**CST8921 – Cloud Industry Trends**

**Lab 2 – Cloud Security trends**

## Introduction

In this lab, I explore and understand cloud security as it pertains to networking, VMs and plays an important role to protect data and business content, such as credit information and customer information from being accessed by an outside network. The idea is to secure different subnets and allow access only to authorized users using a privatized network. That way, developers have a method to access cloud applications without security risks from the public. Policies are also placed to prevent unauthorized usage of the cloud such as creating a resource outside of an intended location. This allows peace of mind so that developers can work on their cloud applications without incurring higher unintended costs.

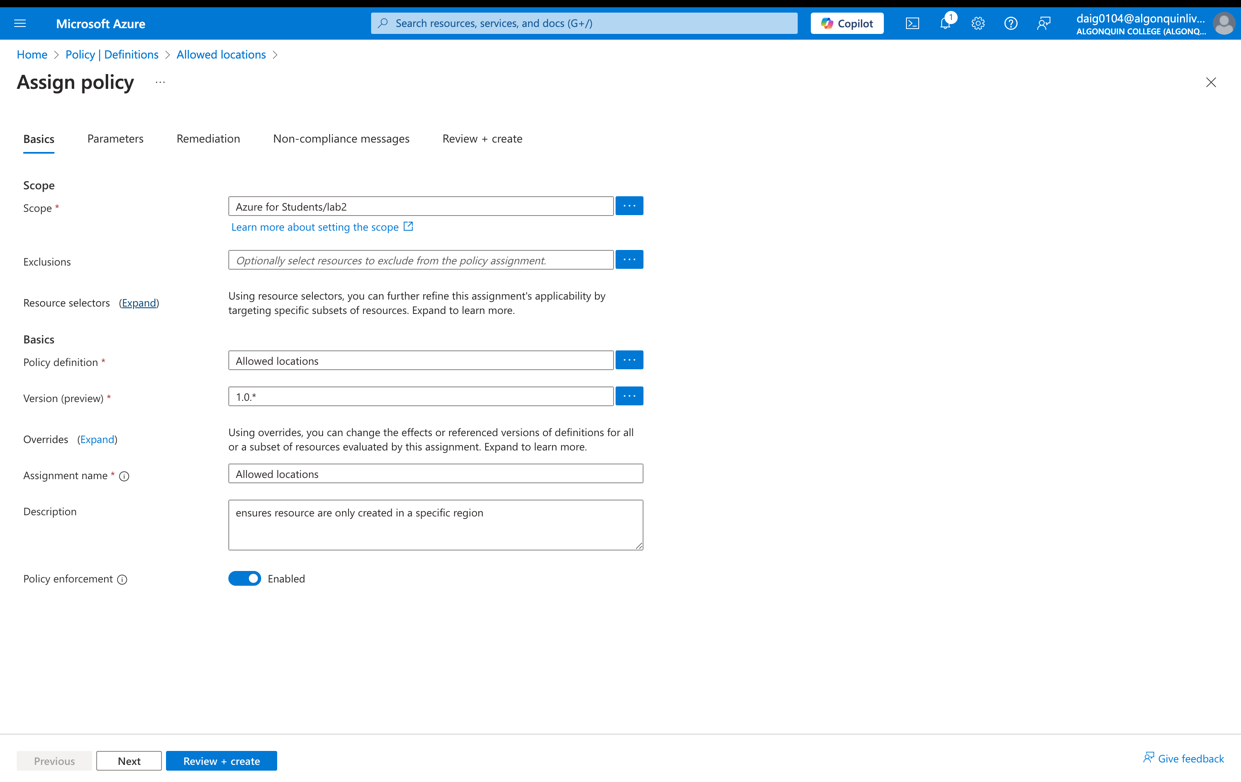
## Objective

The goal of this lab activity is to recognize and put in place cloud a cloud policy that prevents unintended creation of resources. Then, create a virtual network with private and public subnets as well as a Network Security group. The goal is then to apply rules to the private network to deny all outbound communication to the internet, only allow inbound RDP and only allow outbound communication to the storage service. By applying these restrictions, we can secure the storage account from unintended access from non-private virtual networks as well as public network communications. After creating the restrictions, I then test to see if access is denied on a public VM as well as granted access on a private VM

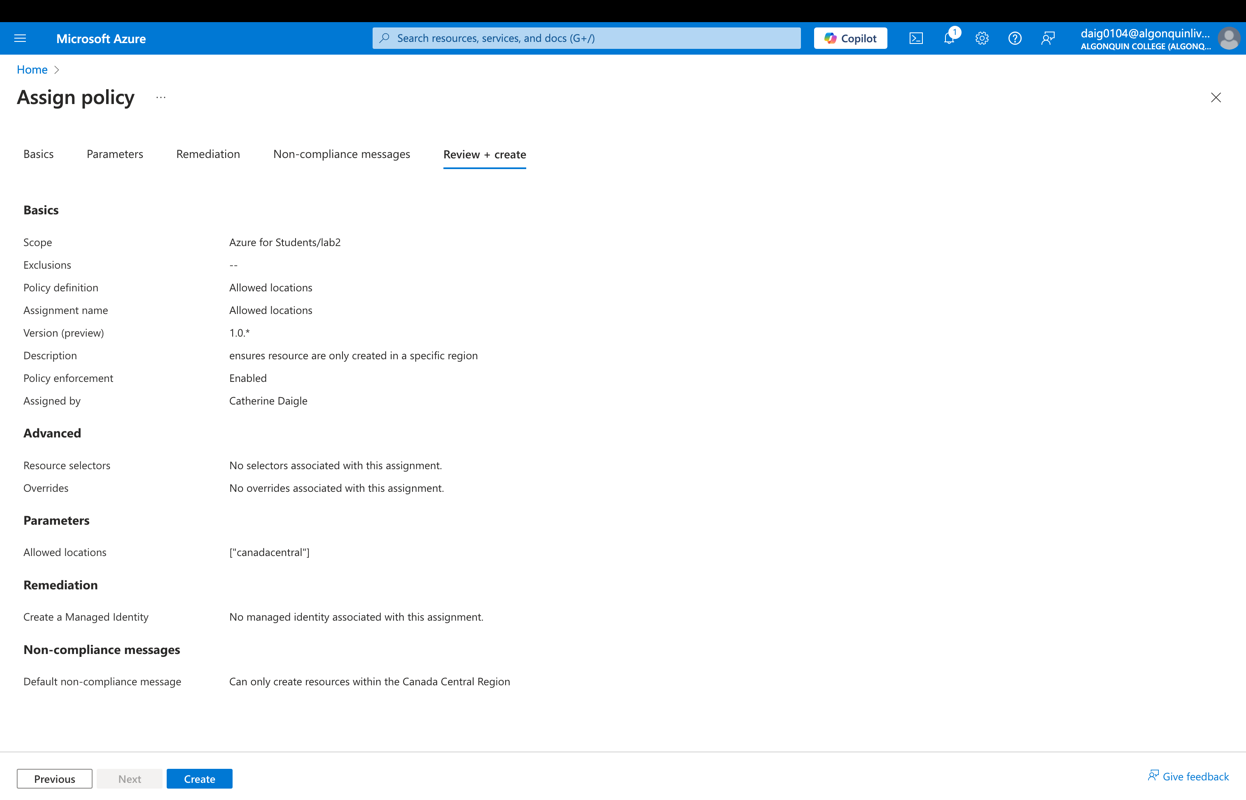
# Steps Covered With Screenshots:

# Cloud Policy:

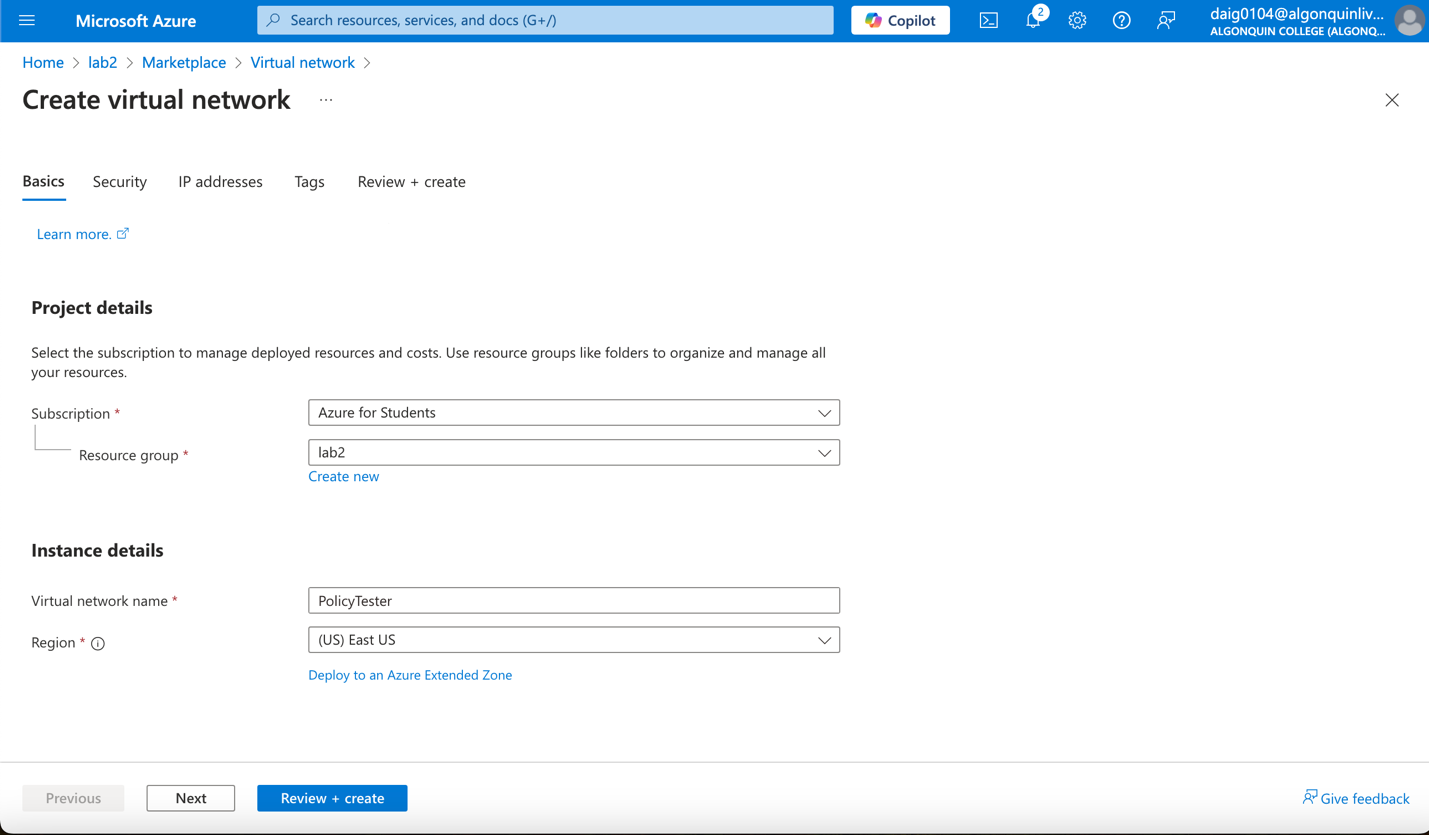
### Task 1: Create an Allowed Locations policy that ensures resource are only created in a specific region. I chose Canada Central



### Policy Review & Creation



### Task 2: Test to ensure resources are only created in the Allowed location I created a VN on a region that is not Canada Central

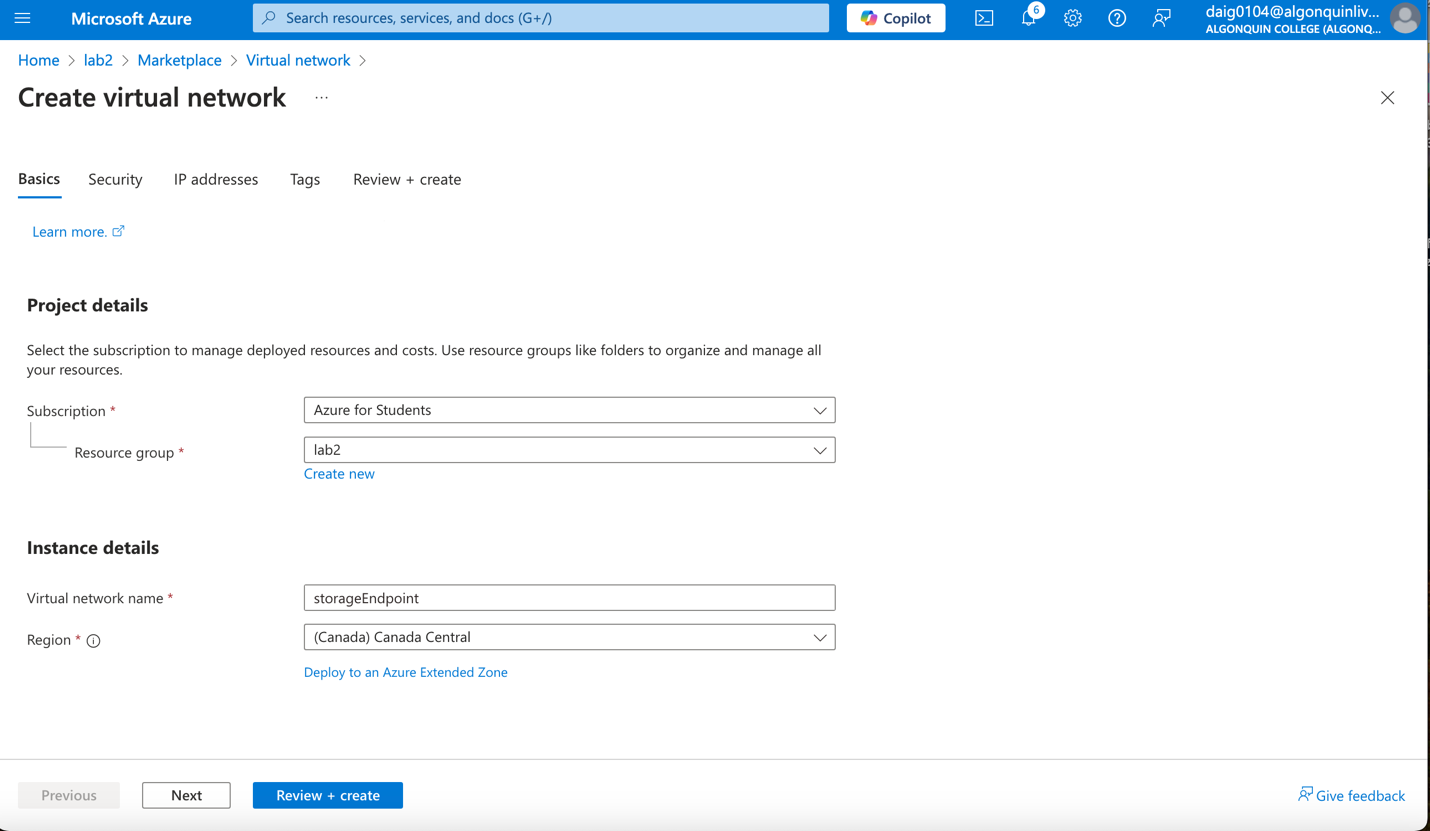


### Here we get an error which means the policy is working and disallowing other regions

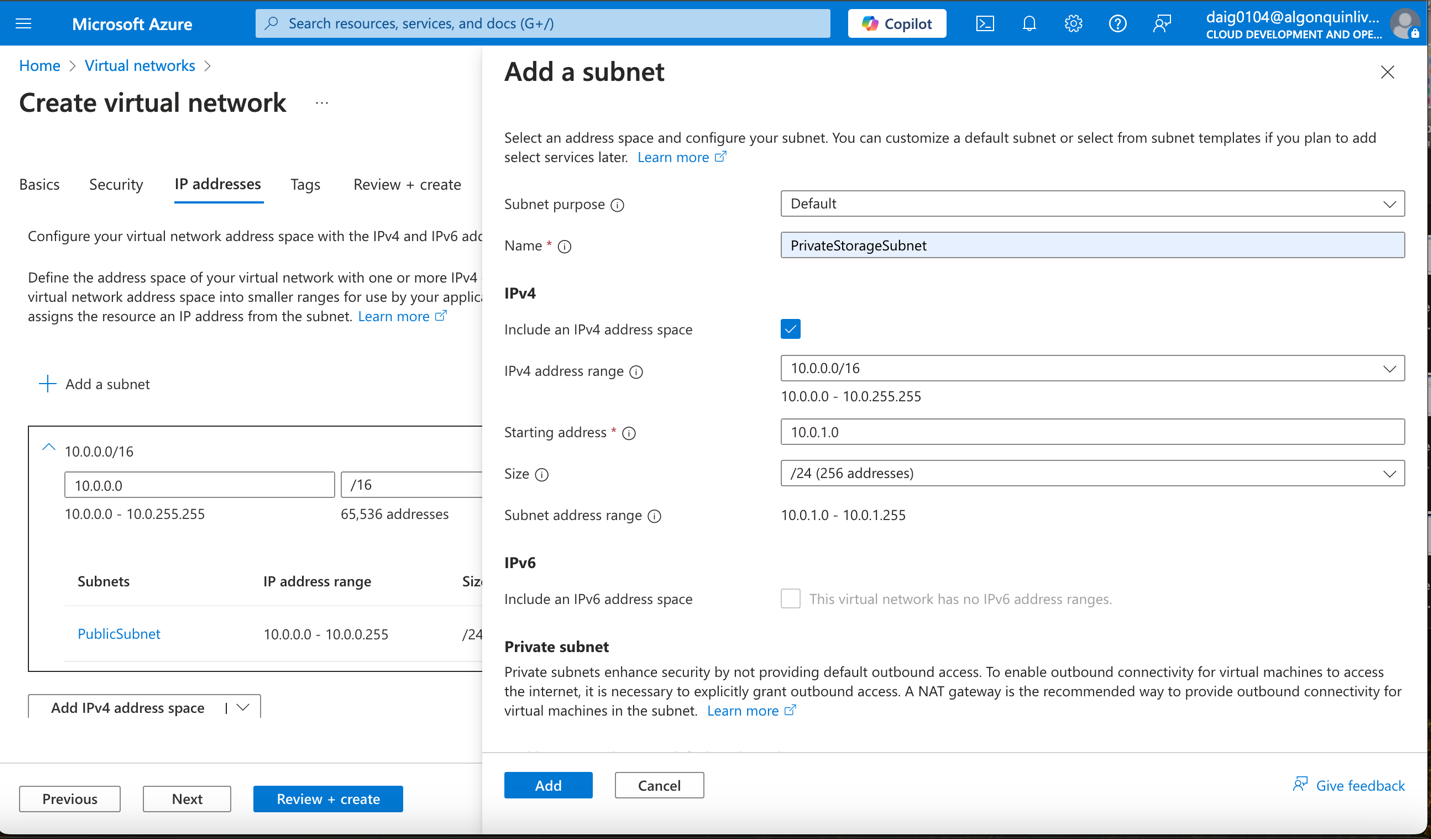


# Service Endpoints and Securing Storage

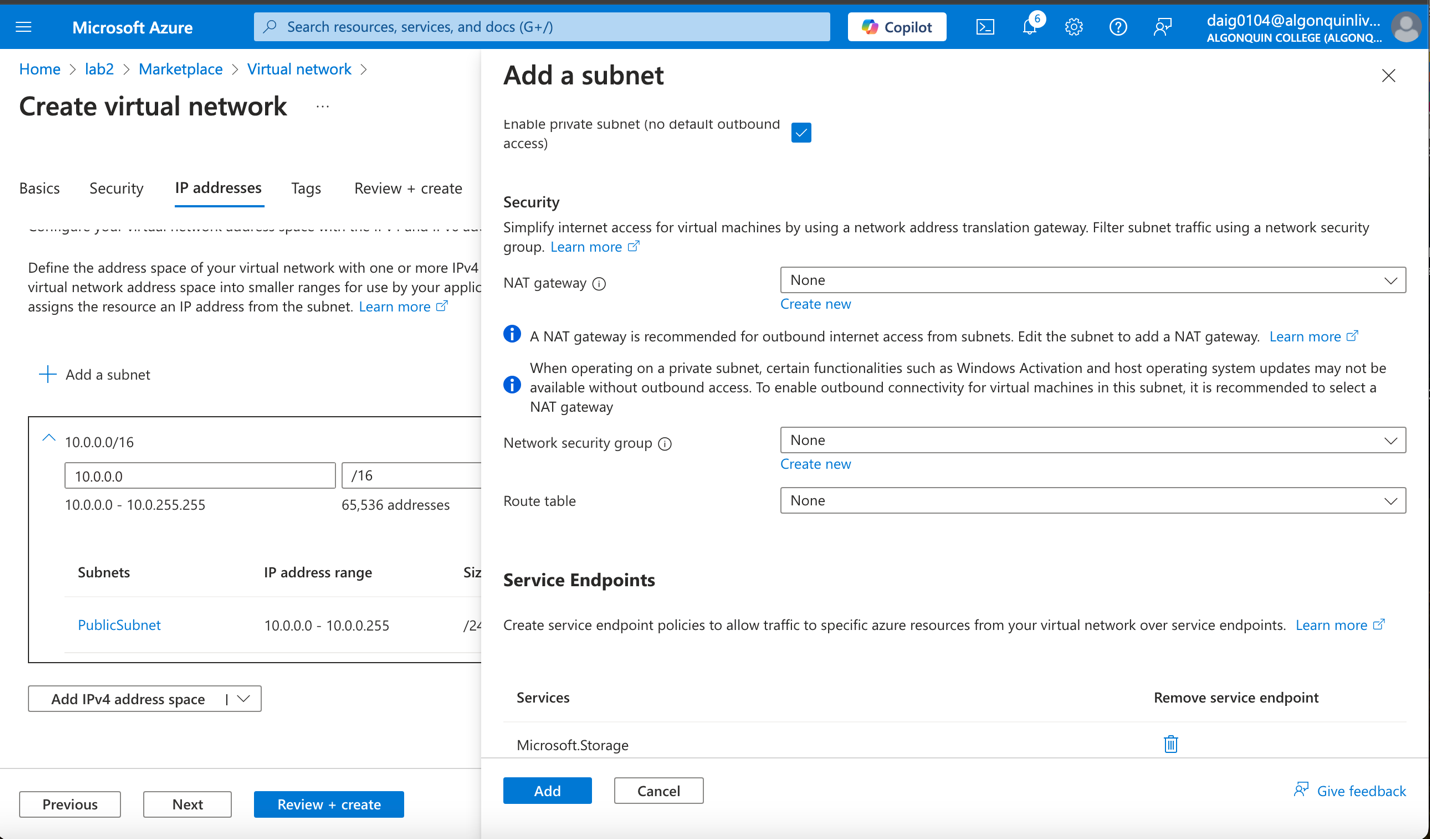
### Task 1: Creating a virtual network in Canada Central region. VN name is storageEndpoint



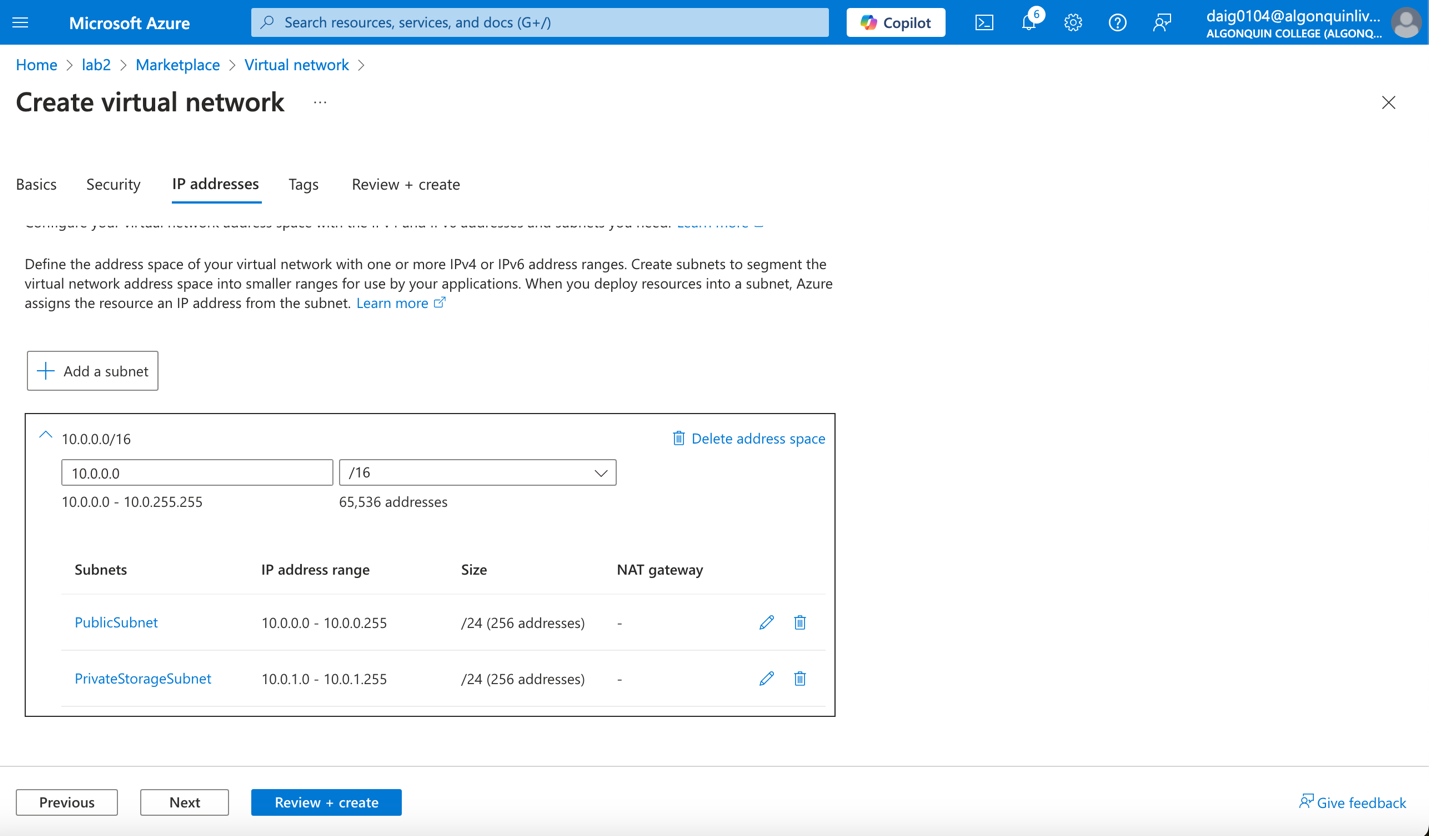
### Task 2: Add a subnet to the virtual network and configure a storage endpoint, the public subnet is the default subnet, renamed and below is the private subnet.



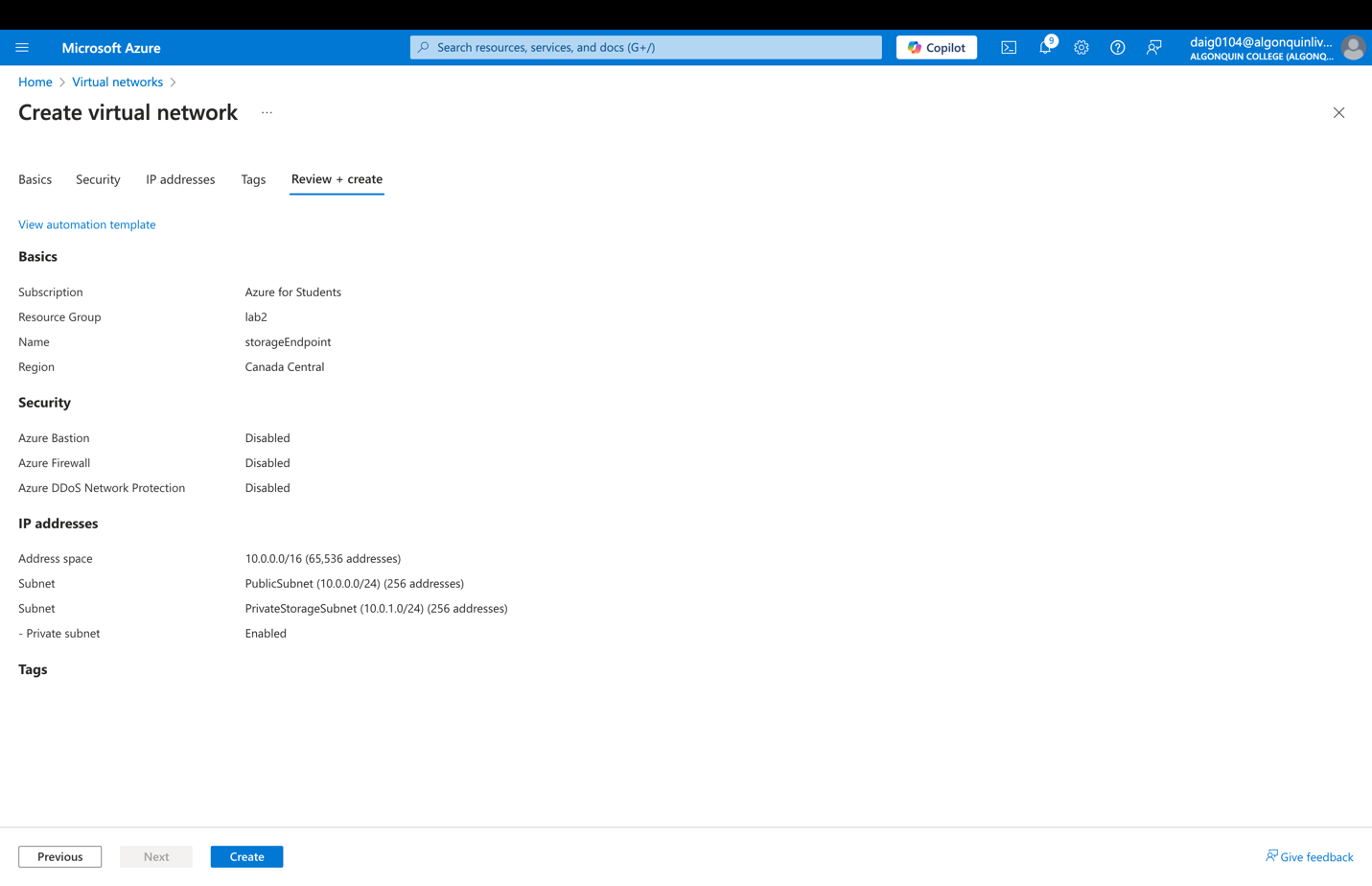
### Configuring Microsoft storage as service endpoint for private endpoint:



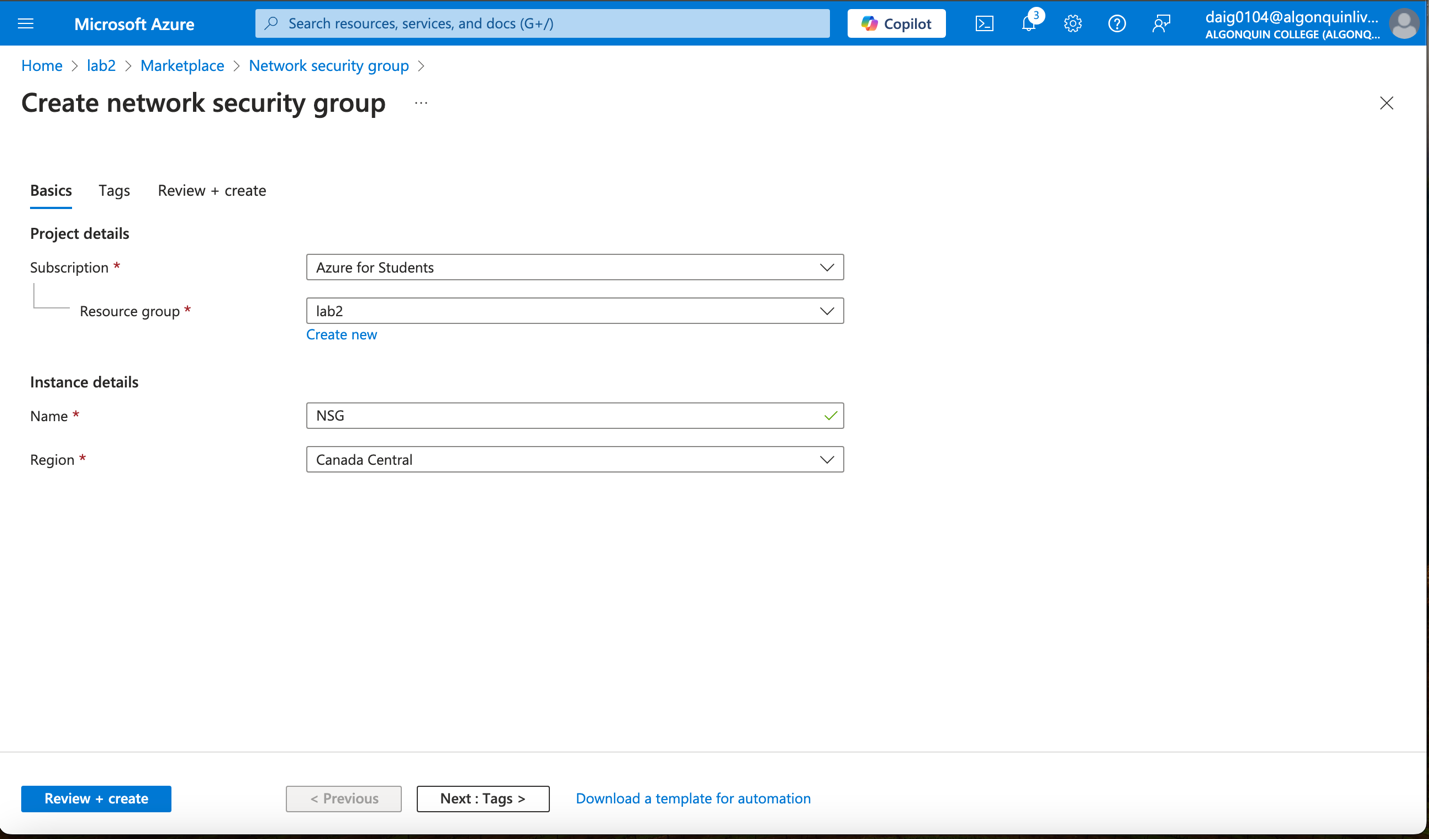
### Both endpoints public and private:



### Review:



### Task 3: create a network security group to restrict access to the subnet below is creation of nsg to Canada central

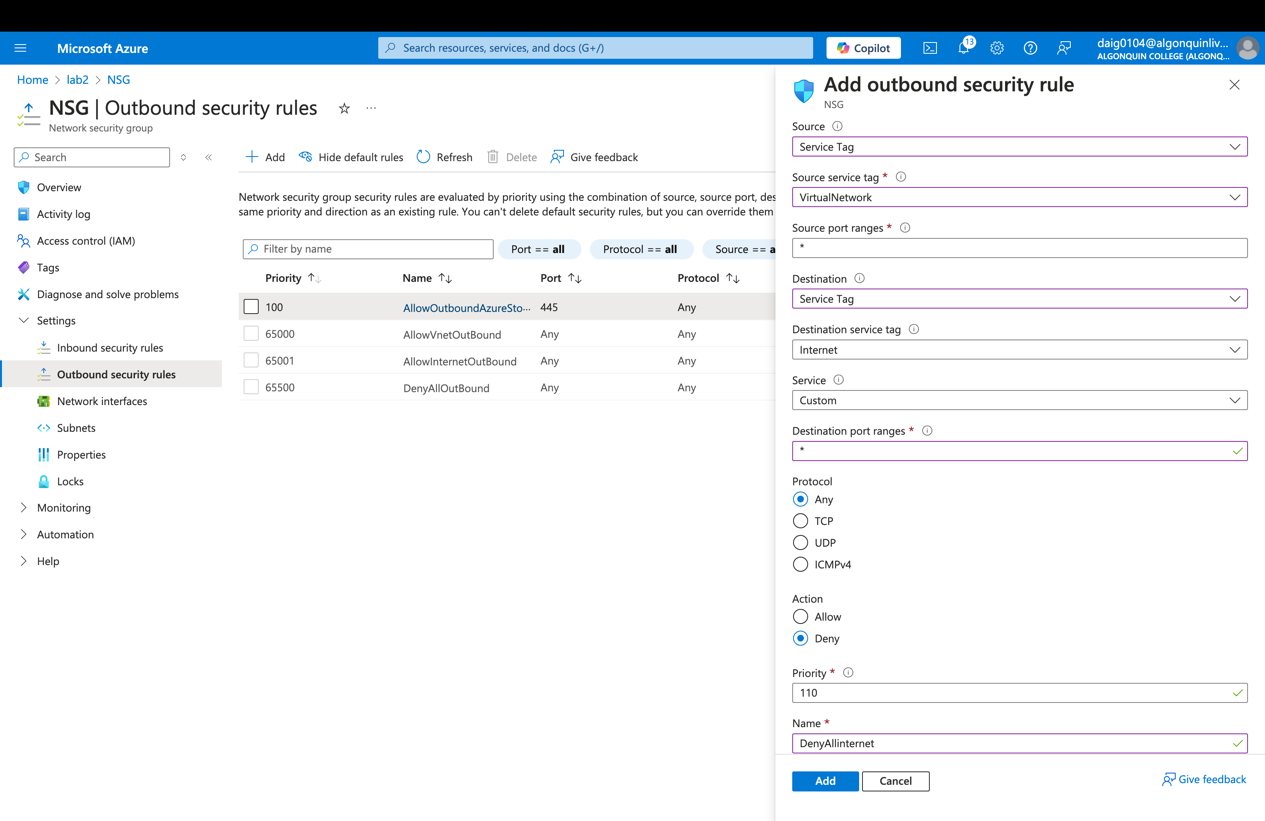


### Create a rule that allows outbound communication to the Azure Storage service it uses VirtualNetwork service tag and the destination service tag is set to Storage

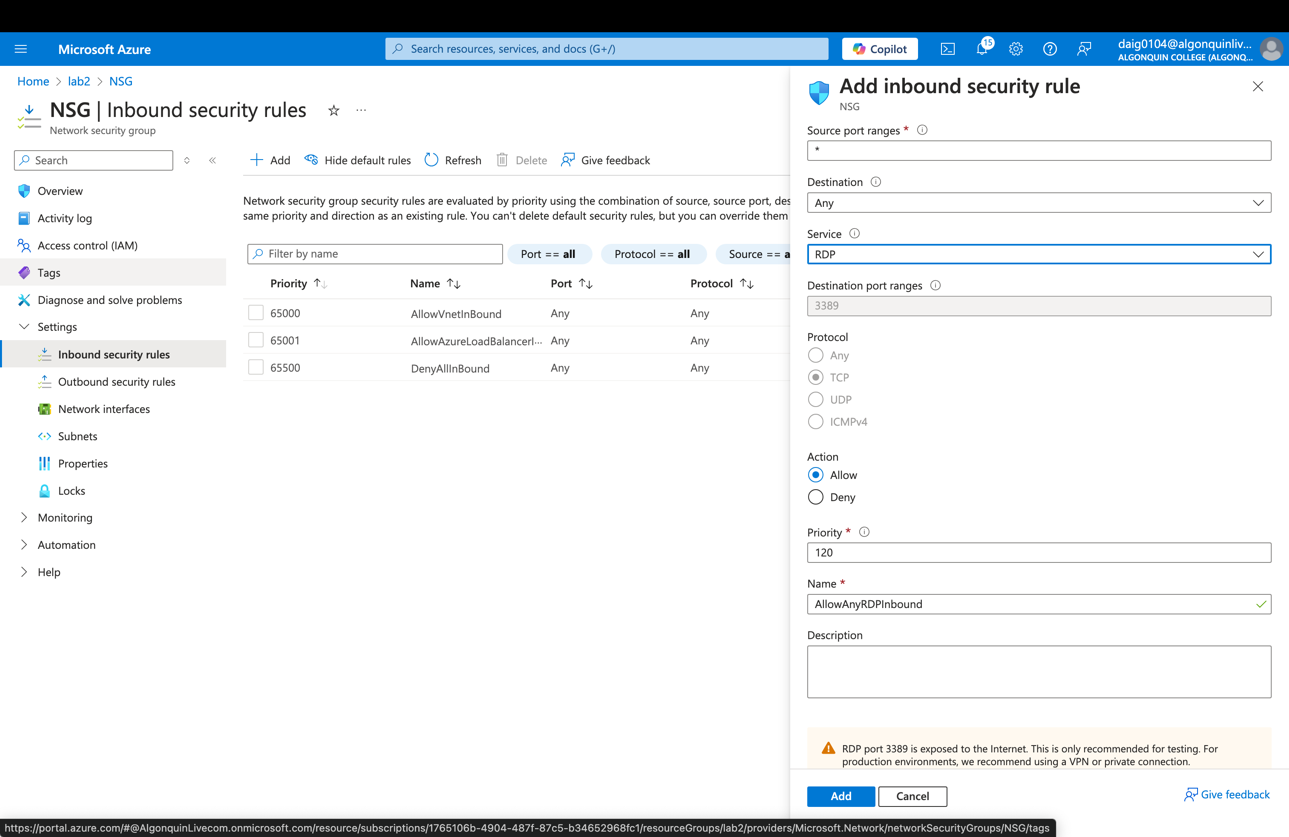


### Task 4: Configure a network security group to allow rdp on the public subnet

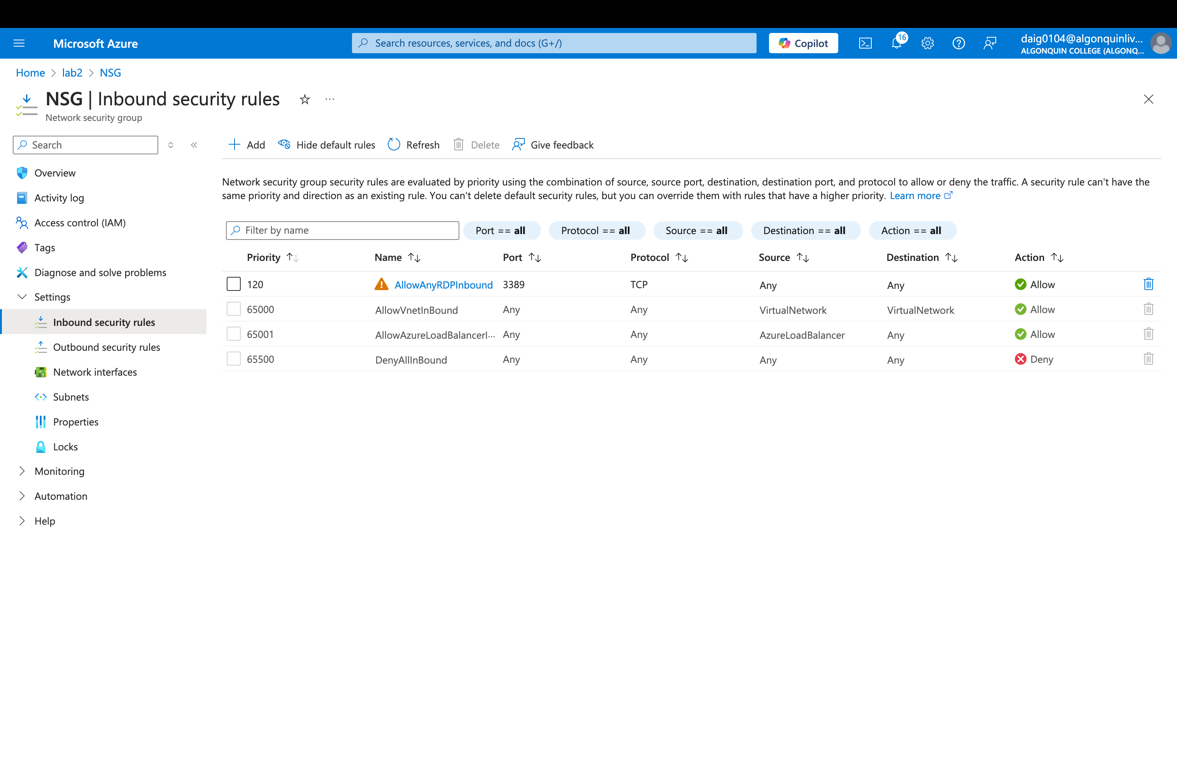
### Create another outbound security rule that denies communication to the internet. The destination service tag is Internet and links to VirtualNetwork as source being lower number priority, this rule overrides DenyAllOutBound



### Create an inbound security rule that allows Remote Desktop Protocol (RDP) traffic to the subnet from Any Destination. The rule overrides a default security rule that allows all inbound traffic from the internet. Below is AllowAnyRDPinbound using RDP service its priority is 120 and lower than the other rule priorities, overriding other rules.

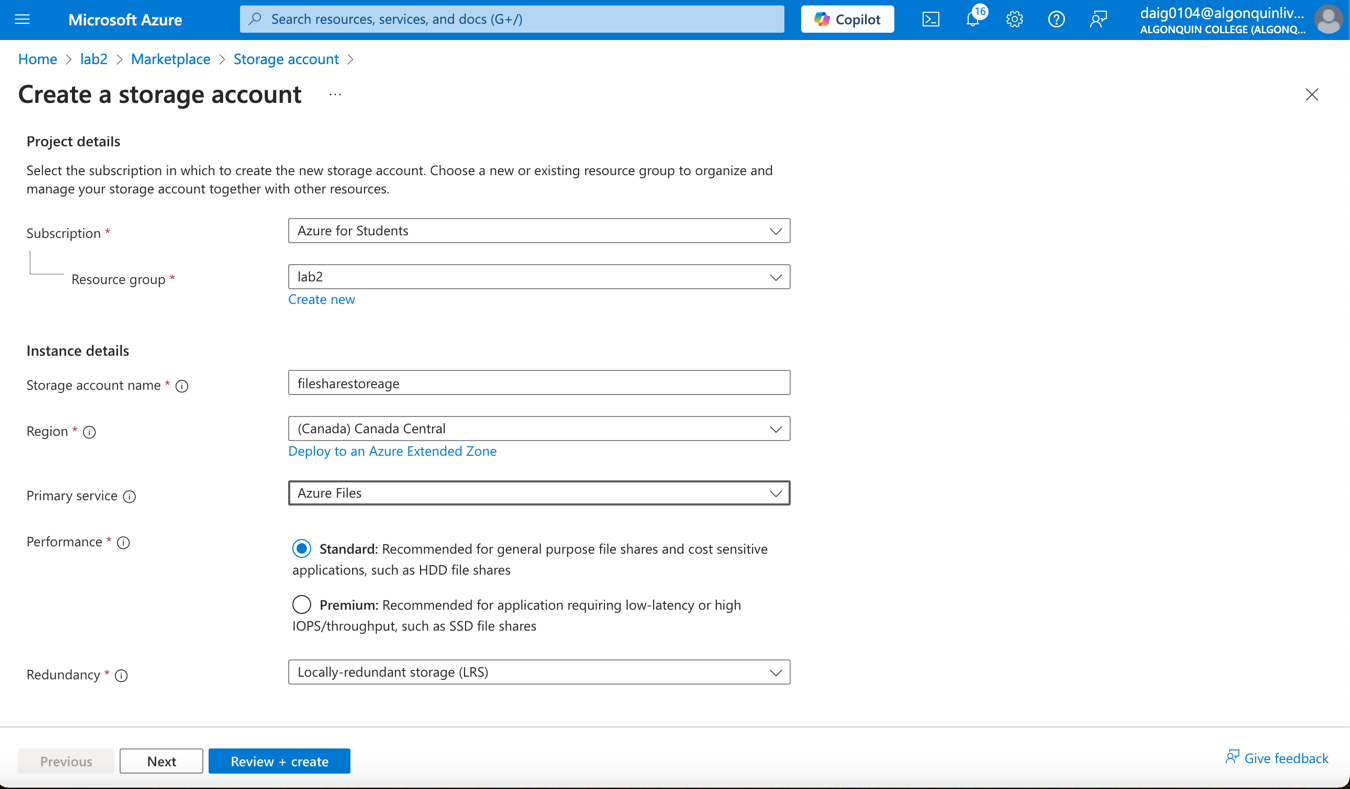


### List of inbound rules.



### Task 5: Create a storage account with a file share

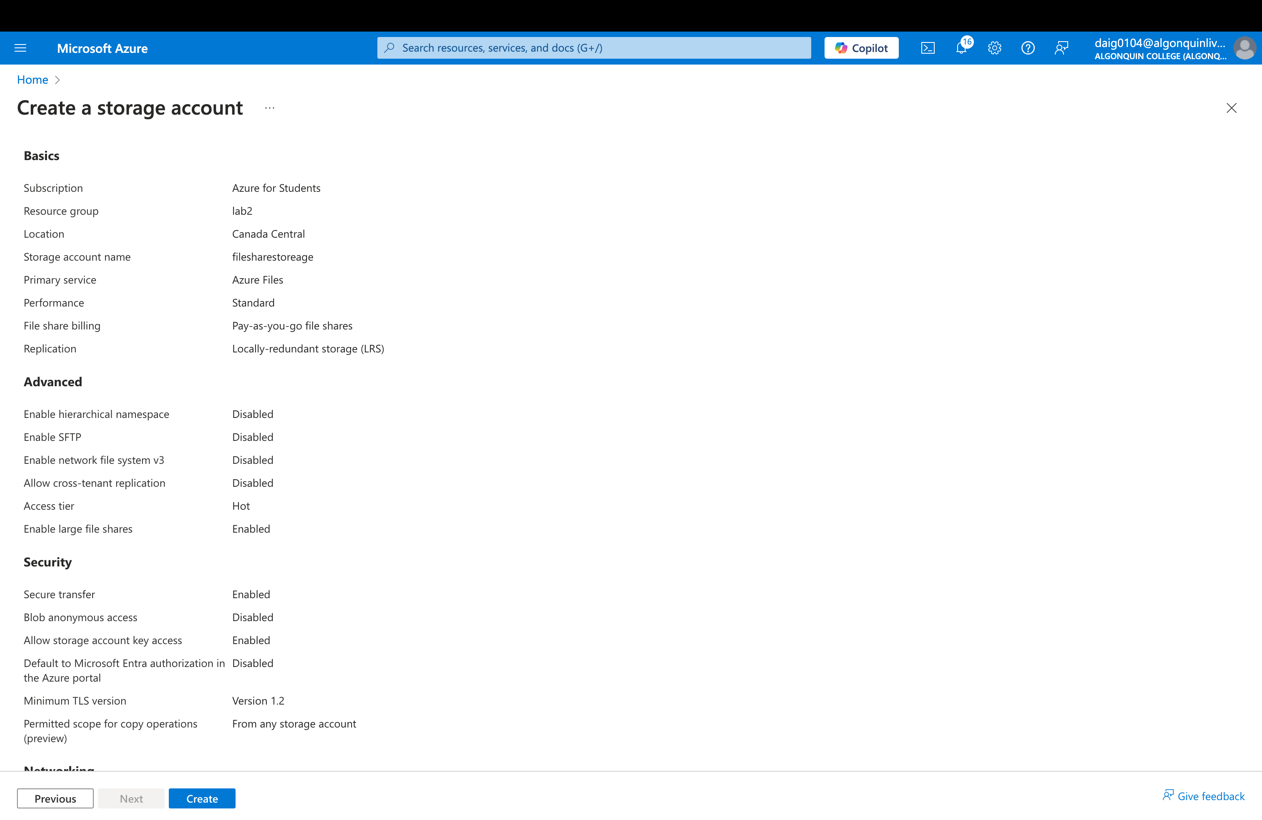
### Creating storage account, with Azure files, locally redundant



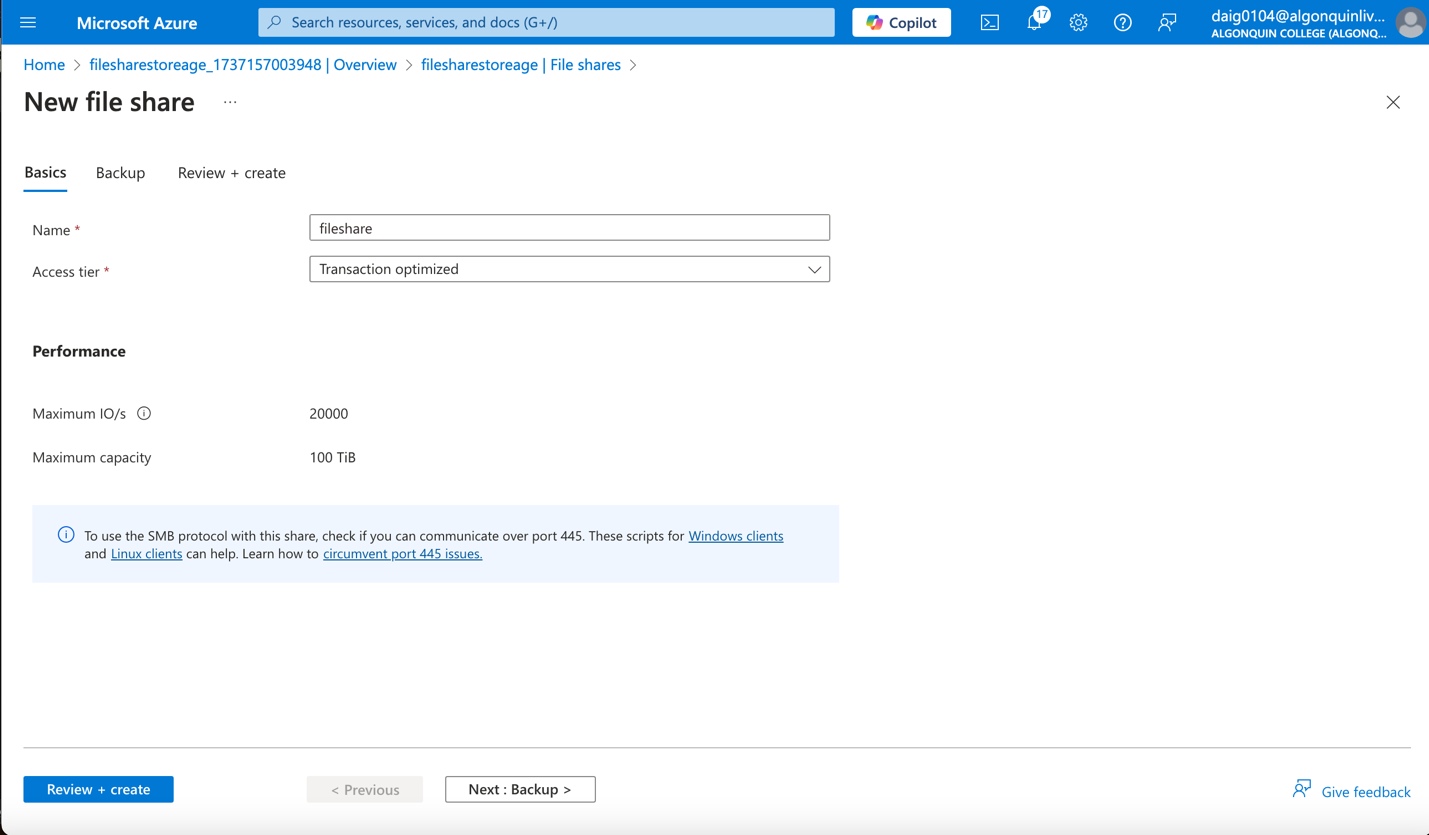
### Connecting the Virtual network to the storageEndpoint VN and setting the subnet to the PrivateStorageSubnet.

### 

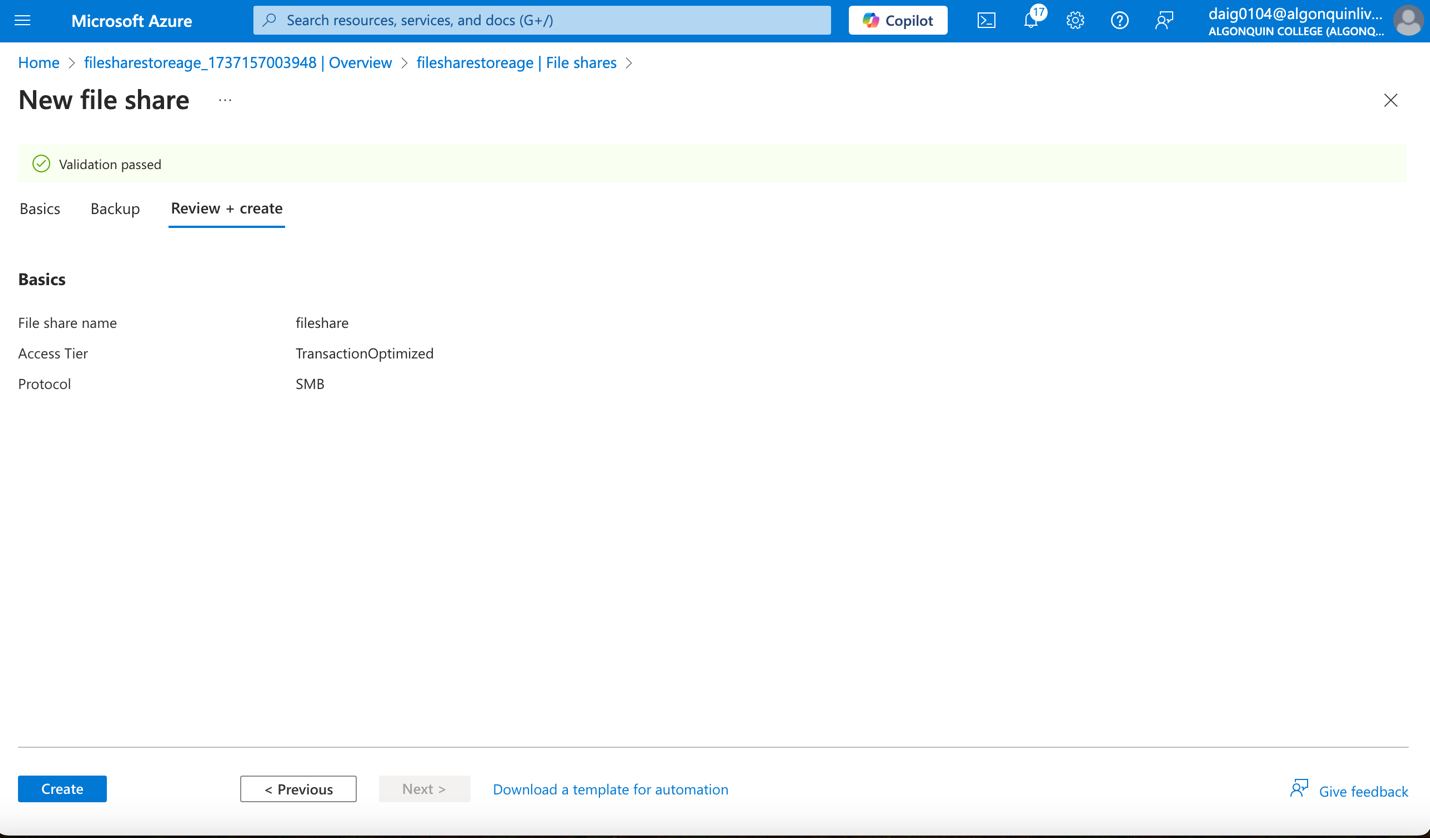
### Review of the storage Account



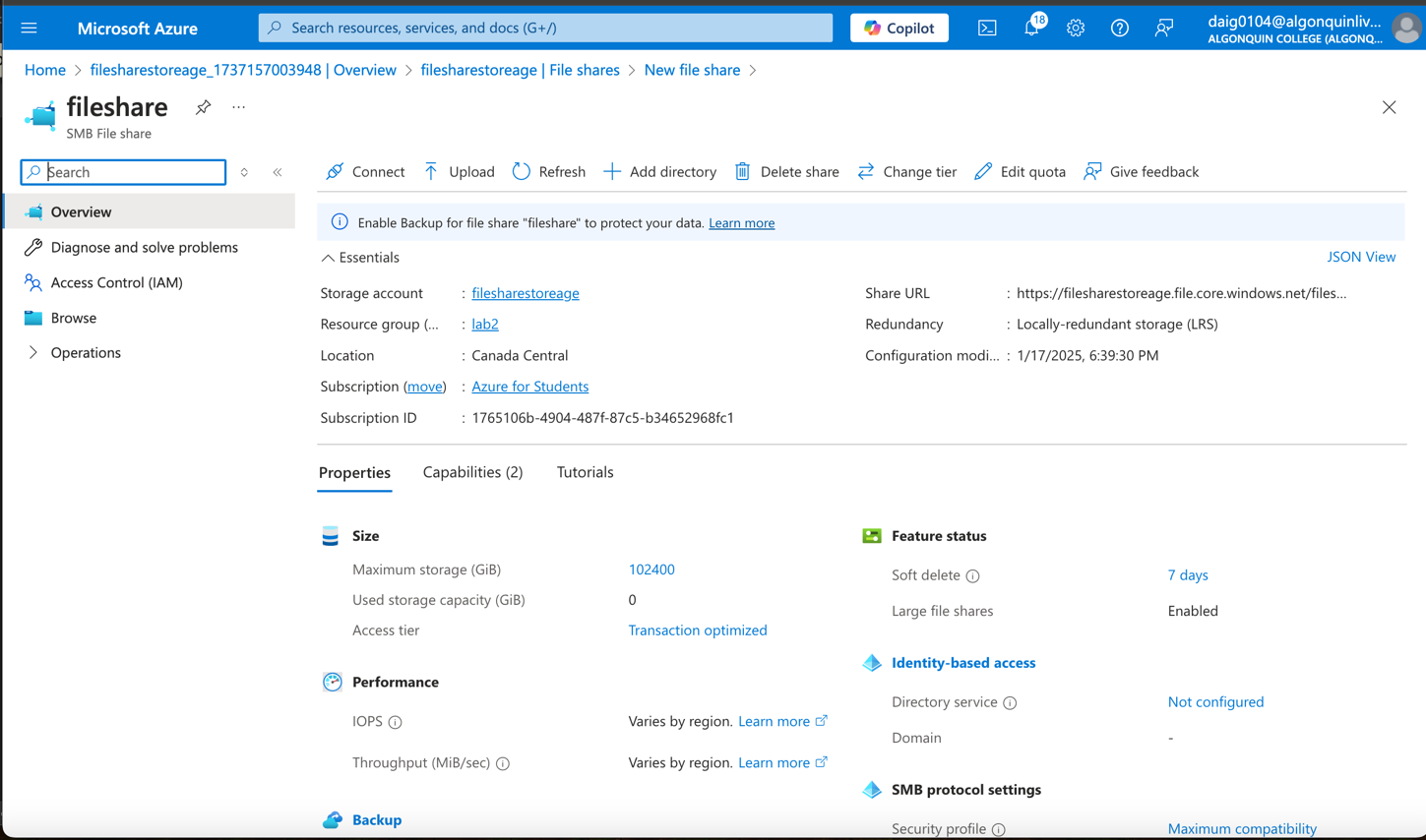
### Creating file share within storage account



### Fileshare Review:

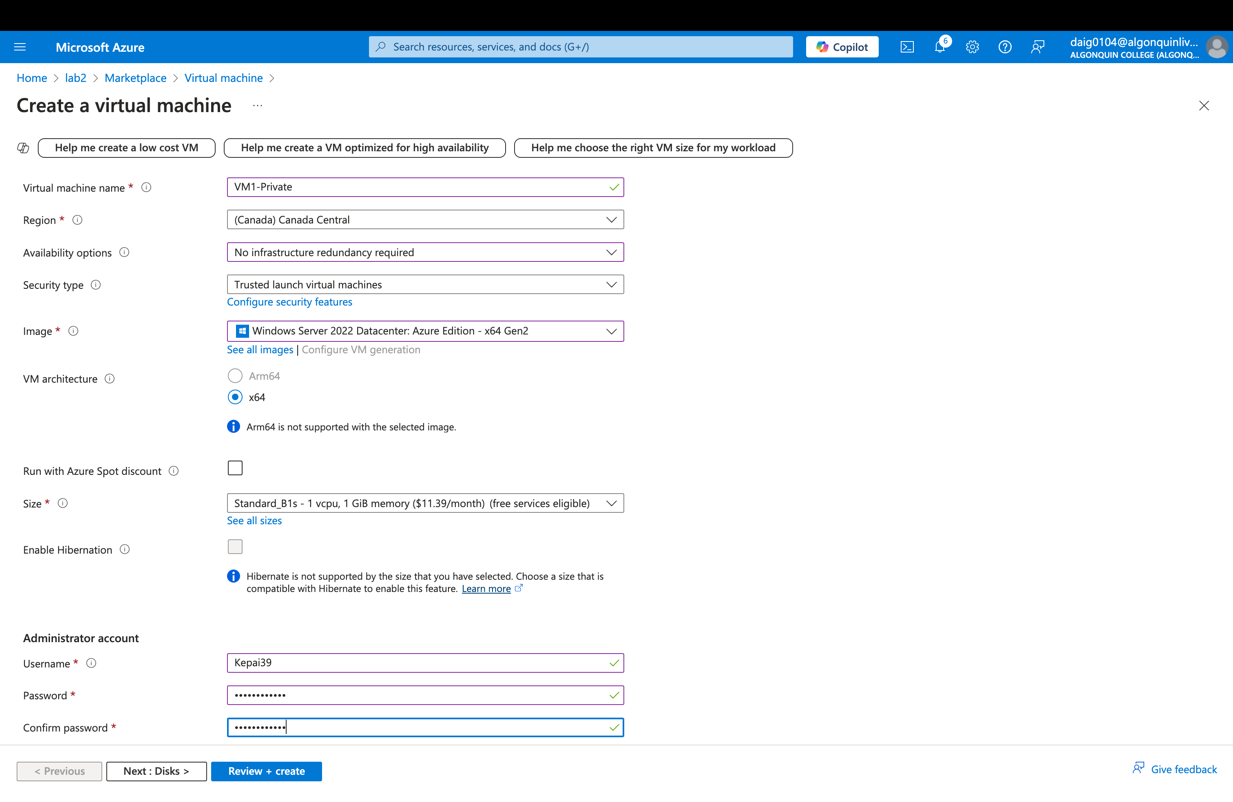


### Deployed Fileshare

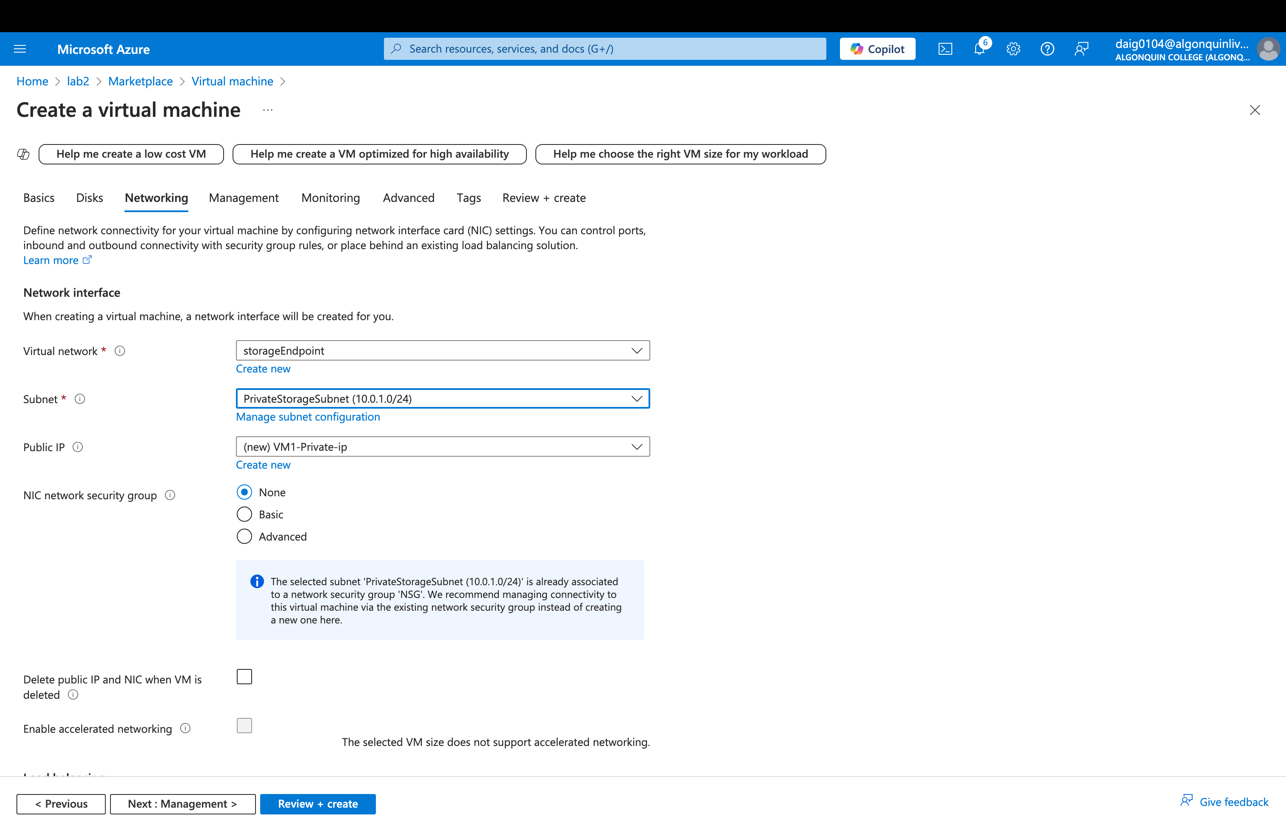


### Task 6: Deploy virtual machines into the designated subnets

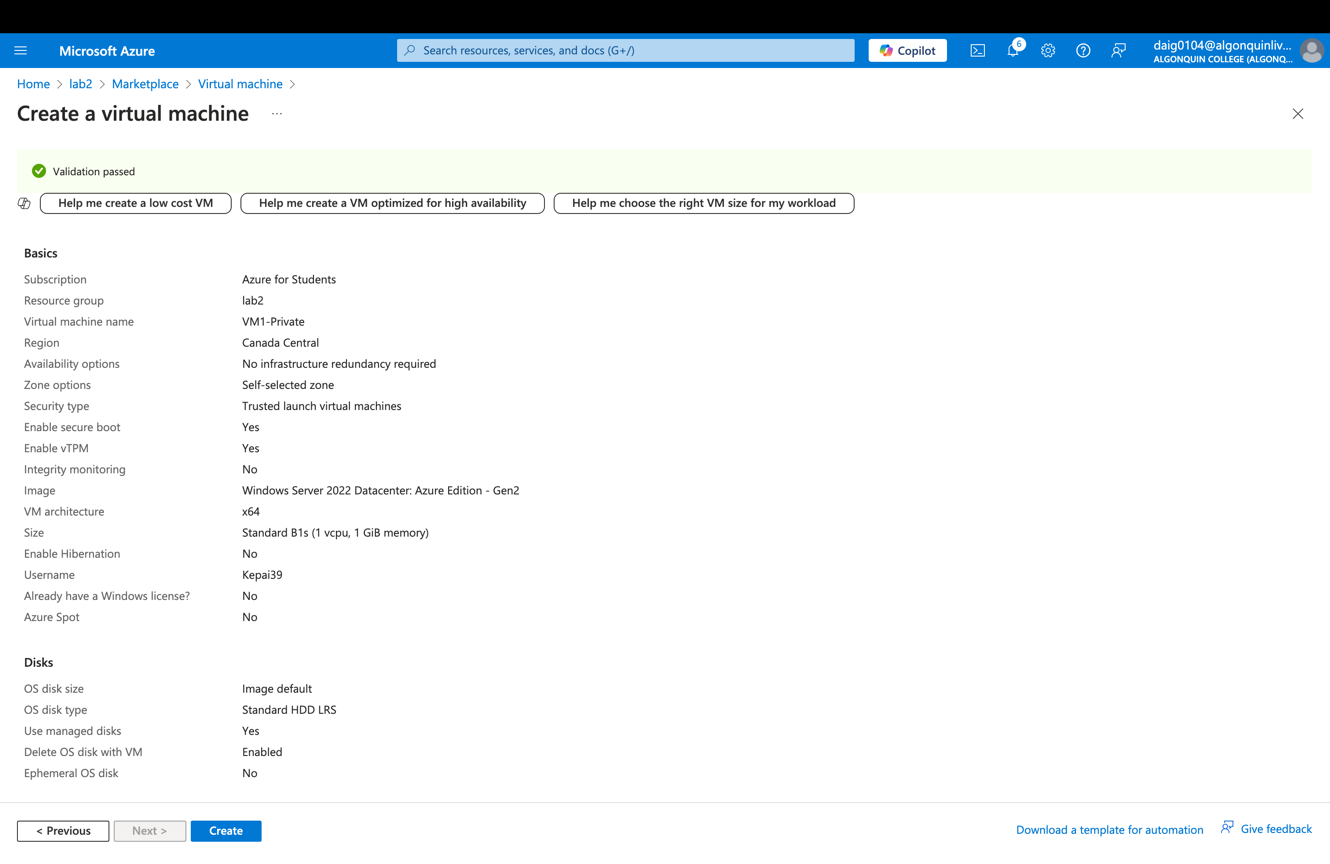
### To test network access to a storage account, deploy a virtual machine to each subnet this is the private vm. It’s using Windows server for a later step, standard B1s for cost efficiency.



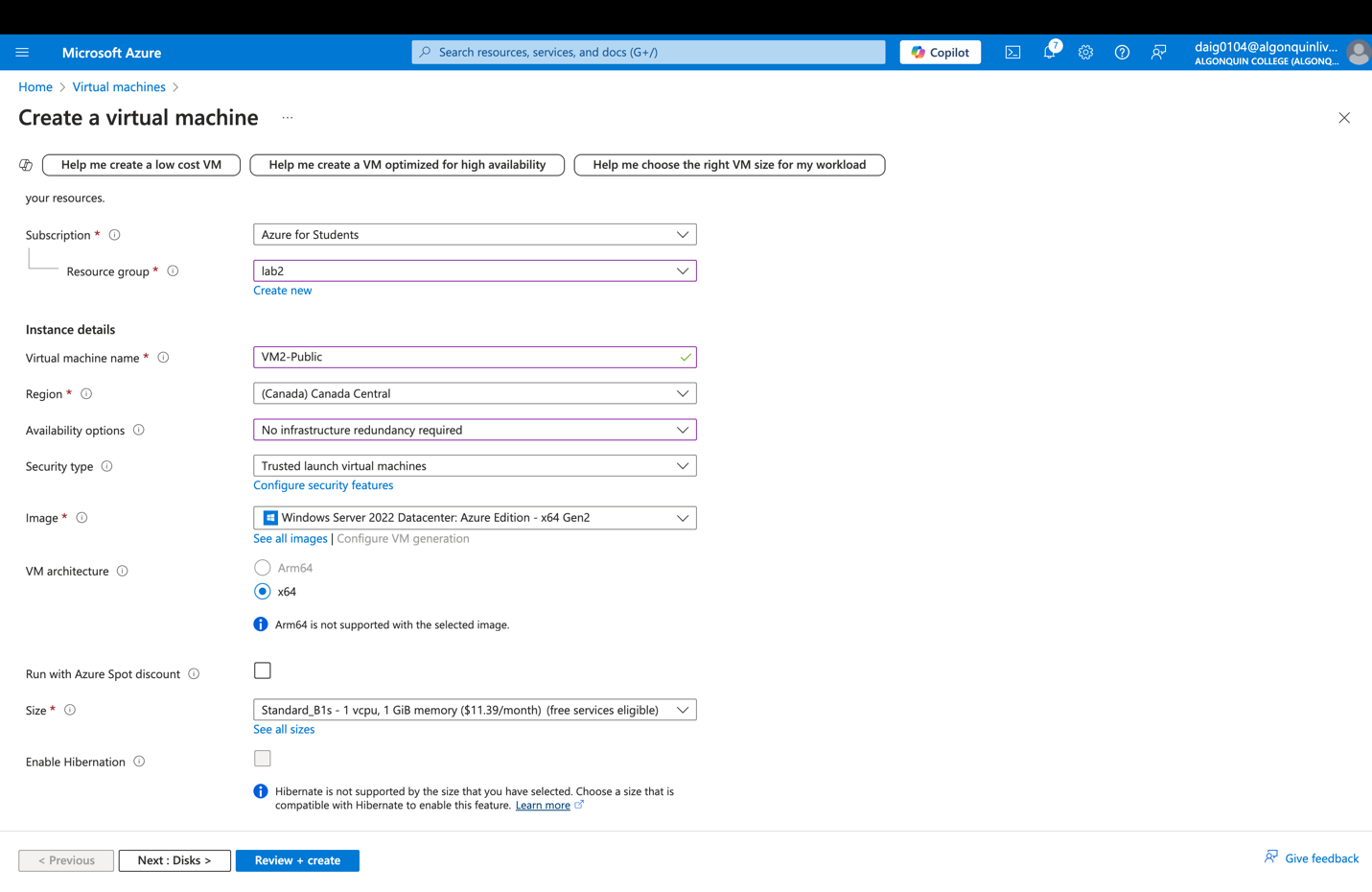
### Connecting to private subnet do not need to set a NIC since we already made a network security group



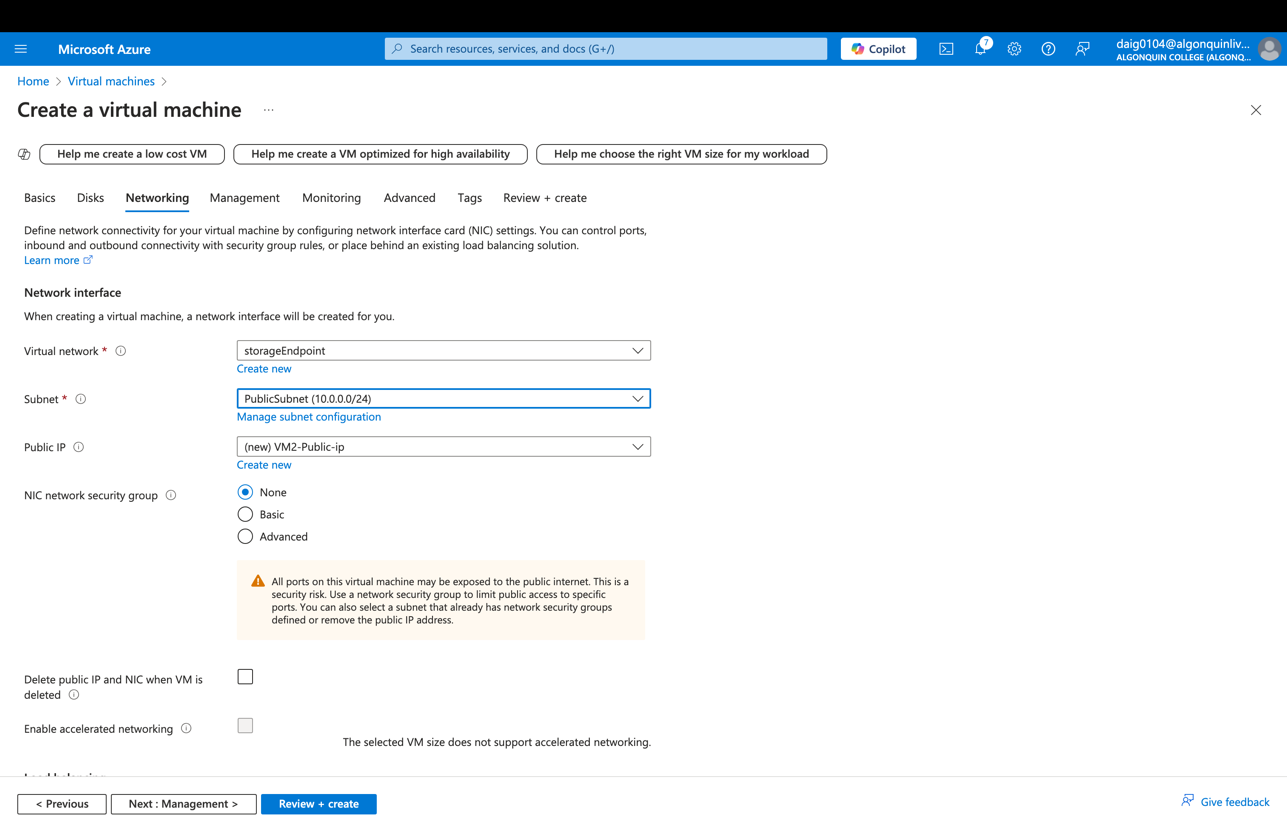
### Review:



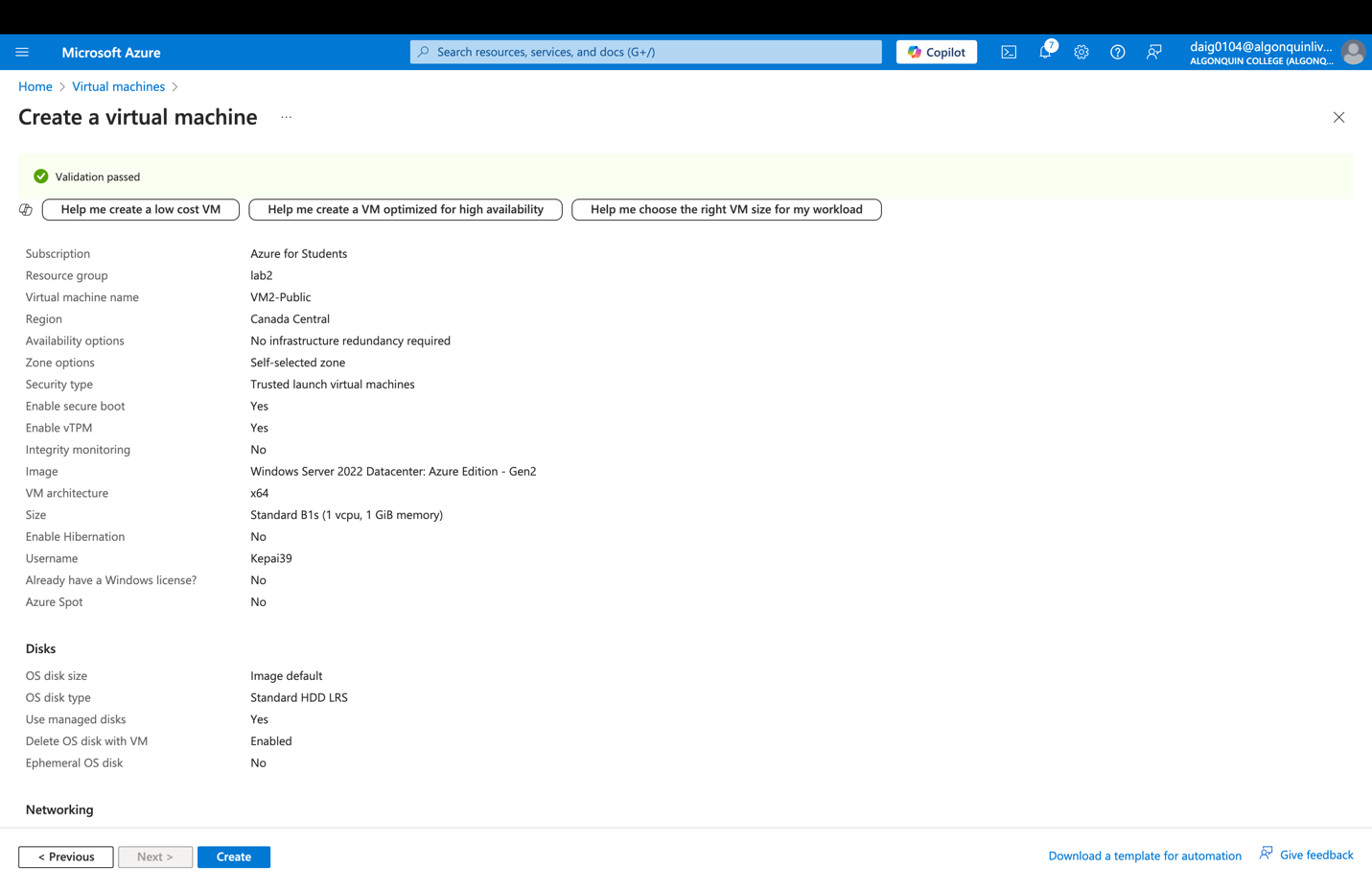
### Creating public VM, again windows server, standard B1s



### Connecting to public subnet, none for NIC since we have a network security group

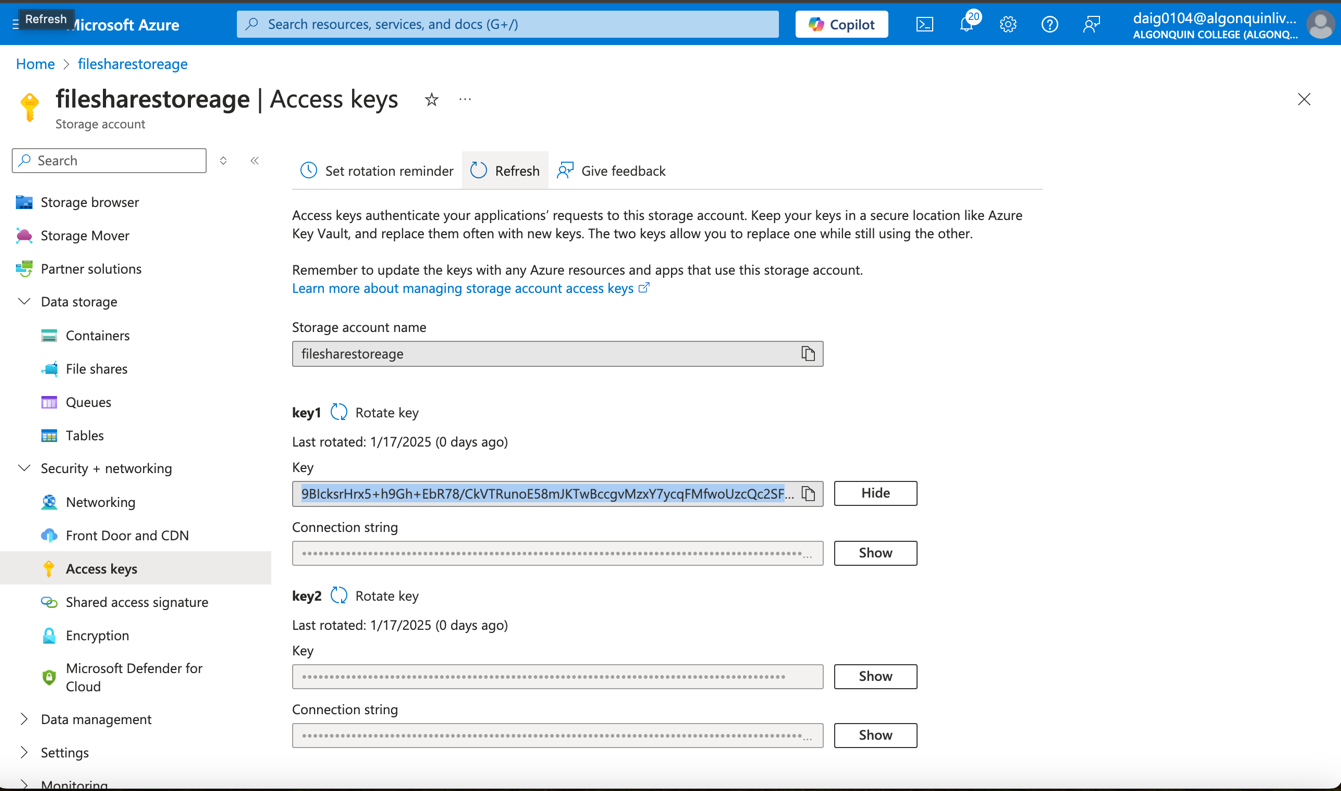


### Review:

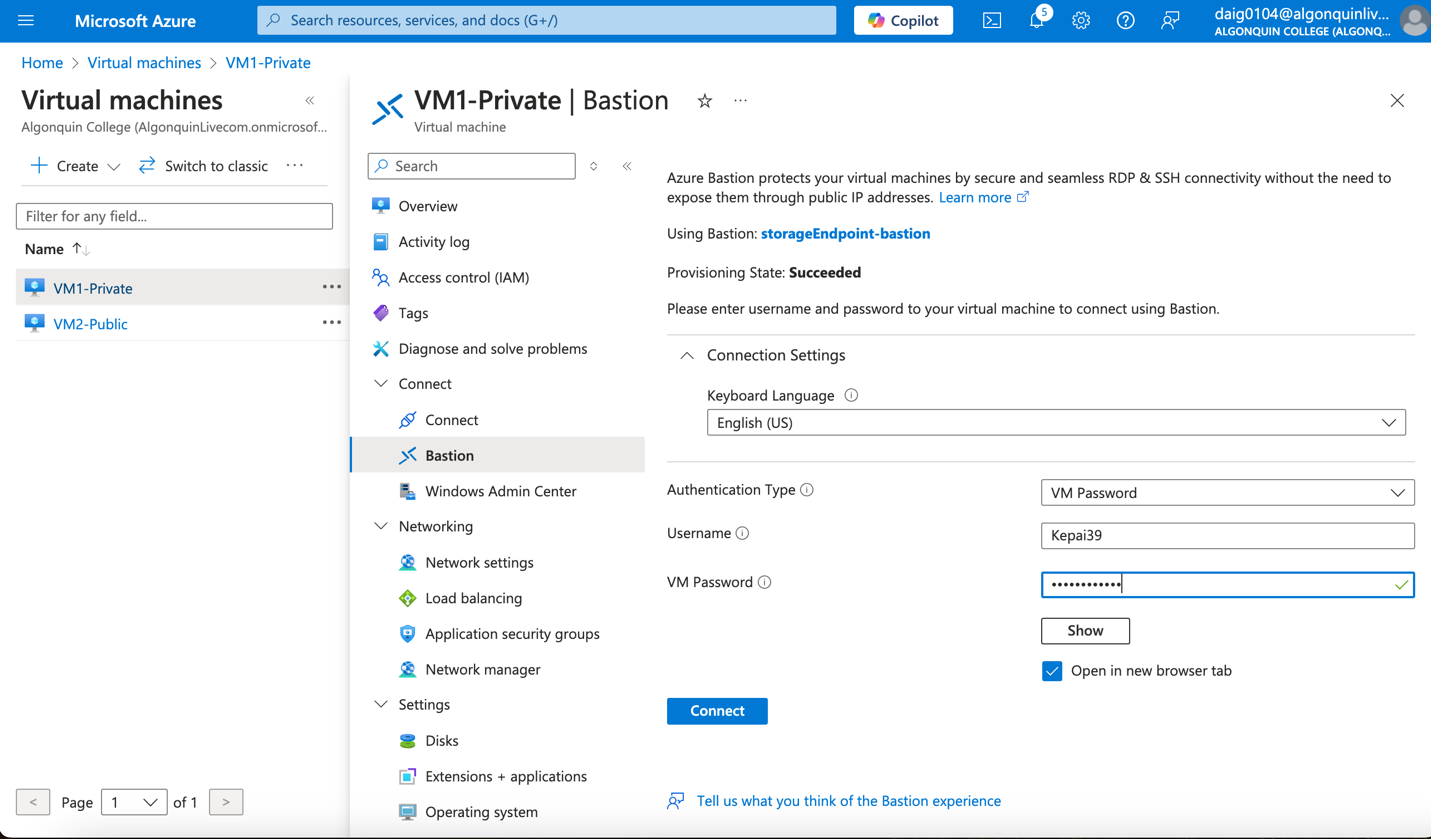


### Task 7: Test the storage connection from the private subnet to confirm that access is allowed

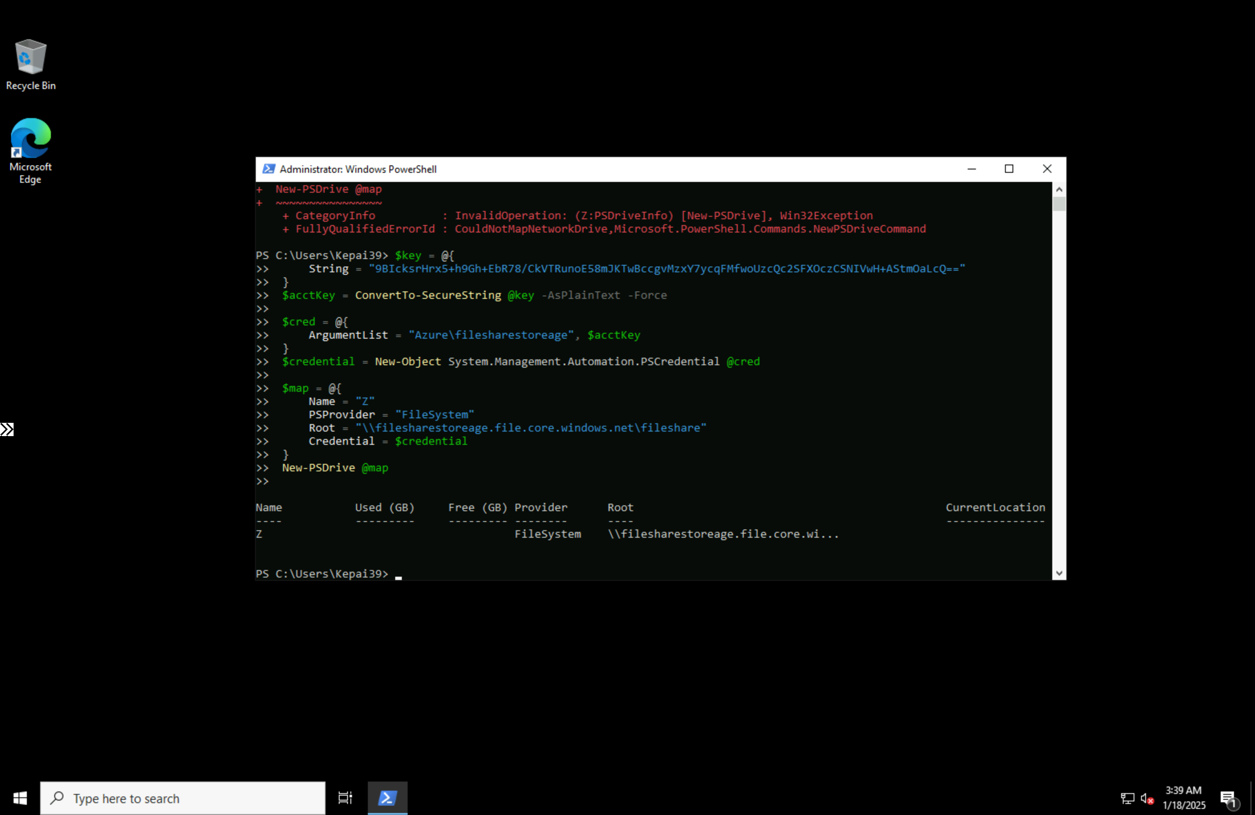
### Get storage account access key



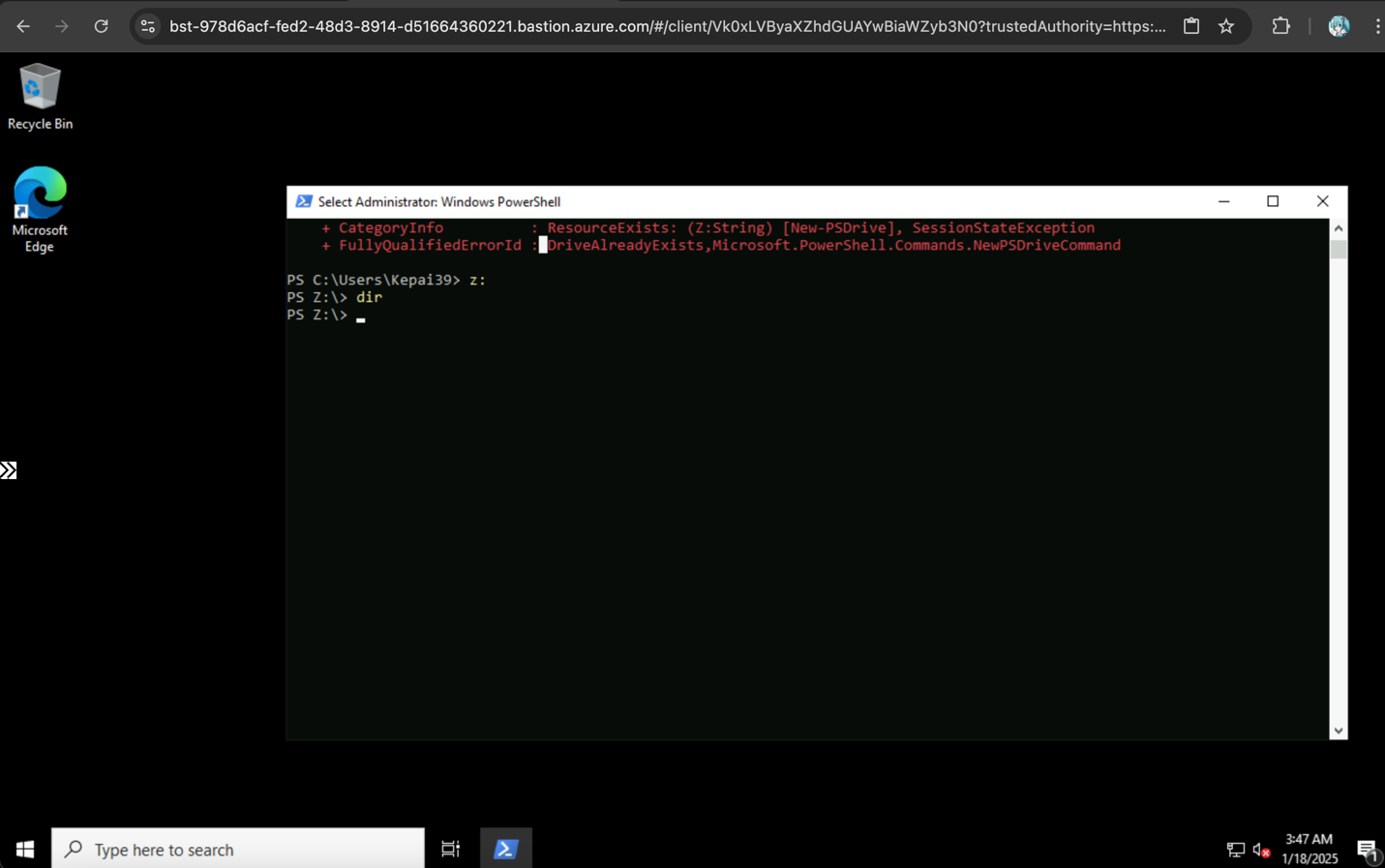
### Creating and connecting to Bastion with username/password



### Powershell of VM1-Private mapping the file share to Z drive using the code below:

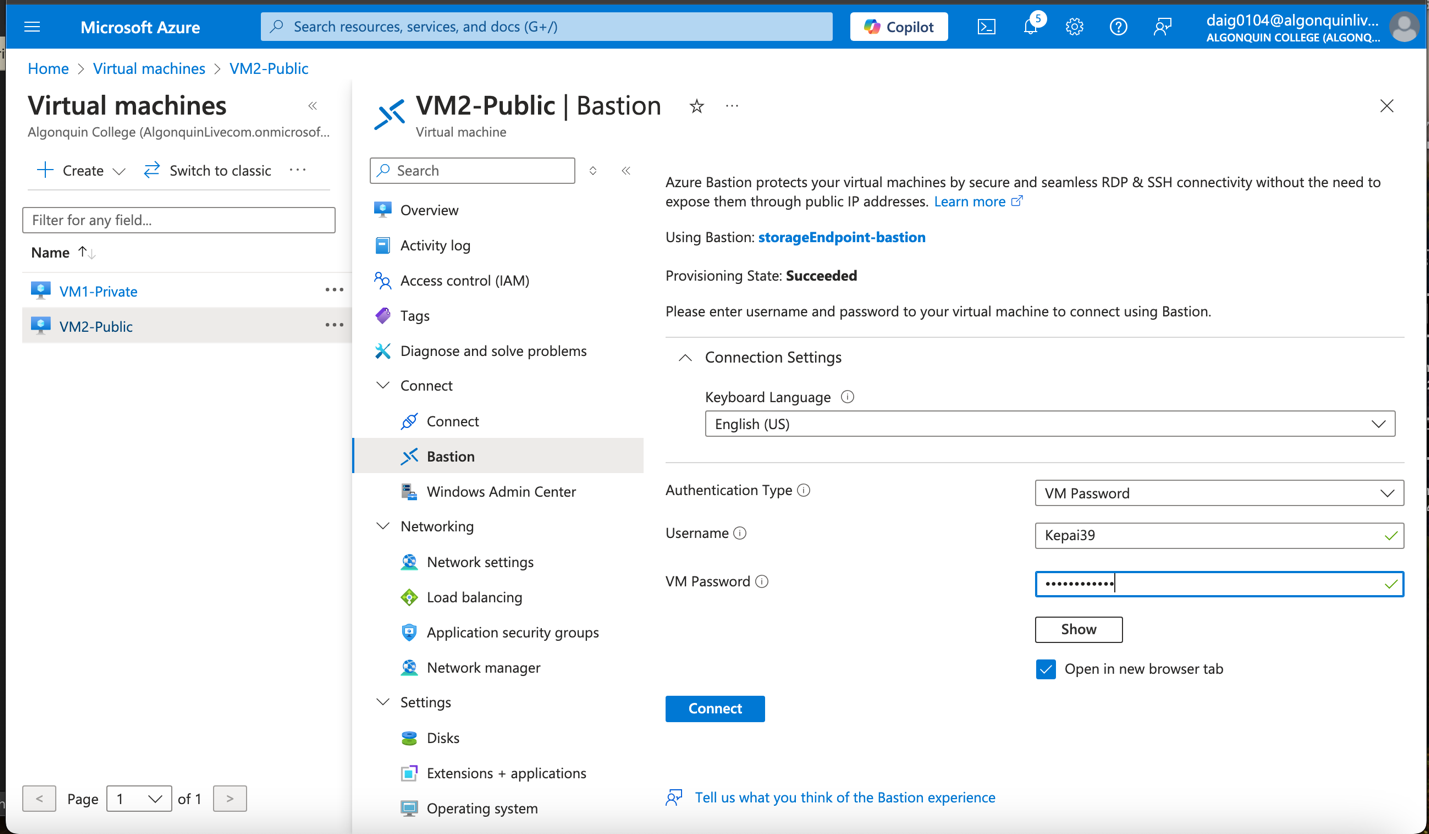


### Checking where the z drive is located (it turns out I had to check via terminal as it does not show up in the visual finder application)

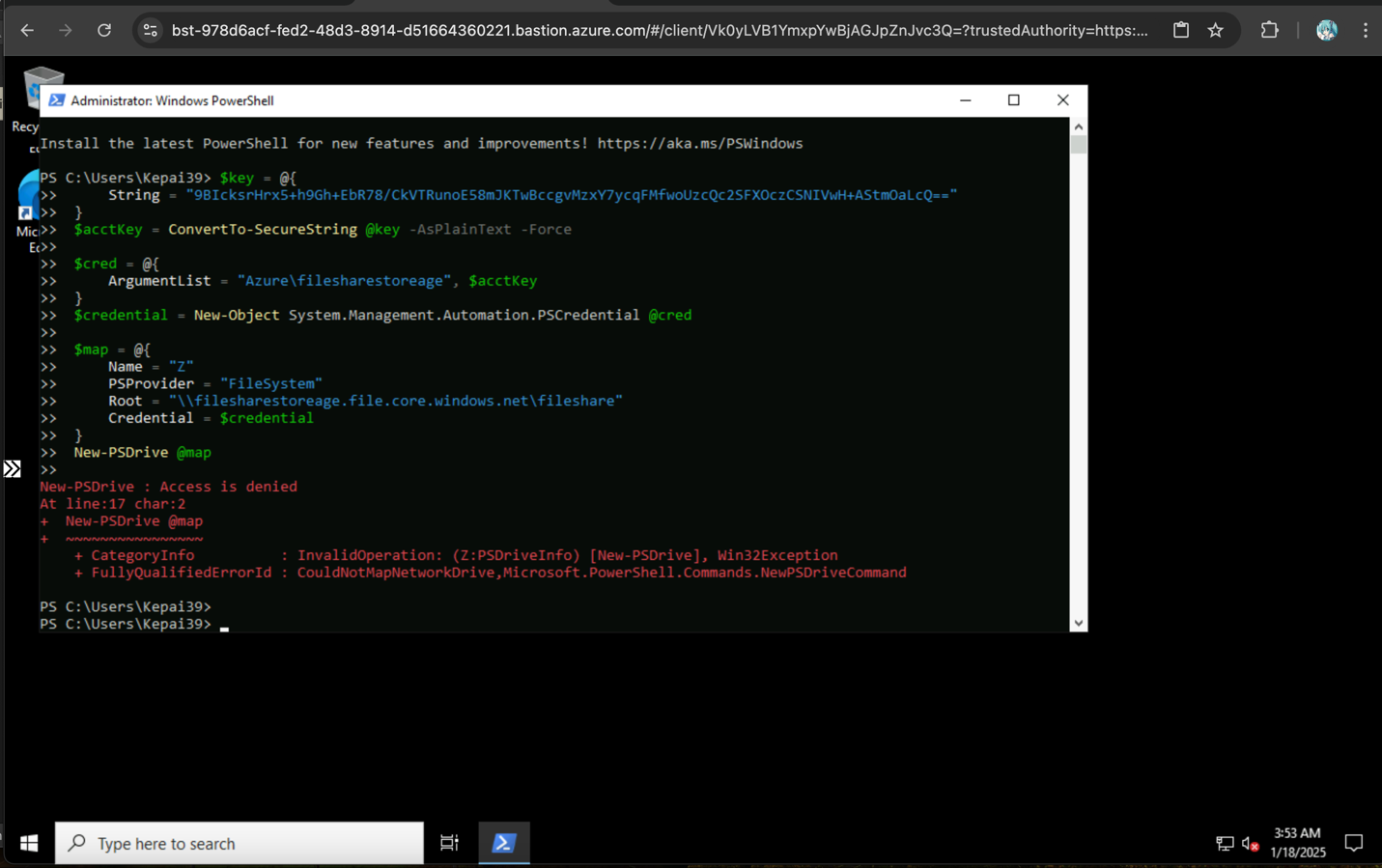


### Task 8: Test the storage connection from the public subnet to confirm that access is denied

### Connecting to VM2-public



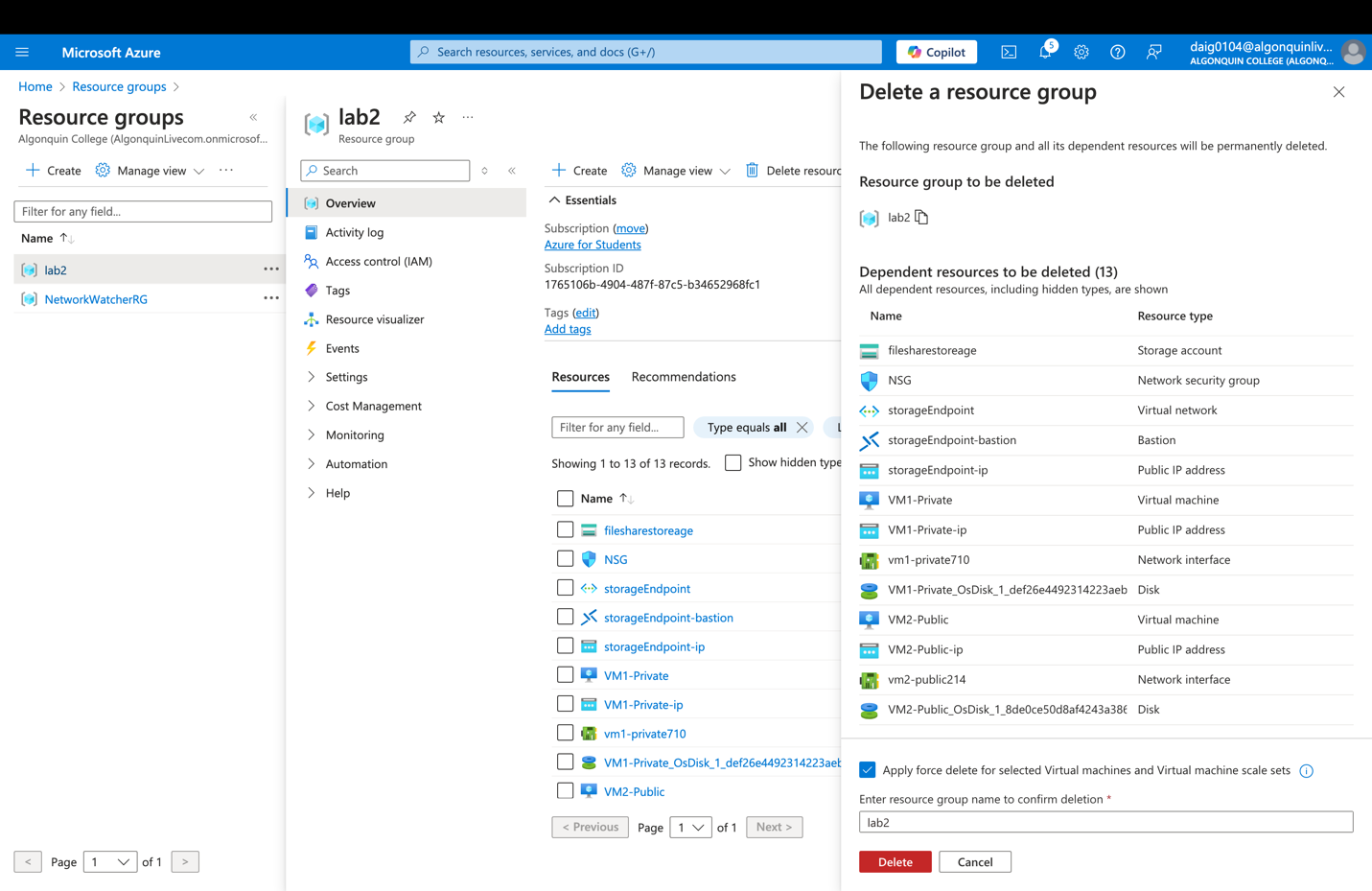
### An error that confirms when mapping the Z drive access is denied when using the same code below:

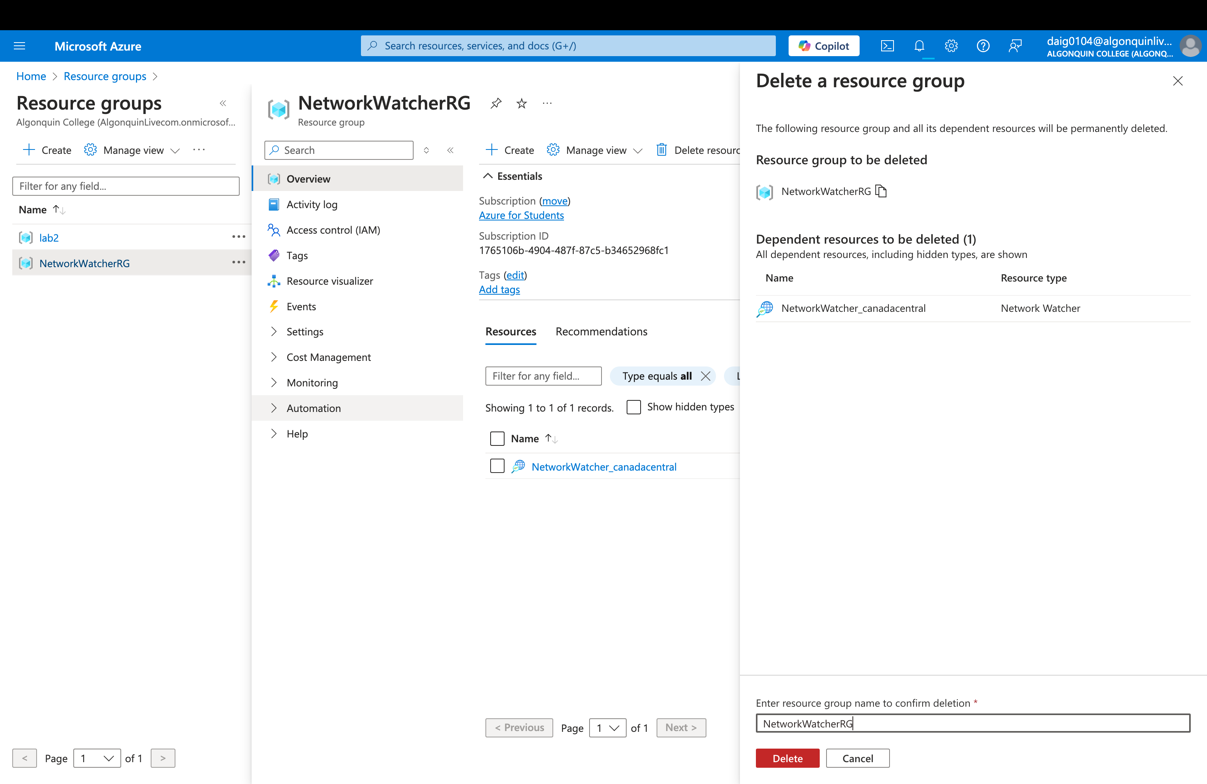


### Confirming that resources outside of the subnet cannot access the storage by attempting to access the file share within Azure portal. It seems access within the Azure portal is denied. (to get to this page its within the filesharestorage account > File Share > fileshare)

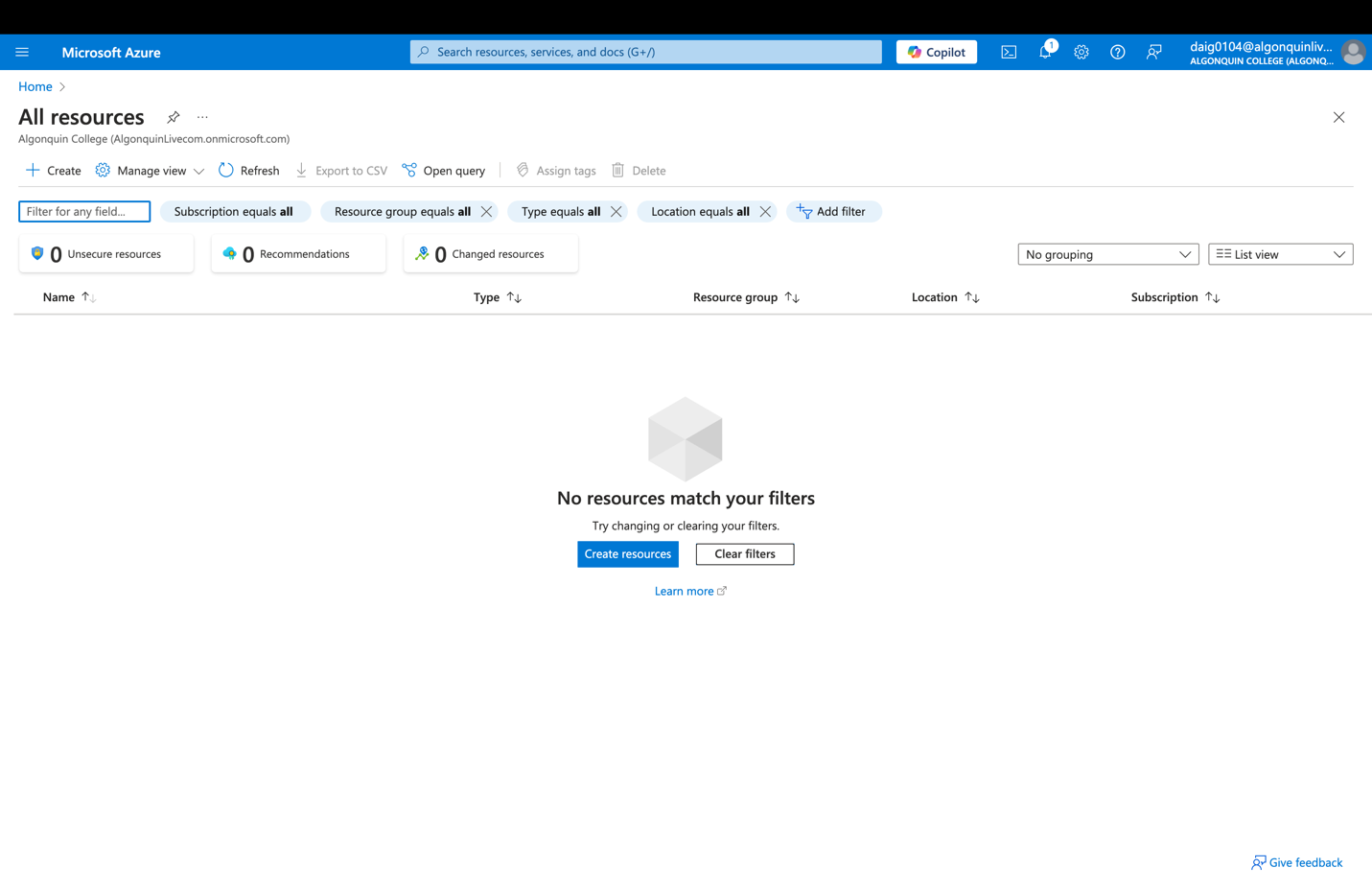


### Task 9: Cleaning up resources by deleting the two resource groups





### The end result of cleaning.

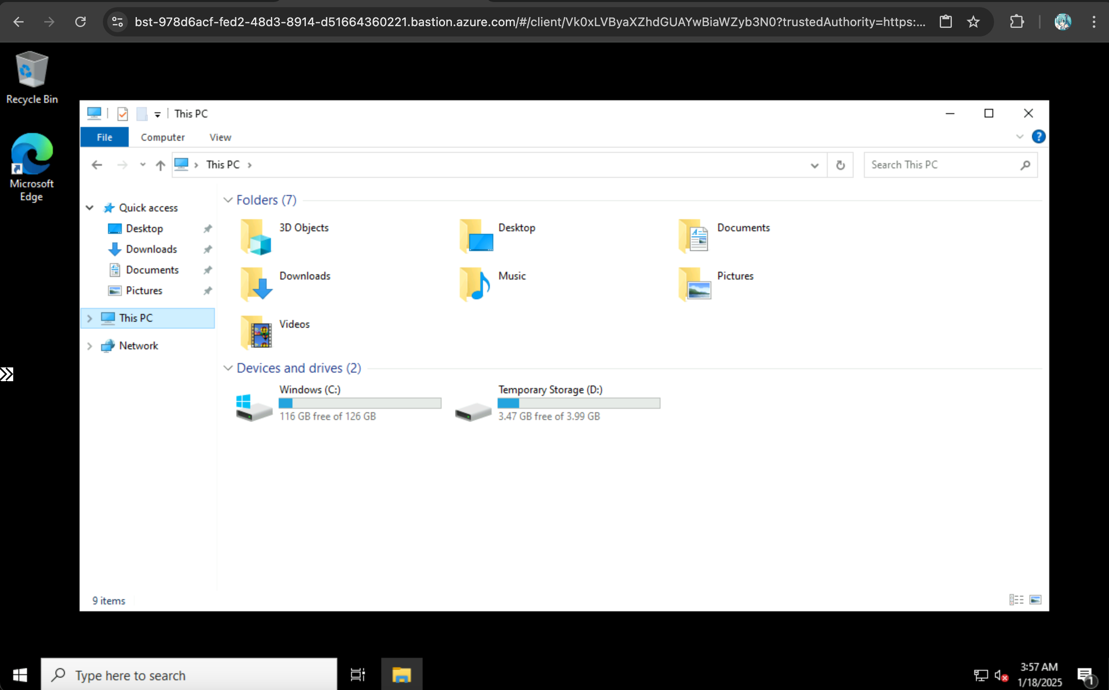


# Results:

The lab results are that I have successfully restricted network access from public networks whilst allowing access within the private subnet. Using the private subnet, I could map a new Z drive within the private VM. The public VM is denied access to map its Z drive. I also implemented a policy preventing resources from being deployed that are not from the Canada Central region.

# Conclusion:

What I found interesting was when mapping the Z drive within the private VM I could not see it within the visual file explorer. I had to check that it exists within the terminal with cd. Below is an example:



My theory is that since it is a file share, the drive is mapped outside the VM and does not apply to the file explorer.

Another learning experience is setting the priorities of the inbound/outbound rules; I found that the lower the priority, the more precedence the rule has. The results are as expected since there are three main restrictions to consider on why the public VM caused an error. One was AllowAnyRDP (Inbound), DenyAllInternet (Outbound) and AllowOutboundAzureStorage (Outbound).   
  
AllowAnyRDP allows the user to use RDP on both public and private VMs, DenyAllInternet denies the VM communication to the Internet, and AllowOutboundStorage allows the virtual network to communicate with the Azure storage. Due to the VM being public and the storage account being connected to the private VN, DenyAllInternet will deny any IP addresses that are outside of the private VN, which causes an error on the public Virtual Machine.

# Works Cited

Microsoft. (2024, August 16). *Tutorial: Restrict network access to PaaS resources with virtual network service endpoints*. Retrieved January 2025, from Microsoft Learn: https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources?tabs=portal

Microsoft. (2024, December 11). *Virtual network service tags*. Retrieved January 2025, from Microsoft Learn: https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview