**File share**

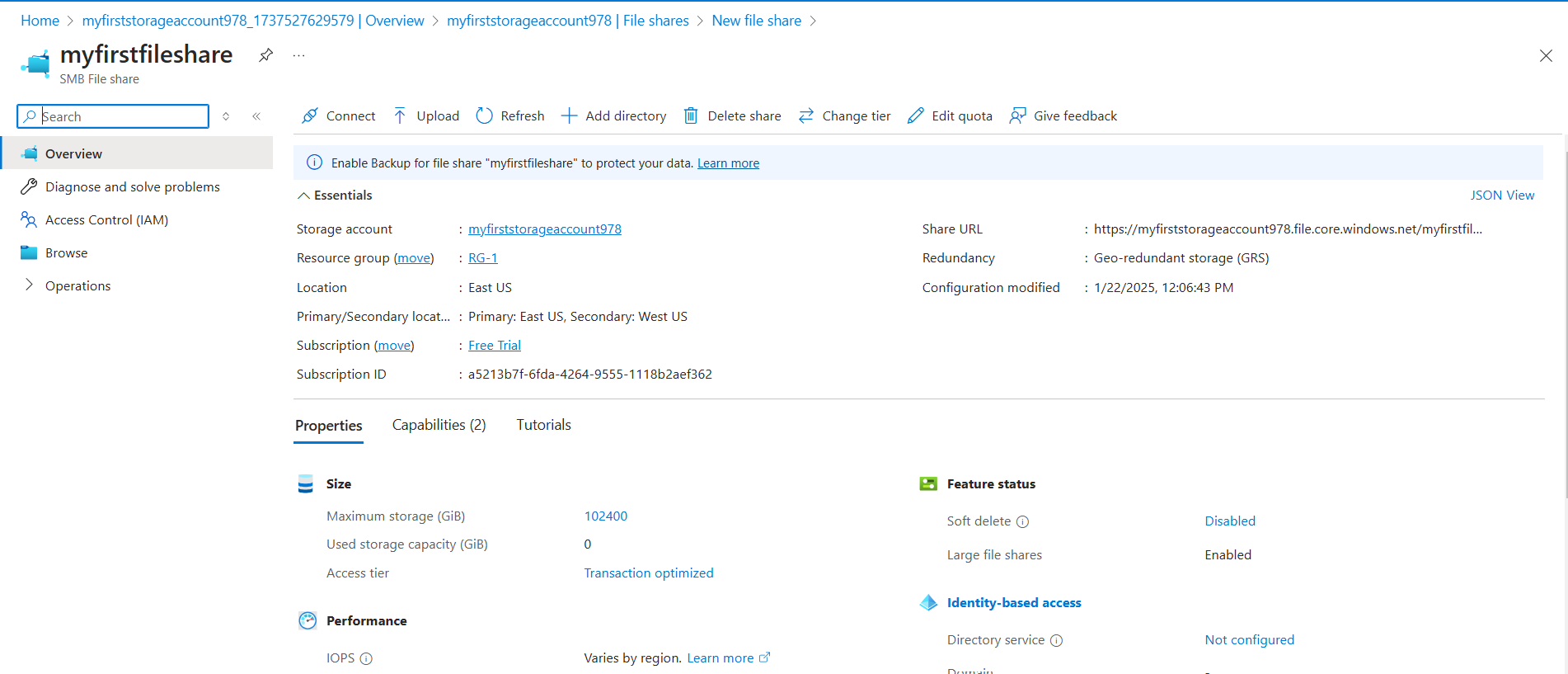
**Azure File Share** is a cloud-based file storage service that provides shared access to files across on-premises, cloud, and edge environments.

**Key Features:**

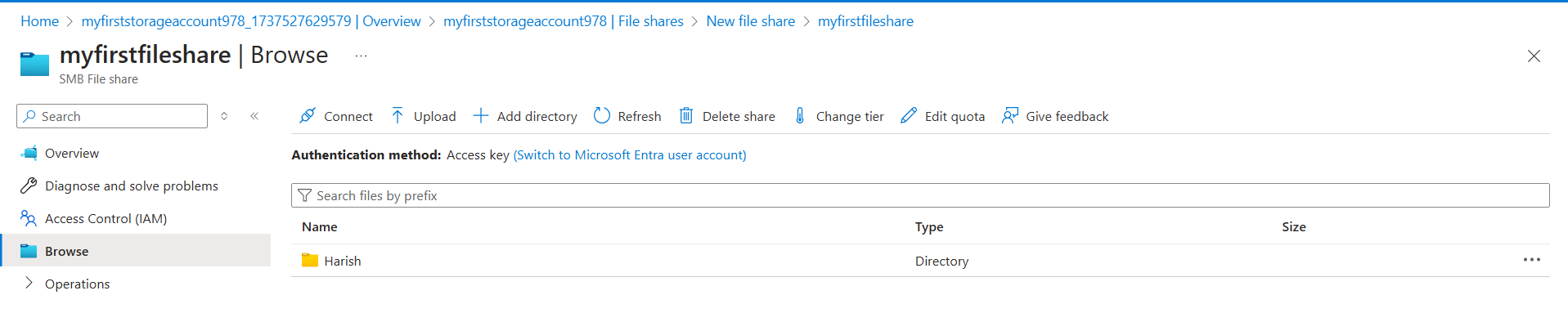
* **Simplified Management:** No need to manage physical servers, operating systems, or storage hardware. Azure handles all the underlying infrastructure.
* **SMB and NFS Protocols:** Supports both SMB and NFS protocols, enabling compatibility with a wide range of operating systems and applications.
* **File Sync:** Synchronizes files between on-premises servers and Azure File Shares, ensuring data consistency across locations.
* **Geo-Replication:** Replicates data across multiple regions for disaster recovery and business continuity.
* **Integration with Azure Ecosystem:** Seamlessly integrates with other Azure services, such as Azure Virtual Machines, Azure Kubernetes Service, and Azure Functions.
* **Security:** Supports encryption at rest and in transit, access controls, and network security groups.
* **Scalability:** Easily scale storage capacity and performance on demand.
* **Global Availability:** Access files from anywhere in the world with low latency.
* Azure file share supports lift and shift scenario it enables us to move or migrate over data from on premise to cloud and vice versa.
* Azure file share provides both classic and hybrid lift and shift scenario’s.
* **Classic lift and shift:** Here both the application and its data are moved to Azure.
* **Hybrid lift and shift:** Here only the application data is moved to Azure Files, and the application continues to run on-premises.
* It is Integration with Azure Active Directory (Azure AD) for security & authentication.
* Maximum capacity of file share is 100TB.
* Maximum capacity of file storage is 4.75TB.
* By default soft delete & default share level permissions are **disabled.**
* It provides centralized storage to all the servers or machines (mainly used in case of migrating on-premises machines to cloud).

**Creating of File Share and connecting it to the Windows VM and Linux VM.**

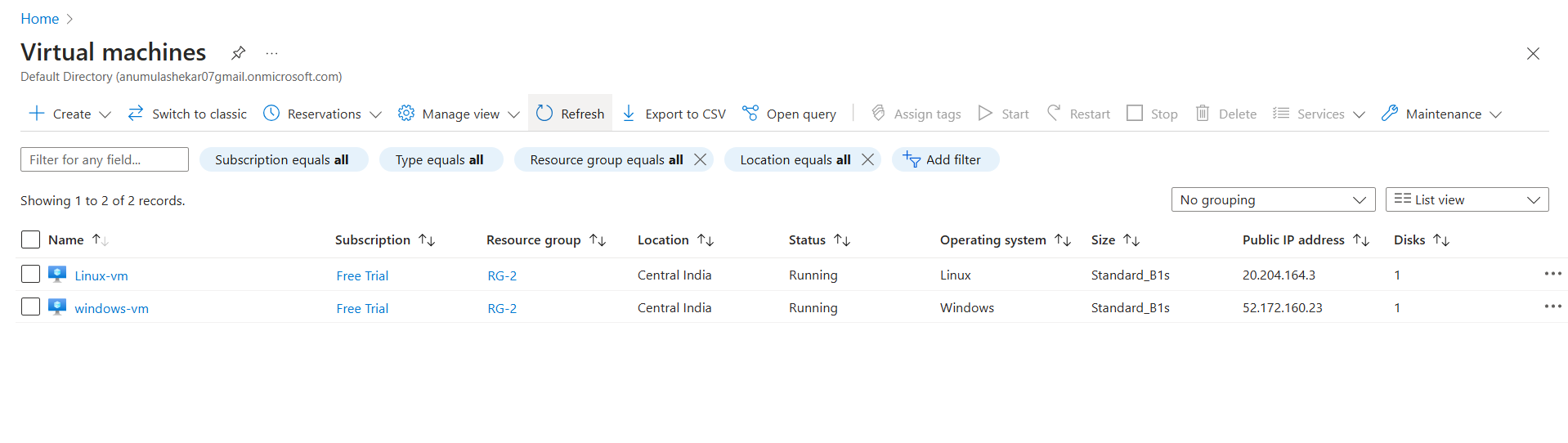
**Step1:** Create the File share by disabling Backup (for demo view).



**Step2:** Now add a directory (folder) to the file share.

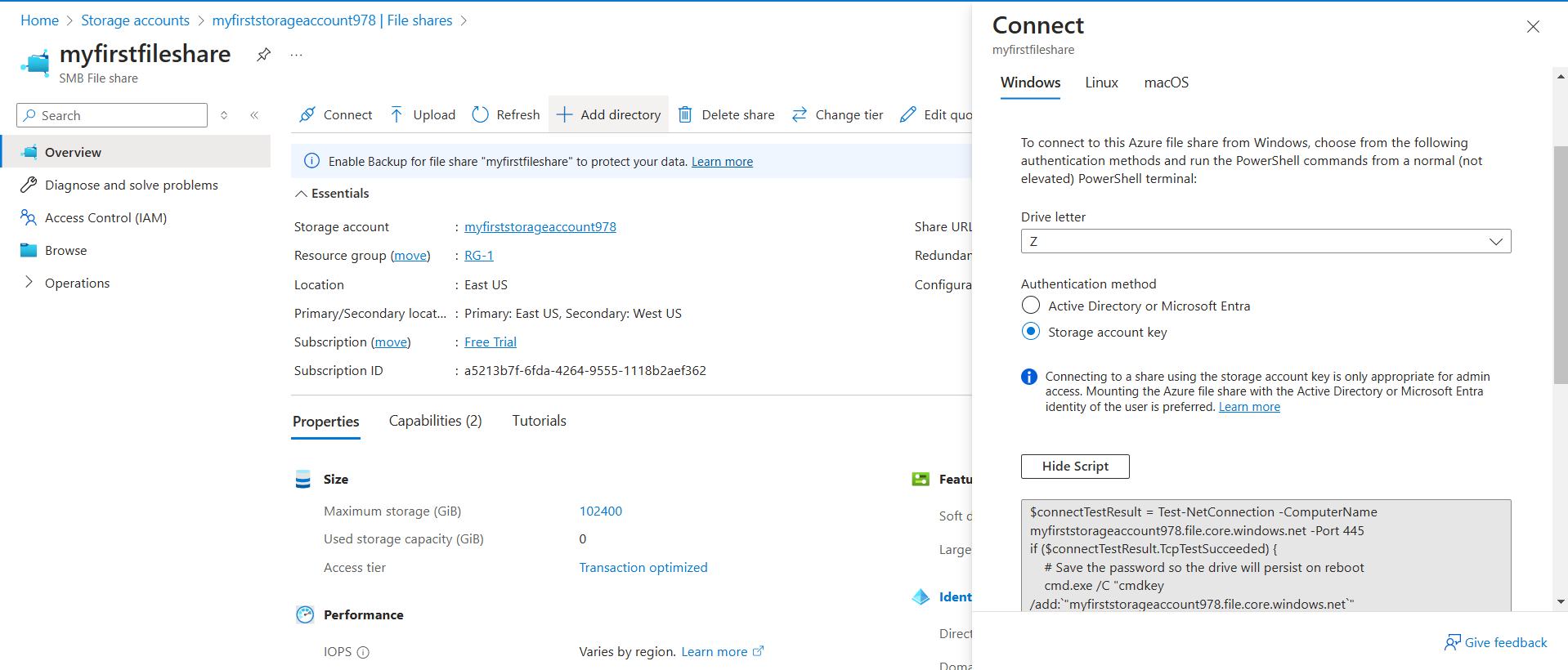


**Step3:** Create both Windows and Linux VM in same resource group.



**Step4:** Connecting of File share with the Windows VM.

Go to🡪File Share🡪connect🡪windows🡪copy the Hide Script and past it in the cmd of Windows VM🡪press Enter.



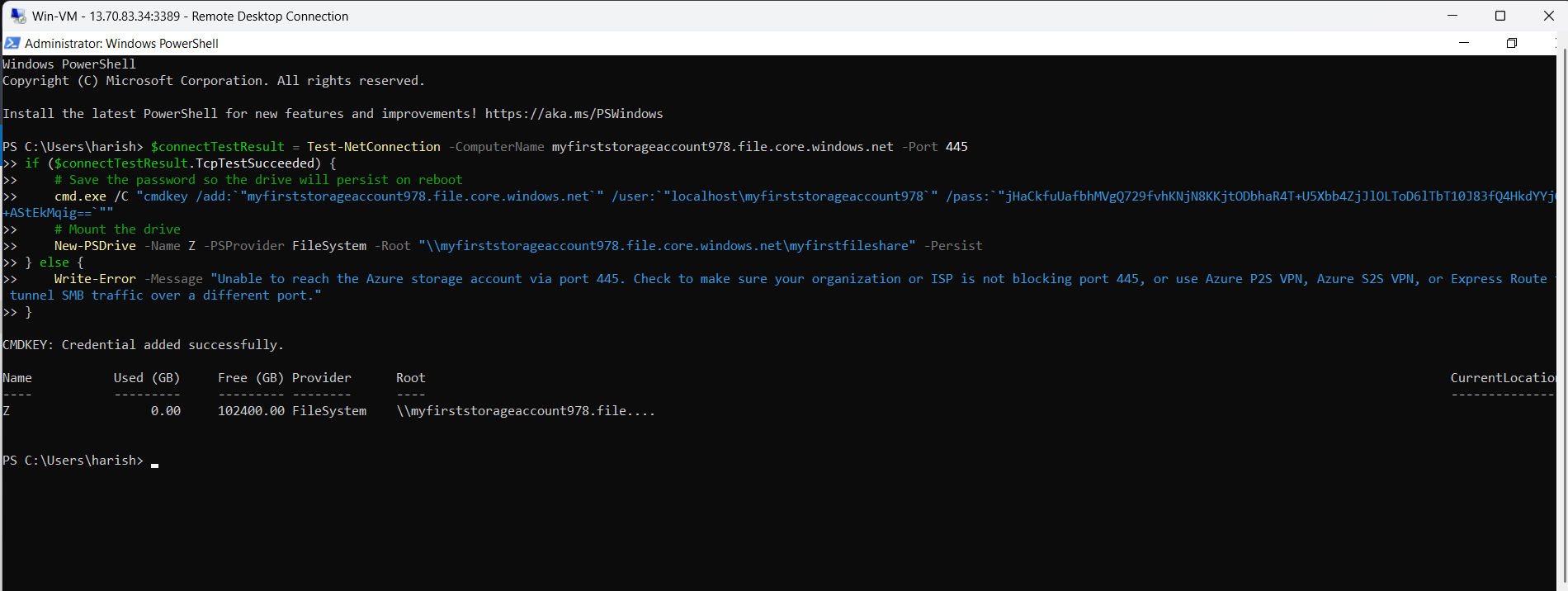
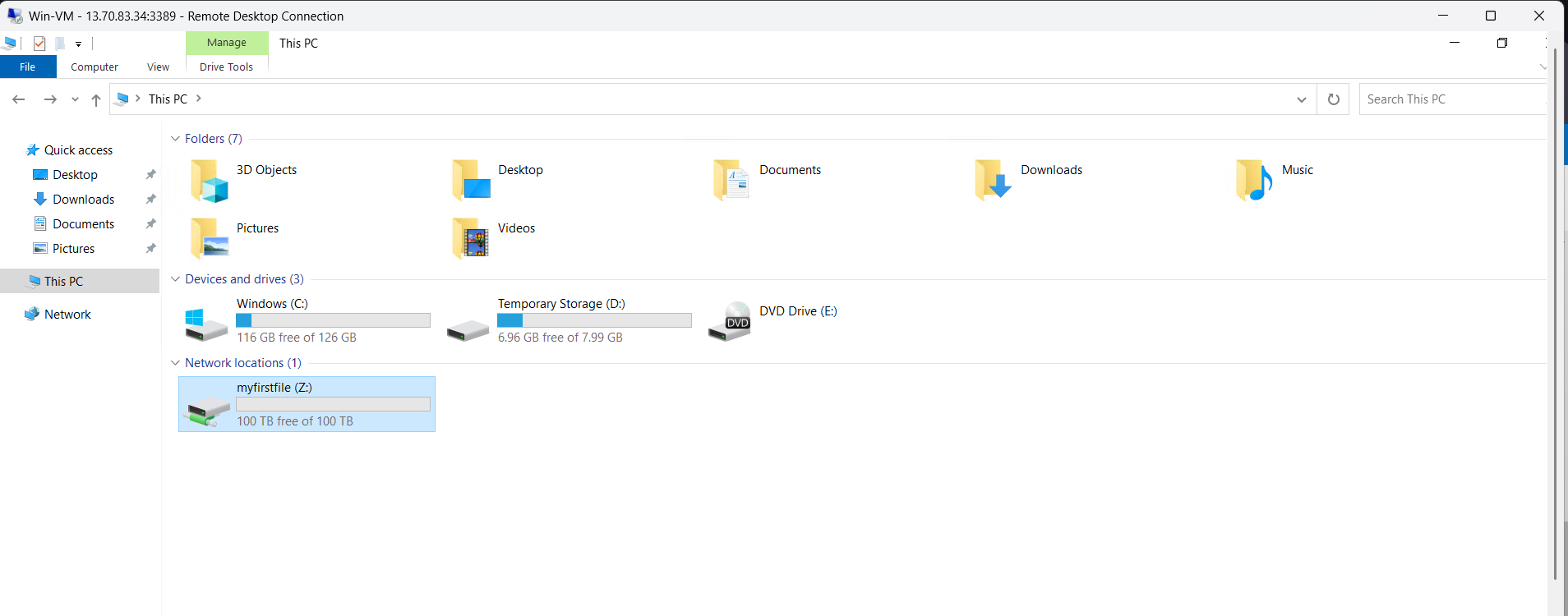


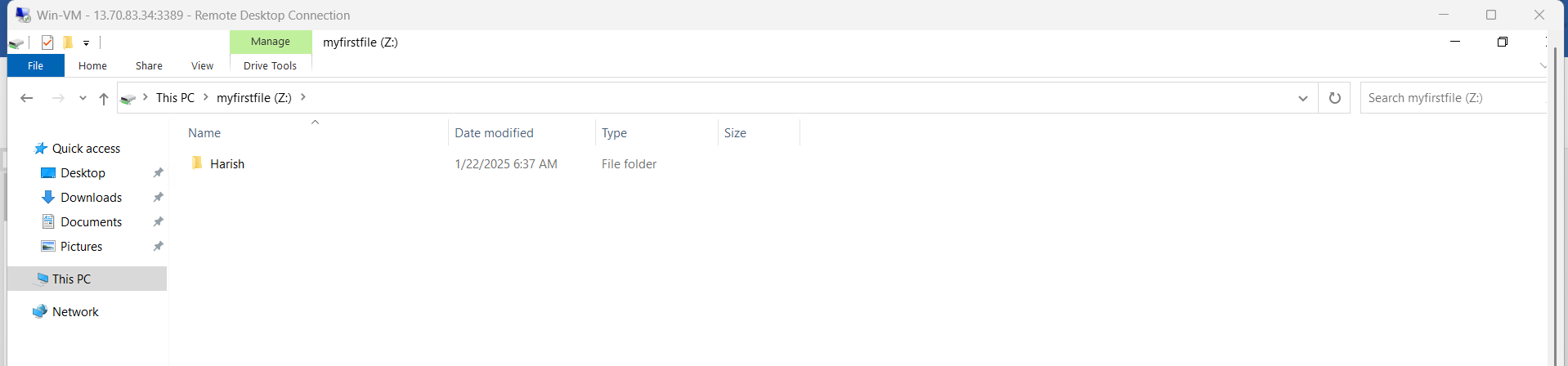
Fig: pasting of Hide Script in the CMD of windows VM.

**Note:** The file share can be connected to the windows VM using “port-445”

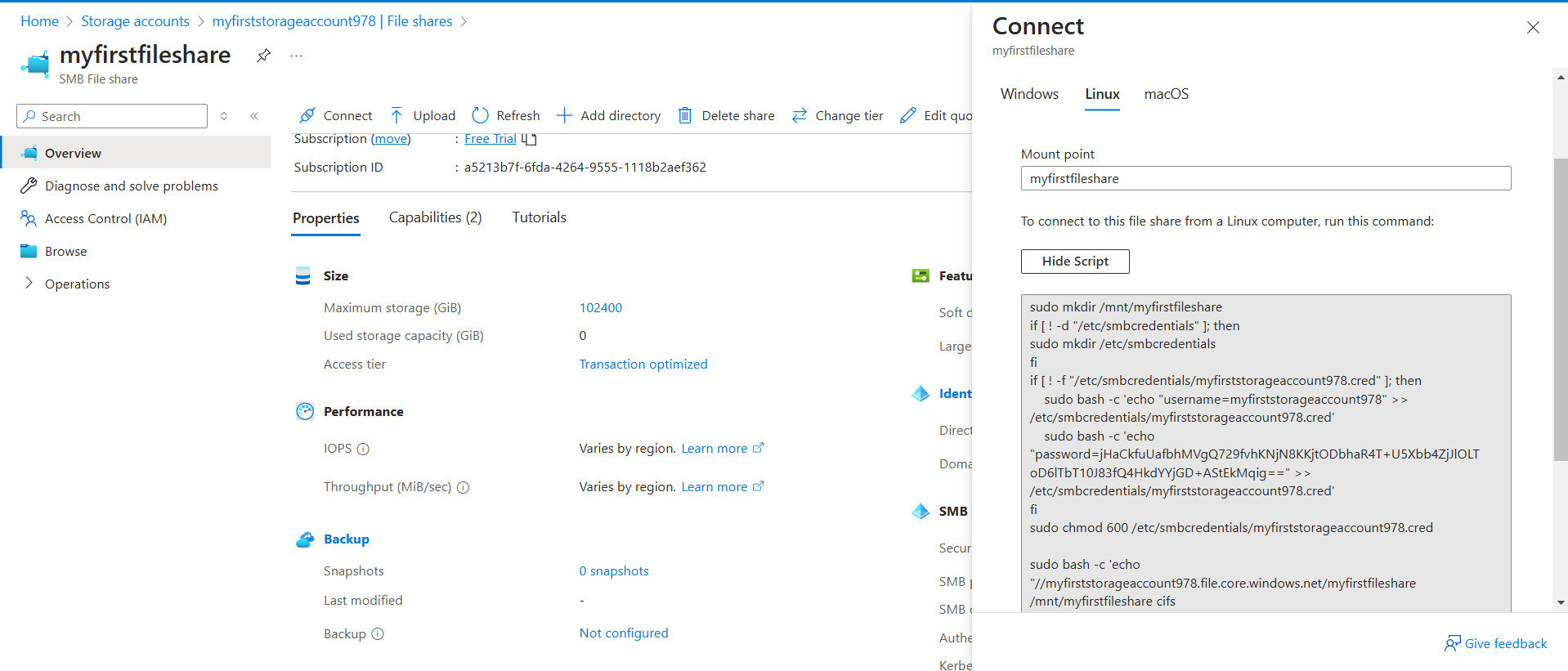
Then the File Share is added to Windows VM as a Z-drive as shown in below figure.

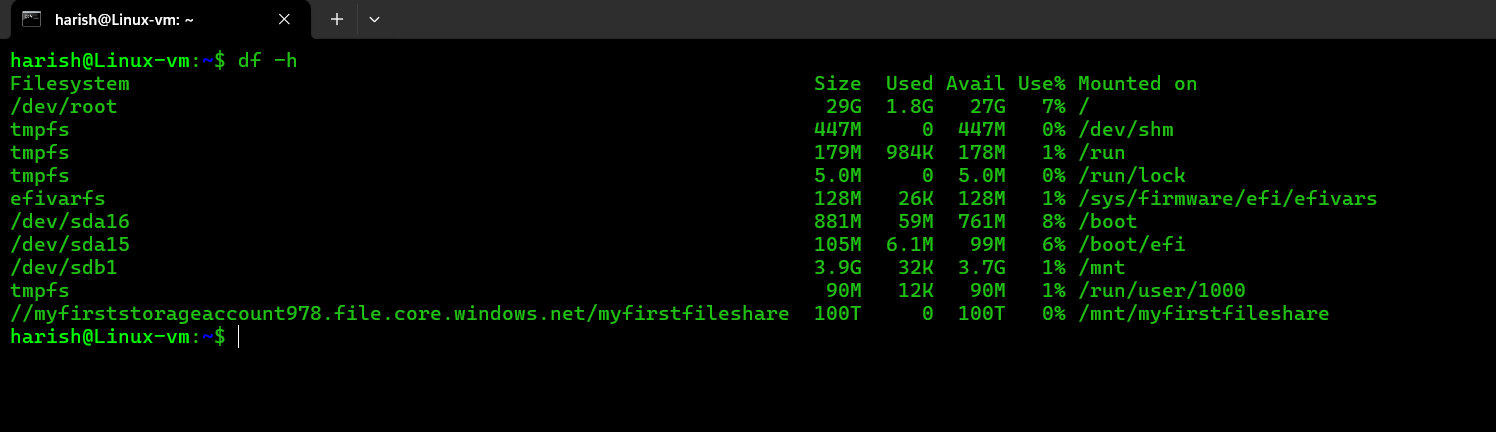


We can create or upload the files, documents from over local machine as well as from cloud.



**Step5:** Now connect the File Share with the Linux VM.

Go to🡪file share🡪connect🡪 select Linux OS🡪 copy the Hide Script and past in the Linux cli and press enter.



The file share (myfirstfileshare) is added to the Linux VM as shown above figure.

**Queue & Table Storage**

We can connect this Queue and Tables by using the URL’s.

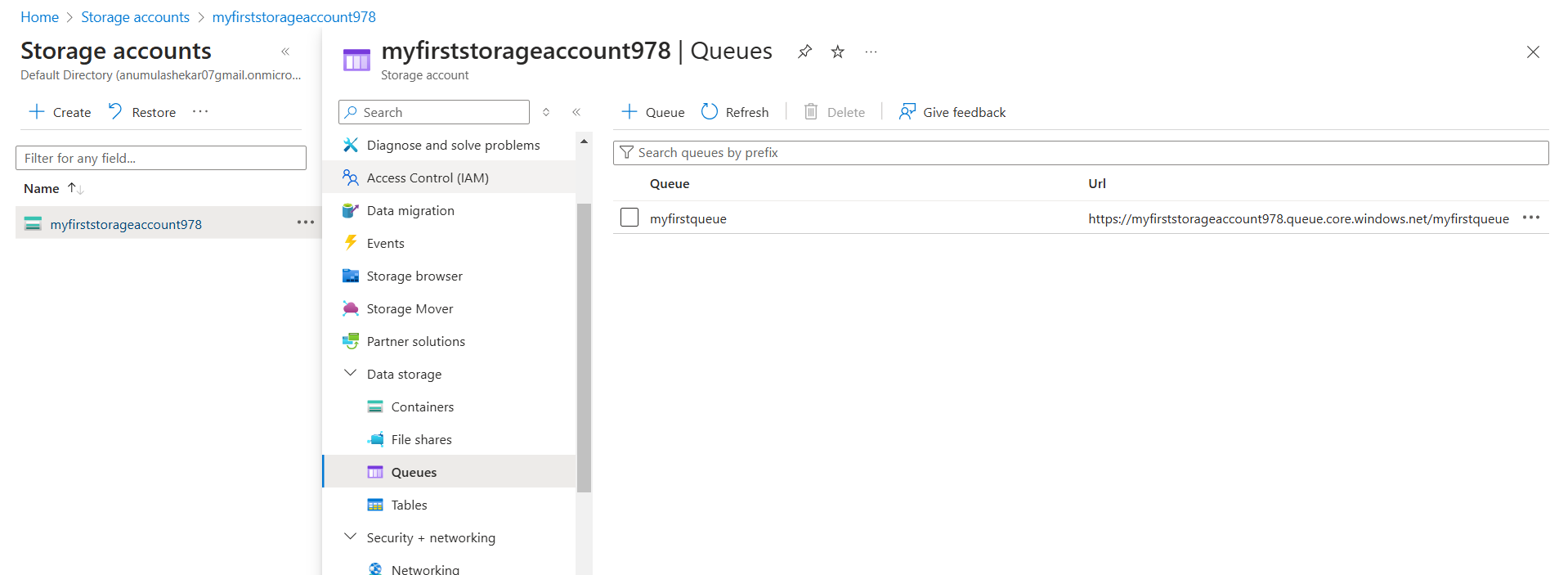


Fig: Queue storage with URL

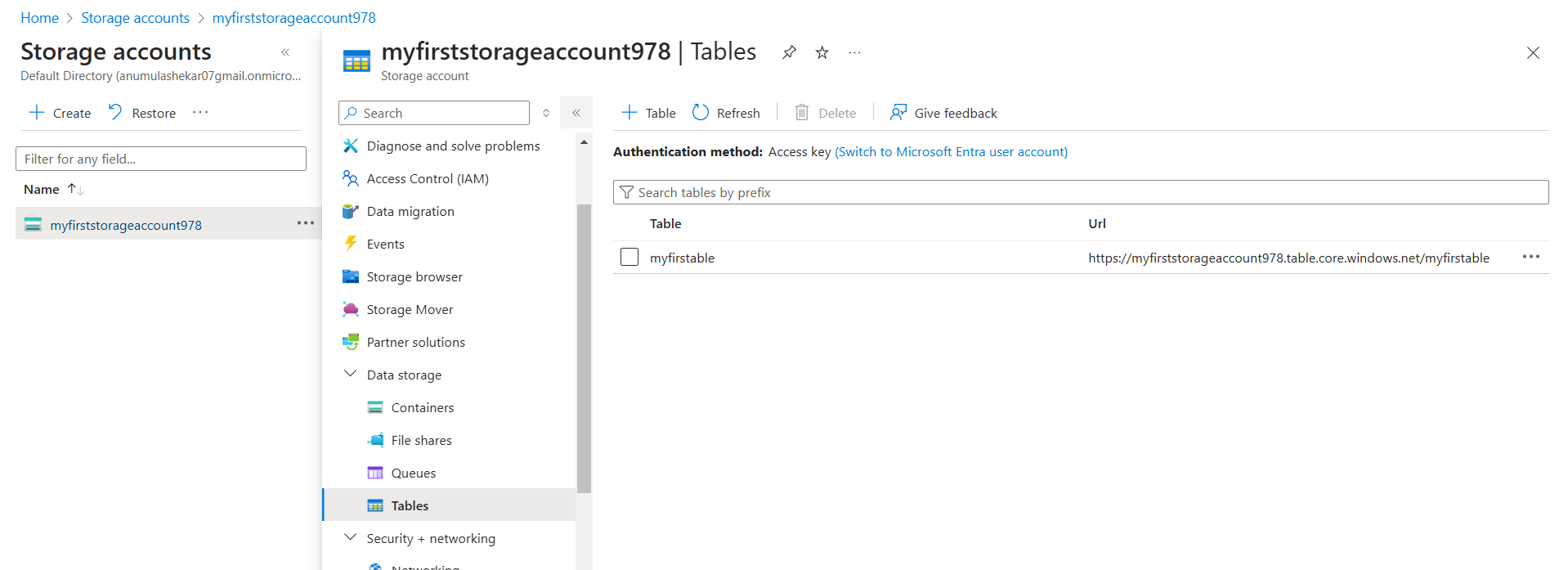


Fig: Table storage with URL.

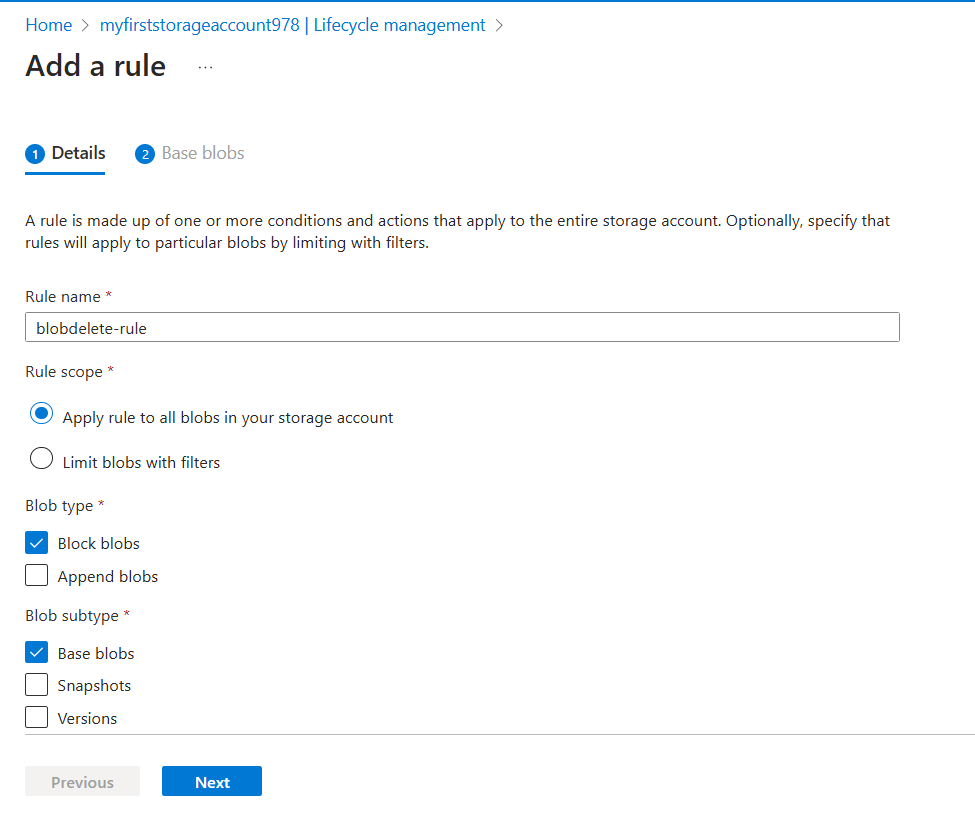
**Lifecycle Management**

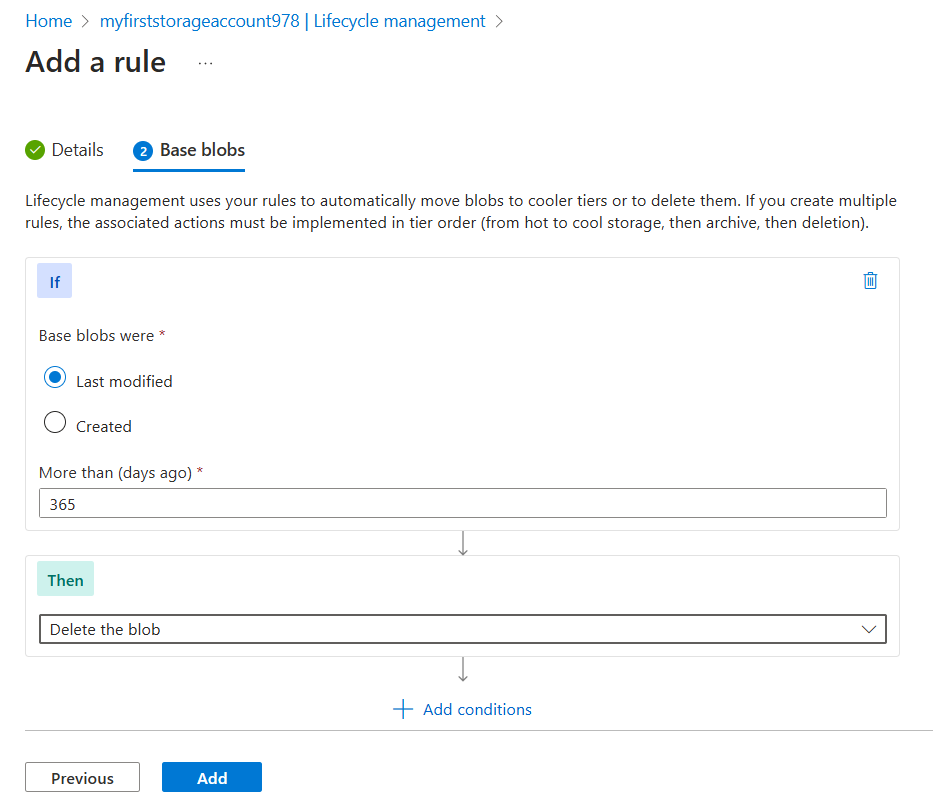
In azure storage service, Lifecycle Management is a feature that helps you automate the management of data stored in **Azure Storage accounts**, including **Blob Storage** and **Azure Data Lake Storage Gen2**.

It uses **lifecycle management policies** **or Rules** to automate the movement of data between access tiers, delete unused data, and optimize storage costs based on your usage patterns.

That means by using Lifecycle management we can Add Rules, to move data between access tiers, deleting of unused date and optimizing of storage cost….

Let’s Add a Rule in Lifecycle Management:

**Step1:** creating of Lifecycle Management Detail.

**Step2:** Configuring of Base blob polices.

From above figure we configured that the data which is stored in Blob that should be deleted after 365 days (the last modified is 365 days back).old data should be deleted.

This means we added the Rule, that any data stored in the Blob container that hasn't been changed or updated within the last year will be automatically removed or deleted.

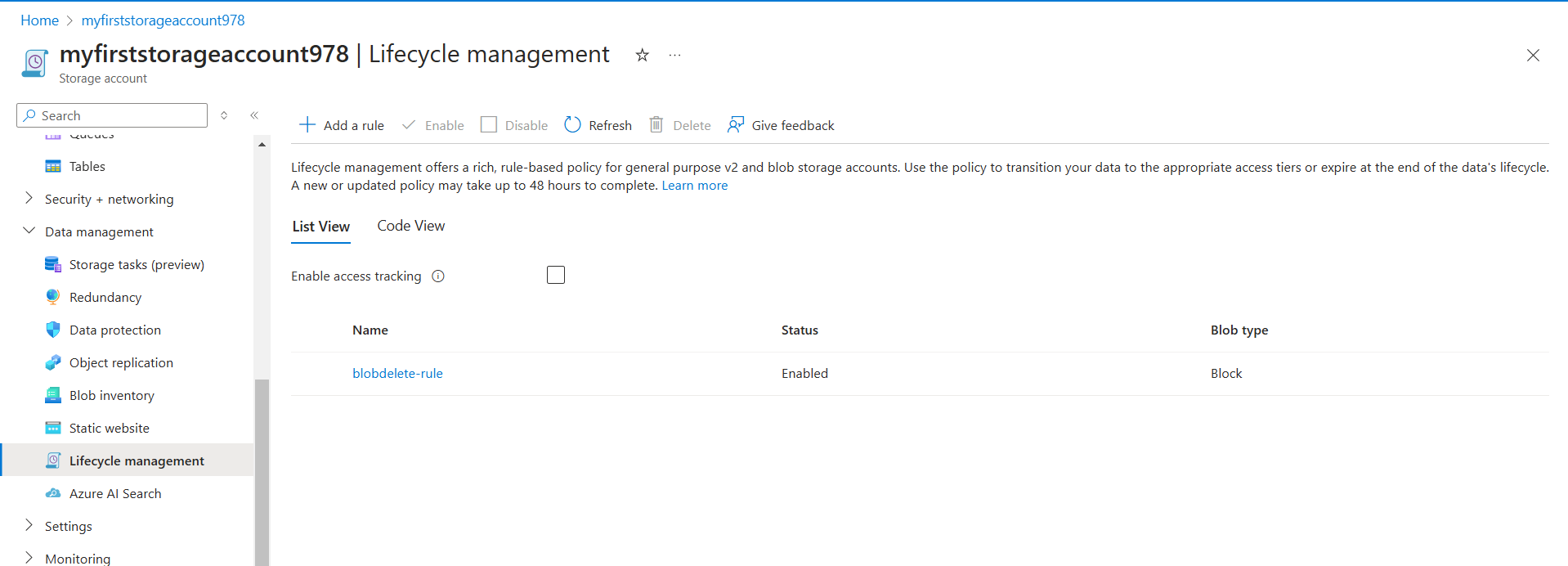


Fig: Rule is added successfully.