😊 Firewall and Network Setting

(Public and Private Endpoints)

Public Endpoints:

Definition:

- Public endpoints are the default endpoints provided by Azure Storage for accessing storage services such as Blob, Table, Queue, and File services over the public internet.

Features:

1. **Accessibility:**
    - Accessible from any network, including the internet.
    - Allows direct access to Azure Storage using the storage account's URL.
2. **Security:**
    - Secure by default through HTTPS.
    - You can configure firewalls and virtual networks to restrict access.
    - Supports Shared Access Signatures (SAS) and Azure Active Directory (AAD) for secure access.
3. **Use Cases:**
    - Suitable for scenarios where the storage needs to be accessed from various locations and networks.
    - Ideal for public-facing applications or when you want to share files with users over the internet.

Private Endpoints:

Definition:

- Private endpoints are network interfaces that connect you privately and securely to a service powered by Azure Private Link. They provide private connectivity from a virtual network (VNet) to Azure Storage without exposing the storage service to the public internet.

Features:

1. **Accessibility:**
    - Accessible only within the VNet or peered VNets.
    - Uses a private IP address from the VNet's address space.

2. **Security:**
    - Completely isolates the traffic to the storage account within your VNet.
    - Does not traverse the public internet, reducing exposure to threats.
    - Supports network security groups (NSGs) to further control access.
3. **Use Cases:**
    - Suitable for internal applications that require secure access to Azure Storage.
    - Ideal for compliance and security-sensitive applications that need to avoid public internet exposure.
    - Enhances security by allowing access to storage accounts only from within specified VNets.

Comparison

Feature	Public Endpoint	Private Endpoint
Network Access	Accessible from the internet	Accessible only within the VNet
IP Address	Public IP address	Private IP address from VNet's address space
Security	Secured via HTTPS, firewalls, SAS, and AAD	Secured via VNet isolation and NSGs
Use Case	Public-facing applications, internet-based access	Internal applications, compliance, and security-sensitive use

Configuring Endpoints in Azure Storage

Configuring Public Endpoints:

1. **Default Setting:**
    - By default, all Azure Storage accounts are accessible via public endpoints.
2. **Restrict Access:**
    - You can restrict access using firewall rules to allow only specific IP addresses or ranges.
    - You can also allow access only from selected VNets.

Configuring Private Endpoints:

1. **Create a Private Endpoint:**

- Navigate to your storage account in the Azure portal.
- Select "Private endpoint connections" under the Networking section.
- Click on "Add Private Endpoint" and follow the wizard to configure the endpoint, choosing the target resource (e.g., Blob service) and specifying the VNet and subnet.

2. **DNS Configuration:**
   - Ensure that the DNS resolution for the private endpoint is configured correctly. Azure can handle this automatically if you're using Azure DNS.

By using public and private endpoints, you can control how your Azure Storage account is accessed, balancing accessibility and security based on your application's needs.

🤔 What are we doing in this Lab?

Objective:

In this lab, we are learning how to secure and manage access to an Azure Storage Account by configuring firewalls, and network settings, and creating virtual and private endpoints.

Steps:

1. **Create and Configure a Storage Account:**
   - Use an existing storage account or create a new one.
2. **Set Up a Virtual Machine (VM):**
   - Deploy a VM with Windows Server 2022.
   - Download the RDP file and log in to the VM.
   - Install Azure Storage Explorer on the VM.
   - Disable IE Enhanced Security Configuration to allow downloads.
3. **Connect Azure Storage Explorer to Storage Account:**
   - Use the access keys from the storage account to establish a connection within Azure Storage Explorer on the VM.
4. **Configure Public Endpoint Access:**
   - Initially, access to the storage account is enabled from all networks.
   - Change the setting to enable access from selected virtual networks and IP addresses only.
   - Add the client IP address to the firewall settings to limit access.

    - Verify that the VM cannot access the storage account due to the restricted settings.

5. **Set Up Service Endpoints:**
    - Configure a service endpoint in the VM's virtual network for Microsoft Storage.
    - Add the existing virtual network to the storage account to restore access from the VM.
6. **Configure Private Endpoint:**
    - Remove the existing connection settings.
    - Create a private endpoint connection for the storage account.
    - Choose the target resource (blob) and configure the virtual network and subnet.
    - Verify that the VM can access the storage account via the private endpoint.
7. **Cleanup:**
    - Delete all created resources after completing the lab.

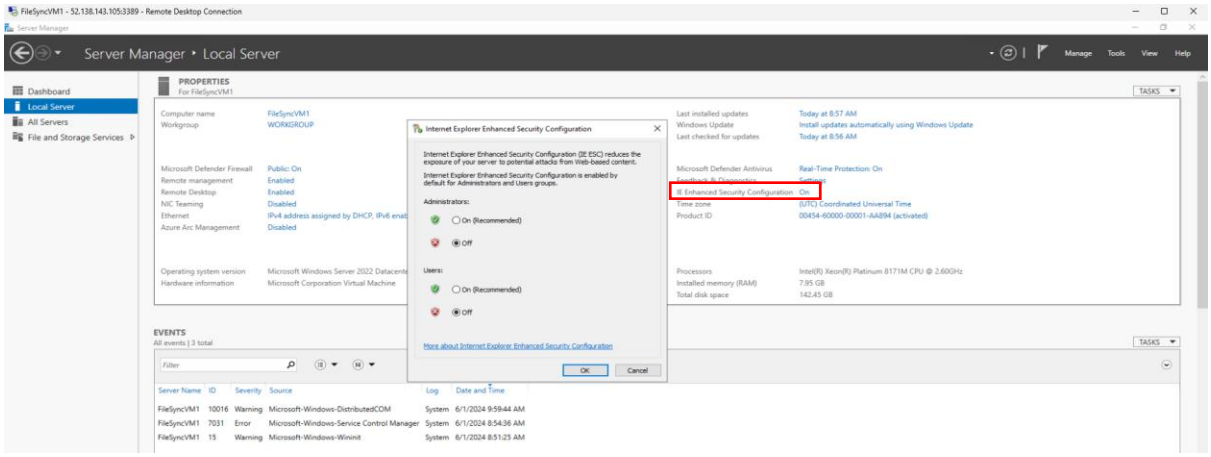
End Goal:

The end goal of this lab is to understand how to:

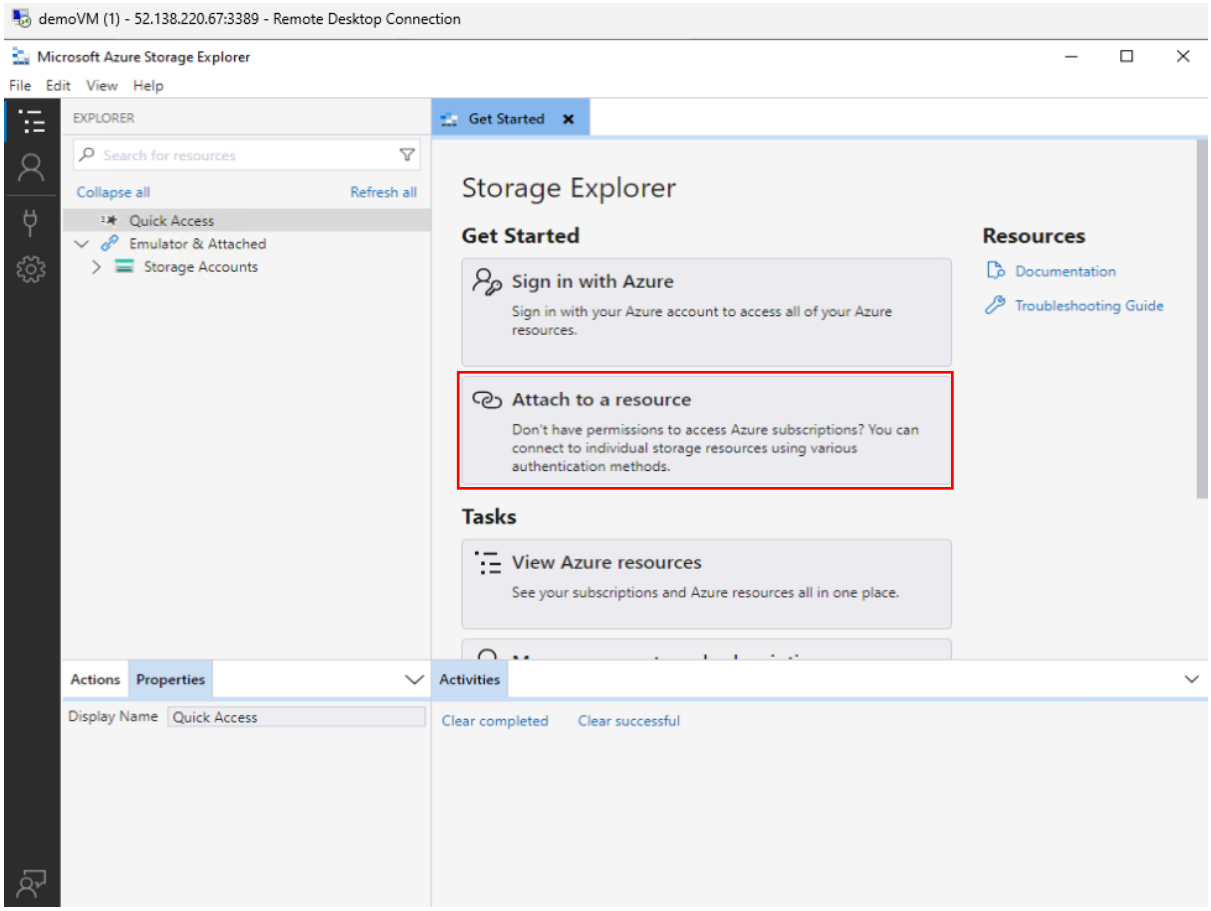
- Secure Azure Storage Accounts by limiting network access.
- Configure and manage public and private endpoints to control how resources access the storage account.
- Use Azure Storage Explorer to manage and verify access settings.

😄 To begin with the Lab

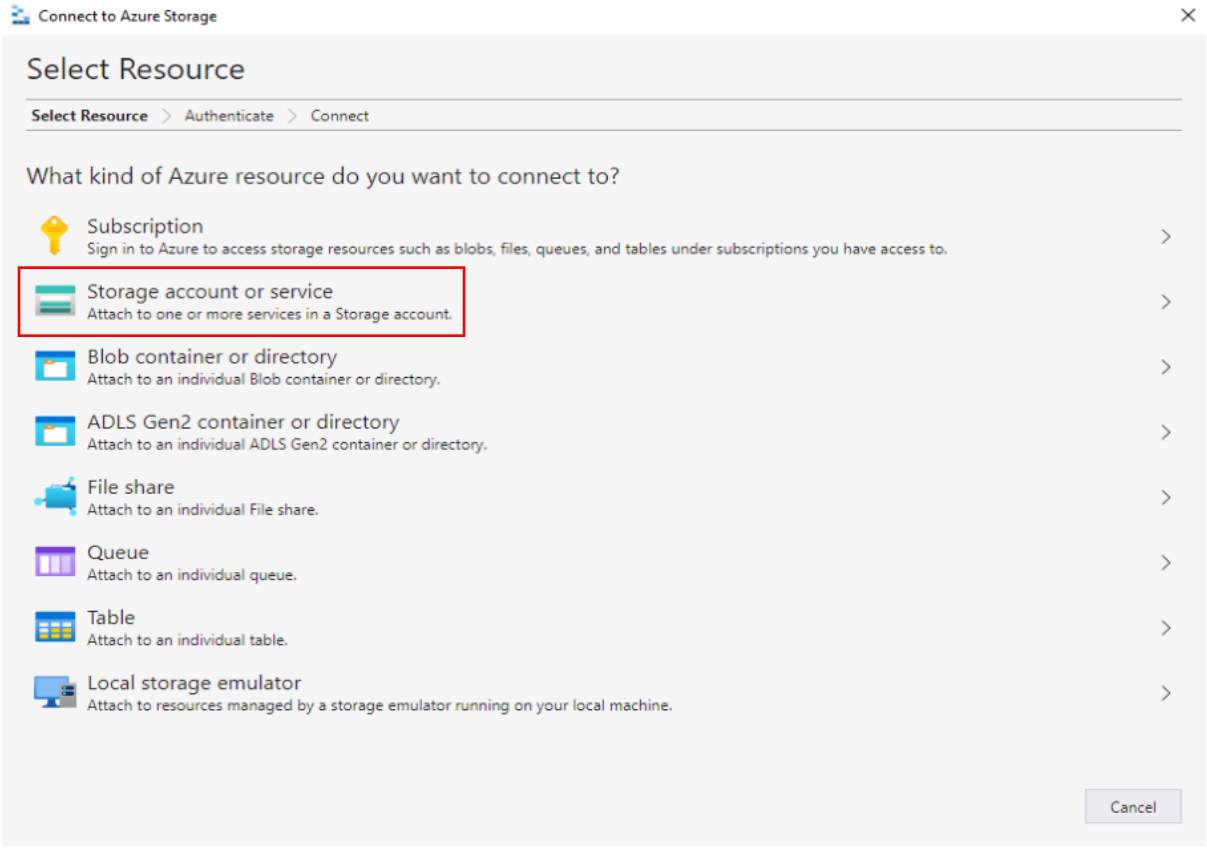
1. In this lab we are going to learn about firewalls and network settings through which we can limit the connection on our Azure Storage Account.
2. For that we should have a storage account, or we can make use of an existing storage account as well.
3. After that we need to create a Virtual Machine using Windows Server 2022.
4. Once the VM is deployed then you need to download the RDP file and login to that. In our VM we are going to download **Azure Storage Explorer**.
5. In the VM you need to go to local servers and **turn off the IE enhanced security configuration**. This will allow us to download and install the **Storage Explorer**.



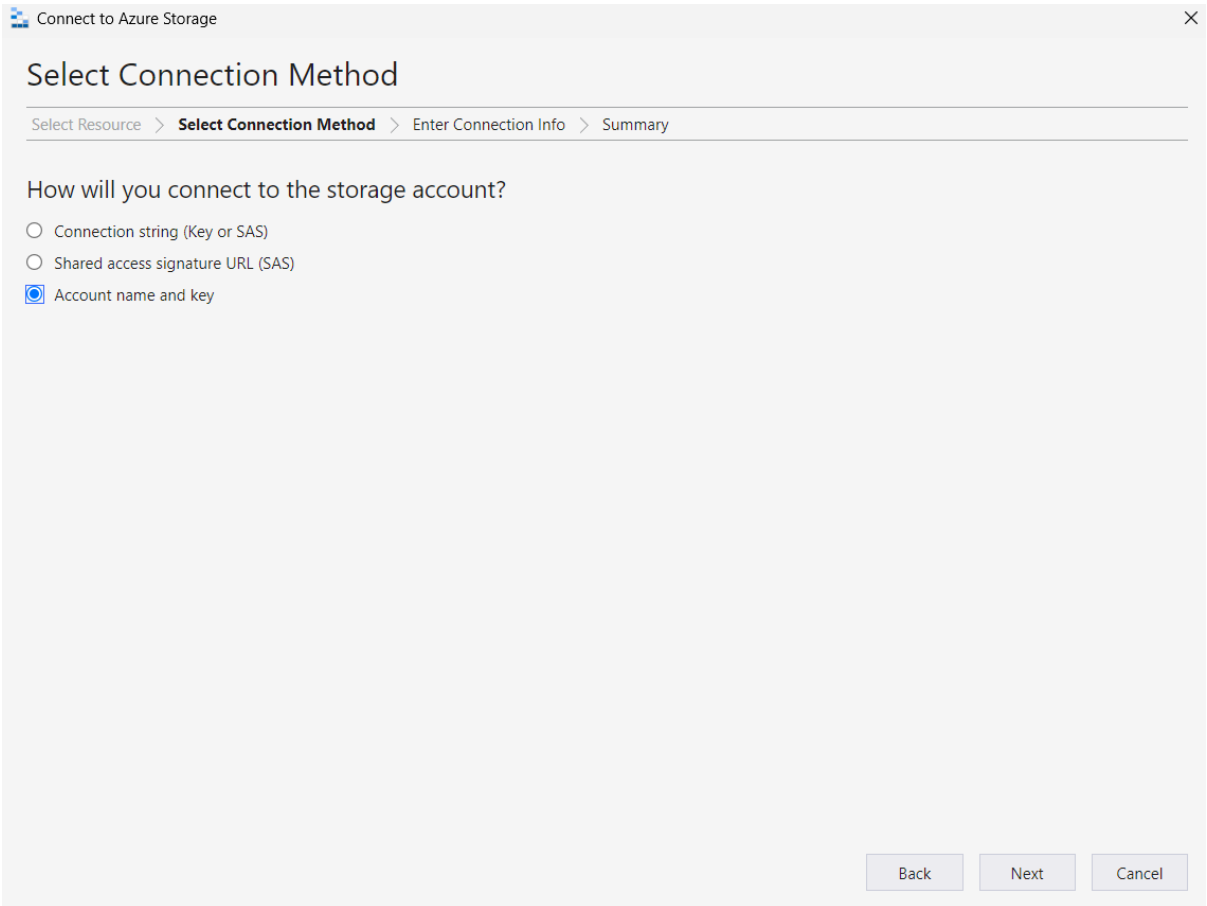
6. Then open the Edge browser search for Azure Storage Explorer and download it. After that, you need to install it too.
7. Then you need to open your storage account and take the access keys from your storage account to establish the connection between Azure Storage Explorer and your storage account in the virtual machine.
8. In your VM in the storage explorer you need to choose to attach to a resource.



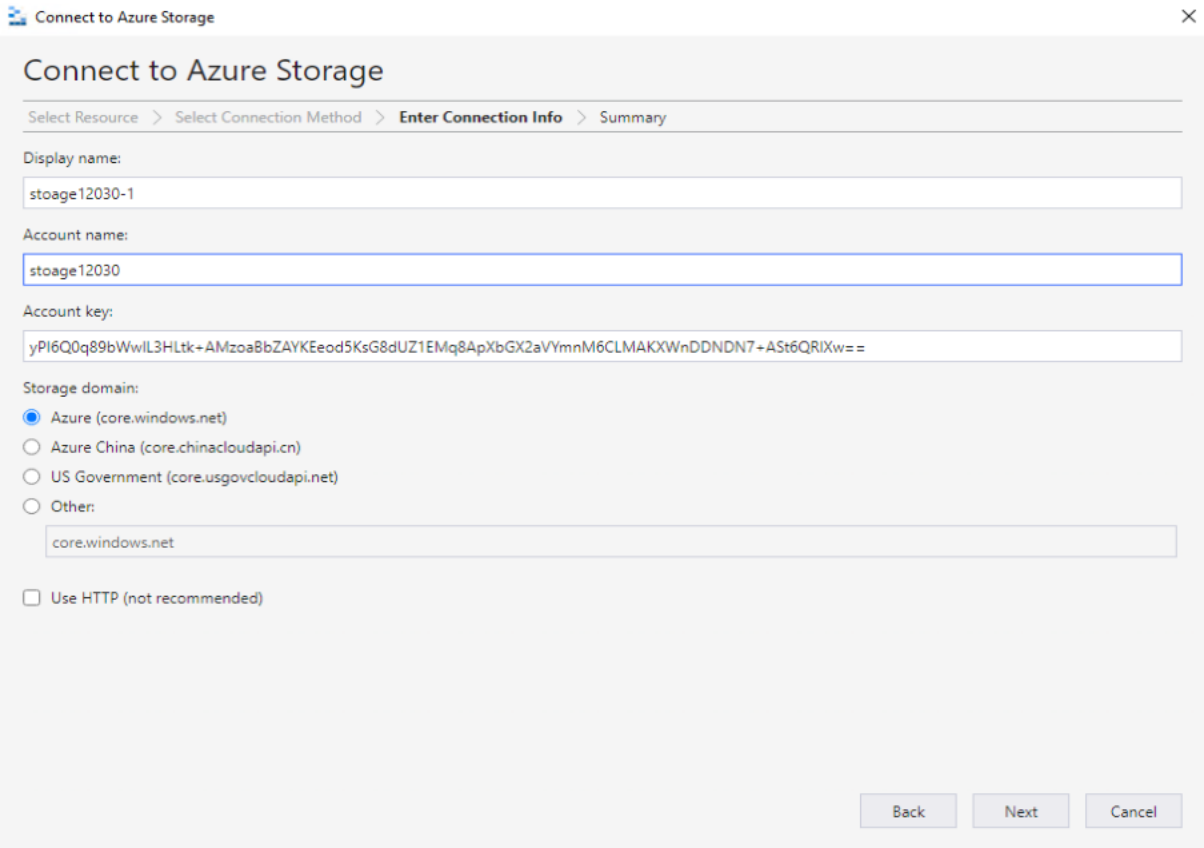
9. Then you need to choose a storage account or service.



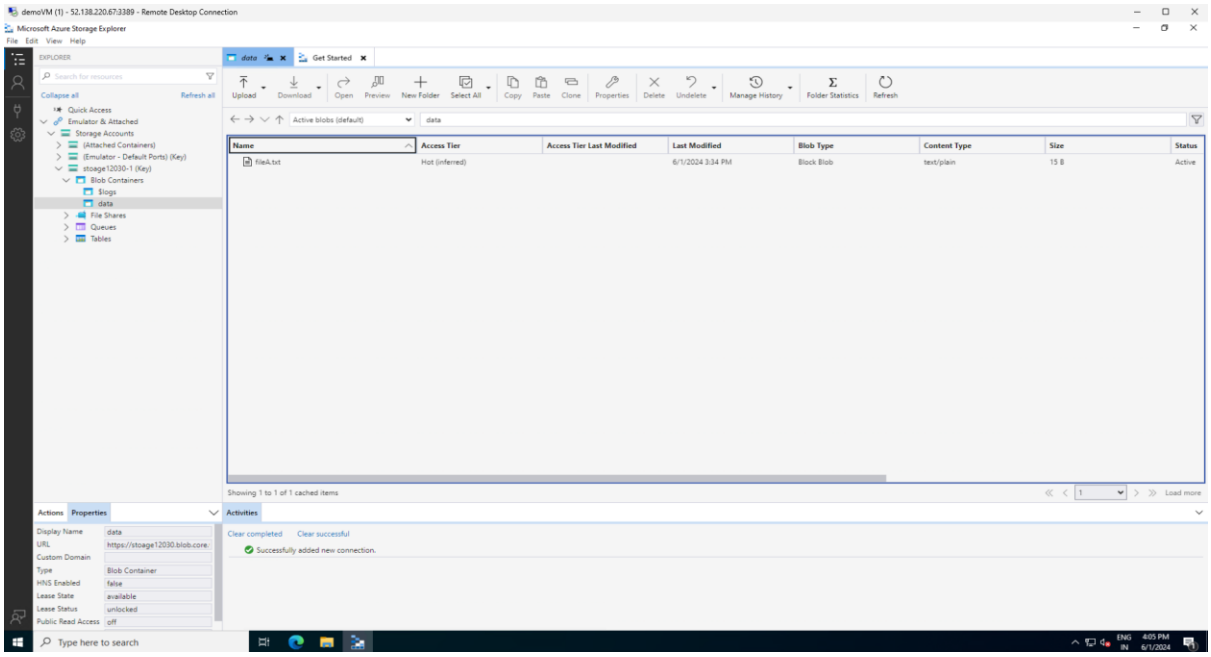
10. After that you need to choose the account name and key.



11. Here you need to put the account key, for that in your storage account go to Access keys take any one of the keys paste it here. Then copy the storage account name and put that here too. After that just click on connect it.

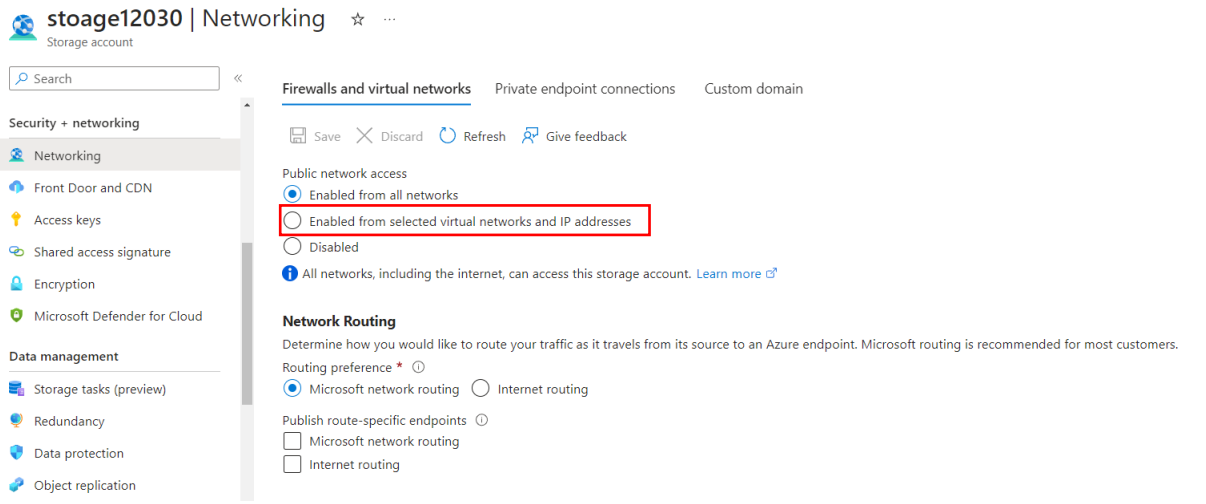


12. Below you can see that we have successfully made the connection.

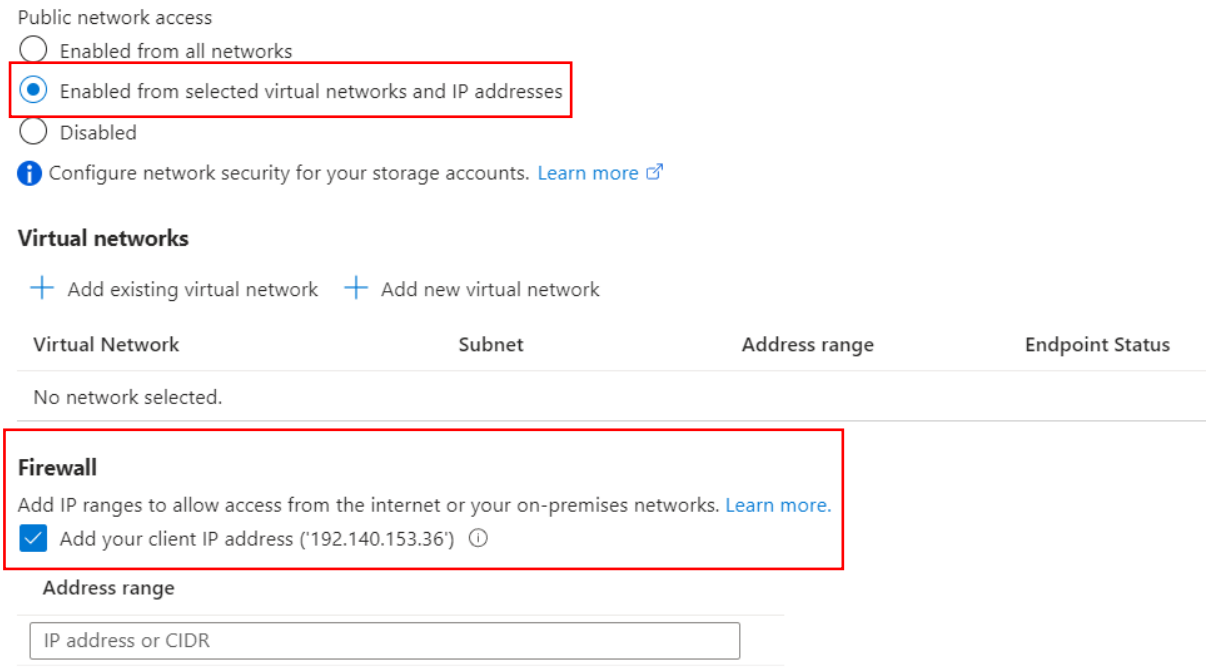


😄 Public Endpoint

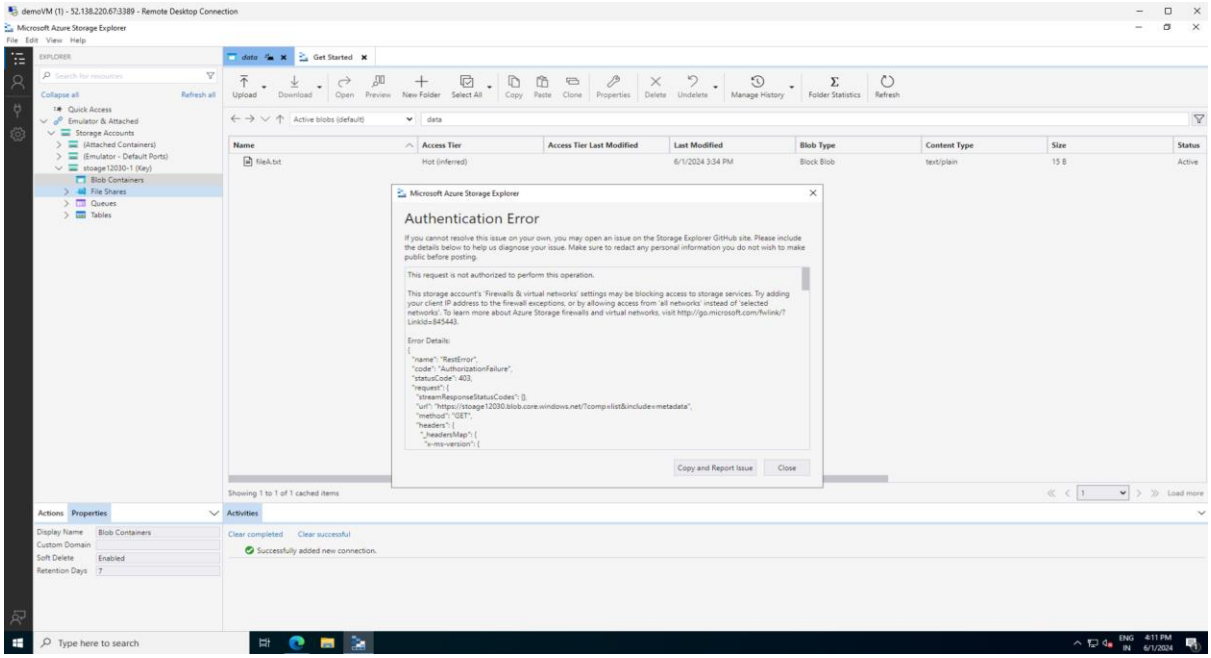
1. Now in your storage account if you go to networking then you will see that it is enabled from all the networks.
2. So, we will change it and choose **enabled from selected virtual networks and IP addresses**. This will limit the connection.



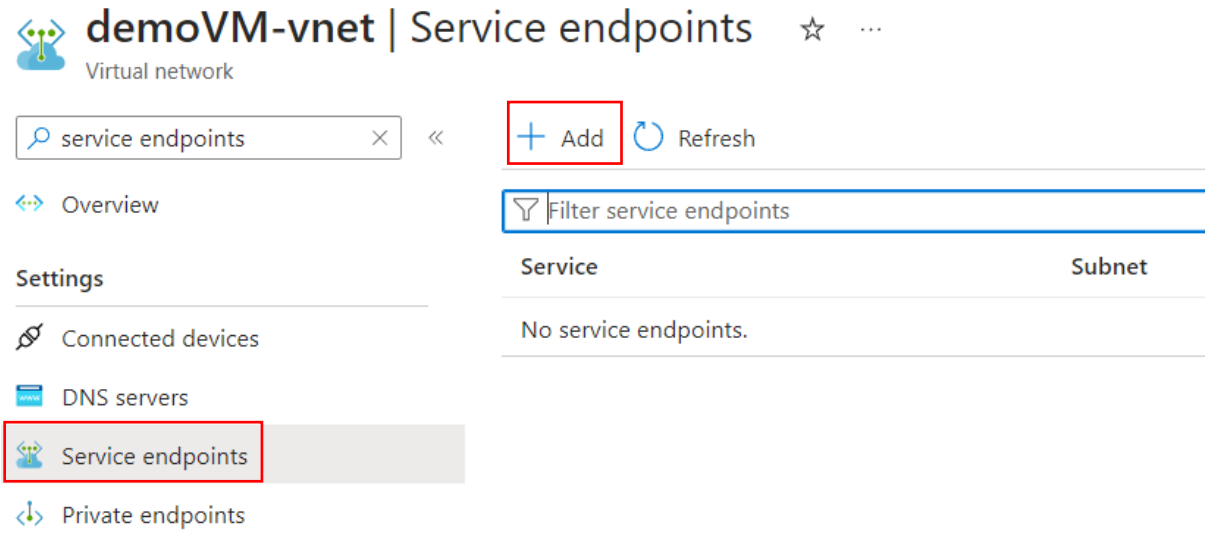
3. Now you need to scroll down and, in the firewall, choose to add your client IP address and then click on save.



4. After that go back to your VM, refresh your storage explorer, and again try to open the blob containers. You will get an error that is because now we have limited access to the storage account.

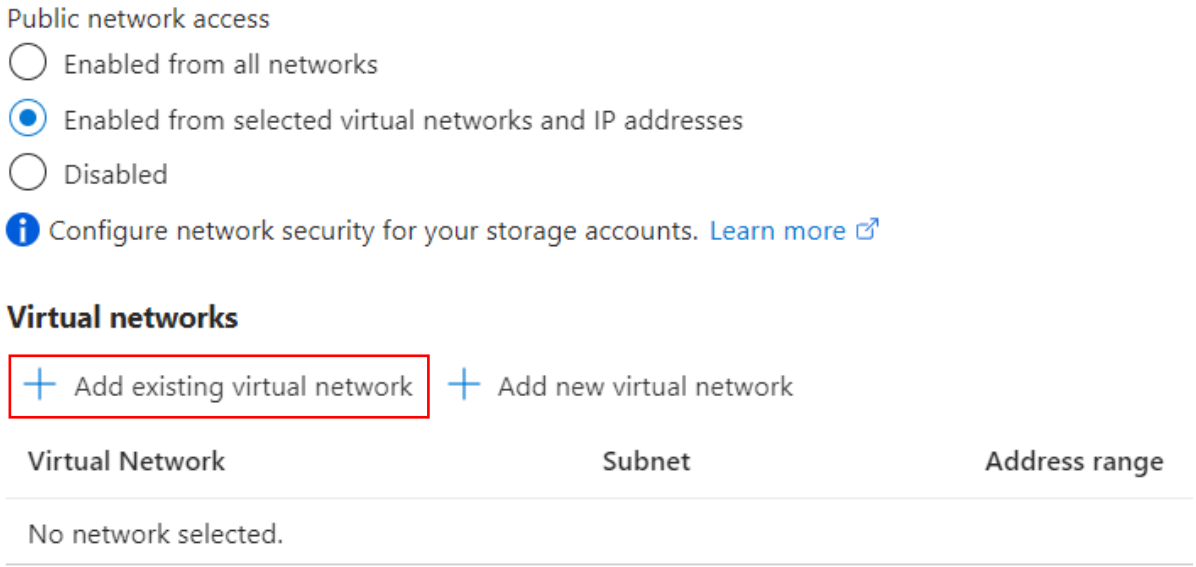


5. Now to establish the connection again in the VM for the storage account, we will use service endpoints which we can find in our VM.
6. From your VM go to Virtual network and go to service endpoints then click on add.

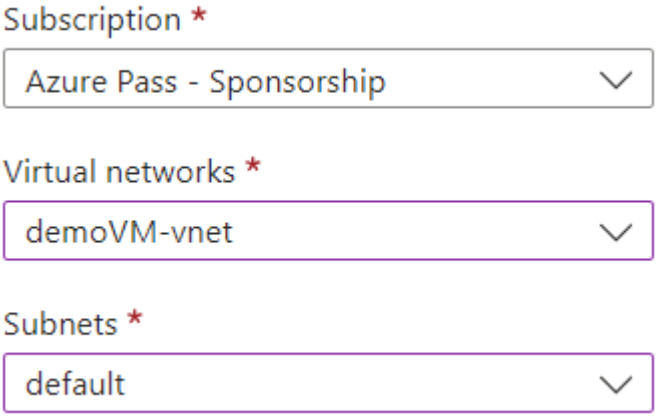


7. Now you just need to choose the service as Microsoft storage and the default subnet that holds our VM. Then just add it.

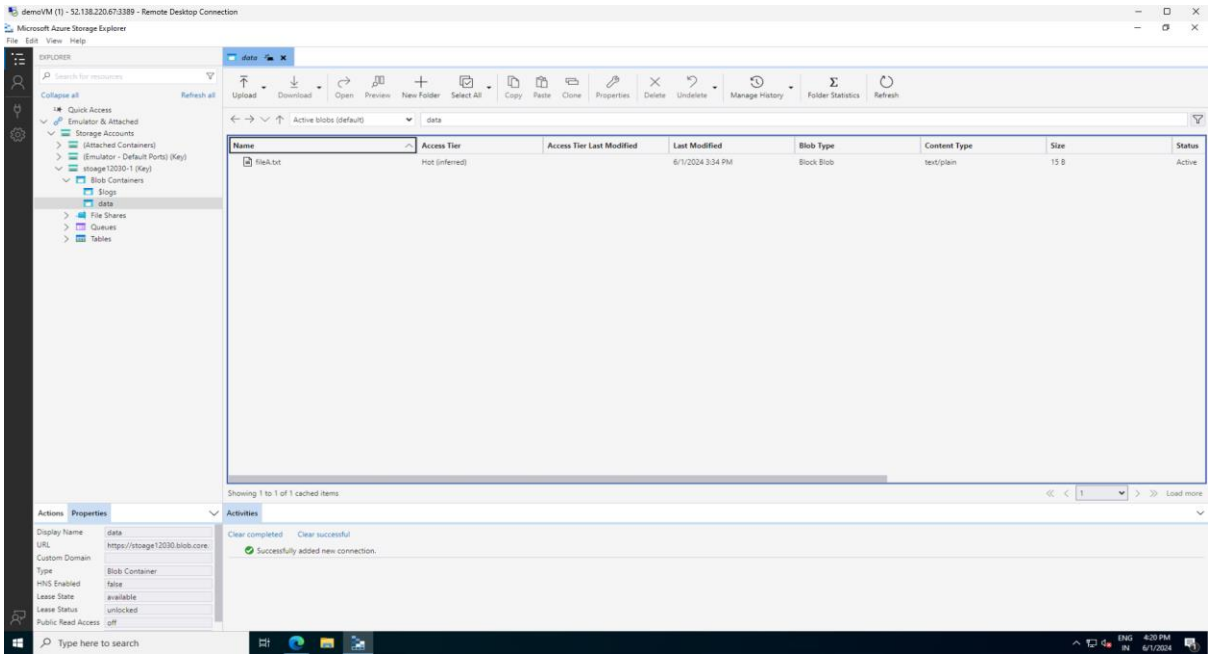
8. The first step is to add a service endpoint, once you have a service endpoint in place you can connect the virtual network or allow connections, with the service endpoint from the virtual network onto the Azure storage account.
9. After that come back to your storage account and refresh the page. Now you need to choose to add an existing virtual network.



10. Then choose the virtual network, the subnet, and click on add.

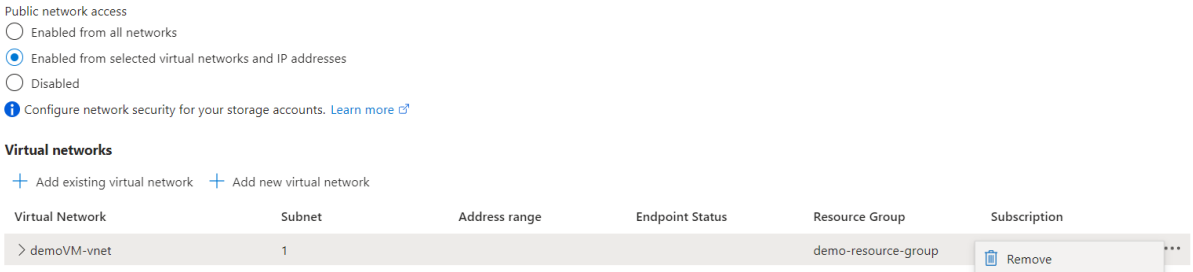


11. Go back to the VM, refresh the storage explorer and go to your blob container this time there is no error.

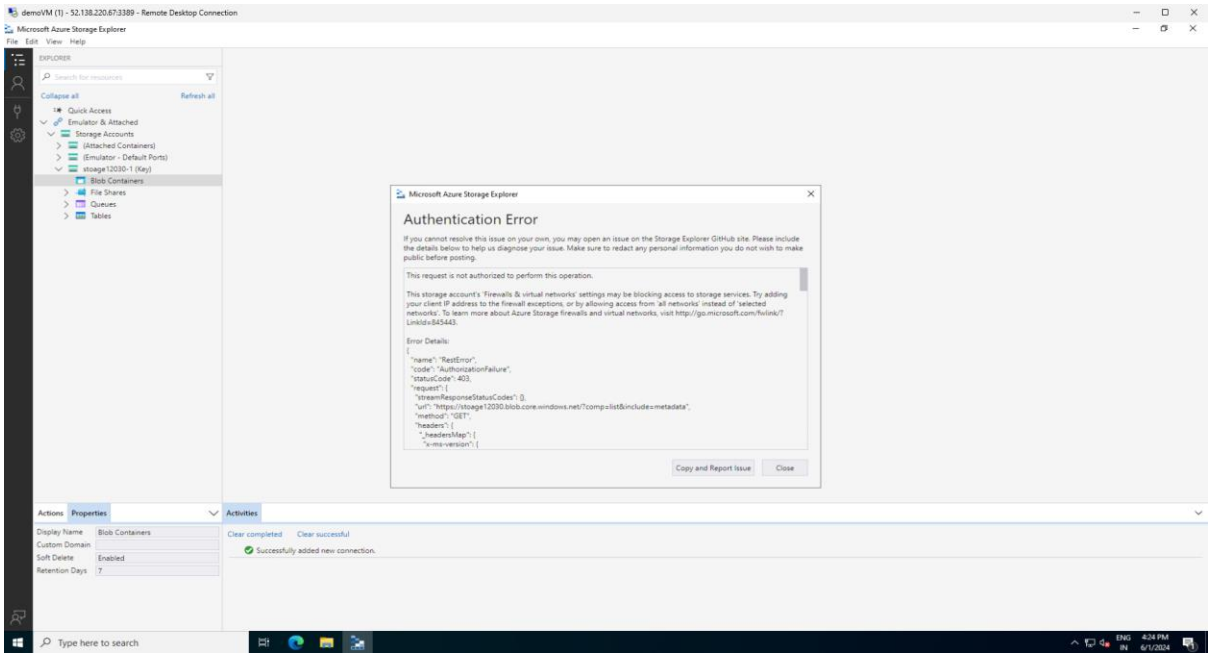


😊 Private Endpoint

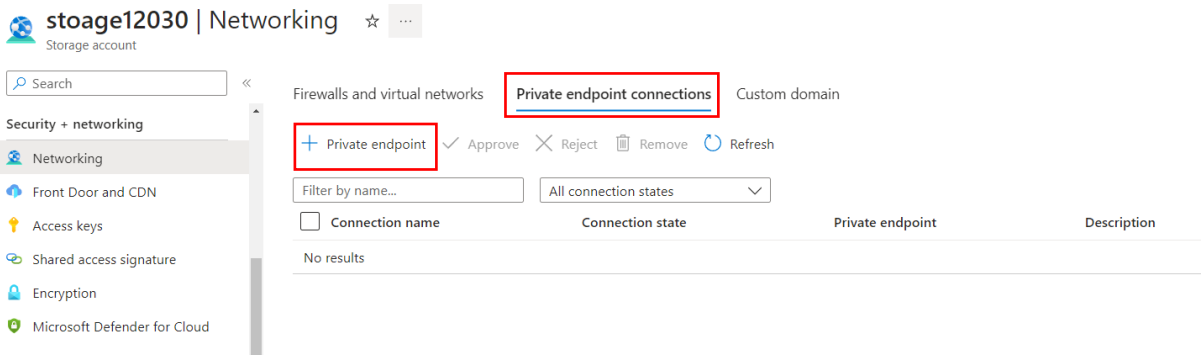
1. Now we are going to create a private endpoint connection, for that first, we are going to remove the connection that we made earlier.



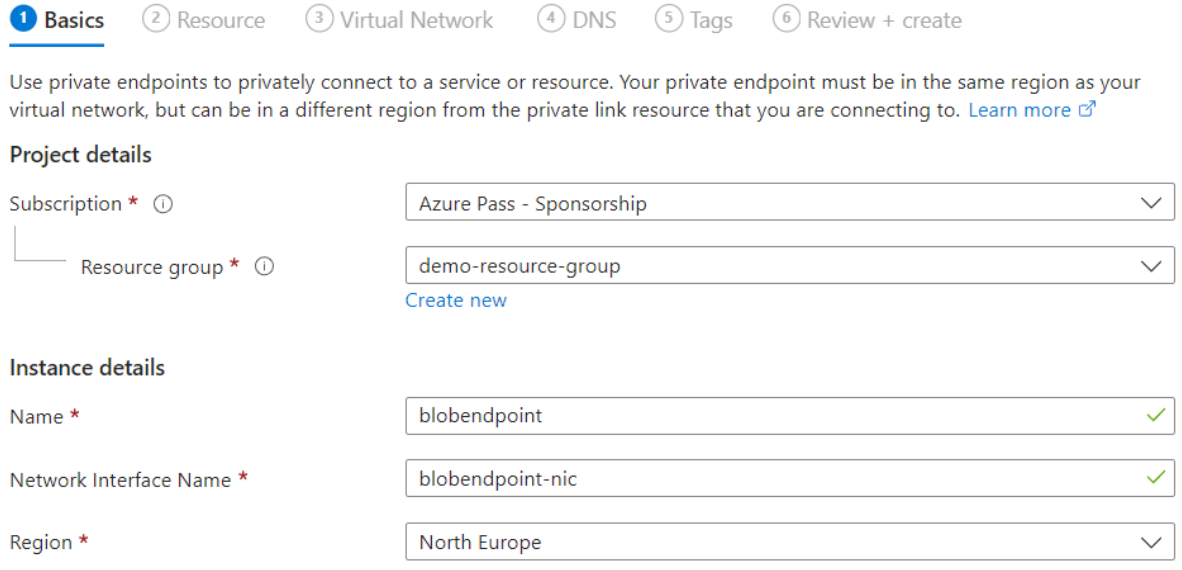
2. And if you go to your VM you will get an error message again.



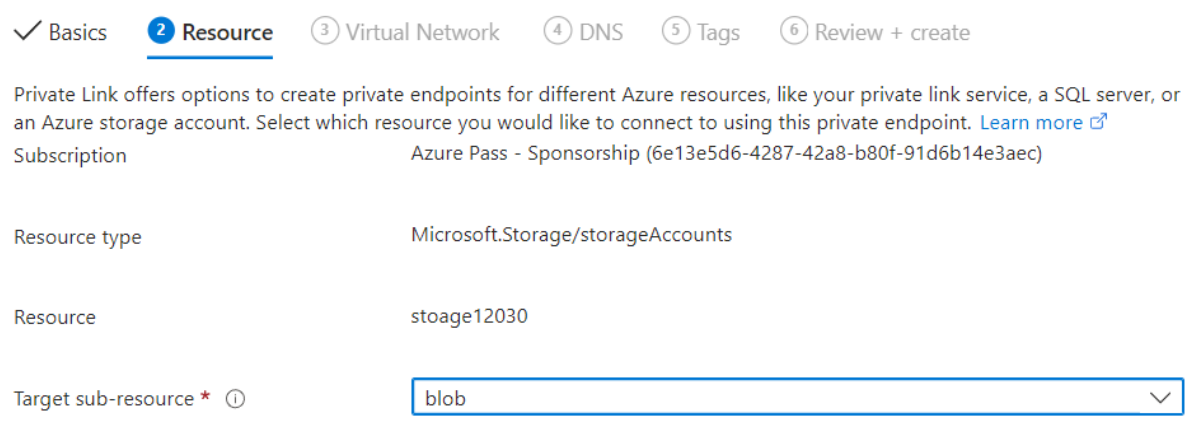
3. Now go to Private endpoint connections and click on Add Private endpoint.



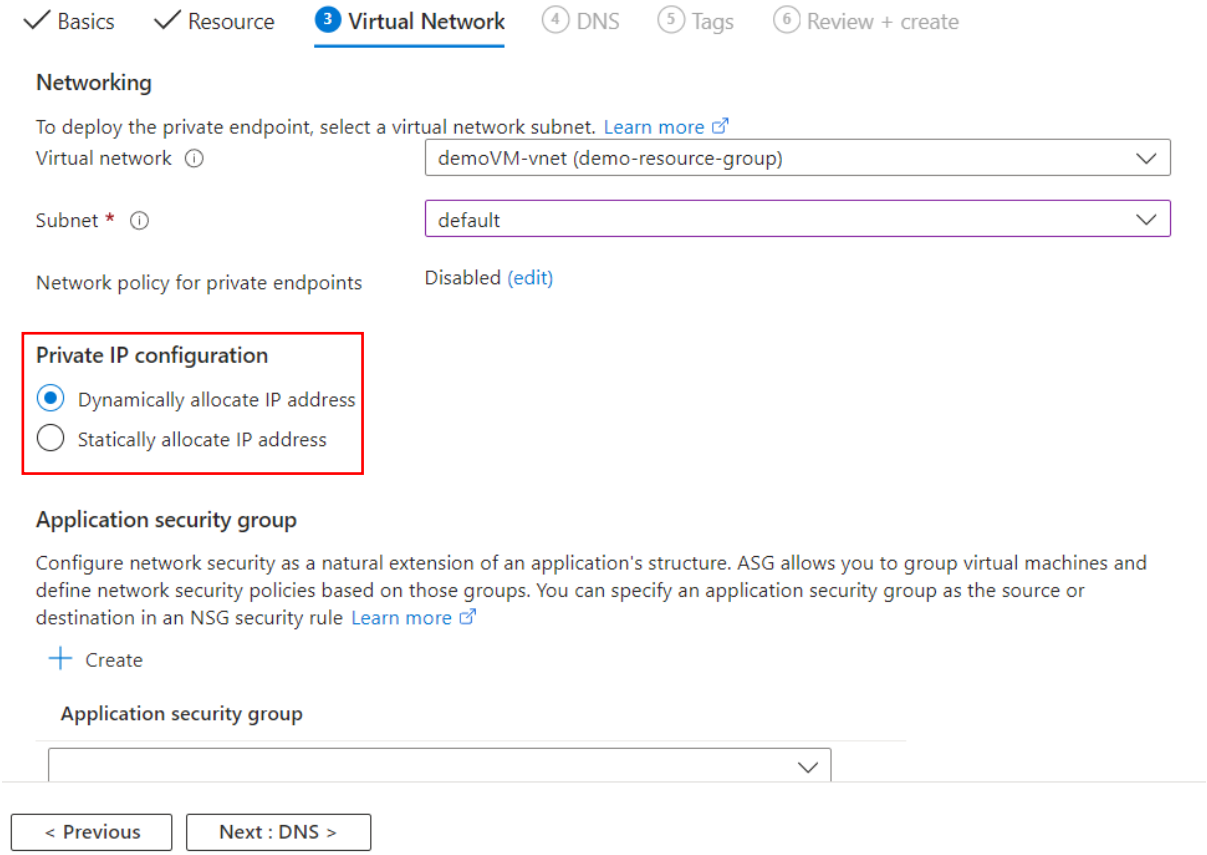
4. First, we will give it a name and choose our resource group.



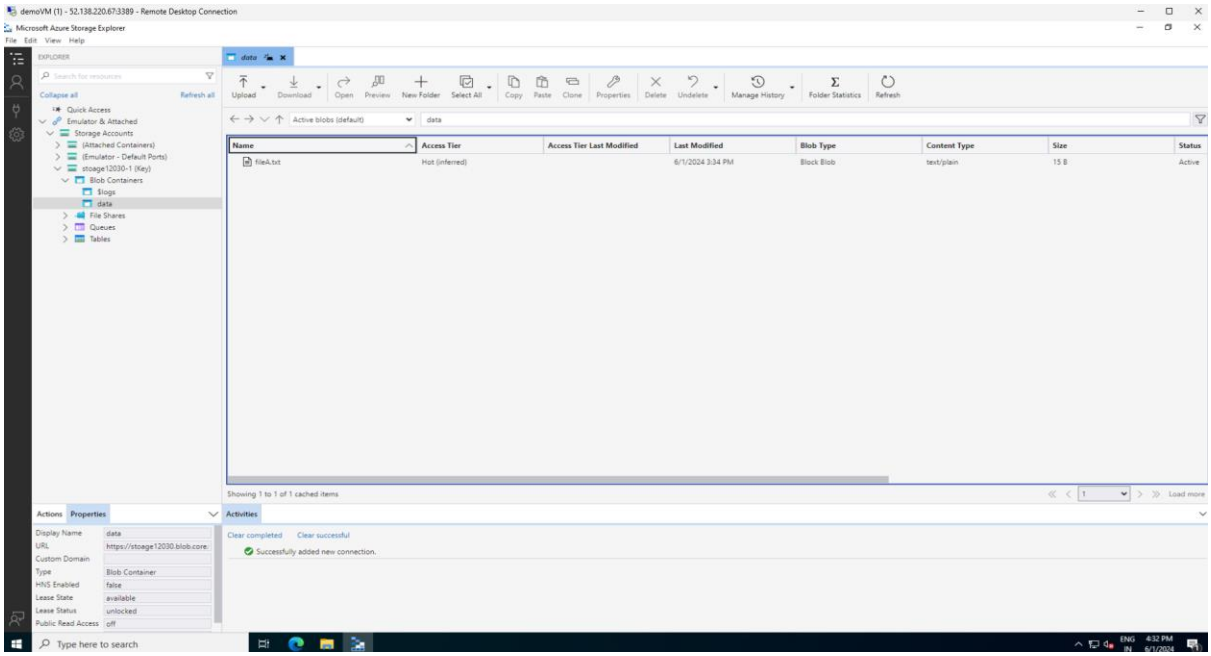
5. Then our target resource is the blob.



6. Now in the virtual network you need to choose the Virtual Network, and the subnet move to the review page, and create your private endpoint.
7. Also you will notice that it will be creating a dynamic private IP address for this endpoint.



8. Once the deployment is complete then you need to go to your VM and refresh the storage explorer again and you will be able to see your blob container.



9. Once you are done then delete your resources.