# CST8921 – Cloud Industry Trends

## Lab 2 Report

### Title

Securing Cloud Resources: Exploring Cloud Security Trends with AWS/Azure/GCP.

### Introduction

In this lab, we delve into crucial aspects of cloud security, focusing on data protection and asset security. Using AWS, Azure, or GCP, participants learn to implement security policies, service endpoints, and network configurations to safeguard cloud resources and prevent unauthorized access, fostering a comprehensive understanding of cloud security concepts.

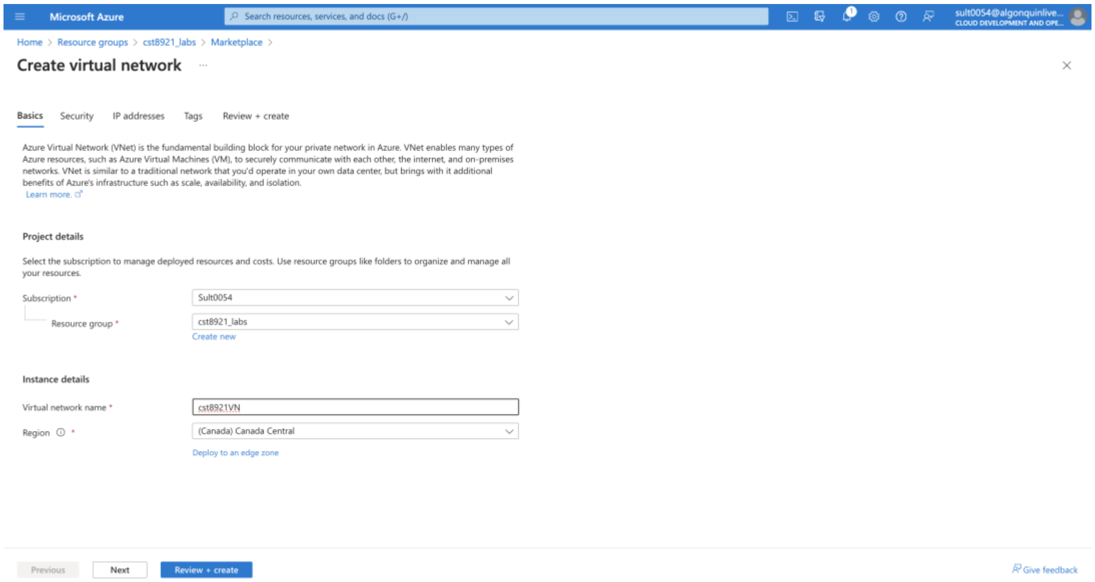
### Steps

Step 1: Create an Allowed Locations Policy

- Set up an Allowed Locations policy to ensure resources are only created in a specific region.

Step 2: Service Endpoints and Securing Storage

- Task 1: Create a virtual network in the Canada Central region.



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home > Resource groups > cst8921_labs > Marketplace >
Basics
Security
IP addresses
Tags
Review + create
Previous
Next
Review + create
Give feedback

Create virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Sult0054

Resource group *: cst8921_labs

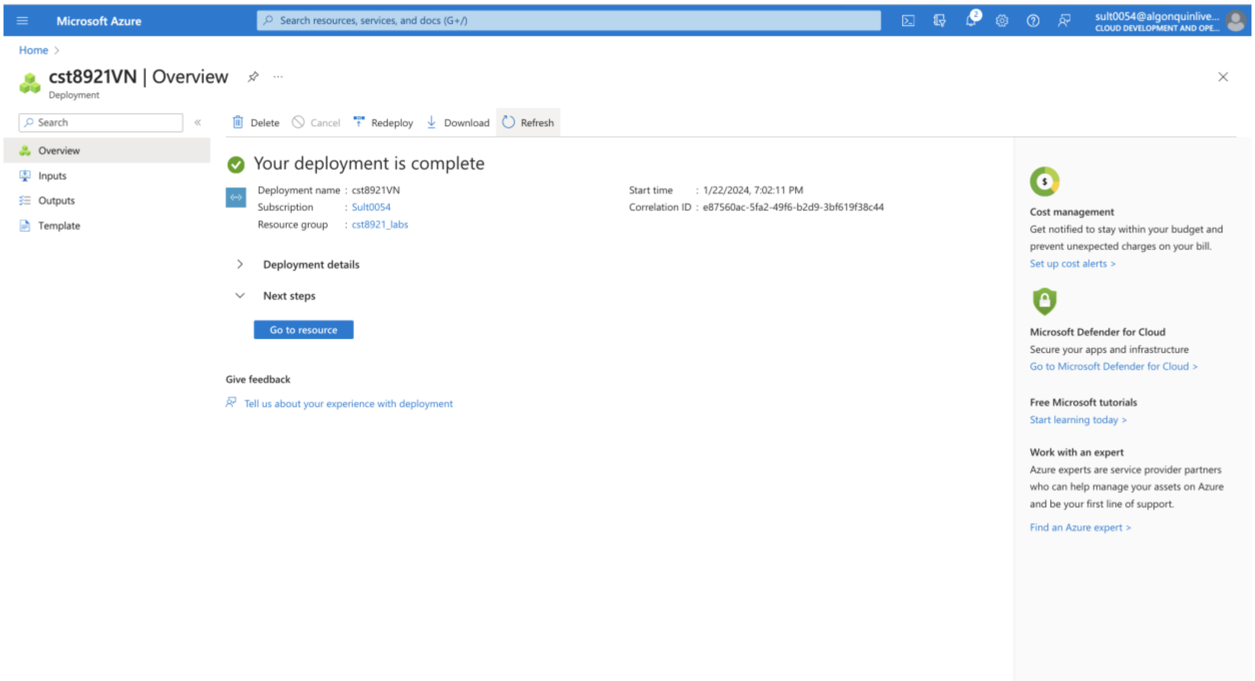
Create new

Instance details

Virtual network name *: cst8921VN

Region *: (Canada) Canada Central

Deploy to an edge zone



cst8921VN | Overview
Deployment

Your deployment is complete

Deployment name : cst8921VN
Subscription : Sult0054
Resource group : cst8921_labs

Start time : 1/22/2024, 7:02:11 PM
Correlation ID : e87560ac-5fa2-49f6-b2d9-3bf619f38c44

> Deployment details

∨ Next steps

Give feedback

Tell us about your experience with deployment

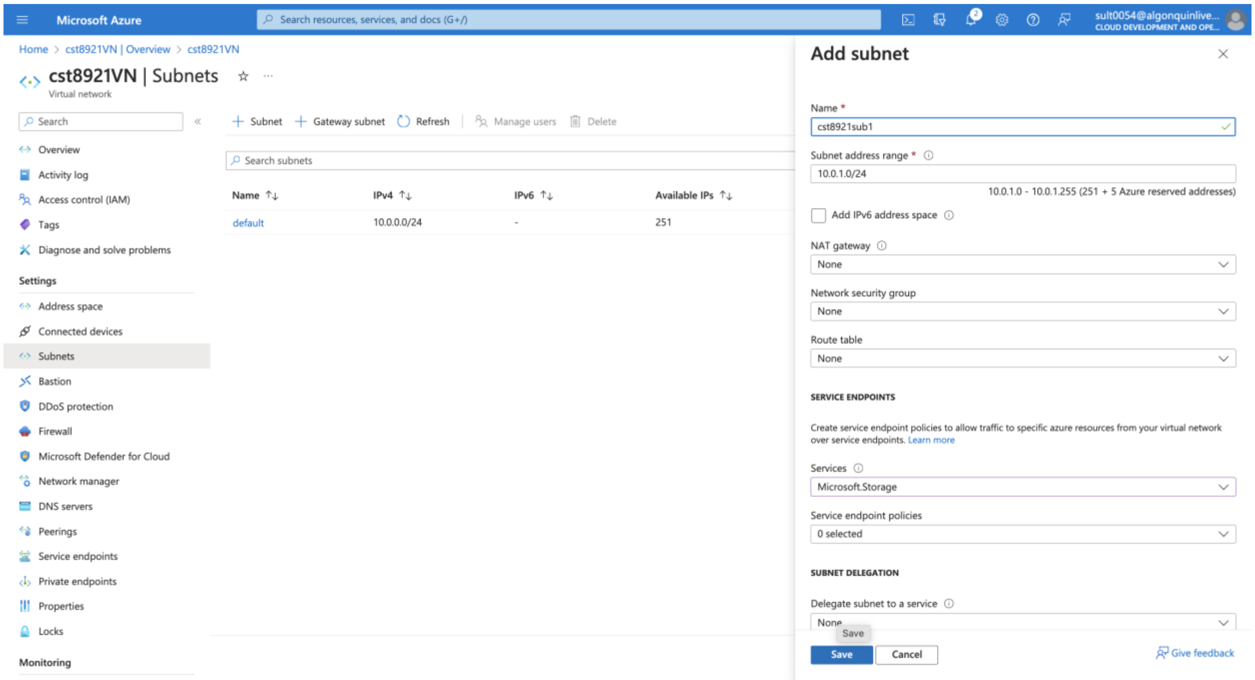
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

- Task 2: Add a subnet to the virtual network and configure a storage endpoint.
  - Enable service endpoint, create a subnet, and select Microsoft Storage as a service endpoint.



cst8921VN | Subnets
Virtual network

| Name ↑↓ | IPv4 ↑↓ | IPv6 ↑↓ | Available IPs ↑↓ |
|---|---|---|---|
| default | 10.0.0.0/24 | - | 251 |

Add subnet

Name *
cst8921sub1

Subnet address range *
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway
None

Network security group
None

Route table
None

SERVICE ENDPOINTS

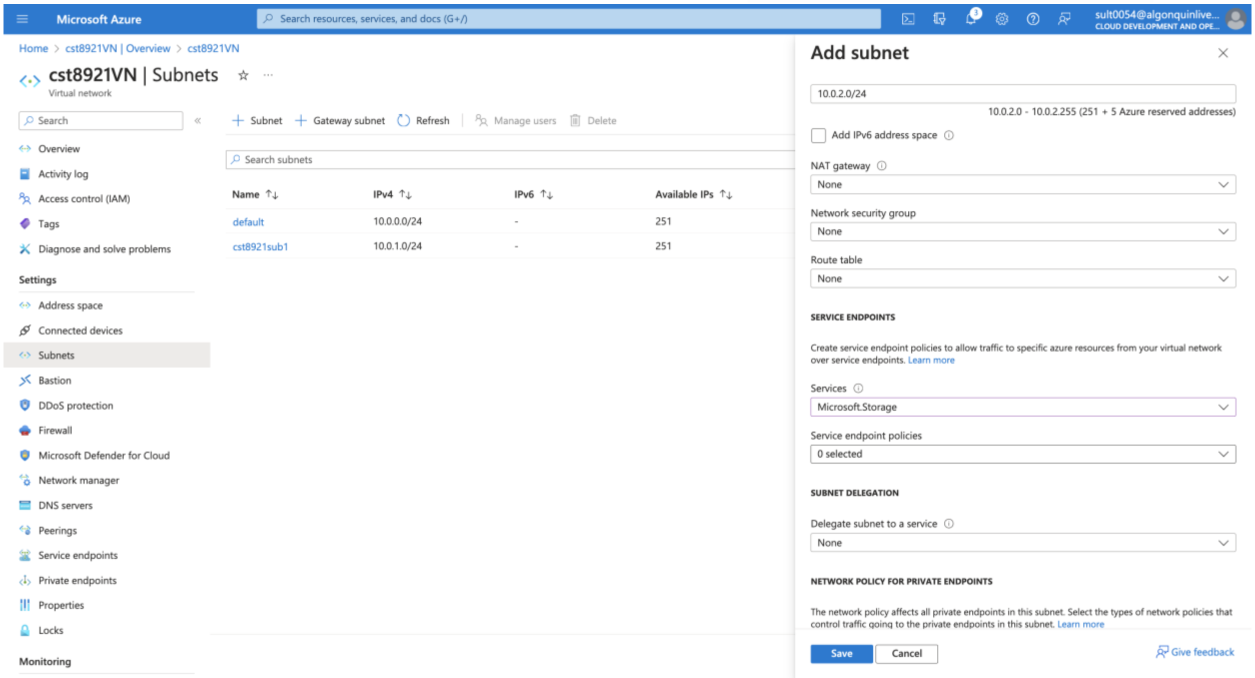
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services
Microsoft.Storage

Service endpoint policies
0 selected

SUBNET DELEGATION

Delegate subnet to a service
None



Home > cst8921VN | Overview > cst8921VN

cst8921VN | Subnets

Virtual network

+ Subnet + Gateway subnet Refresh Manage users Delete

| Name | IPv4 | IPv6 | Available IPs |
|---|---|---|---|
| default | 10.0.0.0/24 | - | 251 |
| cst8921sub1 | 10.0.1.0/24 | - | 251 |

**Add subnet**

10.0.2.0/24

10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway: None

Network security group: None

Route table: None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services: Microsoft.Storage

Service endpoint policies: 0 selected

SUBNET DELEGATION

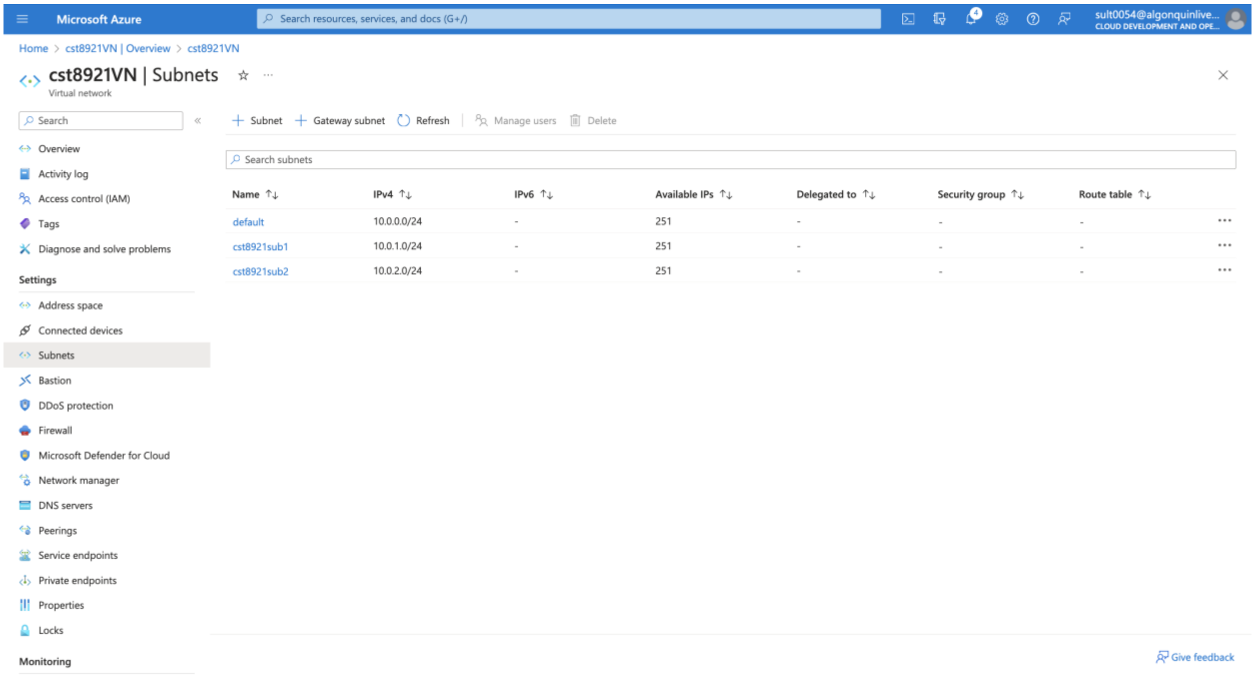
Delegate subnet to a service: None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. Select the types of network policies that control traffic going to the private endpoints in this subnet. Learn more

Save Cancel

- Configure two subnets.



Home > cst8921VN | Overview > cst8921VN

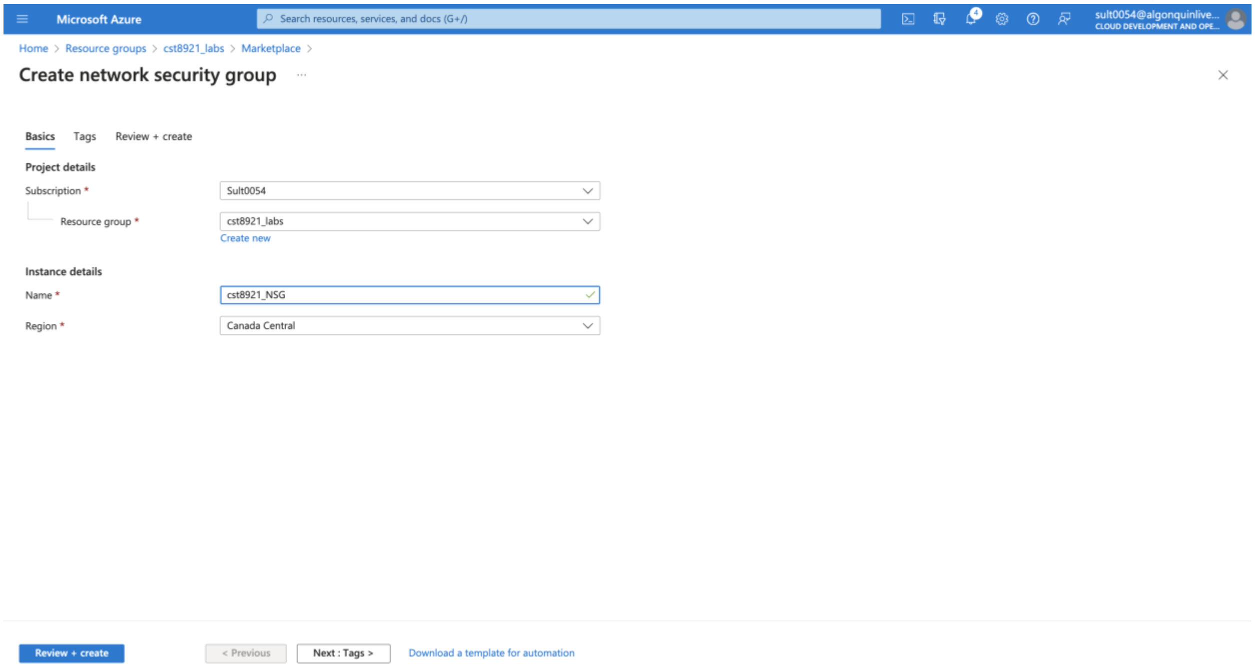
cst8921VN | Subnets

Virtual network

+ Subnet + Gateway subnet Refresh Manage users Delete

| Name | IPv4 | IPv6 | Available IPs | Delegated to | Security group | Route table |
|---|---|---|---|---|---|---|
| default | 10.0.0.0/24 | - | 251 | - | - | - |
| cst8921sub1 | 10.0.1.0/24 | - | 251 | - | - | - |
| cst8921sub2 | 10.0.2.0/24 | - | 251 | - | - | - |

- Task 3: Configure a network security group to restrict access to the subnet.
  - Create an NSG in Canada Central Region.



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home > Resource groups > cst8921_labs > Marketplace >

Create network security group

Basics | Tags | Review + create

**Project details**

Subscription *: Sult0054

Resource group *: cst8921_labs

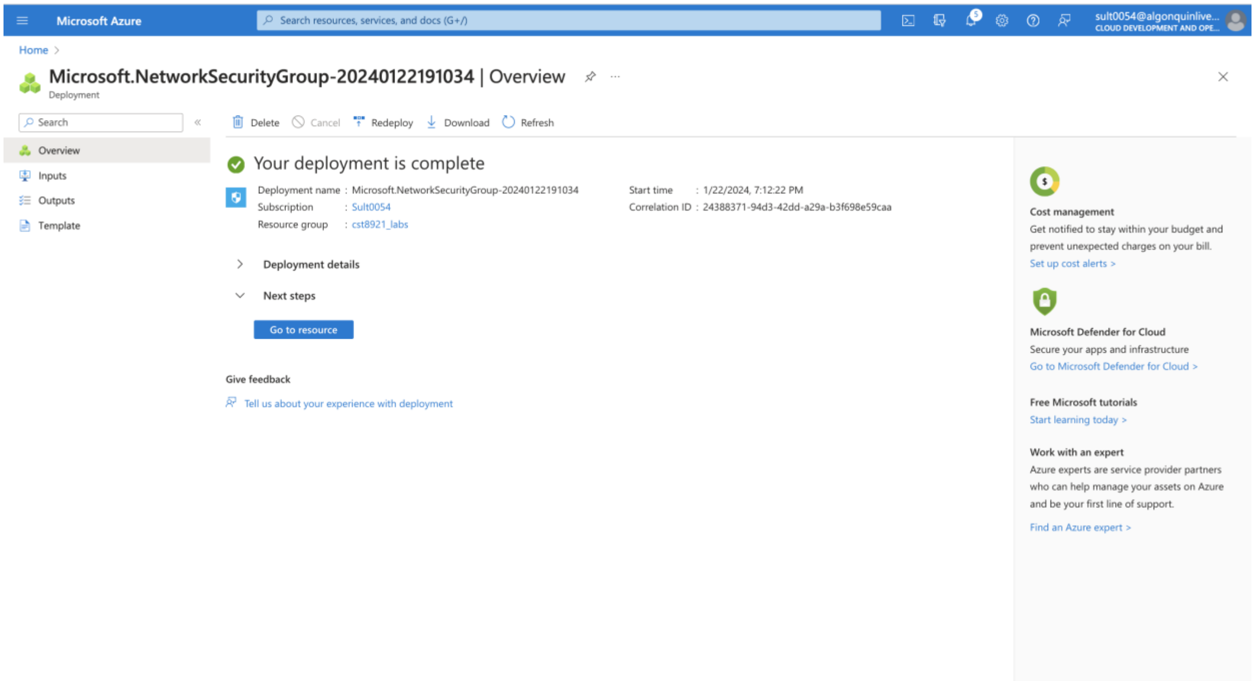
Create new

**Instance details**

Name *: cst8921_NSG

Region *: Canada Central

Review + create
< Previous
Next : Tags >
Download a template for automation



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home >
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Microsoft.NetworkSecurityGroup-20240122191034 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20240122191034
Subscription : Sult0054
Resource group : cst8921_labs

Start time : 1/22/2024, 7:12:22 PM
Correlation ID : 24388371-94d3-42dd-a29a-b3f698e59caa

> Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

**Cost management**

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

**Microsoft Defender for Cloud**

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

**Free Microsoft tutorials**

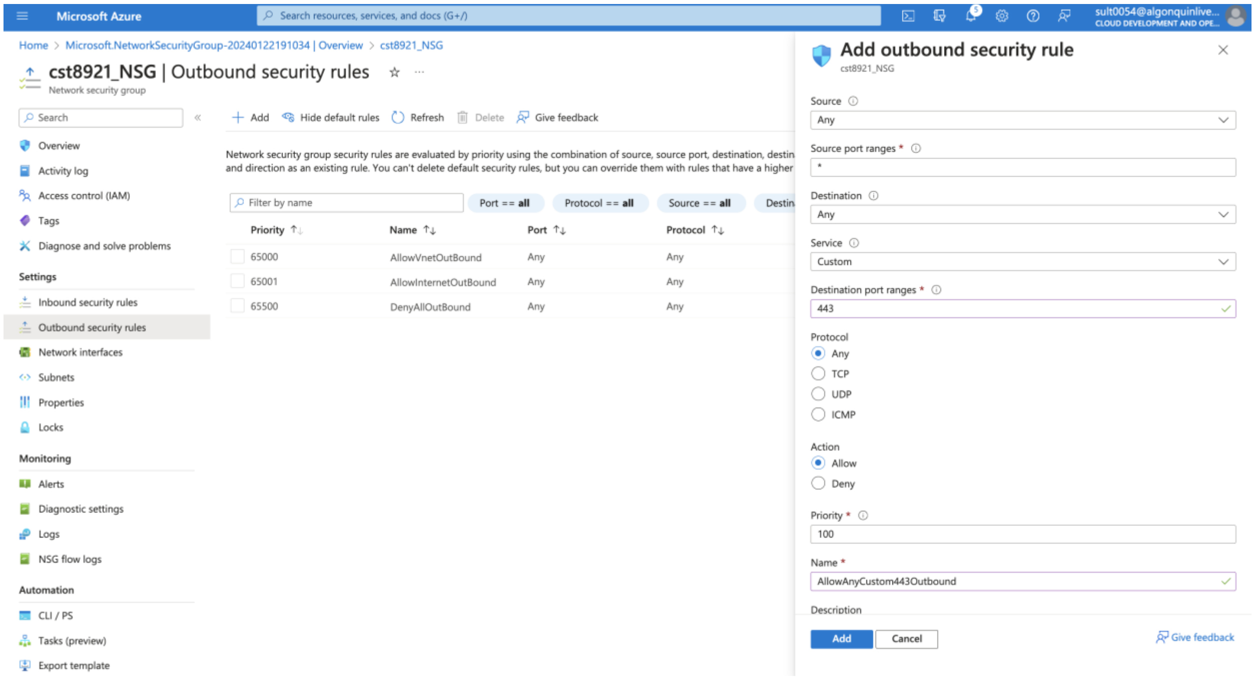
Start learning today >

**Work with an expert**

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Find an Azure expert >

- Create a rule allowing outbound communication to Azure Storage service.



Network security group security rules are evaluated by priority using the combination of source, source port, destination, destin and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher

| Priority | Name | Port | Protocol |
|---|---|---|---|
| 65000 | AllowVnetOutBound | Any | Any |
| 65001 | AllowInternetOutBound | Any | Any |
| 65500 | DenyAllOutBound | Any | Any |

**Add outbound security rule**
cst8921_NSG

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 443

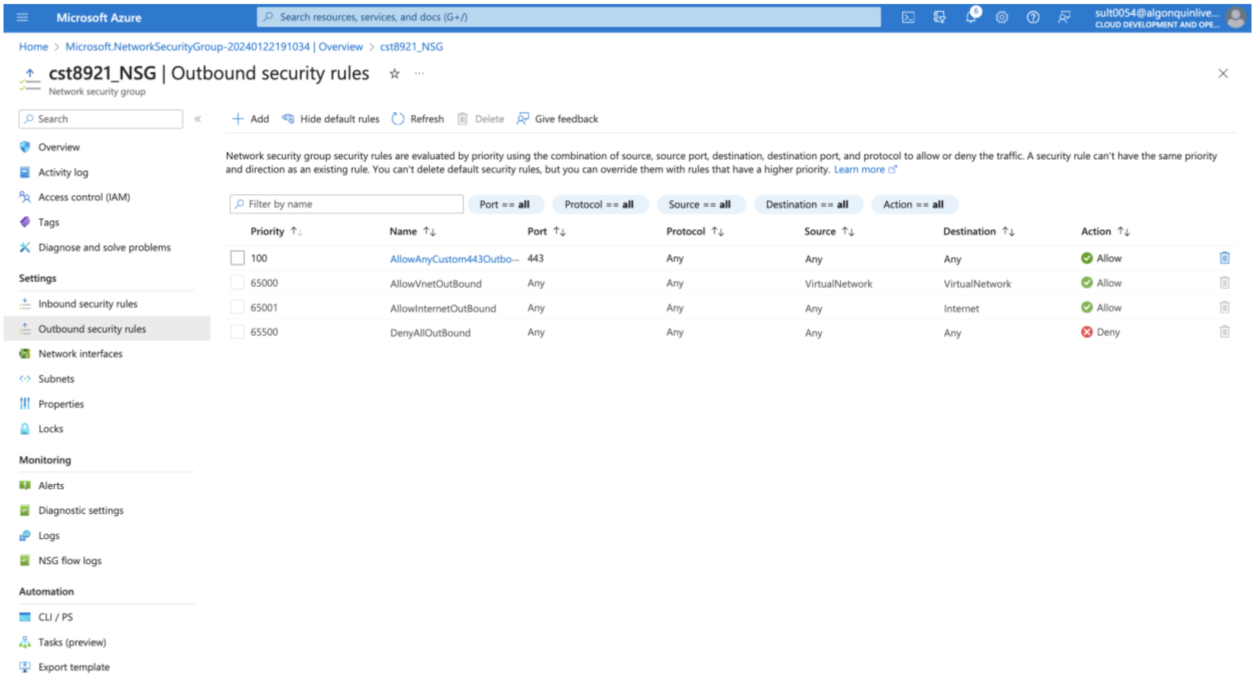
Protocol
● Any
○ TCP
○ UDP
○ ICMP

Action
● Allow
○ Deny

Priority *: 100

Name *: AllowAnyCustom443Outbound

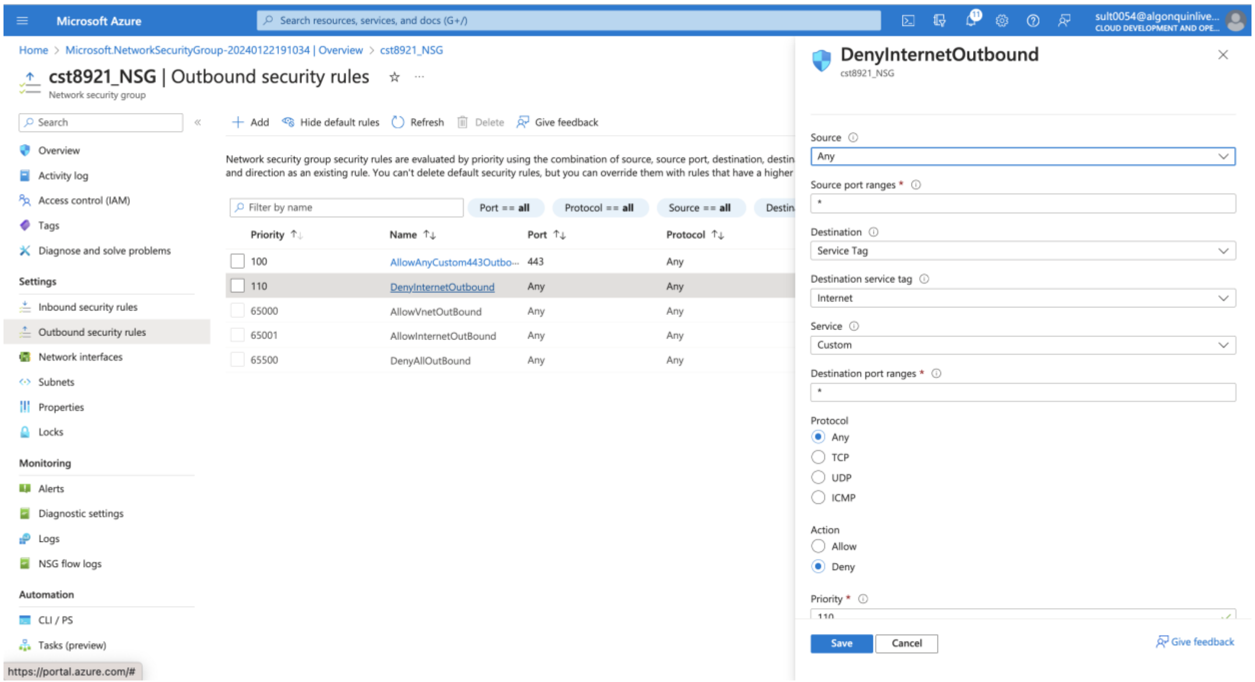
Description



Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 100 | AllowAnyCustom443Outbo... | 443 | Any | Any | Any | ✓ Allow |
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | ✓ Allow |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet | ✓ Allow |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | ✗ Deny |

- Task 4: Configure a network security group to allow RDP on the public subnet.
    - Create outbound security rules and inbound rules for RDP.



cst8921_NSG | Outbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destin
and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher

| Priority | Name | Port | Protocol |
|---|---|---|---|
| 100 | AllowAnyCustom443Outbo... | 443 | Any |
| 110 | DenyInternetOutbound | Any | Any |
| 65000 | AllowVnetOutBound | Any | Any |
| 65001 | AllowInternetOutBound | Any | Any |
| 65500 | DenyAllOutBound | Any | Any |

DenyInternetOutbound

cst8921_NSG

Source: Any

Source port ranges *: *

Destination: Service Tag

Destination service tag: Internet

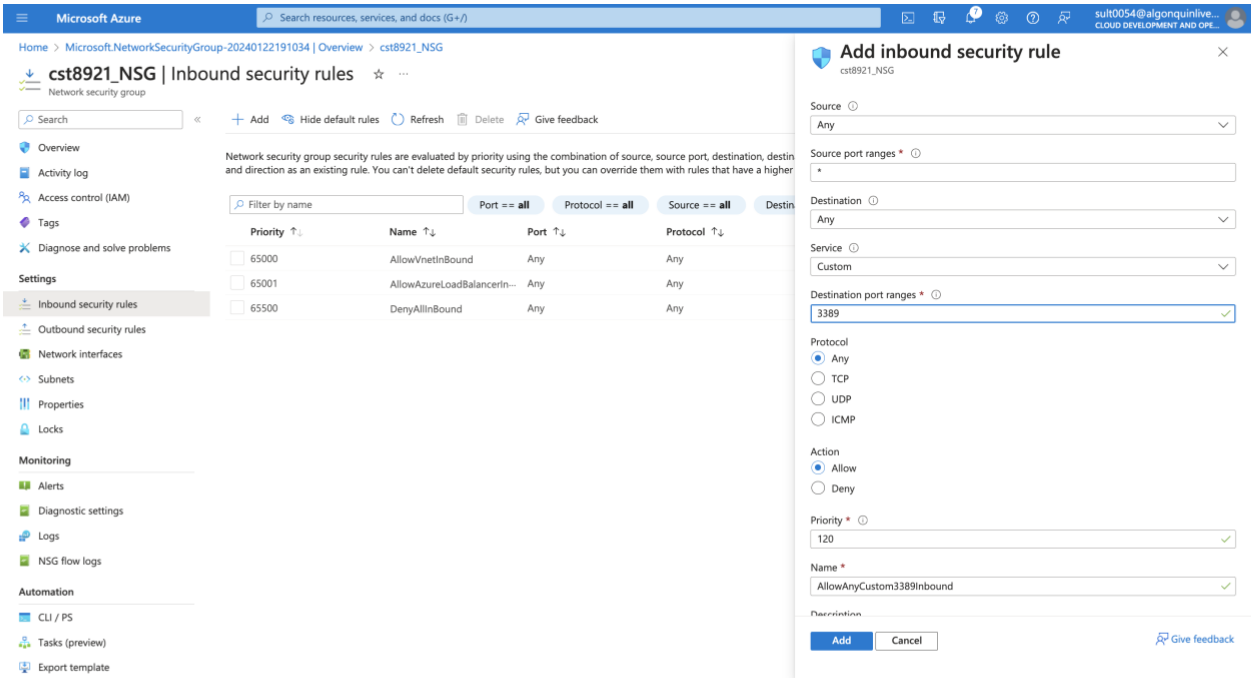
Service: Custom

Destination port ranges *: *

Protocol
● Any
○ TCP
○ UDP
○ ICMP

Action
○ Allow
● Deny

Priority *: 110



cst8921_NSG | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destin
and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher

| Priority | Name | Port | Protocol |
|---|---|---|---|
| 65000 | AllowVnetInBound | Any | Any |
| 65001 | AllowAzureLoadBalancerIn... | Any | Any |
| 65500 | DenyAllInBound | Any | Any |

Add inbound security rule

cst8921_NSG

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 3389

Protocol
● Any
○ TCP
○ UDP
○ ICMP

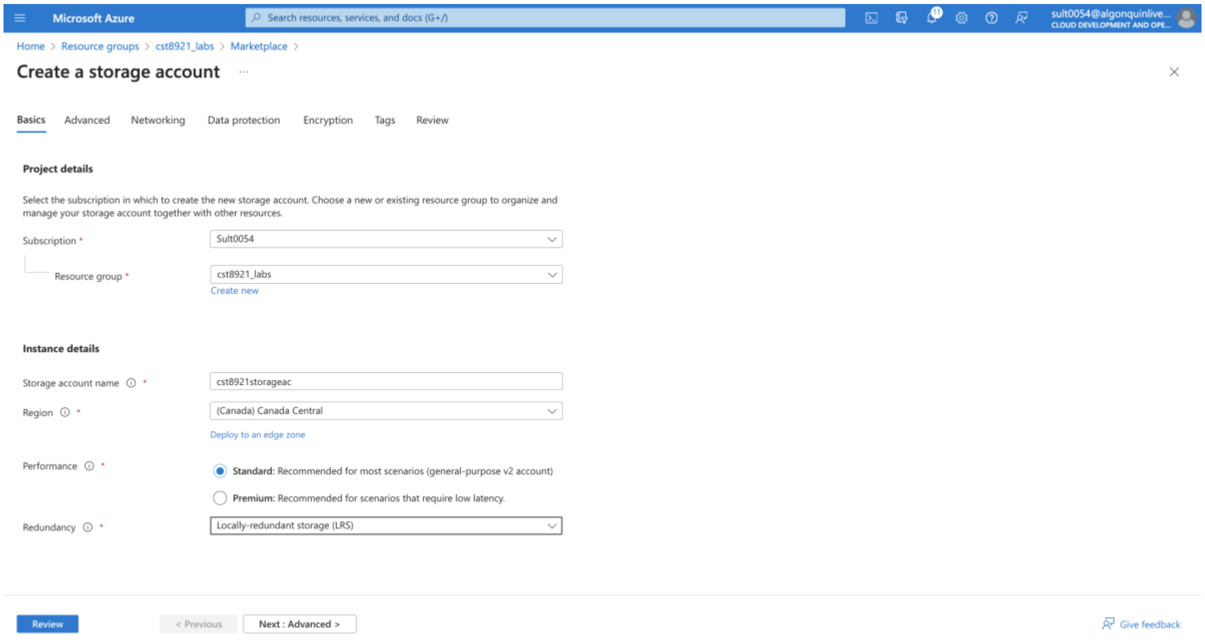
Action
● Allow
○ Deny

Priority *: 120

Name *: AllowAnyCustom3389Inbound

Description

- Task 5: Create a storage account with a file share.


Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home > Resource groups > cst8921_labs > Marketplace >

Create a storage account

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review

**Project details**

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

Subscription * : Sult0054

Resource group * : cst8921_labs

**Instance details**

Storage account name * : cst8921storageac

Region * : (Canada) Canada Central

Performance * :

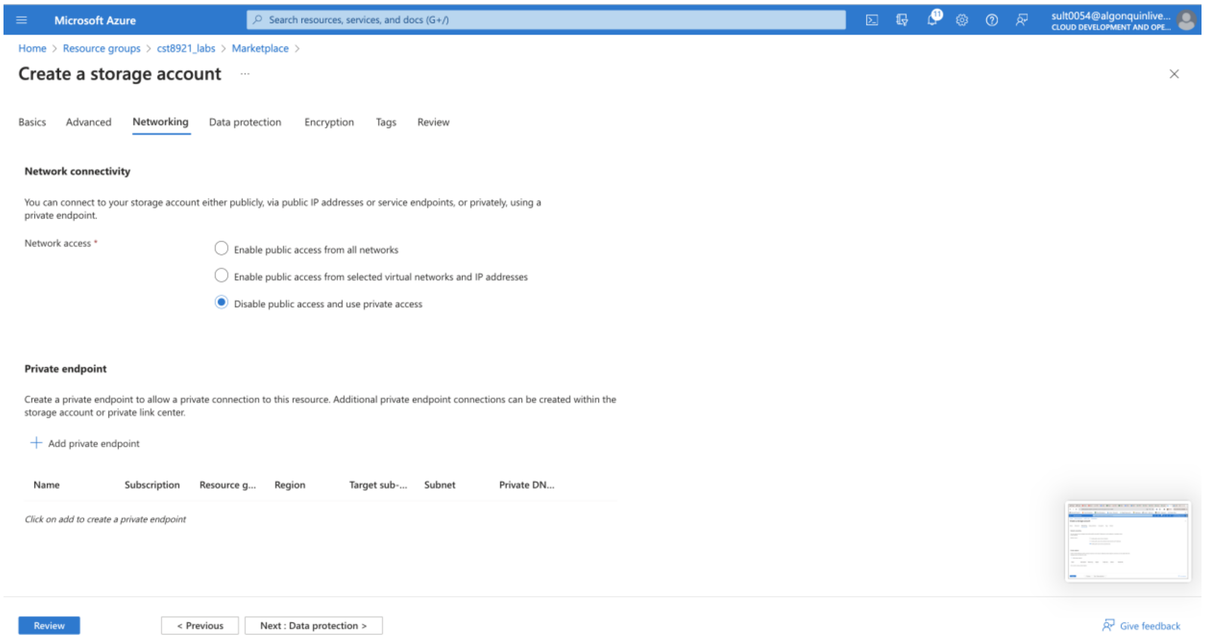
● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy * : Locally-redundant storage (LRS)

AhmadSultan_041034155

Deny network access from the internet, except for the private subnet.



Create a storage account

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

**Network connectivity**

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

○ Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

● Disable public access and use private access

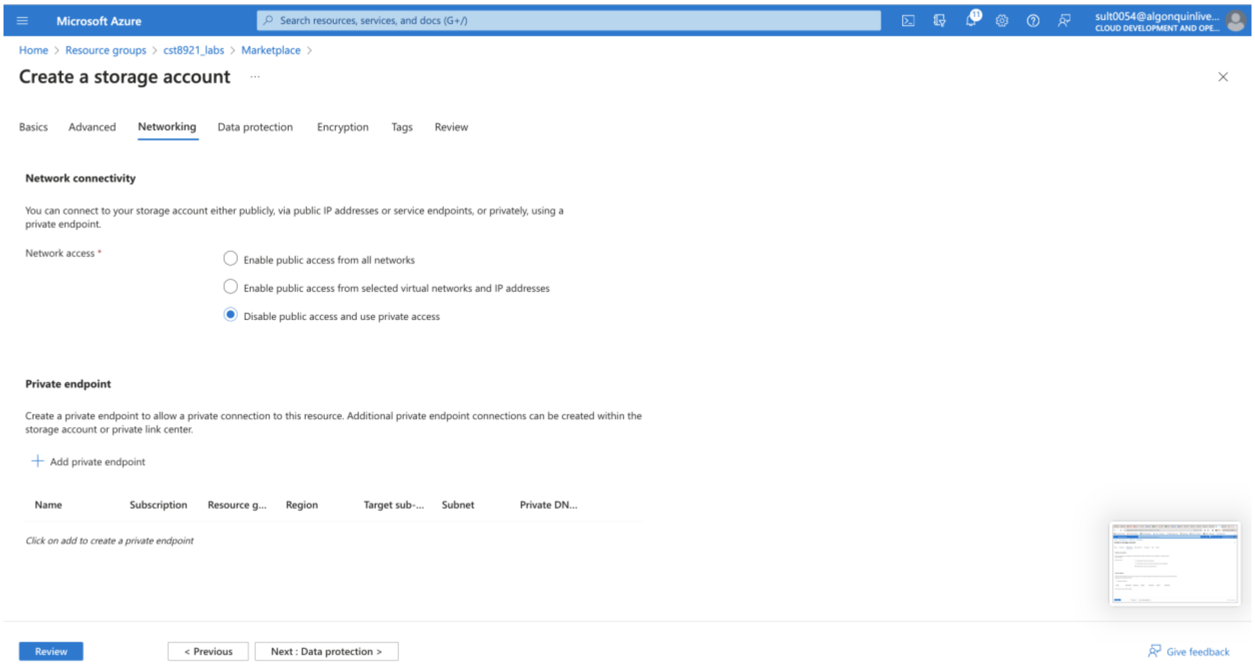
**Private endpoint**

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

+ Add private endpoint

| Name | Subscription | Resource g... | Region | Target sub-... | Subnet | Private DN... |
|---|---|---|---|---|---|---|

*Click on add to create a private endpoint*



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home > Resource groups > cst8921_labs > Marketplace >

Create a storage account

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

**Network connectivity**

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

○ Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

● Disable public access and use private access

**Private endpoint**

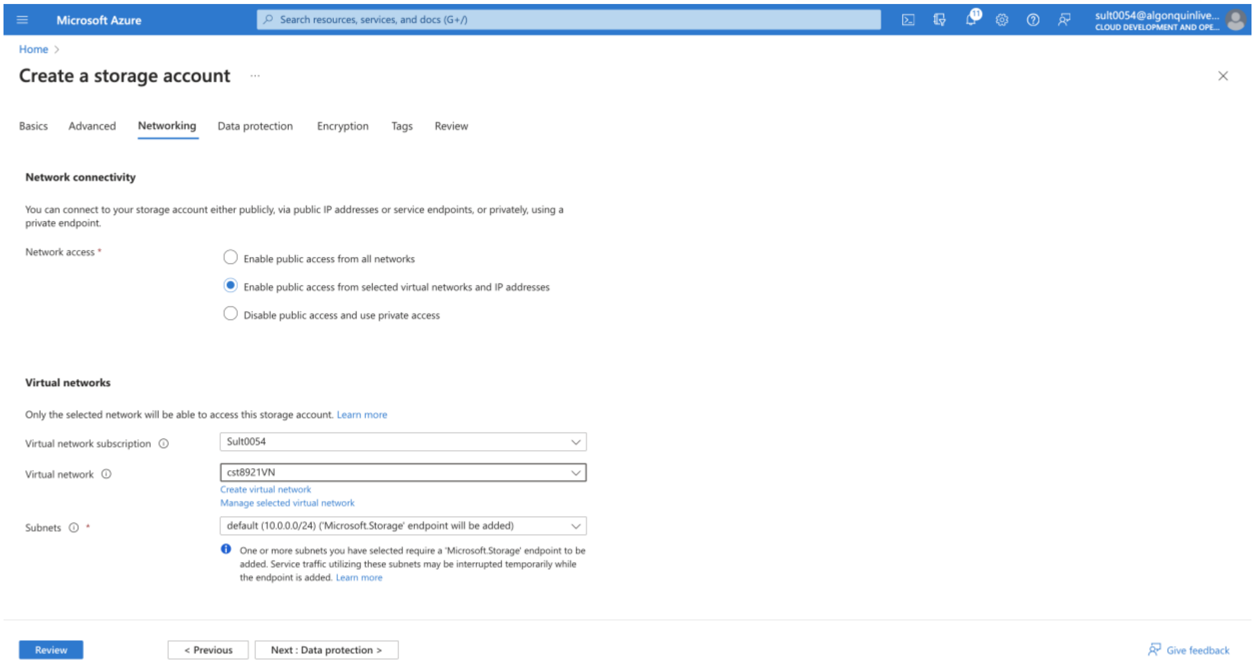
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

+ Add private endpoint

Name | Subscription | Resource g... | Region | Target sub-... | Subnet | Private DN...

*Click on add to create a private endpoint*

Review
< Previous
Next : Data protection >
Give feedback



## Create a storage account

**Network connectivity**

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

○ Enable public access from all networks

● Enable public access from selected virtual networks and IP addresses

○ Disable public access and use private access

**Virtual networks**

Only the selected network will be able to access this storage account. Learn more

Virtual network subscription: Sult0054

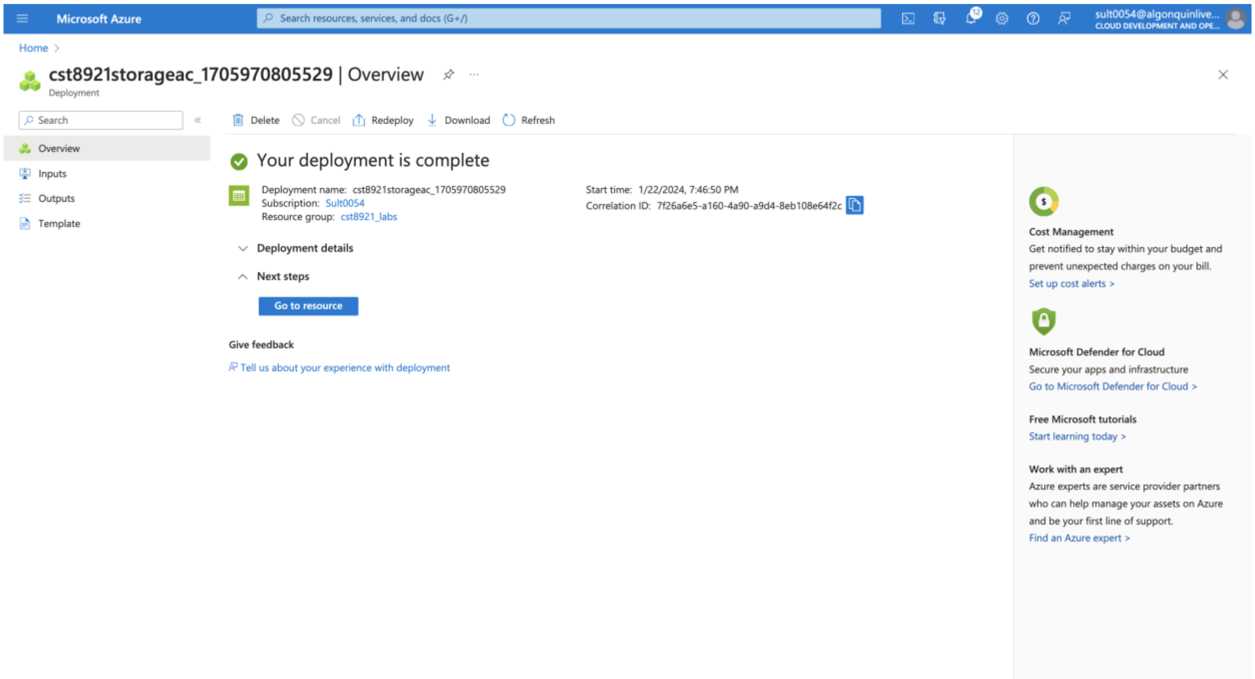
Virtual network: cst8921VN

Create virtual network

Manage selected virtual network

Subnets *: default (10.0.0.0/24) ('Microsoft.Storage' endpoint will be added)

One or more subnets you have selected require a 'Microsoft.Storage' endpoint to be added. Service traffic utilizing these subnets may be interrupted temporarily while the endpoint is added. Learn more



## cst8921storageac_1705970805529 | Overview

### Your deployment is complete

Deployment name: cst8921storageac_1705970805529

Subscription: Sult0054

Resource group: cst8921_labs

Start time: 1/22/2024, 7:46:50 PM

Correlation ID: 7f26a6e5-a160-4a90-a9d4-8eb108e64f2c

Deployment details

Next steps

**Give feedback**

Tell us about your experience with deployment

**Cost Management**

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

**Microsoft Defender for Cloud**

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

**Free Microsoft tutorials**

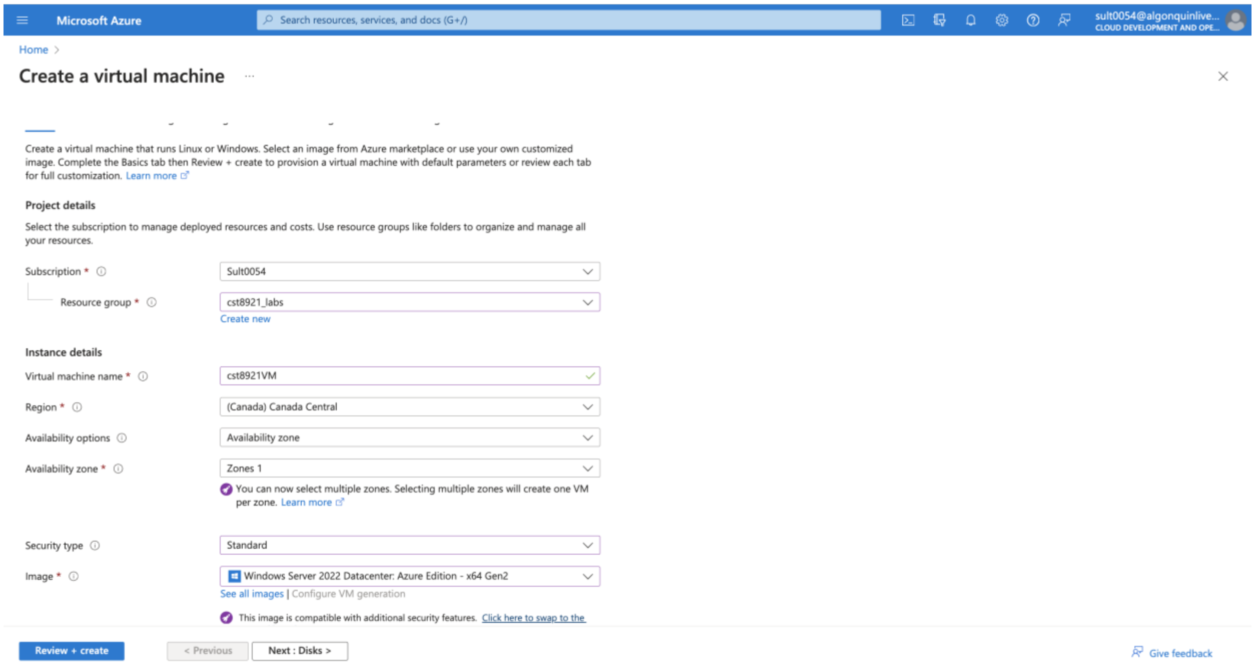
Start learning today >

**Work with an expert**

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Find an Azure expert >

- Task 6: Deploy virtual machines into the designated subnets.



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home >

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Sult0054

Resource group *: cst8921_labs

Create new

**Instance details**

Virtual machine name *: cst8921VM

Region *: (Canada) Canada Central

Availability options: Availability zone

Availability zone *: Zones 1

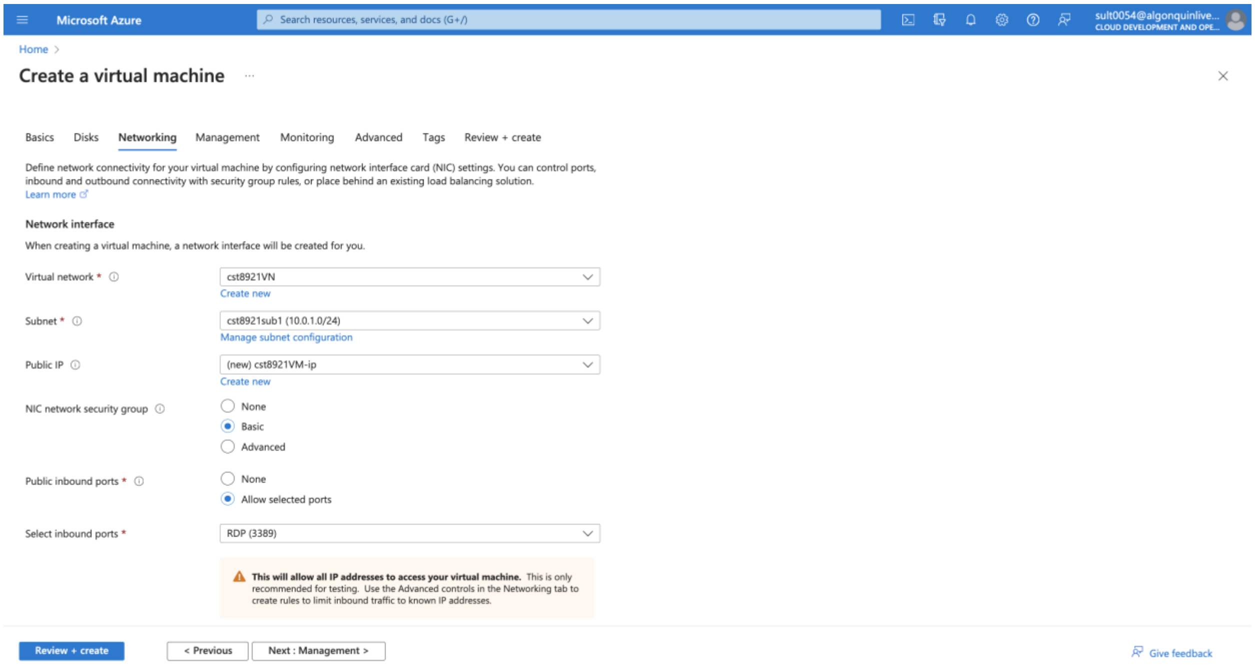
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type: Standard

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

See all images | Configure VM generation

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



Microsoft Azure
Search resources, services, and docs (G+/)
sult0054@algonquinlive...
CLOUD DEVELOPMENT AND OPE...
Home >

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

**Network interface**

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

Virtual network *: cst8921VN

Create new

Subnet *: cst8921sub1 (10.0.1.0/24)

Manage subnet configuration

Public IP: (new) cst8921VM-ip

Create new

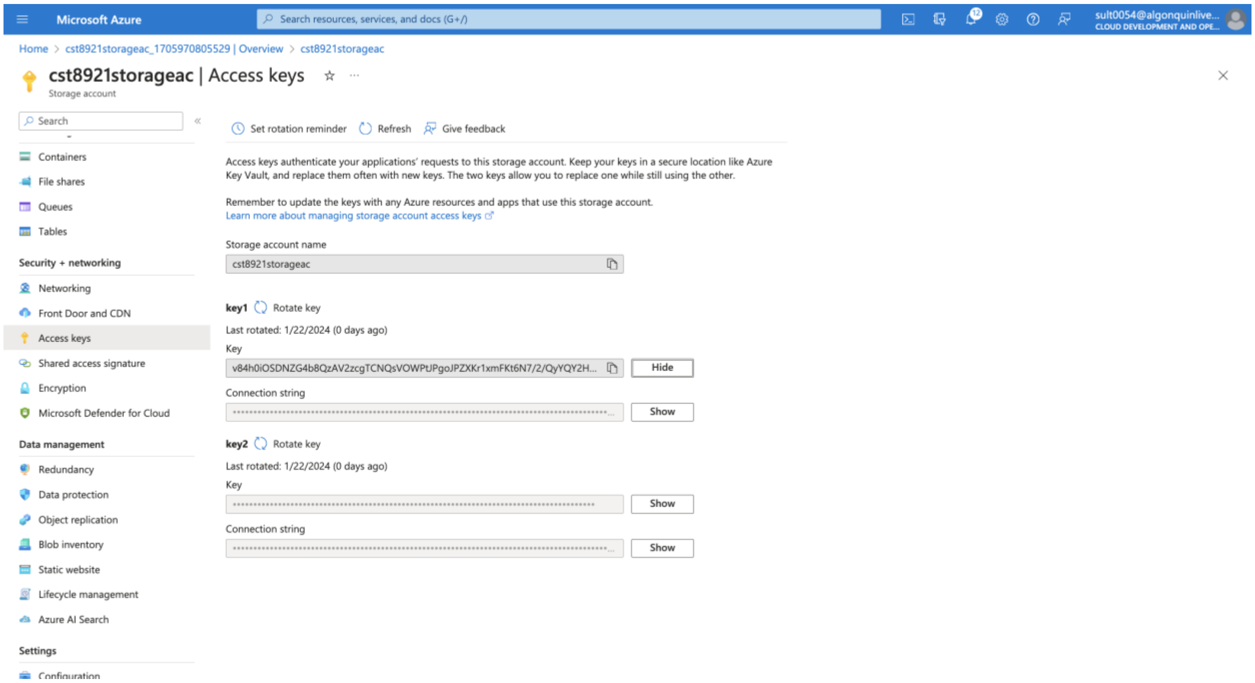
NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: RDP (3389)

**This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

- Task 7: Test the storage connection from the private subnet.



cst8921storageac | Access keys
Storage account

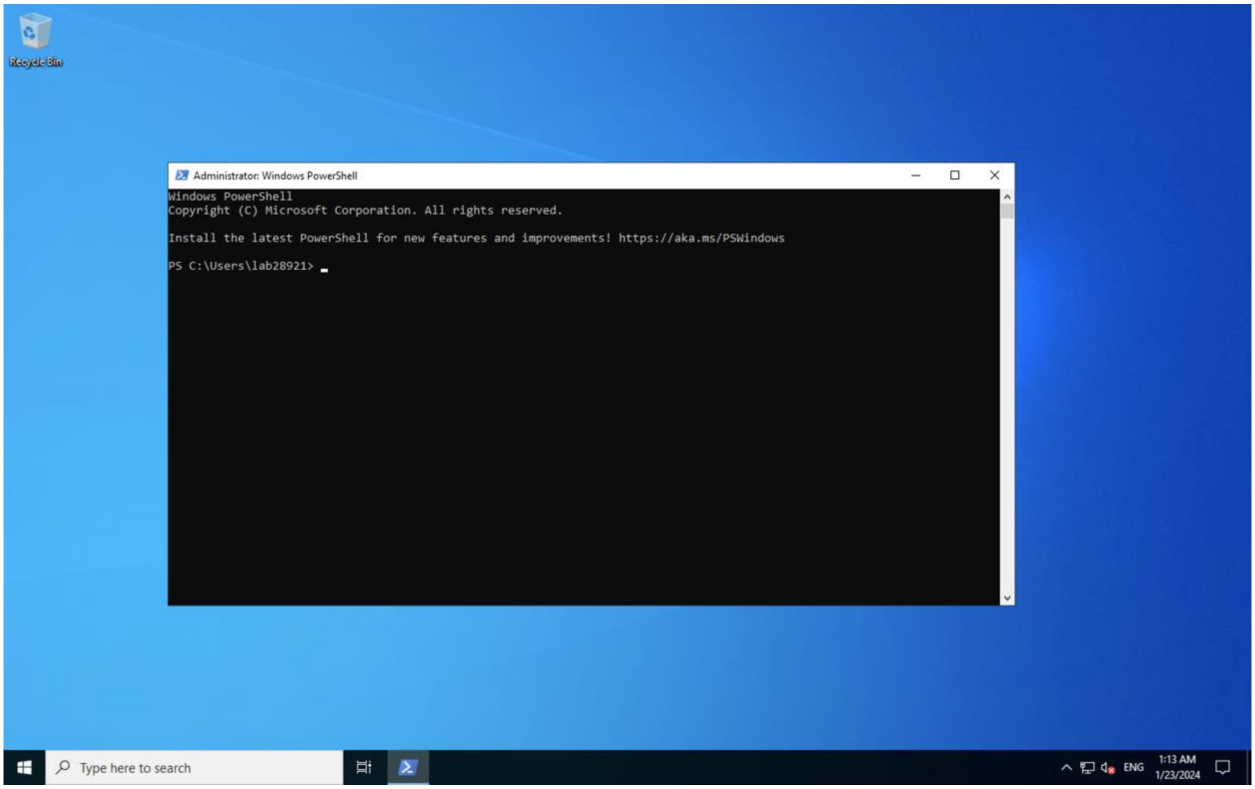
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys

Storage account name: cst8921storageac

**key1**
Last rotated: 1/22/2024 (0 days ago)
Key: v84h0iOSDNZG4b8QzAV2zcgTCNQsVOWPtJPgoJPZXKr1xmFKt6N7/2/QyYQY2H...
Connection string: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••...

**key2**
Last rotated: 1/22/2024 (0 days ago)
Key: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
Connection string: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••...



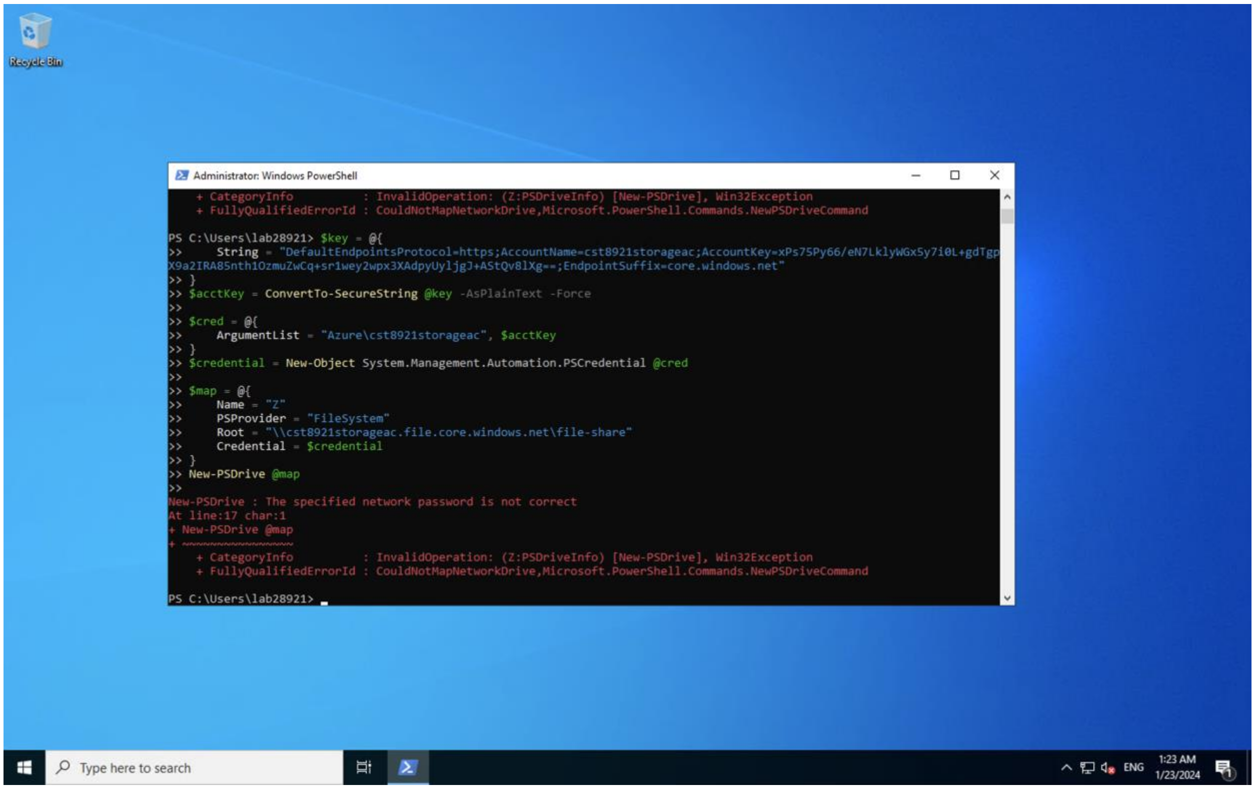
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\lab28921> _
```

## Step 3: Test the Storage Connection from the Public Subnet

- Task 8: Attempt to map the drive to the file share in the storage account from the public subnet to confirm access denial.



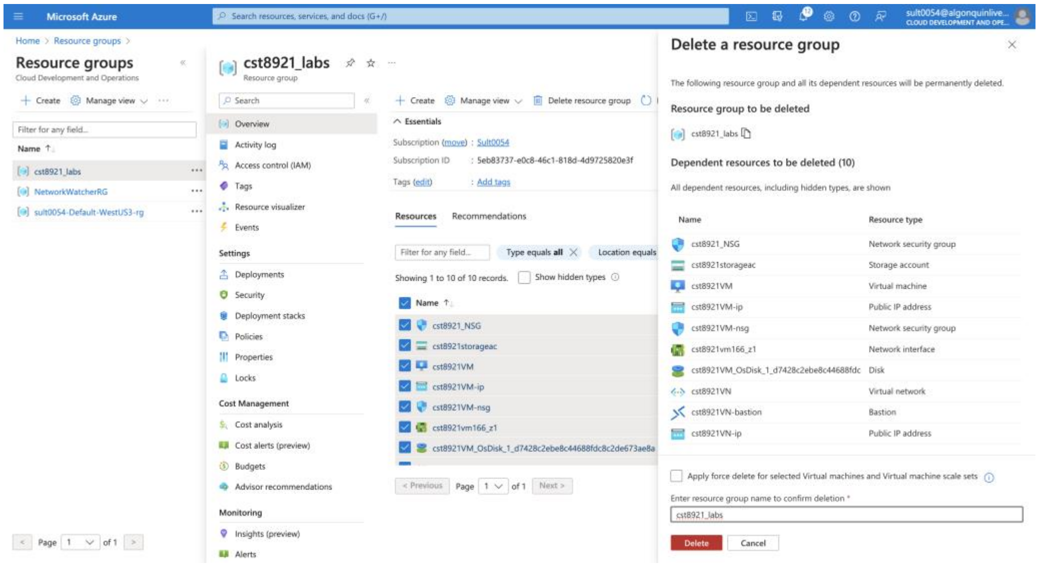
Administrator: Windows PowerShell

```
    + CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exception
    + FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDriveCommand

PS C:\Users\lab28921> $key = @{
>>     String = "DefaultEndpointsProtocol=https;AccountName=cst8921storageac;AccountKey=xPs75Py66/eN7LklyWGx5y7i0L+gdTgp
X9a2IRA85nth1OzmuZwCq+sr1wey2wpx3XAdpyUyljgJ+AStQv8lXg==;EndpointSuffix=core.windows.net"
>> }
>> $acctKey = ConvertTo-SecureString @key -AsPlainText -Force
>>
>> $cred = @{
>>     ArgumentList = "Azure\cst8921storageac", $acctKey
>> }
>> $credential = New-Object System.Management.Automation.PSCredential @cred
>>
>> $map = @{
>>     Name = "Z"
>>     PSProvider = "FileSystem"
>>     Root = "\\cst8921storageac.file.core.windows.net\file-share"
>>     Credential = $credential
>> }
>> New-PSDrive @map
>>
New-PSDrive : The specified network password is not correct
At line:17 char:1
+ New-PSDrive @map
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exception
    + FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDriveCommand

PS C:\Users\lab28921> _
```

Deleting all the resources



Subscription (move) : Sult0054
Subscription ID : 5eb83737-e0c8-46c1-818d-4d9725820e3f
Tags (edit) : Add tags

Showing 1 to 10 of 10 records.

☑ Name ↑
☑ cst8921_NSG
☑ cst8921storageac
☑ cst8921VM
☑ cst8921VM-ip
☑ cst8921VM-nsg
☑ cst8921vm166_z1
☑ cst8921VM_OsDisk_1_d7428c2ebe8c44688fdc8c2de673ae8a

**Delete a resource group**

The following resource group and all its dependent resources will be permanently deleted.

**Resource group to be deleted**

cst8921_labs

**Dependent resources to be deleted (10)**

All dependent resources, including hidden types, are shown

| Name | Resource type |
|---|---|
| cst8921_NSG | Network security group |
| cst8921storageac | Storage account |
| cst8921VM | Virtual machine |
| cst8921VM-ip | Public IP address |
| cst8921VM-nsg | Network security group |
| cst8921vm166_z1 | Network interface |
| cst8921VM_OsDisk_1_d7428c2ebe8c44688fdc | Disk |
| cst8921VN | Virtual network |
| cst8921VN-bastion | Bastion |
| cst8921VN-ip | Public IP address |

☐ Apply force delete for selected Virtual machines and Virtual machine scale sets

Enter resource group name to confirm deletion *
cst8921_labs

Delete Cancel

## Results

Participants successfully implemented cloud security measures, creating policies, configuring service endpoints, and securing storage access. By deploying virtual machines and testing storage connections from specific subnets, the lab provides hands-on experience in ensuring authorized access and preventing unauthorized attempts. The documentation and screenshots in the lab report showcase a thorough understanding of cloud security concepts.