Cyber Shujaa

Cloud Security Specialist

Assignment 18 - Lab 6: Service Endpoints and Securing Storage

NAME: WELDON KIPKIRUI KENEI

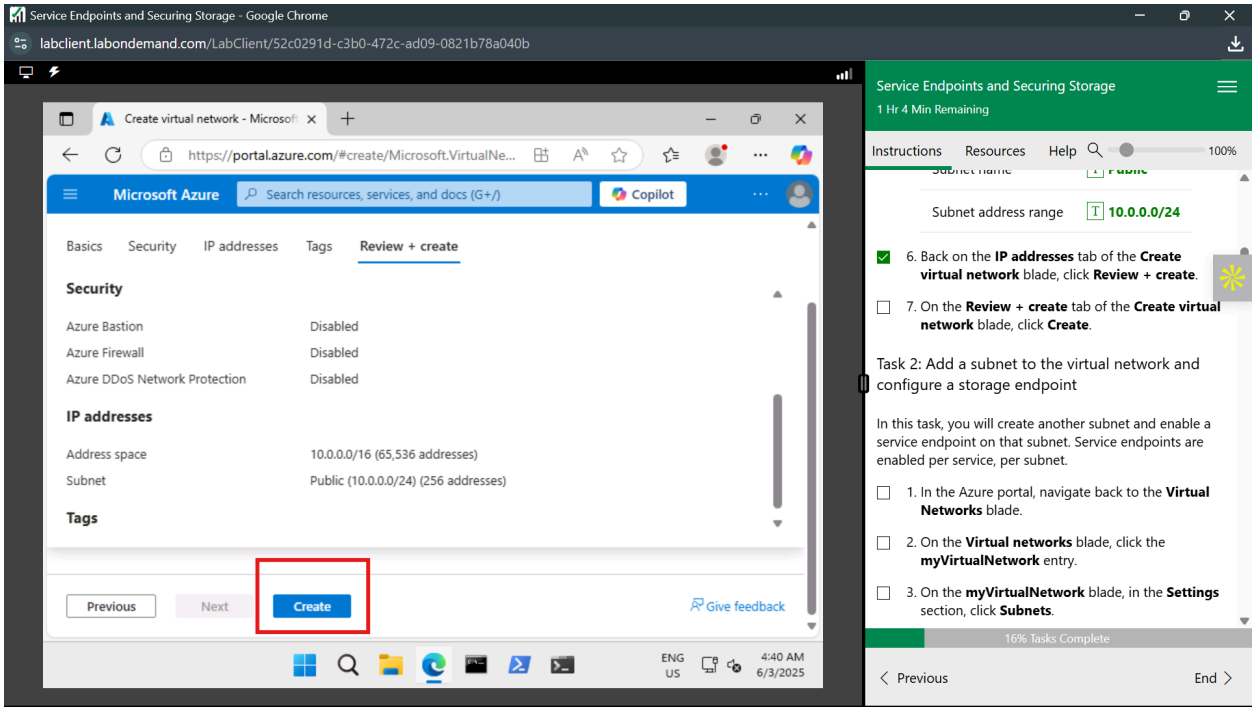
CS NO: ADC-CSS02-25027

Introduction

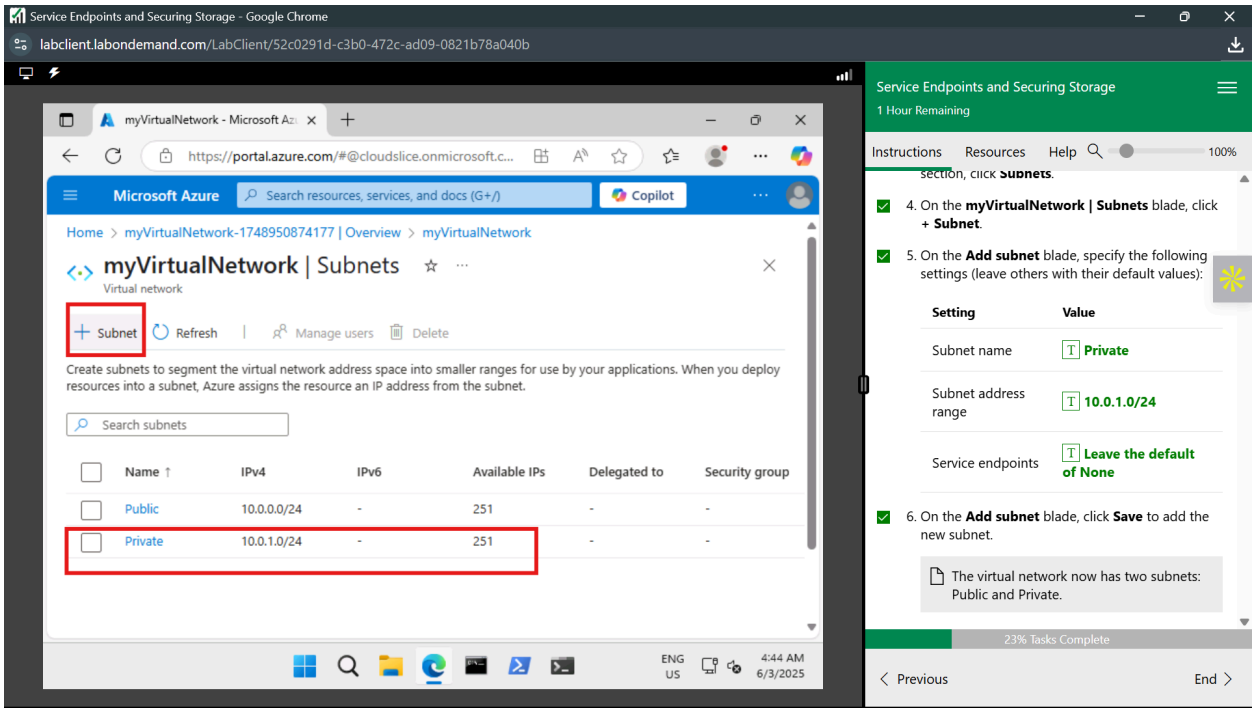
In this lab scenario, we will create a proof of concept to demonstrate securing Azure file shares. Specifically, we want to: Create a storage endpoint so traffic destined to Azure Storage always stays within the Azure backbone network, configure the storage endpoint so only resources from a specific subnet can access the storage, and confirm that resources outside of the specific subnet cannot access the storage.

Service endpoints and security storage

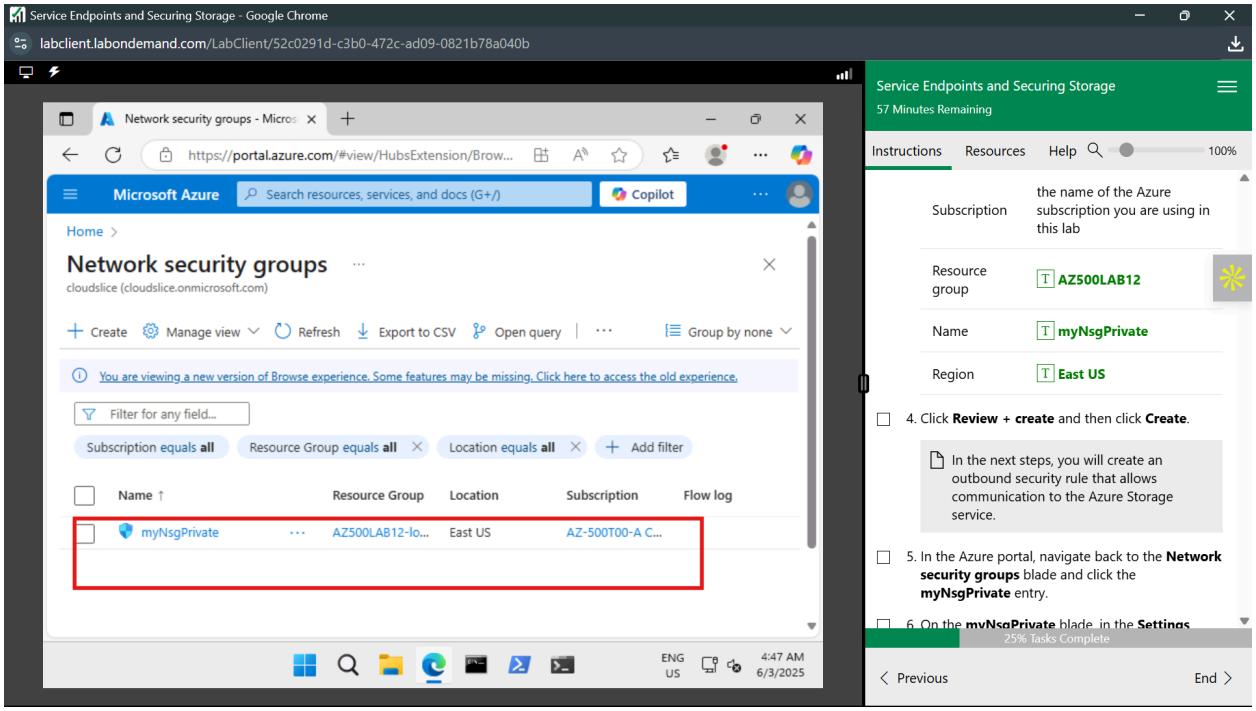
Firstly, we need to create a virtual network using the Azure portal as shown.

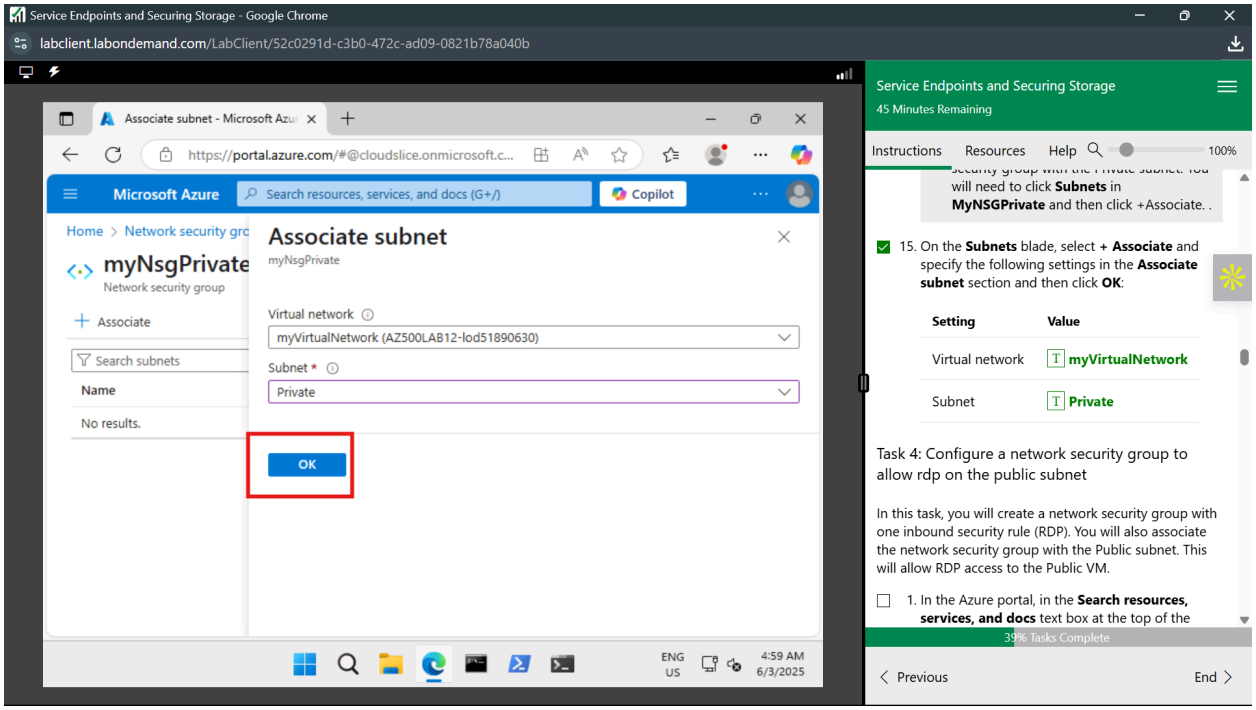


Next, we will create another subnet and enable a service endpoint on that subnet. Service endpoints are enabled per service, per subnet.



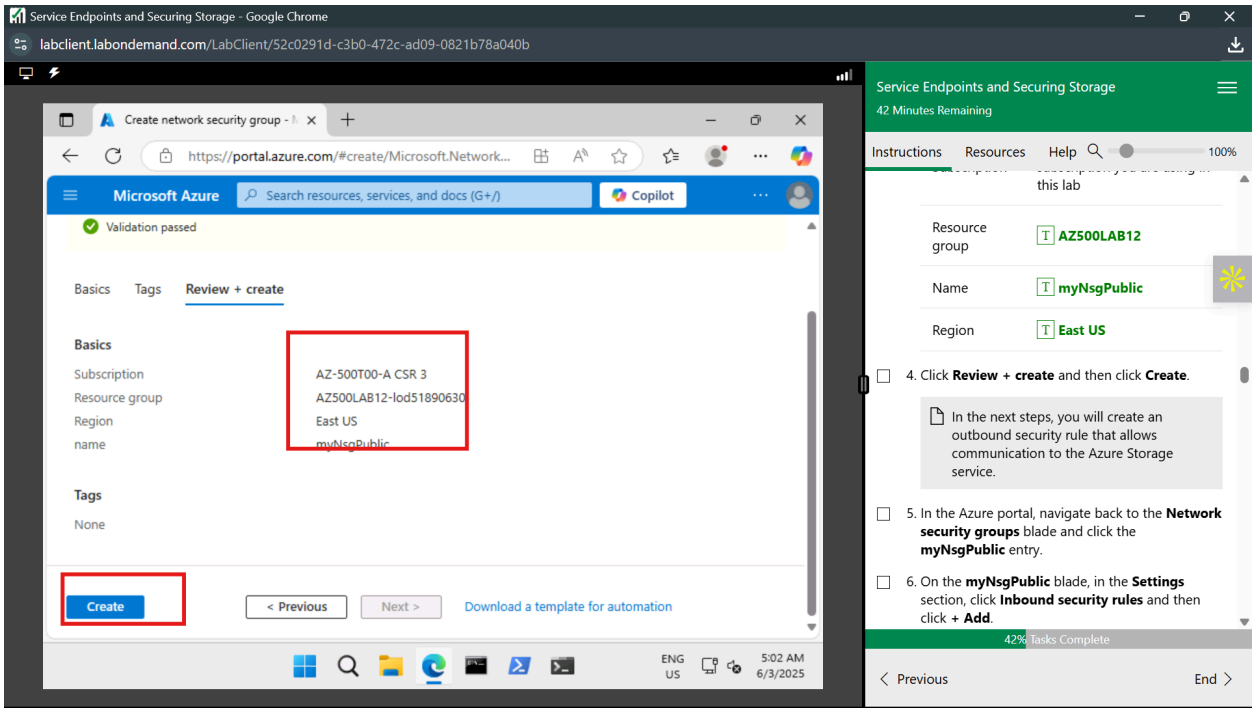
We will then create a network security group with two outbound security rules (Storage and internet) and one inbound security rule (RDP). We will also associate the network security group with the Private subnet. This will restrict outbound traffic from Azure VMs connected to that subnet.



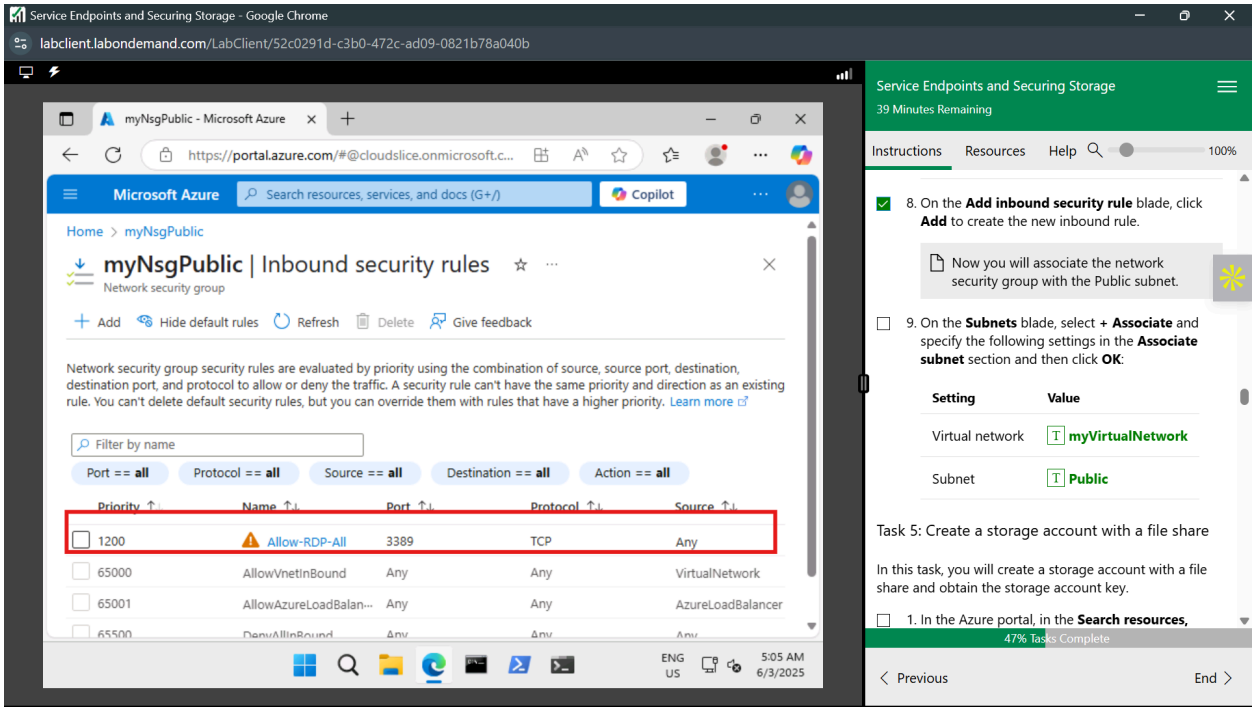


Configure a network security group to allow RDP on the public subnet

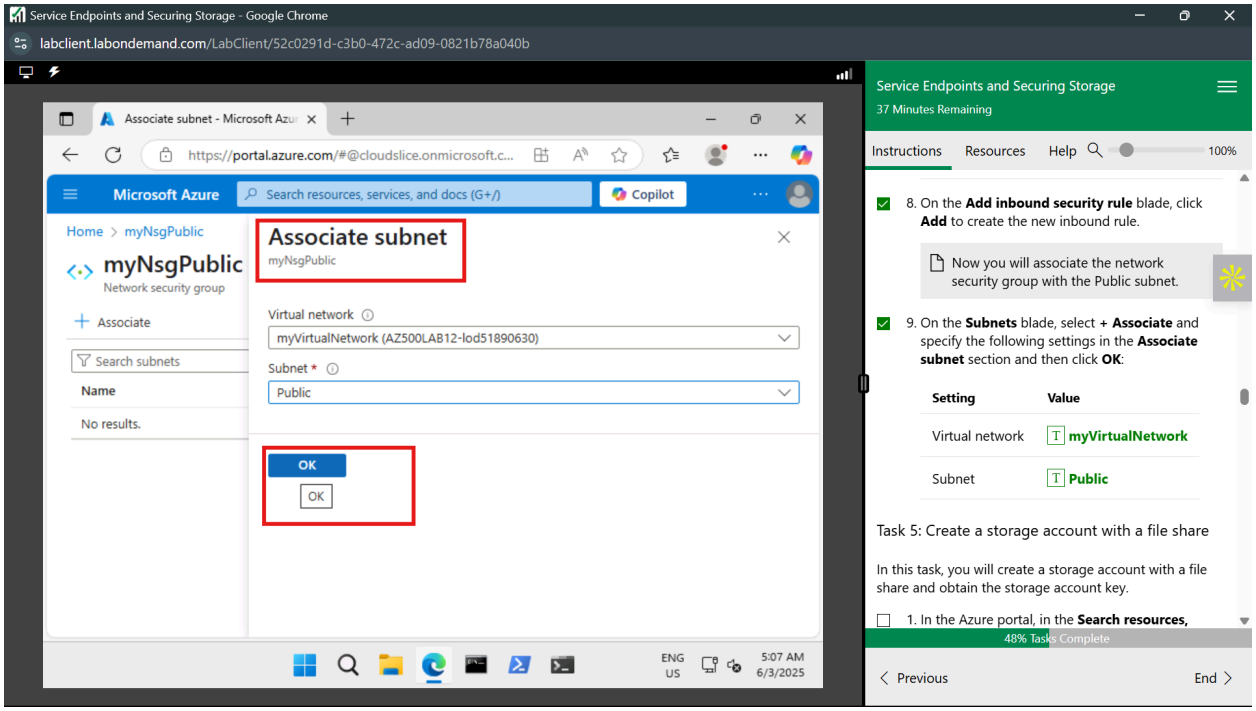
Here, we will create a network security group with one inbound security rule (RDP). We will also associate the network security group with the Public subnet. This will allow RDP access to the Public VM.



We then create the rule as follows;

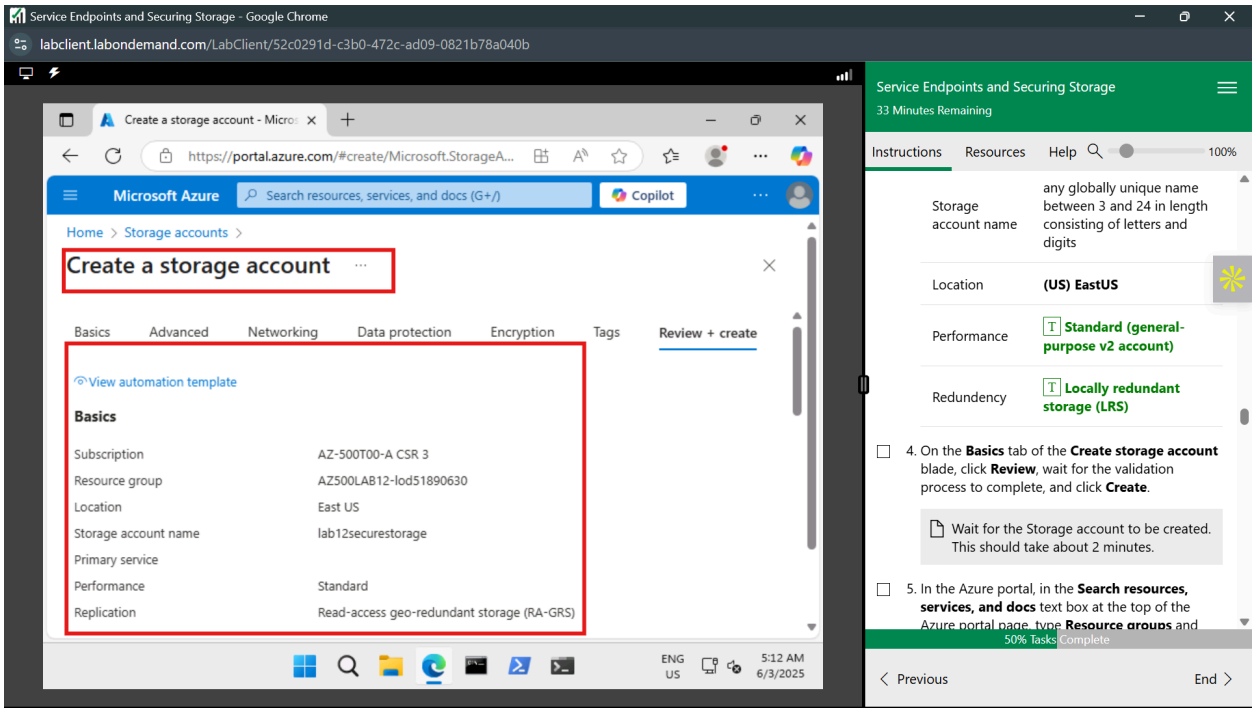


Then we associate it with our public subnet.

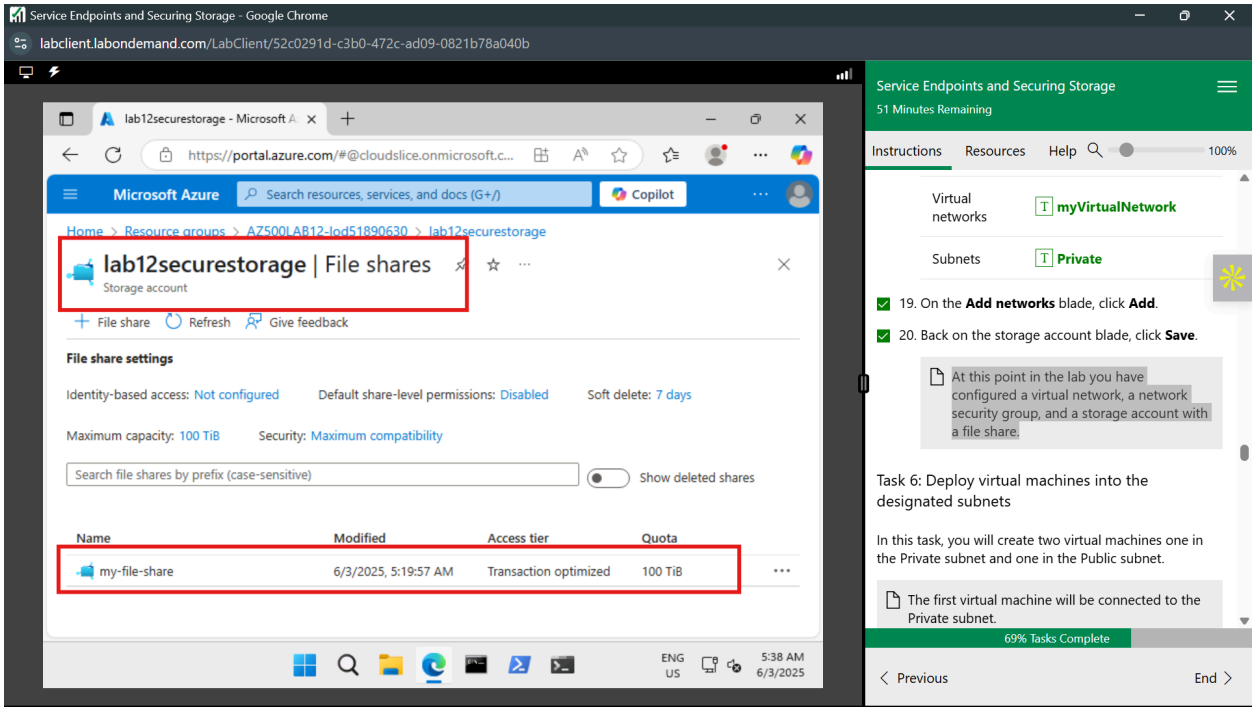


Create a storage account with a file share

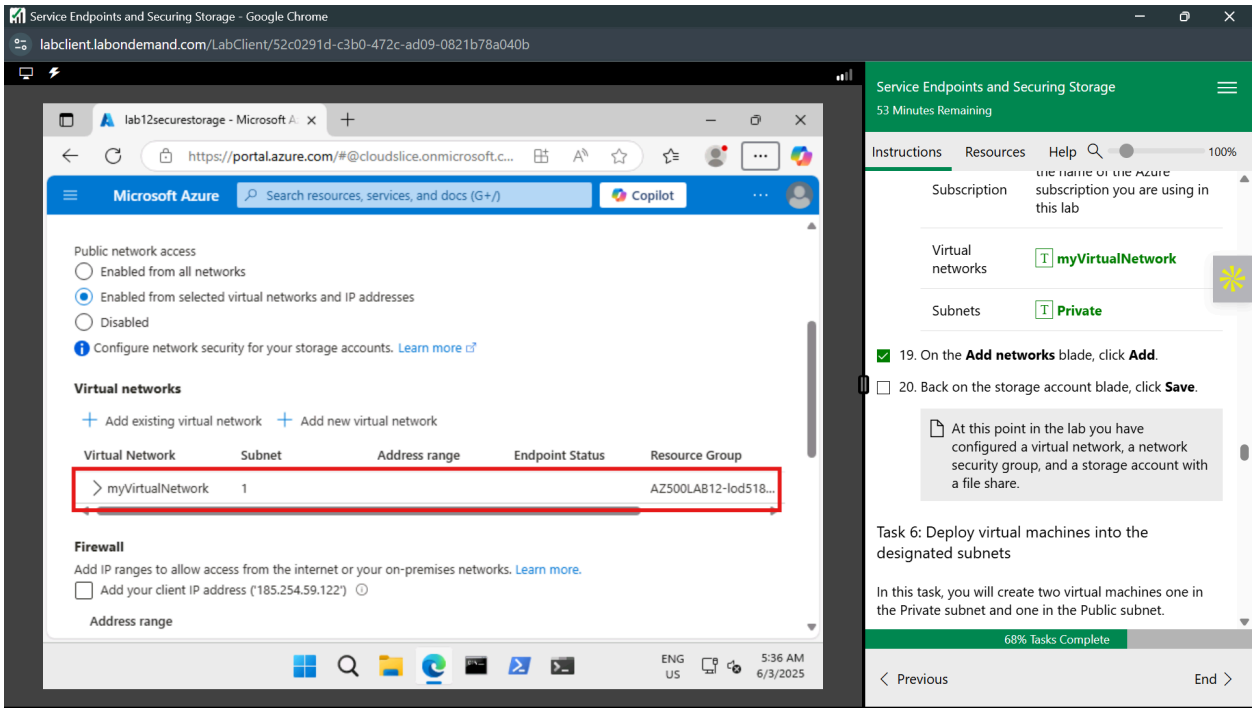
Here, we will create a storage account with a file share and obtain the storage account key.



We created a file share service under our storage account.



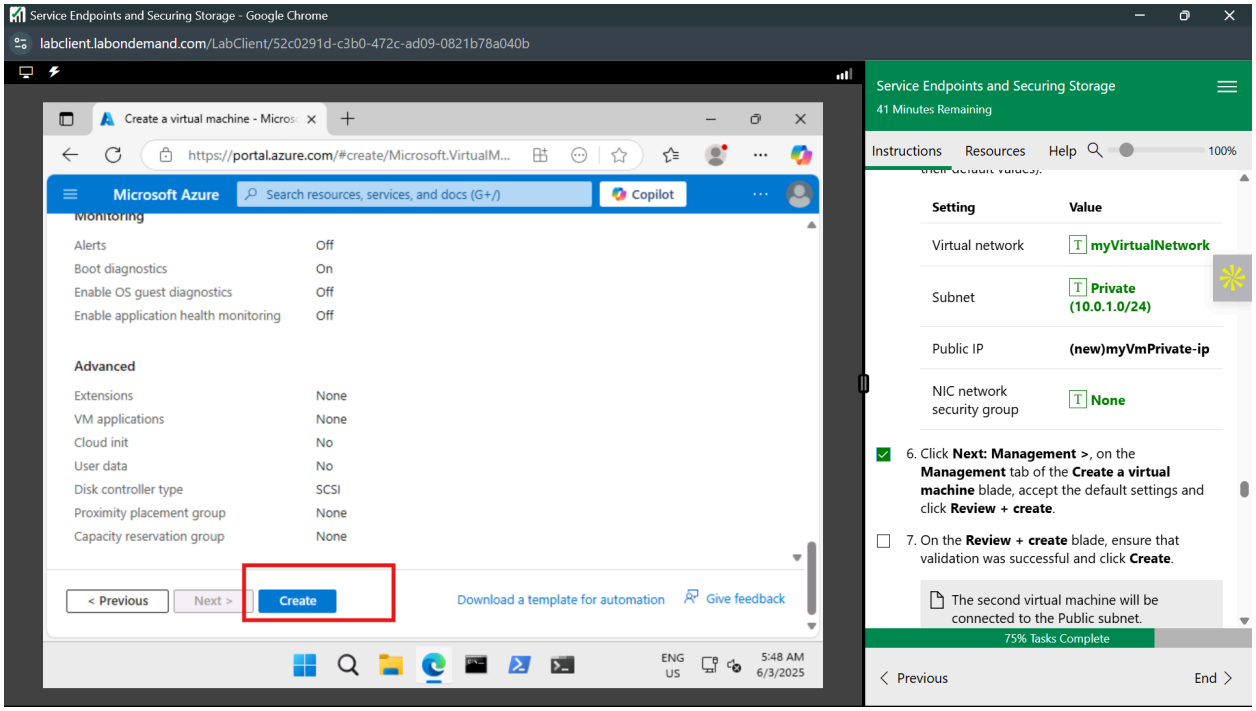
And then we added it to our virtual network



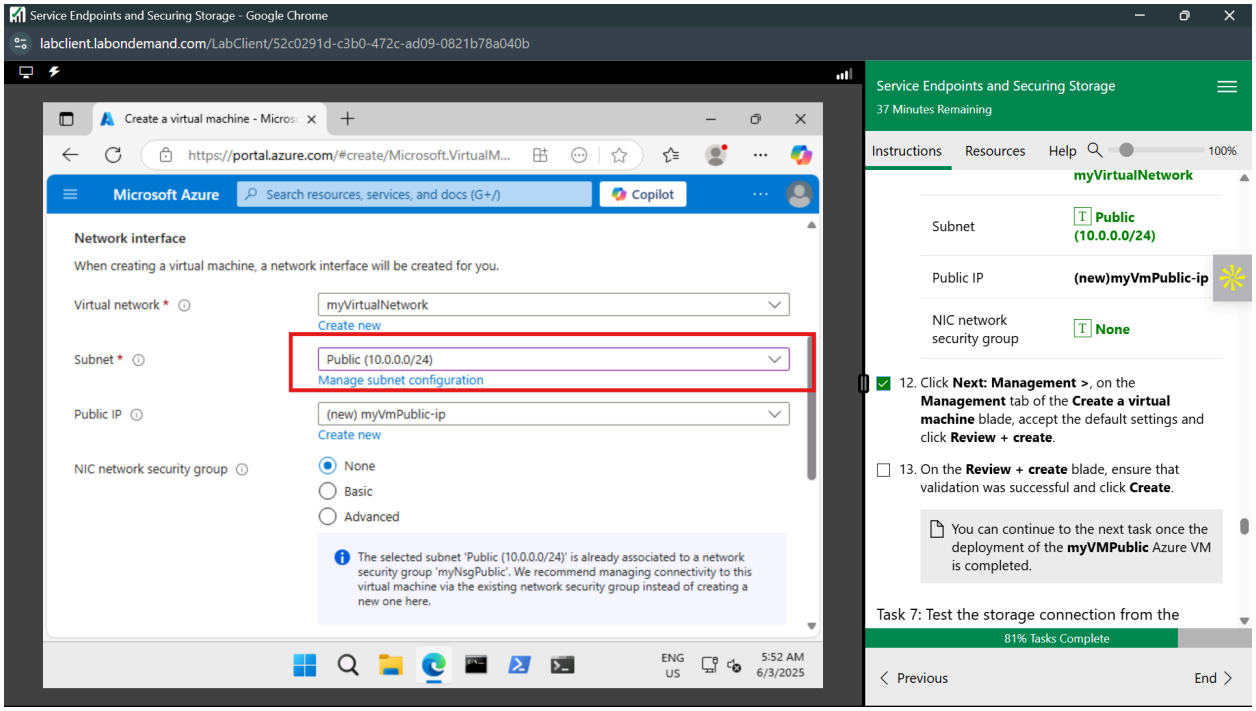
At this point in the lab, we have configured a virtual network, a network security group, and a storage account with a file share.

Deploy virtual machines into the designated subnets

Here, we will create two virtual machines, one in the Private subnet and one in the Public subnet.

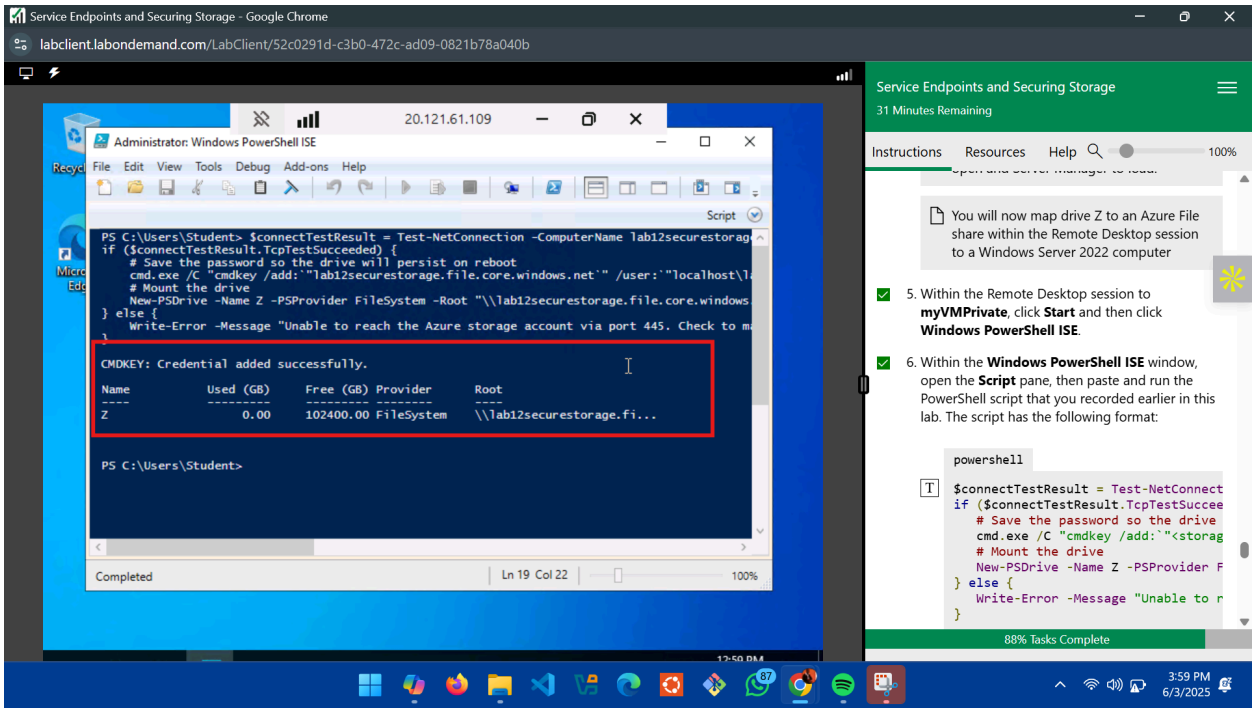


The second virtual machine will be connected to the Public subnet.

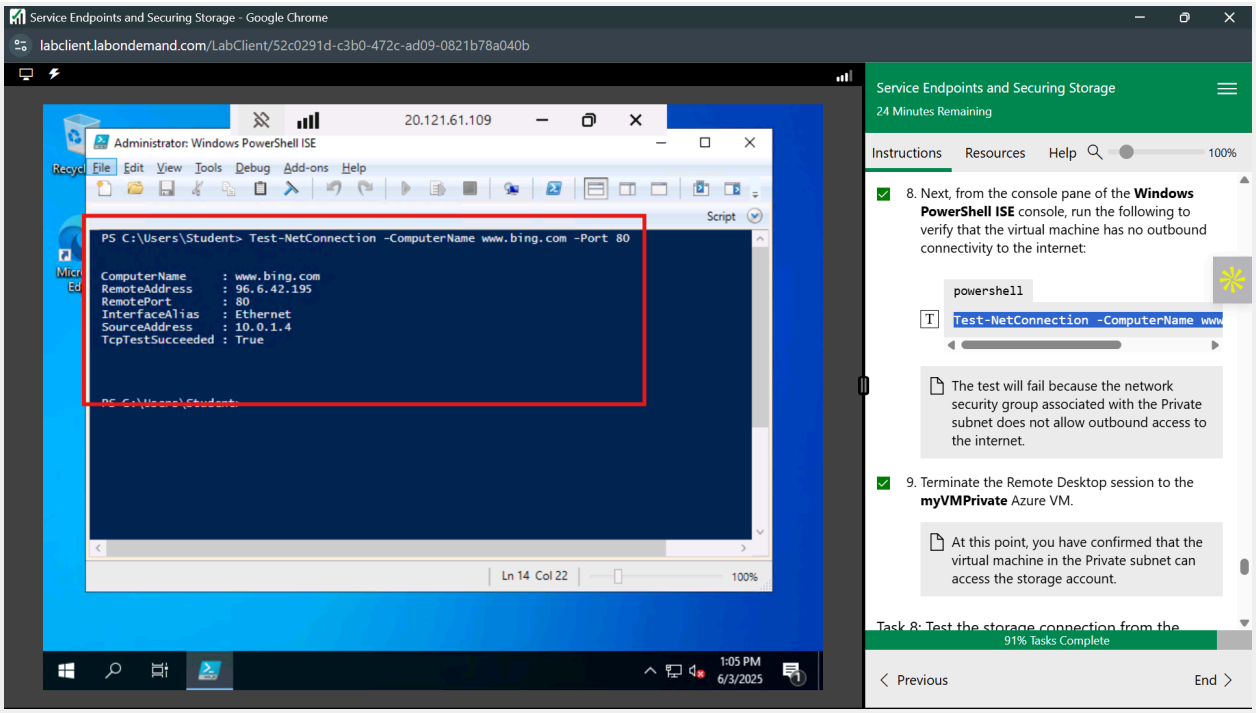


Test the storage connection from the private subnet to confirm that access is allowed

We will connect to the myVMPrivate virtual machine via Remote Desktop and map a drive to the file share.

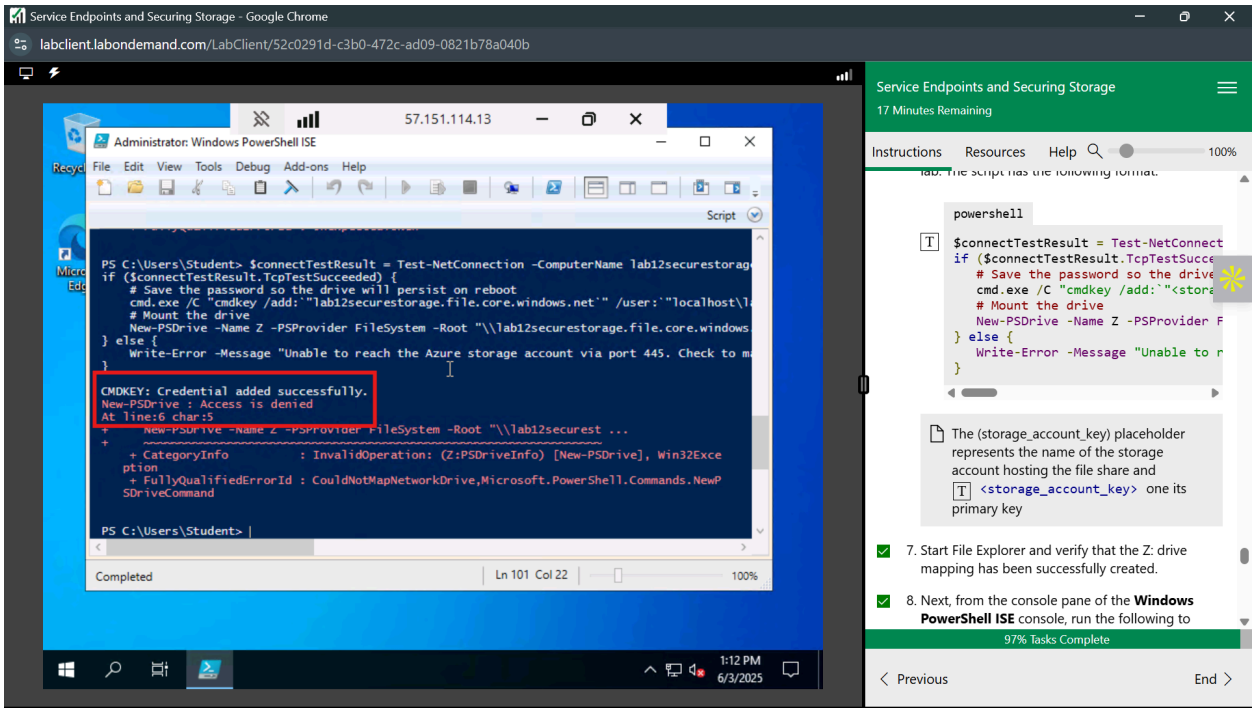


We then test the connection using the `Test-NetConnection -ComputerName www.bing.com -Port 80`



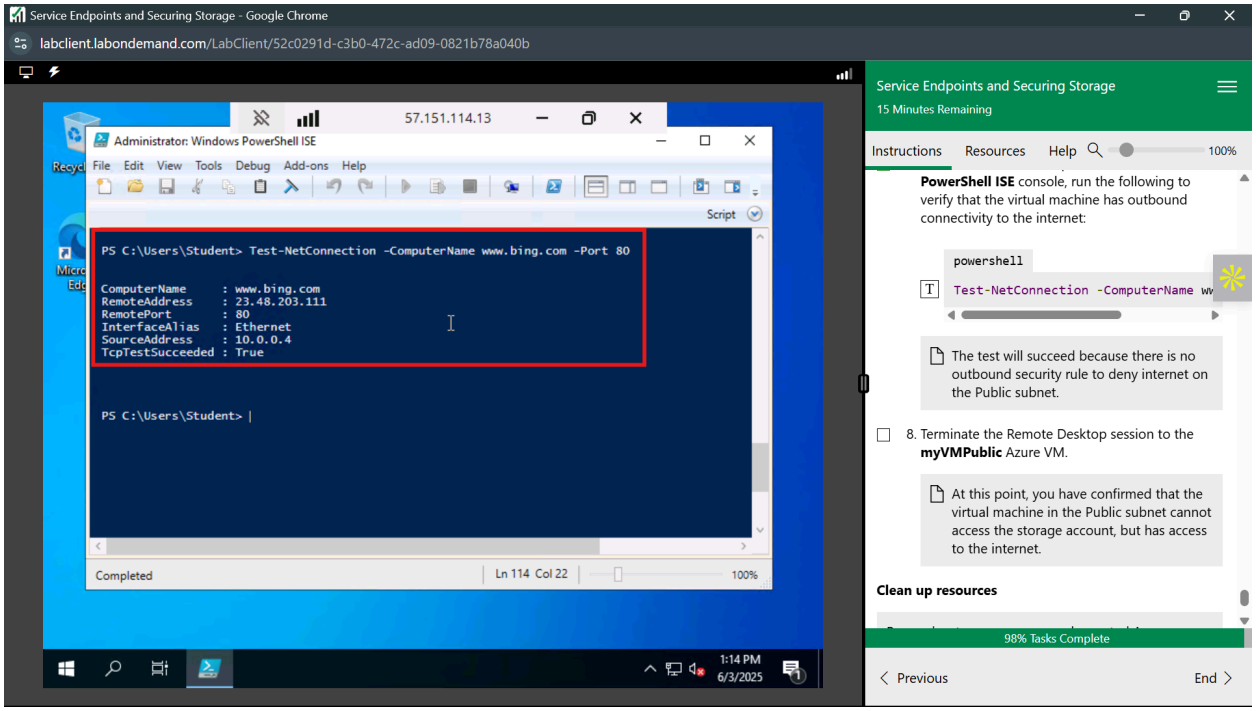
Test the storage connection from the public subnet to confirm that access is denied

We will now map drive Z to an Azure File share within the Remote Desktop session to a Windows Server 2022 computer



Access is denied because the myVmPublic virtual machine is deployed in the Public subnet. The Public subnet does not have a service endpoint enabled for the Azure Storage. The storage account only allows network access from the Private subnet.

We then test for outbound connectivity with the `Test-NetConnection -ComputerName www.bing.com -Port 80` command.



The test will succeed because there is no outbound security rule to deny internet access on the Public subnet.

Conclusion

To conclude, we were able to demonstrate how to secure access of our storage service through network private service endpoints. We were able to keep the traffic of our storage endpoint within the Azure backbone.