

Mount a file share on Windows – Demo

We're going to create a file share in Azure Storage account and mount it with a Windows PC/Server in this demo by using script and "network map" and UNC path options.

Prerequisites: TCP 445 should be allowed for outbound traffic.

Troubleshooting for connectivity issues: <https://learn.microsoft.com/en-us/azure/storage/files/files-troubleshoot-smb-connectivity?tabs=windows#cause-1-port-445-is-blocked>

Mount using "Script" option.

1. Login to your azure portal and create a storage account "csg100320021f90b5f6"
2. Create a file share as shown below and upload some files for testing purposes.

The screenshot displays the Azure portal interface. The top navigation bar shows the path: Home > Storage accounts > csg100320021f90b5f6 | File shares > cs-cloudzdevops-outlook-com-100320021f90b5f6 > csg100320021f90b5f6. The main content area is titled "csg100320021f90b5f6 | File shares" and includes a search bar, a "+ File share" button, and a "Refresh" button. Below this, the "File share settings" section shows: Active Directory: Not configured, Default share-level permissions: Disabled, Soft delete: 7 days, Maximum capacity: 5 TiB, and Security: Maximum compatibility. A table lists the file shares, with one entry: cs-cloudzdevops-outlook-com-100320021f90b5f6, modified on 3/6/2023 at 8:34:26 PM, with a tier of Transaction optimized and a quota of 6 GiB. The bottom section, titled "cs-cloudzdevops-outlook-com-100320021f90b5f6 | Browse", shows the "SMB File share" view. It includes a search bar, a "Connect" button, and an "Upload" button. A table lists the files in the share: .cloudconsole (Directory) and Networking.docx (File).

Home > Storage accounts > csg100320021f90b5f6 | File shares > cs-cloudzdevops-outlook-com-100320021f90b5f6 > csg100320021f90b5f6

csg100320021f90b5f6 | File shares

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

Name	Modified	Tier	Quota
cs-cloudzdevops-outlook-com-100320021f90b5f6	3/6/2023, 8:34:26 PM	Transaction optimized	6 GiB

Home > Storage accounts > csg100320021f90b5f6 | File shares > cs-cloudzdevops-outlook-com-100320021f90b5f6 > csg100320021f90b5f6 | F

cs-cloudzdevops-outlook-com-100320021f90b5f6 | Browse

Search files by prefix

Name	Type
.cloudconsole	Directory
Networking.docx	File

3. Click on "Connect"
4. Select your OS, Drive and Authentication Method as "Storage account key" and then click on "Show Script"

Home > Storage accounts > csg100320021f90b5f6 | File shares > cs-cloudzdevops-outlook-com-100320021f90b5f6 > c

cs-cloudzdevops-outlook-com-100320021f90b5f6 | Browse

SMB File share

Search

Connect Upload Add directory Refresh Delete share

Search files by prefix

Name
.cloudconsole
Networking.docx

Overview

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Snapshots

Backup

Connect

cs-cloudzdevops-outlook-com-100320021f90b5f6

Windows Linux macOS

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

Drive letter

Z

Authentication method

☐ Active Directory

☒ Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory identity of the user is preferred. [Learn more](#)

Show Script

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](#)

5. You'll get a PShell script something like below.

Connect

cs-cloudzdevops-outlook-com-100320021f90b5f6

```
$connectTestResult = Test-NetConnection -ComputerName
csg100320021f90b5f6.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:"csg100320021f90b5f6.file.core.windows.net`"
/user:"localhost\csg100320021f90b5f6`"
/pass:""NYvzlr3PuD4RBHId9iBZ0N+NOYOBW5Mawz0XMVG1ZP4aF98wNgnQm2ioA
ba8ISksAXbJE1b3FfhQ+ASTl62CBQ=="`"
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\csg100320021f90b5f6.file.core.windows.net\cs-cloudzdevops-outlook-com-
100320021f90b5f6" -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 \(VPN\)](#)

```
$connectTestResult = Test-NetConnection -ComputerName
csg100320021f90b5f6.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"csg100320021f90b5f6.file.core.windows.net`"
/user:`"localhost\csg100320021f90b5f6`"
/pass:`"NYvzlr3PuD4RBHId9iBZ0N+NOYOBW5Mawz0XMVG1ZP4aF98wNgnQm2ioAba8ISksAXbJE1b3F
fhQ+ASTl62CBQ=="`"
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\csg100320021f90b5f6.file.core.windows.net\cs-cloudzdevops-outlook-com-
100320021f90b5f6" -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."
}

```

- If you run this script from your local, ensure outbound TCP port 445 is allowed. Most of the ISP providers do not allow and same happened for you. This you can test by running below cmd

Test-NetConnection -Port 445 -ComputerName <storageaccountname>.file.core.windows.net

```

PS D:\Data\Pers\MyBuz\Trainer\Materials\Azure\scripts> Test-NetConnection -Port 445 -ComputerName csg100320021f90b5f6.file.core.windows.net
WARNING: TCP connect to (52.239.202.8 : 445) failed
WARNING: Ping to 52.239.202.8 failed with status: TimedOut

ComputerName      : csg100320021f90b5f6.file.core.windows.net
RemoteAddress     : 52.239.202.8
RemotePort        : 445
InterfaceAlias    : Wi-Fi
SourceAddress     : 10.0.0.208
PingSucceeded     : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False

```

- You should get True for “TcpTestSucceeded” and then only your script will run successfully and amount the azure file share. with TcpTestSucceeded is false, you’ll get error something like below.

```

PS D:\Data\Pers\MyBuz\Trainer\Materials\Azure\scripts> .\CheckIfSMBAllowed.ps1
WARNING: TCP connect to (52.239.202.8 : 445) failed
WARNING: Ping to 52.239.202.8 failed with status: TimedOut
D:\Data\Pers\MyBuz\Trainer\Materials\Azure\scripts\CheckIfSMBAllowed.ps1 : 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.
At line:1 char:1
+ .\CheckIfSMBAllowed.ps1
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,CheckIfSMBAllowed.ps1

```

- In this case, you can create a WIN 2012 or above version VM and run same script.

```

PS C:\Users\admin11\Documents> Test-NetConnection -Port 445 -ComputerName csg100320021f90b5f6.file.core.windows.net

ComputerName      : csg100320021f90b5f6.file.core.windows.net
RemoteAddress     : 52.239.202.8
RemotePort        : 445
InterfaceAlias    : Ethernet
SourceAddress     : 10.0.0.4
TcpTestSucceeded  : True

```

- Go ahead and run the script (step#5) from PShell ISE and you will be output as shown below.

```
Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

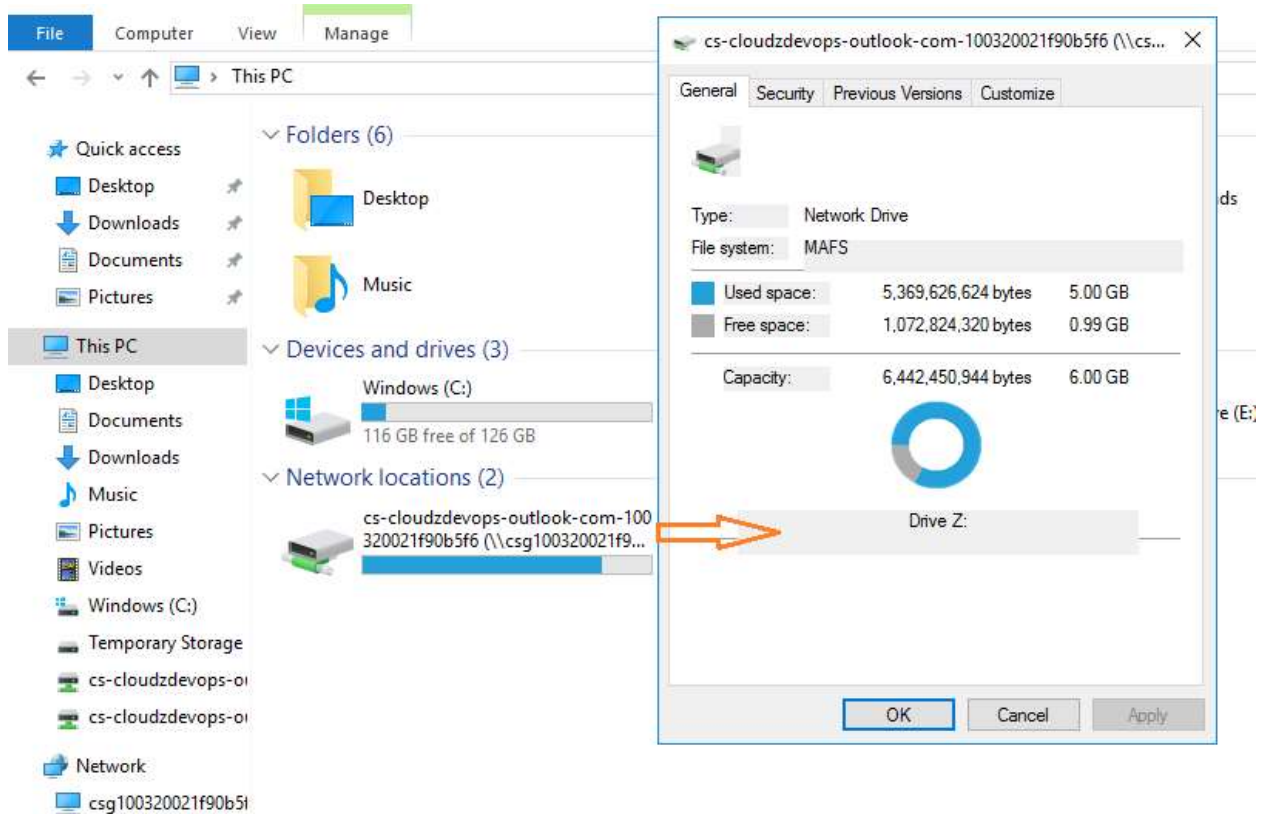
smb.ps1 X
1 $connectTestResult = Test-NetConnection -ComputerName csg100320021f90b5f6.file.core.windows.net -Port 445
2 if ($connectTestResult.TcpTestSucceeded) {
3     # Save the password so the drive will persist on reboot
4     cmd.exe /C "cmdkey /add:"csg100320021f90b5f6.file.core.windows.net" /user:"localhost\csg100320021f90b5f6" /pass:"NYvz1r3PuD4RBHid9iBZON+NQY0Bw5MawzC"
5     # Mount the drive
6     New-PSDrive -Name Y -PSProvider FileSystem -Root "\\csg100320021f90b5f6.file.core.windows.net\cs-cloudzdevops-outlook-com-100320021f90b5f6" -Persist
7 } else {
8     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 us
9 }

PS C:\Users\admin11\Documents> C:\Users\admin11\Documents\smb.ps1

CMDKEY: Credential added successfully.

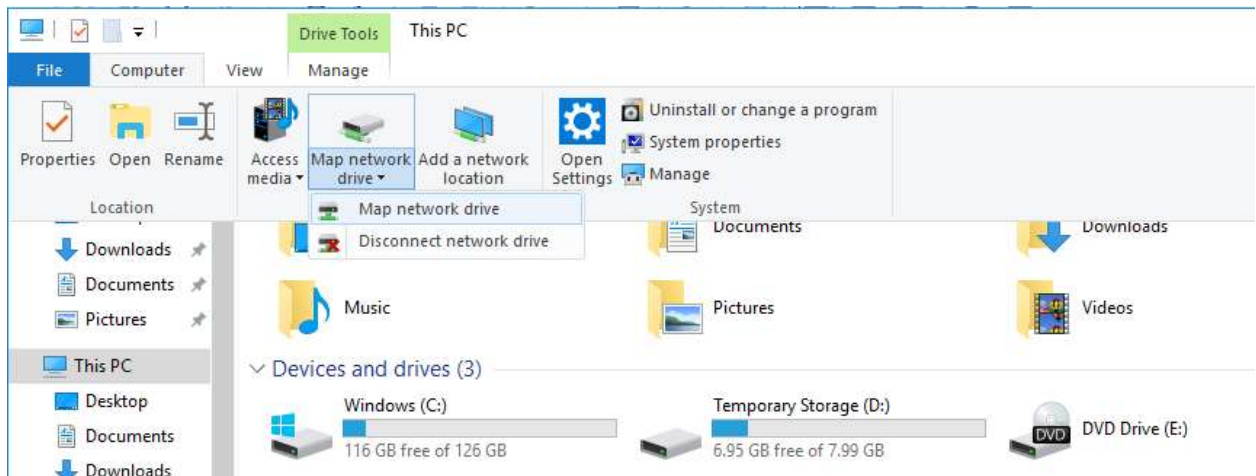
Name      Used (GB)  Free (GB) Provider      Root
-----
Y          5.00    1.00  FileSystem    \\csg100320021f90b5f6.file.core...
```

10. You can now go to your drive and notice the Azure Files share mounted.

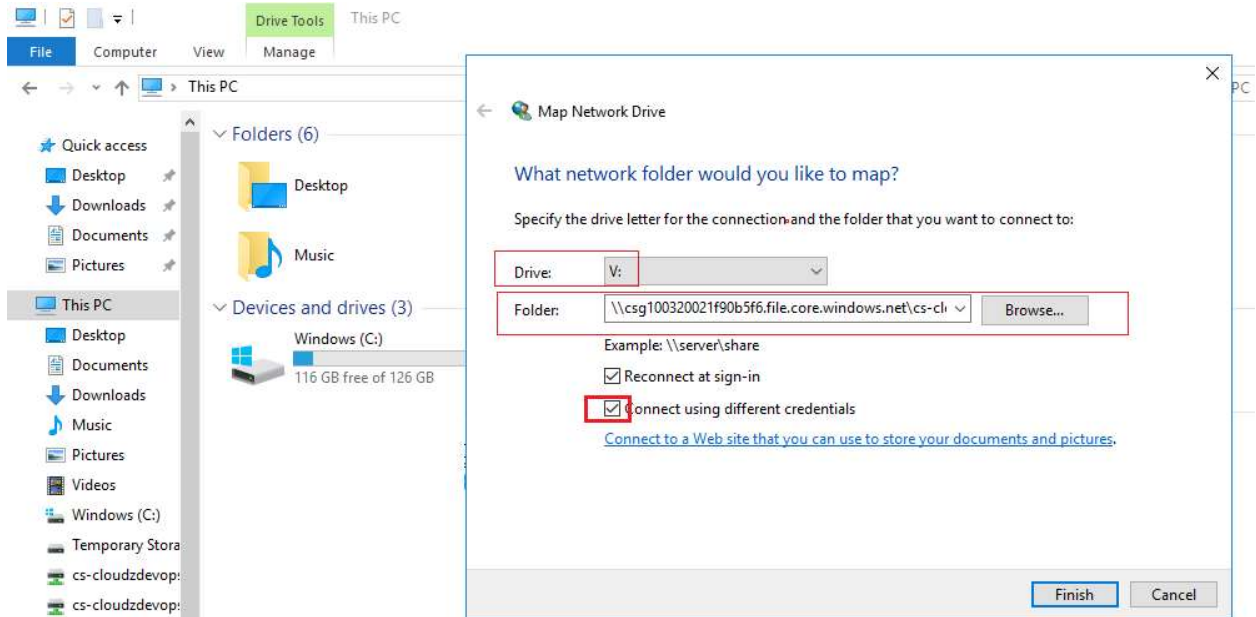


Mount using “Network Map” option

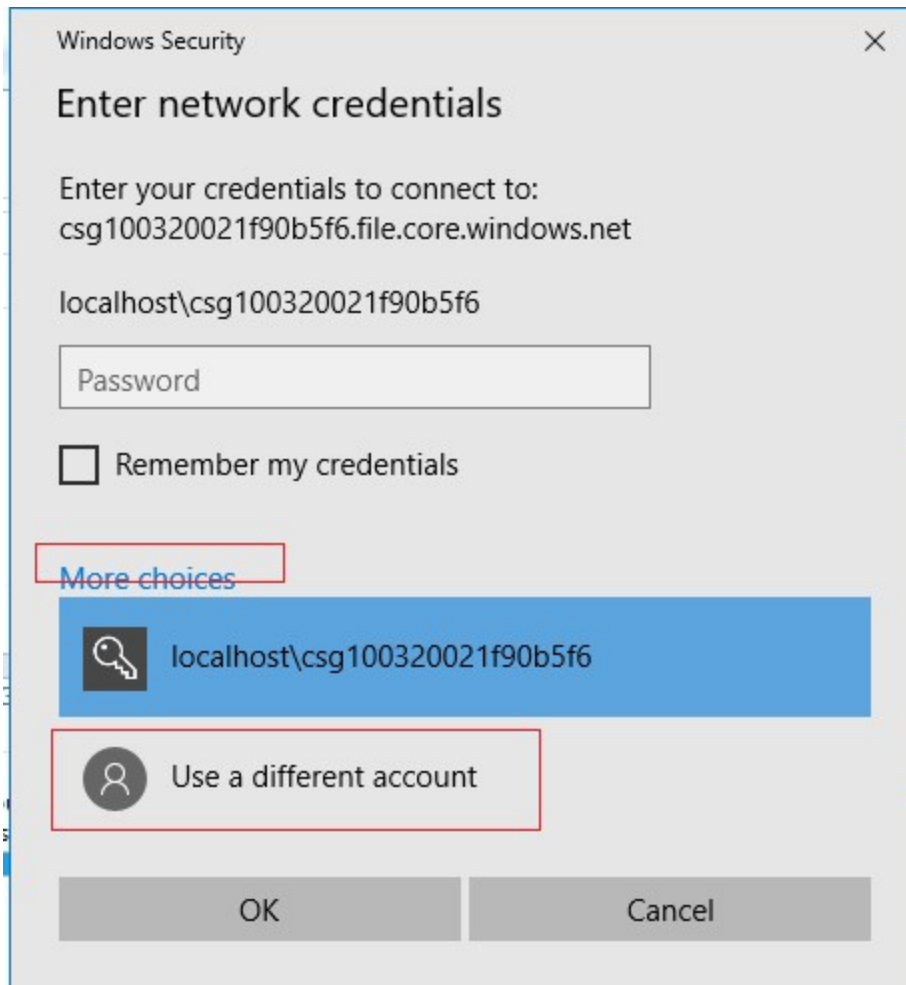
11. In the same VM where you performed above option, click “Computer” → “Map network drive” → “Map network drive”



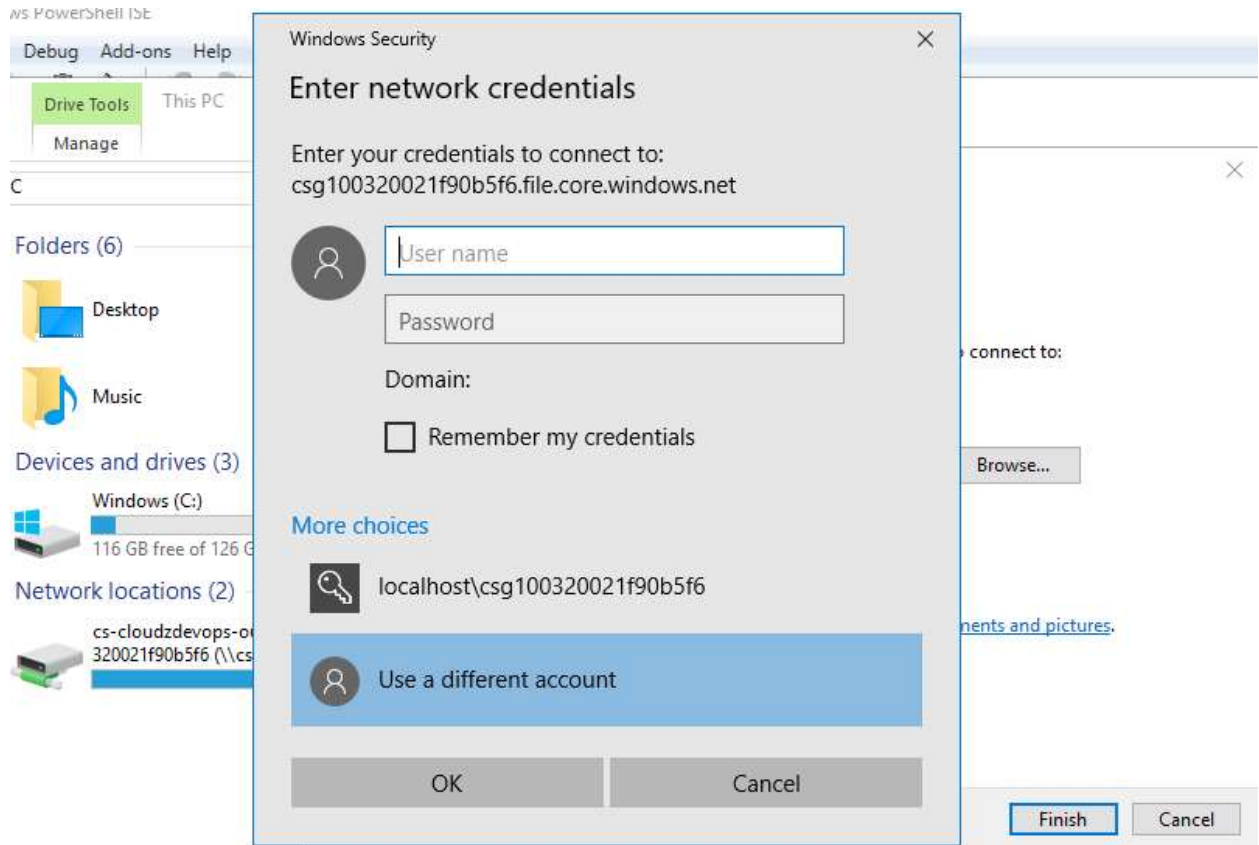
12. Select the drive letter you wanted, in Folder, copy past the storage account followed by azure file share something like “\\csg100320021f90b5f6.file.core.windows.net\cs-cloudzdevops-outlook-com-100320021f90b5f6”



13. Ensure you check “Connect using different credentials” and then click “Finish”
14. When you get prompt for credentials, click “More choices”, and select “Use a different account”



15. You will be prompted to enter "User name" and "Password". Enter you "storage account name" against "User name" and "storage account key" which you can get as shown in below step against "Password".



16. Get storage account key : go to your storage account → Access Keys → Show → Copy your storage account key

csg100320021f90b5f6 | Access keys ☆ ...

Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Data storage
 - Containers
 - File shares
 - Queues
 - Tables
- Security + networking
 - Network policies

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.
[Learn more about managing storage account access keys](#)

Storage account name
 csg100320021f90b5f6

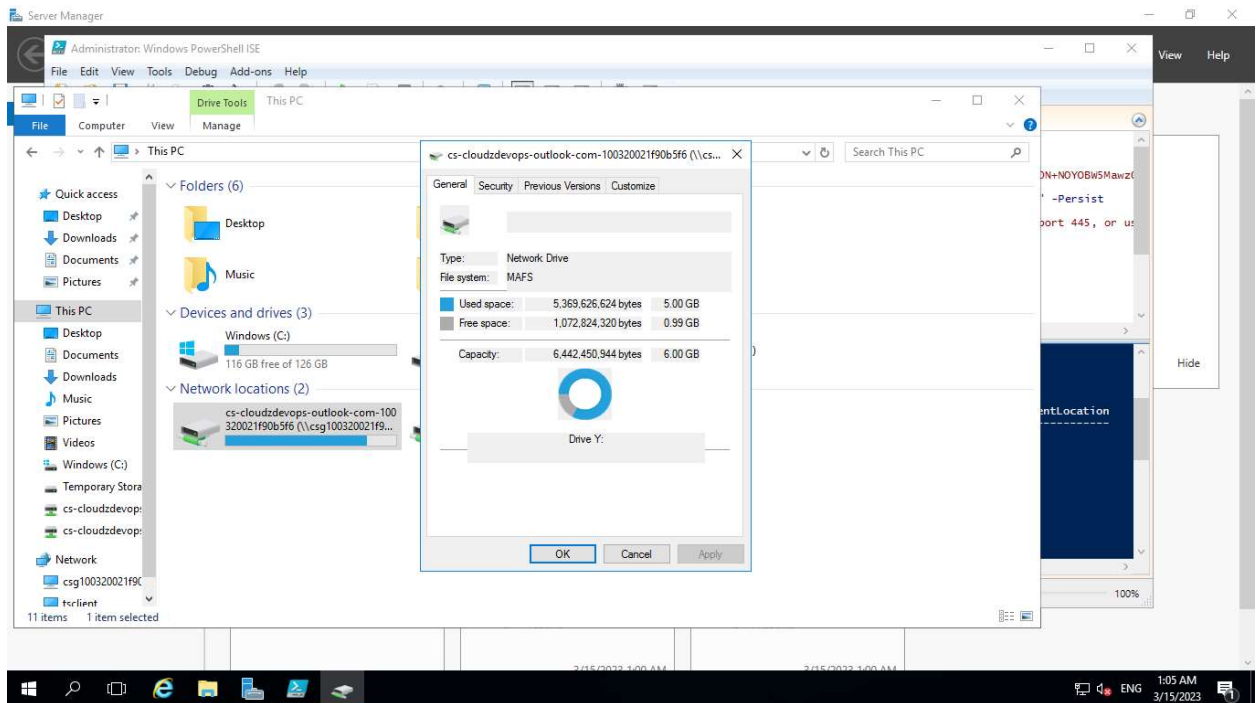
key1 🔁 Rotate key
 Last rotated: 3/6/2023 (7 days ago)
 Key
 NYvzlr3PuD4R8Hid9iBZ0N+NOYOBW5Mawz0XMVG1ZP4aF98wNgnQm2ioAba8l...

Connection string

key2 🔁 Rotate key
 Last rotated: 3/6/2023 (7 days ago)
 Key

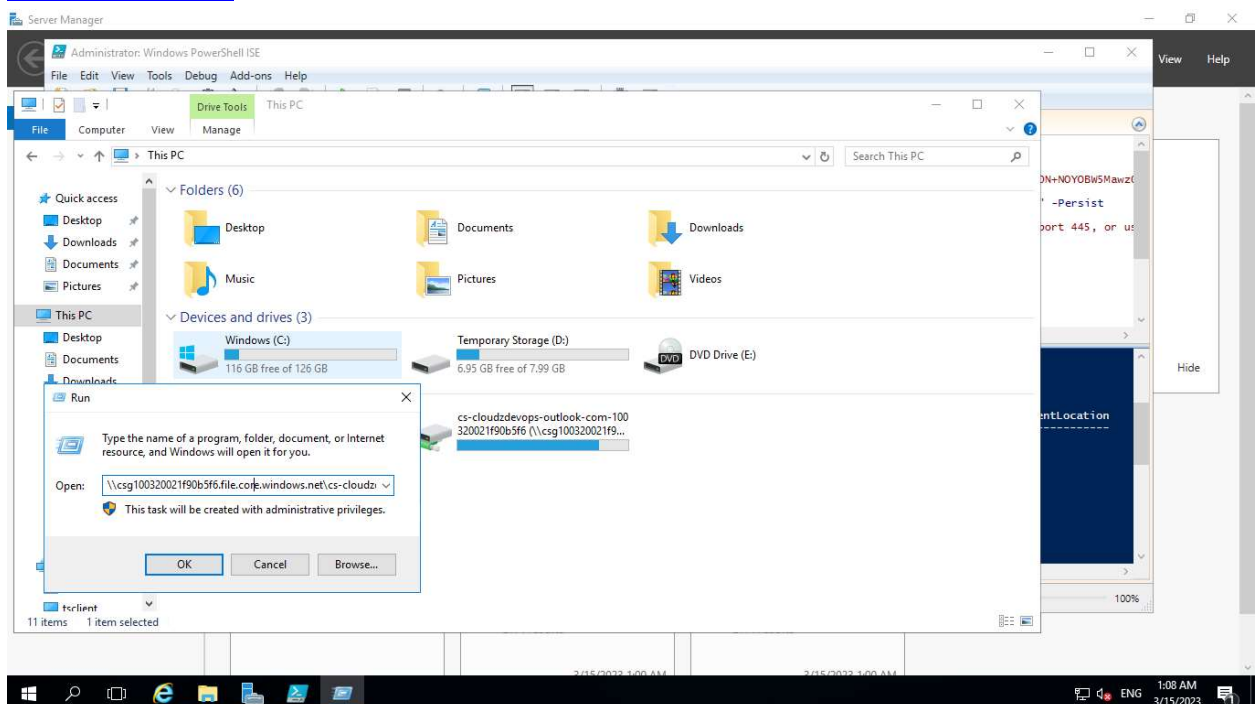
Connection string

17. Once you mount it successfully by clicking “Ok” on step # 15, your azure drive will be mounted with your Win PC/Server as shown below.

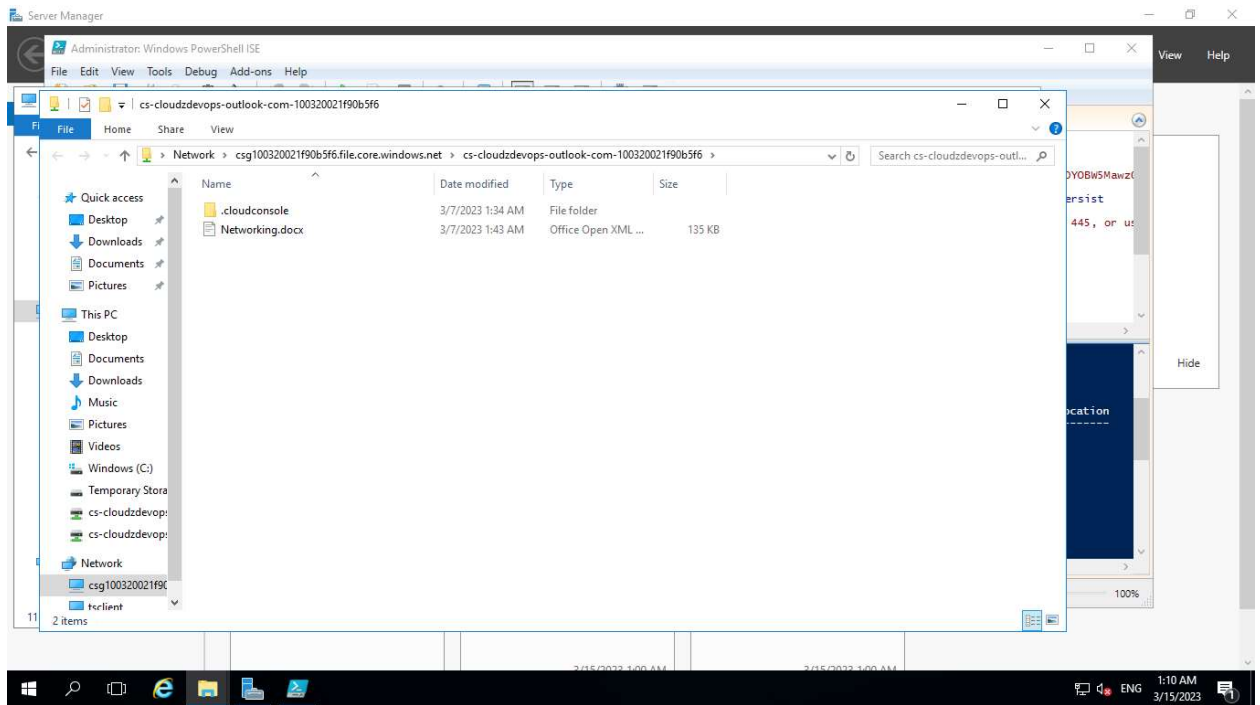


Access Azure File Share using “UNC path” option

18. In your PC / VM → Start → Run → Copy paster your storage account followed by azure file share name such as <\\csg100320021f90b5f6.file.core.windows.net\\cs-cloudzdevops-outlook-com-100320021f90b5f6>



19. Click Ok. You will be taken to Azure File Share wherein you can copy paste files from your PC/Windows.



20. If prompts for credentials, use your azure portal login user name and password.