### Web App For Startup Business

### Week 3: 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. Introduction

This report outlines the implementation of Azure storage solutions, including the setup of Azure storage accounts, Blob Storage configuration, and backup solutions for virtual machines (VMs) and files. The objective is to ensure efficient data storage and robust backup strategies that support business continuity.

### 2. Azure Storage Accounts Setup

#### **2.1 Creating a Storage Account**

**1-Login to Azure Portal**:

-Open your web browser and navigate to [portal.azure.com](https://portal.azure.com" \t "C:\\Users\\TOPSYS~1\\AppData\\Local\\Temp\\_new).

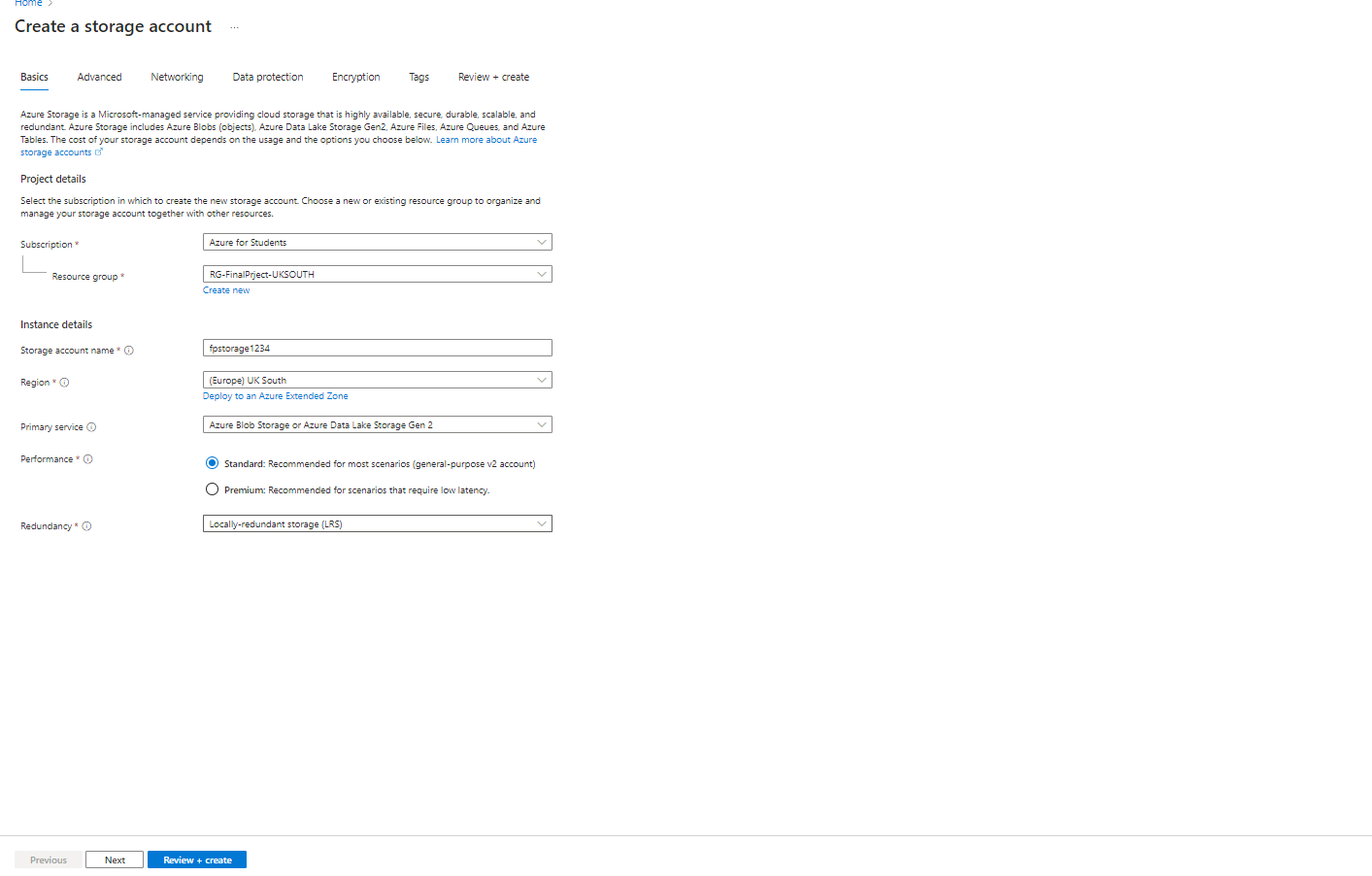
-Enter your credentials to log in.

**2-Select ‘Storage Accounts’**:

-In the left-hand navigation pane, click on “Storage accounts.”

**3-Create a new Storage Account**:

* 1. Click on the “+ Create” button.
  2. Choose the appropriate subscription.
  3. Select or create a Resource Group.
  4. Enter a unique name for the storage account.
  5. Select the region where the data will be stored.
  6. Choose performance (Standard or Premium) and replication options (e.g., LRS, GRS).

**4-Review and Create**:

-After filling in all required fields, click “Review + create,” and then click “Create” after validation.

#### {C4DE4064-6910-4693-B911-937D06DB778E}

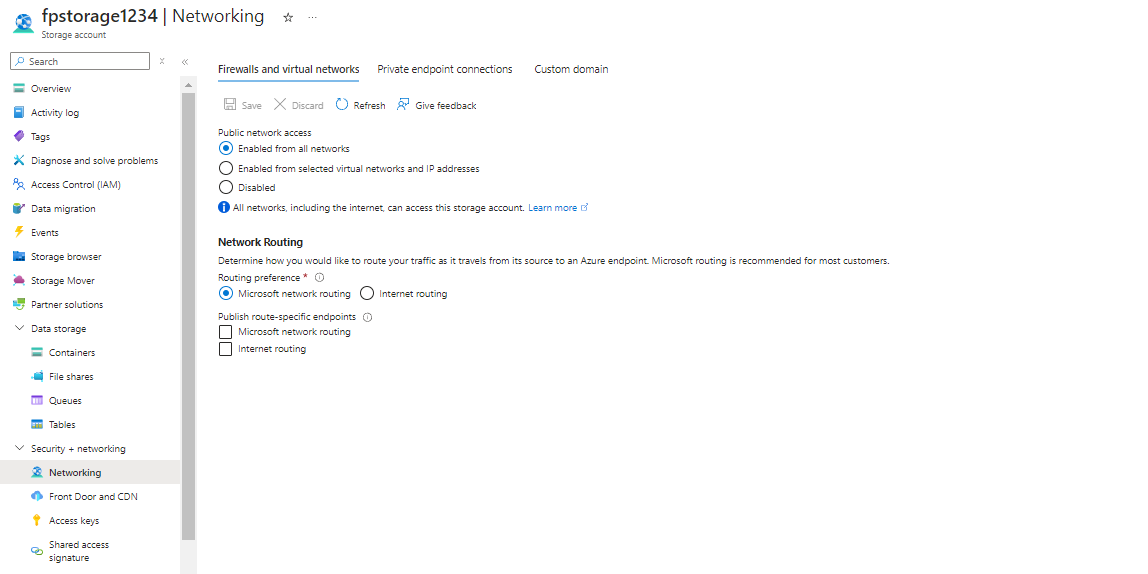
#### 2.2 Configuring Storage Account Settings

**1-Access Control (IAM)**:

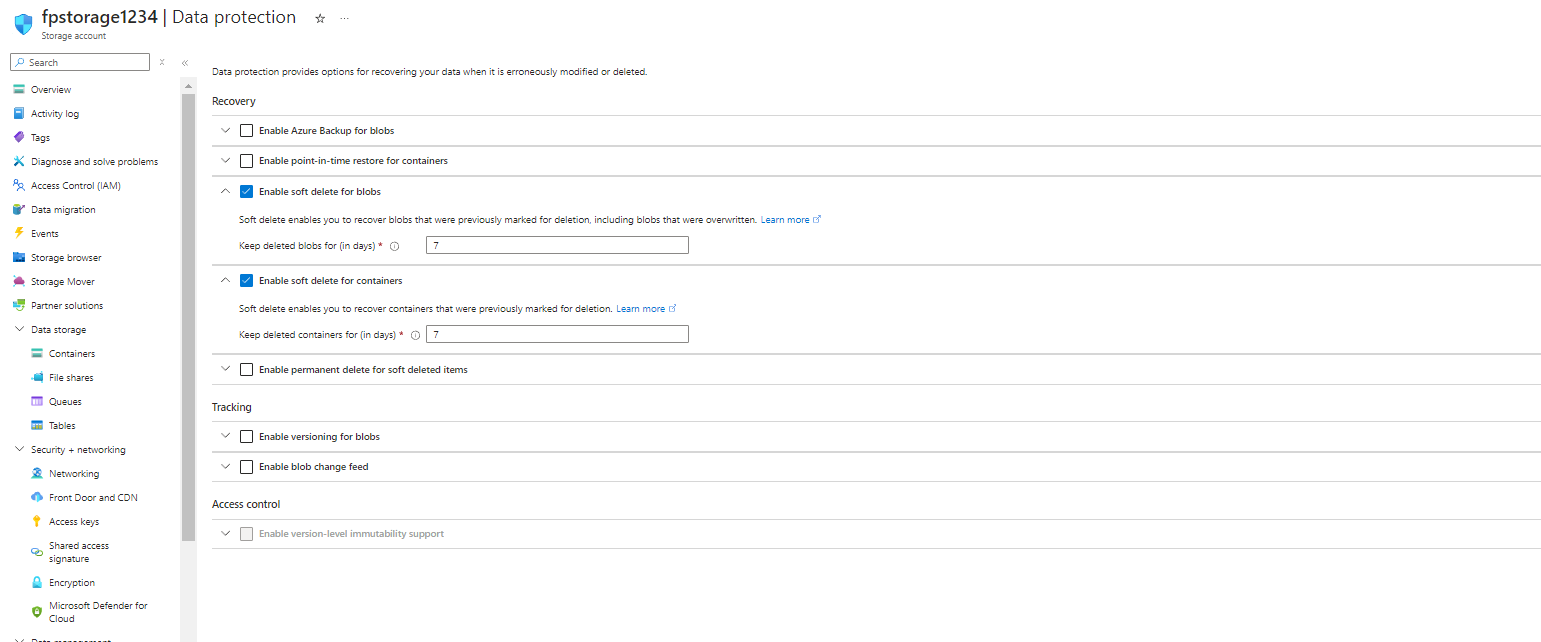
-Navigate to the “Access Control (IAM)” section to configure roles and permissions for users and applications.

**2-Networking**:

-Under “Networking,” set virtual network rules and configure public access settings as needed.

**3-Data Protection**:

-Enable soft delete and point-in-time restore features for added data protection.



### 3. Blob Storage Configuration

#### 3.1 Creating a Blob Container

**1-Navigate to the Storage Account**:

-In the Azure portal, select the storage account you just created.

**2-Select ‘Containers’**:

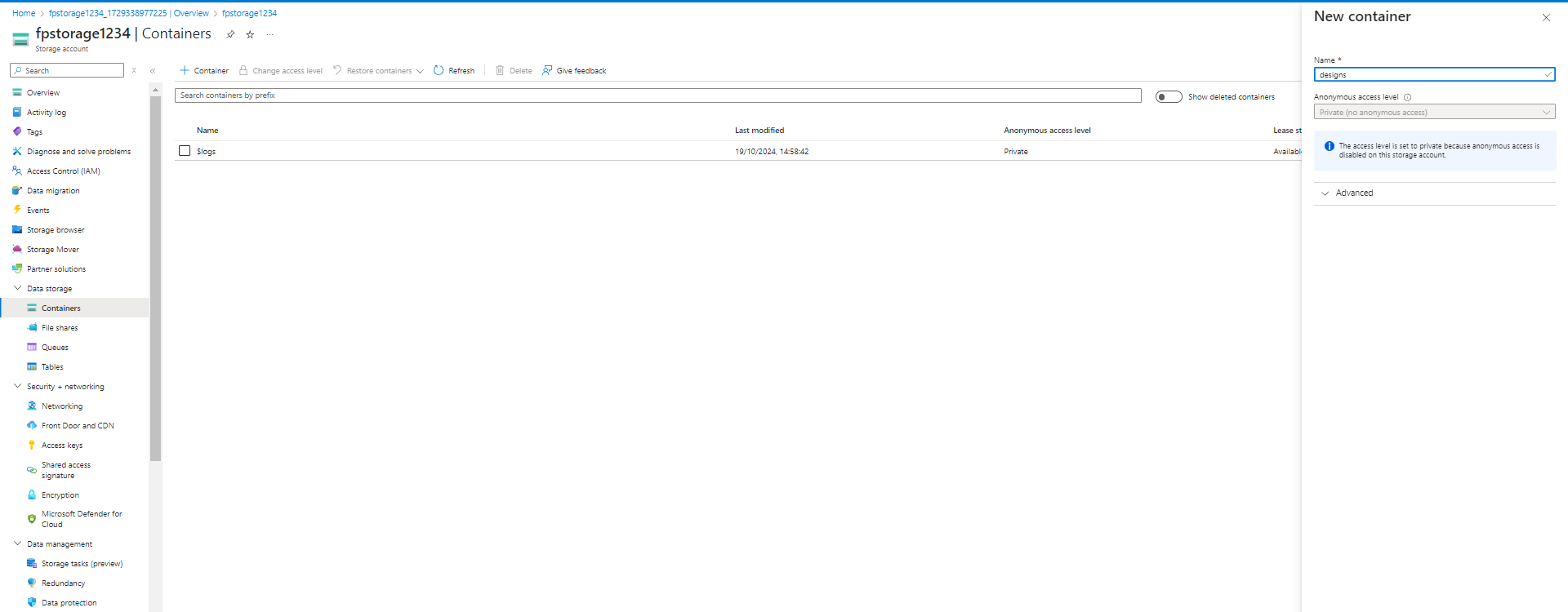
-In the left sidebar, click on “Containers” under the Data Storage section.

**3-Create a new Blob Container**:

-Click on the “+ Container” button.

-Provide a name for the container and set its access level (Private, Blob, or Container).

Click “Create.”



### 4 File Share Configuration

### 4.1 File Share Configuration

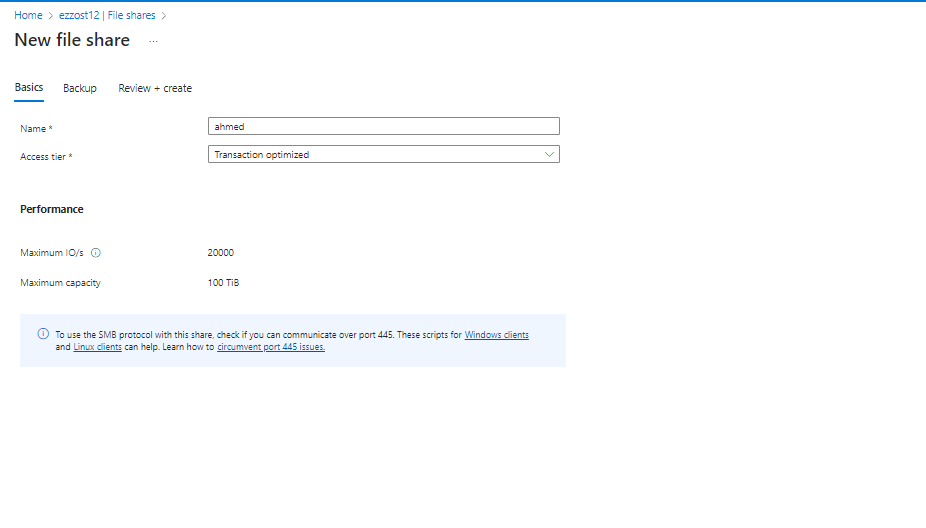
**1-Select ‘File Shares’**:

-In the left sidebar, click on “**File Shares**” under the Data Storage section.

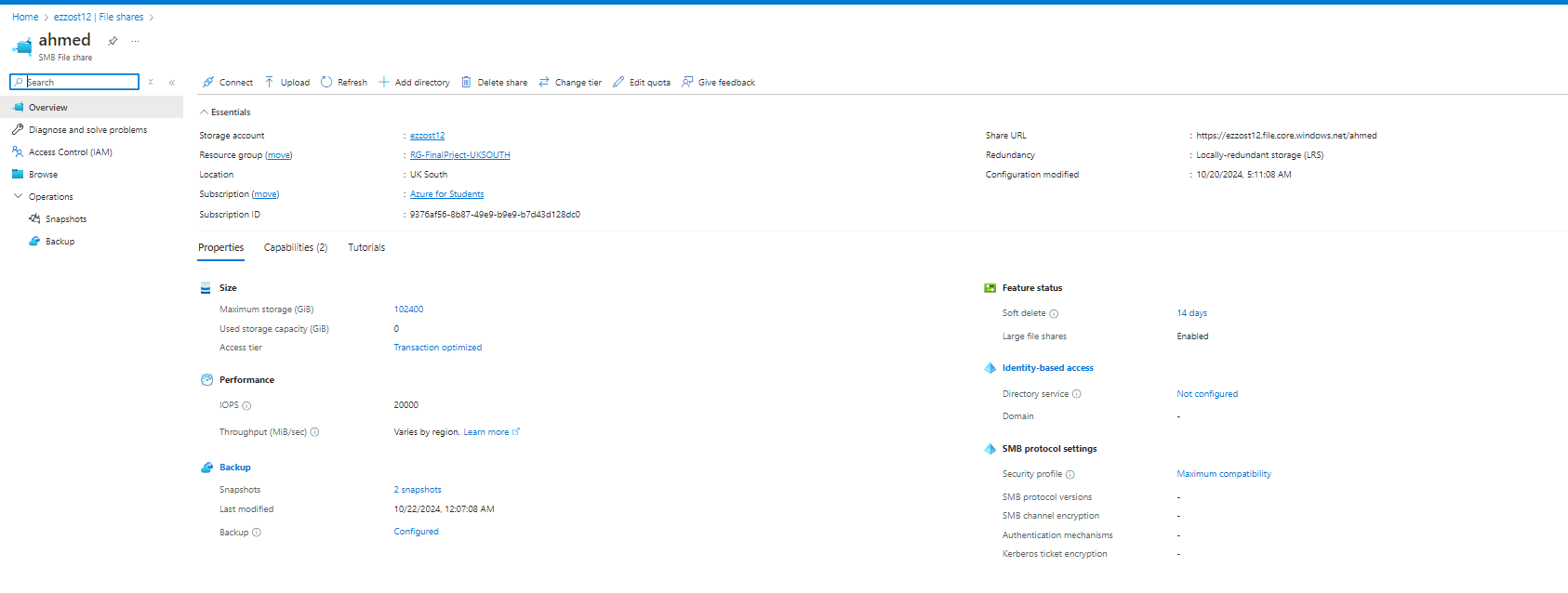
**2-Create a new File Shares**:

-Click on the “+ **File Shares**” button.

1. **Provide a name for the container**

****

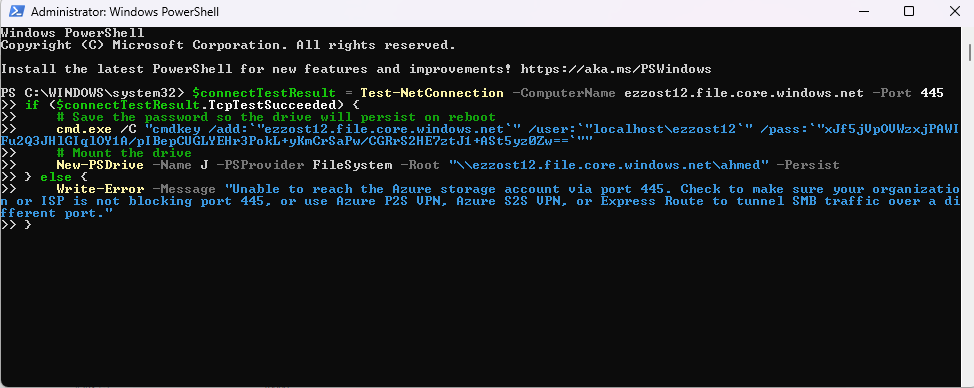
**Fig(1)**

**Fig(2)**

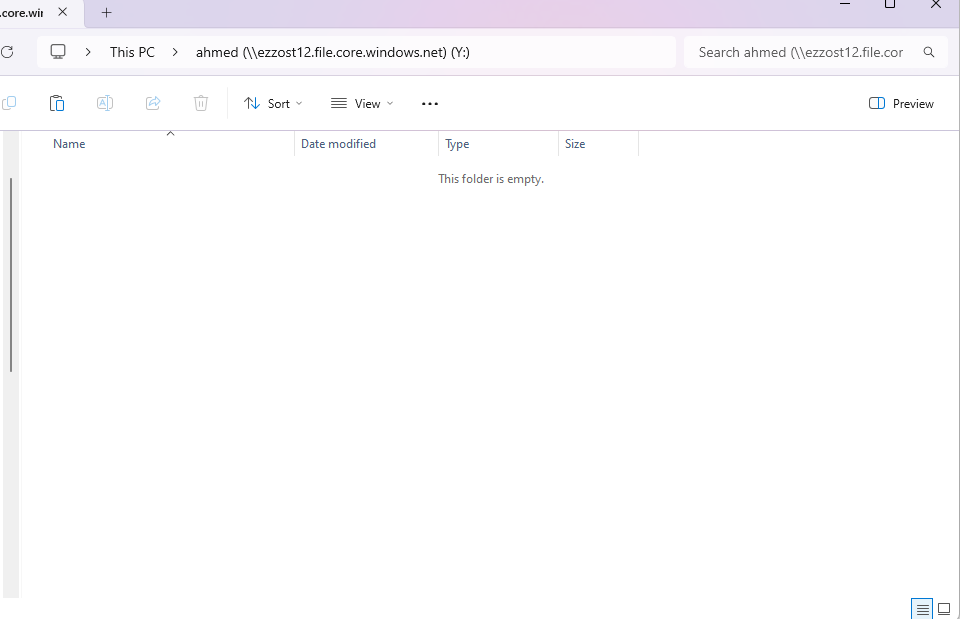
### 4.2 Mounting The File Share

- Open the computer that the **HR (VM1-Fp)** are using

- copy the connection string from the file share in the sorage account and open **Power Shell** and put it



- File share will appear

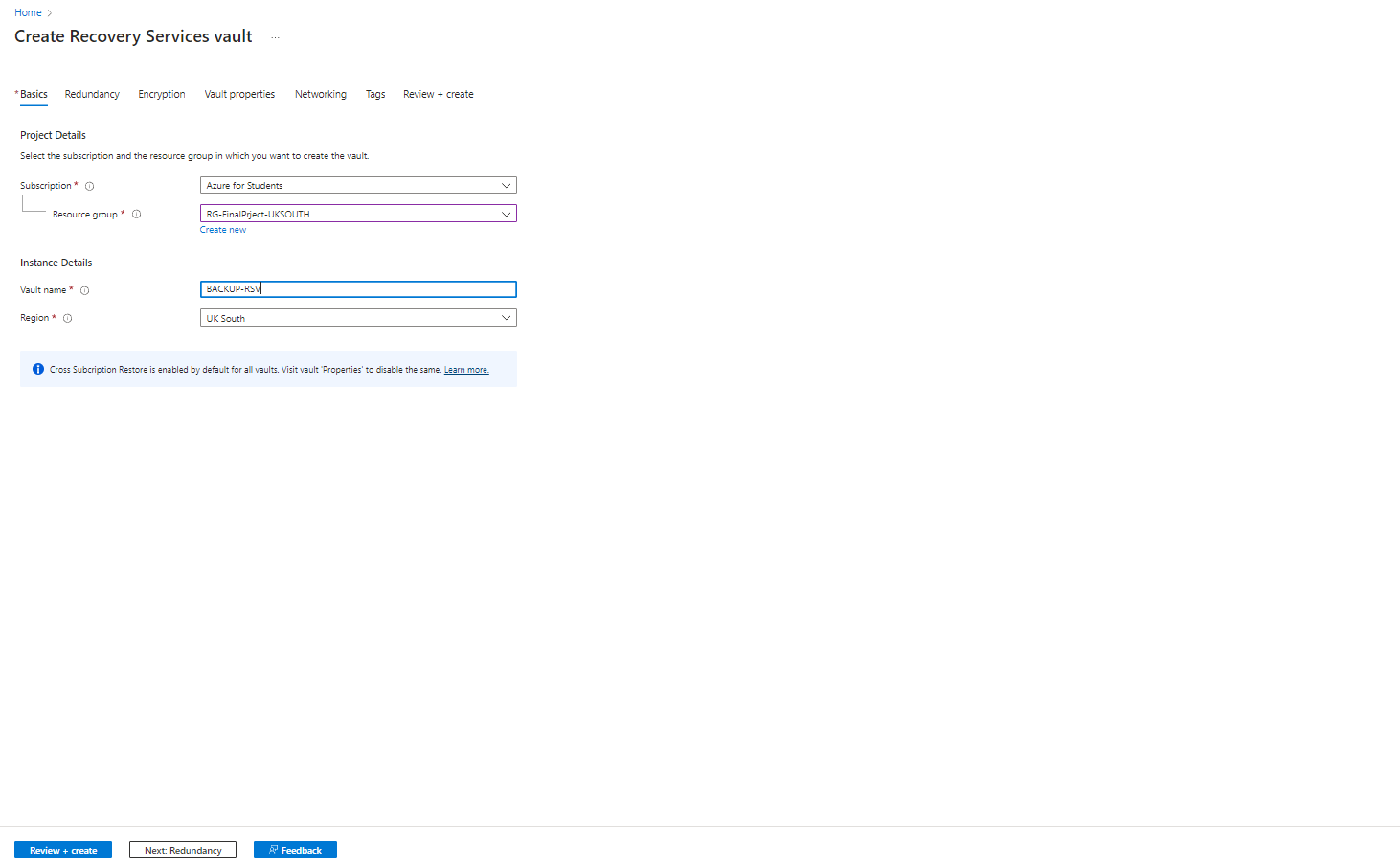


### 5. Backup Solutions for VMs and Files

#### 5.1 Setting Up Backup for Azure VMs

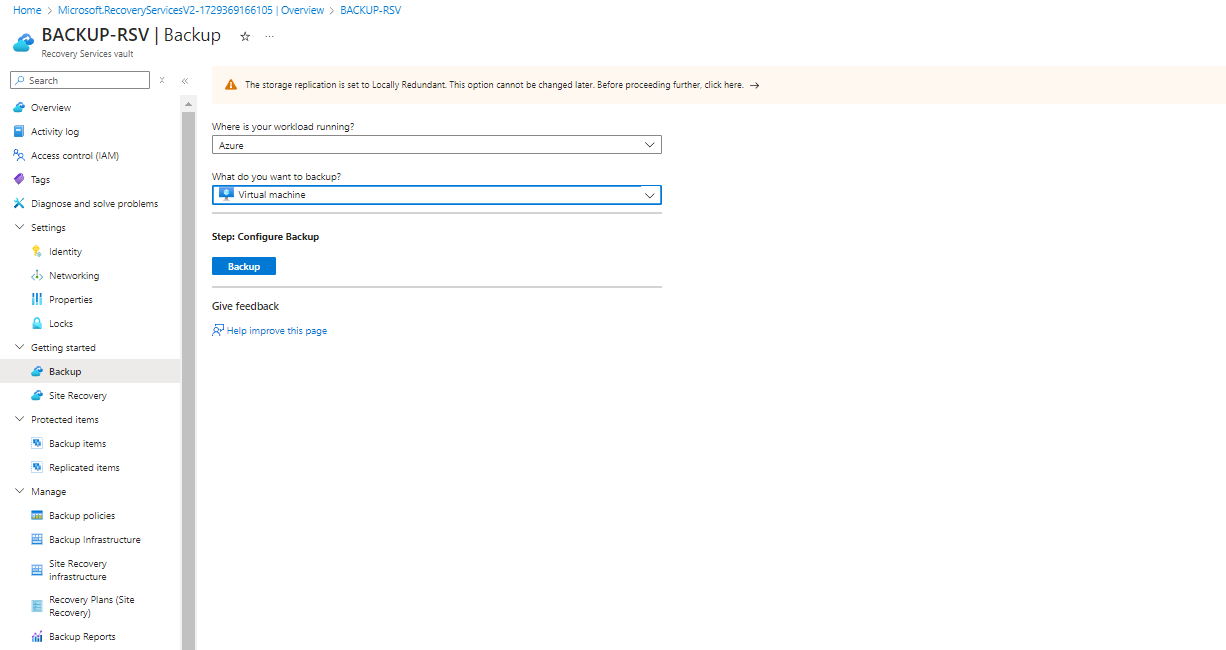
**1-Navigate to Recovery Services Vault**:

-Search for and select “Recovery Services vaults” in the Azure portal.

**2-Configure Backup**:

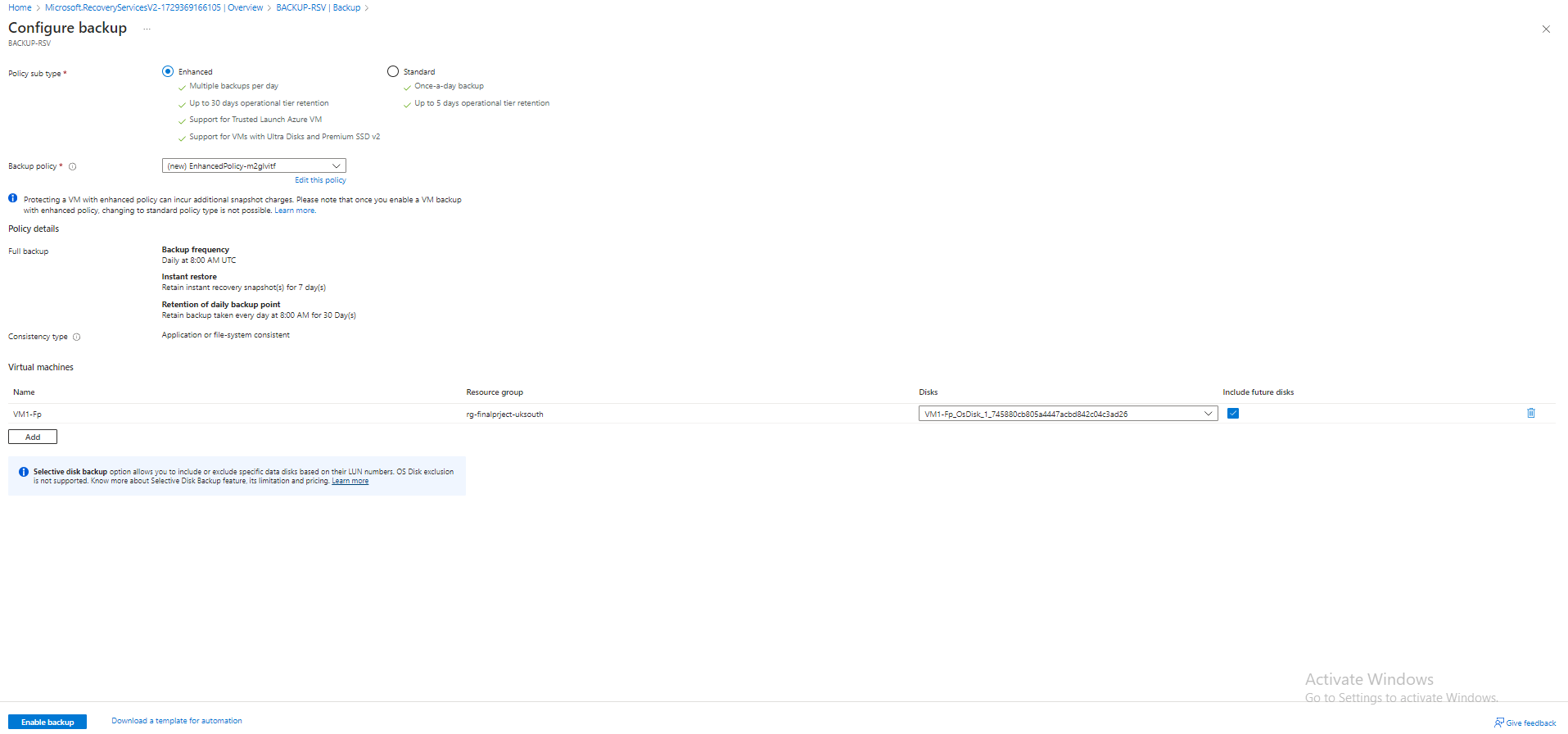
-Select an existing vault or create a new one.

-Click on “Backup” and choose “Azure Virtual Machine” as the backup goal.

****

**3-Select VMs**:

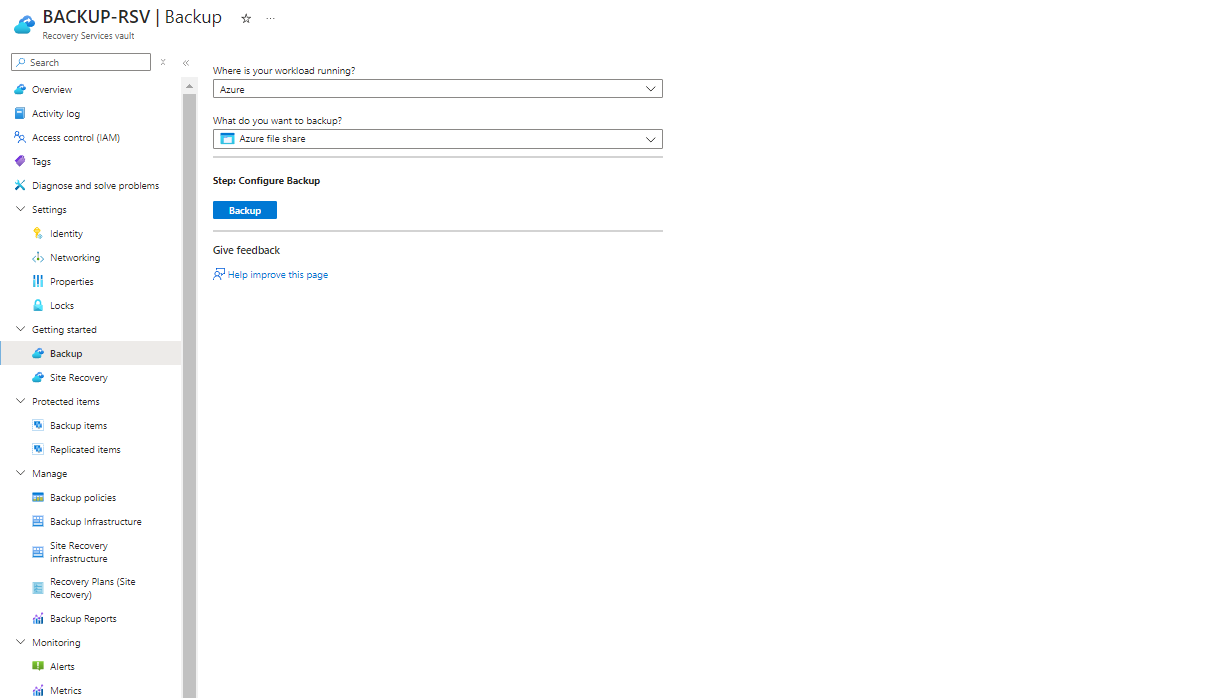
-Choose the VMs you want to back up and configure the backup policy settings according to your requirements.

**4-Enable Backup**:

-Review the settings and click “Enable backup.”

#### 5.2 Configuring File Backup Solutions

**1-Configure Backup**:

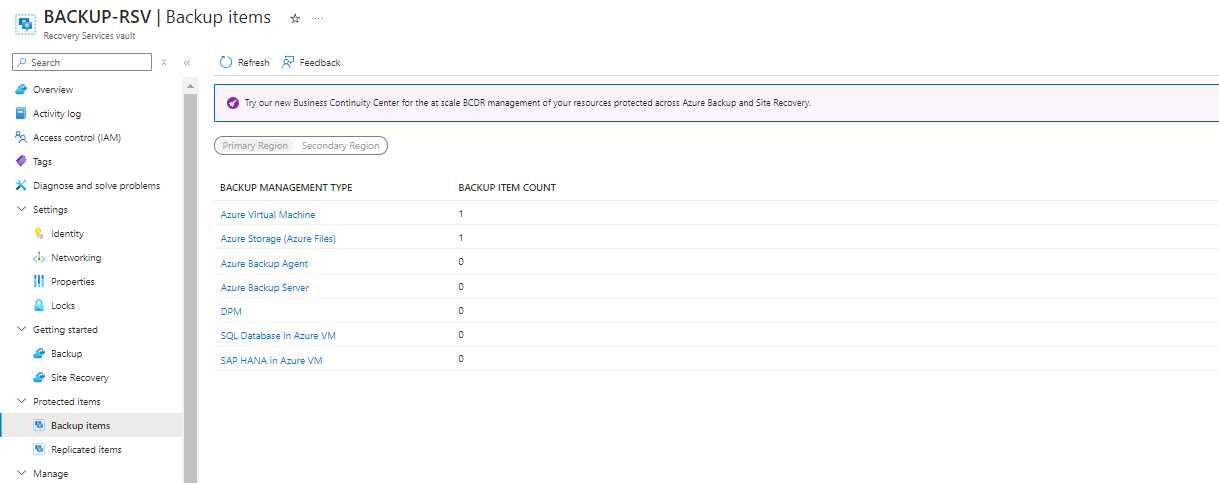


**2-Select File Share**:

-Leverage the Recovery Services Vault to backup file shares as needed.

### {68F55E1C-D463-4A3C-A78D-39444B97ABE0}

**4.3 BackUp Items For VM and File Share** :



### 5. Conclusion

The implementation of Azure storage solutions has been successfully completed. Storage accounts were created, Blob Storage was configured, and backup solutions for both VMs and files have been established. These measures ensure data integrity and availability, aligning with organizational data management goals.