

Microsoft Azure storage

Introduction

In this article, I will guide you through what an Azure storage account is, how to create one, and how to configure a private endpoint to ensure secure connectivity to your storage account resources.

To configure a storage account using an Azure private endpoint, make sure you have the following resources created in your Azure subscription:

1. A Resource group (check my previous article on how to create a Resource group)
2. A virtual network and subnet (check my previous article on how to create virtual networks and subnets)
3. A Storage account
4. A File share
5. Files uploaded to the file share
6. Disabled public network access for the file share
7. A Private Endpoint
8. A Virtual machine
9. Verification of the Azure private endpoint configuration

Azure Storage

An Azure storage account contains all of your Azure Storage data objects, including blobs, files, queues, and tables. It provides a unique namespace for your data that is accessible from anywhere in the world over HTTP or HTTPS. Data stored in your account is durable, highly available, secure, and massively scalable.

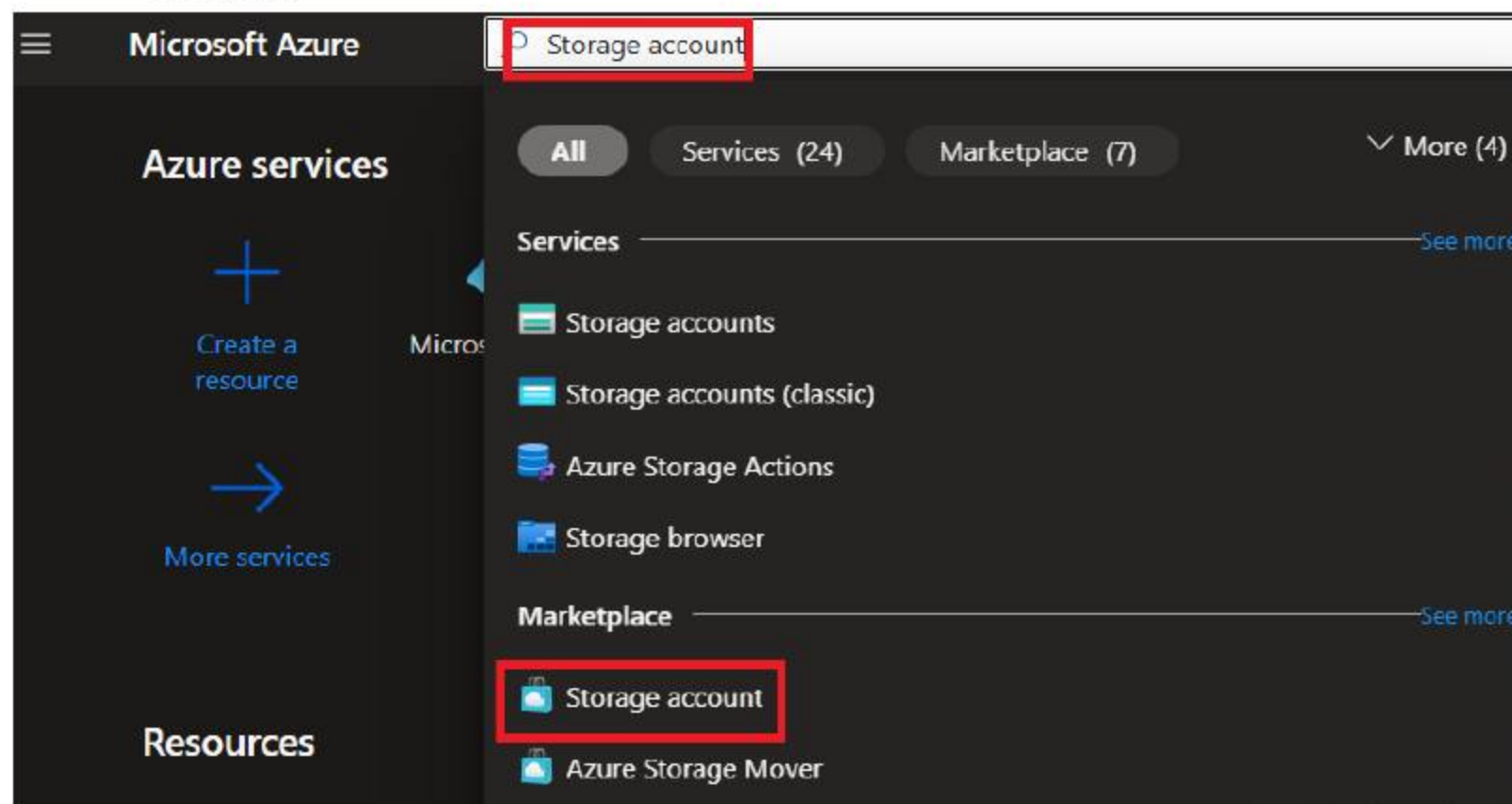
[In this article](#), we will focus specifically on Azure Files.

Note: When creating a storage account, the name of the storage account must be unique across all existing storage account names in Azure and must only contain lowercase letters and numbers.

Step 1: Create Azure Storage Account

1. Sign in to the [Azure portal](#).

2. In the top search box, type **Storage account**, then select it under the **Marketplace** section.



Basic tab > Project details:

A screenshot of the 'Create a storage account' form in the Microsoft Azure portal. The form is divided into several tabs: 'Basics', 'Advanced', 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review'. The 'Basics' tab is selected. Under the 'Project details' section, the 'Subscription' dropdown is set to 'ABCOFCLOUD' and the 'Resource group' dropdown is set to 'Sarah1-RG'. Both dropdowns are highlighted with red boxes. Below this, the 'Instance details' section shows the 'Storage account name' as 'techbysara' and the 'Region' as '(US) East US', both highlighted with red boxes. The 'Performance' section has the 'Standard' option selected, and the 'Redundancy' section has 'Geo-redundant storage (GRS)' selected. At the bottom, there are buttons for 'Review', '< Previous', and 'Next : Advanced >'.

3. **Subscription** > Select the subscription where you want to create the storage account (for example, **ABCOFCLOUD**).

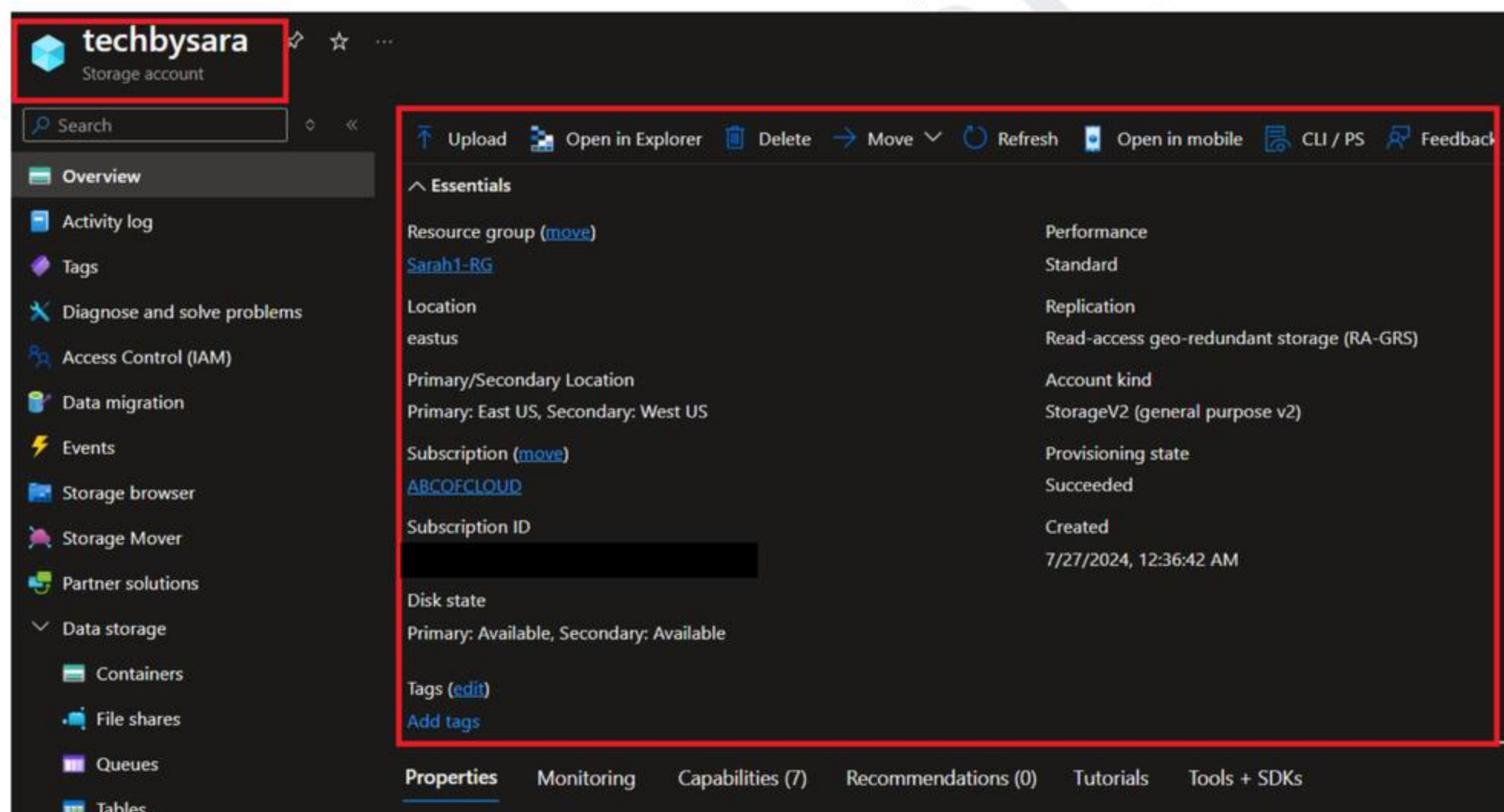
4. **Resource group** > Select the resource group to deploy your resources in (for example, **Sarah1-RG**).
5. **Storage account name** > Enter a unique name for your storage account (for example, **techbysara**).
6. **Region** > Select your preferred geographic location (for example, **East US**).
7. **Performance** > Select **Standard** to create a general-purpose v2 account. This option provides access to all standard Azure Storage services, including blobs, files, queues, tables, and disks.
8. **Redundancy** > Select **Geo-redundant storage (GRS)**. This setting replicates your data three times within the primary datacenter and three times in a secondary region for extra protection.
9. **Read access** > Check this option to ensure your data remains readable even if the primary region becomes unavailable.

Advanced tab > Keep the default settings.

Networking tab > **Network connectivity** > **Enable public access from all networks**.

Encryption tab > Data is encrypted by default using Microsoft-managed keys (keep default settings).

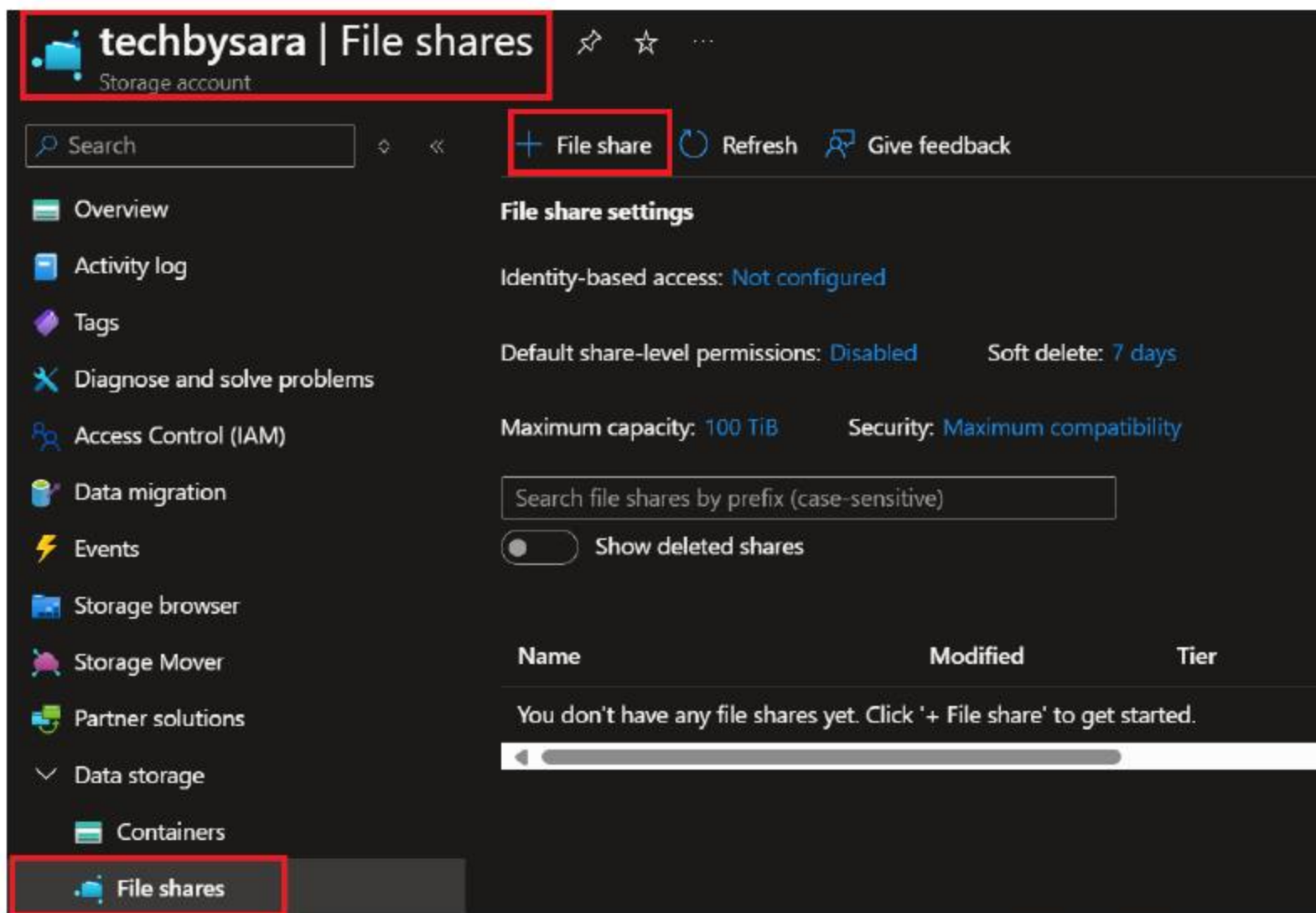
10. Select **Review + create**. Once validation succeeds, select **Create**.



The techbysara storage account has been successfully created.

Step 2: Create File Shares

1. Navigate to your new storage account (for example, **techbysara**).
2. Under the **Data storage** section in the left menu, select **File shares**.
3. On the File shares page, select **+ File share**.



This opens the **New file share** creation page.

New file share

Basics Backup Review + create

Name * techbysara-files

Access tier * Transaction optimized

Performance

Maximum IO/s ① 20000

Maximum capacity 100 TiB

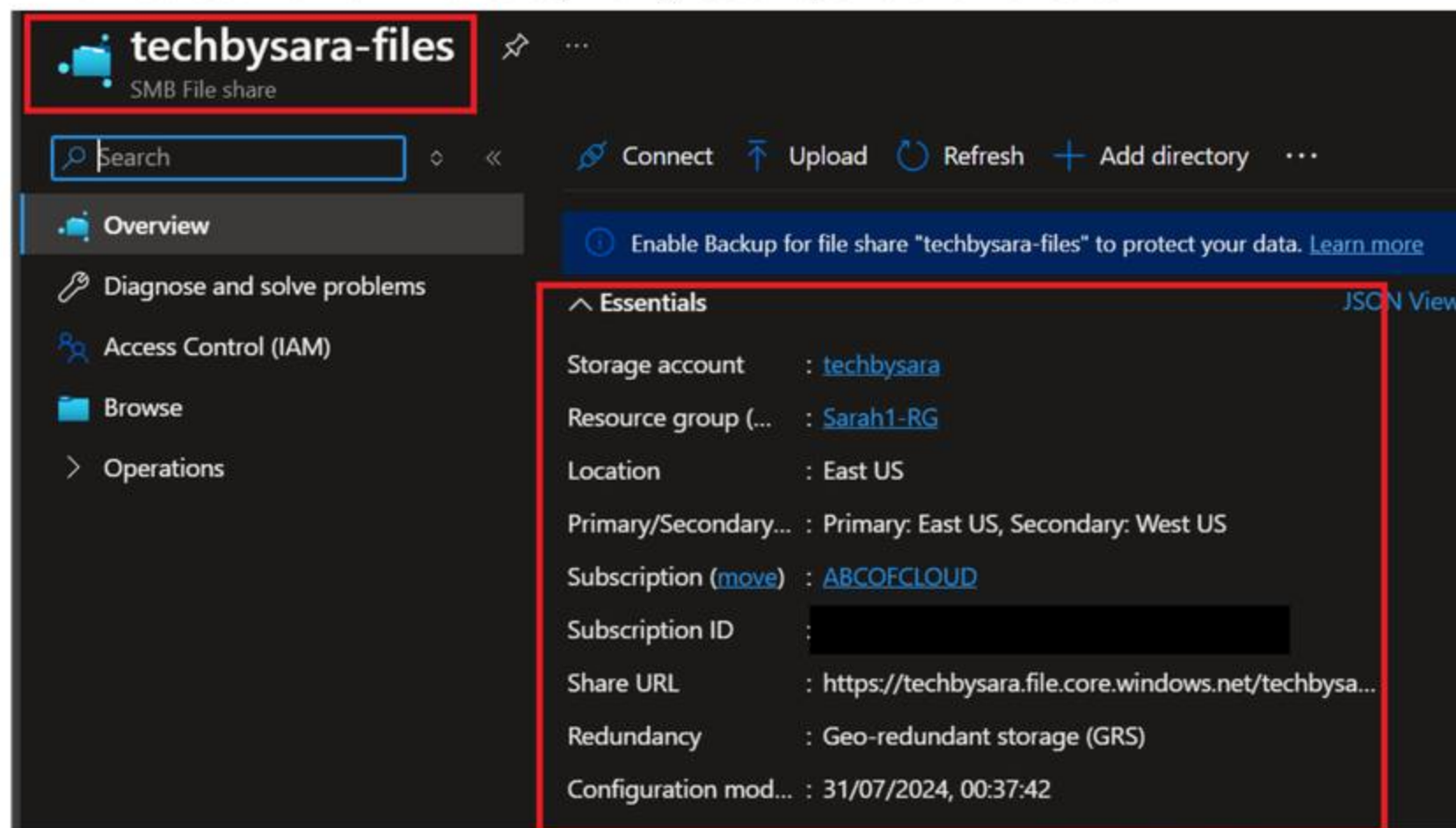
① To use the SMB protocol with this share, check if you can communicate over port 445. These scripts for [Windows clients](#) and [Linux clients](#) can help. Learn how to [circumvent port 445 issues](#).

Review + create < Previous Next : Backup > Give feedback

Basics tab:

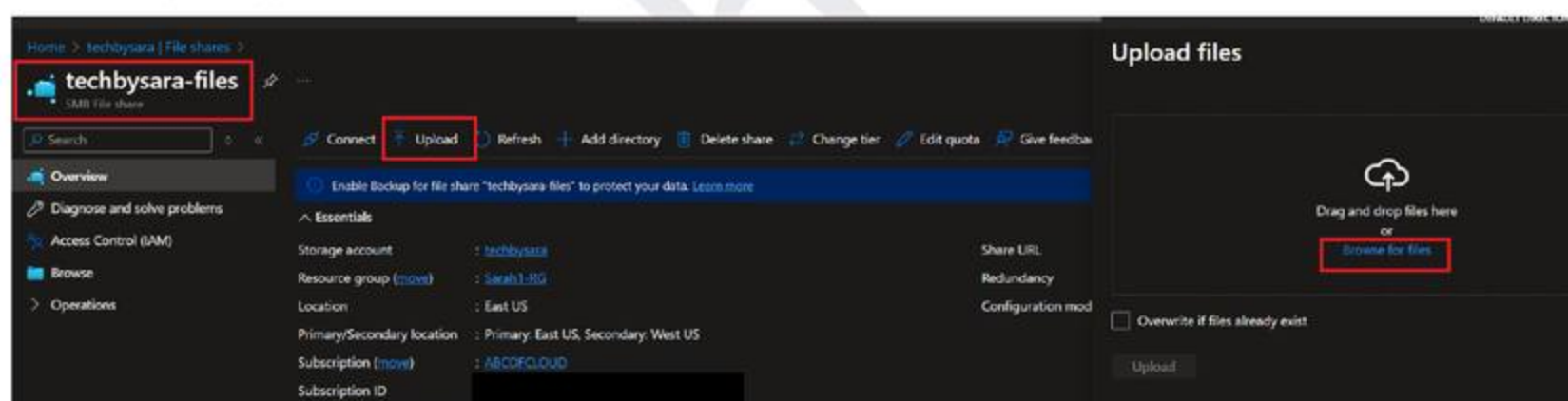
4. **Name** > Enter a name for the file share (for example, **techbysara-files**).
5. **Access tier** > Select a tier suited to your workload (for example, **Transaction optimized**).
6. **Maximum IO/s** > This shows the max I/O requests per second supported (for example, **20000**).

7. **Maximum capacity** > Set the capacity limit (for example, **100 TiB**).
- Backup tab** > For this walkthrough, uncheck **Enable backup**.
8. Select **Review + create**, verify details, and click **Create**.

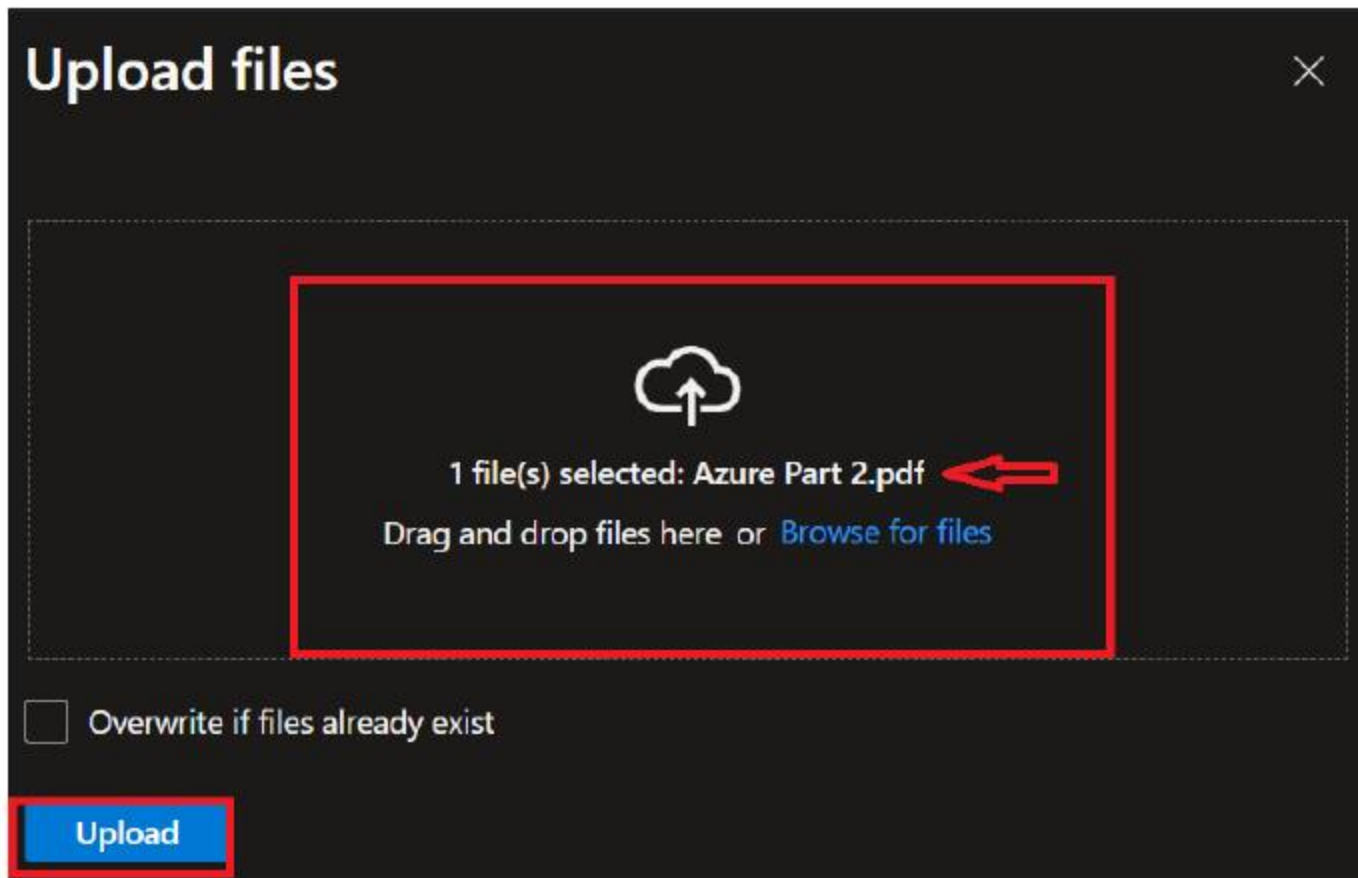


Step 3: Upload Files to File Shares

9. Upload Files > From the recently created file share > Select Upload > Click "Browse for files".

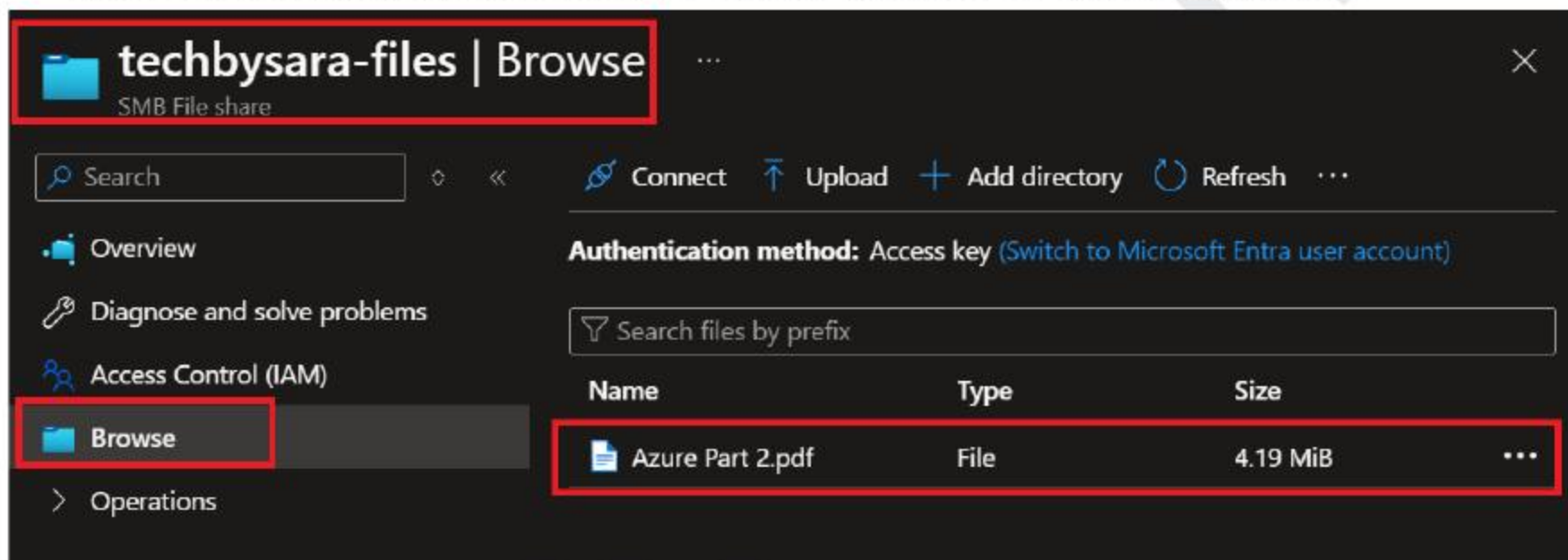


10. Select file from your preferred folders > Click Upload.



11. To confirm we can access recently uploaded files > select Browse from File shares page.

12. Access confirmed. In the image below, we can see uploaded files.



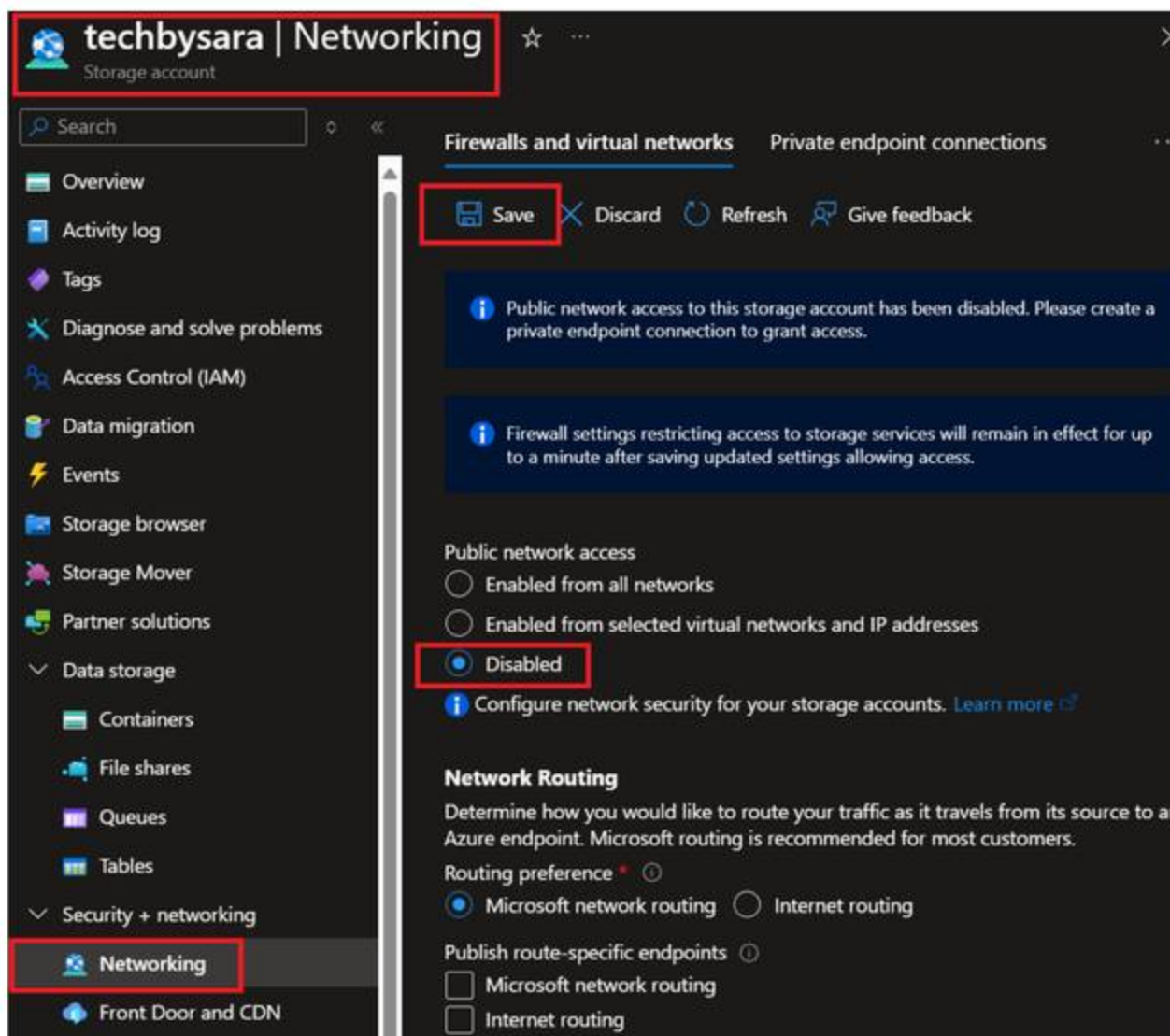
Successfully uploaded files.

Step 4: Disable Public Network Access

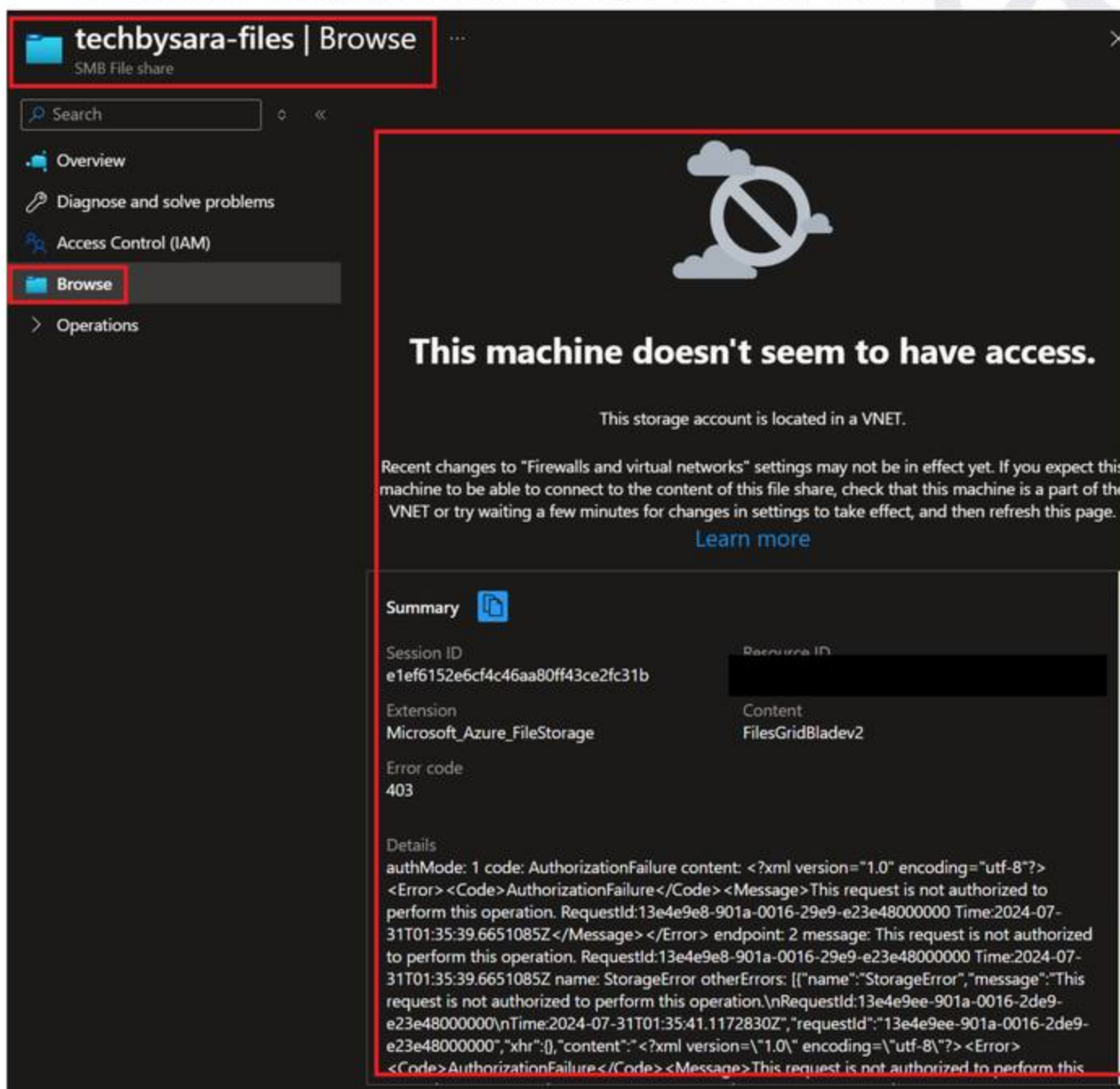
13. Open your Storage account (for example, **techbysara**).

14. In the left panel under **Security + networking**, select **Networking**.

15. Under **Public network access**, select **Disabled**, then click **Save**.



16. Confirm that public network access is now denied from external devices.

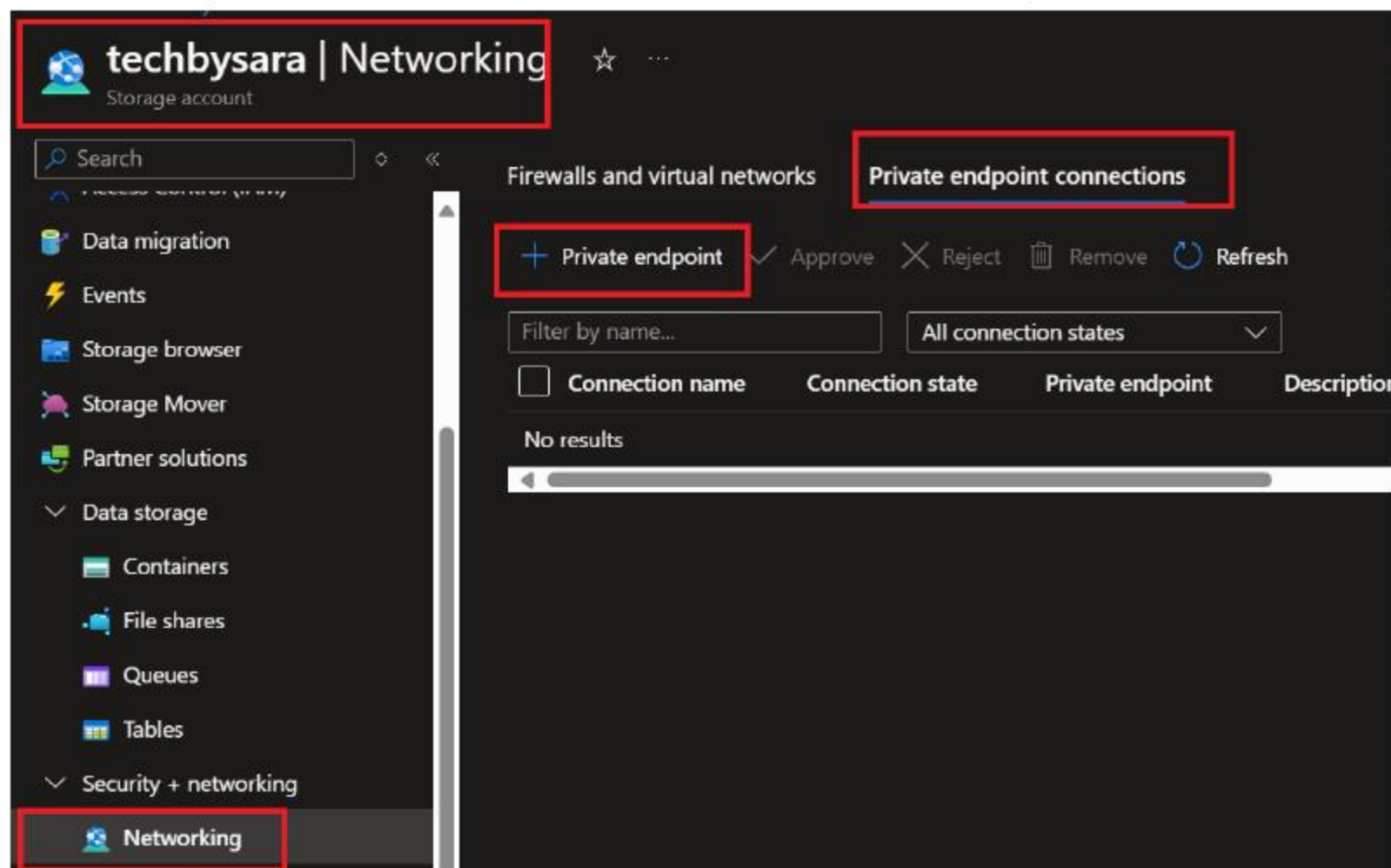


Successfully disabled public network access to the storage account.

Step 5: Create a Private Endpoint

An Azure private endpoint acts as a network interface inside your virtual network (VNet). When configured for a storage account, it establishes secure, private connectivity for clients on that network by assigning an IP address directly from your virtual network subnet range.

1. In your Storage account page, go to **Security + networking** > **Networking** > **Private endpoint connections**, then select **+ Private endpoint**.



Basics tab:

2. **Subscription** > Select your Azure subscription (for example, **ABCOFCLOUD**).
3. **Resource group** > Select your resource group (for example, **Sarah1-RG**).
4. **Name** > Enter a name for your private endpoint (for example, **techbysara-Endpoint**).
5. **Region** > Select the same region as your virtual network (for example, **East US**).

Create a private endpoint

1 Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Network Interface Name *

Region *

< Previous **Next : Resource >**

6. Click **Next: Resource** > Under **Target sub-resource**, select **file**.

Create a private endpoint

✓ Basics 1 Resource 2 Virtual Network 3 DNS 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription

Resource type

Resource

Target sub-resource *

< Previous **Next : Virtual Network >**

- Click **Next: Virtual Network** > Select your target virtual network and subnet (for example, **TechbysarVNET | Sarah1-RG** and **Finance-Subnet**).
- Private IP configuration** > Select **Dynamically allocate IP address**.

Create a private endpoint

✓ Basics

✓ Resource

3 Virtual Network

4 DNS

5 Tags

6 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network

TechbysaraVNET (Sarah1-RG)

Subnet

Finance-Subnet

Network policy for private endpoints

Disabled [\(edit\)](#)

Private IP configuration

☒ Dynamically allocate IP address
 ☐ Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

+ Create

Application security group

< Previous

Next : DNS >

- Click **Next: DNS** to leave Azure automatic DNS configuration enabled, select **Review + create**, and click **Create**.

Create a private endpoint

✓ Basics

✓ Resource

✓ Virtual Network

4 DNS

5 Tags

6 Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-file-core-wind...	ABCOFCLLOUD	Sarah1-RG	(new) privatelink.file.core....

< Previous

Next : Tags >

The screenshot displays the Azure portal interface for a private endpoint named "Techbysara-Endpoint". The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Monitoring, Automation, and Help. The main area shows the "Essentials" tab with the following configuration details:

Property	Value
Resource group (move)	Sarah1-RG
Location	East US
Subscription (move)	ABCOFCLOUD
Subscription ID	
Provisioning state	Succeeded
Virtual network/subnet	TechbysaraVNET/Finance-Subnet
Network interface	Techbysara-Endpoint-nic
Private link resource	techbysara
Target sub-resource	file
Connection status	Approved
Request/Response	Auto-Approved
Tags (edit)	Add tags

Successfully created the Techbysara-Endpoint private endpoint.

Confirm Virtual Network Link

After creating a private endpoint, verify that the DNS configuration is properly linked. Once linked, virtual machines within the virtual network can seamlessly reach the private DNS zone.

In your Private endpoint page, select **DNS configuration** to review settings.

The screenshot displays the Azure portal interface for the "Techbysara-Endpoint | DNS configuration" page. The left sidebar shows the "DNS configuration" option selected under the "Settings" category. The main area shows the "Private DNS integration" section with the following configuration details:

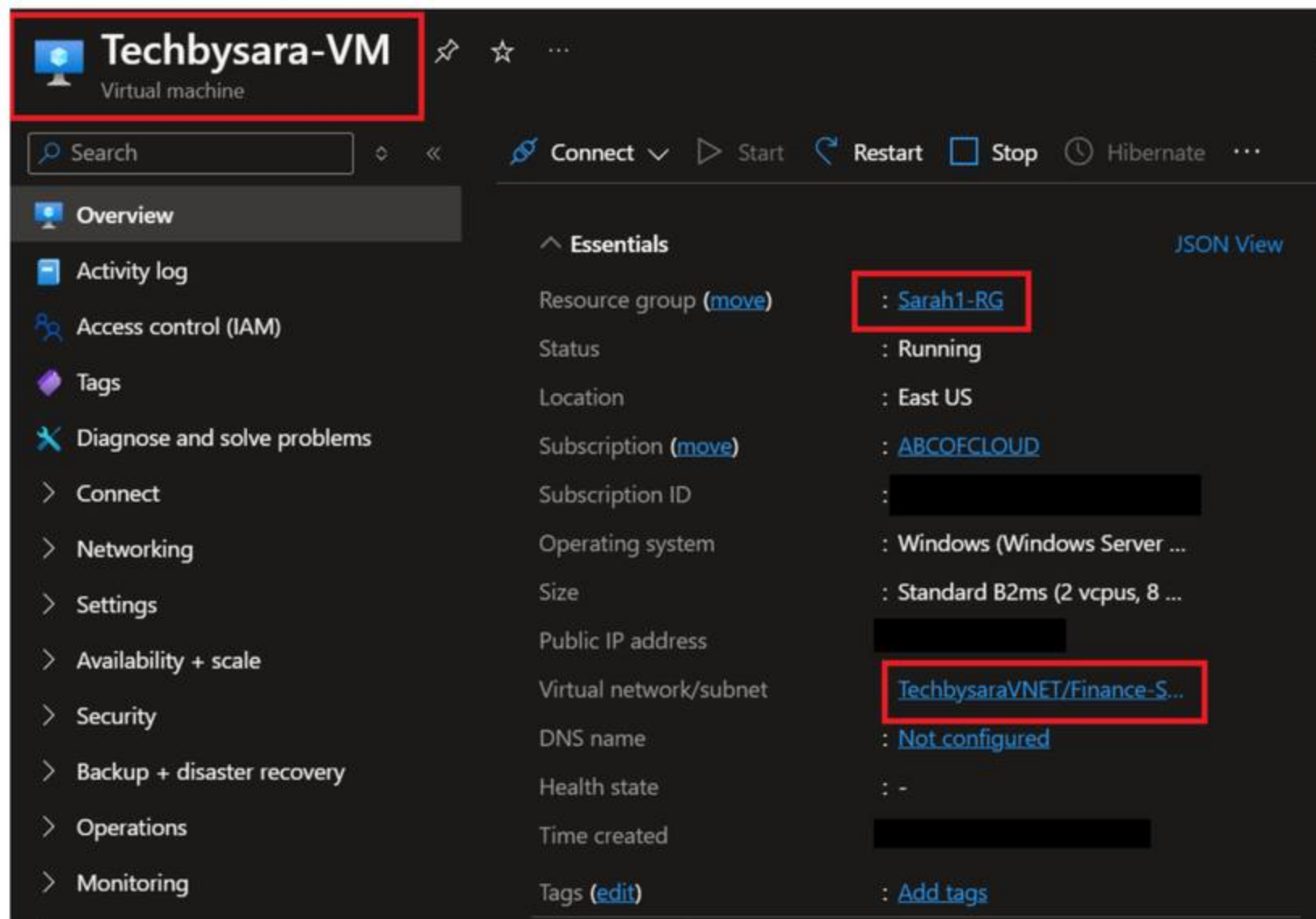
Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
privatelink-file-core-windows-net			ABCOFCLOUD	privatelink.file.core.windows.net	default
	techbysara.privatelink.file.core.windows...	192.168.70.68			

DNS configuration confirmed.

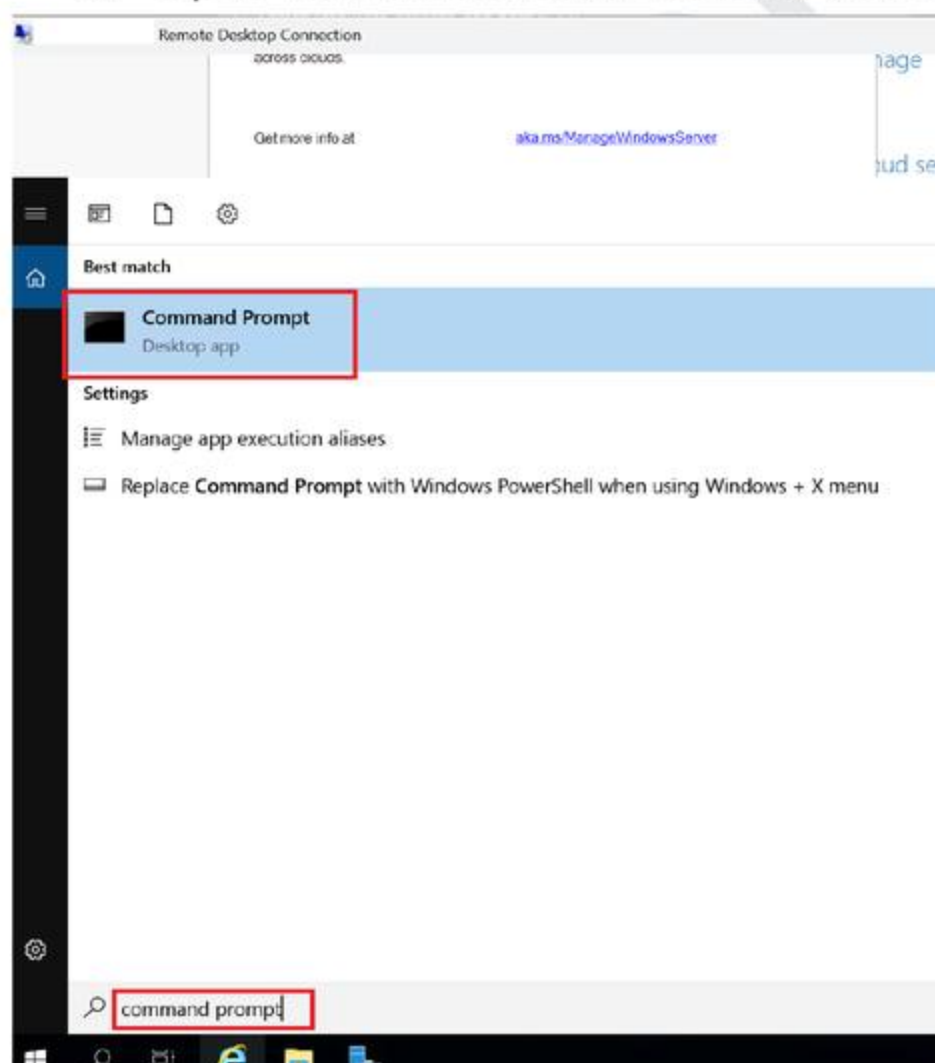
Step 6: Verify Connection from Virtual Machine

Follow these steps to confirm that a virtual machine in the same virtual network connects to the Azure Storage account via the private endpoint.

1. Log in to your virtual machine.



2. Open the Start menu, search for **Command Prompt**, and launch it.



3. Type **ipconfig** and press Enter to check network adapter details.

4. Run the nslookup command using your private link URL (for example, **nslookup techbysara.privatelink.file.core.windows.net**).

If the VM is properly connected via the private endpoint, Command Prompt will display the internal IP address assigned to the private endpoint.

```
- Remote Desktop Connection

Server Manager ▸ Dashboard

WELCOME TO SERVER MANAGER

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.6054]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\TechbysaraVM>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : z3hwr1f02owe5i1elvoimuqwl1a.bx.internal.cloudapp.net
    Link-local IPv6 Address . . . . . : fe80::46d:2cf0:a8de:1e5e%6
    IPv4 Address. . . . . : 192.168.70.69
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 192.168.70.65

C:\Users\TechbysaraVM>nslookup techbysara.privatelink.file.core.windows.net
Server:      Unknown
Address: 168.63.129.16

Non-authoritative answer:
Name:   techbysara.privatelink.file.core.windows.net
Address: 192.168.70.68

C:\Users\TechbysaraVM>
```