Student Name:	**Weight: 3%**
Student ID:	**Marks: /10**

Lab: Azure File Services

Lab Objectives

In this lab, you'll explore how to create and manage Azure File services. You will:

1. Create an Azure File Share.
2. Connect to an Azure File Share.
3. Add a data disk to an Azure VM.
4. Create a cloud synchronized file server.
5. Create a file share snapshot.

Lab Requirements

- Up to date browser
- Azure account
- A selection of .pdf files that can be stored in Azure

Instructions

1. Working individually, follow the procedure below.
2. Take screenshots, as described in the *Marking Criteria* section.
3. Create a document that includes all screenshots appropriately titled and described, and then upload it to Brightspace, as indicated by your instructor.
4. Be sure to include your name and student ID in the document.

Marking Criteria

Screenshots	Marks
File share mapped to H: drive with a visible file path	/4
Healthy file synch group with cloud and server endpoints	/5
Created snapshot	/1
Total	/10

Note: This icon indicates when a screenshot is required.

Source: Flatiron.com, Freepik, Image: screenshot_983871

Procedure

One of the first uses of computer networks was to share files, and file sharing is still a primary focus of industry storage. For example, as an instructor, I have a home drive that allows me to store files in the data center and access them from SAIT's network. Azure File Storage allows you to connect to file shares in the cloud using SMB and, in some regions, NFS.

- □ Read the article: Azure Blob Storage vs Azure File Storage (https://www.smikar.com/azure-blob-storage-vs-azure-file-storage/).

Part 1: Create an Azure File Share

□ If you don't already have a storage account, create one.

□ From the main page of your storage account, select **File Shares** from the blade menu and click the **+ File Share** button.

□ Give your file share a name, and then click the **Tier** drop-down.

Note the slightly different tiers for file shares versus what you saw with blob storage.

□ Select **Hot**, which is optimized for general file sharing, read the specifications for this tier and create the share.

□ Read the **File Share Settings** across the top of the screen.

□ Click the file share to go to its main page, and then upload a few .pdf files to the share.

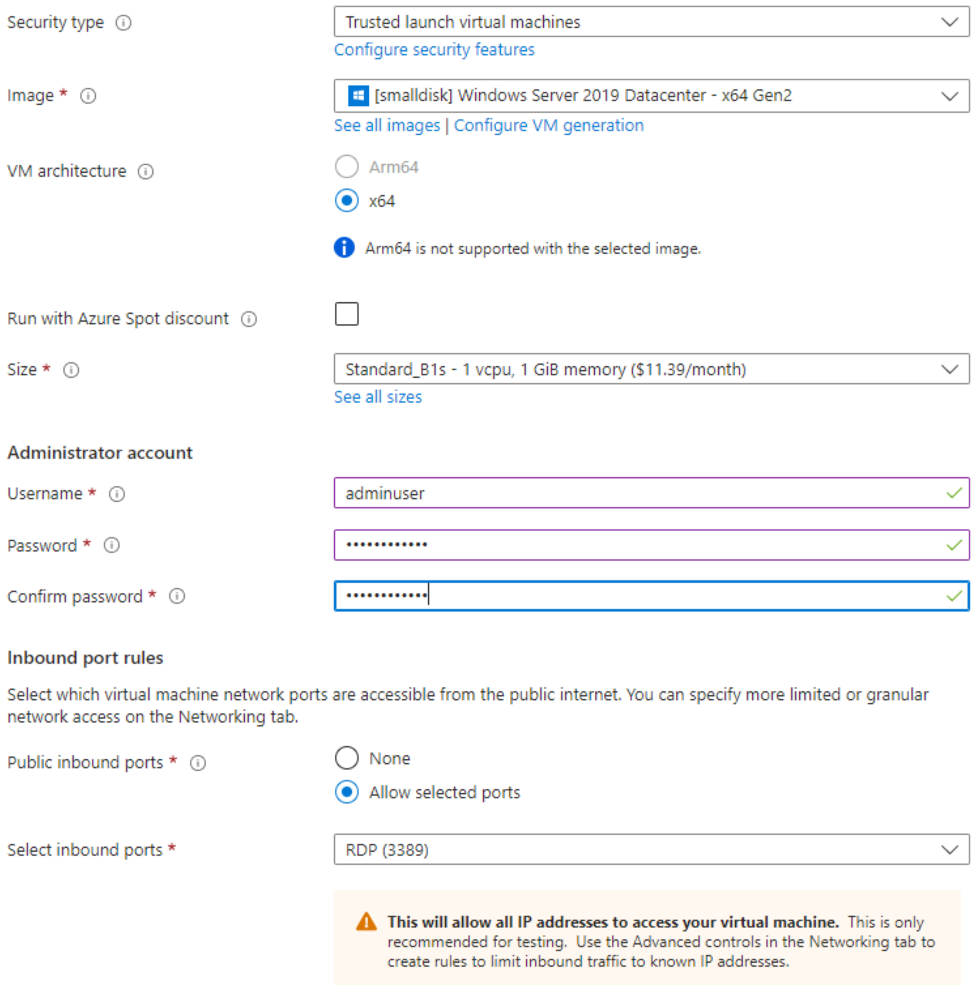
□ Click the **+ Add Directory** button and create another directory (folder) for your share.

Part 2: Connect to an Azure File Share

The file share uses the SMB protocol and most ISPs will block port 445, so it is very possible that you would be unable to connect from where you are to the file share. Networking components like VPNs can be used to circumvent this problem, but we haven't covered that unit yet, so you'll connect instead from a virtual machine in the cloud.

□ Create a small disk Windows 2019 Datacenter -x64 Gen2 virtual machine with the RDP port open.

Azure's file shares use SMB v3.x, so you need a virtual machine that can speak that protocol.



Security type ⓘ: Trusted launch virtual machines
Configure security features

Image * ⓘ: [smalldisk] Windows Server 2019 Datacenter - x64 Gen2
See all images | Configure VM generation

VM architecture ⓘ: ○ Arm64 ● x64
Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ: □

Size * ⓘ: Standard_B1s - 1 vcpu, 1 GiB memory ($11.39/month)
See all sizes

Administrator account

Username * ⓘ: adminuser

Password * ⓘ: ••••••••••••

Confirm password * ⓘ: ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ: ○ None ● Allow selected ports

Select inbound ports *: RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Connect to the new virtual machine via RDP.

□ Set the firewalls to allow SMB file and print sharing (port 445).

Note: For a reminder, see: SMB: File and printer sharing ports should be open (https://learn.microsoft.com/en-us/windows-server/storage/file-server/best-practices-analyzer/smb-open-file-sharing-ports).

□ Go to the main page for your file share and select **Connect** from the top menu.

A menu appears with options to connect from Windows, Linux or Mac.

□ Choose *Windows*.

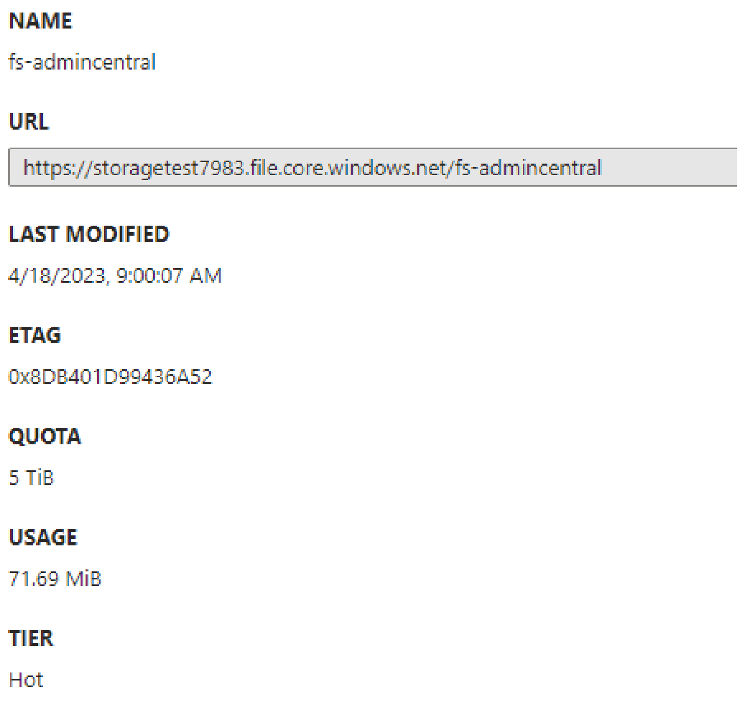
□ Select **H** as the drive letter. This is a common selection for creating a home drive.

□ For authentication, choose **Storage Account Key**.

□ Click the **Show Script** button to see a PowerShell script that you can use to connect to this file share. Browse through the script and identify the sections where it saves the password and mounts the drive.

Instead of using this file, you can use the standard UNC name.

□ In the Azure Portal, on the main page for your file share, select **Properties** from the blade menu and copy the URL.



NAME
fs-admincentral

URL
https://storagetest7983.file.core.windows.net/fs-admincentral

LAST MODIFIED
4/18/2023, 9:00:07 AM

ETAG
0x8DB401D99436A52

QUOTA
5 TiB

USAGE
71.69 MiB

TIER
Hot

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Change the URL to an UNC name.

See: File path formats on Windows systems (https://learn.microsoft.com/en-us/dotnet/standard/io/file-path-formats) if you have forgotten UNC names.

In the example above, the URL is:

`https://storagetest7983.file.core.windows.net/fs-admincentral`

So, the UNC name would be:

`\\storagetest7983.file.core.windows.net\fs-admincentral`

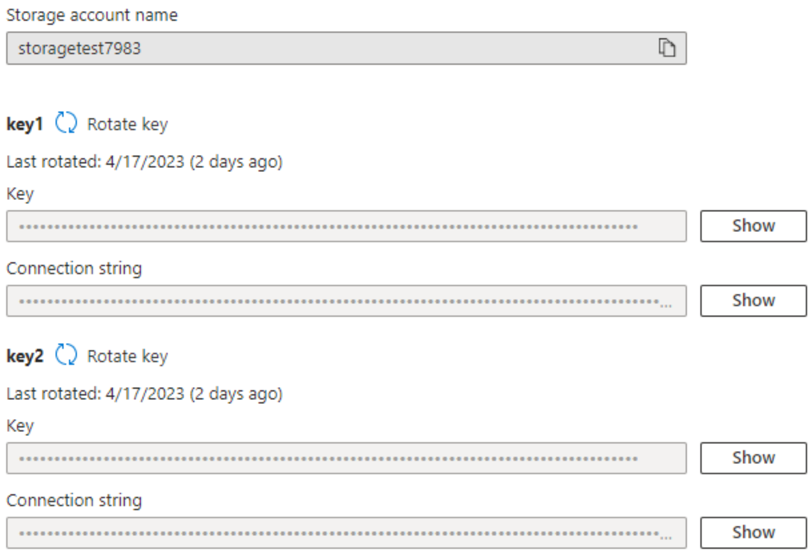
□ In the virtual machine, select the **Start** button, type **run** to bring up the *Run* box and enter your UNC name.

□ When you press Enter, it should request your credentials.

□ Go back to the file share’s main page in the Azure portal. Click the **Connect** button and look at the authentication method. It should be set to *Storage Account Key*. These will be discussed more in the security section of this course.

□ When you created the storage account, two access keys were created. Go to the main page for the storage account and select **Access Keys** from the blade menu.

□ The *Storage Account Name* is your username. Click **Show** and copy on either of the two keys and use that as the password.



Storage account name: storagetest7983

key1 Rotate key

Last rotated: 4/17/2023 (2 days ago)

Key: •• Show

Connection string: •••... Show

key2 Rotate key

Last rotated: 4/17/2023 (2 days ago)

Key: •• Show

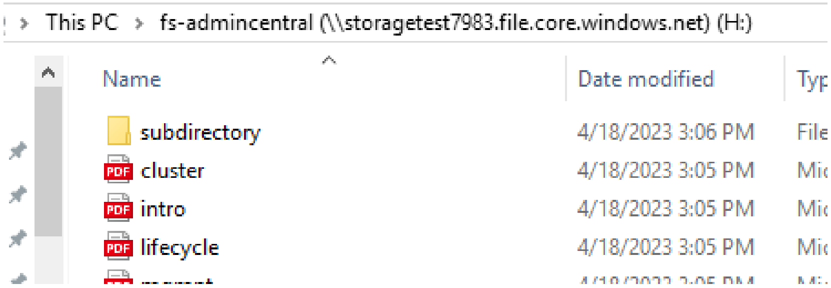
Connection string: •••... Show

© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Once you have pressed the Enter key, you should be connected to the file share.

□ Map your file share to the **H:** drive on your virtual machine.



This PC > fs-admincentral (\\storagetest7983.file.core.windows.net) (H:)

Name	Date modified	Typ
subdirectory	4/18/2023 3:06 PM	File
cluster	4/18/2023 3:05 PM	Mic
intro	4/18/2023 3:05 PM	Mic
lifecycle	4/18/2023 3:05 PM	Mic

© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Create a new document in the share and check that it shows up in the file share in the Azure portal.

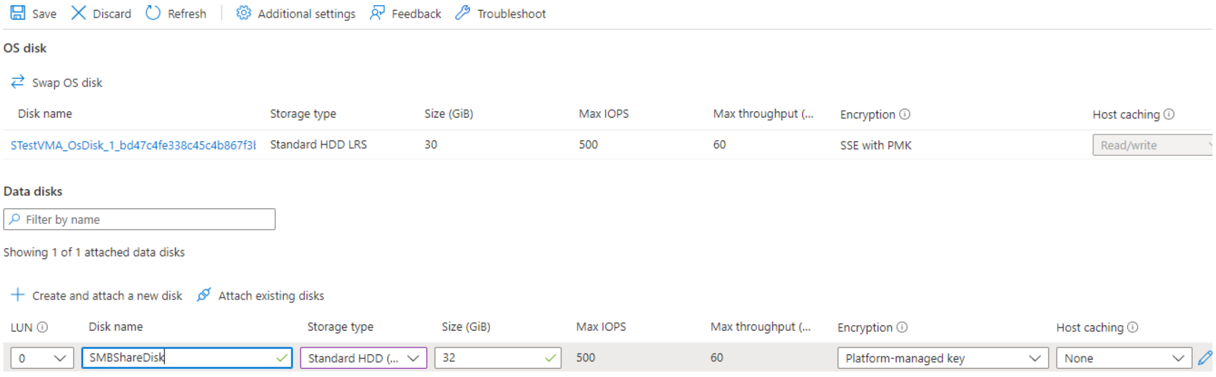
□ Disconnect the file share in your virtual machine when you are finished.

Part 3: Add a Data Disk to an Azure VM

Previously in this lab, the virtual machine you created acted as an SMB client. In this section, your virtual machine will act as an SMB file server, synchronized with Azure using the Azure File Sync service. The VM we selected has a small disk, so firstly you'll add a data disk.

□ In the Azure portal, go to the main page for the virtual machine and select **Disks** from the blade menu.

□ Click **+ Create and Attach a New Disk** in the center menu and create a disk with the options shown below.



OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption	Host caching
STestVMA_OsDisk_1_bd47c4fe338c45c4b867f3l	Standard HDD LRS	30	500	60	SSE with PMK	Read/write

Data disks

Filter by name

Showing 1 of 1 attached data disks

LUN	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption	Host caching
0	SMBShareDisk	Standard HDD (...	32	500	60	Platform-managed key	None

© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Save the disk and return to the RDP connection to your virtual machine.

□ Open the disk manager and connect and format the new disk with NTFS.

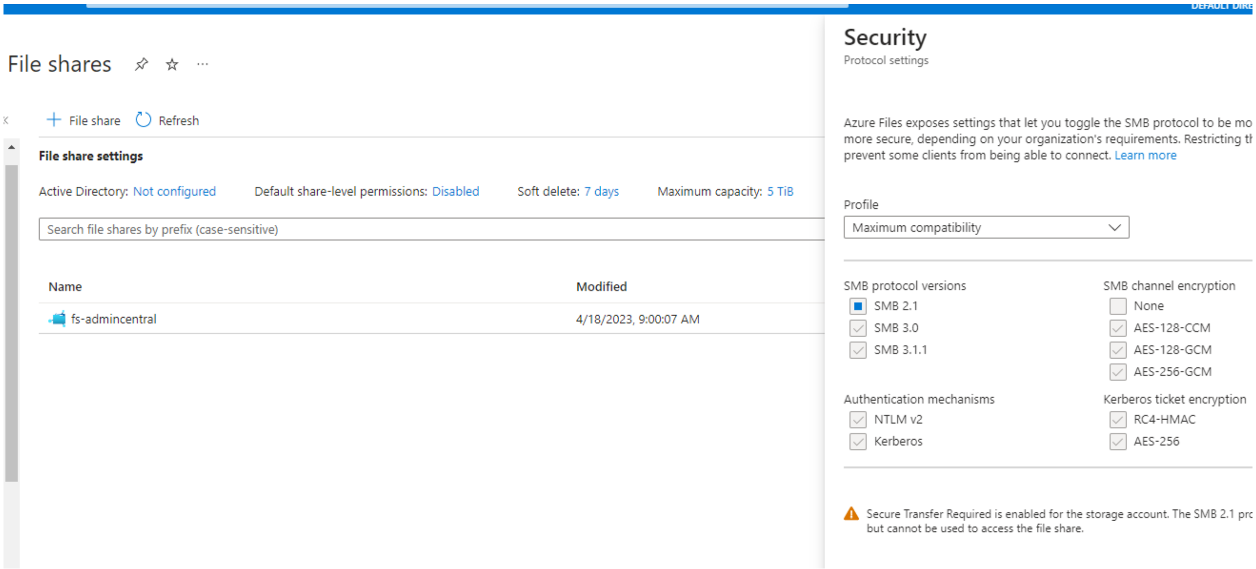
Part 4: Create a Cloud Synchronized File Server

☐ Perform the following on your Azure virtual machine:

- Disable *IE Enhanced Security Configuration* in the server manager.
- Ensure the SMB File and Print share port is open on the firewall.
- Create an SMB file share on the new disk on the server.

☐ Perform the following in the Azure portal:

- Make sure everything you create is in the same region as your file share. You can use the same resource group as well.
- Check your SMB compatibility by going to the main page of your storage account, selecting **File Shares** from the blade menu and clicking **Maximum Compatibility**.



File share settings

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

Search file shares by prefix (case-sensitive)

Name	Modified
fs-admincentral	4/18/2023, 9:00:07 AM

Security

Protocol settings

Azure Files exposes settings that let you toggle the SMB protocol to be mo
more secure, depending on your organization's requirements. Restricting th
prevent some clients from being able to connect. Learn more

Profile: Maximum compatibility

SMB protocol versions	SMB channel encryption
■ SMB 2.1	☐ None
☑ SMB 3.0	☑ AES-128-CCM
☑ SMB 3.1.1	☑ AES-128-GCM
	☑ AES-256-GCM

Authentication mechanisms	Kerberos ticket encryption
☑ NTLM v2	☑ RC4-HMAC
☑ Kerberos	☑ AES-256

⚠ Secure Transfer Required is enabled for the storage account. The SMB 2.1 prc
but cannot be used to access the file share.

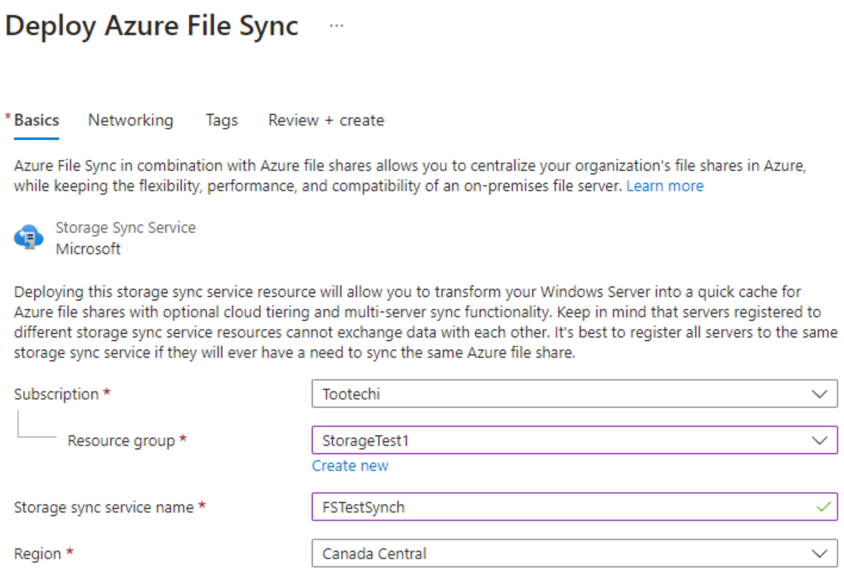
© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

- The current requirement for the File Sync service is **SMB 3.1.1** protocol version, **NTLM v2** authentication and **AES-128-GCM**, but that can change, so for now leave everything selected.
- Ensure that the **SMB Allow storage account key access** is enabled by going to the main page for the storage account and selecting **Configuration** from the blade menu.

☐ To create the Azure Sync Service, search for *Azure File Sync* and select it under *MarketPlace*.

☐ Enter the same resource group and region as your storage account, give it a name and click **Next** to go to the *Networking* page.



Deploy Azure File Sync ...

Azure File Sync in combination with Azure file shares allows you to centralize your organization's file shares in Azure, while keeping the flexibility, performance, and compatibility of an on-premises file server. Learn more

Storage Sync Service
Microsoft

Deploying this storage sync service resource will allow you to transform your Windows Server into a quick cache for Azure file shares with optional cloud tiering and multi-server sync functionality. Keep in mind that servers registered to different storage sync service resources cannot exchange data with each other. It's best to register all servers to the same storage sync service if they will ever have a need to sync the same Azure file share.

Subscription *	Tootechi
Resource group *	StorageTest1 Create new
Storage sync service name *	FSTestSynch ✓
Region *	Canada Central

© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Allow access from all networks, and then review and create the resource.

□ To install the Azure File Sync agent, first collect the following information:

- The deployment name for the Storage Sync Service
- The Azure subscription ID to use for the deployment
- The Resource Group for the deployment (the same as for the storage account)
- The deployment location (the same as for the storage account)

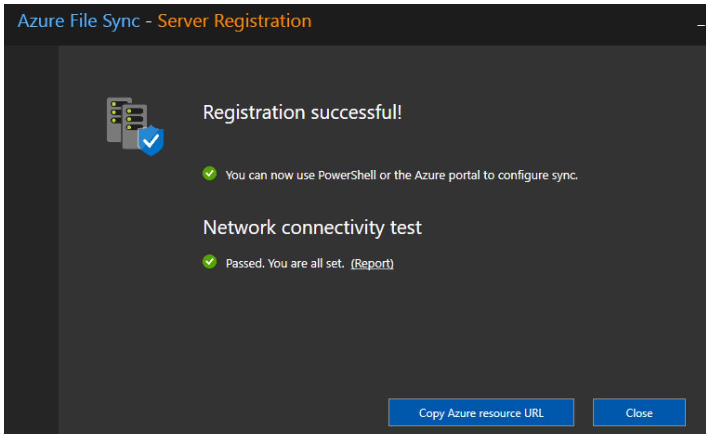
□ On your virtual machine, download and install the agent (with default selections) from the link: https://www.microsoft.com/en-us/download/details.aspx?id=57159.

After the agent is installed, it must be registered with the sync service to create a trust relationship between the server and the sync service.

□ When the Registration window appears and asks for the *Azure Environment*, select **Azure Cloud** and click **Sign in**.

□ Enter the subscription, resource group and sync service information and click **Register**.

□ Once the service is registered, copy the URL.



Azure File Sync - Server Registration

Registration successful!

✓ You can now use PowerShell or the Azure portal to configure sync.

Network connectivity test

✓ Passed. You are all set. (Report)

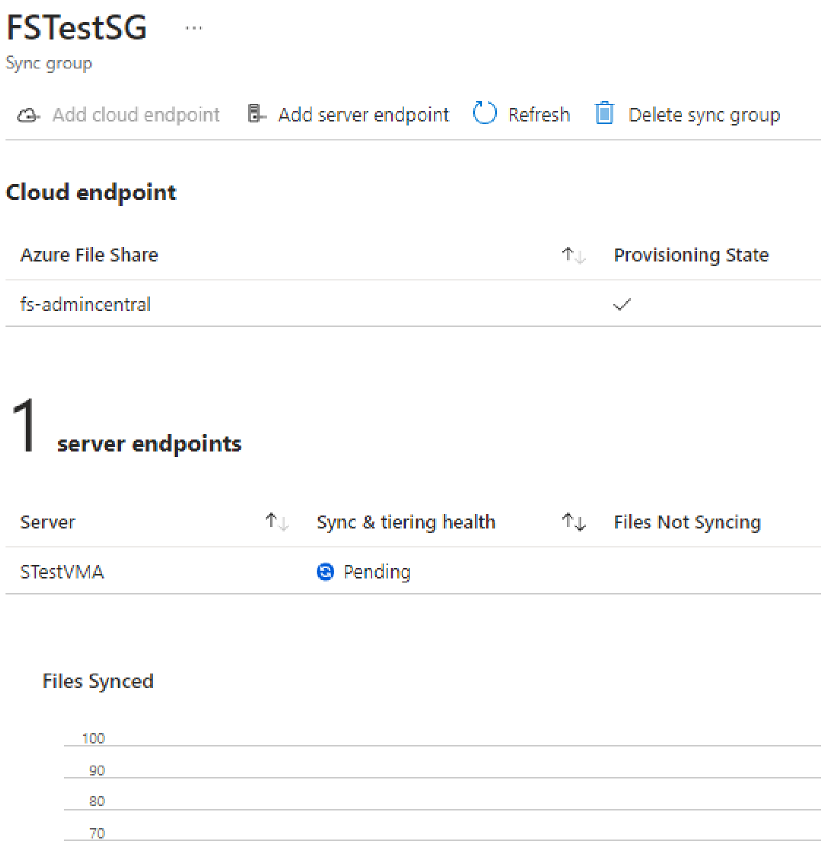
© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

Next, create a sync group that defines the topology for the service, including which cloud endpoints belong to the service and which server endpoints belong to the service (local file share).

- ☐ In the main page for your sync service select **+ Sync Group** from the top menu.
- ☐ Enter a name for the group, the subscription, the storage account and select the file share you already have that contains some .pdf files.
- ☐ Create the group. This creates the cloud endpoint.
- ☐ Go to the main page for your sync service and select **Registered Servers** from the blade menu.
- ☐ Make sure your server is properly registered and shows as *Online*.
- ☐ When the group is created, go to its main page and select **Add Server Endpoint** from the top menu.
- ☐ Select the server you registered and the path to your SMB share.
- ☐ Click the drop-down arrow for **Initial Sync** and note the selections. You want to merge the contents, so make that selection and create the server endpoint.

  Note: It will take some time to create and sync everything and you may have to refresh the window. You will see the *Sync and Tiering Health* as *Pending* until everything is complete.



FSTestSG ···

Sync group

Add cloud endpoint · Add server endpoint · Refresh · Delete sync group

Cloud endpoint

Azure File Share ↑↓	Provisioning State
fs-admincentral	✓

1 **server endpoints**

Server ↑↓	Sync & tiering health ↑↓	Files Not Syncing
STestVMA	Pending	

© 2023, Microsoft Azure. Used with permission from Microsoft.

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Go back to your virtual machine and open File Explorer.

☐ Navigate to your share on the data disk. You should see the .pdf files that were in the cloud have synced to your server.

File synchronization is bi-directional but files changed in the cloud may take up to 24 hours to synchronize with the server endpoints. Files changed on the server should synchronize quite quickly.

☐ Create a new file or folder in the share on your virtual machine.

☐ Refresh the storage account a few times to see the new file and/or folder in the cloud.

Note: To force the change, use the `Invoke-AzStorageSyncChangeDetection` PowerShell command
See details at: Invoke-AzStorageSyncChangeDetection (https://learn.microsoft.com/en-us/powershell/module/az.storagesync/invoke-azstoragesyncchangedetection).

If you want to delete the resources here to save costs, you must do things in order. To delete everything:

1. Unregister the server from the sync group.
2. Delete the server endpoints.
3. Delete the cloud endpoints.
4. Delete the sync group.
5. Delete the sync service.
6. Delete the resource group.

Part 5: Create a File Share Snapshot

In the previous lab you learned about versioning storage objects, in this section you are going to create a snapshot (point-in-time replica) of your storage.

□ If you do not have a storage account, create one with a file share and several .pdf documents.

□ From the file shares main page select **Snapshots** from the blade menu.

□ Select **+ Snapshot** from the top menu and enter a relevant comment.

□ Click your created snapshot to see the copy of the files from the file share.

□ Return to the file share’s main page and delete one of the files.

Note: Refresh to make sure it’s gone.

□ Go back to the snapshot, select the file you deleted, and then click the three dots on the far right.

□ Select **Restore** to go to the *File Properties* page.

□ Restore the file as a copy and give it a name you can recognize.

□ Check that the file has been restored to the file share.