**Endpoints**

**Endpoint in Azure**

In the context of Azure, an endpoint refers to a specific entry point or access point for a service or resource within the Azure cloud platform. It's essentially a designated address or URL that allows applications or users to interact with a particular Azure service.

**Types of Endpoints in Azure**

1. **Public Endpoints:**
   * These are the standard endpoints that are publicly accessible over the internet.
   * They have a publicly routable IP address.
   * Examples:
     + Web applications accessible via a public URL.
     + APIs exposed to the internet.
2. **Private Endpoints:**
   * These endpoints provide secure and private access to Azure services within a virtual network (VNet).
   * They use a private IP address from the VNet's address space.
   * Traffic between the VNet and the service travels over the Azure backbone network, bypassing the public internet.
   * This enhances security and reduces latency.
   * Examples:
     + Accessing Azure Storage from within a VNet.
     + Connecting to Azure SQL Database privately.
3. **Service Endpoints:**
   * These allow virtual networks (Vnet) to securely and directly connect to supported Azure services.
   * They enable private IP addresses within the VNet to reach the endpoint of an Azure service without requiring a public IP address on the VNet.
   * This improves security and performance.
   * Examples:
     + Connecting to Azure Storage using service endpoints.
     + Accessing Azure Key Vault using service endpoints.
4. **Custom Endpoints:**
   * These are user-defined endpoints that allow access to specific resources or services within a virtual network.
   * They provide granular control over network traffic and security.
   * Examples:
     + Creating a custom endpoint to access a specific application running in an Azure App Service.
     + Defining a custom endpoint to allow access to a specific database server.
5. **VPN Endpoints:**
   * These endpoints are used to establish secure connections between on-premises networks and Azure virtual networks using Virtual Private Networks (VPNs).
   * They enable secure and encrypted communication between the two networks.

**Key Considerations**

* The choice of endpoint type depends on the specific requirements of your application or service.
* Public endpoints are generally simpler to set up but may have security implications.
* Private endpoints and service endpoints offer enhanced security and performance but require careful configuration.
* Custom endpoints provide the most flexibility but require advanced networking knowledge.

**Service Endpoints vs. Private Endpoints in Azure**

**Service Endpoints** and **Private Endpoints** are both mechanisms in Azure that allow you to securely connect your virtual network (VNet) to Azure services (PAAS service). However, they differ in their approach and capabilities:

**Service Endpoints:** (one-to-many internal communication)

* **Concept:** Service Endpoints allow your VNet to directly access supported Azure services (PAAS services) over the “Azure backbone network”.
* **How it works:** When you enable a service endpoint for a specific service (e.g., Storage, SQL Database), your VNet is granted direct access to that service's public endpoint. However, the traffic remains within the Azure network, bypassing the public internet.
* **Security:** While traffic stays within Azure, it still reaches the service's public endpoint.
* **Ease of use:** Relatively easy to configure.
* **Limitations:** Only works with a limited set of Azure services.
* It enables one**-**to-many internal communication between the PAAS services through the Azure Backbone Network.

**Note1:** You don't need to manage any public IP addresses specifically for service endpoints.

**Note2**: while creating service endpoint it cannot delete Public IP.

Internet

Not accessed using internet

Azure Environment

Virtual Network (Vnet)

Direct communication

Storage Account-1

Subnet

Direct communication

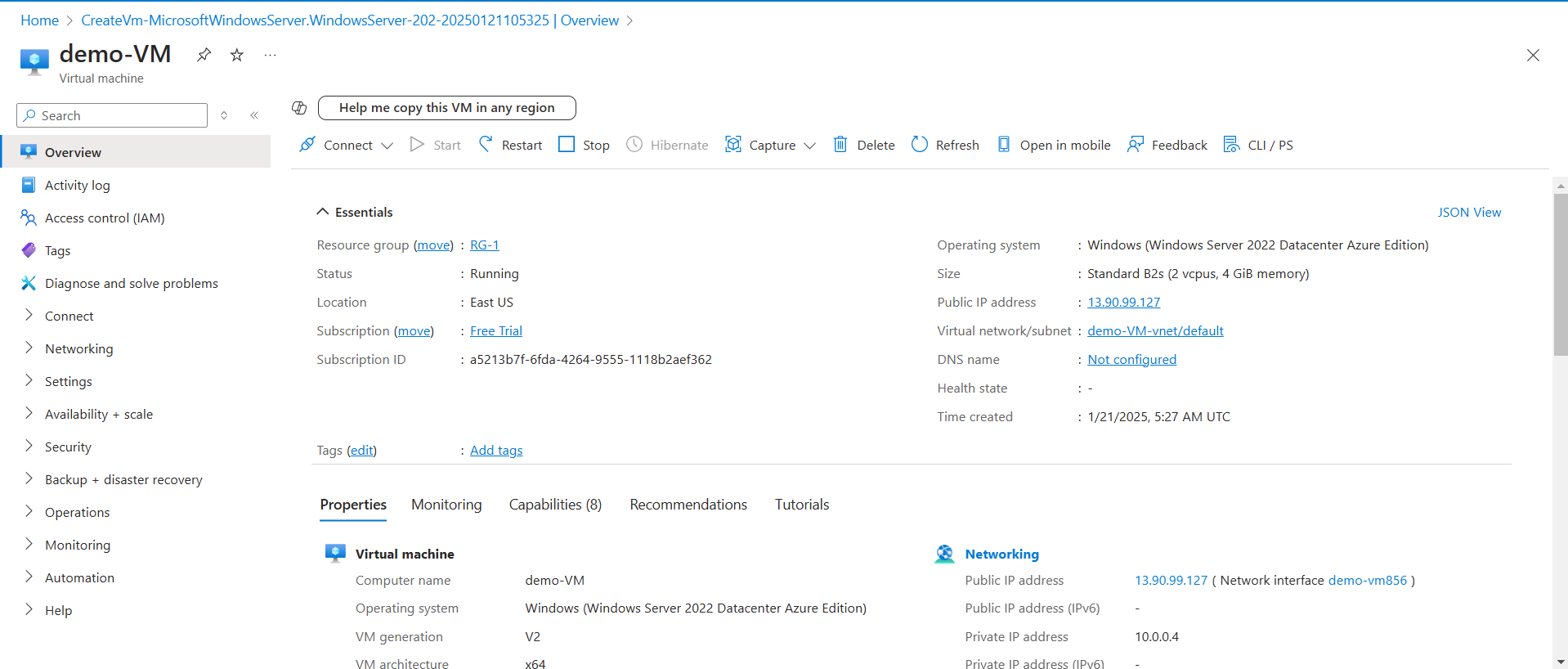
Storage Account-2

Windows VM

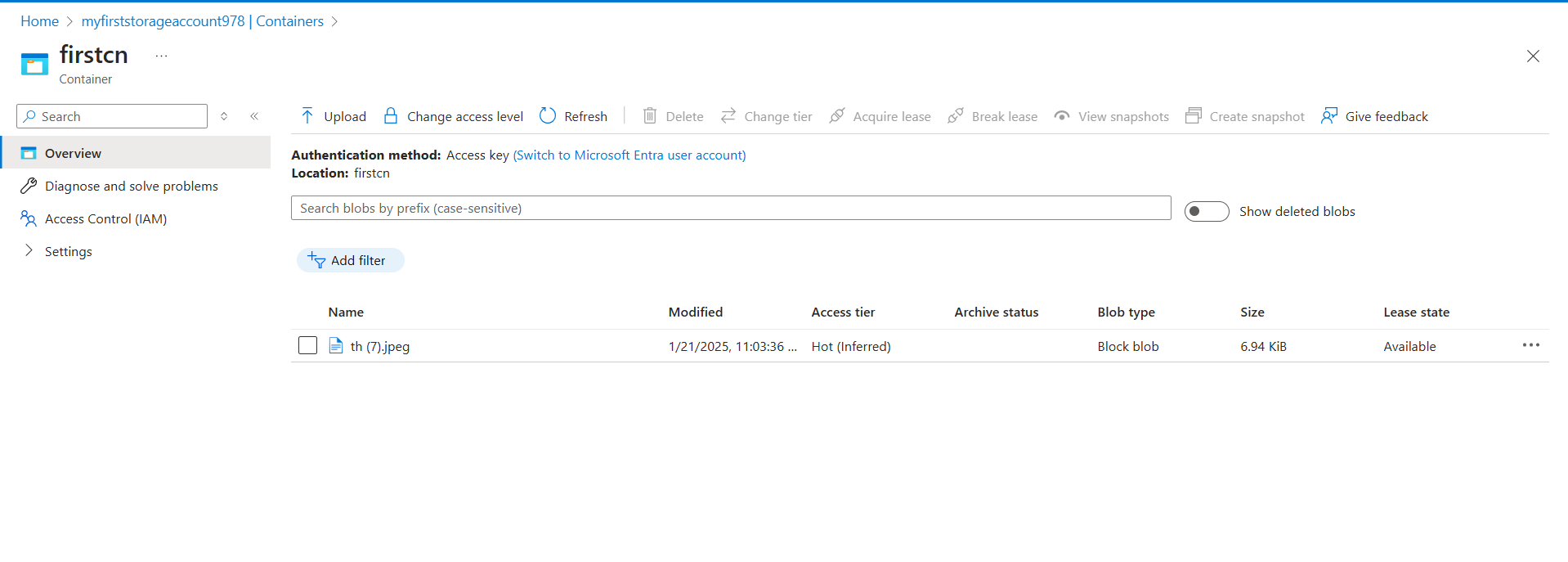
**Fig:** service endpoint working process.

**Let’s work with the service endpoint:**

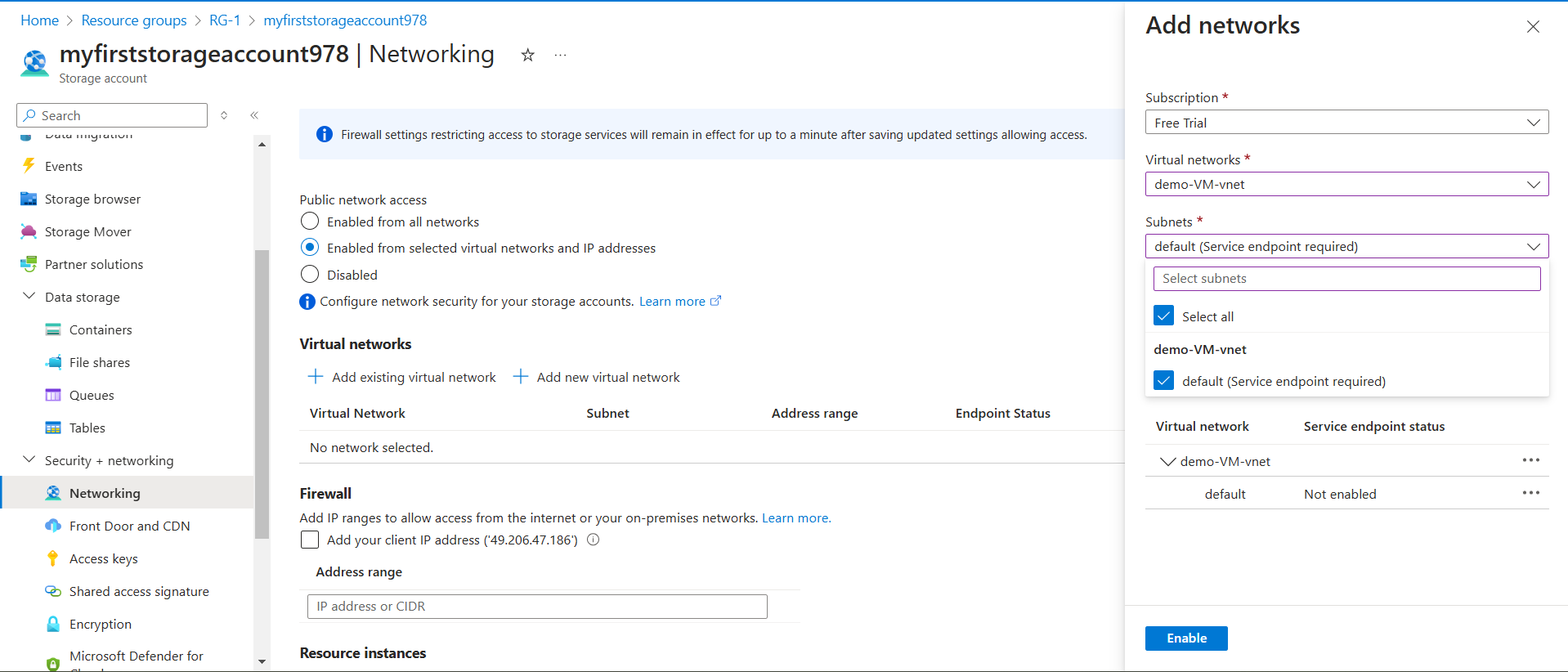
**Step1**: create the windows virtual machine (demo-VM).



**Step2**: create the storage account, within storage account create a container and upload any file in it.



**Step3:** Enable the Service endpoint for the storage account.

Go to 🡪storage-account🡪security + networking🡪networking🡪Enabled from selected virtual networks and IP addresses🡪Add existing virtual network🡪enable service endpoint🡪add & sacv.

**Fig:** Enabling of service end point.

**Step4**: Now brows the image or file with URL from local machine and windows VM (demo-VM) which is uploaded in container.

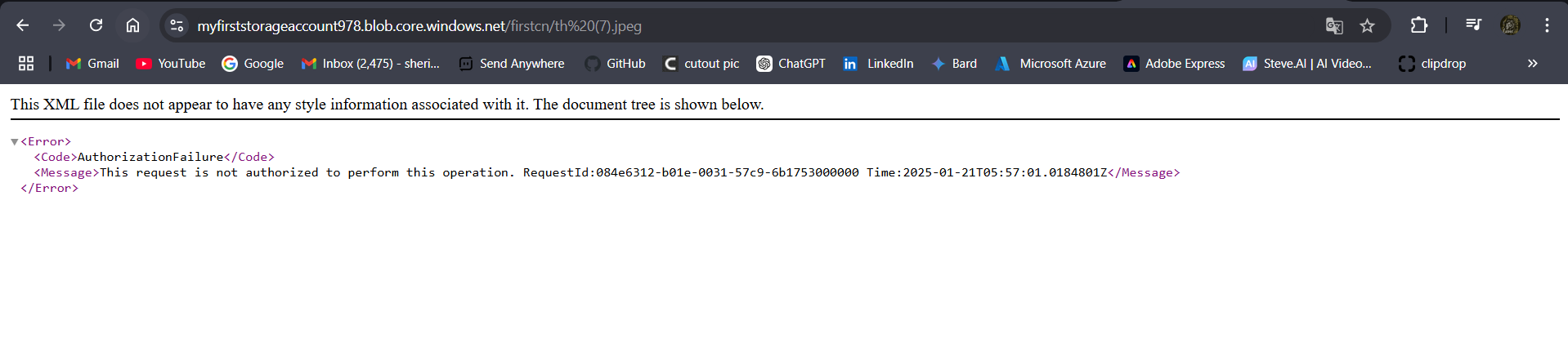
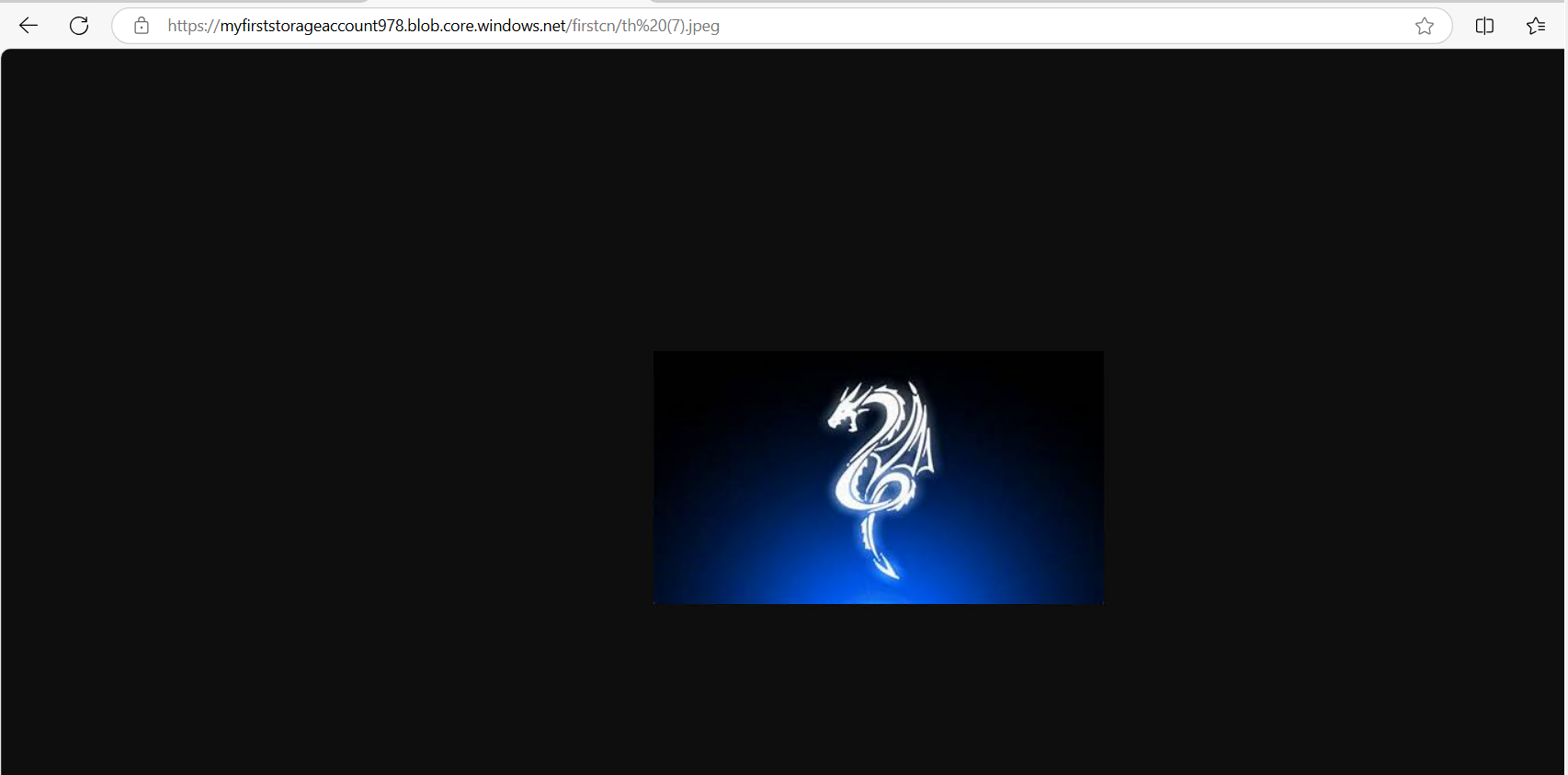


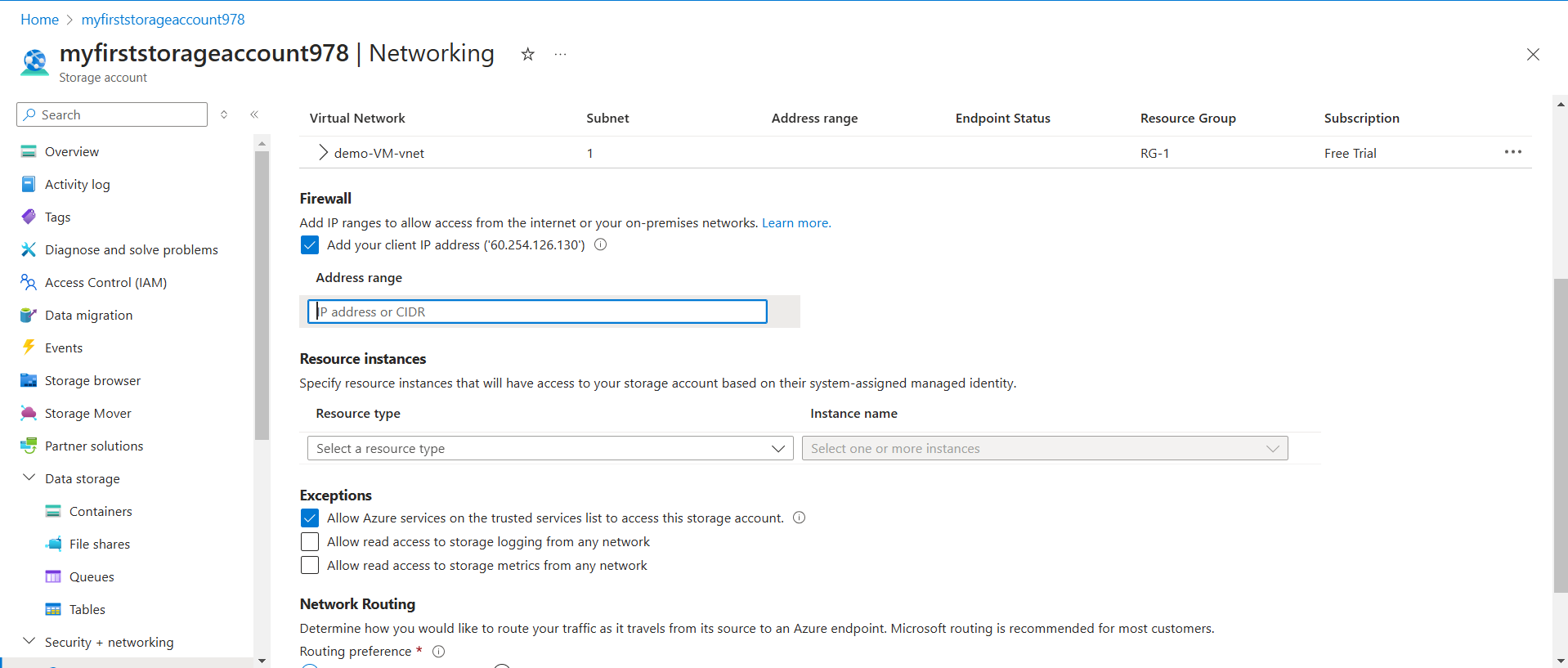
Fig: browsing of image URL from local Machin.



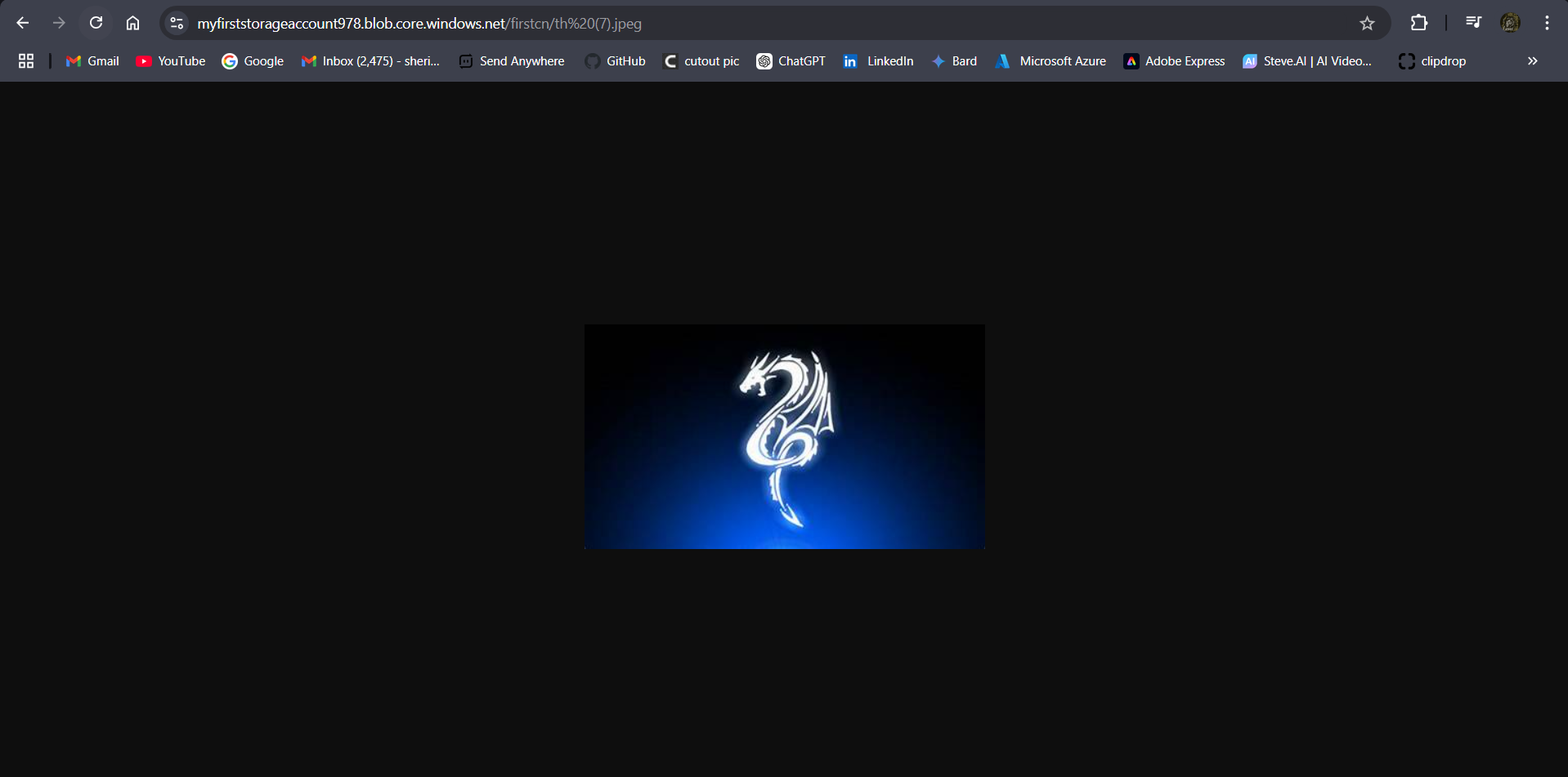
**Fig:** Browsing of image URL from windows VM (demo-VM).

**Note:** Here we only given access to the Vnet (demo-VM-vnet) [in which windows VM (demo-VM) is created] but not to the local Machin public IP. So we can only access the image from demo-VM which is created in demo-VM-vnet.

Now let’s give the access to the public IP of our local VM.



**Fig:** Adding our client public IP address (local Machin).

****

**Fig:** Browsing of image from client machine (local Machin).

Now we can get the image while browsing from both local Machin and from demo-VM which is created in demo-VM-vnet.

**Private Endpoints:** (one-to-one internal communication)

* **Concept:** Private Endpoints create a private connection between your VNet and a supported Azure service.(PAAS services)
* **How it works:** A private endpoint is assigned a private IP address from your VNet's address space. This effectively brings the Azure service into your “private network”.
* **Security:** Provides the highest level of security as traffic never leaves your private network.
* **Flexibility:** Can be used with a wider range of Azure services and even some third-party services.
* **Complexity:** More complex to set up due to the need for private IP addresses and potential DNS configuration changes.
* It is enables one**-**to-one internal communication between the PAAS services through Private Network.
* **Fig:** Private Endpoint is created
* While creating the private endpoint, Private DNS is created as shown in below figure.

Not accessed using internet



Azure Environment

Vnet

Storage Account

Subnet

NIC

It assigns the private IP to the storage account.

**Fig:** Private endpoint working process.

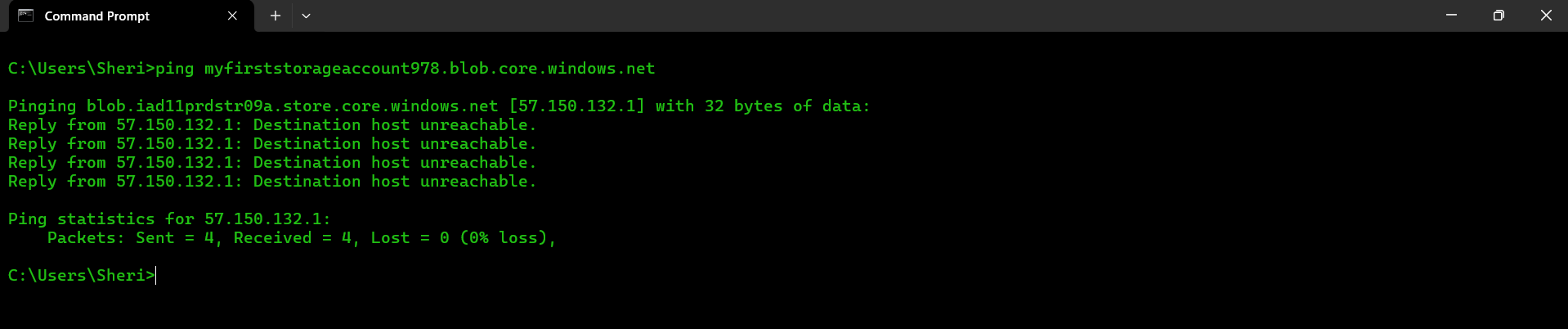
While creating or enabling private endpoint it will create NIC card with private IP which is taken from the Vnet IP address space and it is assigned to the PAAS service (blob storage) by deleting the public IP of PAAS service (blob storage). As shown in above figure.

**Now let’s work with the Private Endpoint:**

Step1: check the Public IP of blob storage.

Ping the public endpoint of blob (URL of image) in cmd to check the Public IP of blob.

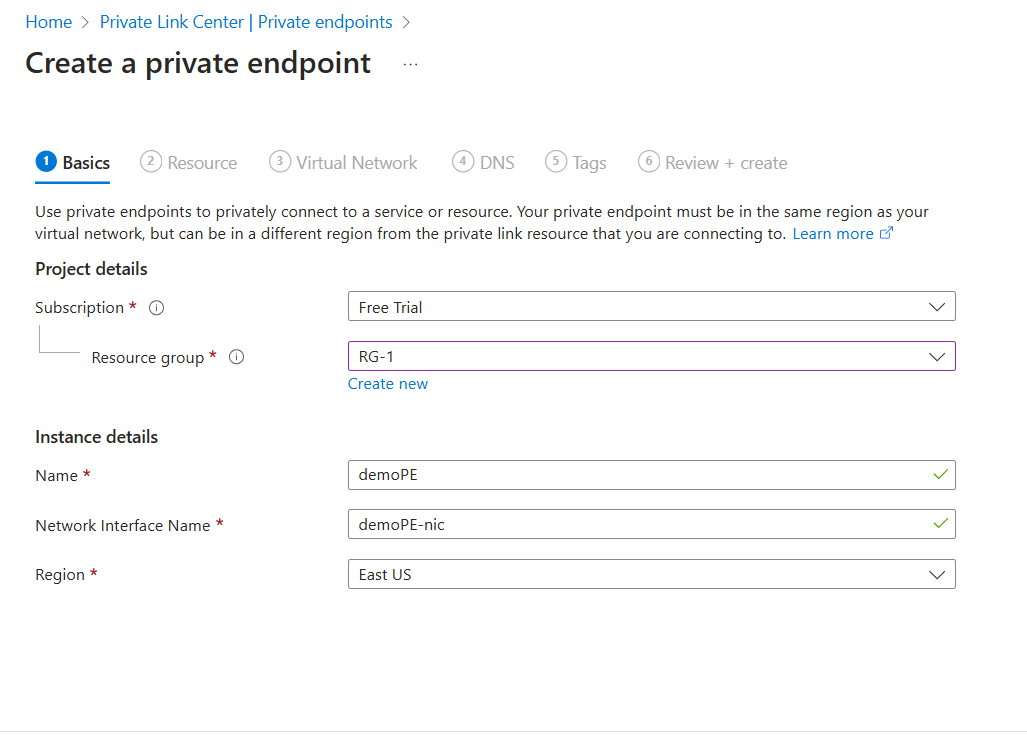
Public endpoint: myfirststorageaccount978.blob.core.windows.net.



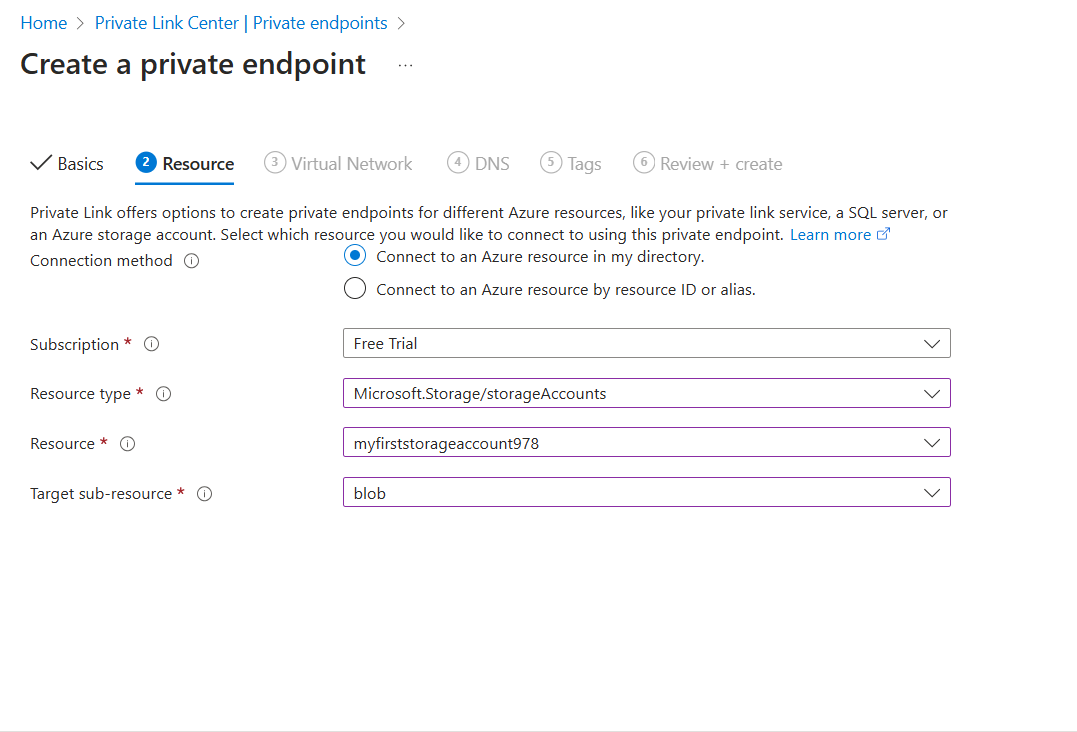
**Fig:** ping of public end point of blob

In above figure [57.150.132.1] is the public IP of blob storage (PAAS service) in which image is uploaded.

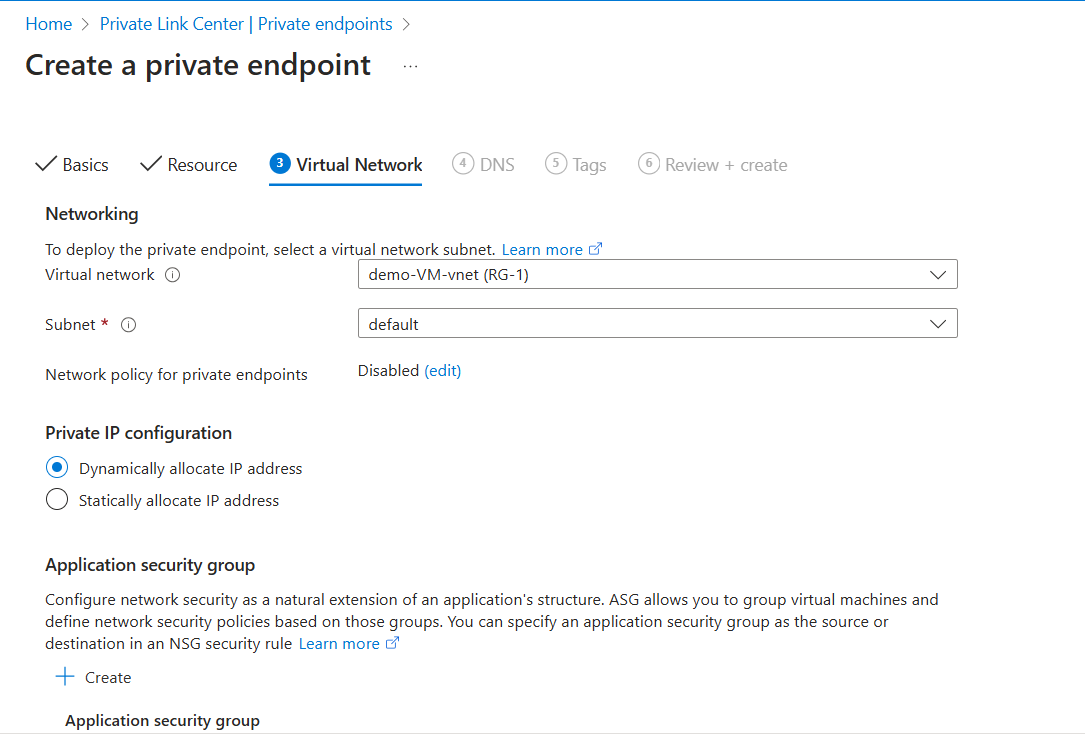
**Step2:** create the Private endpoint.



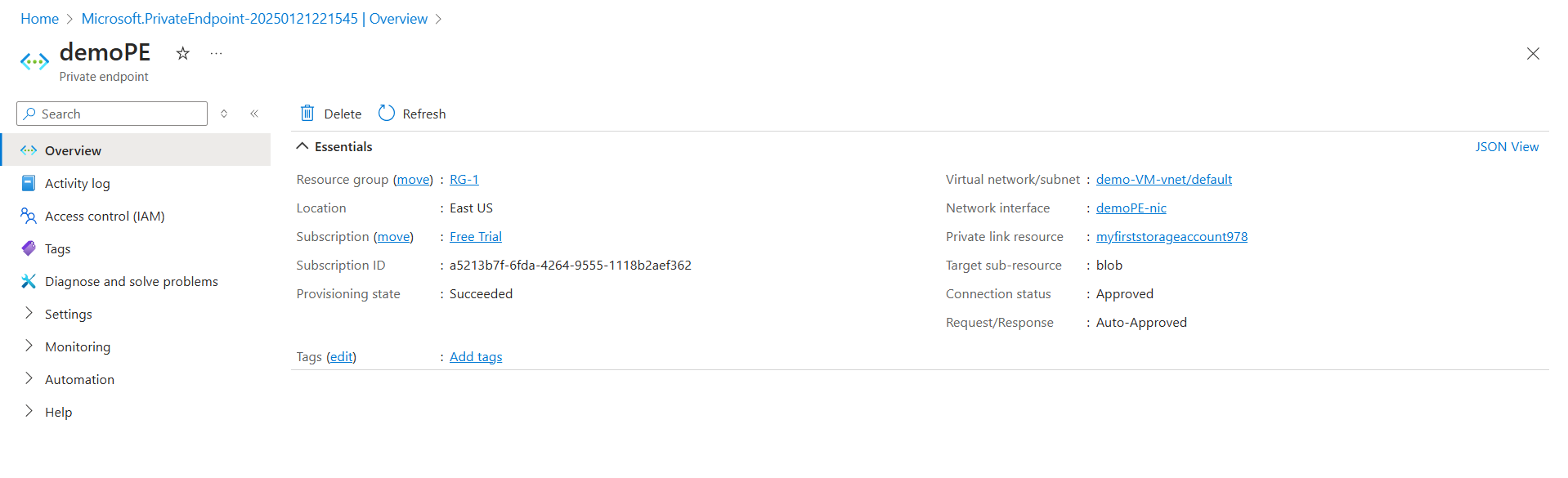
**Fig:** Adding of NIC card while creating private endpoint



**Fig:** adding of resource (PAAS services) while creating private endpoint

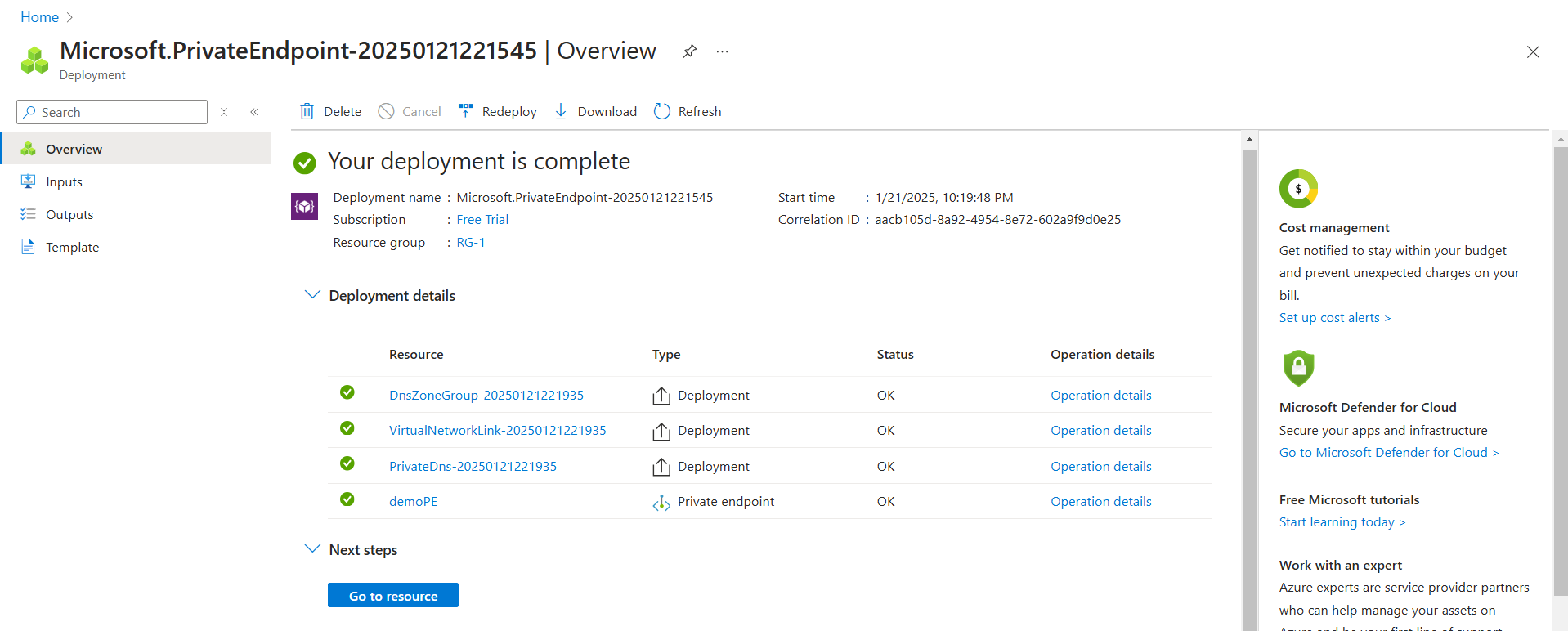
****

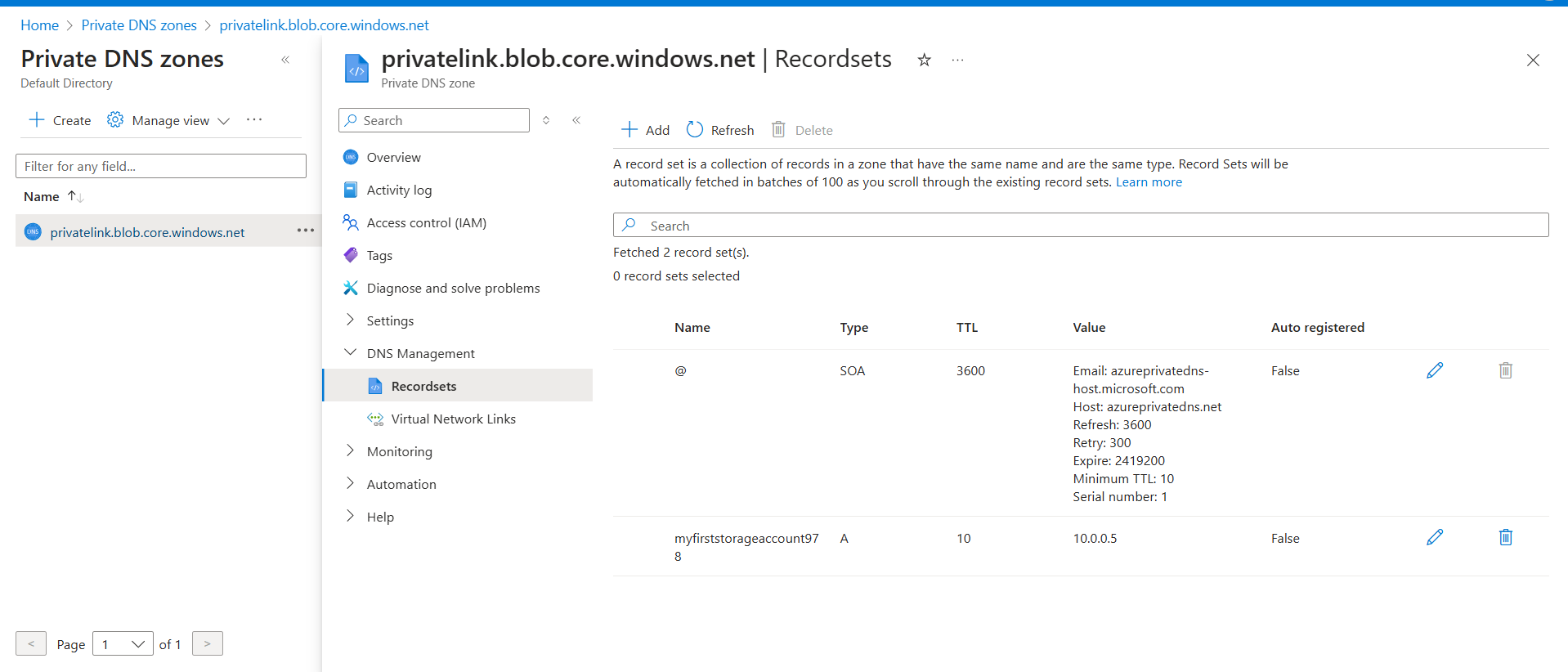
**Fig:** Adding of Vnet and Subnet in which our VM is created while creating private end point.

****

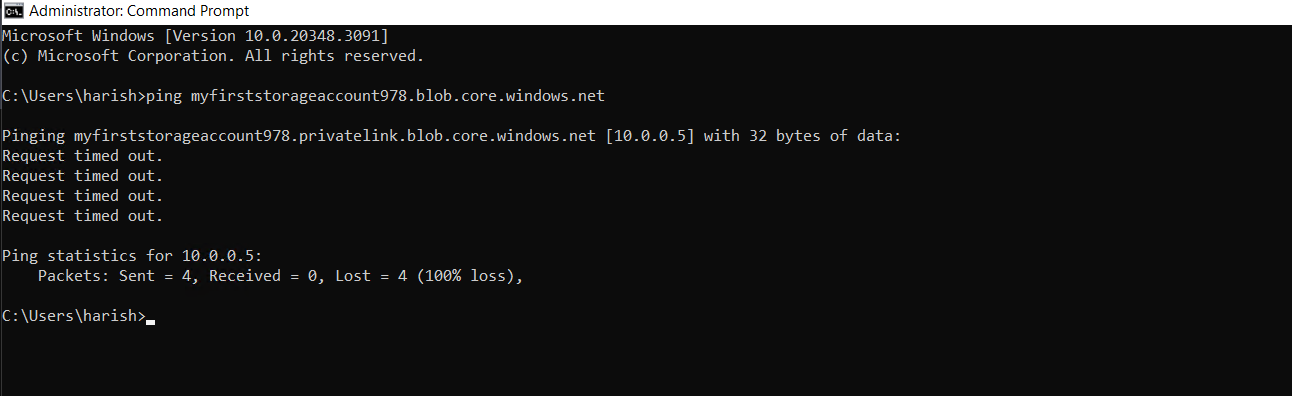
**Fig:** Private Endpoint is created

**Note:** while creating the private endpoint, Private DNS is created as shown in below figure.

****

****

**Step3:** Now once again check the IP of blob (PAAS service) whether it is private or public IP.

So that ping the image URL in cmd in order to check IP whether it is private or public.

From above figure the IP is changed from Public to Private IP by asigning NIC to the PAAS services. There for creating private endpoint will delete the Public IP of any PAAS services

**In simple terms:**

* **Service Endpoint:** Like a guest list for a party, allowing access to the party (Azure service) but still within the party's public area.
* **Private Endpoint:** Like a private room within the party venue, providing exclusive and secure access.

**Here's a table summarizing the key differences:**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Service Endpoint** | **Private Endpoint** |
| **Connectivity** | Direct to Azure service's public endpoint | Private connection within your VNet |
| **Security** | Traffic stays within Azure | Traffic remains entirely within your private network |
| **Ease of use** | Easier to configure | More complex to set up |
| **Supported services** | Limited to specific Azure services | Wider range of Azure and third-party services |

**Note:** Both Service Endpoints and Private Endpoints primarily focus on secure communication within a single virtual network (VNet) in Azure.