**Lab 18: Azure ML Workspace Security – Associated Resources**

**Introduction:**

Azure Machine Learning workspaces work closely with other resources, such as storage accounts and key vaults, which also need to be secured. Securing these associated resources involves disabling public access and integrating them with a Virtual Network (VNet) to ensure they connect properly and securely. In this lab, you will configure these security settings for the storage account and key vault.

**Objectives:**

* Disable public access for the associated storage account and key vault.
* Configure service endpoints for secure access.
* Set up private endpoints for the associated resources.

**Steps:**

**Part 1: Disabling Public Access**

**Step 1:** Disable Public Access for the Storage Account

* **Explanation**: Disabling public access prevents unauthorized traffic from accessing the storage account.
* **How to Do It**:
  + In the Azure portal, navigate to your storage account.
  + Go to the "Networking" section.
  + Under "Public network access," select "Enabled from selected virtual networks and IP addresses."
  + Click "Add existing virtual network."
  + Select the VNet and subnet you created previously.
  + Click "Save."

**Step 2:** Disable Public Access for the Key Vault

* **Explanation**: Preventing public access ensures that only approved networks can reach the key vault.
* **How to Do It**:
  + In the Azure portal, navigate to your key vault.
  + Go to the "Networking" section.
  + Under "Public network access," select "Enabled from selected virtual networks and IP addresses."
  + Click "Add existing virtual network."
  + Select the VNet and subnet you created previously.
  + Click "Save."

**Part 2: Configuring Service Endpoints**

**Step 1:** Configure Service Endpoints in the Virtual Network

* **Explanation**: Service endpoints allow the VNet to securely access Azure services over a private address space.
* **How to Do It**:
  + In the Azure portal, navigate to the VNet you created previously.
  + Go to the "Subnets" section.
  + Click on the desired subnet to edit its settings.
  + Scroll down to the "Service endpoints" section.
  + Select the services you want to enable endpoints for (e.g., "Microsoft.Storage").
  + Click "Save."

**Part 3: Creating Private Endpoints**

**Step 1:** Create a Private Endpoint for the Storage Account

* **Explanation**: A private endpoint secures the connection between the storage account and the VNet.
* **How to Do It**:
  + In the "Networking" section of the storage account, go to the "Private endpoint connections" tab.
  + Click "+ Private endpoint."
  + Fill in the Subscription, Resource group, Network interface name, and Region, then click "Next."
  + In the "Resource" tab, choose "blob" for the Target sub-resource.
  + Click "Next."
  + Configure the VNet and DNS settings, then click "Review + create."
  + Once created, repeat the process for the "file" sub-resource.

**Step 2:** Create a Private Endpoint for the Key Vault

* **Explanation**: This ensures the key vault is securely accessed via a private IP address in the VNet.
* **How to Do It**:
  + In the "Networking" section of the key vault, go to the "Private endpoint connections" tab.
  + Click "+ Private endpoint."
  + Fill in the Subscription, Resource group, Network interface name, and Region, then click "Next."
  + In the "Resource" tab, choose "vault" for the Target sub-resource.
  + Click "Next."
  + Configure the VNet and DNS settings, then click "Review + create."

**Summary:**

In this lab, you secured associated resources of the Azure Machine Learning workspace by disabling public access, configuring service endpoints, and creating private endpoints. These configurations ensure that your resources are protected from unauthorized access and only accessible via secure network paths.