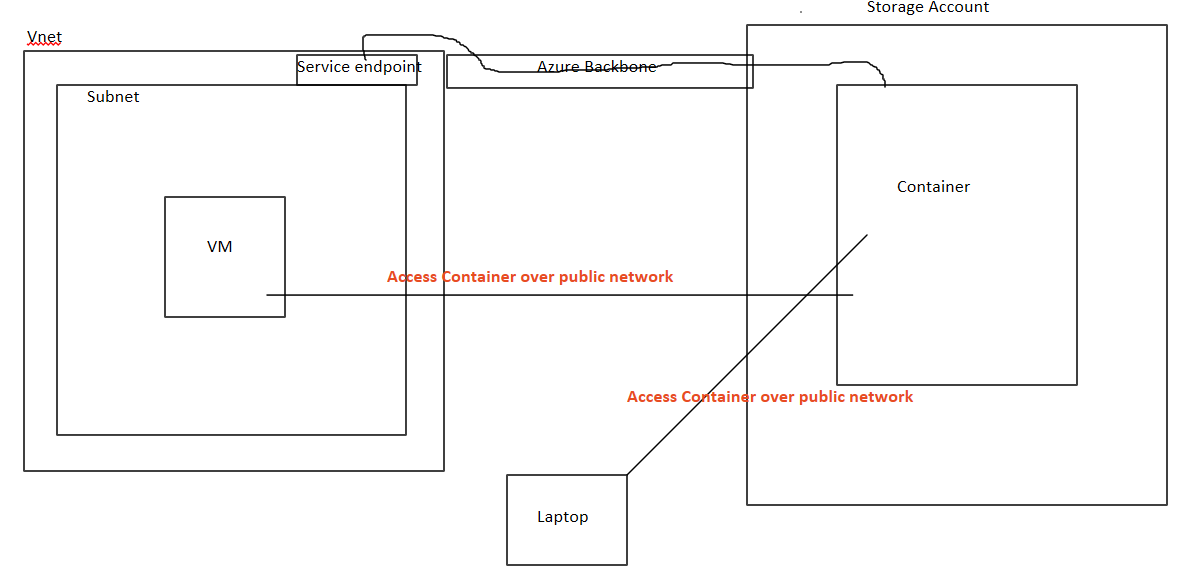
**Service Endpoint**

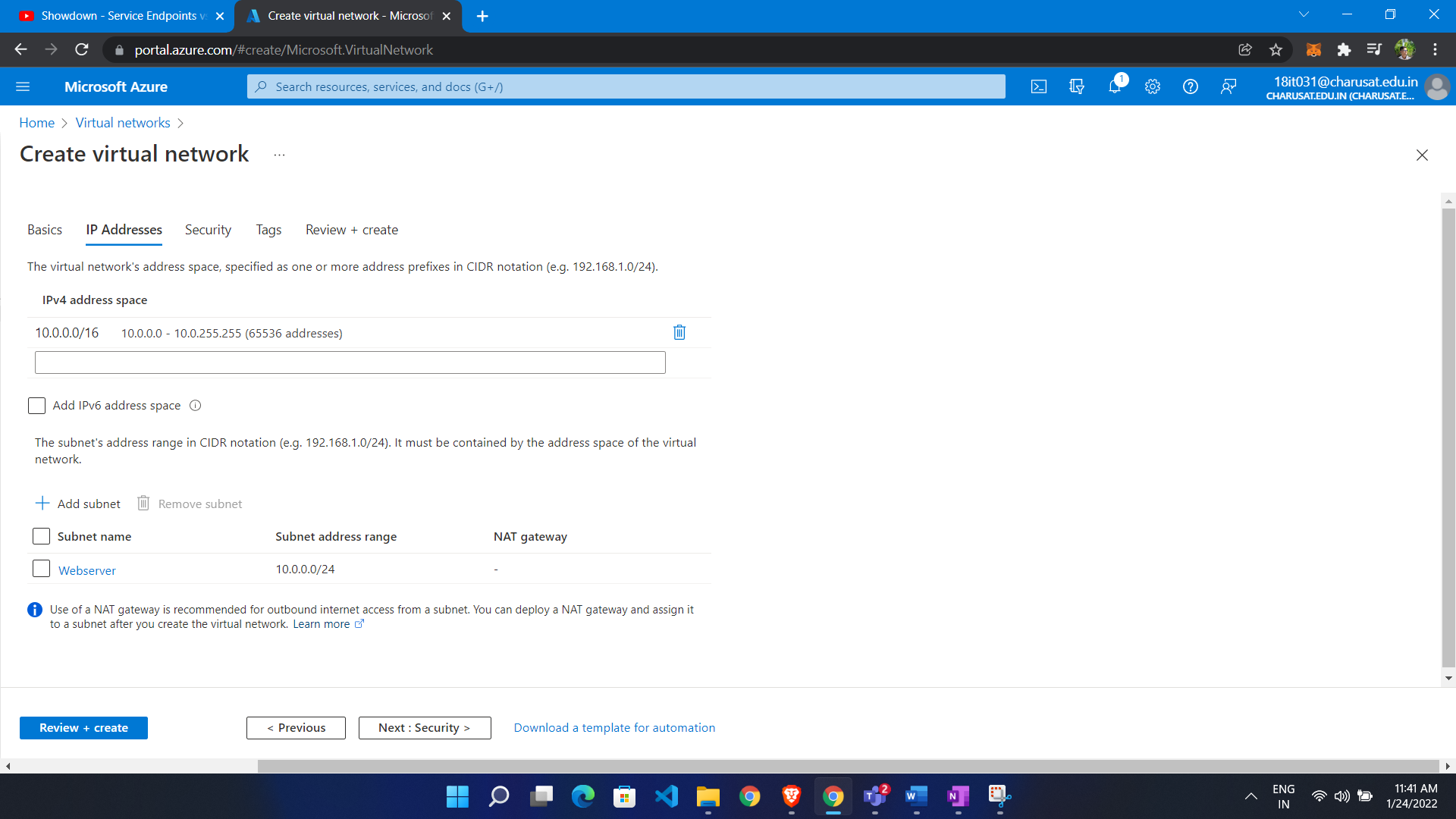


When we want to access container in storage account that we access it via public internet.

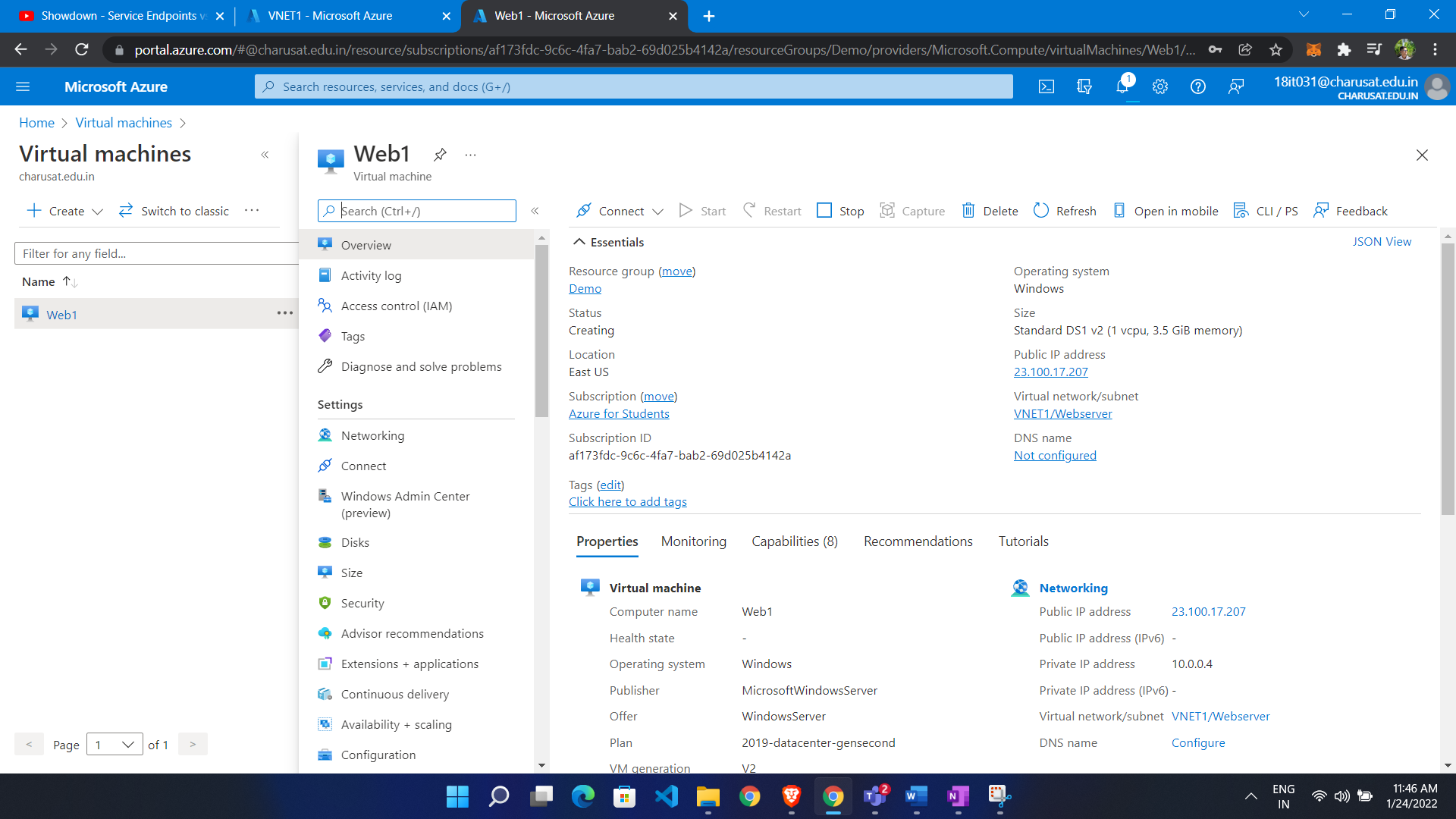
When we add service endpoint we attach service endpoint to subnet so traffic is not go from public internet it goes from Azure backbone

**Configuration:**

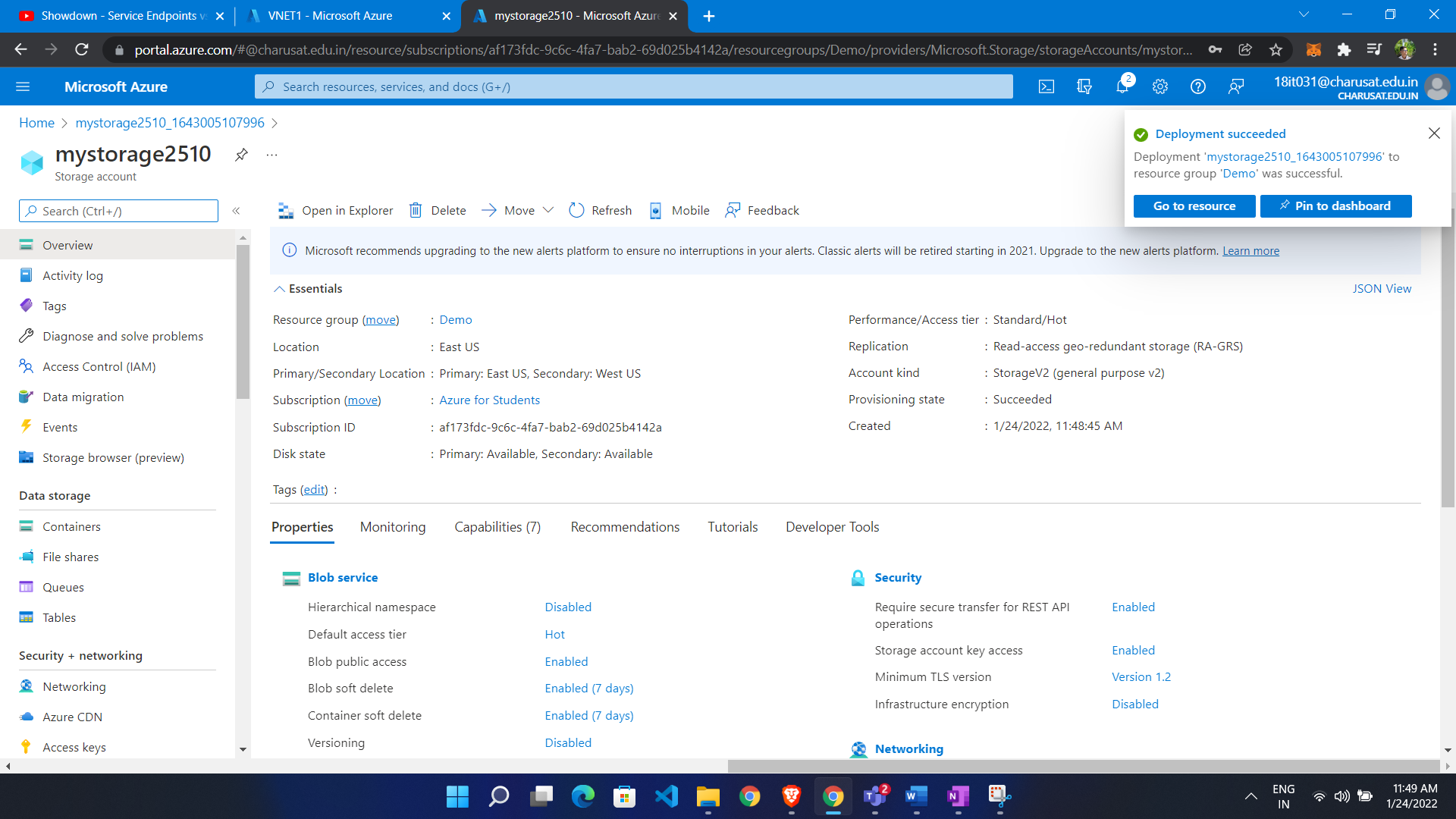
Add Vnet with webserver subnet



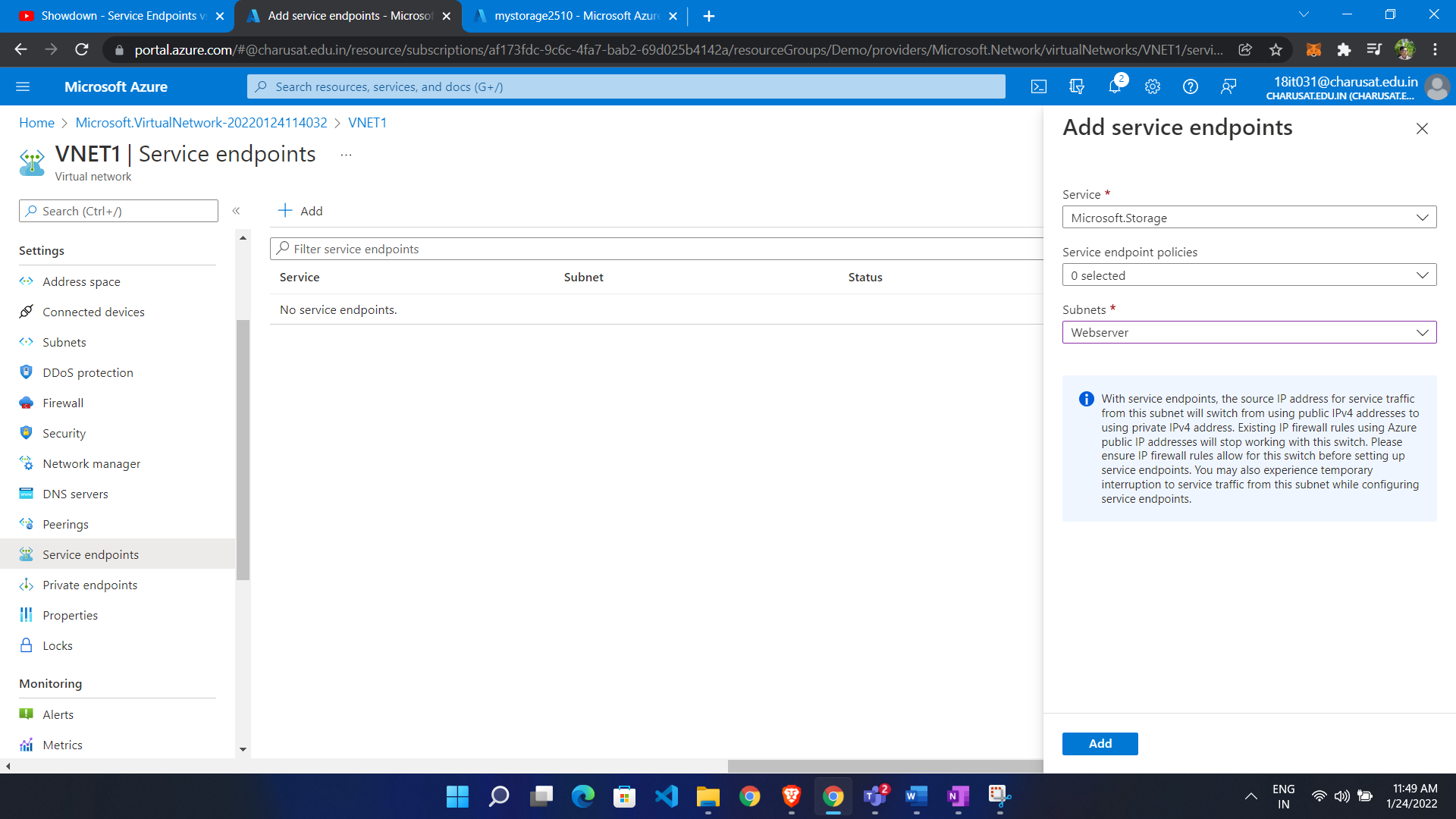
Make VM in subnet



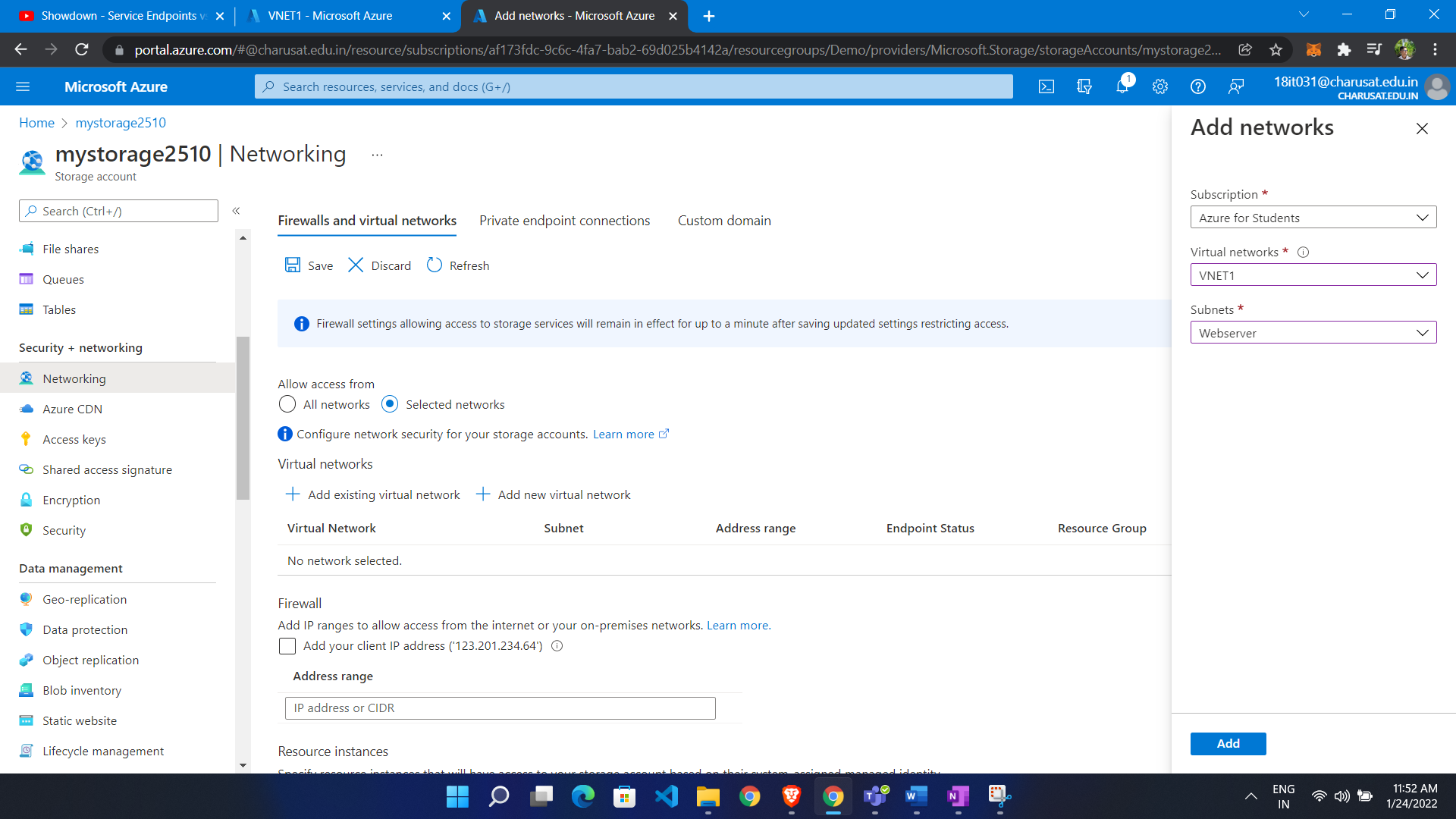
Create storage account:



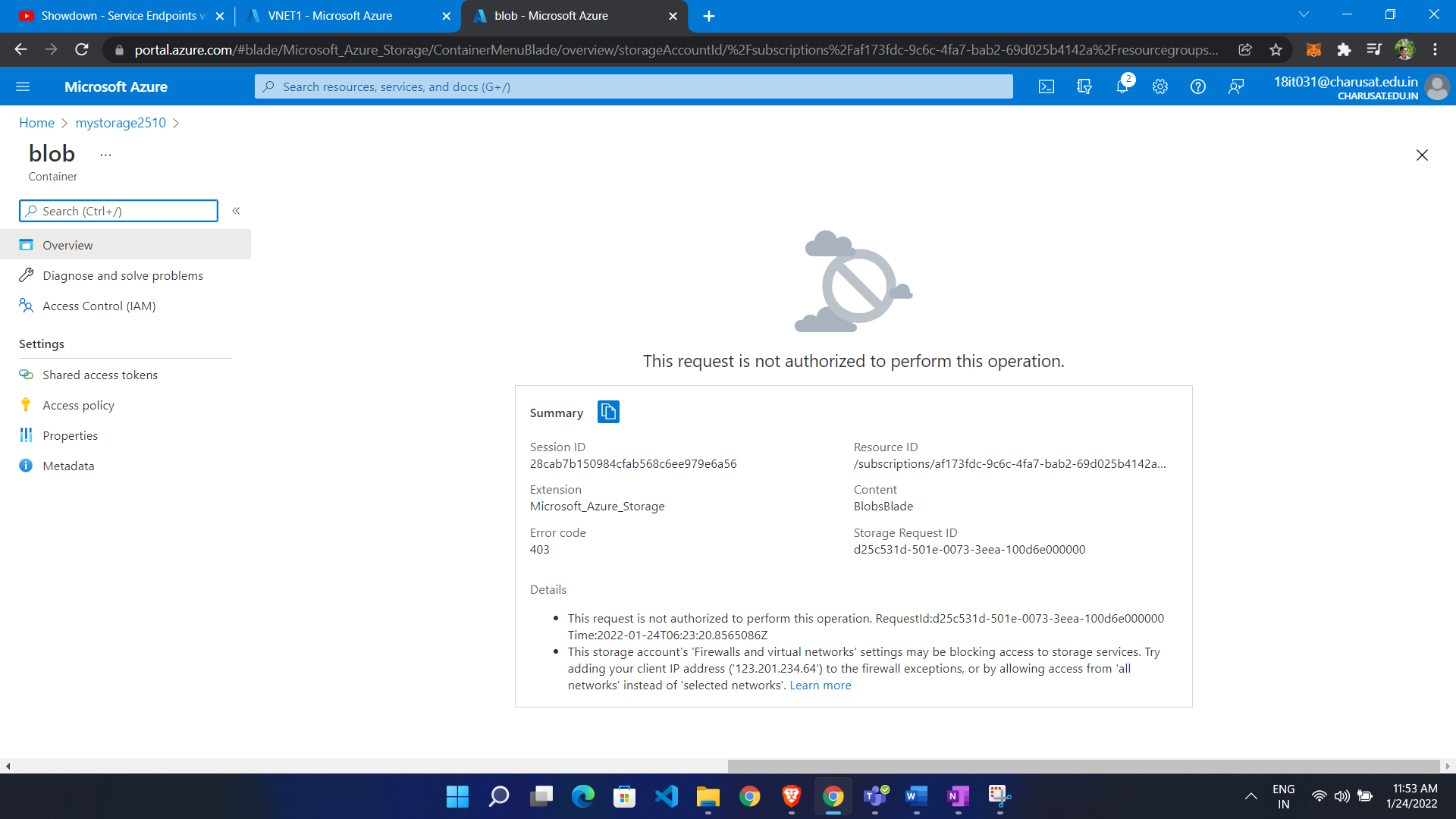
Add service endpoint



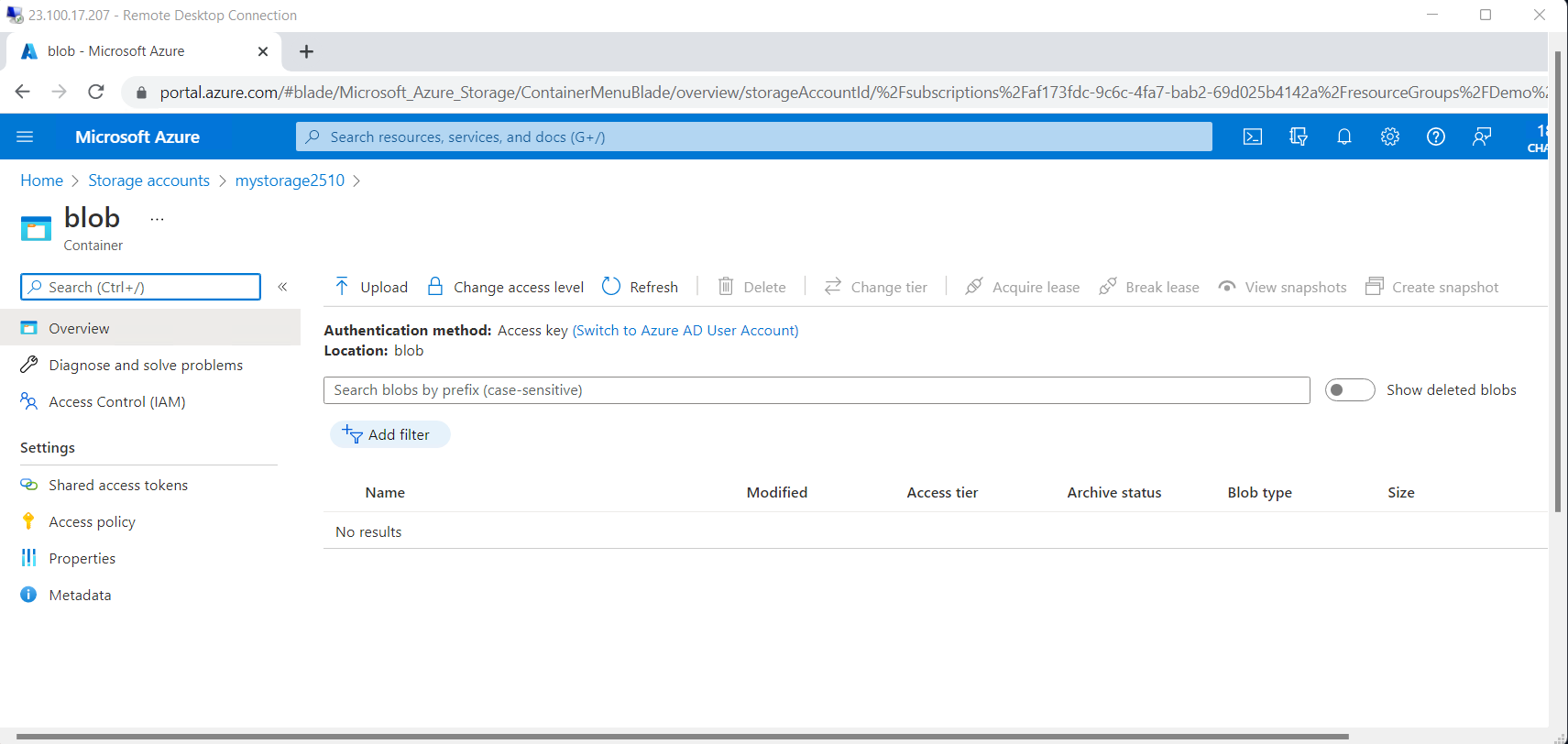
Add Virtual network to storage account



Now we are not able to access storage account publicly

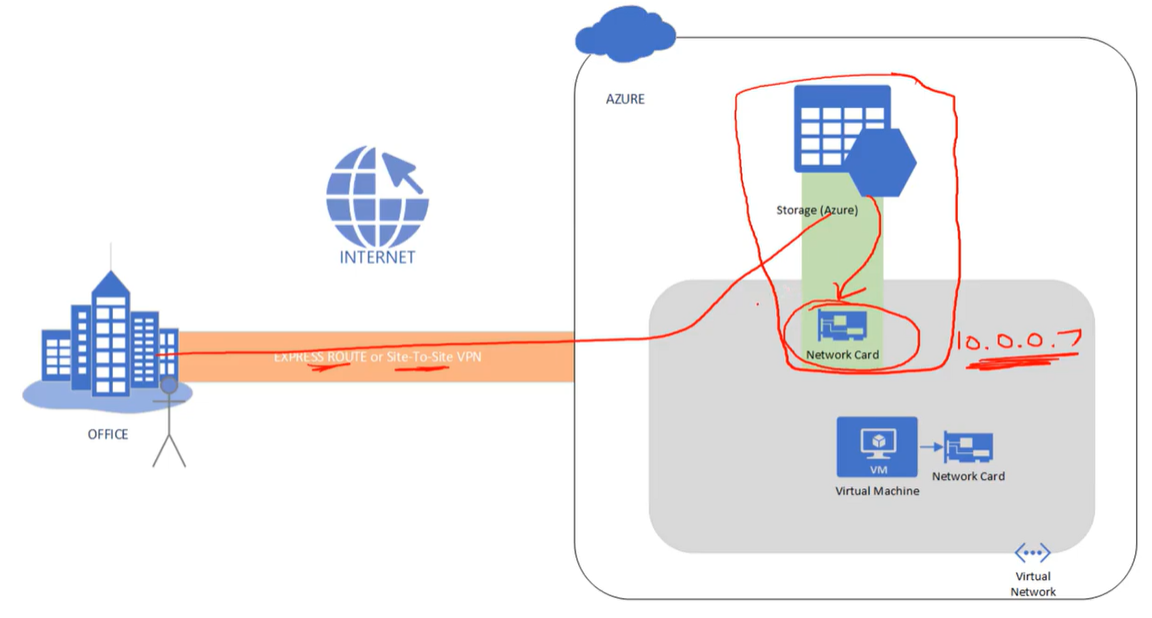


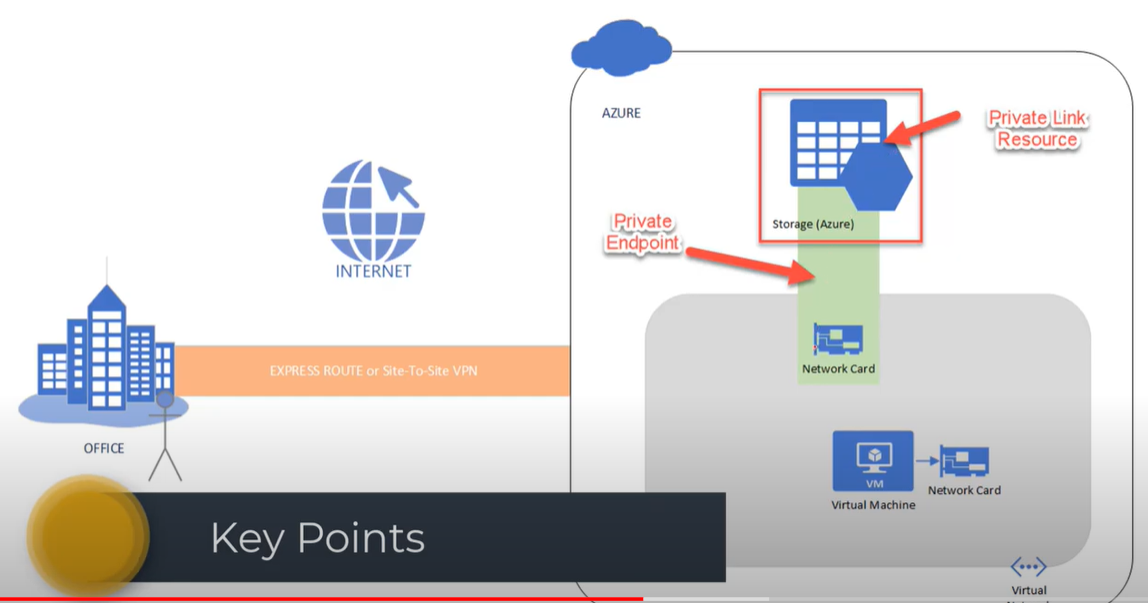
We access through it vm in that subnet



Private Endpoint:

Private endpoint extend public service to virtual network. virtual network card linked to that service. So storage account get private ip so now it is connected to site to site



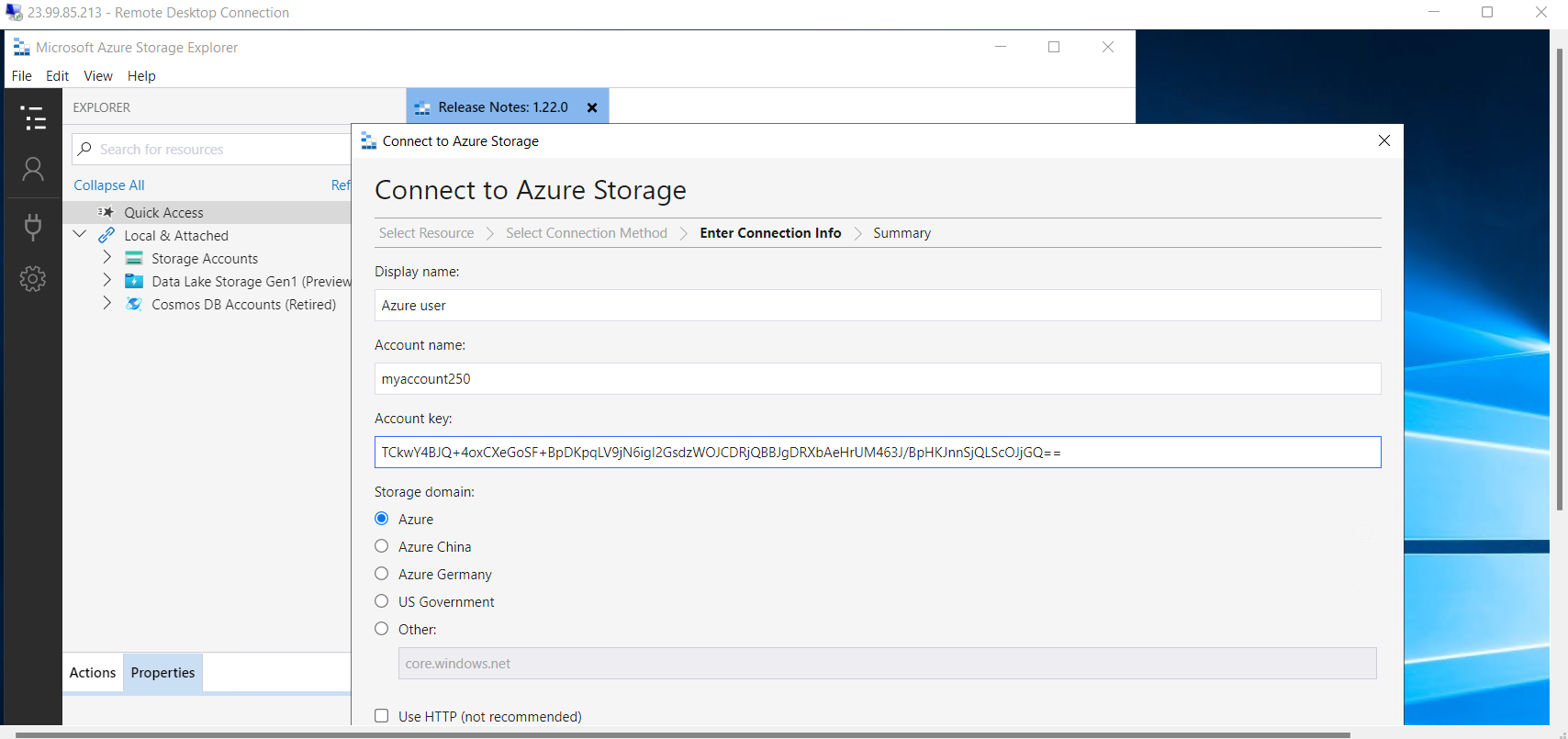


For same private resources we have multiple endpoints

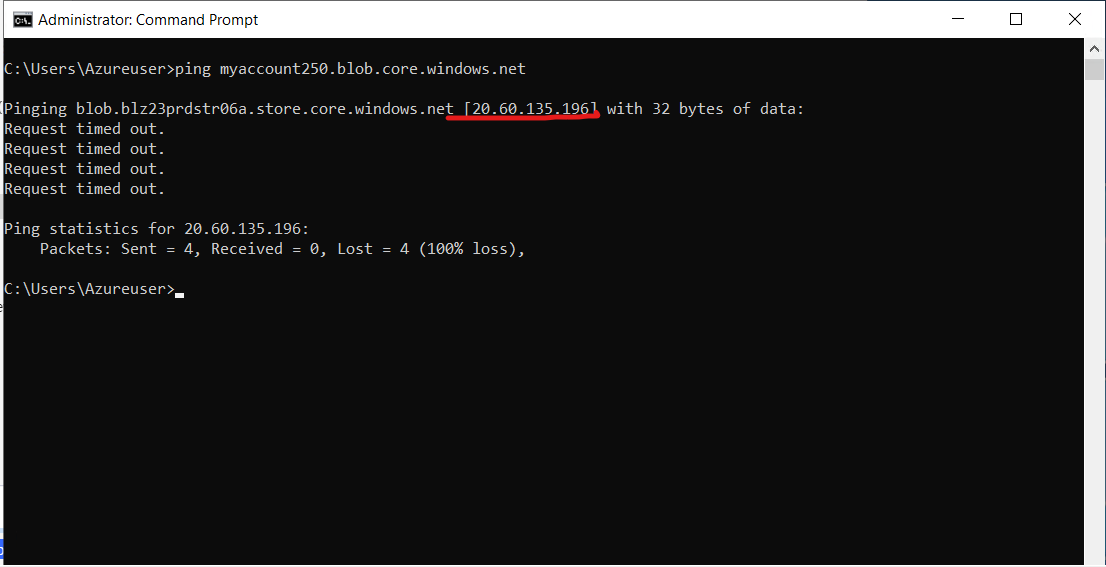
For one virtual network we have multiple private endpoints

**Configuration:**

Create Vnet in it one vm and make storage account

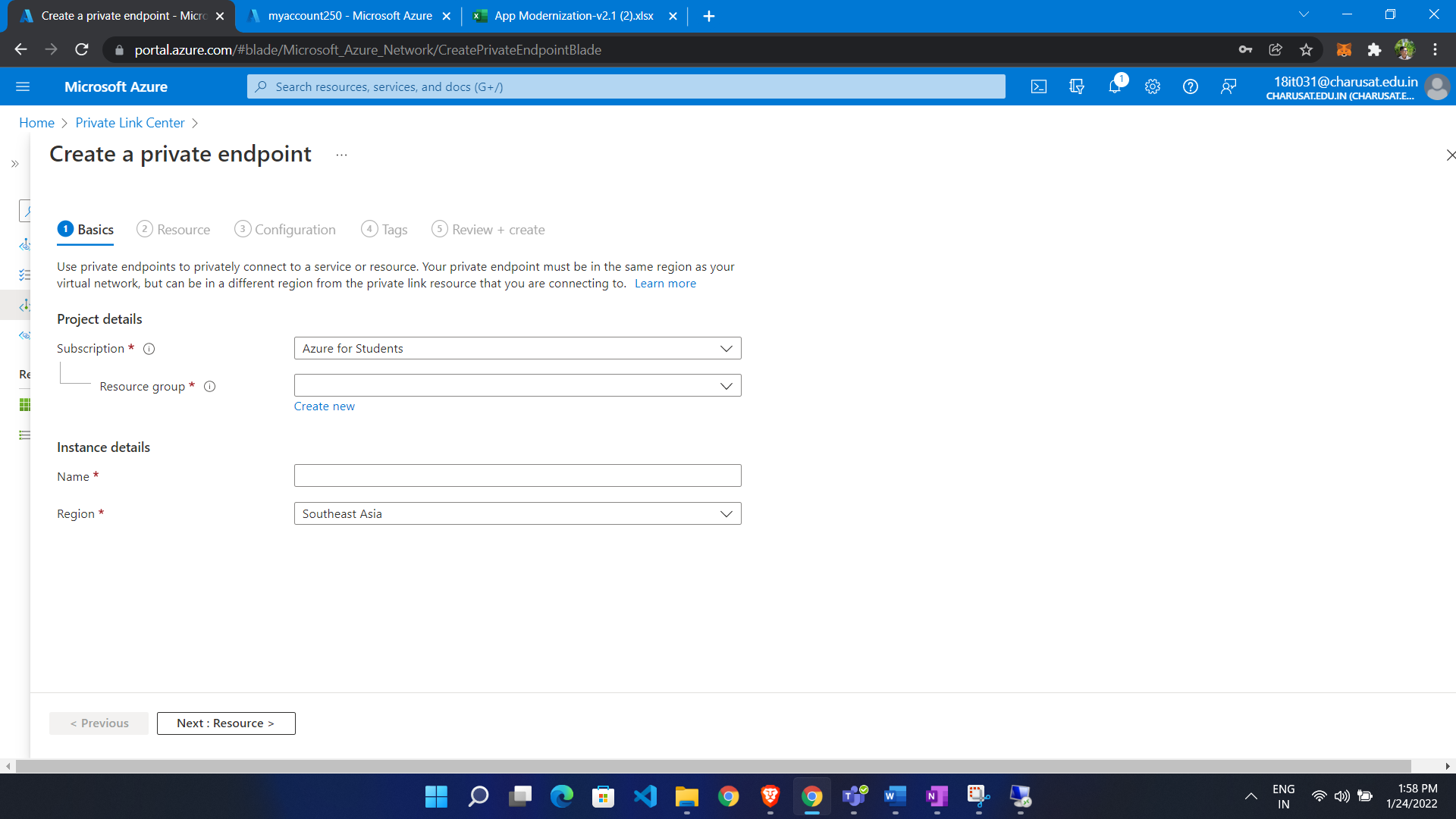


Now we are going to ping storage account from VM

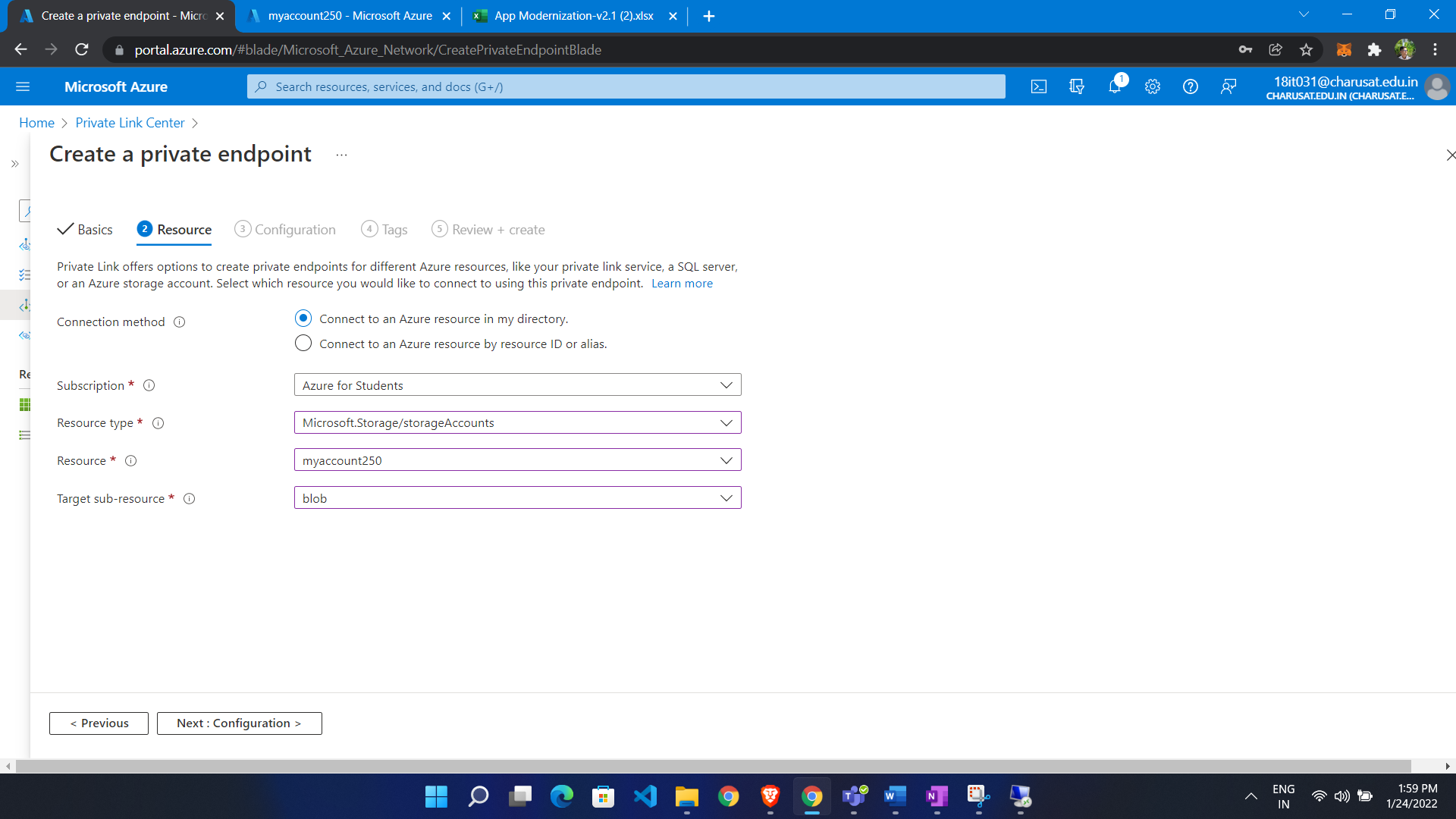


We see that we get public ip address

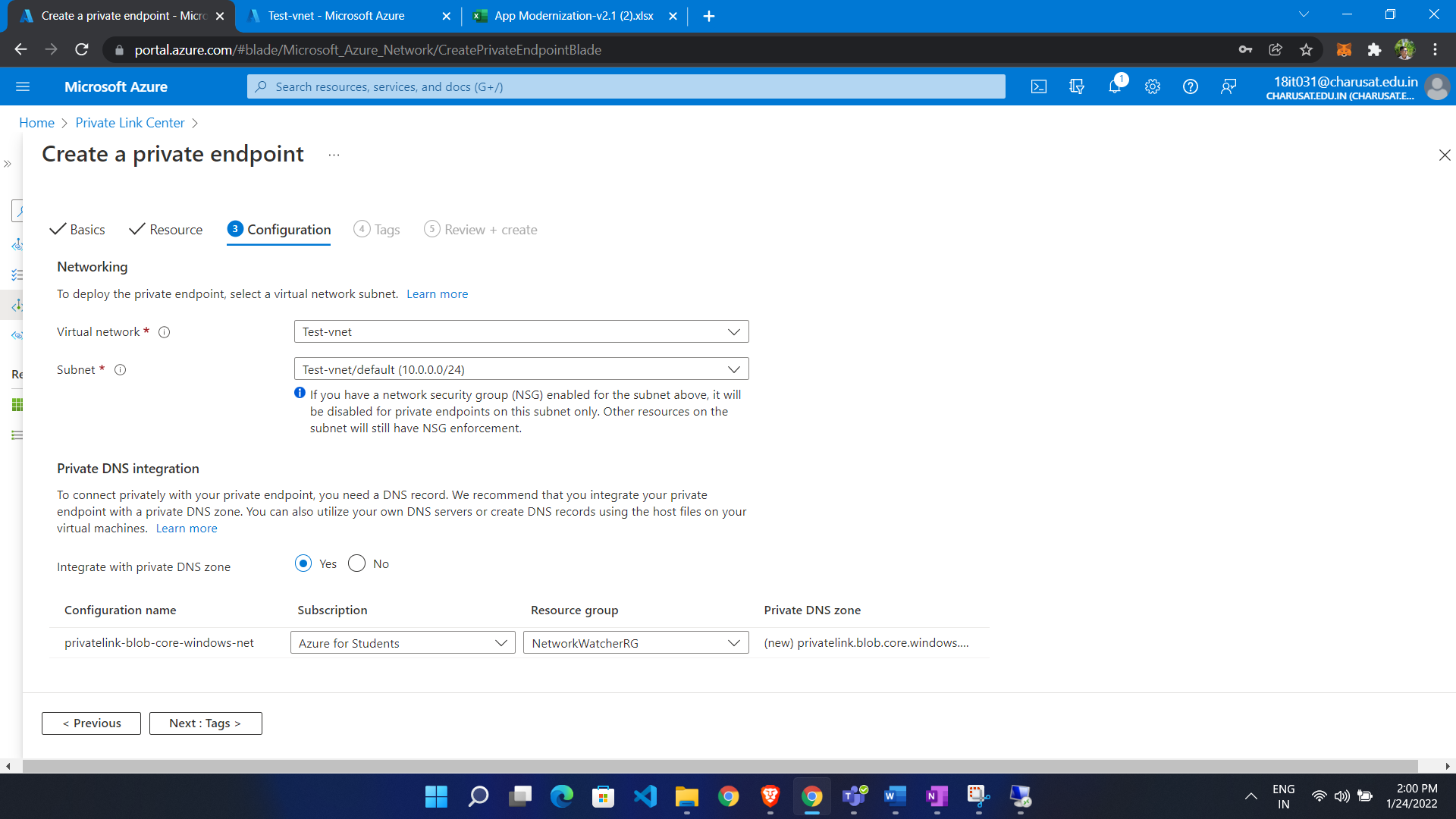
Create Private endpoint:



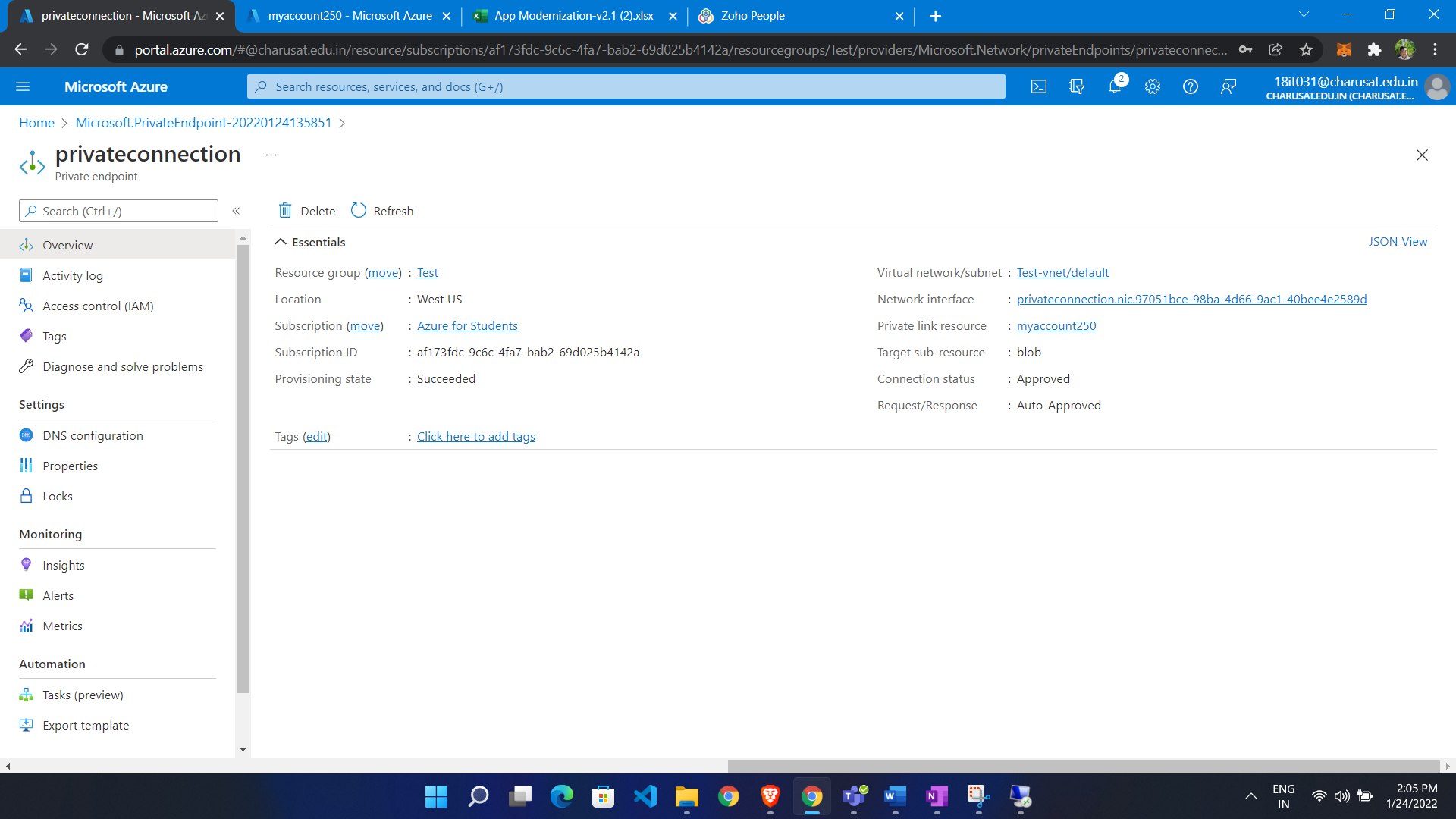
Select resource



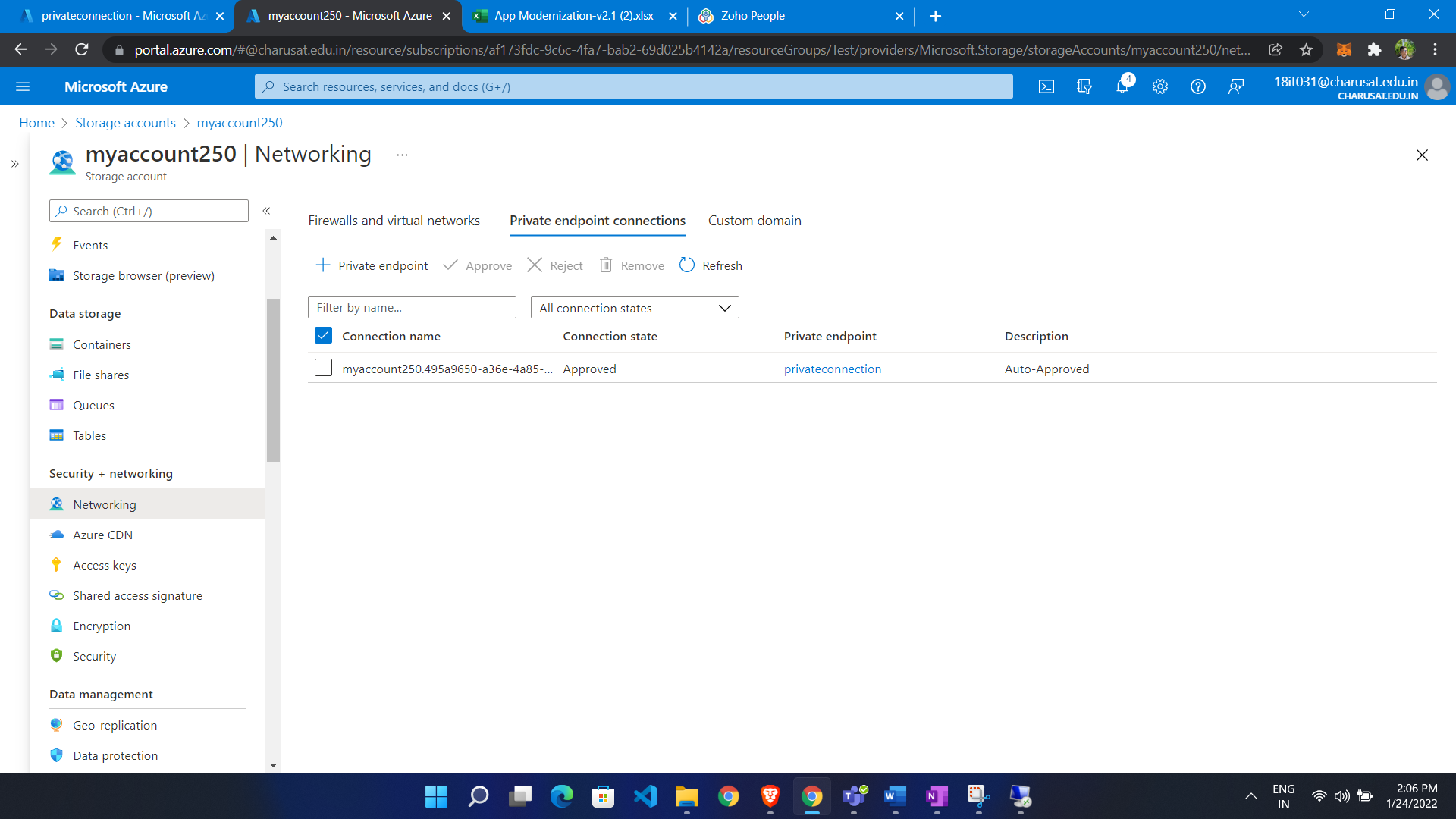
Configure it to a virtual network

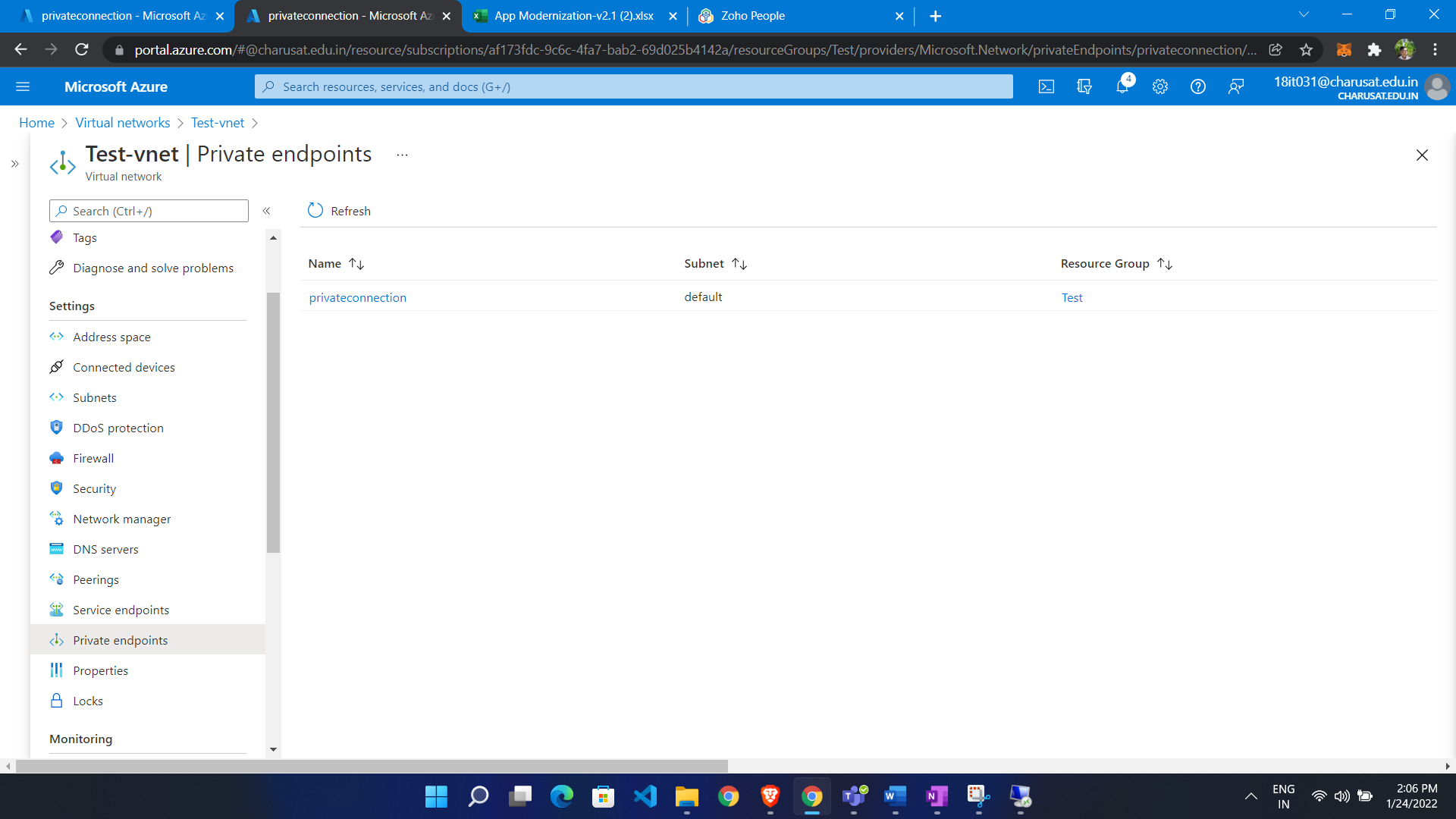


Created

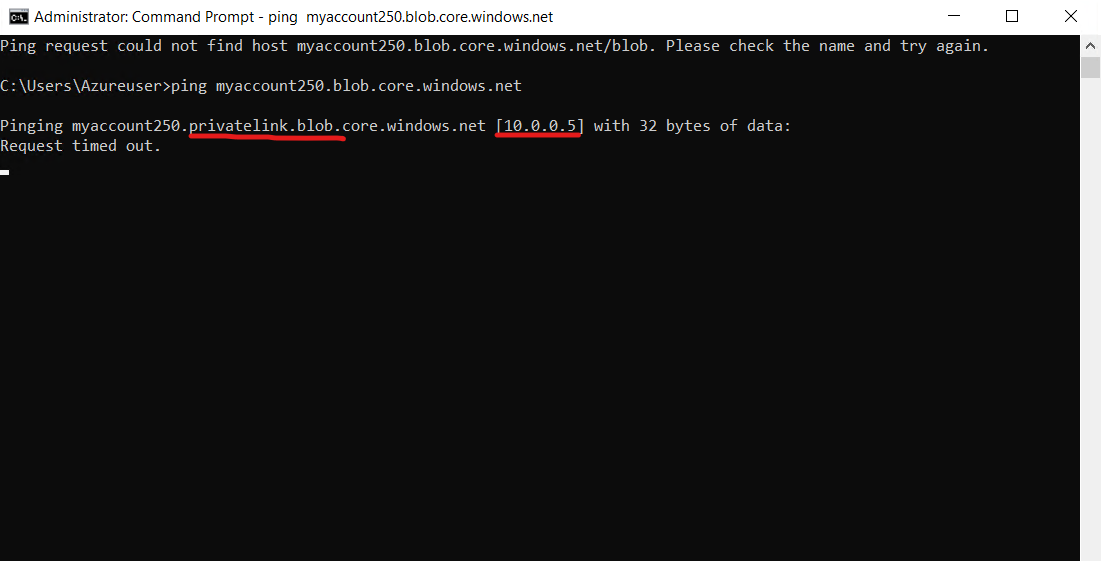


It is also attached to storage account and virtual network

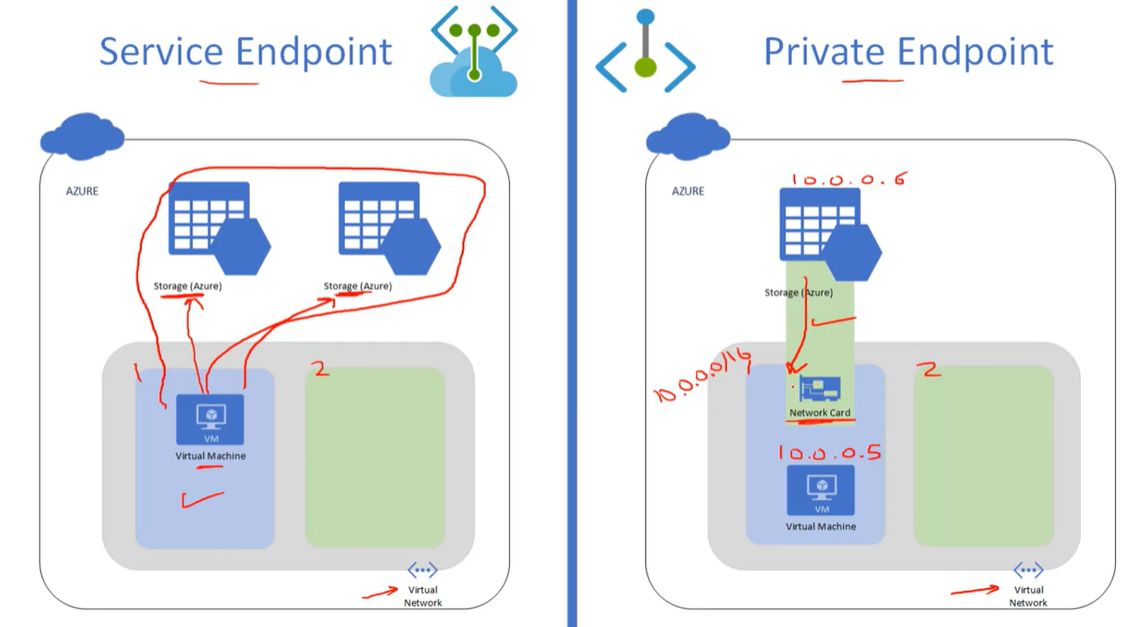




Now we get Response from private ip



Service end point vs private endpoint:



* In service endpoint all storage account know the the vm in that subnet (**when we enable service it grant to all storage account)**
* Private Ip **is one to one connection between subnet of your vnet and one specific resource** of service.
* In service endpoint vm is still connection to pubic ip of storage account (connection go over Microsoft backbone)
* In private endpoint it connect via private ip address
* In service endpoint as well traffic goes from Microsoft backbone but it is out side vnet so we need to configure additional
* In service endpoint If we have on premises connected to azure via site to site or express route so if on premises want to connect to that storage account then we allow that public ip in firewall
* In private ip it connect with private ip and connected to storage account so no need to do in firewall setting

**When use service endpoint:**

When we want multiple resource of same service

Want free of cost