**Core Services Sandbox**

Topics Covered

* Azure Resource Group management
* Virtual machine (VM) deployment (Linux, SSH access)
* Azure Storage (Blob storage with containers)
* Network Security Groups (NSGs) and inbound port rules
* SSH access and networking validation
* Resource cleanup

Summary

This project demonstrates how to provision and manage core Azure services using the Azure Portal. The tasks include creating a Linux virtual machine with SSH authentication, configuring blob storage and uploading a file, applying basic network security rules, and verifying connectivity through SSH and HTTP traffic testing. It provides hands-on experience with foundational Azure components ideal for beginners.

Scenario

You're tasked with setting up a basic sandbox environment in Microsoft Azure to simulate common cloud infrastructure components. This includes a secure Linux VM, a storage account with blob container access, and customized network security rules to restrict unwanted HTTP access while maintaining SSH accessibility. At the end, you'll clean up all resources to avoid ongoing costs.

1. Create Resource Group

* **Azure Portal** → **Resource groups**
* Click **+ Create**
* **Resource Group Name**: az900-project1-rg
* **Region**: East US
* Click **Review + create** → **Create**

**2. Deploy a Linux Virtual Machine (Free Tier)**

* Go to **Virtual Machines** → **+ Create** → **Azure virtual machine**

Basics Tab:

* **Subscription**: Choose your active subscription
* **Resource Group**: az900-project1-rg
* **Virtual Machine Name**: az900linuxvm
* **Region**: East US
* **Image**: Ubuntu Server 20.04 LTS – Gen2
* **Size**: Standard\_B1s (Free tier eligible)
* **Authentication type**: SSH public key
* Generate new key pair → Download the private key (private\_key.pem file)
* **Username**: azureuser (default or your choice)

Disks Tab:

* **OS Disk Type**: Standard SSD

Networking Tab:

* **Public Inbound Ports**: Allow selected ports → Select **SSH (22)**
* **Network Security Group**: Create new NSG
* Click **Review + create** → **Create**

**3. Create a Storage Account**

* Go to **Storage accounts** → **+ Create**

Basics Tab:

* **Resource Group**: az900-project1-rg
* **Storage account name**: az900project1sa *(must be globally unique)*
* **Region**: East US
* **Performance**: Standard
* **Redundancy**: Locally-redundant storage (LRS)
* Click **Review + create** → **Create**

**4. Upload File to Blob Storage**

* Open your storage account az900project1sa
* **Containers** → Click **+ Container**
  + **Name**: demo-container
  + **Public access level**: Private (no anonymous access)
* Click into the container → Click **Upload**
  + Select a small file (e.g., .txt) → Click **Upload**

**5. Configure Network Security Rule to Block HTTP**

* Go to **Virtual Machines** → Open az900linuxvm
* Navigate to **Networking** → **Inbound port rules**
* Click **+ Add inbound port rule**:  
  + **Source**: Any
  + **Protocol**: TCP
  + **Destination Port Ranges**: 80
  + **Action**: Deny
  + **Priority**: 1000
  + **Name**: Block-HTTP
* Click **Add**

**6. Verify Networking Behavior**

* Get the **Public IP Address** from your VM overview
* Open a browser → Try visiting http://<Public-IP>

Expected result: Page will **not load** due to HTTP block rule

**7. SSH into Your Linux VM**

Open terminal and run:

chmod 400 <path-to-private\_key.pem>

ssh -i <path-to-private-key.pem> azureuser@<VM-Public-IP>