### Web App For Startup Business

### Week 2: Deploy and Manage Azure Resources

**Students :**

1. **Ahmed Nasr Ahmed**
2. **Mohamed Mostafa**
3. **Abdulrahman Atef**
4. **Mahmoud Khaled**
5. **Ahmed Ali**
6. **Salah Ahmed**

### ****1. Network Configuration (VNets, Subnets)****

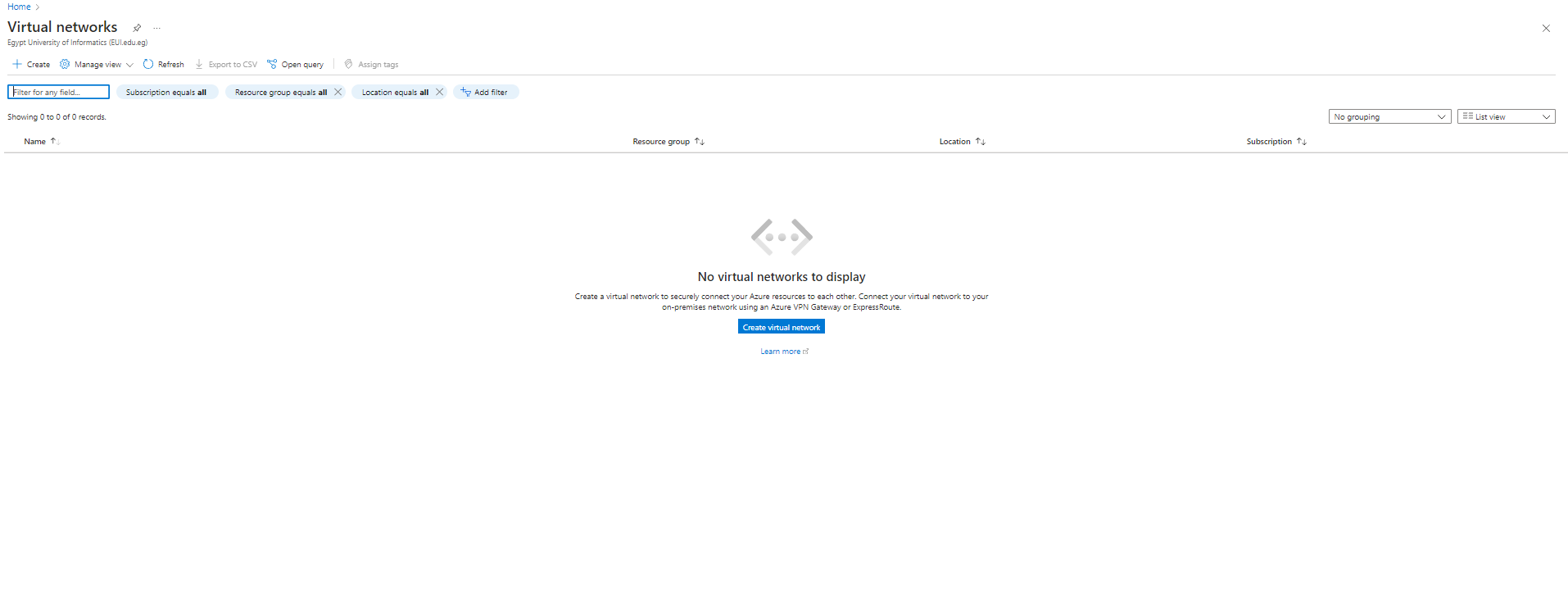
#### ****Overview:****

The network setup includes the creation of Virtual Networks (VNets), Subnets, and Network Security Groups (NSGs). These are critical components for enabling communication between resources while ensuring security through firewall rules.

#### ****Steps:****

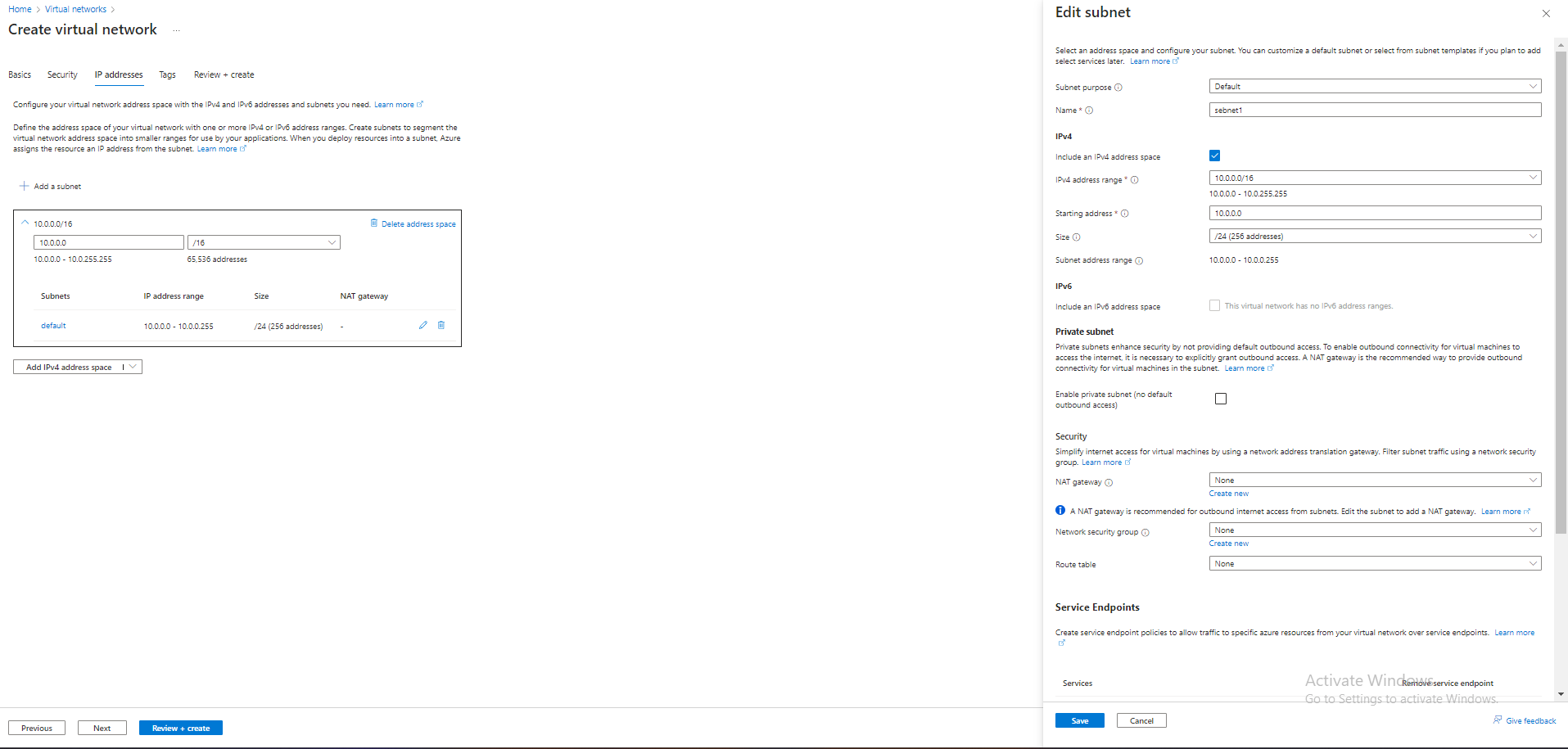
**1-Create a Virtual Network (VNet):**

-In the **Azure Portal**, navigate to **Create a Resource** and select **Virtual Network**.



-Define the VNet details:

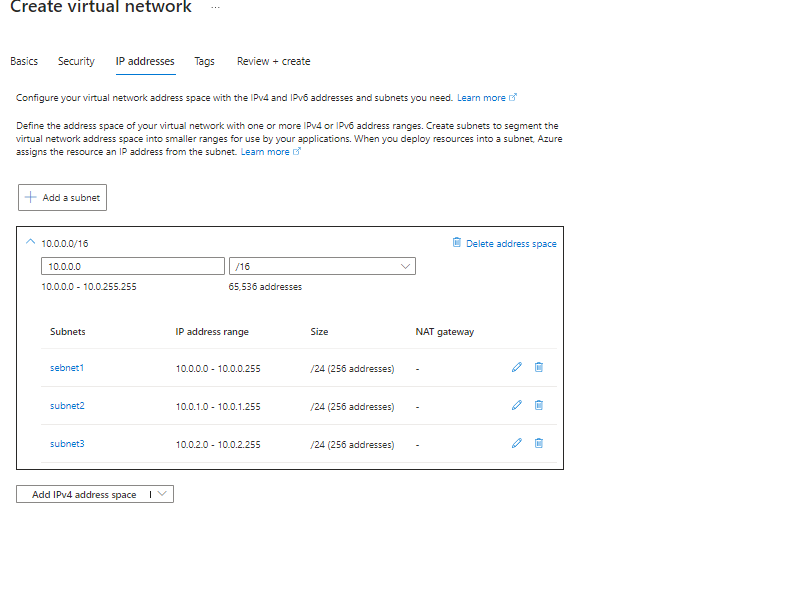
* + - **Name**: VM1-Fp-vnet
    - **Address Space**: 10.0.0.0/16



**2-Create a Subnet:**

-Within the VNet, create a subnet where your VM will reside:

* + - **Subnet Name**: VNet1
    - **Address Range**: 10.0.0.0/24



**3-Configure the Network Security Group (NSG):**

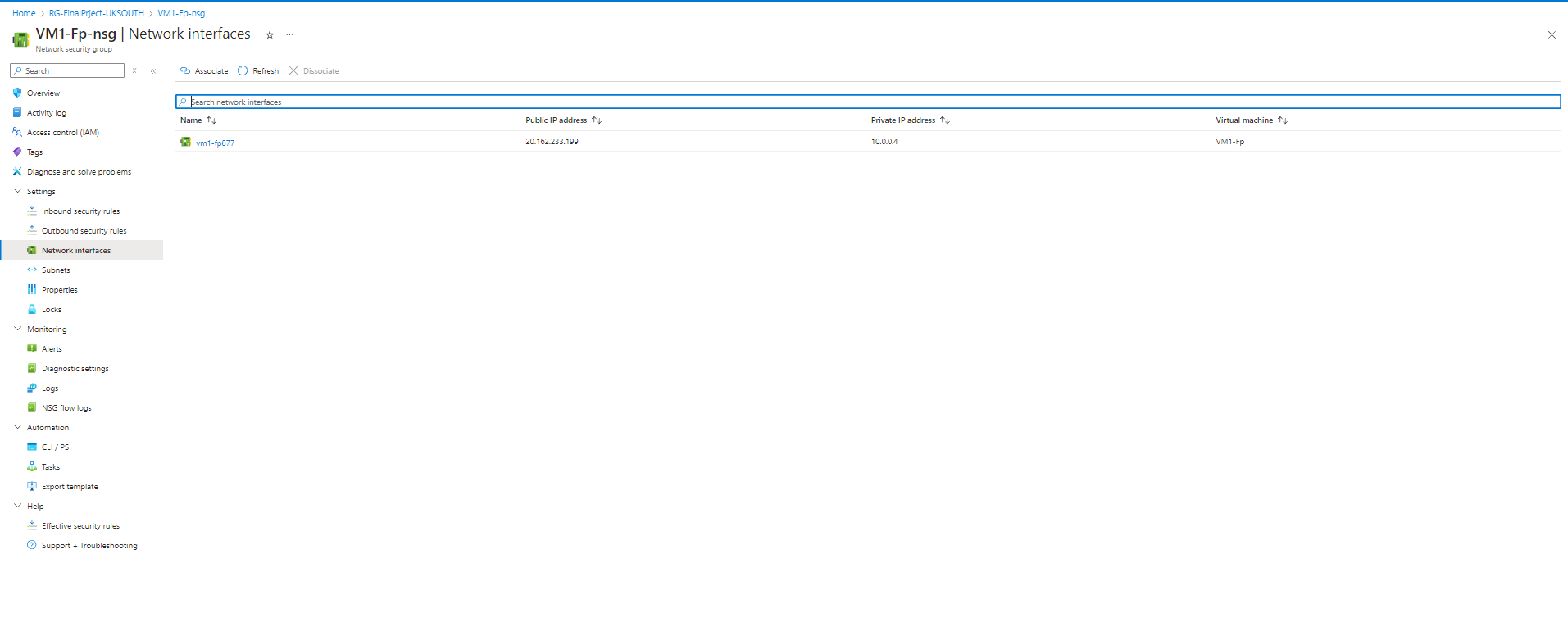
-NSGs control the traffic allowed to and from network interfaces.

-Create an NSG and set inbound and outbound rules:

* + - **Inbound Rule**: Allow RDP (TCP port 3389)
    - **Outbound Rule**: Allow all traffic to the internet.

**4-Assign NSG to the VM’s NIC:**

-Attach the created NSG to the VM’s **Network Interface** to ensure only permitted traffic can reach the VM.

****

### ****2. Virtual Machines (VMs) Deployment and Configuration****

#### ****Overview:****

You need to deploy and configure Virtual Machines (VMs) within Microsoft Azure. The deployment process includes choosing the appropriate VM sizes, selecting a region, configuring the operating system, and assigning networking settings (public and private IPs).

#### ****Steps:****

**1-Deploy the VM:**

-Navigate to the **Azure Portal** and select **Create a Resource**.

-Choose **Virtual Machine** from the resource list.

-Enter the necessary details for the VM such as:

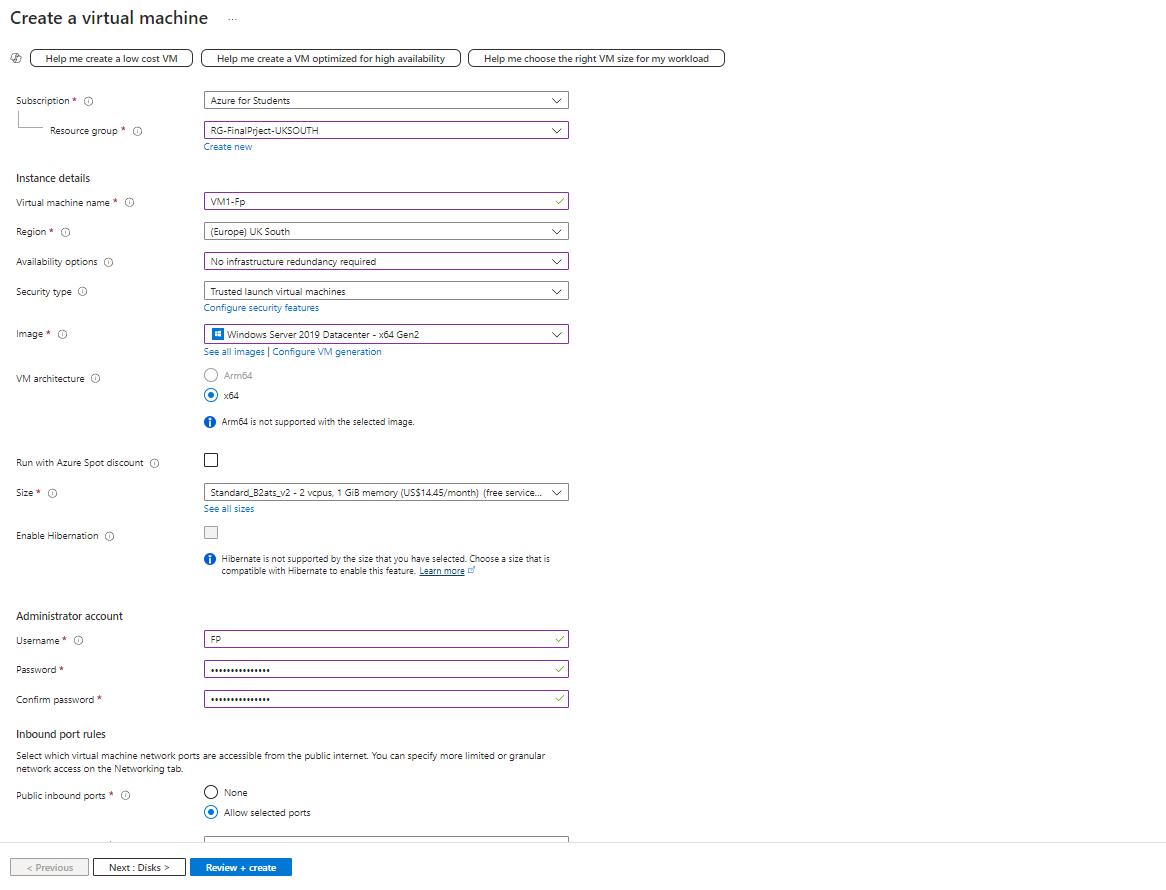
**-VM Name**: VM1-FP

**-Region**: UK South

**-Size**: Standard\_B2ats\_v2 ( 2 vcpus , 1Gib memory )

**-Operating System**: Windows Server 2019

-Configure **Administrator Account** by providing the username and password for accessing the VM.

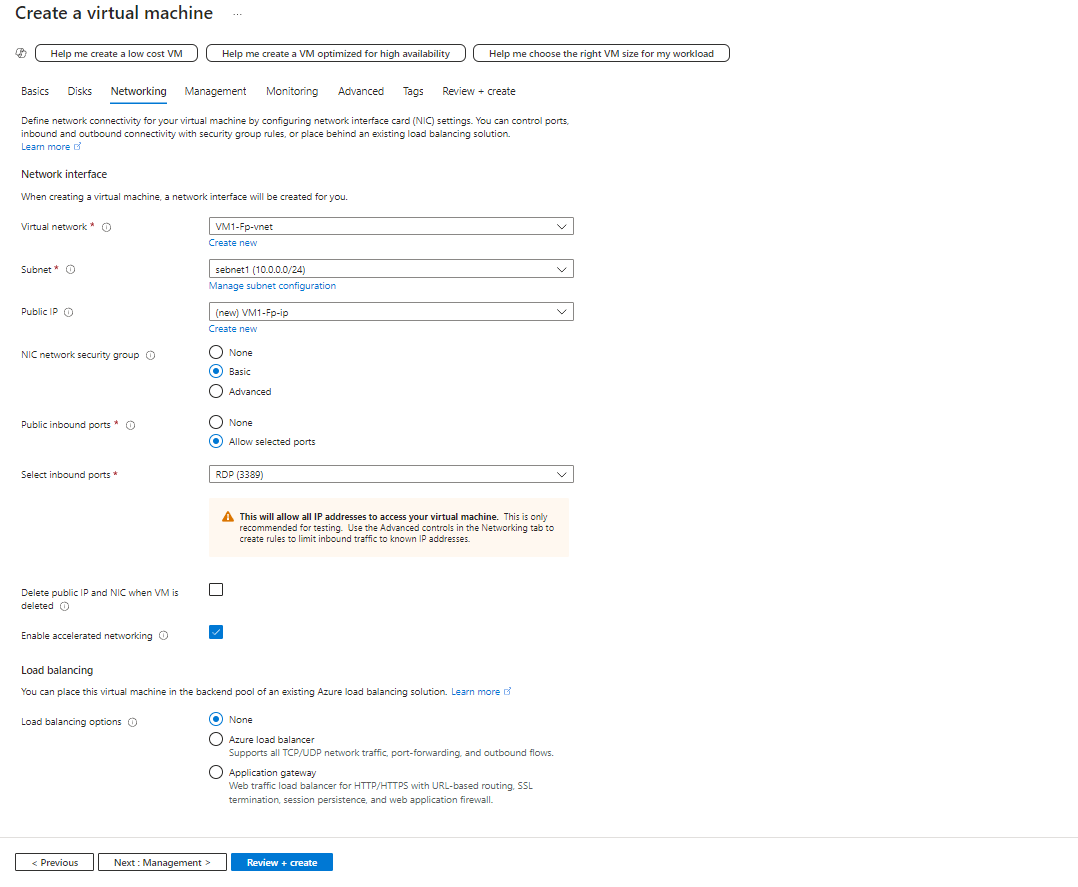


**2-Configure Networking:**

-Set up the virtual network (VNet) and subnet for the VM.

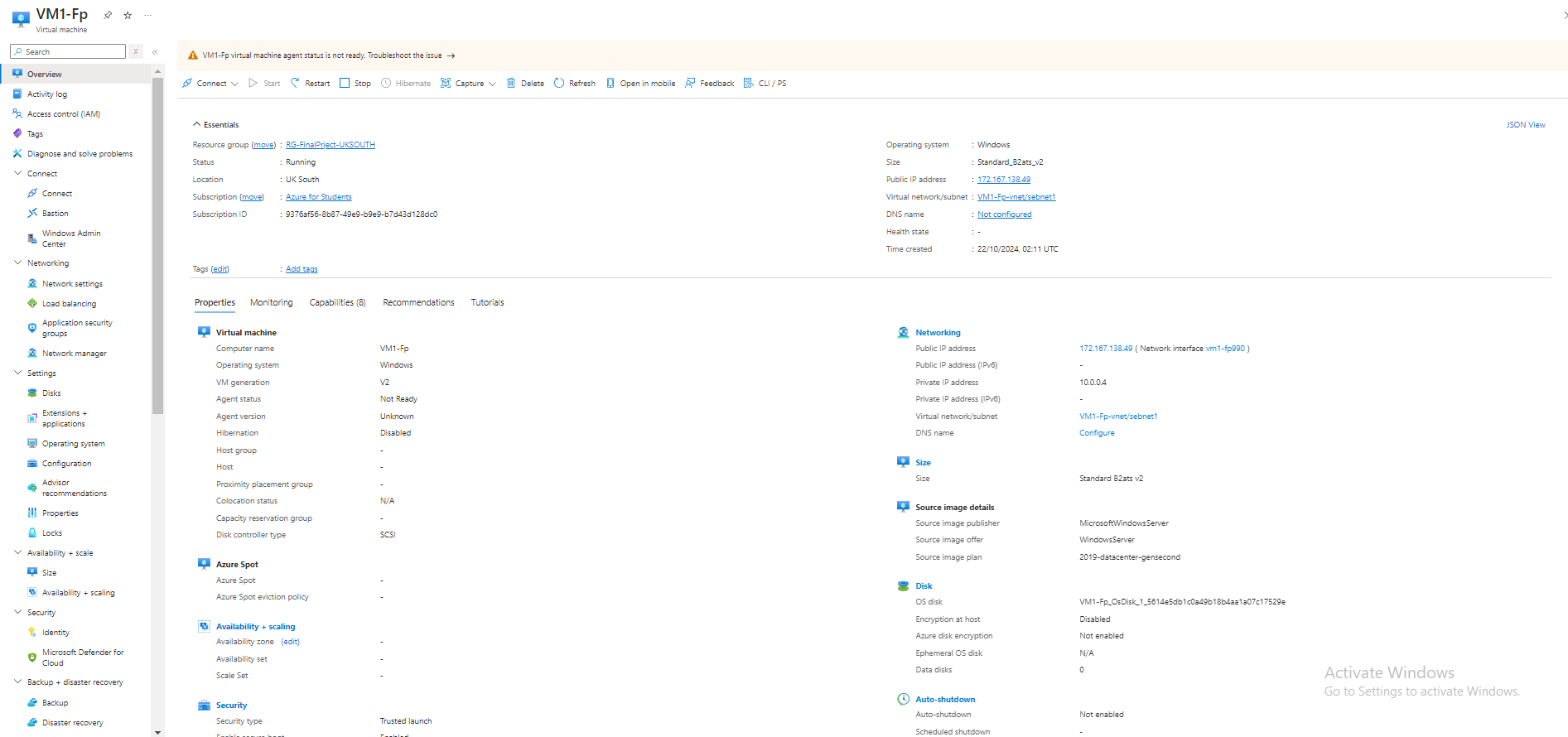
-Assign a **Public IP Address** to allow external access and a **Private IP** for internal network communication.

-Attach a **Network Security Group (NSG)** to secure the network interface by defining inbound/outbound rules (e.g., allowing RDP).



**3-Start the VM:**

-Once deployed, navigate to the VM’s page to verify that the VM status is “Running” and check the assigned IPs.



### ****3. Entra ID Directory Setup****

#### ****Overview:****

Entra ID is responsible for managing user identities and controlling access to resources within Azure. The goal is to create users, assign them to groups, and apply role-based access control (RBAC) to manage permissions.

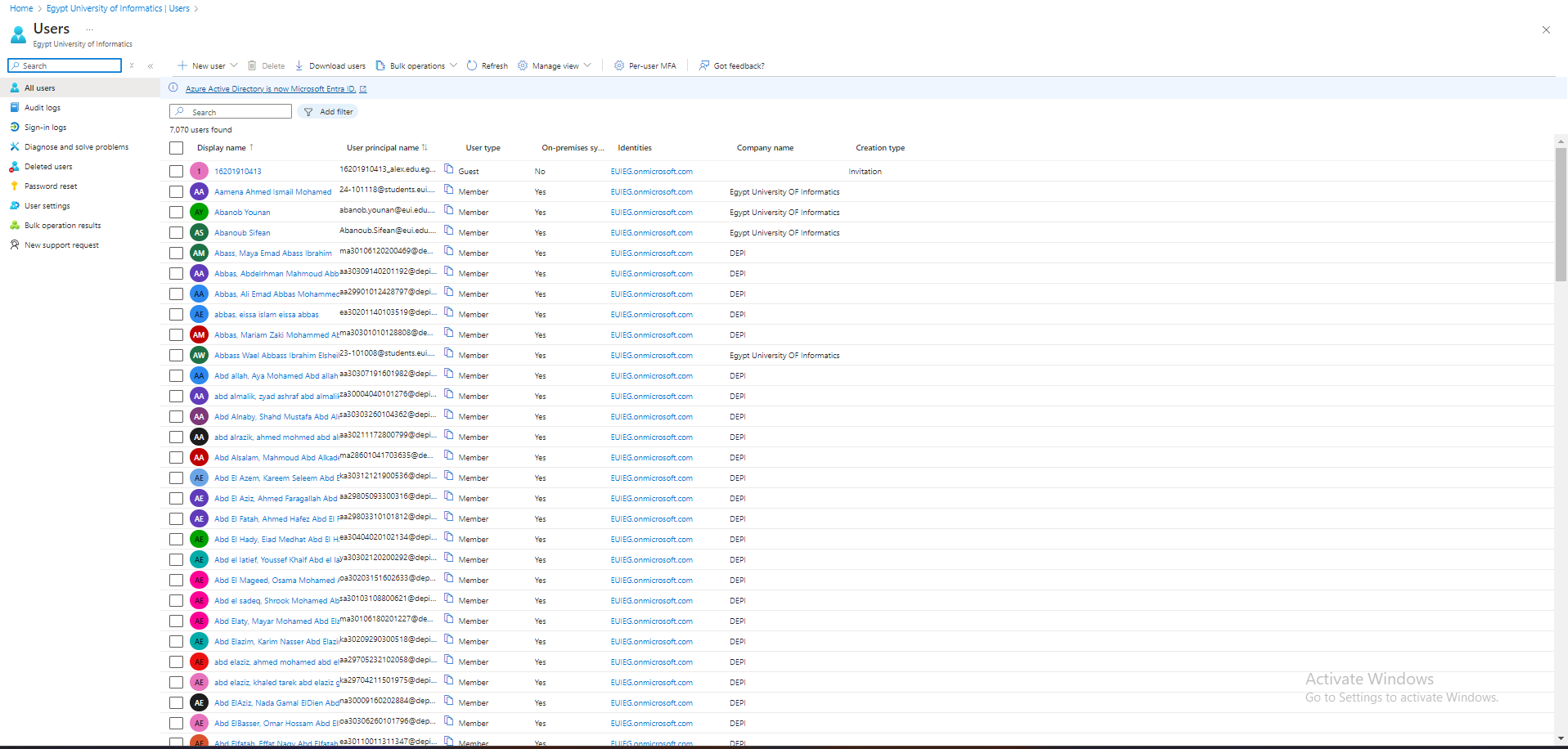
#### ****Steps:****

**1-Create Users in Entra ID:**

-In the **Azure Portal**, go to **Entra ID Directory** > **Users** > **New User**.

-Create users such as:

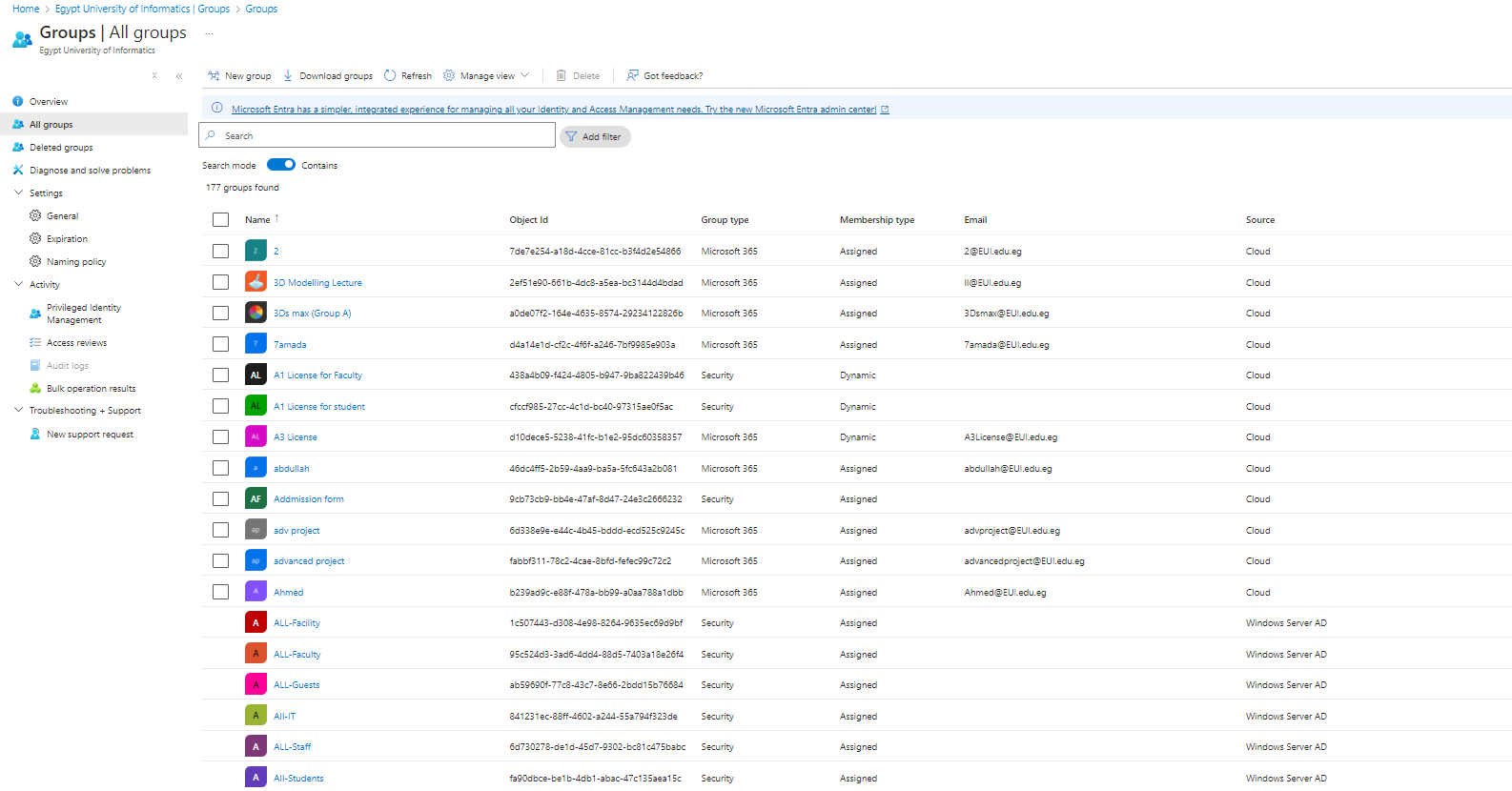
* + - **User 1**: Ali Saber
    - **User 2**: Mohamed Samy



**2-Create Groups in Entra ID:**

Under **Groups**, create groups for organizing users:

* + - **Group 1**: AdminGroup
    - **Group 2**: UsersGroup

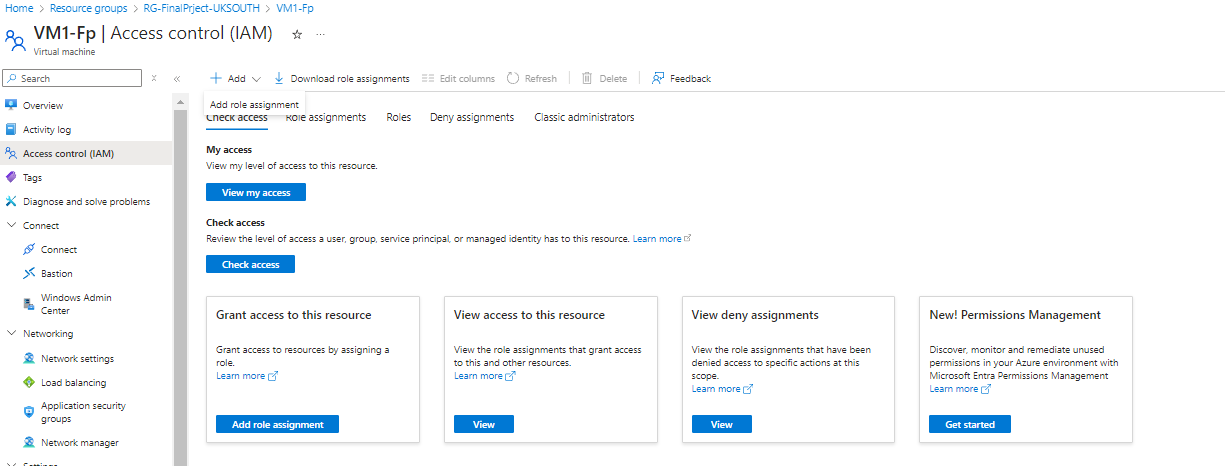


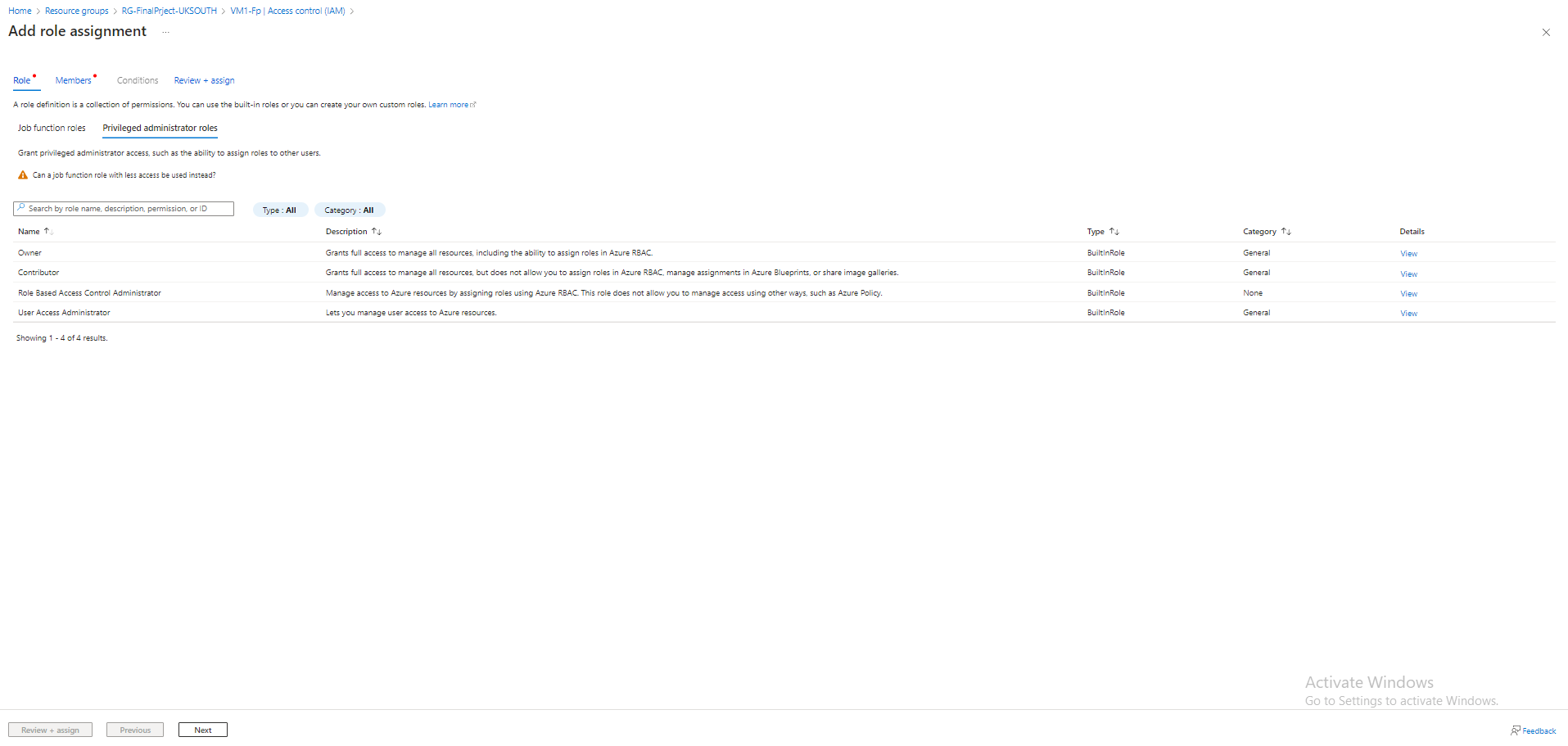
**3-Assign Role-Based Access Control (RBAC):**

-Navigate to **Access Control (IAM)** for the resource (e.g., VMs).

-Assign roles to users or groups:

* + - **AdminGroup**: Assigned **Owner** role (full access to resources).
    - **UsersGroup**: Assigned **Reader** role (read-only access).





**4-Verify Access:**

-Ensure the roles are correctly assigned by testing the access permissions of users.