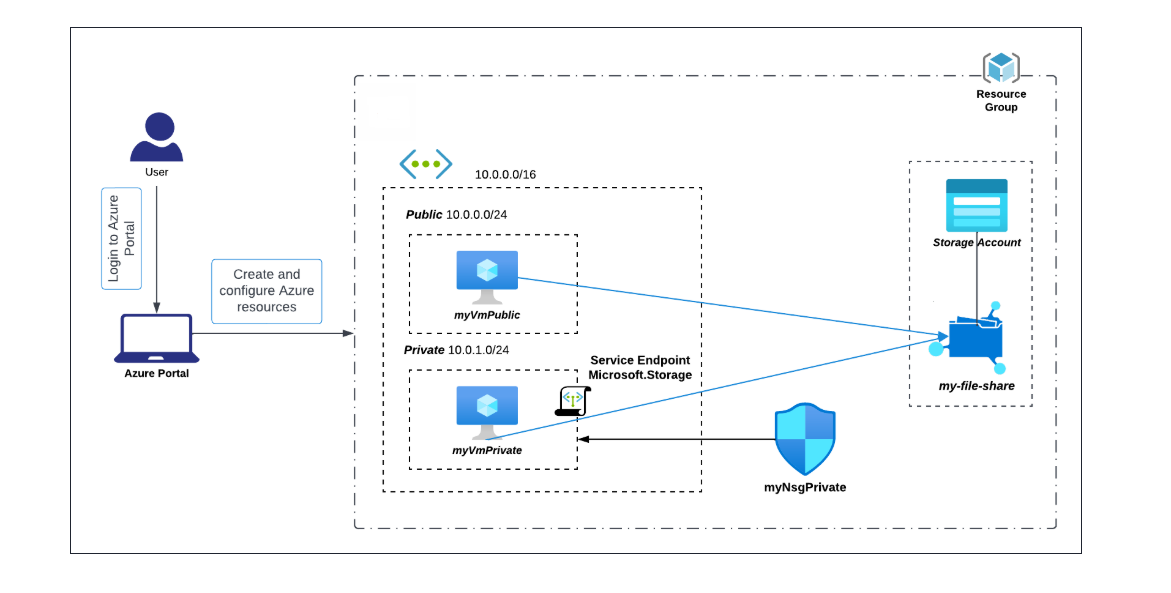
**Service Endpoint and Securing Storage**

The purpose of this lab is to gain hands-on experience with core Azure networking and storage services. The lab focuses on learning how to:

* Create and configure **virtual networks** and **subnets** in Azure.
* Use **Network Security Groups (NSGs)** to control inbound and outbound traffic.
* Configure **service endpoints** to securely access **Azure Storage Accounts** from specific subnets.
* Deploy **virtual machines (VMs)** into isolated subnets and test connectivity.
* Understand how Azure's **firewall and network policies** impact resource accessibility.
* Use **Azure Files** to create and map a **file share** to a Windows VM.

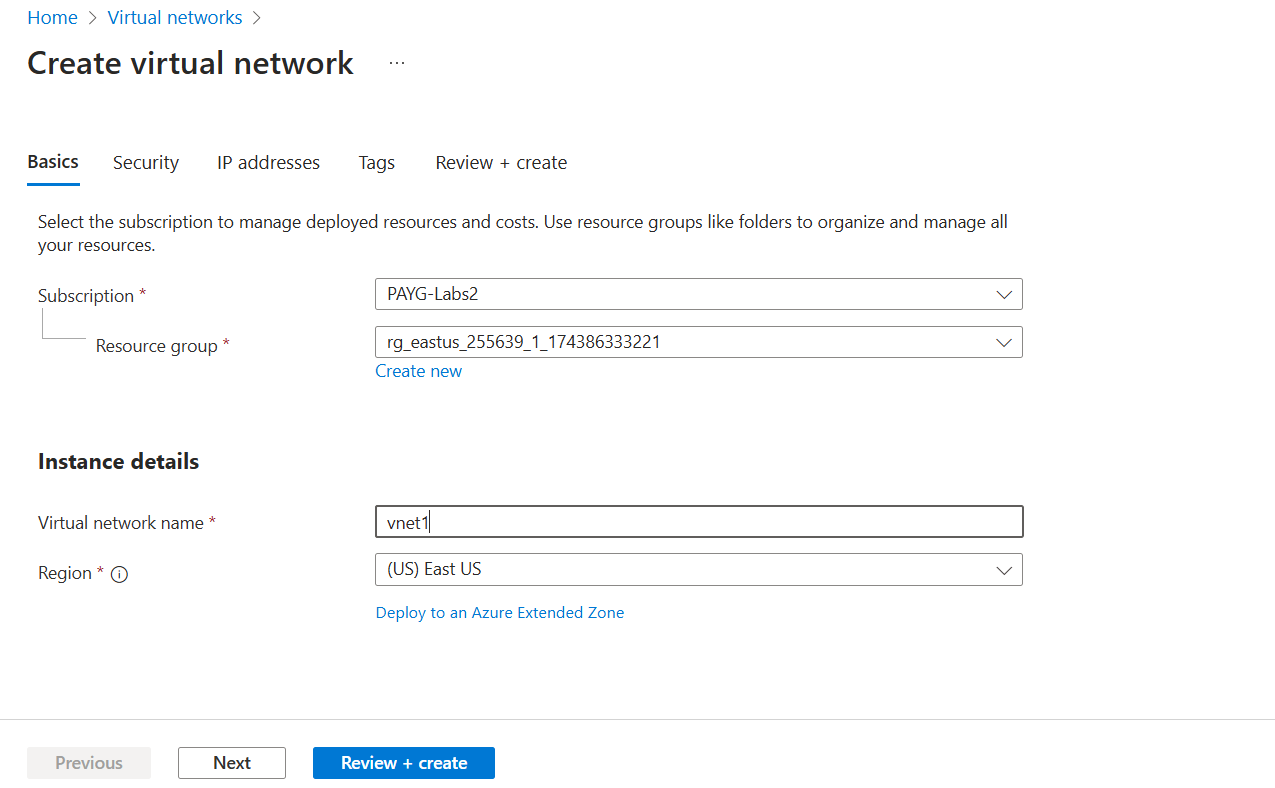
This exercise helps build foundational knowledge for managing secure, scalable, and well-structured cloud environments on Microsoft Azur

**Architechure:**

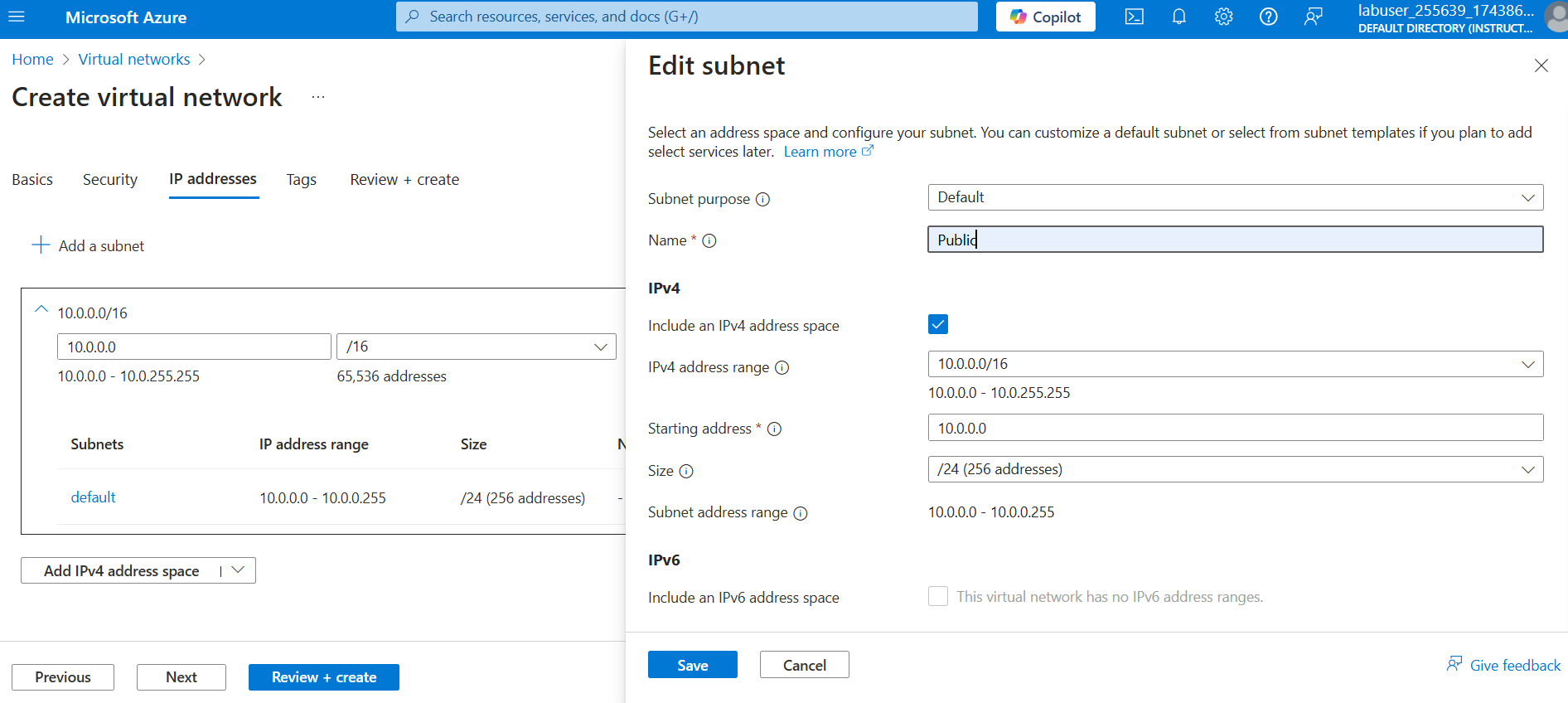


**Task1: Sign in to Azure portal**

**Task2: Creating azure vnet**



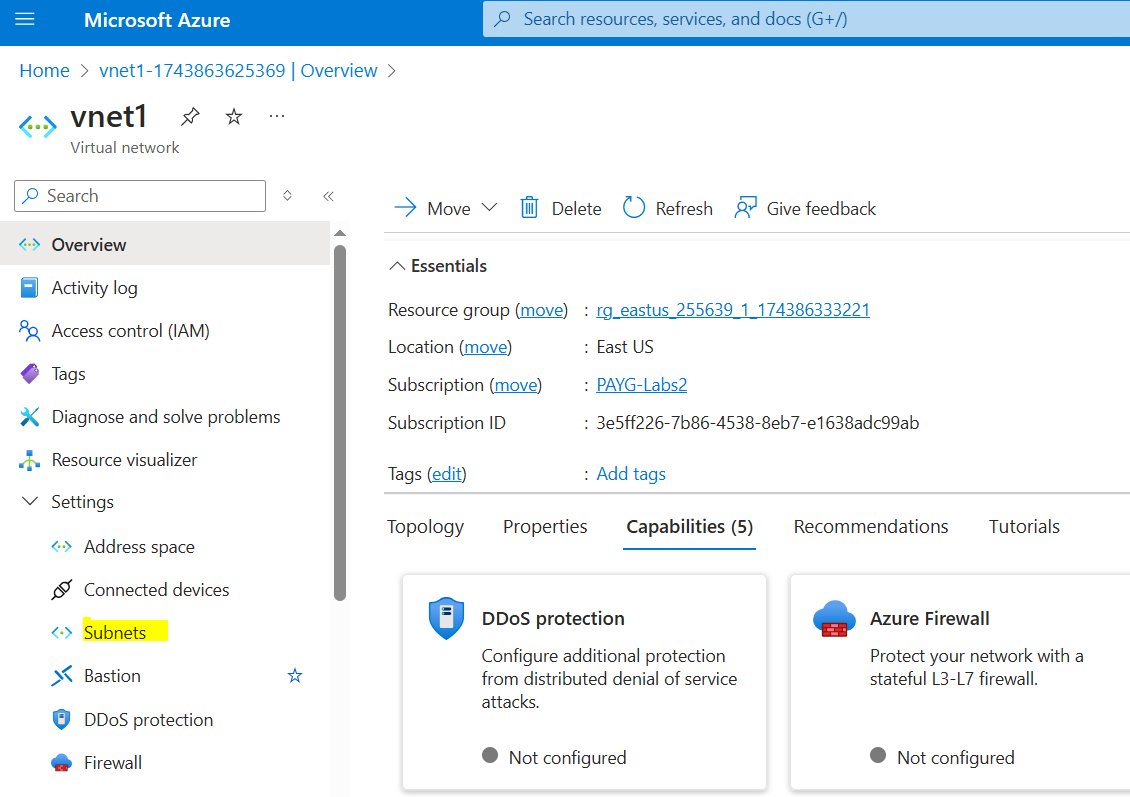
In the IP addresses section, under Subnets click on edit or create new on **Public** subnet



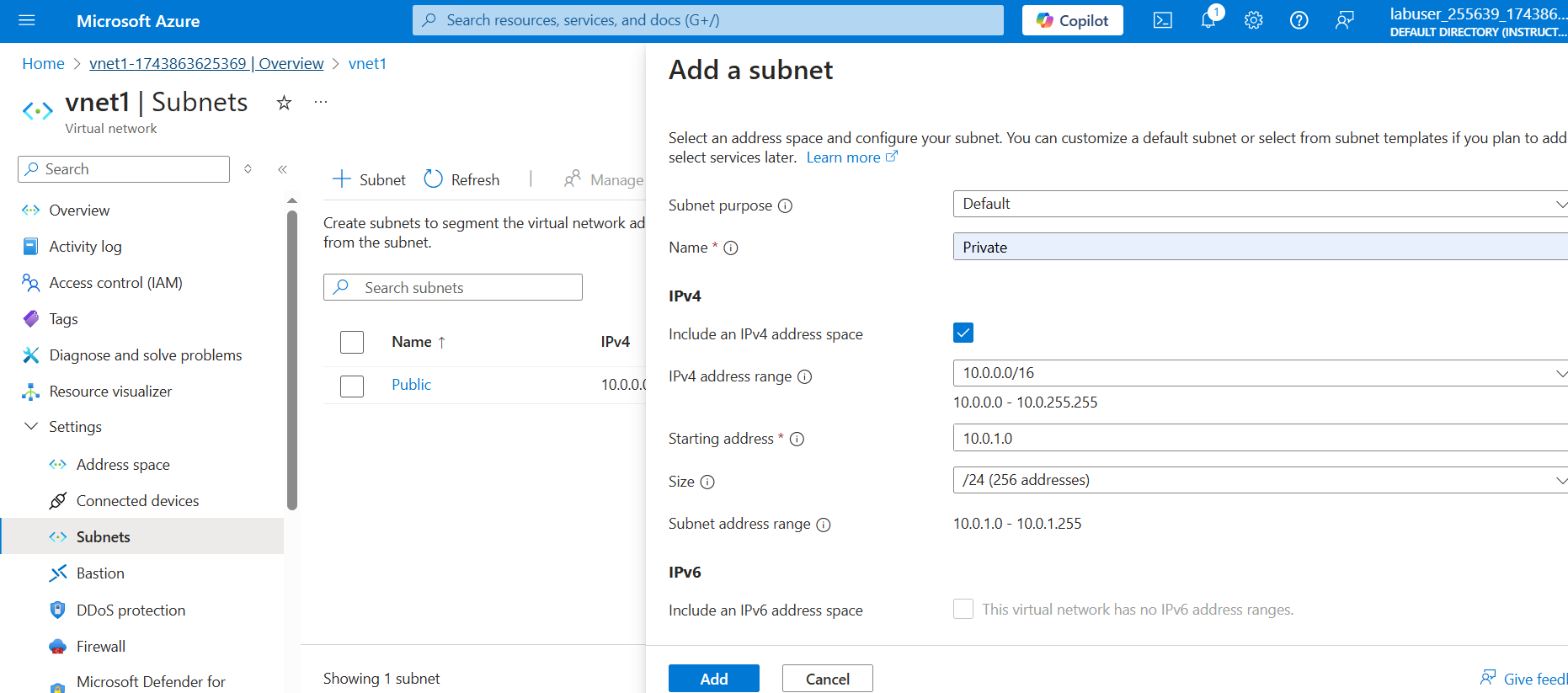
Save and than click on **Review+create**

## **Task 3: Add a subnet and configure a storage endpoint**

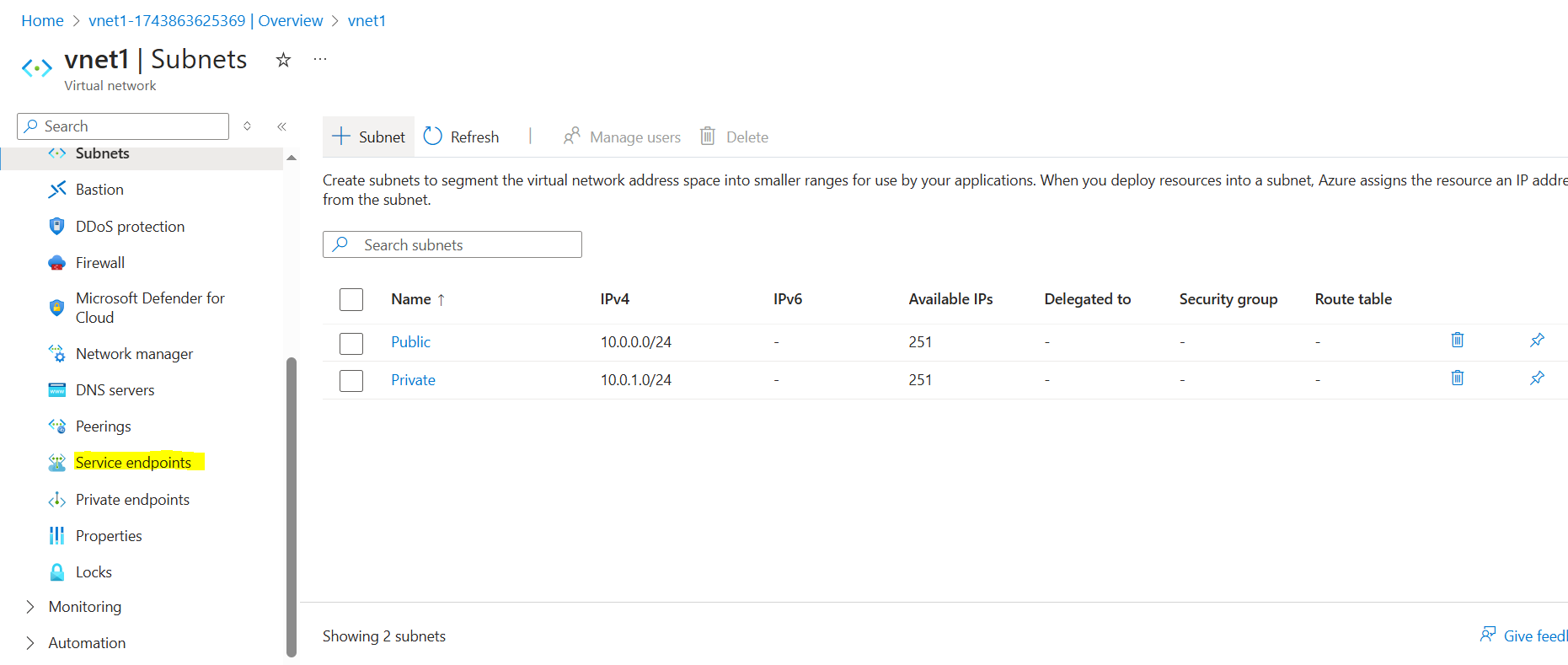
Now in the **vnet1** under settings click on **subnets**



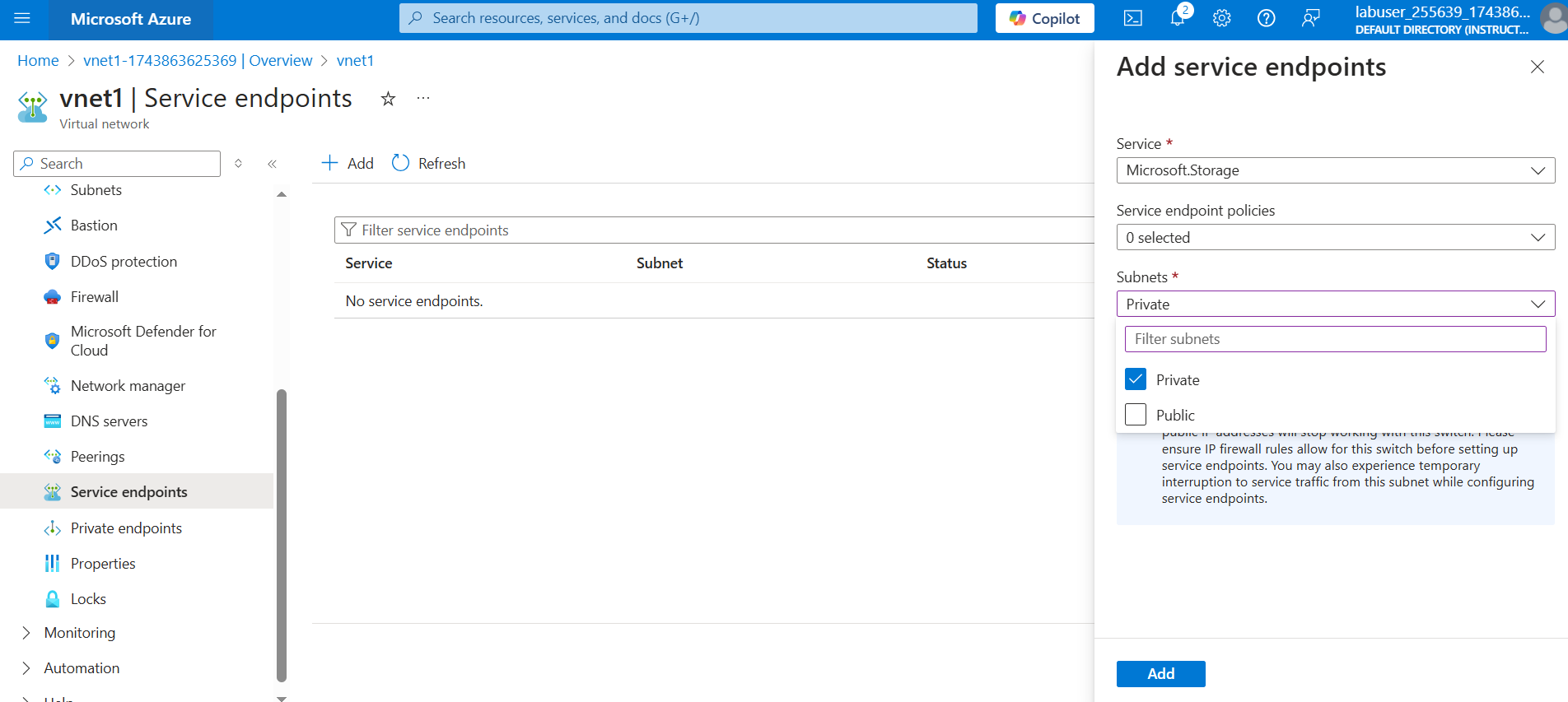
Create new subnet **Private** with the details as shown in the image



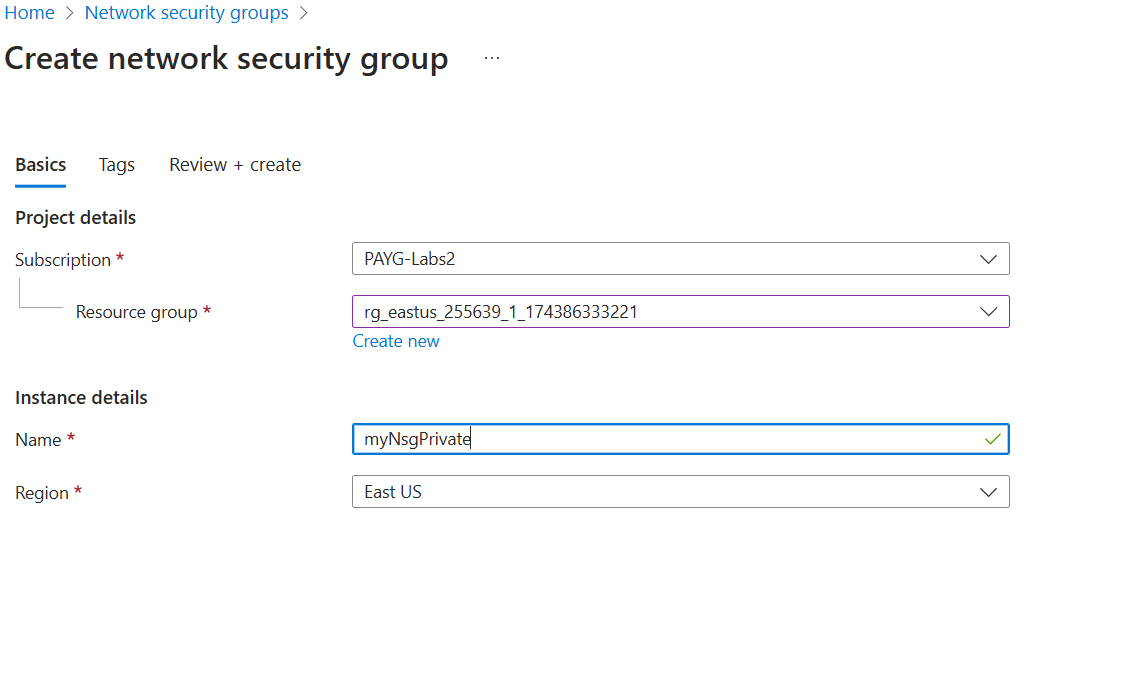
Now create service endopoint



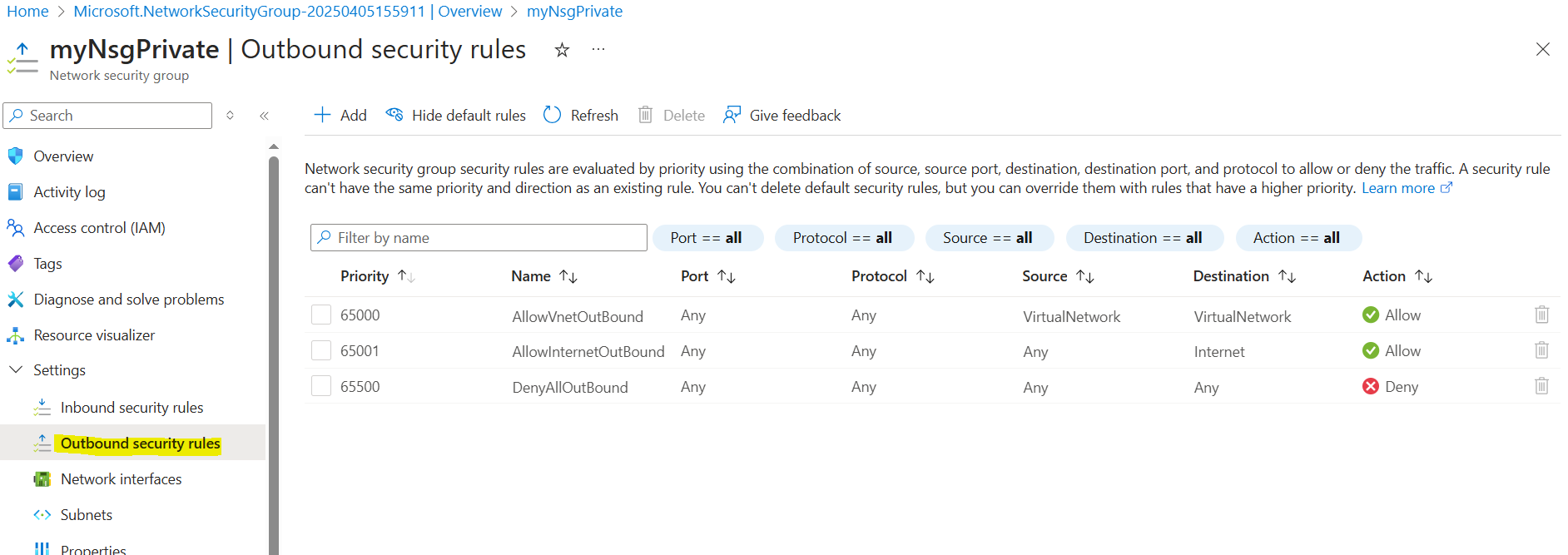
with the details as given in the image



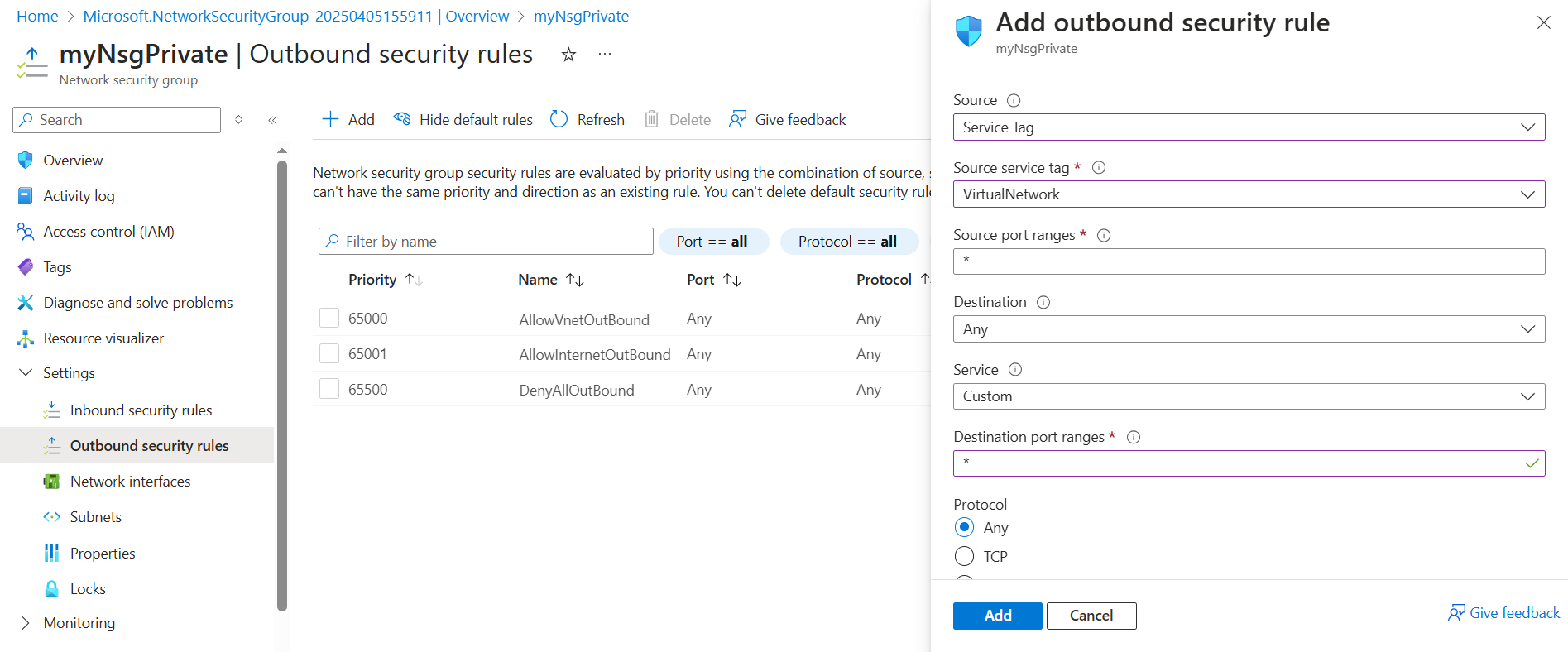
## **Task 4: Configure an NSG to restrict access to the subnet**

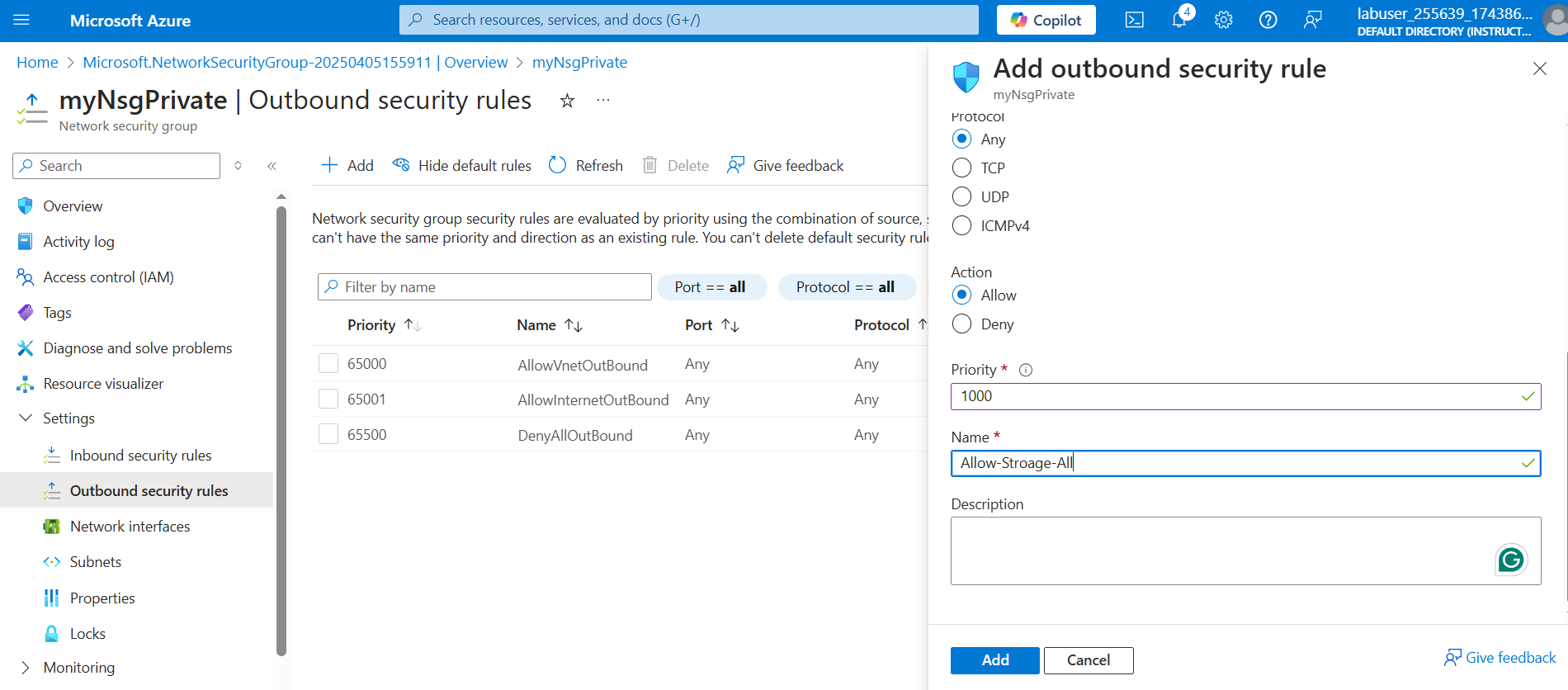


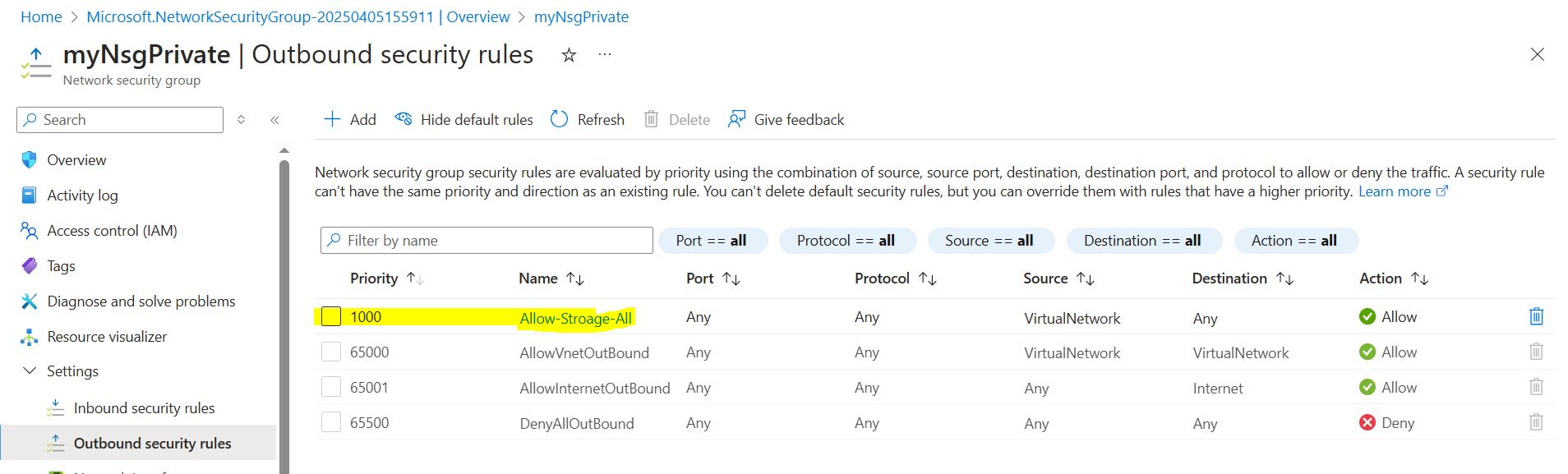
For outbound security rules



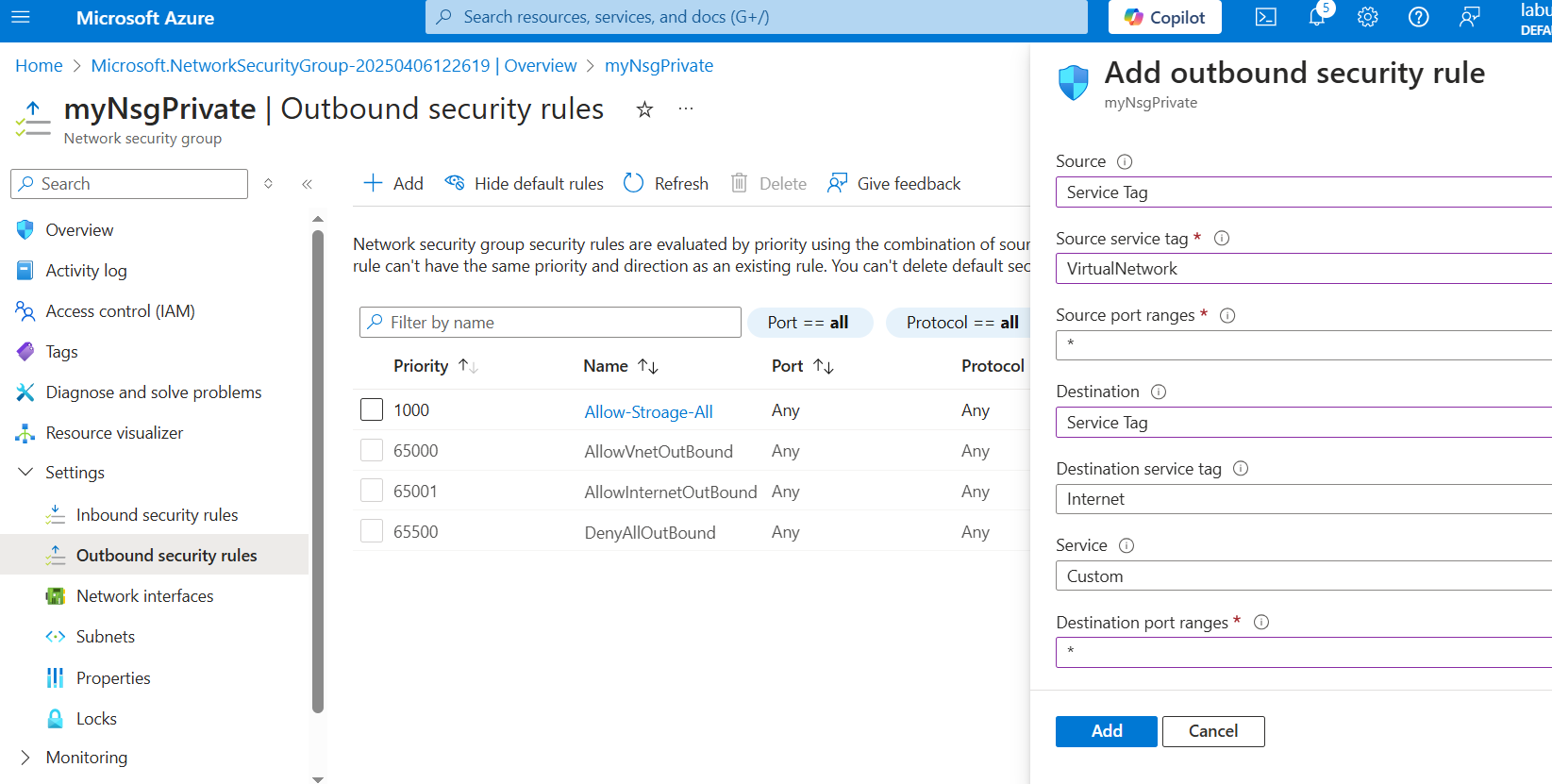
detais given in the image, for accessing subnet under this resources by storage account

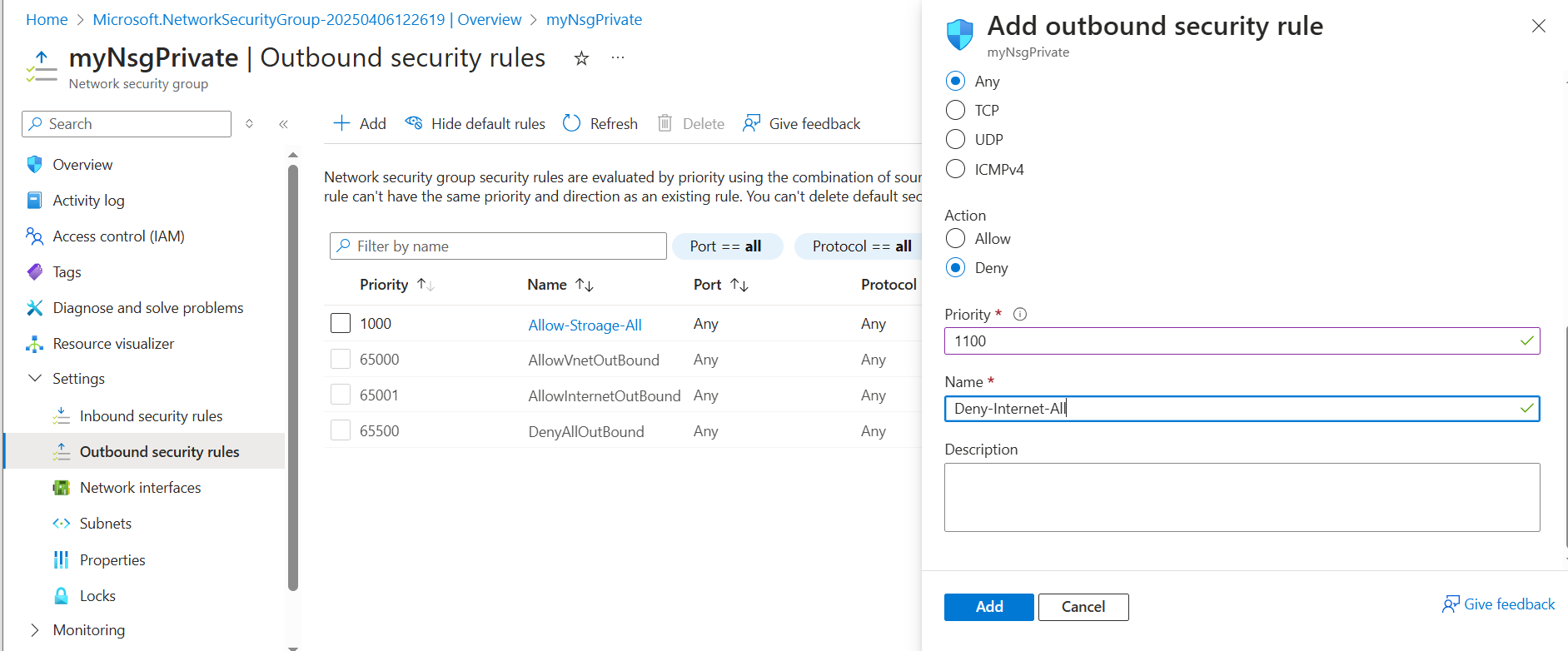




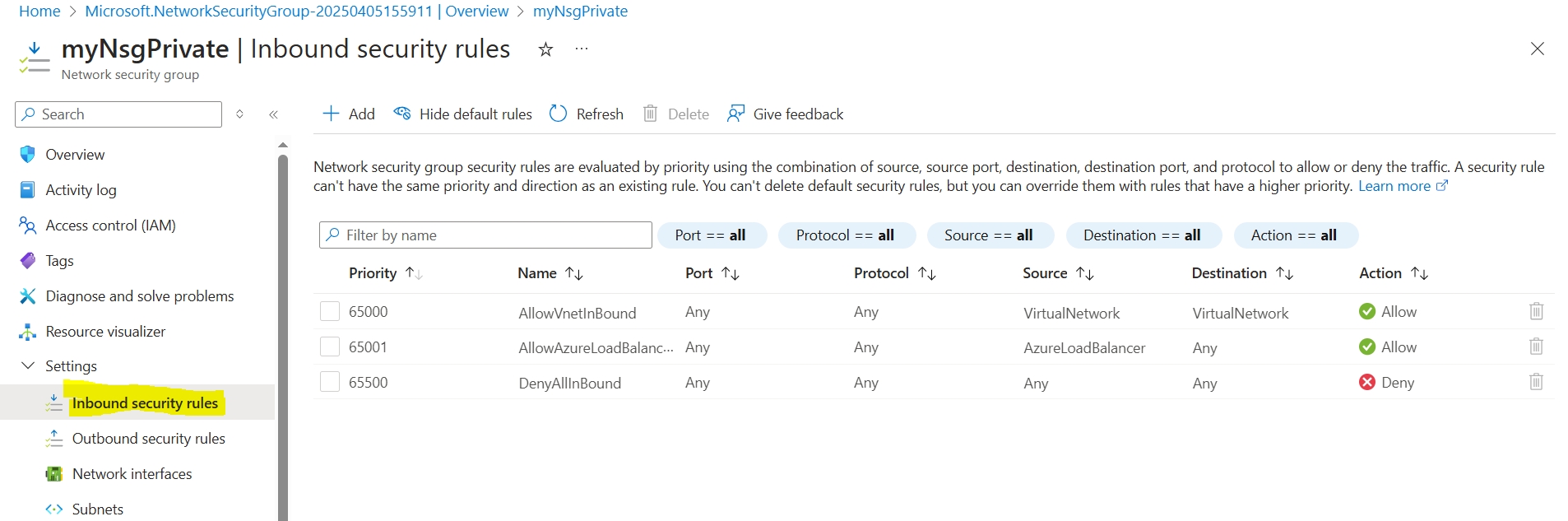


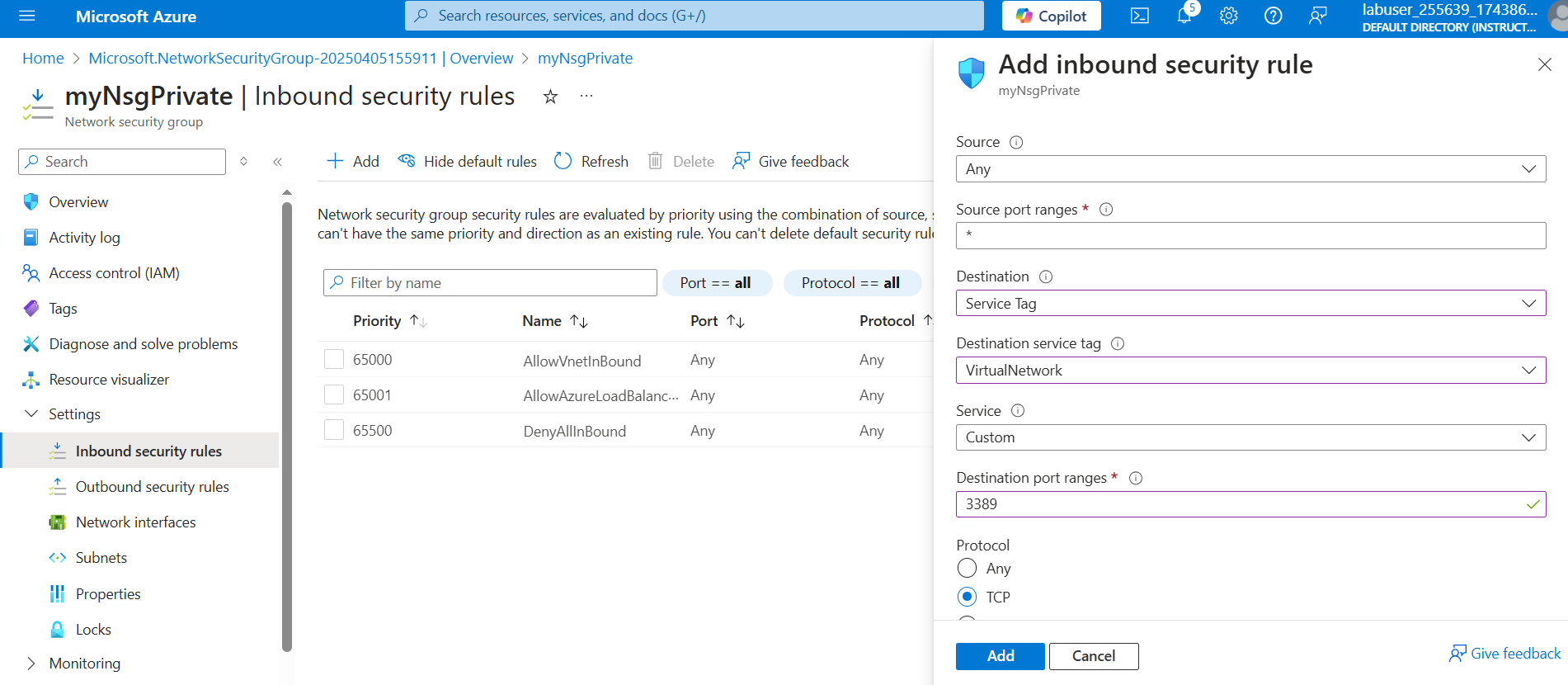
Configuring another NSG do deny all internet traffic

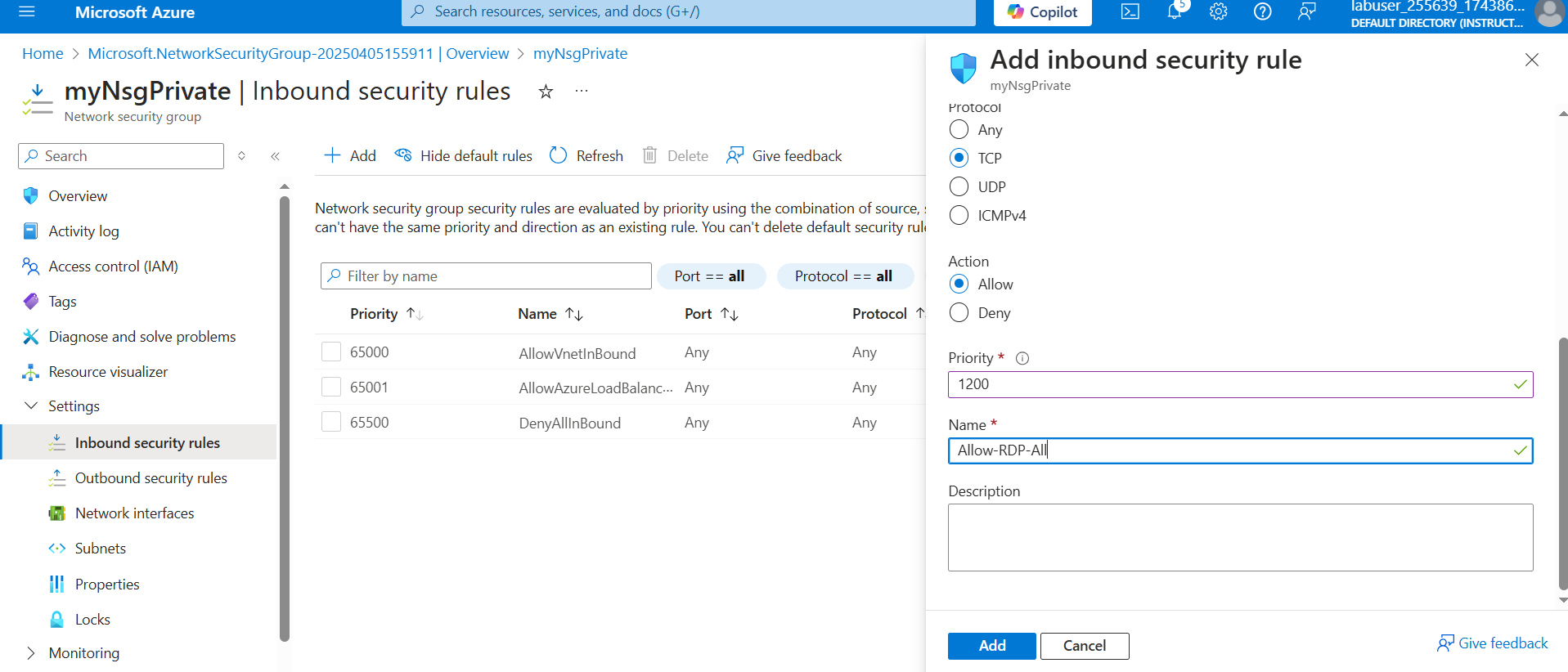




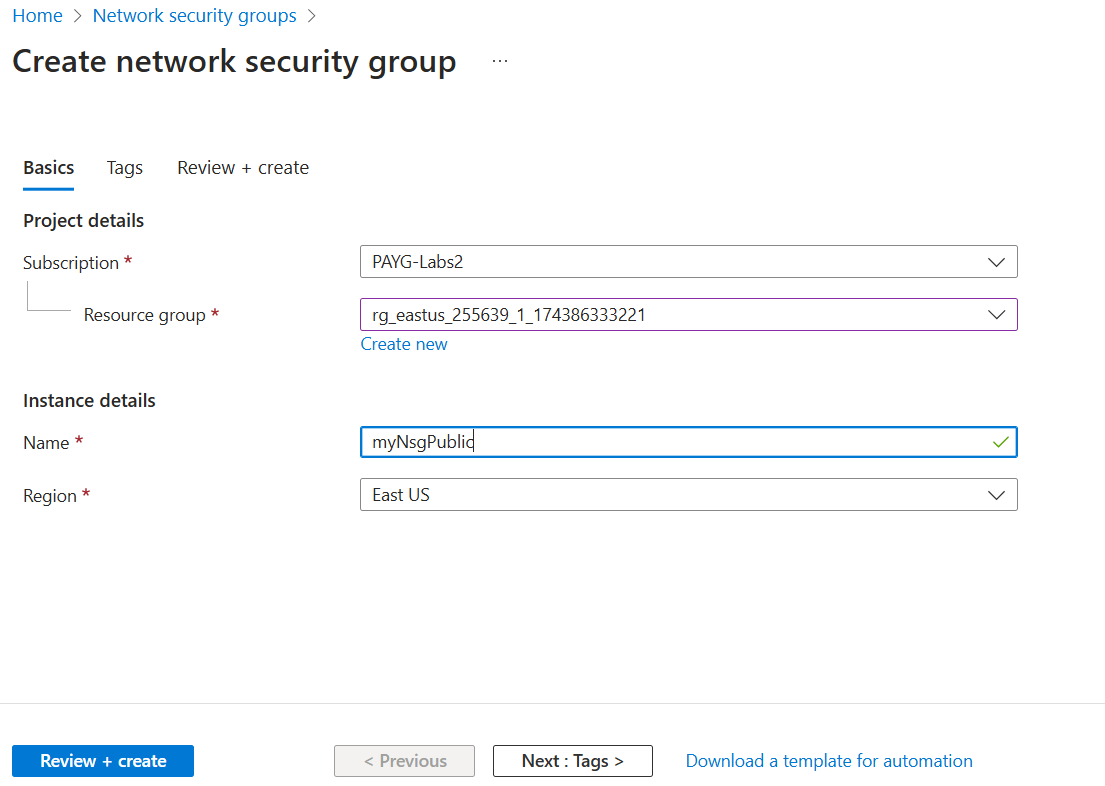
Now configuring inbound for subnet to allow for RDP on port 3389

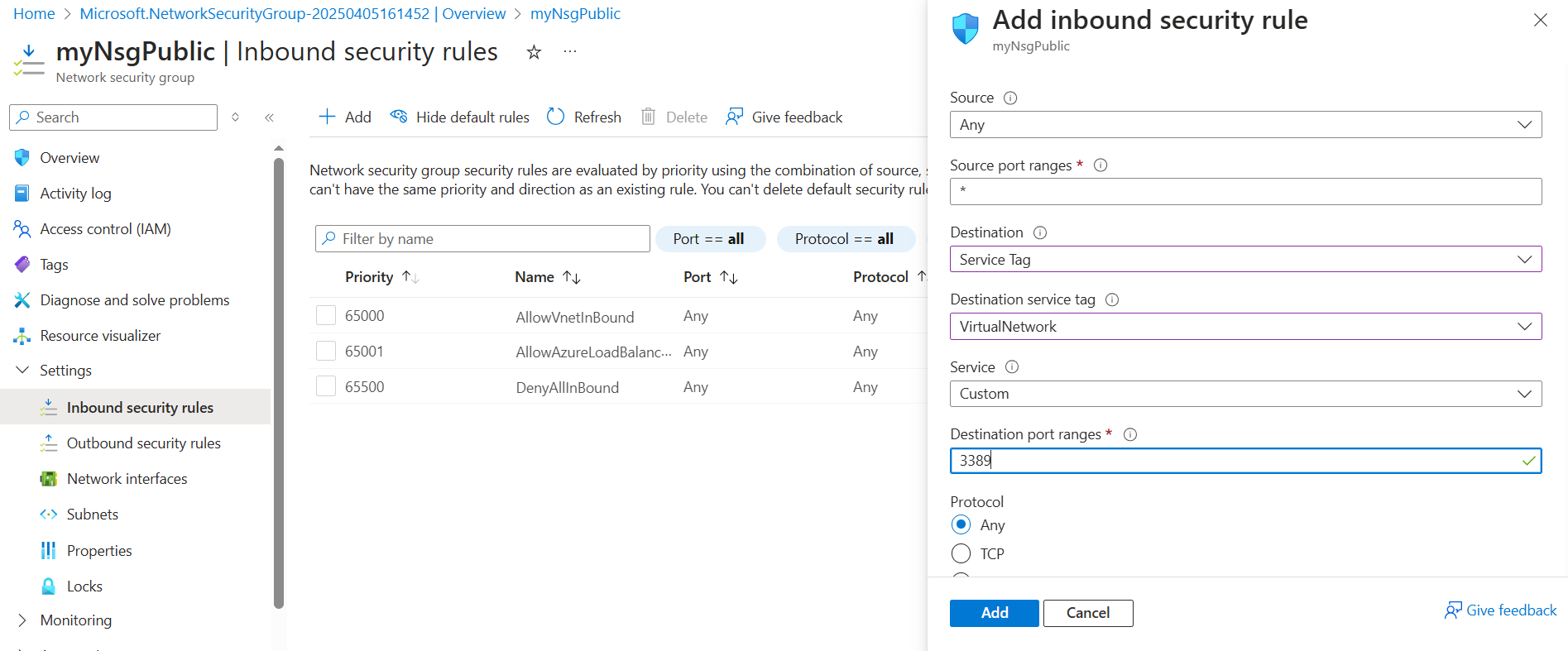


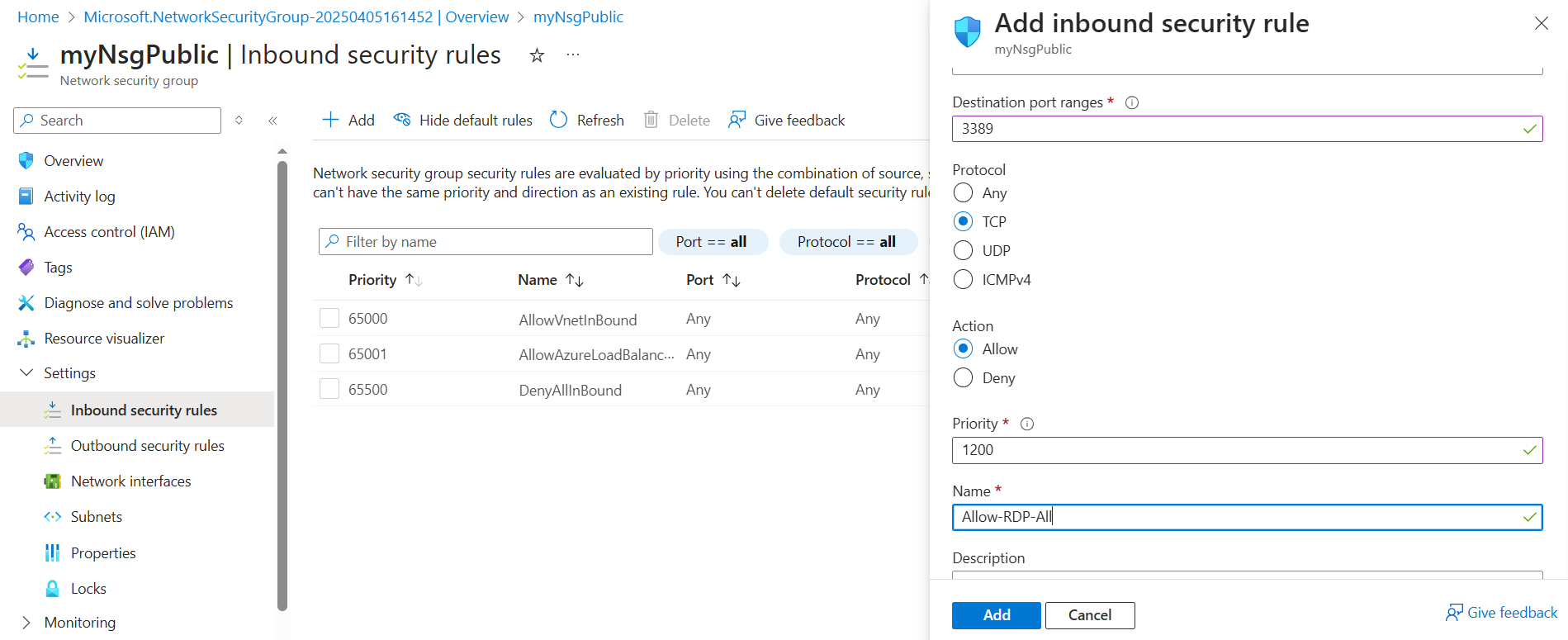




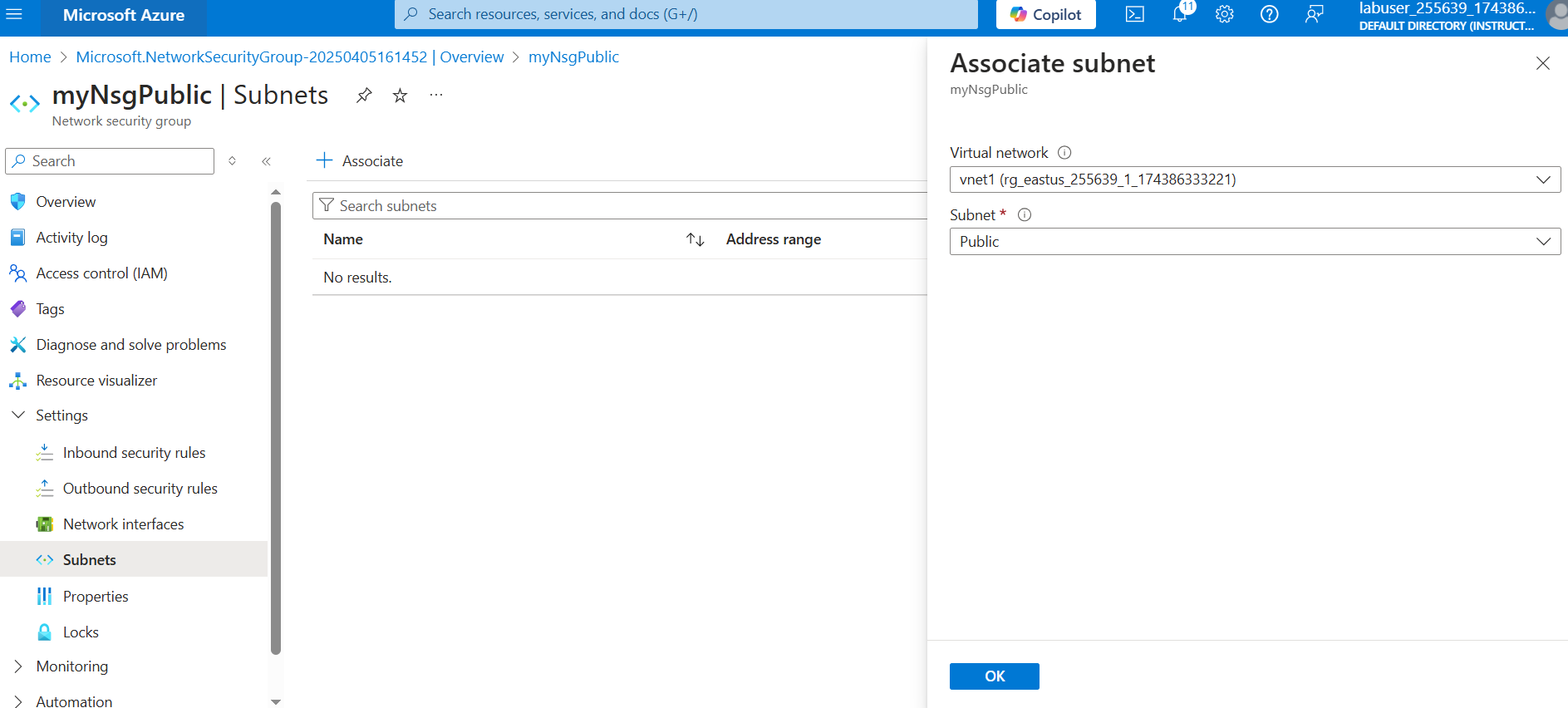
## **Task 5: Configure an NSG to allow rdp on the public subnet**



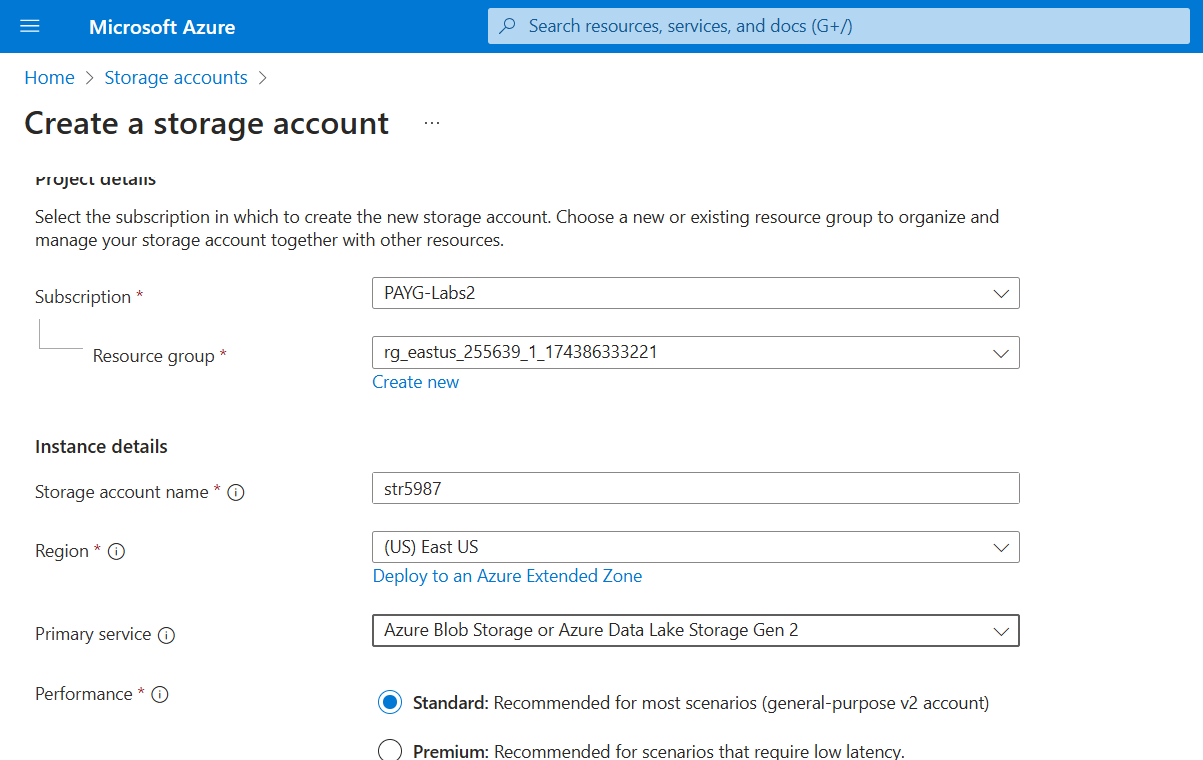


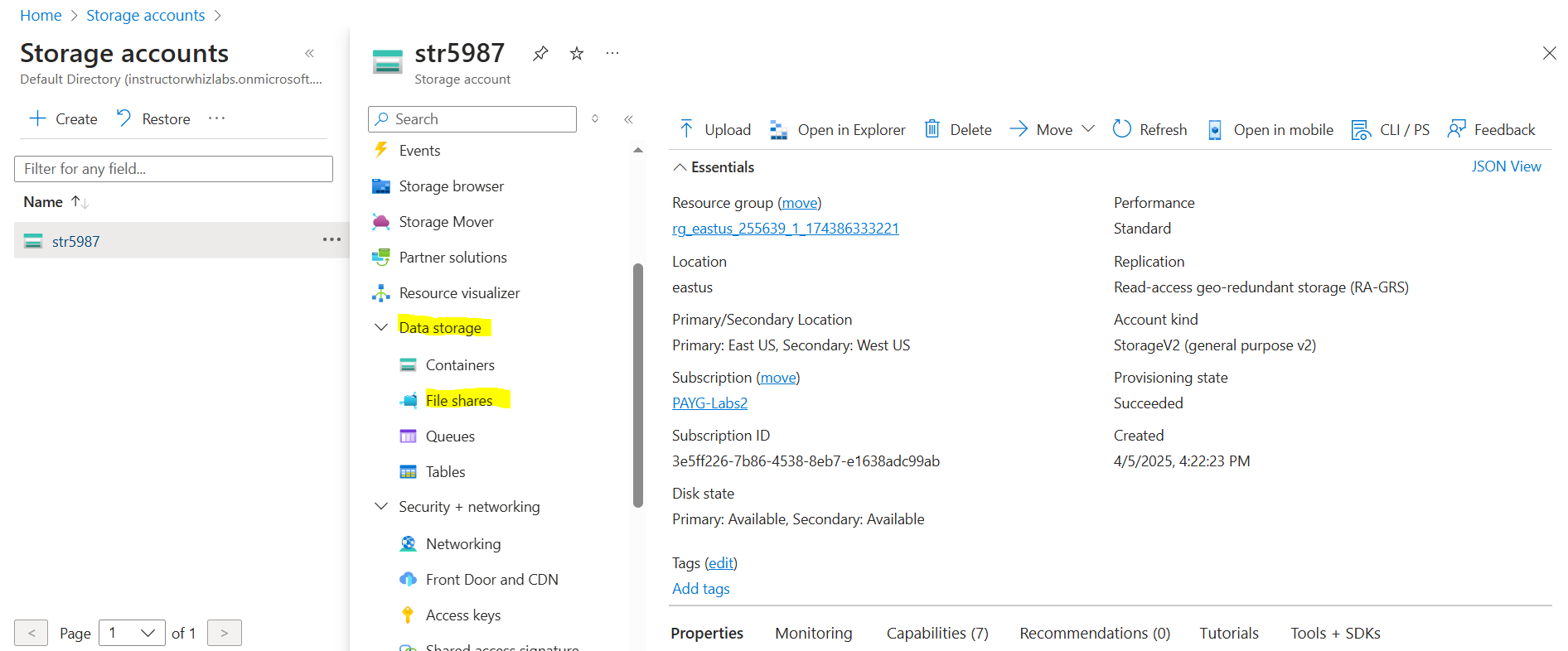


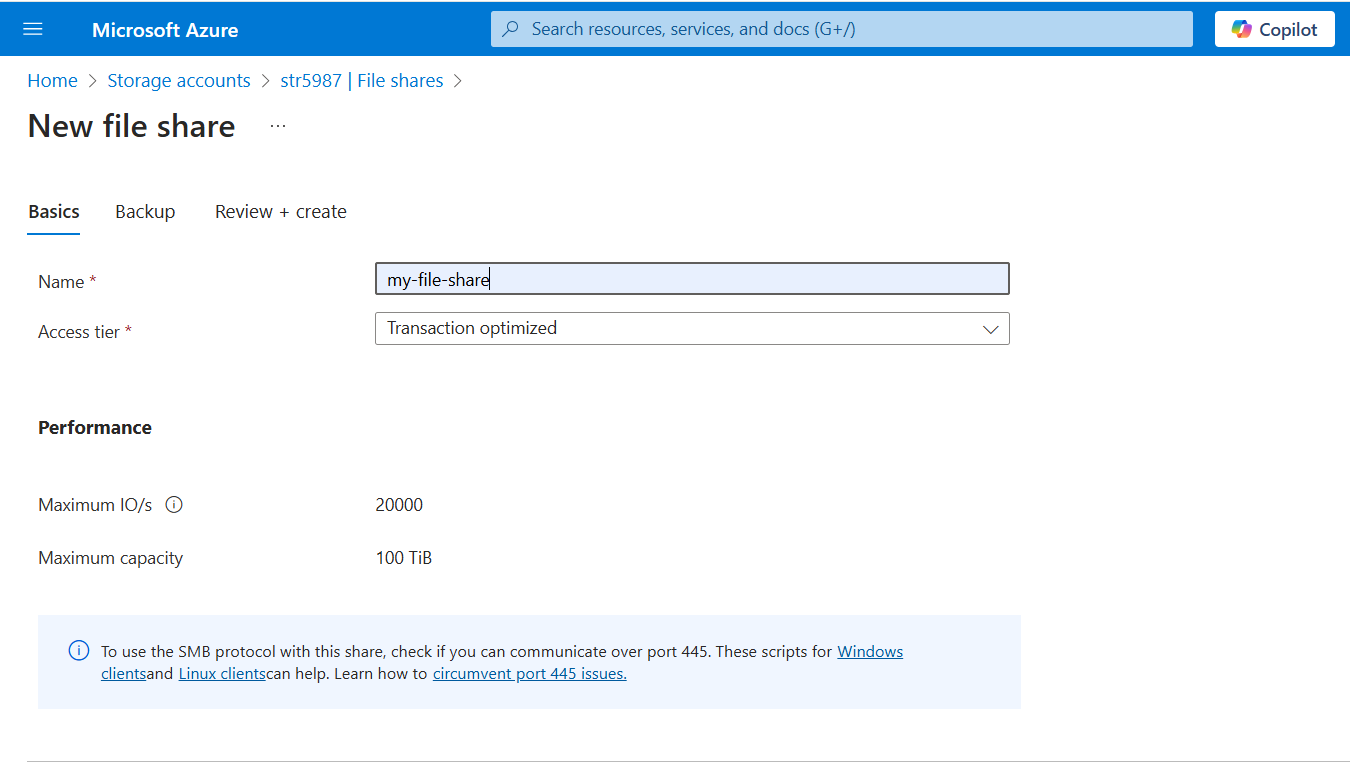
Accossiating security group to public subnet.

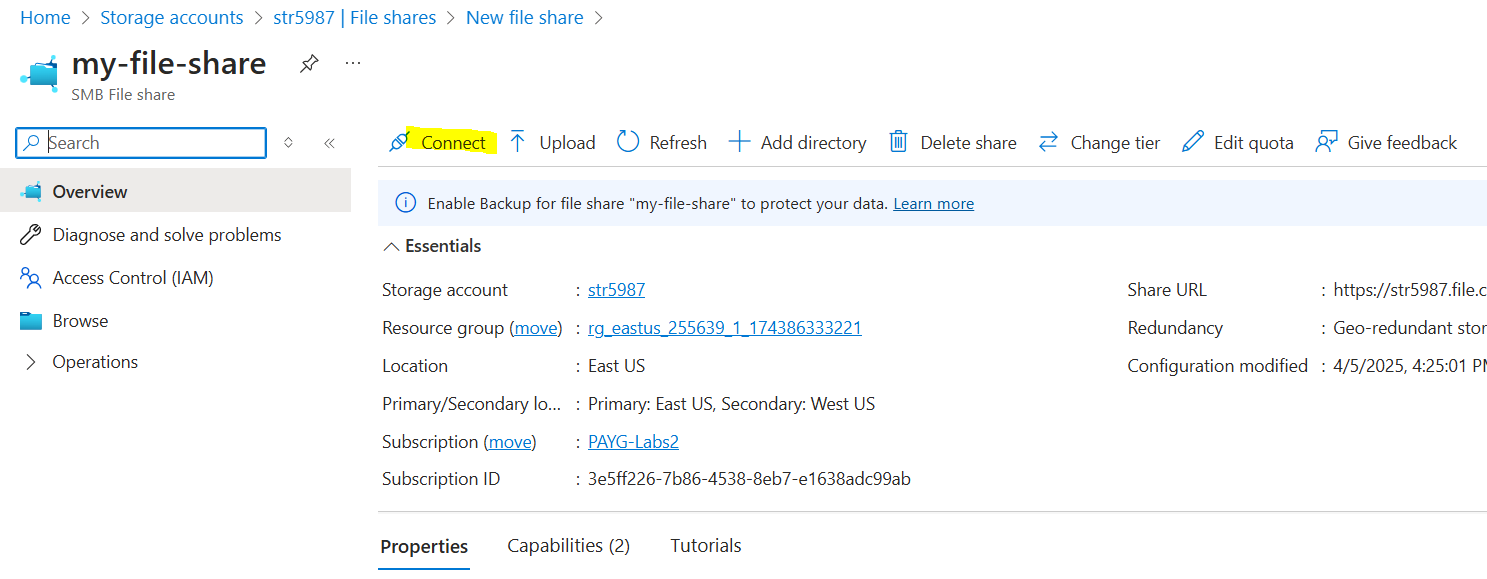


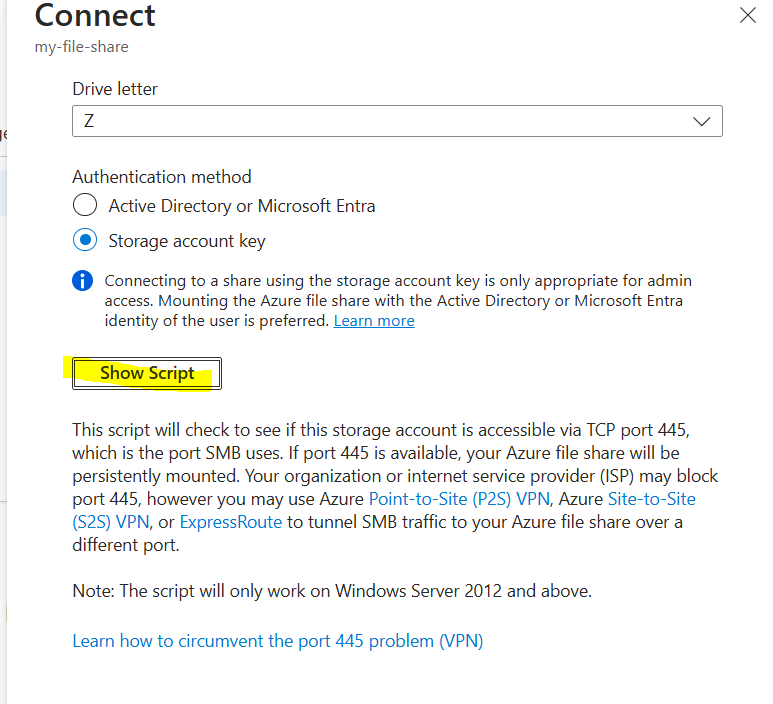
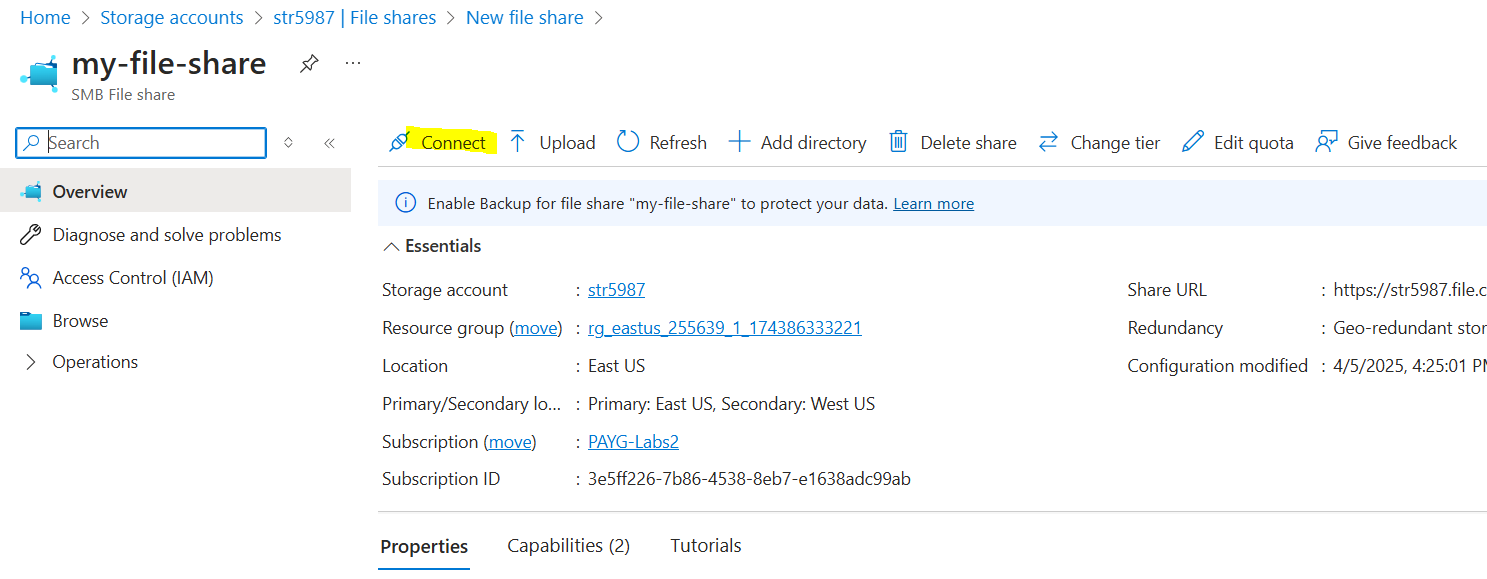
## **Task 6: Create a storage account with a file share**

****

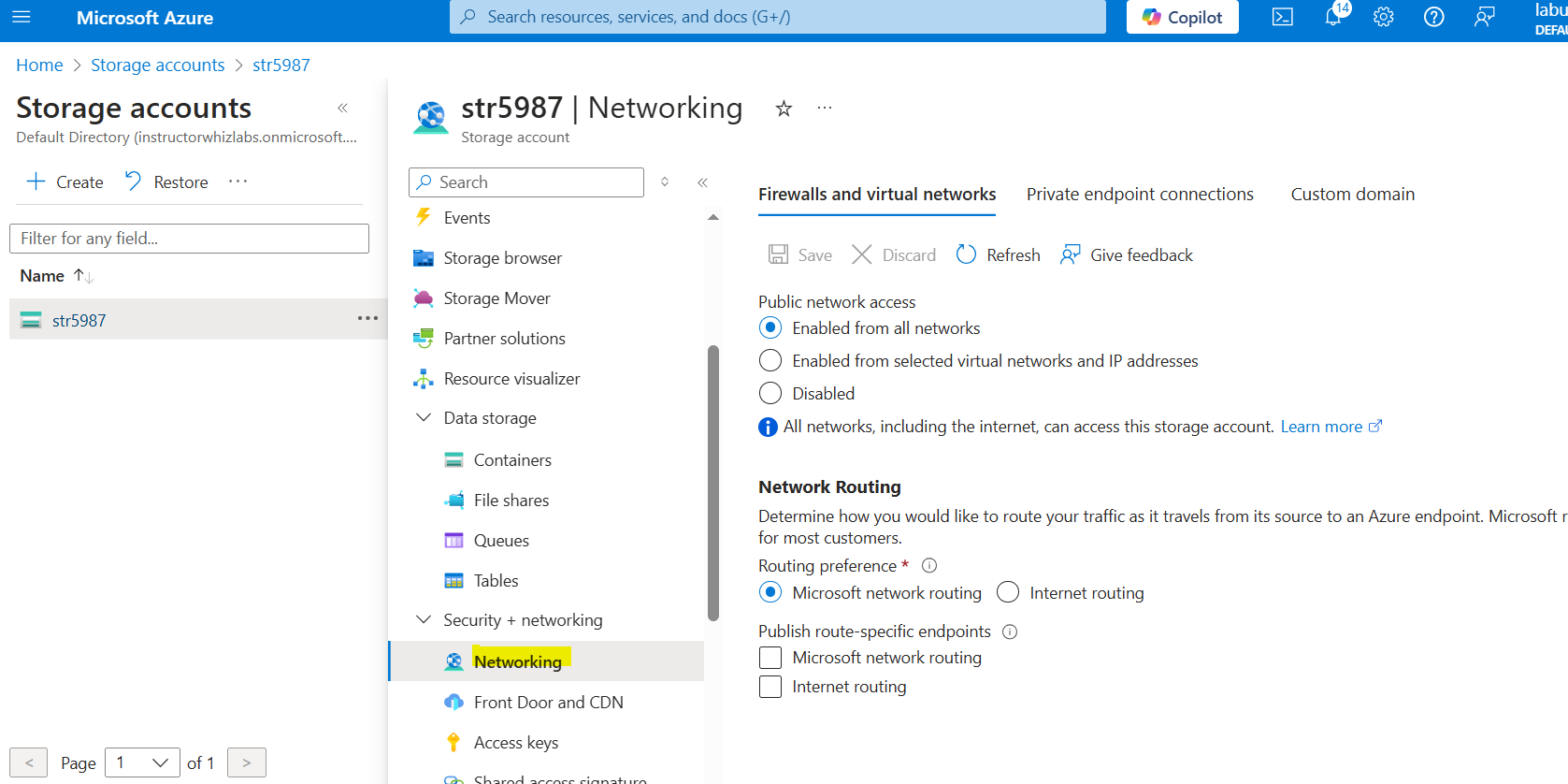
****

****

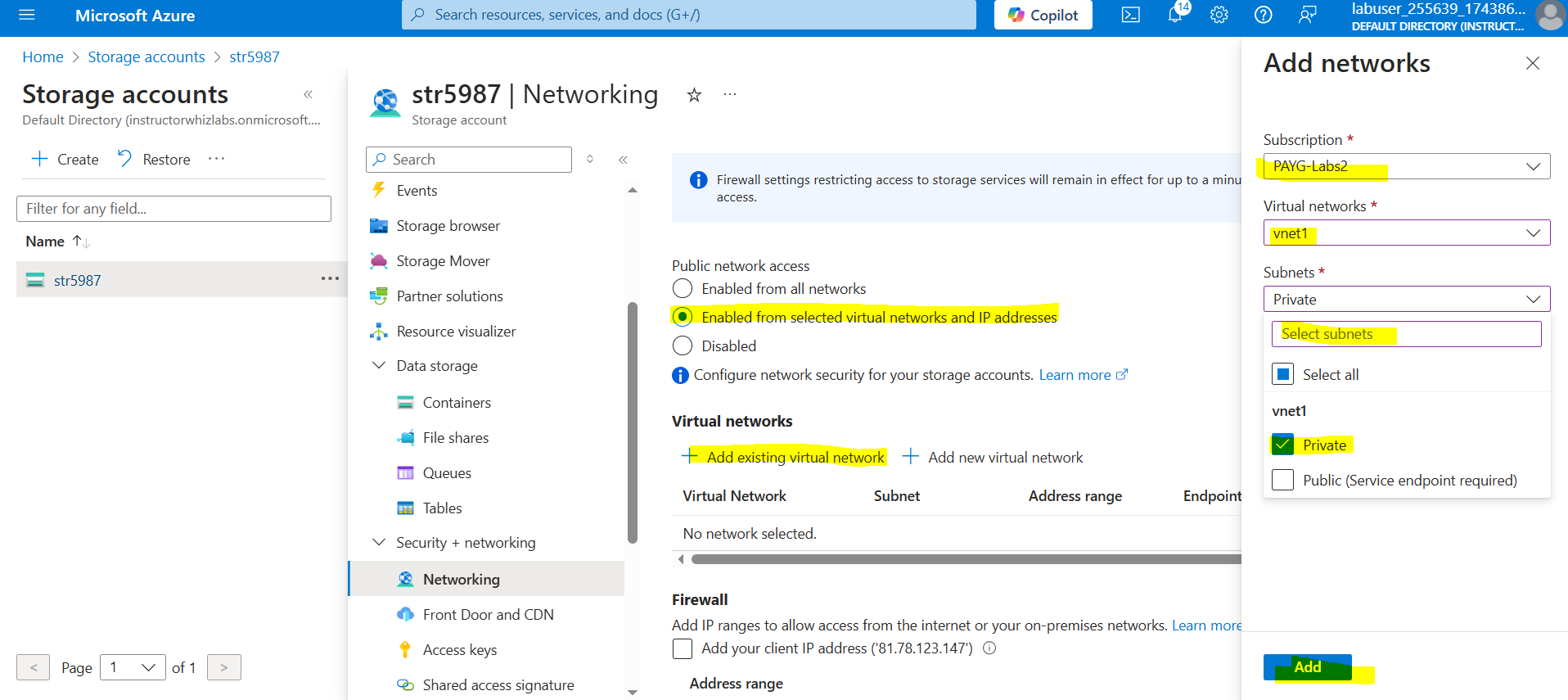
****

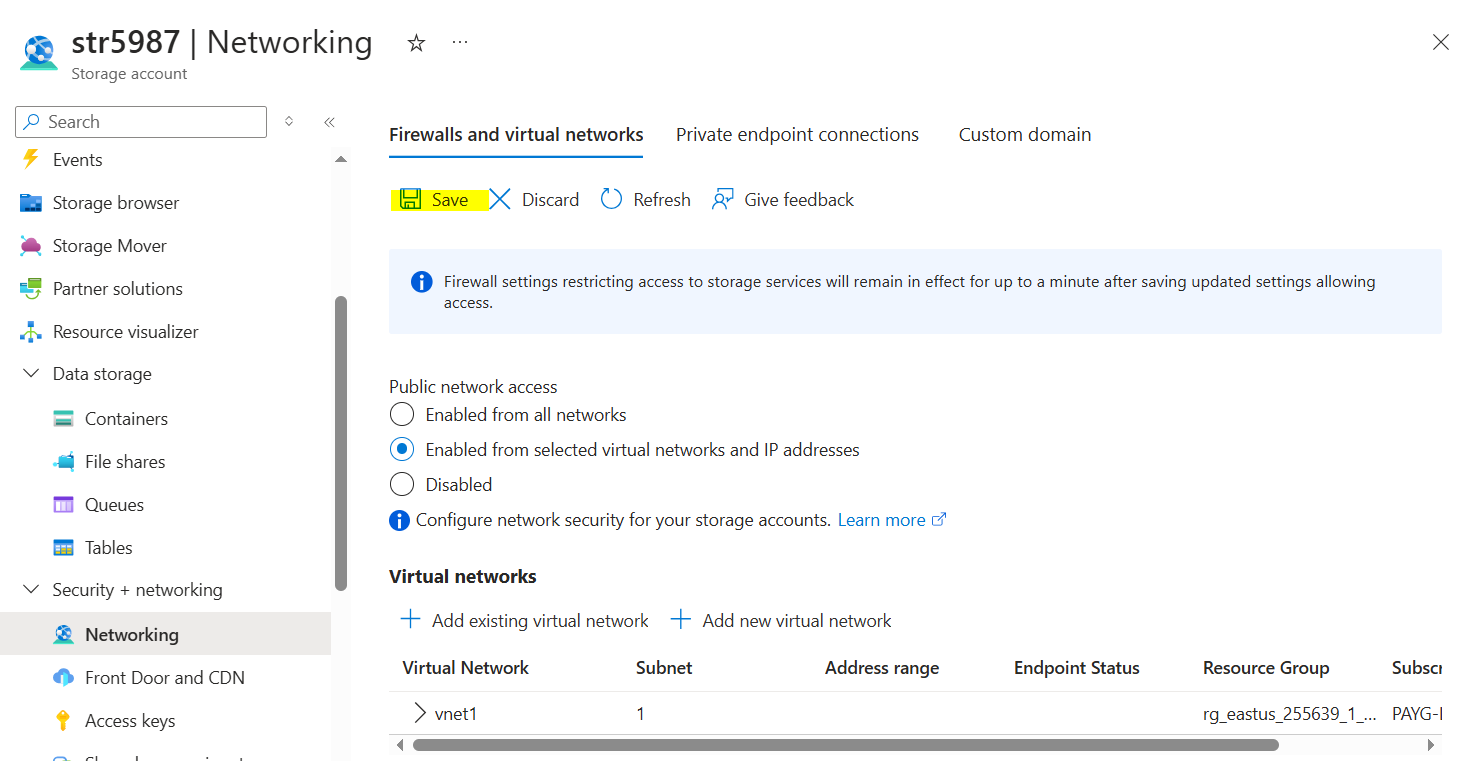
****

**Copy that script some where, will use later in the vm to attach or test connectivity**

****

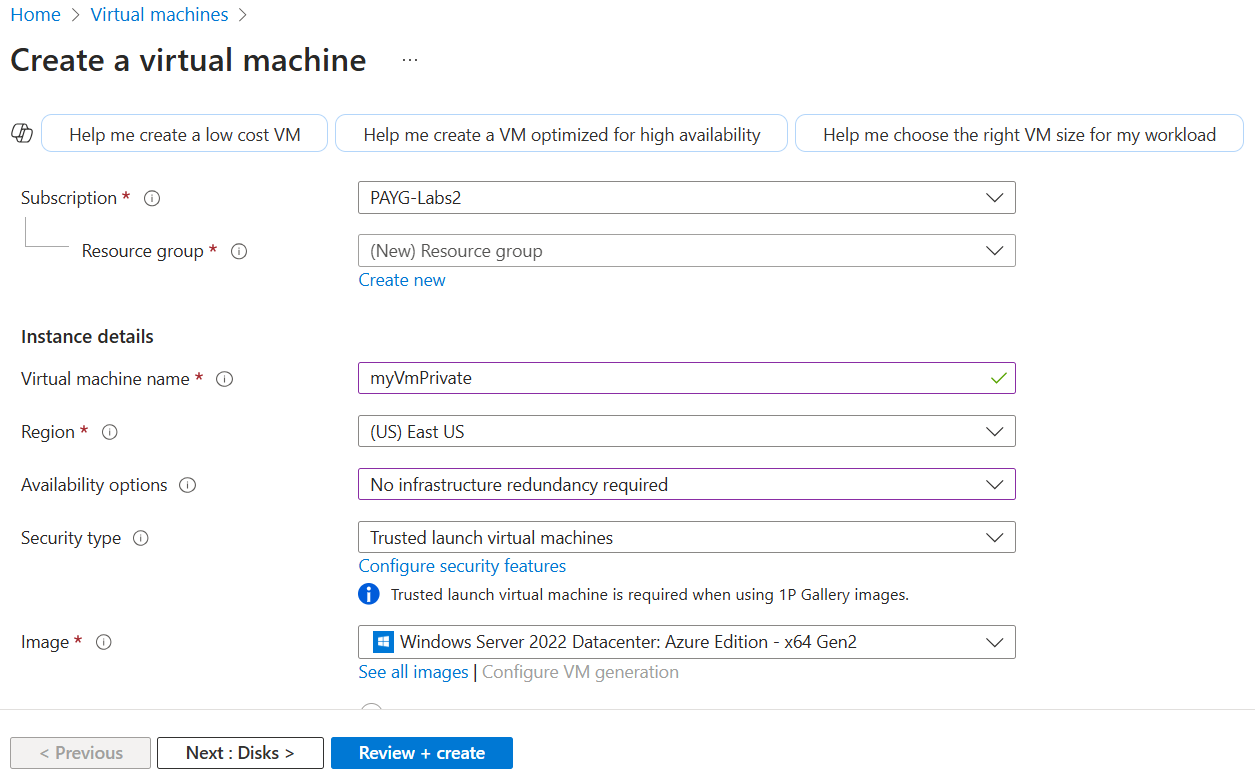
**Now I am restricitng my storage account to allow connection from specefic part and later i will check it from different resources**

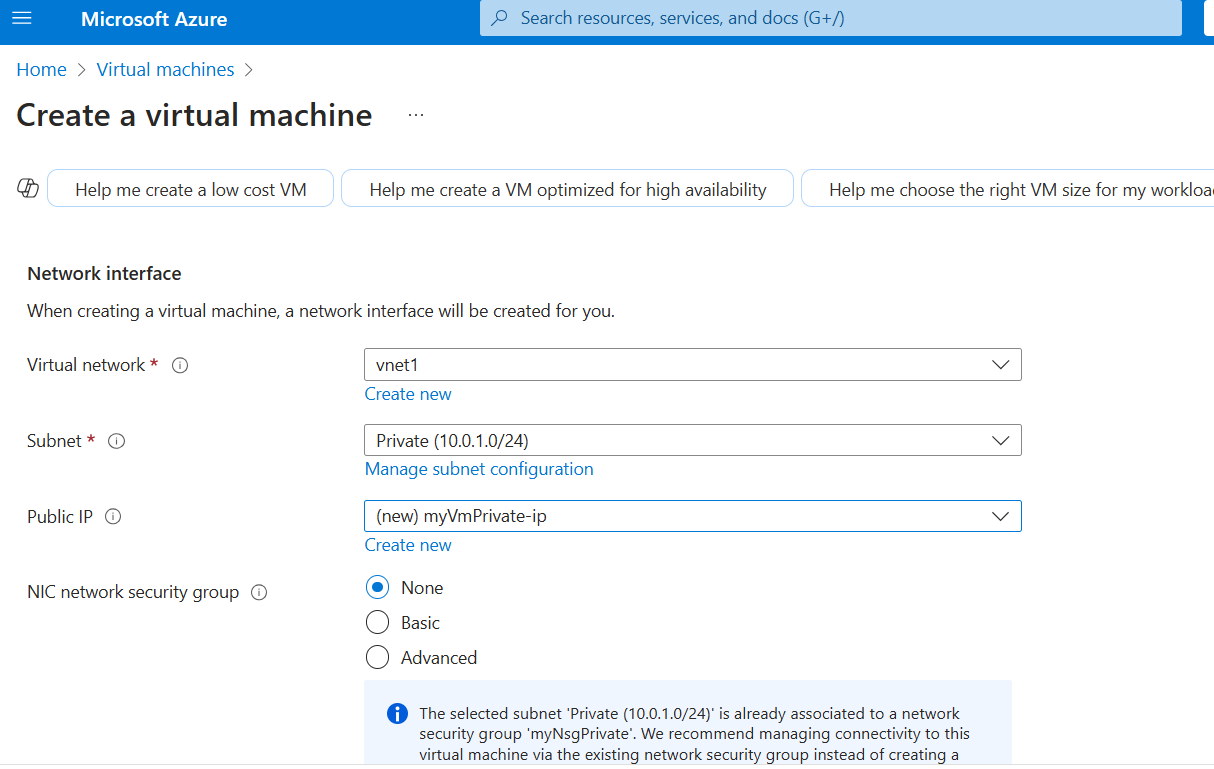
****

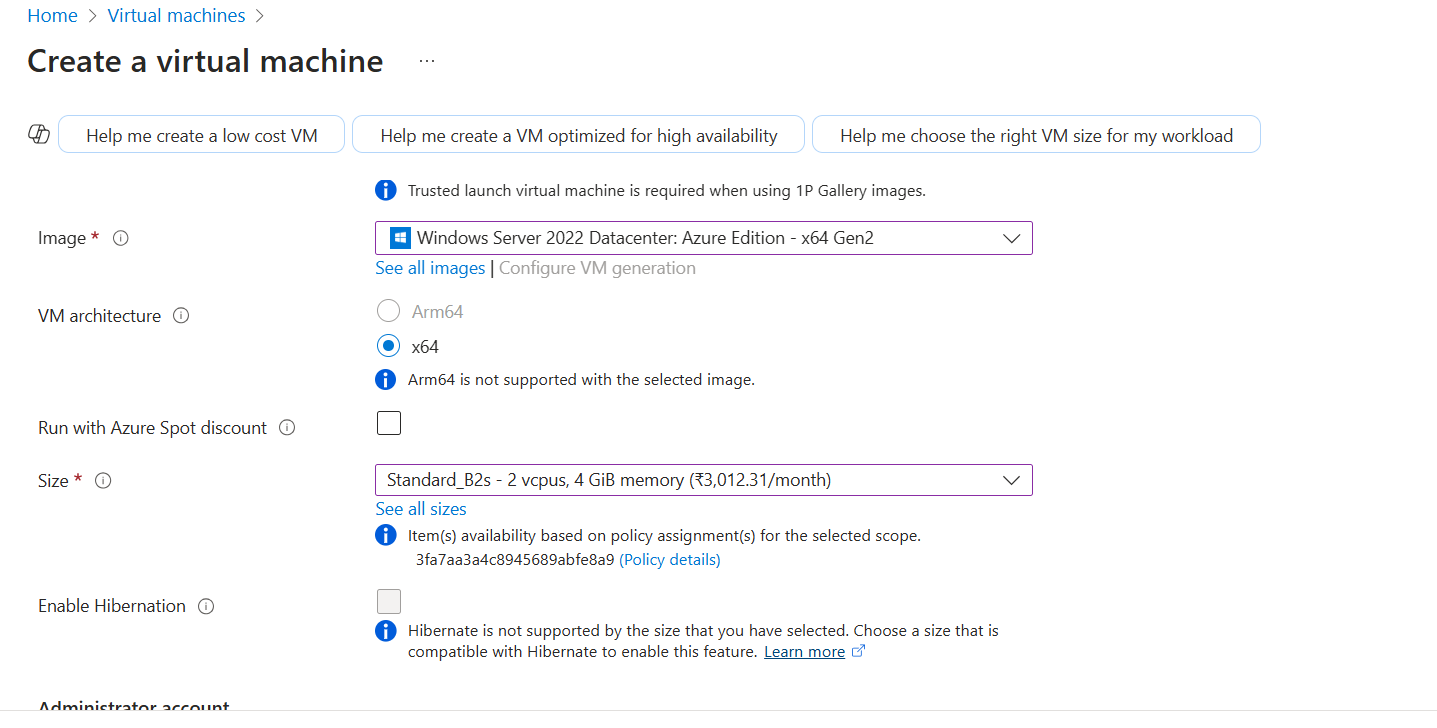
****

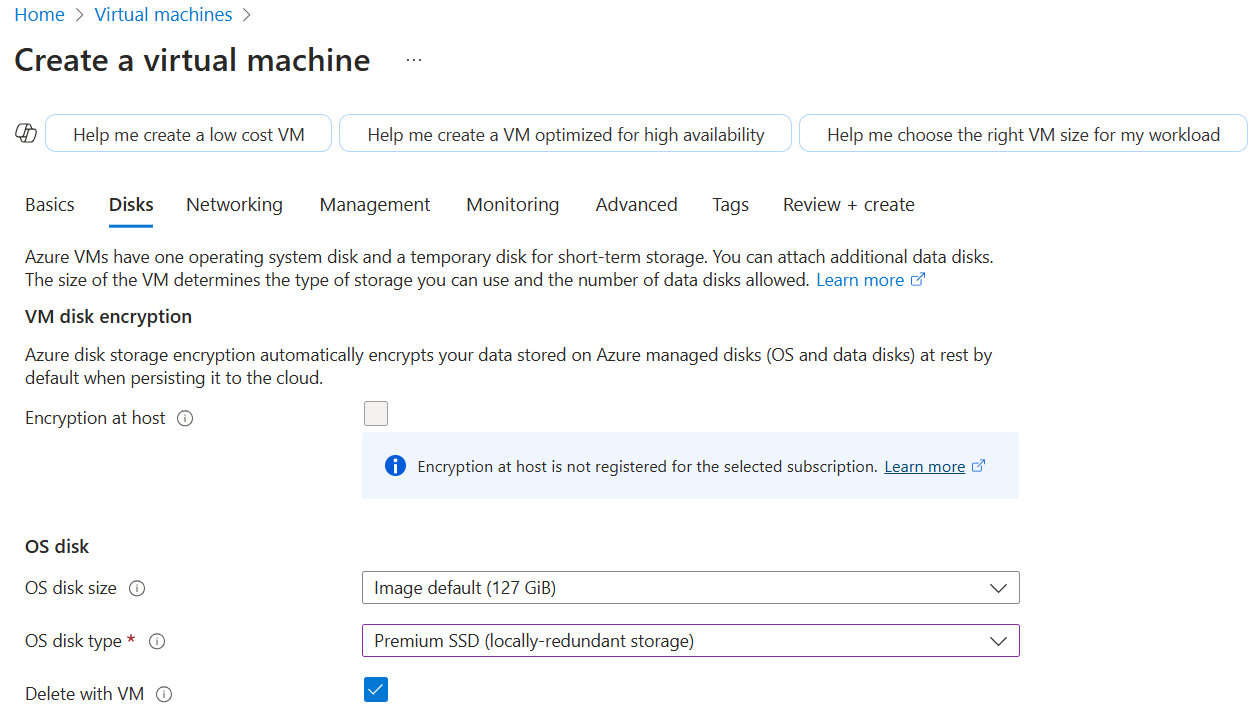
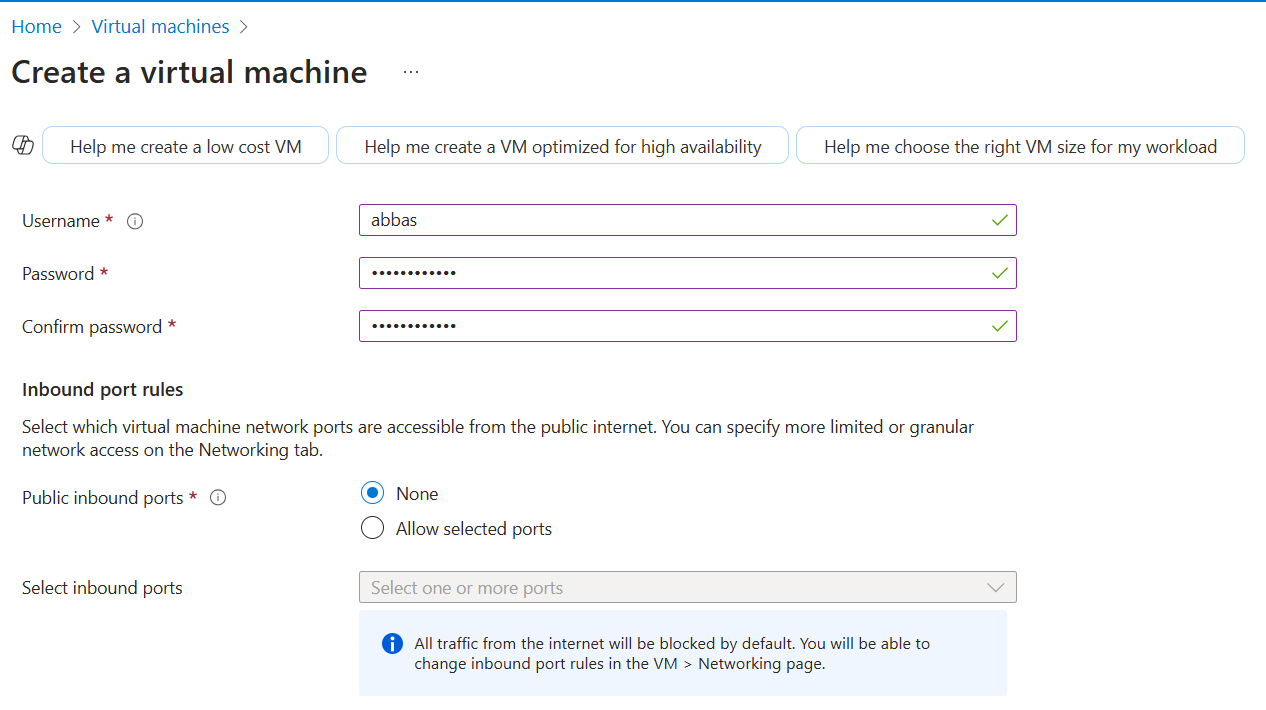
## **Task 7: Deploy virtual machines**

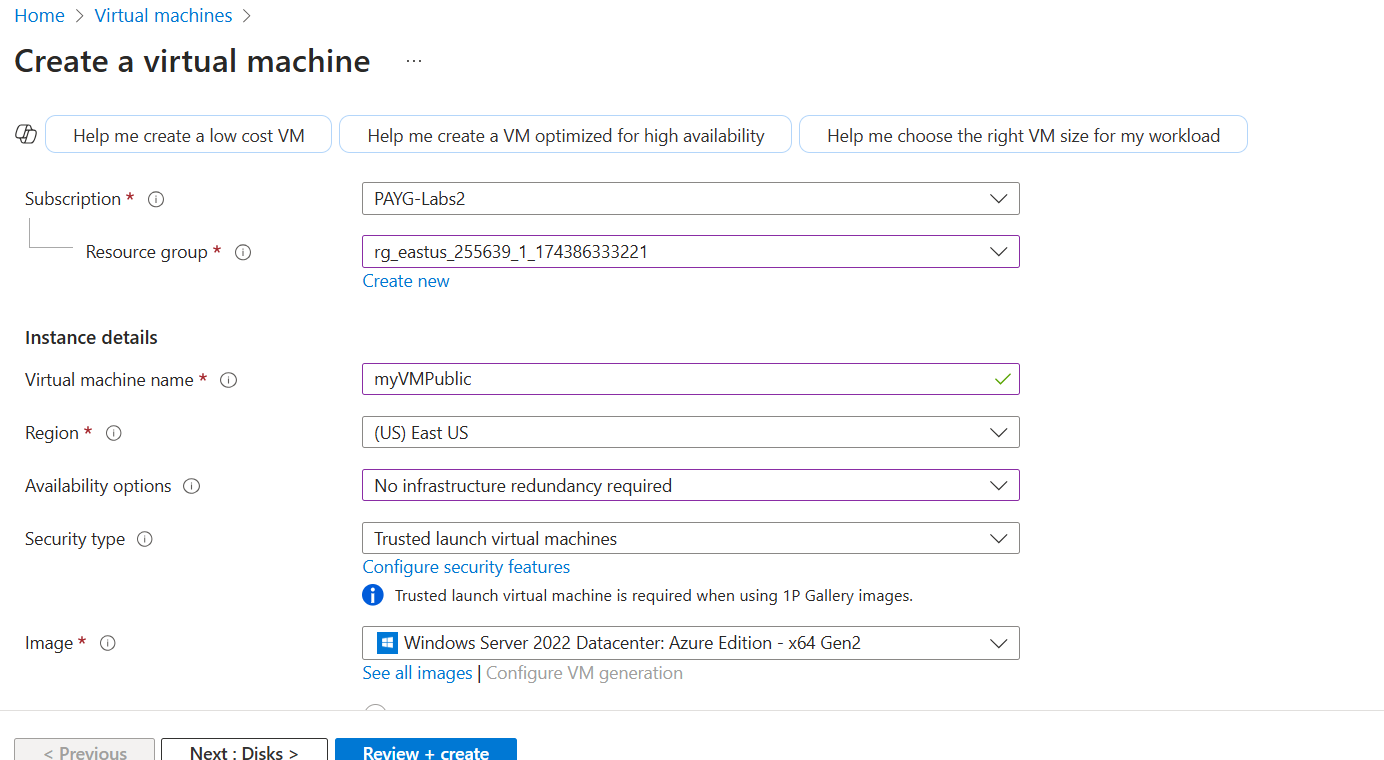
I will deploy to vms one in public subnet and one in private subnet

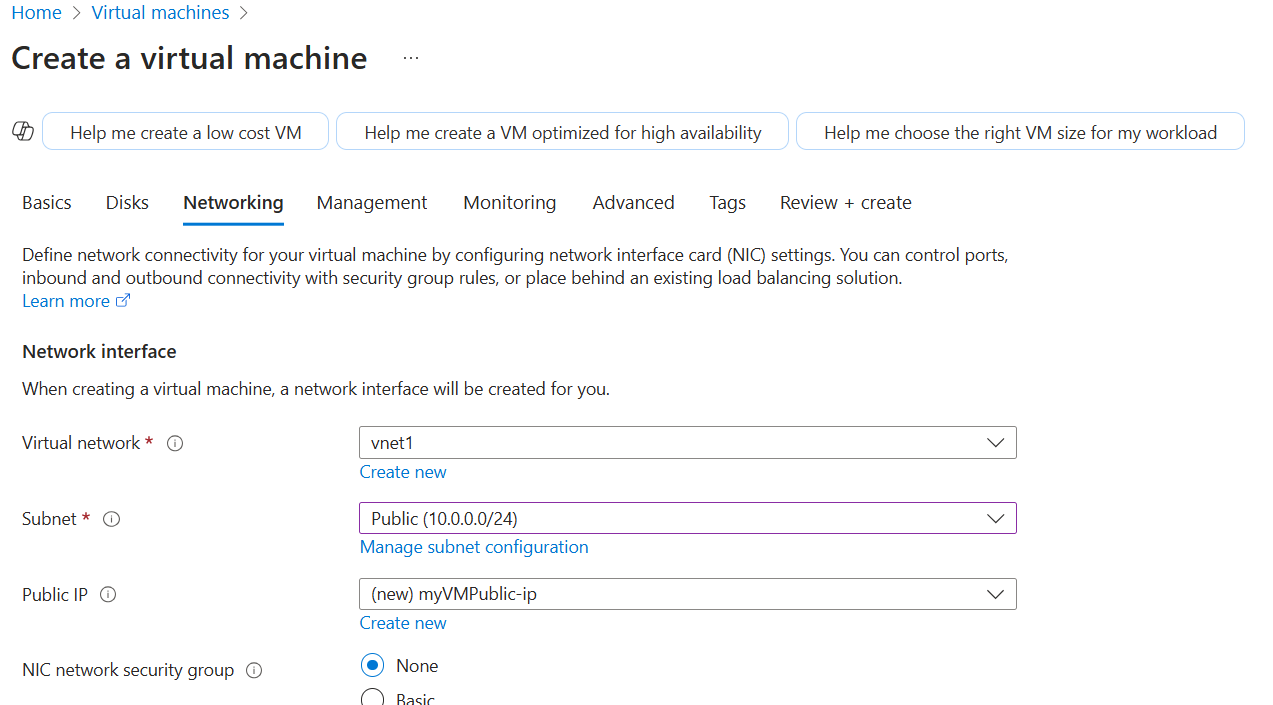
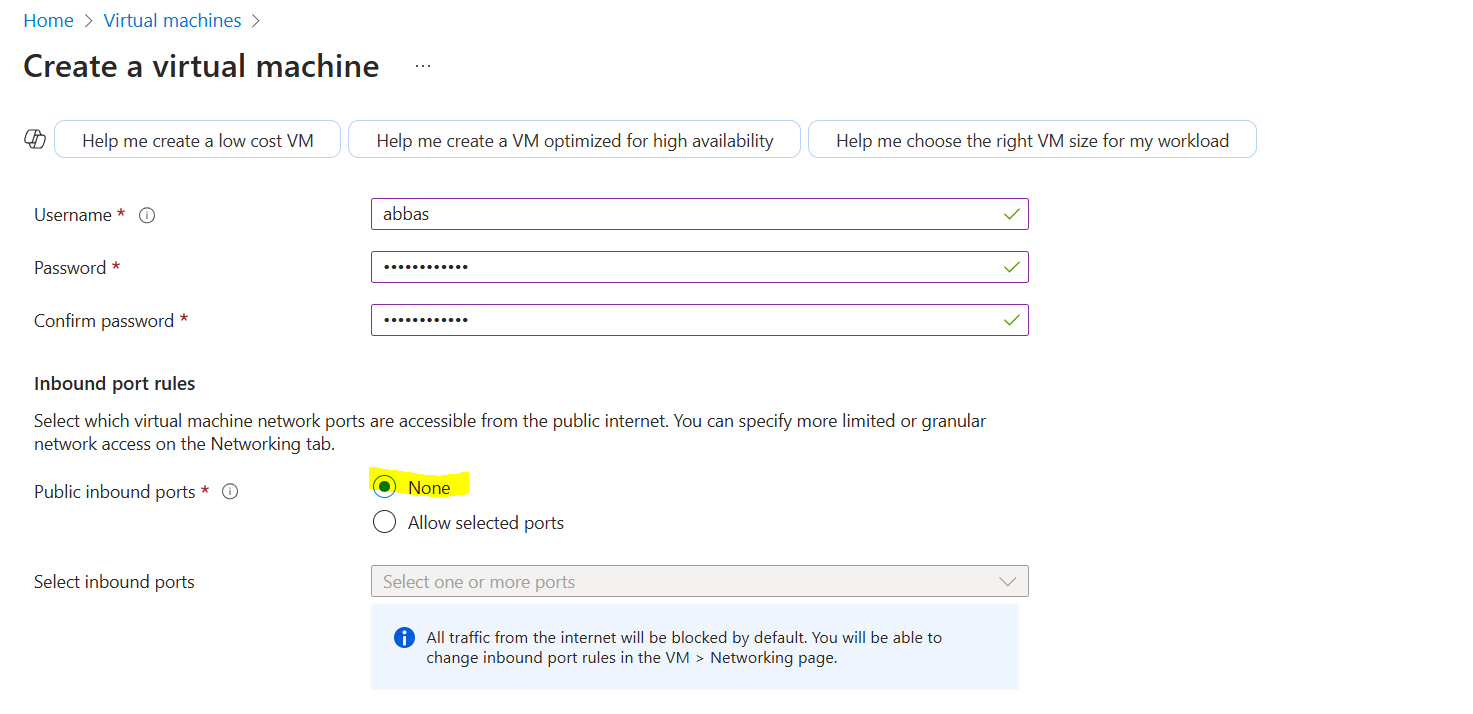
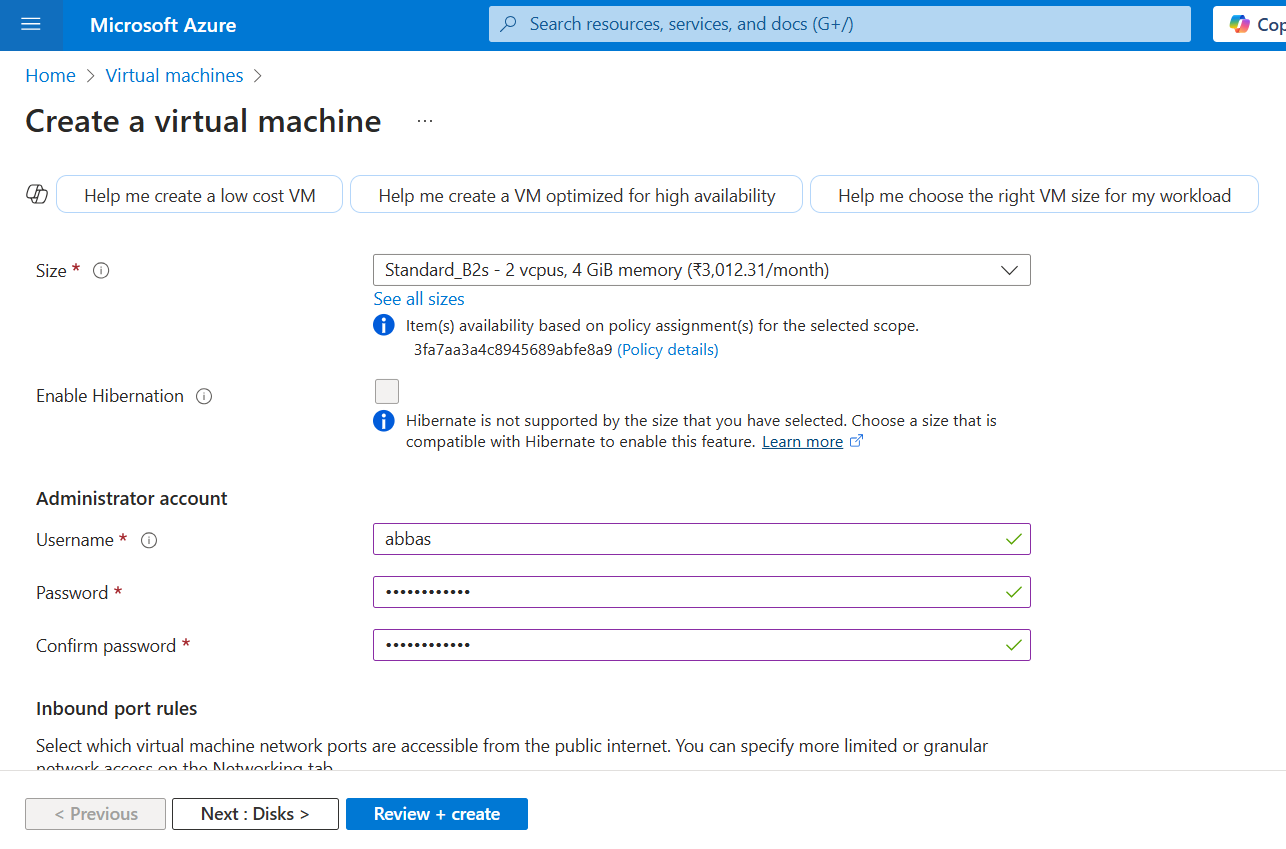
****

****

****

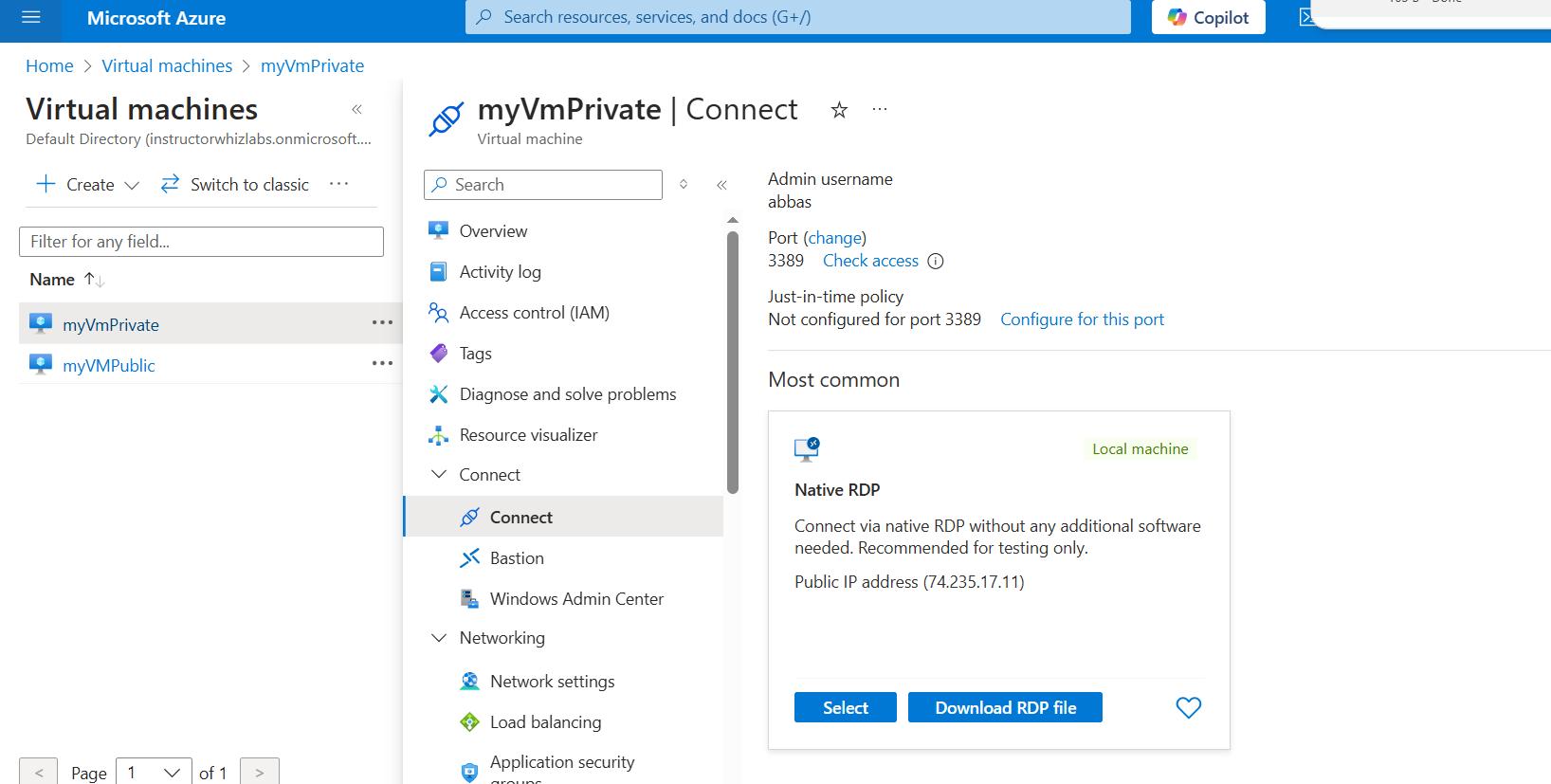
****

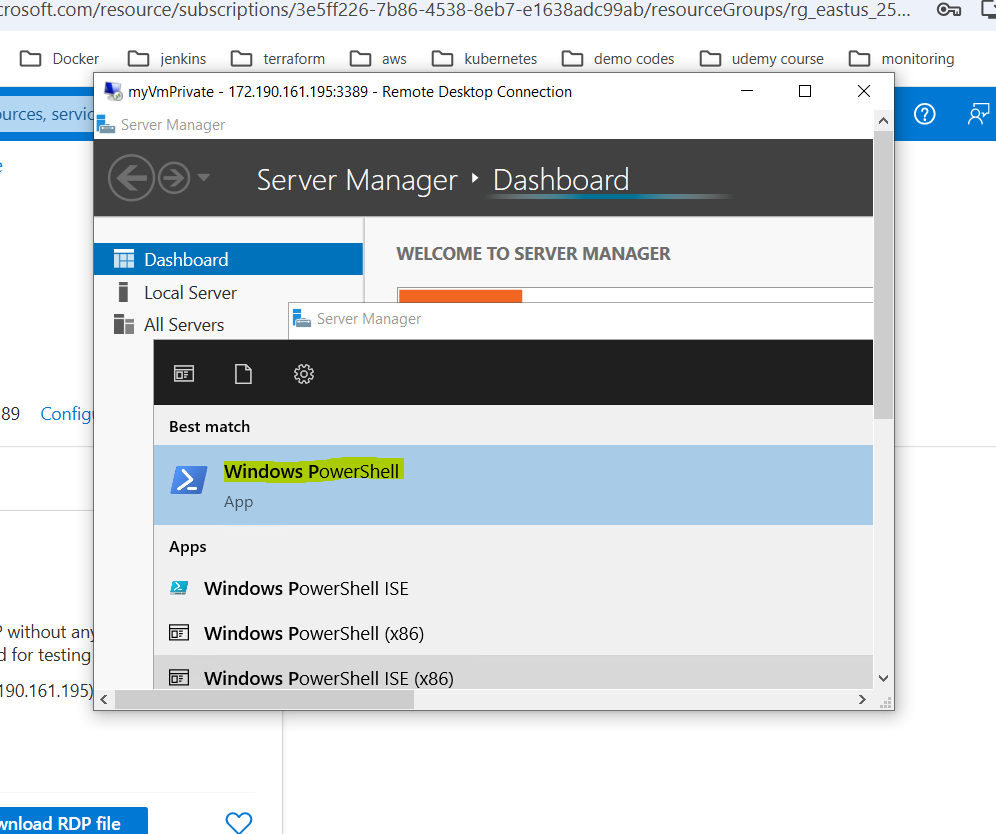
****

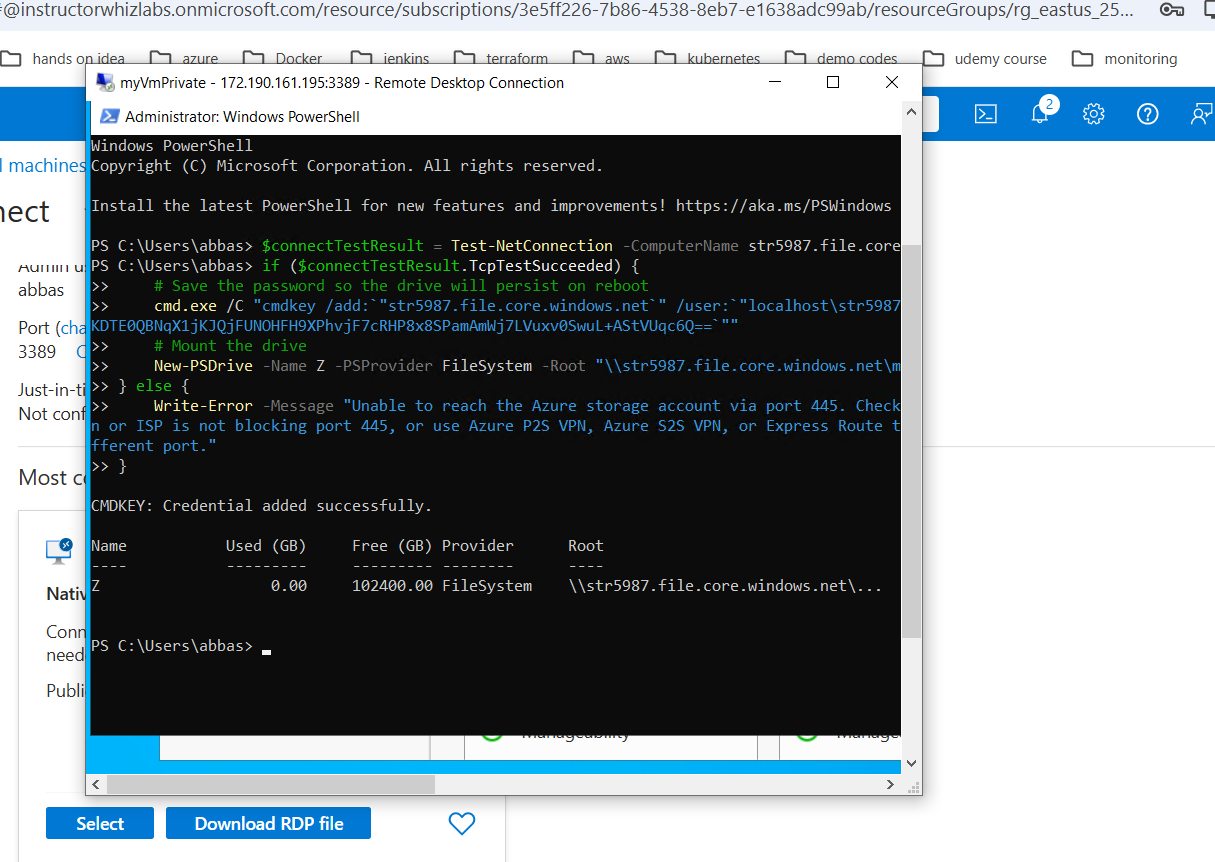
****

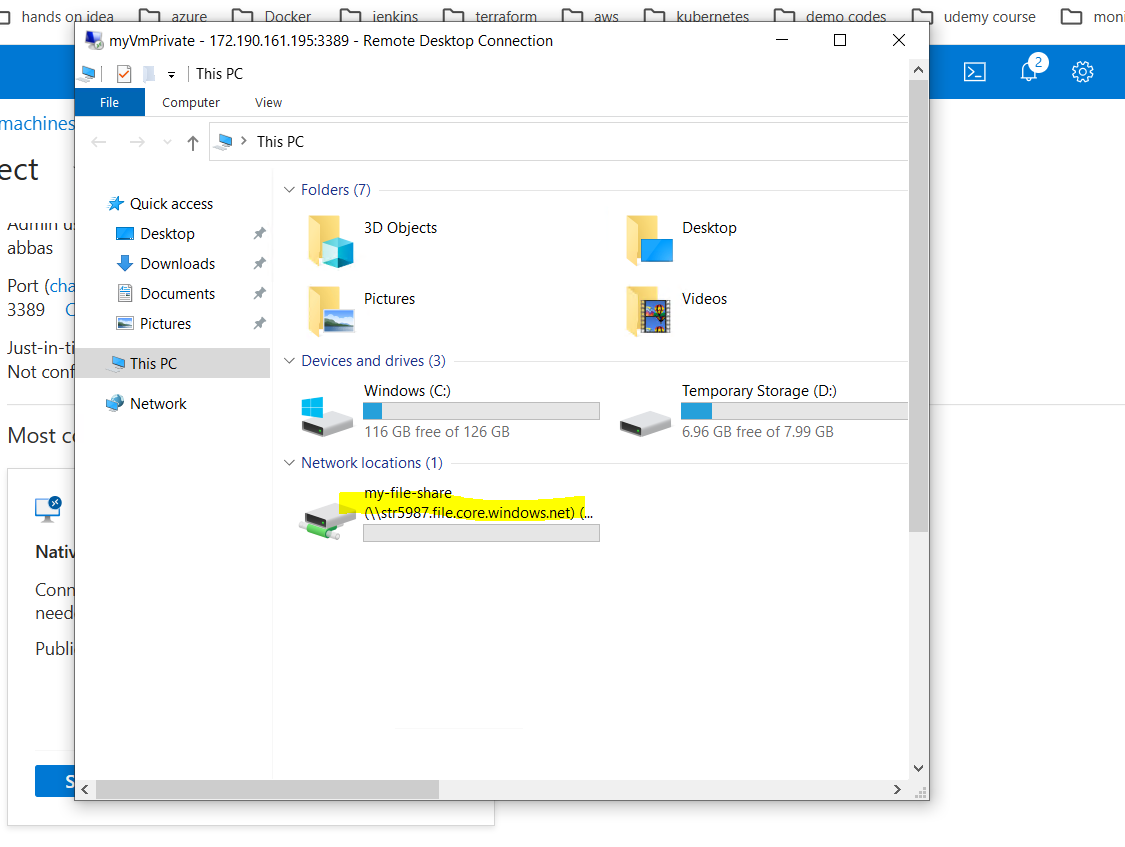
## **Task 8: Test the storage connection from the private subnet to confirm that access is allowed**

**Now the last task I will connect my private vm which is from the private subnet**

****

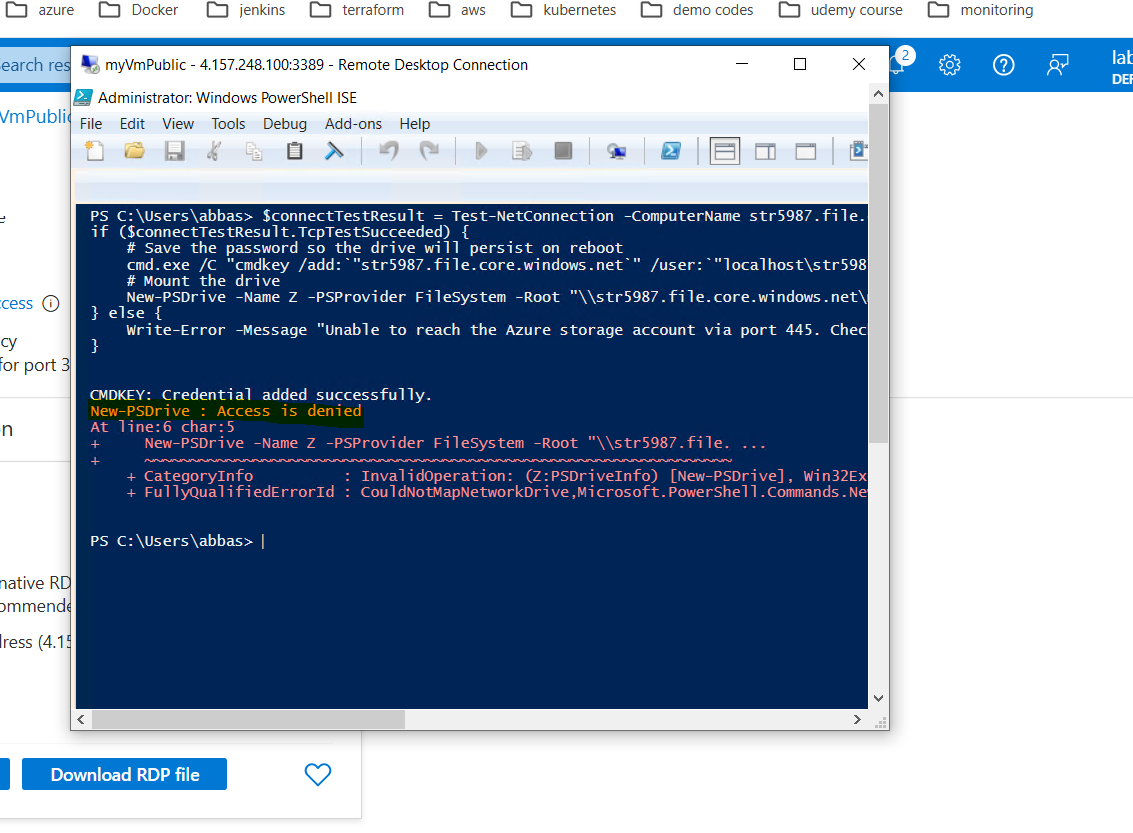
****

**Its connected successdully as expected**

****

## **Task 9: Test the storage connection from the public subnet to confirm that access is denied**

So as shown image the access from public subnet as denied

****

**Finally Terminate all the resources.**