



AZURE FILE SHARE USIGN VIRTUAL MACHINE

Login to your Azure Portal,

👉 Step 1: Create a storage account (You can either create a new storage account or can use an existing account).

The screenshot shows the Azure Storage accounts page. On the left, there's a sidebar with various service links, and 'Storage accounts' is highlighted with a red box. In the main area, there's a 'Create' button also highlighted with a red box. Below it, there's a section for 'Free training from Microsoft' and a message stating 'No virtual machines to display'.

👉 Step 2: Once your storage account is ready to use, look for File shares. Create a new file share.

Home > demoonstorage_1692210452815 | Overview > demoonstorage

demoonstorage | File shares

Storage account

Search + File share Refresh

File share settings

Active Directory (SMB): Not configured Default share-level permissions: Disabled Soft delete: 7 days Maximum capacity: 5 TiB

Security: Maximum compatibility

Search file shares by prefix (case-sensitive) Show deleted shares

Name	Modified	Tier	Quota
You don't have any file shares yet. Click '+ File share' to get started.			

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage browser Storage Mover

Data storage

Containers File shares **Queues** Tables

Security + networking

Networking

- Enter the name and select the access tier to hot (frequently accessing)
- Click on Review + Create

Home > demoonstorage_1692210452815 | Overview > demoonstorage | File shares >

New file share

... X

Basics Backup Review + create

Name * Tier *

Performance

Maximum IO/s Maximum capacity Large file shares

💡 You can improve performance and maximum share capacity by enabling large file shares for this storage account. [Learn more](#)

Review + create [< Previous](#) [Next : Backup >](#) Give feedback

- When it is done, click on browse & upload some temporary files.

Home > demoonstorage_1692210452815 | Overview > demoonstorage | File shares > New file share >

filesharedemo SMB File share

Search Connect Upload Refresh Add directory Delete share Change tier Edit quota Give feedback

Overview Diagnose and solve problems Access Control (IAM) **Browse** Operations Snapshots Backup

Enable Backup for file share "filesharedemo" to protect your data. [Learn more](#)

Essentials

Storage account	: demoonstorage	Share URL	: https://demoonstorage.file.core.windows.net/filesharedemo
Resource group (move)	: Practice	Redundancy	: Geo-redundant storage (GRS)
Location	: Central India	Configuration modified	: 8/17/2023, 12:00:58 AM
Primary/Secondary location	: Primary: Central India, Secondary: South India		
Subscription (move)	: Azure subscription 1		
Subscription ID	: f55b27c1-cfe0-448c-9ca5-8454eecfeb4e		

Properties Capabilities (2) Tutorials

Size

Maximum capacity	: 5 TiB
Used capacity	: 0 B
Tier	: Hot

Feature status

Soft delete	: 7 days
Large file shares	: Disabled

Performance

Maximum IO/s	: 1000
--------------	--------

Active Directory

Directory service	: Not configured
Domain	: -

JSON View

Home > demoonstorage_1692210452815 | Overview > demoonstorage | File shares > New file share > filesharedemo

filesharedemo | Browse SMB File share

Search Connect **Upload** Add directory Refresh Delete share

Authentication method: Access key (Switch to Azure AD User Account)

Search files by prefix

Name: No files found.

Upload files

1 file(s) selected: 3144120.png

Drag and drop files here or [Browse for files](#)

Overwrite if files already exist

Upload

- After the Files are Uploaded, click on connect.

💡 **Step 3:** For connecting with our file share storage, we will need a virtual machine. So, lets create a Windows VM.

The screenshot shows the Azure portal interface for a virtual machine named 'demofileshare'. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking selected), Connect, Windows Admin Center, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Availability + scaling, and Configuration. The main content area displays the 'Essentials' section with details such as Resource group (Practice), Status (Running), Location (Central India), Subscription ID (f55b27c1-cfe0-448c-9ca5-8454eefeb4e), and Tags (edit). Below this is a 'Properties' tab with tabs for Virtual machine (selected) and Networking. A JSON View link is located in the top right corner.

- Go to the Networking tab and Add an inbound rule, Allowing port 445 (for file share storage).

The screenshot shows the 'Networking' tab for the 'demofileshare' virtual machine. The left sidebar is identical to the previous screenshot. The main content area shows a table of network security group rules. A red box highlights the 'Add inbound port rule' button at the top right. The table lists rules for RDP (port 3389), HTTPS (port 443), HTTP (port 80), AllowAnyCustom445Inbound (port 445), AllowVnetInBound (Any port), AllowAzureLoadBalancerInBound (Any port), and DenyAllInBound (Any port). Rule 320 (HTTPS) is also highlighted with a red box. A 'Need help?' section at the bottom provides links to understand Azure load balancing, quickstart guides for creating a public load balancer and using Application Gateway, and a configuration link.

- Now, connect with your created Virtual Machine.

Step 4: Go Back to your File Share Overview and click on Connect.

Connect

filesharedemo

Hide Script

```
$connectTestResult = Test-NetConnection -ComputerName demoonstorage.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:demoonstorage.file.core.windows.net" /user:"localhost\demoonstorage" /pass:"VPYs9pV6KZD84PwDGg3oAH42ldBSutf4RYBURg7GQpdCwFADj1MJQg662DJK7tjgx9ltxd/K+AStEq9jvg="""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\\demoonstorage.file.core.windows.net\filesharedemo" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
}
```

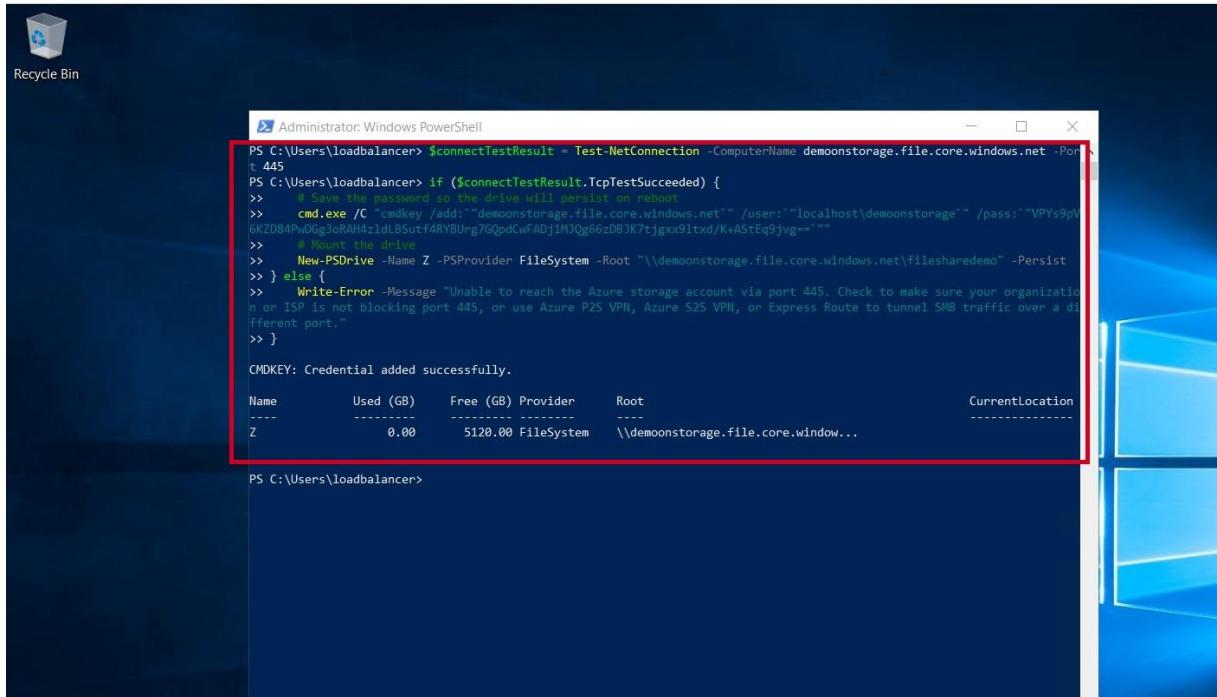
This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure Point-to-Site (P2S) VPN, Azure Site-to-Site (S2S) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.

Note: The script will only work on Windows Server 2012 and above.

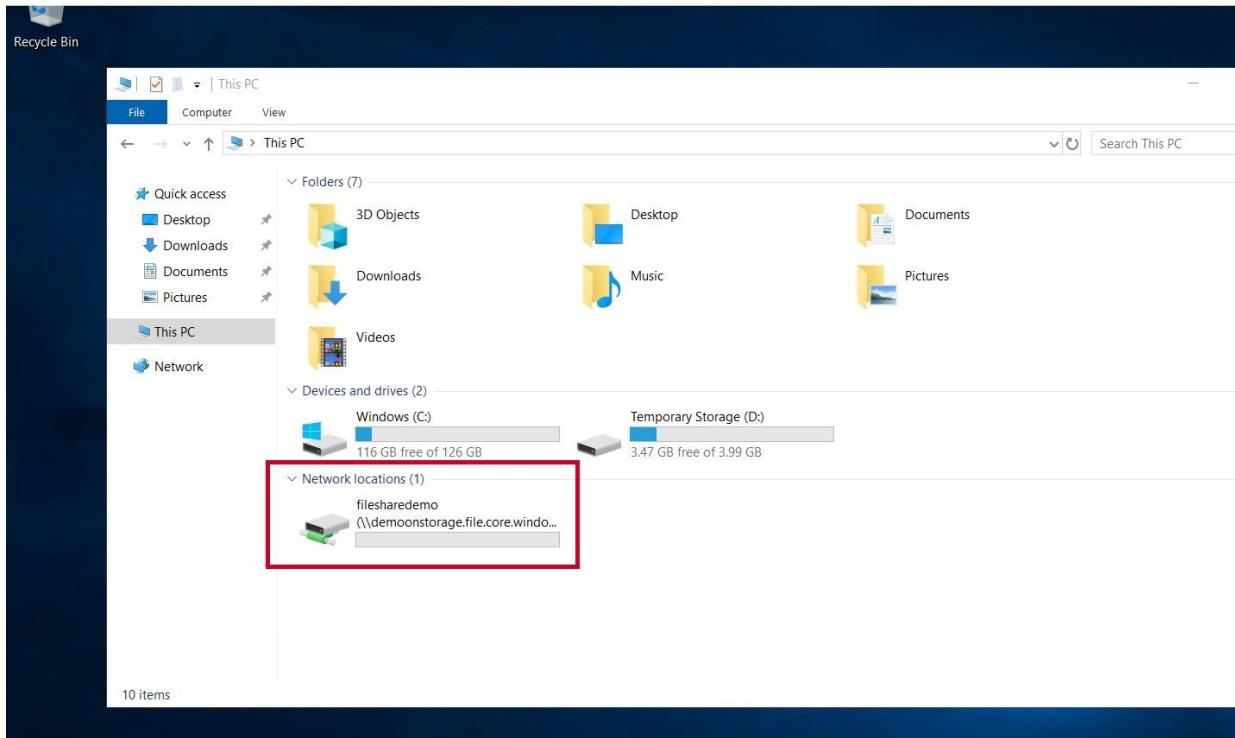
Learn how to circumvent the port 445 problem (VPN)

- Select the Windows option and Copy the Given Script.

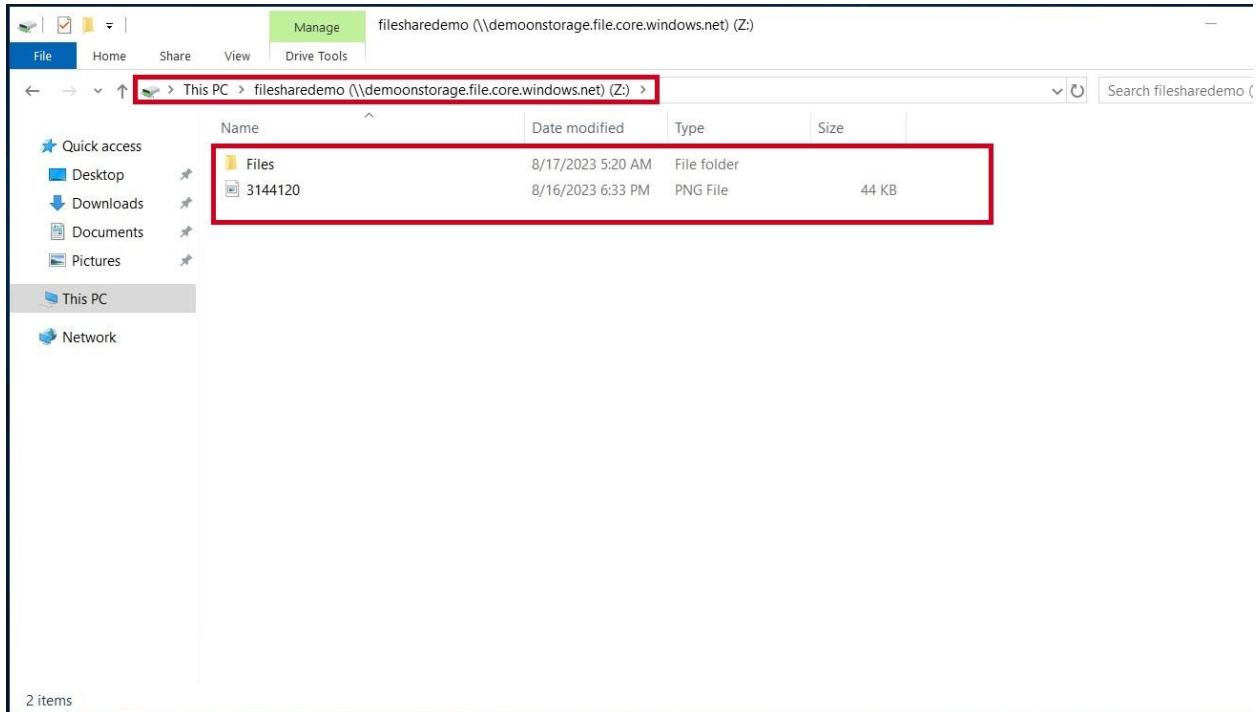
Step 5: Come to your running VM, search and open PowerShell, Copy the script and run it on PowerShell.



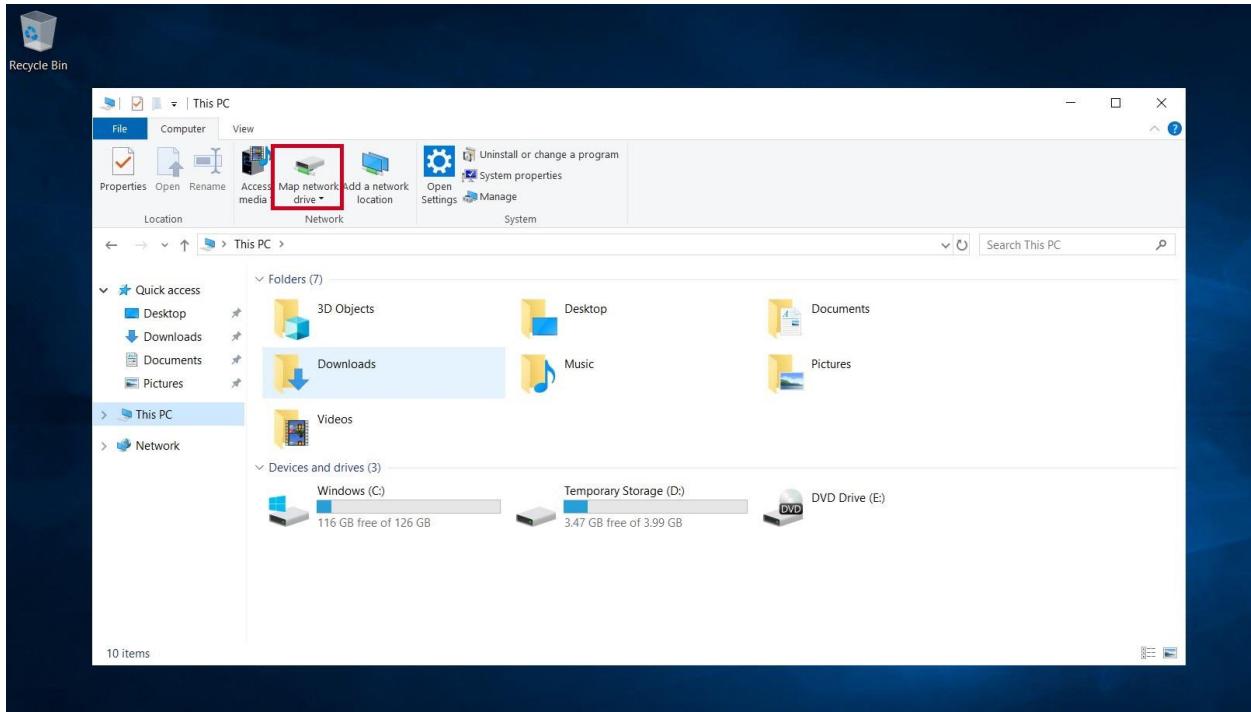
- You can see the Credentials have been successfully added.
- Go to this pc and you'll see New Network Location has been Added, that is your File Share Storage .



- Open the Newly Created Drive, here you can see the Uploaded files.



- ❖ Alternate Way to Connect: -
- Open this PC, Click on Map Network Device.



- Select the following URL and paste.

Microsoft Azure Search resources, services, and docs (G+/-) anujpal48916@gmail.co... DEFAULT DIRECTORY (ANUJPALA...)

Home > filesharedemo

filesharedemo | Browse ...

SMB File share

Search

Connect Upload + Add directory Refresh Delete share

Authentication method: Access key (Switch to Azure AD User Account)

Search files by prefix

Name

Files

3144120.png

Connect

filesharedemo

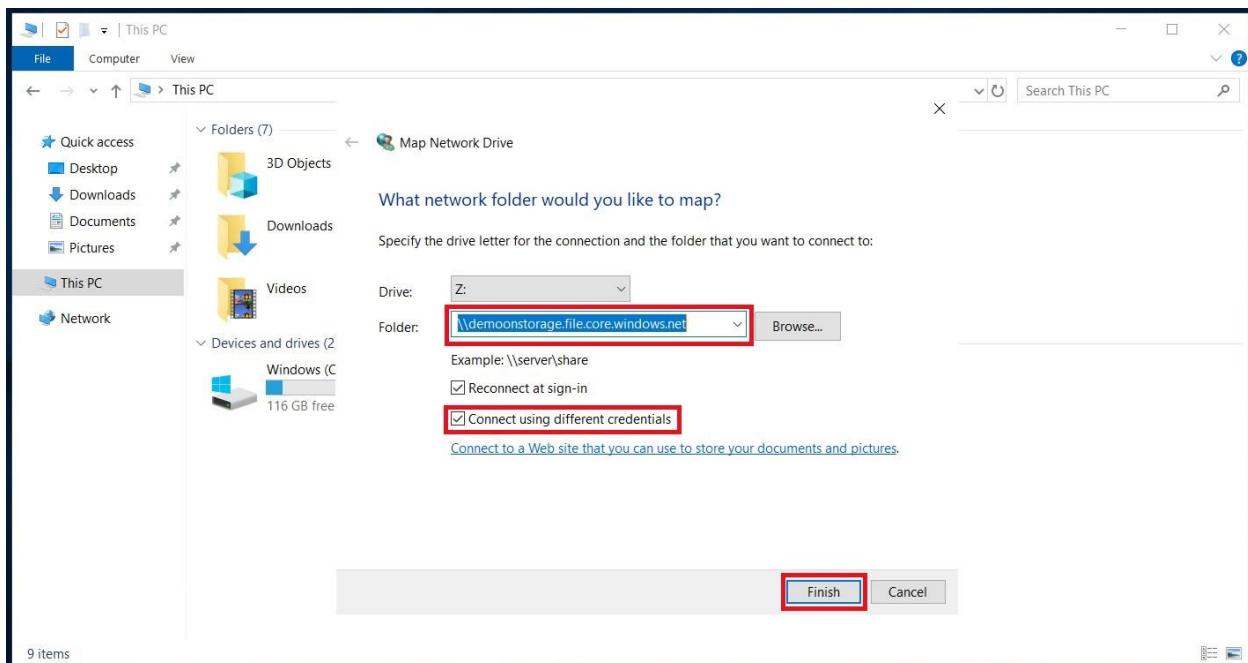
Hide Script

```
$connectTestResult = Test-NetConnection -ComputerName demoonstorage.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:"demoonstorage.file.core.windows.net" /user:[localhost\demoonstorage] $userId"
    /pass:"$PVY9pV6KZD84PwDG3oRAH4zIdLBSut4RYBurg/GQpdCwFADj1M1Qg66zD
    BJK7tjgx9ltxd/K+AStEq9jvg==" password
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root \\demoonstorage.file.core.windows.net\filesharedemo" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445.
    Check to make sure your organization or ISP is not blocking port 445, or use Azure
    P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different
    port."
}
```

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure Point-to-Site (P2S) VPN, Azure Site-to-Site (S2S) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.

Note: The script will only work on Windows Server 2012 and above.

Learn how to circumvent the port 445 problem (VPN)



- Select the Checkbox and Click on Finish.
- Enter the Network Credentials and Click on OK.



- The New Network Location has been Added Successfully.

