***Service Endpoint:-***

In Azure, a **Service Endpoint** provides secure, direct connectivity between Azure virtual networks and Azure services over the Azure backbone network, bypassing the internet. By enabling service endpoints, you can improve security by restricting access to Azure services to specific virtual networks, reducing potential exposure to external threats.

**Key Benefits of Service Endpoints**

* **Enhanced Security:** Service endpoints allow traffic to Azure services like Azure Storage, SQL Database, and Cosmos DB to stay within the Azure network, minimizing internet exposure.
* **Improved Performance:** Traffic is routed over the Azure backbone, which is optimized for lower latency and higher reliability.
* **Simplified Network Configuration:** Service endpoints make it easier to control access policies by allowing specific virtual networks to access Azure services directly.

**How Service Endpoints Work**

When you enable a service endpoint, the virtual network (VNet) associated with it can communicate with the Azure service in the same region or across regions. Once configured, you can use network security rules to restrict access to only traffic coming from the VNet through the endpoint.

**Example of Service Endpoint in Azure**

Let's say you have:

1. An Azure **Virtual Network (VNet)** hosting a virtual machine (VM) that needs to connect securely to an **Azure Storage Account**.
2. A **storage** that should be accessible only to resources within the VNet and not over the public internet.

***Steps to Deploy a Service Endpoint for Azure Storage***

**1. Create a Resource Group**

1. In the Azure Portal, search for **Resource groups** in the search bar.
2. Click **Create**.
3. Enter the following details:
   * **Subscription**: Select your subscription.
   * **Resource group name**: Provide a name for the resource group (e.g., MyStorageRG).
   * **Region**: Choose a region close to you (e.g., East US).
4. Click **Review + create** and then **Create**.

**2. Create a Virtual Network and Subnet**

1. In the Azure Portal, search for **Virtual networks** and click **Create**.
2. Select the resource group you just created (MyStorageRG).
3. Enter a **Name** for the virtual network (e.g., MyVNet).
4. Choose the same **Region** as the resource group.
5. In the **IP Addresses** section, specify the IP range for the virtual network (e.g., 1.1.0.0/16).
6. In the **Subnet** section:
   * **Name**: Provide a name for the subnet (e.g., MySubnet).
   * **Subnet address range**: Specify a range within the VNet (e.g., 11.0.0.0/24)
7. Click **Review + create** and then **Create**.

**3. Create a Storage Account**

1. In the Azure Portal, search for **Storage accounts** and click **Create**.
2. Select the resource group MyStorageRG.
3. Enter a **Storage account name** (e.g., mystorageacct123).
4. Set the **Region** to match the region of your VNet (e.g., East US).
5. Select the **Performance** and **Redundancy** options according to your needs.
6. Click **Review + create** and then **Create**.

**4. Configure the Service Endpoint for Storage**

1. After the storage account is created, go back to the **Virtual networks** resource.
2. Select the virtual network you created (MyVNet), then go to **Subnets** in the left-hand menu.
3. Click on the **MySubnet** subnet.
4. In the **Service endpoints** section, select **+ Add service endpoint**.
5. From the **Service** dropdown, choose **Microsoft.Storage**.
6. Ensure the **Regions** dropdown includes the region of your storage account (e.g., East US).
7. Click **Add**.

**5. Secure Access to the Storage Account Using the Service Endpoint**

1. Navigate to your **Storage account** (mystorageacct123) in the Azure portal.
2. In the left menu, select **Networking**.
3. Under **Firewalls and virtual networks**, choose **Selected networks** to restrict access to the virtual network.
4. Click **+ Add existing virtual network**.
   * Choose the **Virtual network** (MyVNet) and the **Subnet** (MySubnet) where you enabled the service endpoint.
5. Click **Save** to apply the settings.

**Summary of What You’ve Set Up:**

* A **service endpoint** for Microsoft.Storage on the subnet, allowing secure, private access to the storage account from within the VNet only.

***Verification of Service Endpoint Configuration for Azure Storage Access:***

After setting up the service endpoint to connect securely from a specific Virtual Network (VNet) to the Azure Storage account, you conducted a verification test to confirm that only allowed network resources could access the storage.

1. **Step 1: Attempting Access from the Allowed Virtual Network**  
   Using the command:

bash

az storage blob upload-batch --account-name mystorageacct112 --destination serviceendpoint1 --source .

you successfully uploaded files from the VM residing within the configured VNet to the designated storage container. This confirmed that resources within the permitted VNet could interact with the storage account as intended.

1. **Step 2: Testing Access from an External Virtual Network**  
   You then attempted the same file upload operation from a VM located in a different, unapproved VNet. This attempt was blocked with a message indicating that access was denied due to the storage account’s network rules. The error confirmed that the network restrictions configured in the storage account firewall were correctly blocking access from networks outside the approved VNet.

This two-part verification validates that:

* The service endpoint is functioning as expected, allowing only approved network resources access to the storage account.
* The storage account’s firewall and network settings are correctly configured to enforce access restrictions based on the specified VNet.

This process demonstrates a secure implementation, ensuring that only resources within the authorized VNet can access the Azure Storage account while blocking all other network traffic.





