - x64 Gen2 (selected)

Below the image selection, a note states: "This image is compatible with additional security features. Click here to swap to the Trusted launch security type." At the bottom of the form, there is a 'VM architecture' section with a radio button for 'Arm64' (selected), and navigation buttons: '< Previous', 'Next : Disks >', and a blue 'Review + create' button.

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

The screenshot shows the 'Create a virtual machine' wizard on the 'Administrator account' step. The 'Size' dropdown is set to 'Standard_B1s - 1 vcpu, 1 GiB memory (\$11.39/month) (free services eligible)'. The 'Administrator account' section includes fields for 'Username' (donna), 'Password', and 'Confirm password', all of which have green checkmarks indicating they are valid. Navigation buttons at the bottom include '< Previous', 'Next : Disks >', and a blue 'Review + create' button.

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

The screenshot shows the 'Create a virtual machine' wizard on the 'Inbound port rules' step. Under 'Public inbound ports', the 'None' option is selected. A note below states: 'All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.' Navigation buttons at the bottom include '< Previous', 'Next : Disks >', and a blue 'Review + create' button.

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.

The screenshot shows the Microsoft Azure portal interface for creating a Network Security Group. The top navigation bar includes 'Microsoft Azure', a search bar, and user account information. The main page title is 'Create network security group'. A 'Name *' field contains 'nsg-1'. Under 'Inbound rules', there is a single rule: '1000: default-allow-rdp' allowing 'Any' RDP (TCP/3389). A link '+ Add an inbound rule' is available. Under 'Outbound rules', it says 'No results.' and there is a link '+ Add an outbound rule'. At the bottom left is a blue 'OK' button.

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.

The screenshot shows the Microsoft Azure portal interface for creating a new Virtual Machine. The top navigation bar includes 'Microsoft Azure', a search bar, and user account information. The main page title is 'Create a virtual machine'. In the 'Network interface' section, 'Virtual network *' is set to '8912-vnet1' and 'Subnet *' is set to 'Subnet-1-8912 (10.0.0.0/24)'. Under 'NIC network security group', the 'Advanced' option is selected. The 'Configure network security group *' dropdown shows '(new) nsg-1'. Other options like 'Delete NIC when VM is deleted' and 'Enable accelerated networking' are present but not checked. At the bottom are buttons for '< Previous', 'Next : Management >', and a prominent blue 'Review + create' button.

Overview of the created virtual machine.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the main title is '8912-VM1' under the 'Virtual machine' category. A left sidebar contains various management options like Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Network settings, Load balancing, Application security groups, Network manager, Settings, Availability + scale, Security, Backup + disaster recovery, and Operations. The main content area is titled 'Overview' and includes sections for 'Essentials' (Resource group: CST8912demo, Status: Running, Location: Canada Central, Subscription: Azure for Students, etc.) and 'Properties' (Virtual machine details like Computer name, Operating system, VM generation, VM architecture). There's also a 'Networking' section showing Public and Private IP addresses. A 'Tags (edit)' section is present at the bottom of the main content area.

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.

The screenshot shows the Microsoft Azure portal interface. The title is 'storage1cst8912 | Access keys'. The left sidebar has categories like Storage browser, Storage Mover, Partner solutions, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN), and Access keys (which is selected). The main content area displays two sets of access keys: 'key1' and 'key2'. Each key has a 'Rotate key' button, a timestamp (Last rotated: 10/22/2024 (0 days ago)), and a 'Key' field with a 'Show' button. Below each key is a 'Connection string' field containing a DefaultEndpointsProtocol=https:AccountName=storage1cst8912;AccountKey=W... URL. A note at the top says: 'Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.' It also links to 'Learn more about managing storage account access keys'.

6. Adding a Blob Container

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

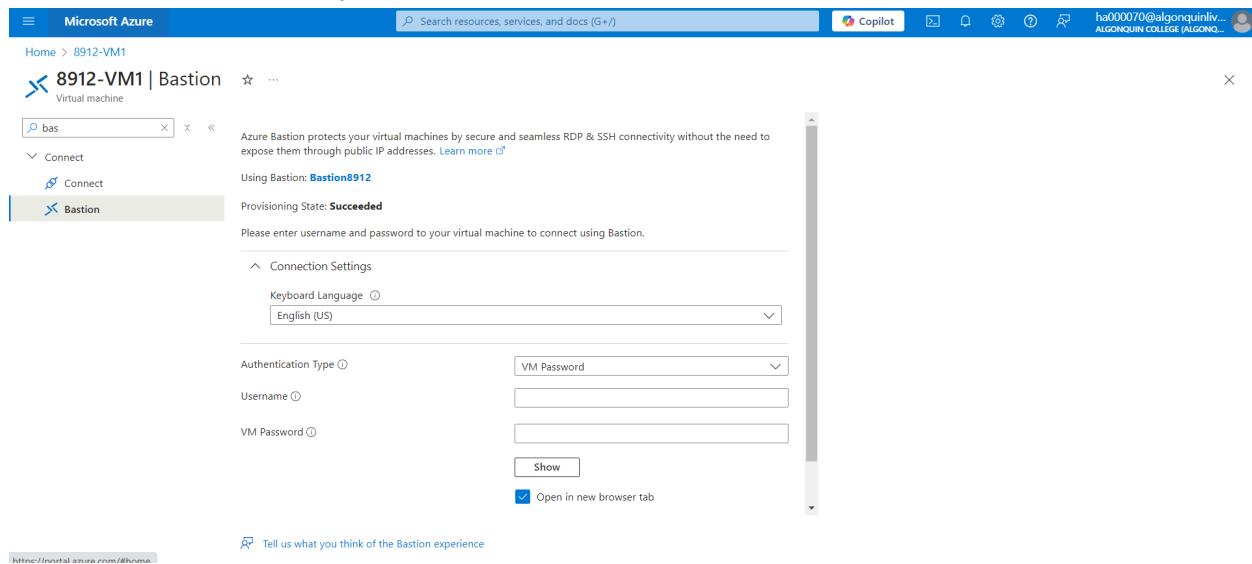
The screenshot shows the Microsoft Azure Storage Containers page for the storage account 'storage1cst8912'. On the left, the navigation menu is expanded to show 'Containers' under 'Data storage'. The main area displays a table of existing containers, including '\$logs' and 'container8912'. A 'New container' dialog box is open on the right, prompting for a name ('container8912') and access level ('Private (no anonymous access)'). A note indicates that anonymous access is disabled. A 'Create' button is at the bottom of the dialog.

container8912 is successfully created.

The screenshot shows the Microsoft Azure Storage Containers page for the storage account 'storage1cst8912'. The 'Containers' section lists '\$logs' and 'container8912'. A success message in a toast notification states 'Successfully created storage container' and 'Successfully created storage container 'container8912''. The 'Show deleted containers' toggle switch is visible at the bottom of the table.

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.

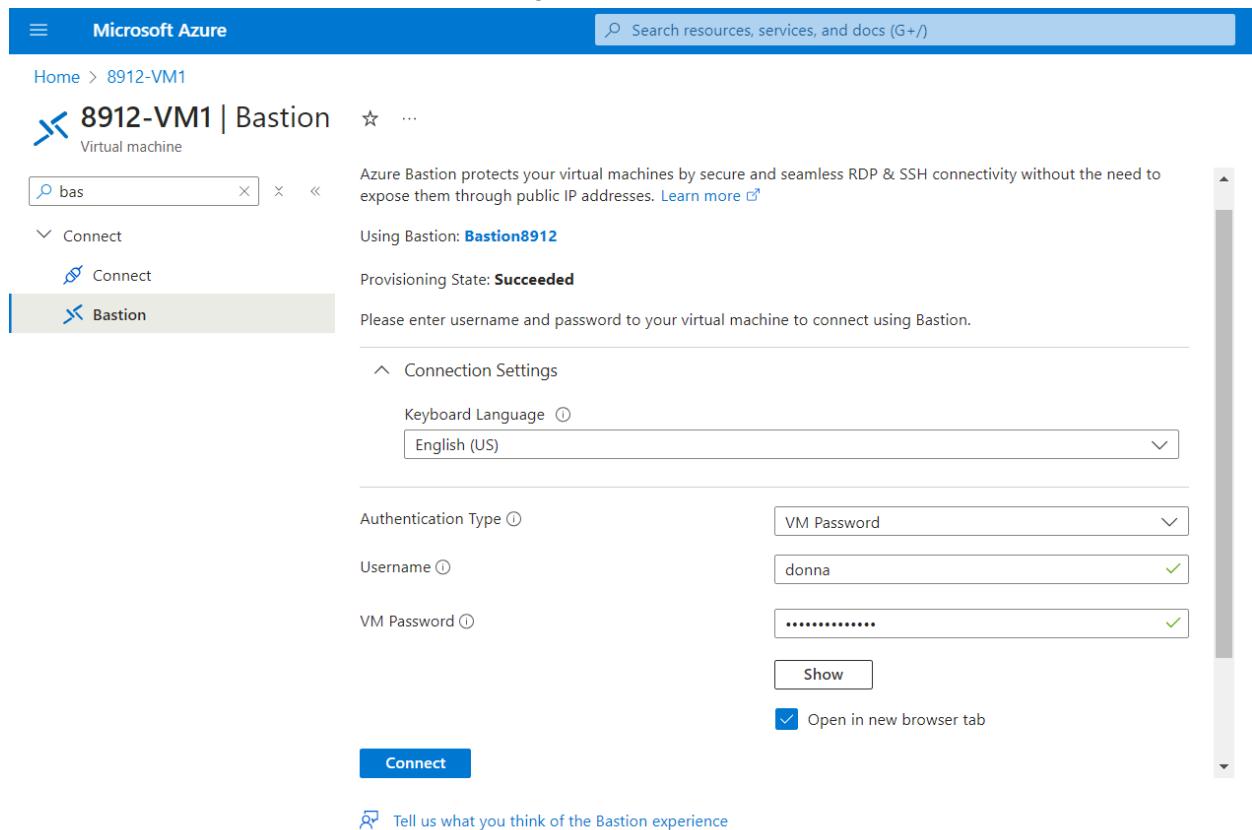


The screenshot shows the Microsoft Azure portal interface for connecting to a virtual machine named 8912-VM1 via Bastion. The 'Bastion' tab is selected in the navigation bar. The main area displays connection settings, including:

- Keyboard Language: English (US)
- Authentication Type: VM Password
- Username: (empty field)
- VM Password: (empty field)
- Show password button
- Open in new browser tab checkbox (unchecked)

A note at the top states: "Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)". Below the form, there's a link to "Tell us what you think of the Bastion experience".

Username and password is entered to log in.

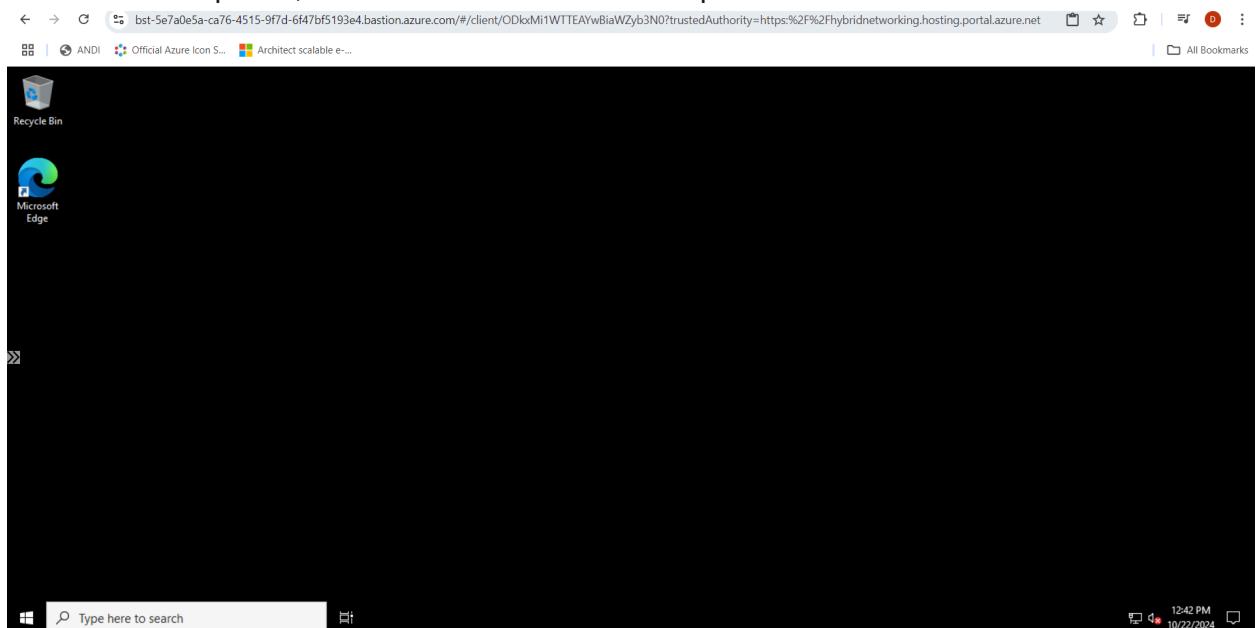


The screenshot shows the Microsoft Azure portal interface for connecting to a virtual machine named 8912-VM1 via Bastion. The 'Bastion' tab is selected in the navigation bar. The main area displays connection settings, with the following changes made:

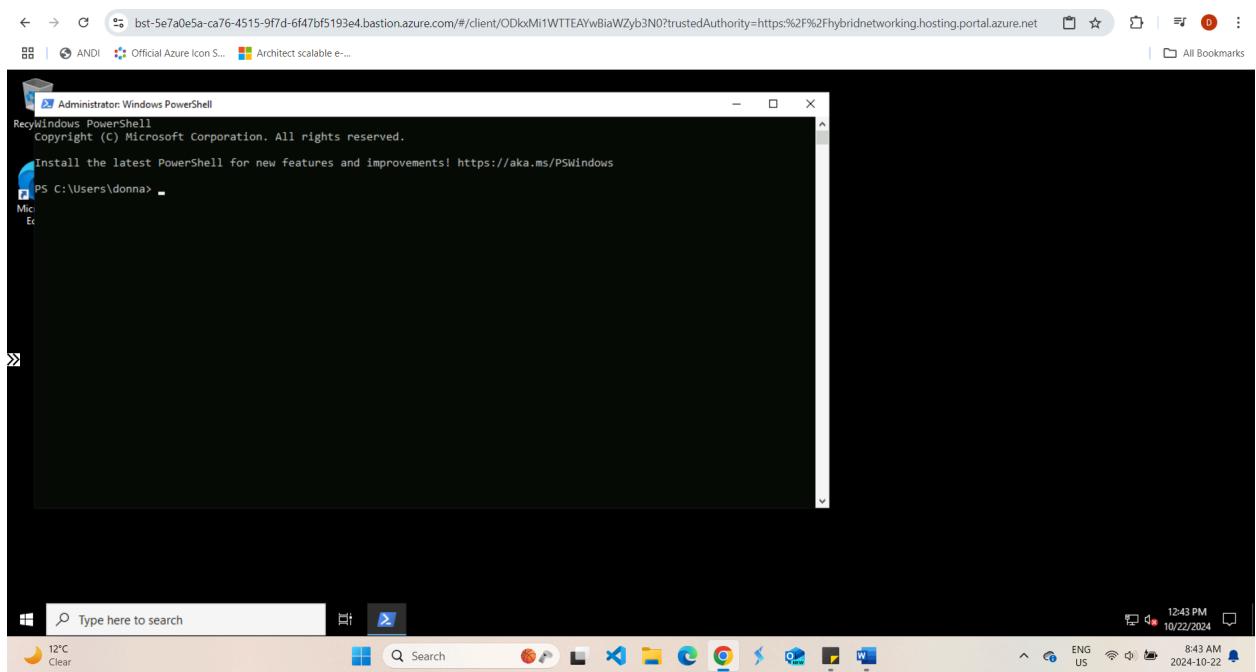
- Keyboard Language: English (US)
- Authentication Type: VM Password
- Username: donna
- VM Password: (redacted)
- Show password button
- Open in new browser tab checkbox (unchecked)

A note at the top states: "Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)". Below the form, there's a link to "Tell us what you think of the Bastion experience".

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

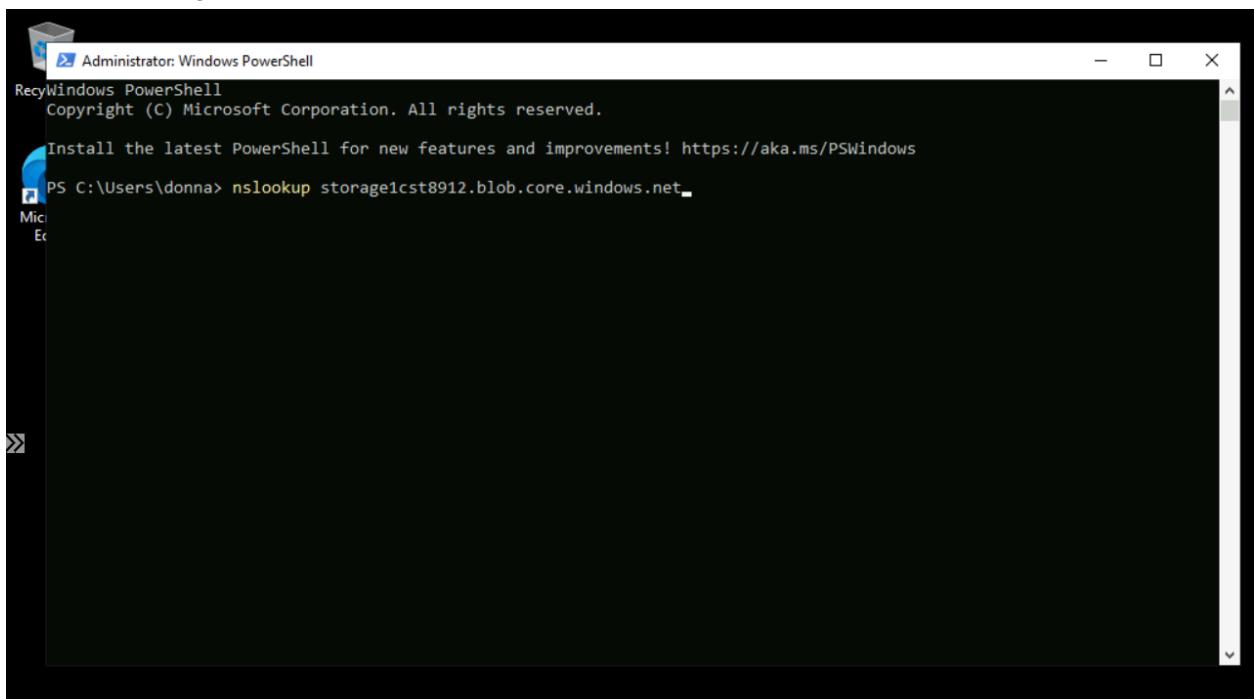


Powershell is opened on the server.



The following command is entered in the powershell:

```
nslookup storage1cst8912.blob.core.windows.net
```



A screenshot of an Administrator Windows PowerShell window. The title bar reads "Administrator: Windows PowerShell". The window displays the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

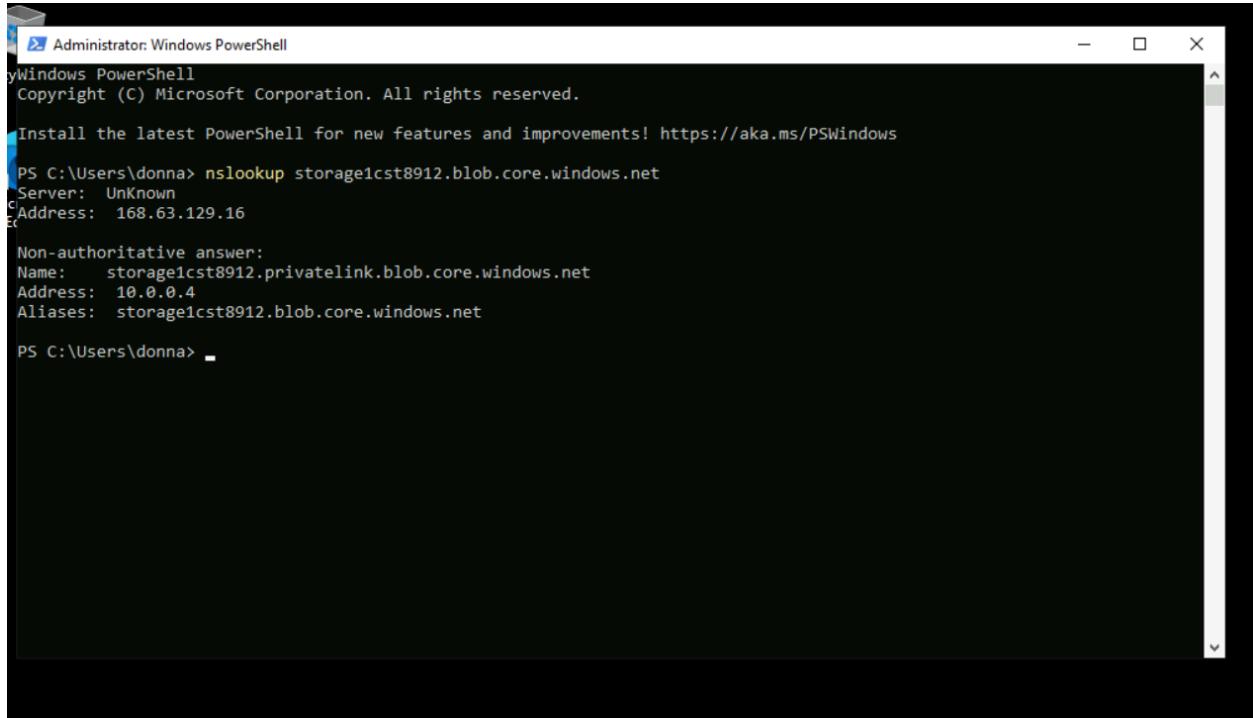
PS C:\Users\donna> nslookup storage1cst8912.blob.core.windows.net
```

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 10.0.0.4 is the address of the storage account, and is most likely the subnet we set above (Subnet-1-8912).



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the following command and its 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>
```

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)

The screenshot shows the Microsoft Azure portal interface for changing the VM size. The left sidebar shows the navigation path: Home > 8912-VM1 > Virtual machine > Size. The main content area displays a list of 396 VM sizes. The 'B2s' row is highlighted, indicating it is selected. The table includes columns for VM Size, Type, vCPUs, RAM (GiB), Data disks, Max IOPS, and Local storage (GiB). A note at the top states: "If the virtual machine is currently running, changing its size will cause it to be restarted. Stopping the virtual machine may reveal additional sizes." A 'Resize' button is visible at the bottom left of the table.

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

The screenshot shows the Microsoft Azure portal interface for the updated VM overview. The left sidebar shows the navigation path: Home > 8912-VM1 > Virtual machine > Overview. The main content area displays the VM's properties under the 'Essentials' tab. The 'Properties' tab is selected, showing details like Resource group (CST8912demo), Status (Updating), Location (Canada Central), Subscription (Azure for Students), and Subscription ID (68bc7947-18d3-4475-b568-0794e595cbe6). The 'Networking' tab is also visible. A note at the top states: "Advisor (1 of 1): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s)." A 'JSON View' link is located in the top right corner of the properties table.

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

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

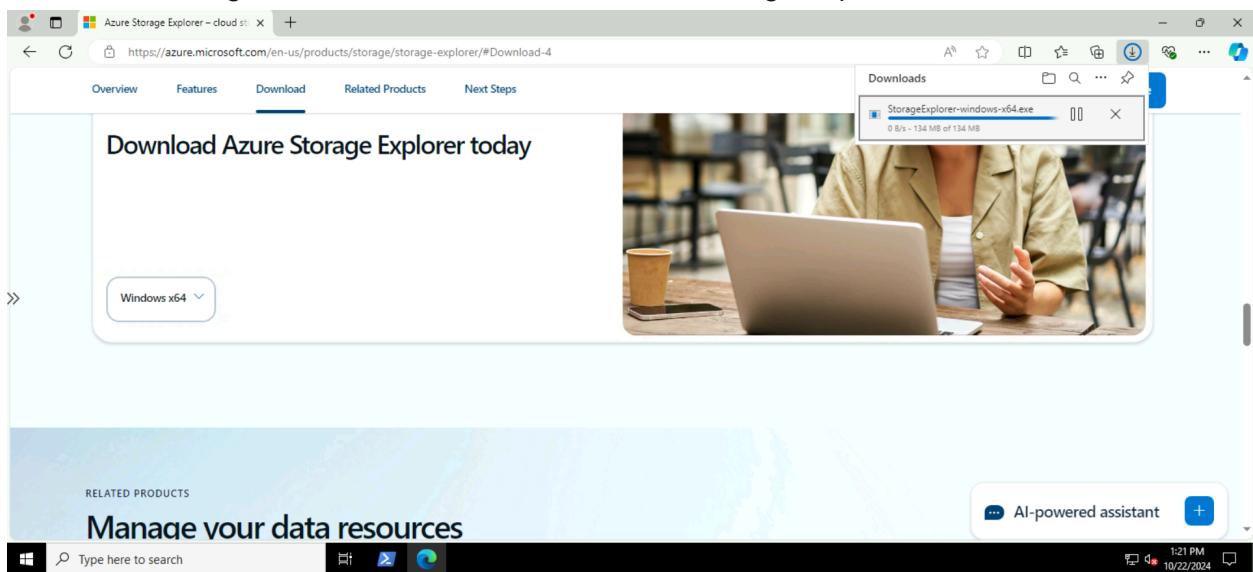
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

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

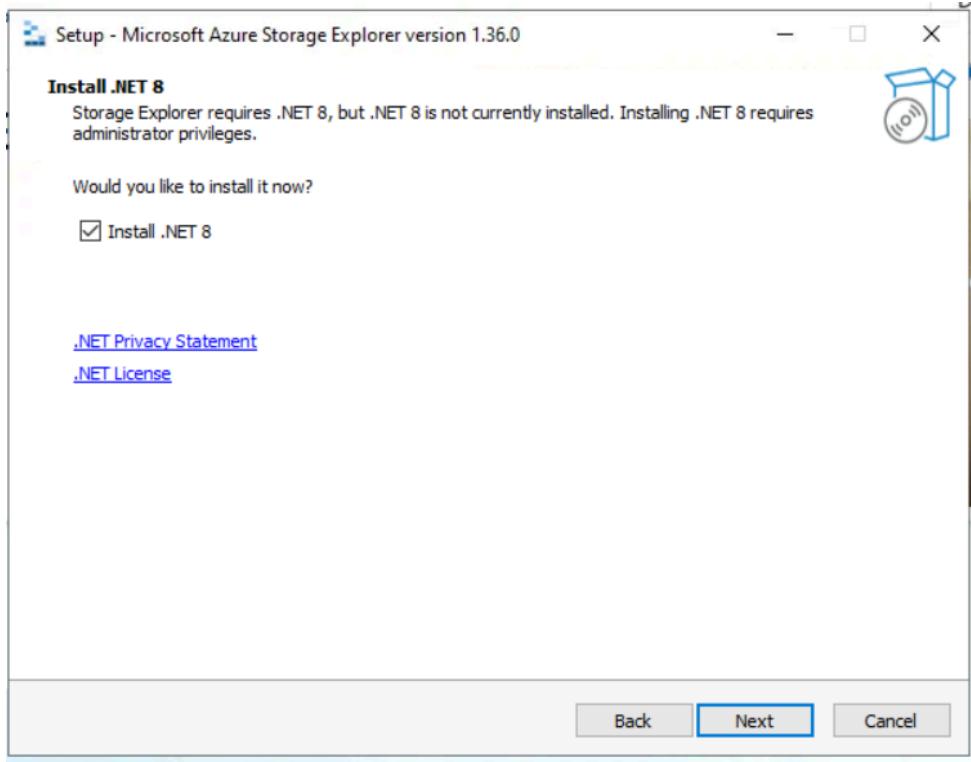
Non-authoritative answer:
Name: storage1cst8912.privatelink.blob.core.windows.net
Address: 10.0.0.4
Aliases: storage1cst8912.blob.core.windows.net

PS C:\Users\donna>
```

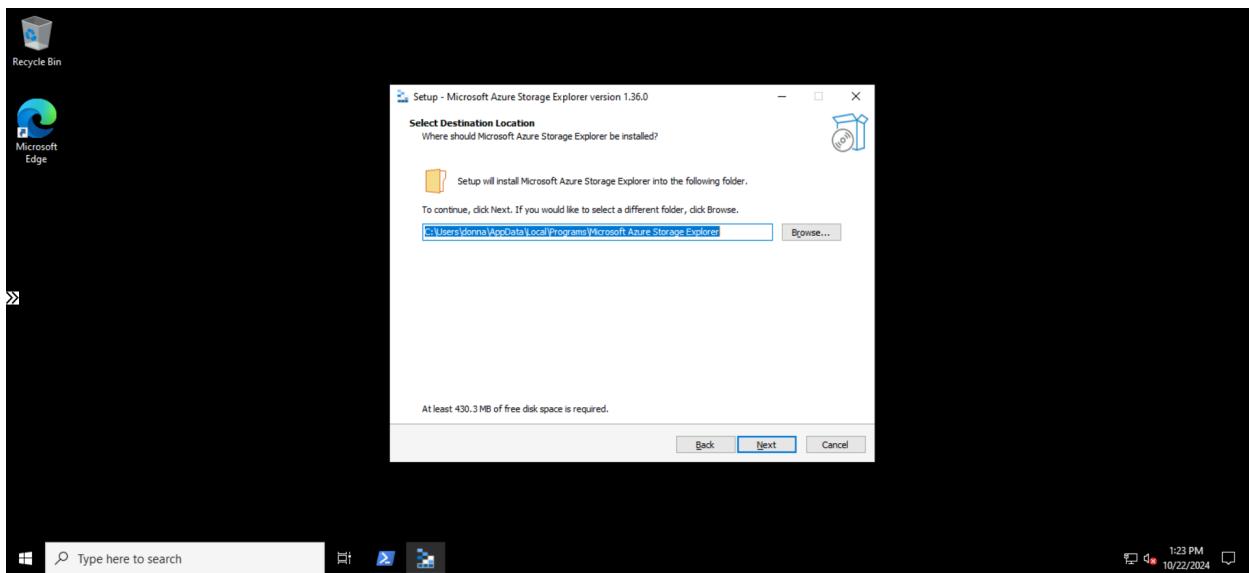
Use Microsoft Edge to download the Microsoft Azure Storage Explorer.



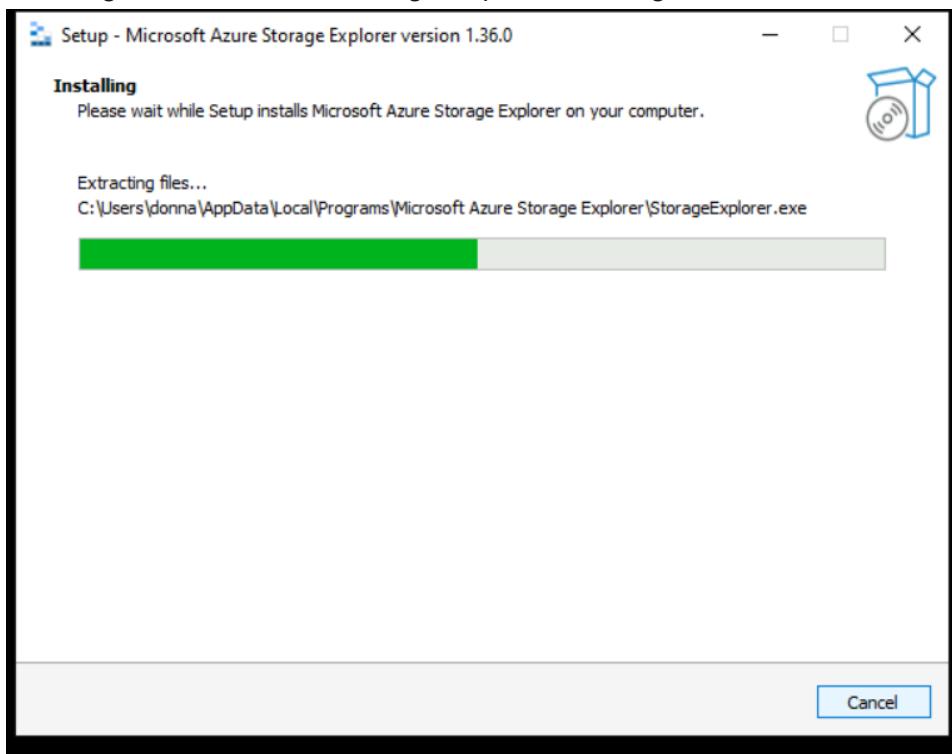
Installing Microsoft Azure Storage Explorer



Installing Microsoft Azure Storage Explorer in file location.

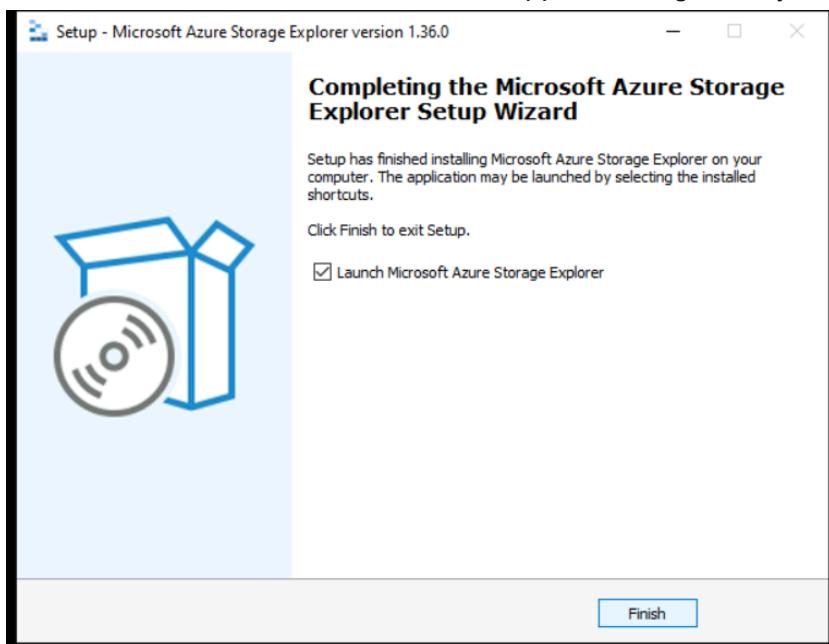


Installing Microsoft Azure Storage Explorer, loading.

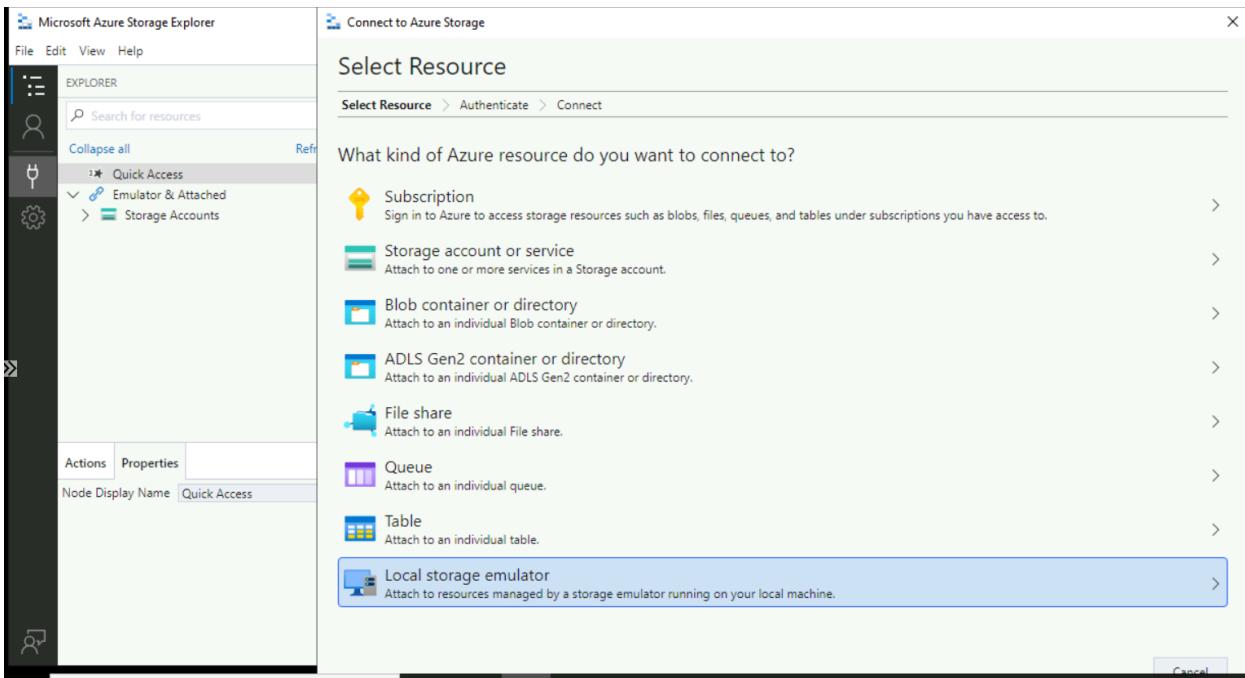


Installing Microsoft Azure Storage Explorer, completed.

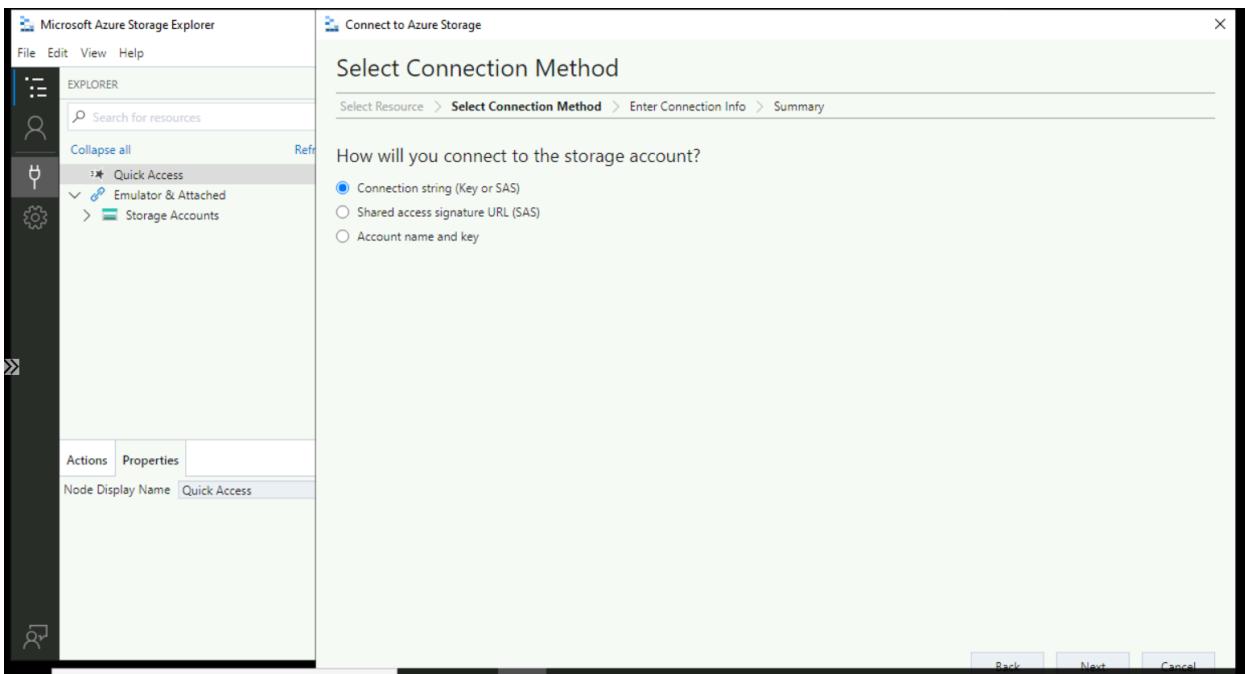
Launched is left checked to launch the application right away.



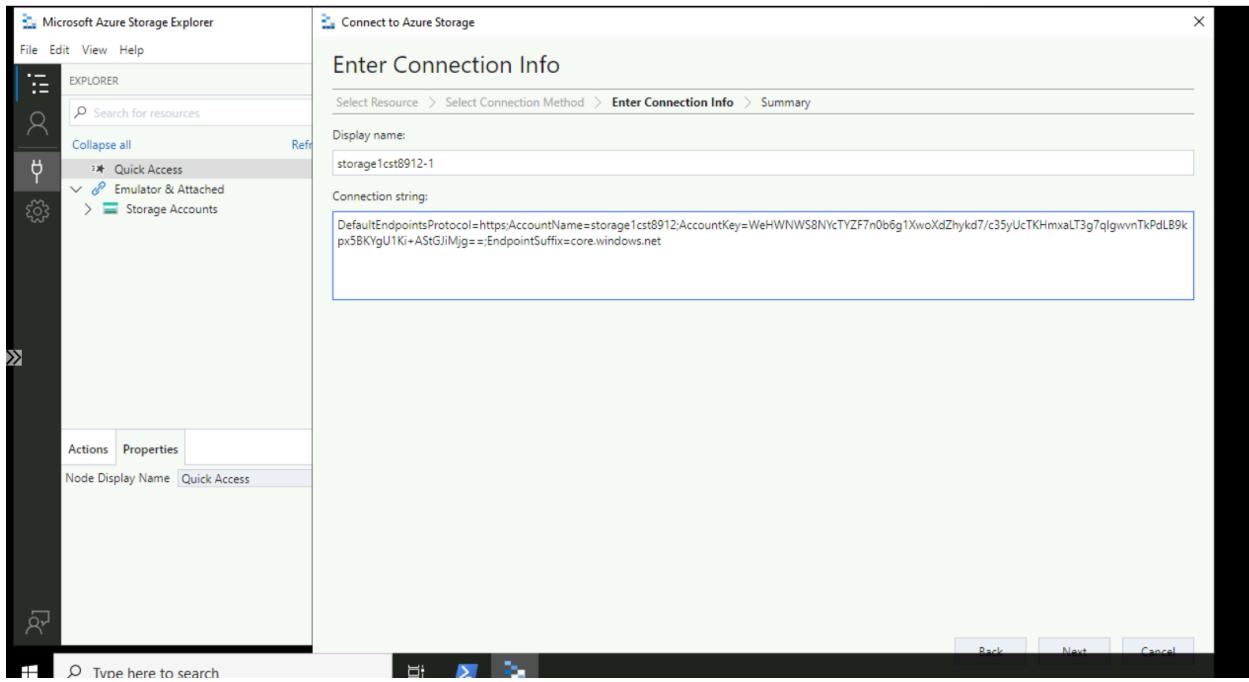
Accessed the “Select resource” by selecting the power plug button.
Select “Local storage emulator” to connect to the storage account created previously.



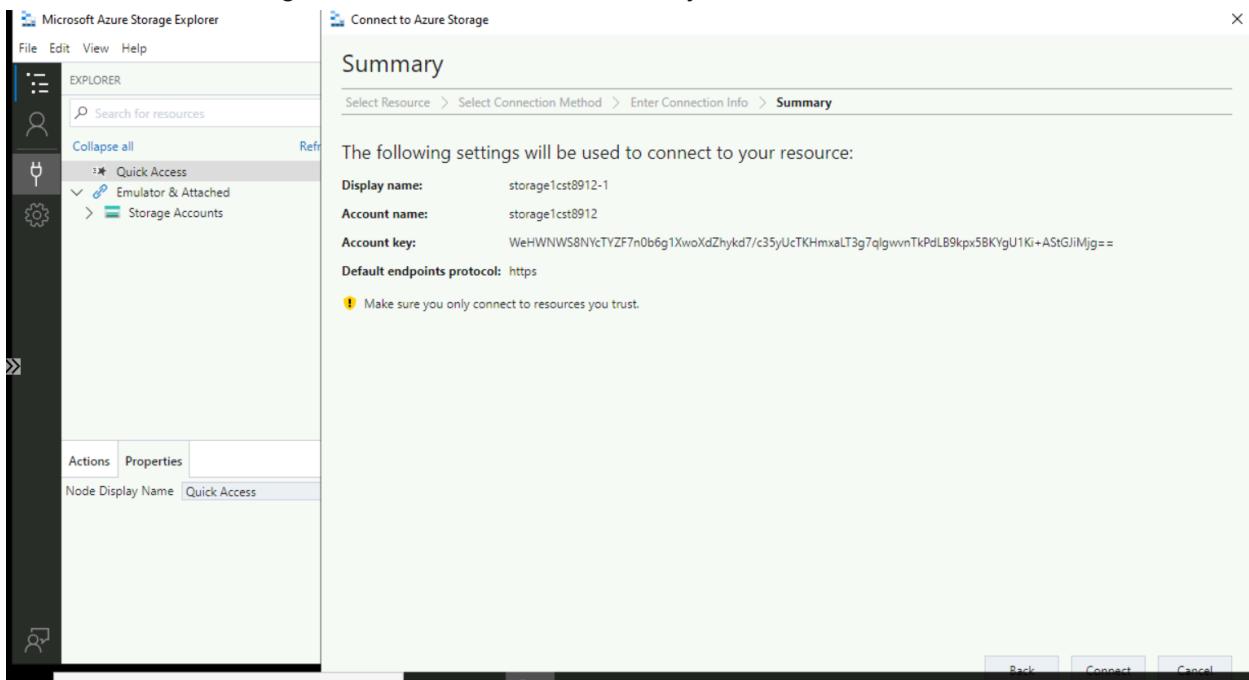
Select connection string as the method to connect to the storage account.



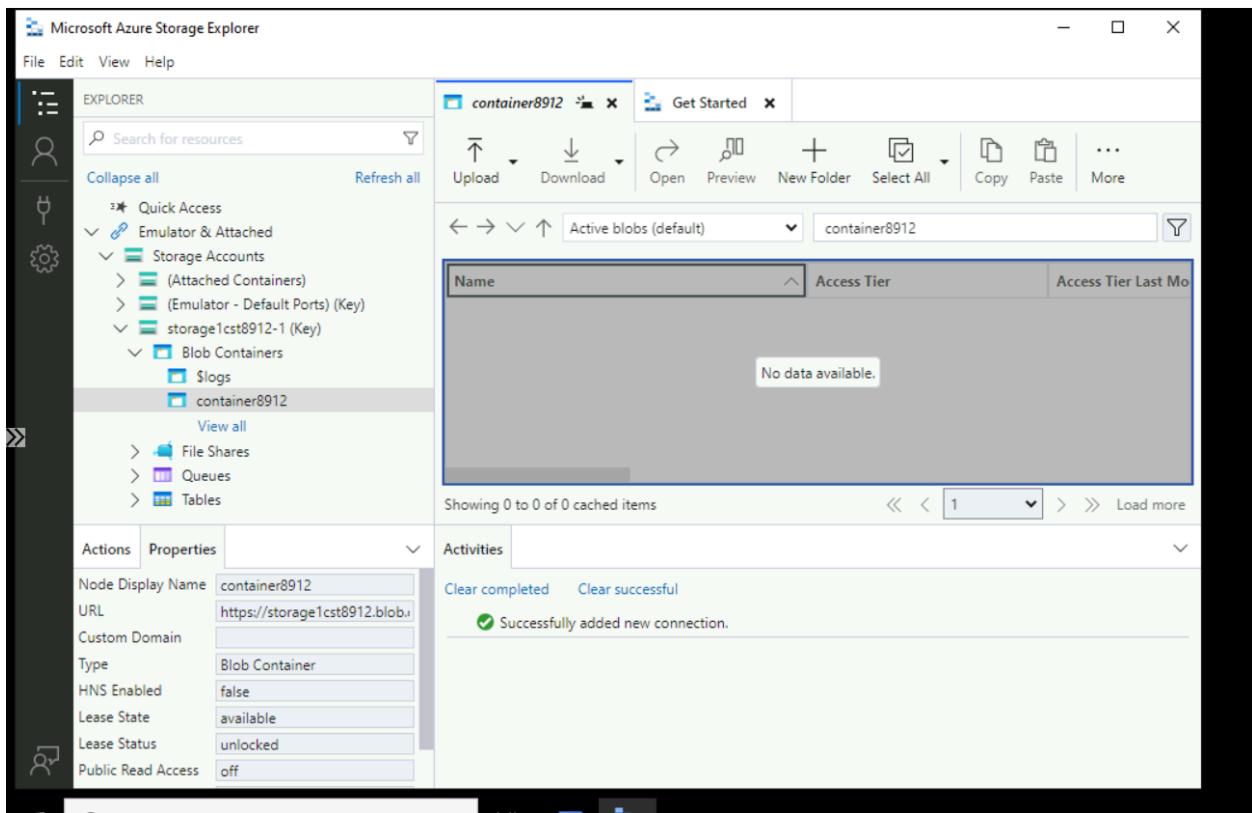
The connection string for key1 previously copied is pasted in the connection string input box.
The display name is automatically generated.



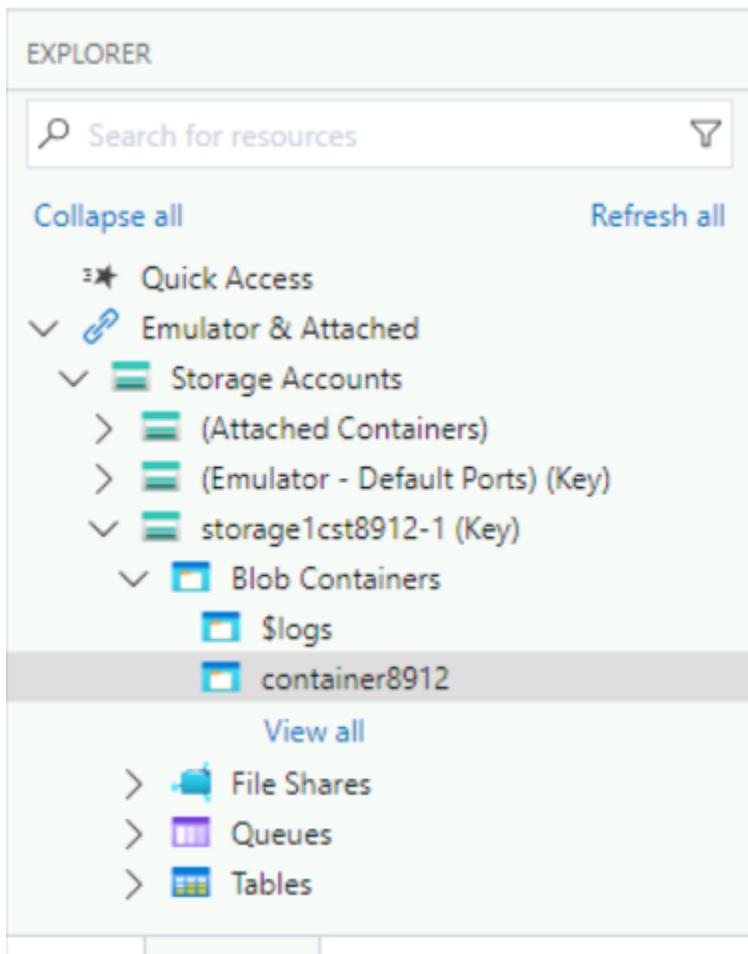
The connection settings are reviewed in the Summary tab, and then connect is selected.



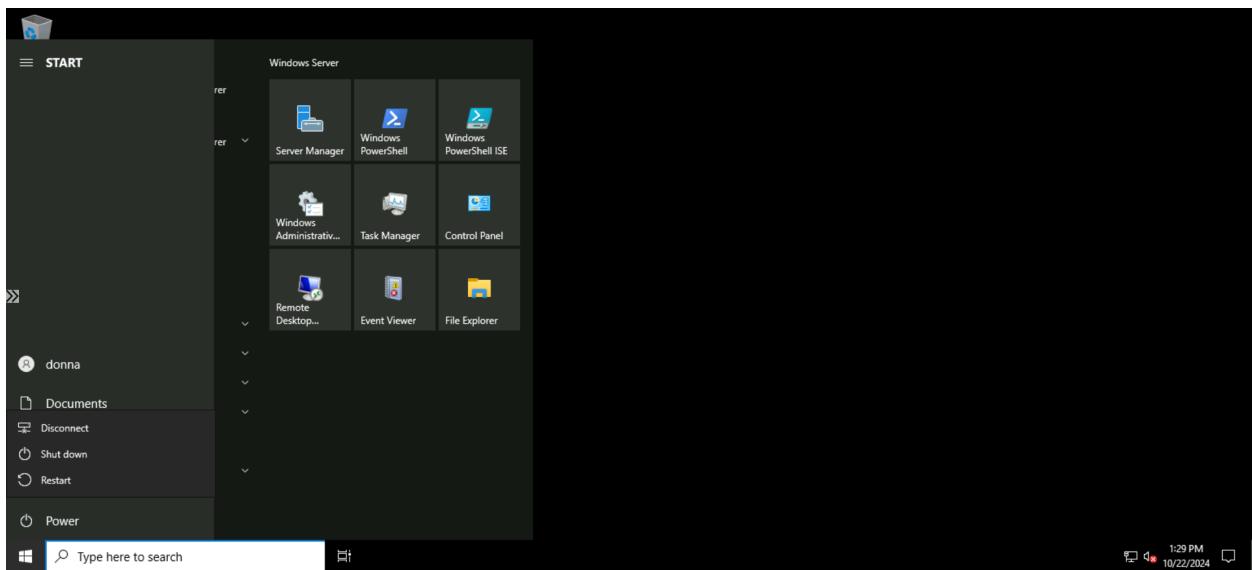
The storage account (storage1cst8912) is connected and expanded to show the container (container 8912) that was created. The connection is successful.



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 screenshot shows the Microsoft Azure Resource Groups page. The left sidebar lists 'Resource groups' with 'CST8912demo' selected. The main area shows the 'Overview' tab for 'CST8912demo'. A modal window titled 'Delete a resource group' is open, listing dependent resources: 8912-VM1 (Virtual machine), 8912-vm1229 (Network interface), 8912-VM1_OsDisk_1_9921a3be3170415c9db9 (Disk), 8912-vnet1 (Virtual network), Bastion8912 (Virtual machine), nsrg-1 (Network interface), Privateendpoint8912 (Private endpoint), Privateendpoi (Private endpoint), privatenetlink.b (Virtual machine scale set), public-ip (Public IP address), and storageaccount8912 (Storage account). A 'Delete confirmation' message states: 'Deleting this resource group and its dependent resources is a permanent action and cannot be undone.' Buttons for 'Delete' and 'Go back' are present. Below the modal, an input field asks 'Enter resource group name to confirm deletion' with 'CST8912demo' typed in.

The automatic resource group NetworkWatcherRG is deleted.

The screenshot shows the Microsoft Azure Resource Groups page. The left sidebar lists 'Resource groups' with 'NetworkWatcherRG' selected. The main area shows the 'Overview' tab for 'NetworkWatcherRG'. A modal window titled 'Delete a resource group' is open, stating: 'The following resource group and all its dependent resources will be permanently deleted.' It lists the 'Resource group to be deleted' as 'NetworkWatcherRG' and the 'Dependent resources to be deleted (1)' as 'NetworkWatcher_rg_canadacentral'. A 'Delete confirmation' message states: 'Deleting this resource group and its dependent resources is a permanent action and cannot be undone.' Buttons for 'Delete' and 'Go back' are present. Below the modal, an input field asks 'Enter resource group name to confirm deletion' with 'NetworkWatcherRG' typed in.

Both resource groups are successfully deleted.



Notifications

X

[More events in the activity log →](#)

[Dismiss all](#) ▾

✓ Deleted resource group CST8912demo X

Deleted resource group CST8912demo

a few seconds ago

✓ Deleted resource group NetworkWatcherRG X

Deleted resource group NetworkWatcherRG

7 minutes ago



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

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a search bar and a Copilot button. The main heading is "Resource groups" with a "Create" button. Below it, a message says "No resource groups to display". A sub-message explains: "Resource groups provide a logical container to manage and organize Azure resources, simplifying administration and enabling efficient resource management." There are filter options at the bottom: "Subscription equals all", "Location equals all", and "Add filter". The status bar at the bottom shows the date and time as 2024-10-22 9:40 AM.

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

The screenshot shows the Microsoft Azure All resources page. At the top, there's a search bar and a Copilot button. The main heading is "All resources" with a "Create" button. Below it, a message says "No resources match your filters". A sub-message says "Try changing or clearing your filters." with buttons for "Create resources" and "Clear filters". There are filter options at the bottom: "Name ↑", "Type ↑↓", "Resource group ↑↓", "Location ↑↓", and "Subscription ↑↓". The status bar at the bottom shows the date and time as 2024-10-22 9:40 AM.

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-a-zure-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>

