

Configure Azure Files

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/1-introduction>

Introduction

Completed

Azure Files offers fully managed file shares in the cloud that are accessible via industry standard protocols. Azure File Sync is a service that allows you to cache several Azure Files shares on an on-premises Windows Server or cloud virtual machine.

In this module, your company has a large repository of organizational documents. Offices are located in different geographical regions, and users need the most current versions of the documents. You're researching how to implement Azure Files shares to provide a central location for the documents.

Learning objectives

In this module, you learn how to:

- Identify storage for file shares.
- Compare file shares to blob storage.
- Configure Azure file shares, file share snapshots, and soft delete.
- Use Azure Storage Explorer to access your file share.

Skills measured

The content in the module helps you prepare for [Exam AZ-104: Microsoft Azure Administrator](#).

Prerequisites

- Familiarity with shared file systems.
- Familiarity with navigating the Azure portal.

2. Compare storage for file shares and blob data

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/2-compare-files-to-blobs>

Compare storage for file shares and blob data

Completed

[Azure Files](#) offers fully managed file shares in the cloud. You can access Azure file shares by using the Server Message Block (SMB), Network File System (NFS), and HTTP protocols. Clients can connect to Azure file shares from Windows, Linux, and macOS devices.

Things to know about Azure Files

Here are some characteristics of Azure files:

- **Serverless deployment.** An Azure file share is a PaaS offering of a fully managed file share that doesn't require any infrastructure. You don't need to take care of any VMs, operating systems, or updates.
- **Almost unlimited storage.** A single Azure file share can store up to 100 terabytes (TiB) of files, and a file can be up to 4 TiB in size. The files are organized in a hierarchical folder structure in the same way as on on-premises file servers.
- **Data encryption.** The data on an Azure file share is encrypted at rest in an Azure datacenter and in transit on a network.
- **Access from anywhere.** By default, clients can access Azure file shares from anywhere if they have internet connectivity.
- **Integration into an existing environment.** You can control access to Azure file shares by using Microsoft Entra identities or AD DS identities that are synced to Microsoft Entra ID. This helps ensure that users can have the same experience accessing an Azure file share as when they access an on-premises file server.
- **Previous versions and backups.** You can create Azure file share snapshots that integrate with the Previous Versions feature in File Explorer. You can also use Azure Backup to back up Azure file shares.
- **Data redundancy.** Azure file share data replicates to multiple locations in the same Azure datacenter or across many Azure datacenters. The replication setting of the Azure storage

account that includes the file share controls the data redundancy.

Things to consider when using Azure Files

There are many common scenarios for using Azure Files. As you review the following suggestions, think about how Azure Files can provide solutions for your organization.

- **Consider replacement and supplement options.** Replace or supplement traditional on-premises file servers or NAS devices by using Azure Files.
- **Consider global access.** Directly access Azure file shares by using most operating systems, such as Windows, macOS, and Linux, from anywhere in the world.
- **Consider lift and shift support.** *Lift and shift* applications to the cloud with Azure Files for apps that expect a file share to store file application or user data.
- **Consider using Azure File Sync.** Replicate Azure file shares to Windows Servers by using Azure File Sync. You can replicate on-premises or in the cloud for performance and distributed caching of the data where it's being used. We take a closer look at Azure File Sync in a later unit.
- **Consider shared applications.** Store shared application settings such as configuration files in Azure Files.
- **Consider diagnostic data.** Use Azure Files to store diagnostic data such as logs, metrics, and crash dumps in a shared location.
- **Consider tools and utilities.** Azure Files is a good option for storing tools and utilities that are needed for developing or administering Azure VMs or cloud services.

Compare Azure Files to Azure Blob Storage

It's important to understand when to use Azure Files to store data in file shares rather than using Azure Blob Storage to store data as blobs. The following table compares different features of these services and common implementation scenarios.

Azure Files (file shares)	Azure Blob Storage (blobs)
Azure Files provides the SMB and NFS protocols, client libraries, and a REST interface that allows access from anywhere to stored files.	Azure Blob Storage provides client libraries and a REST interface that allows unstructured data to be stored and accessed at a massive scale in block blobs.
- Files in an Azure Files share are true directory objects. - Data in Azure Files is accessed through file shares across multiple virtual machines.	- Blobs in Azure Blob Storage are a flat namespace. - Blob data in Azure Blob Storage is accessed through a container.

Azure Files (file shares)	Azure Blob Storage (blobs)
Azure Files is ideal to lift and shift an application to the cloud that already uses the native file system APIs. Share data between the app and other applications running in Azure. Azure Files is a good option when you want to store development and debugging tools that need to be accessed from many virtual machines.	Azure Blob Storage is ideal for applications that need to support streaming and random-access scenarios. Azure Blob Storage is a good option when you want to be able to access application data from anywhere.

3. Manage Azure file shares

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/3-manage-file-shares>

Manage Azure file shares

Completed

Azure Files offers two industry-standard file system protocols for mounting Azure file shares: the Server Message Block (SMB) protocol and the Network File System (NFS) protocol. Azure file shares don't support both the SMB and NFS protocols on the same file share, although you can create SMB and NFS Azure file shares within the same storage account.

Types of Azure file shares

Azure Files supports two storage tiers: premium and standard. Standard file shares are created in general purpose (GPv2) storage accounts, while premium file shares are created in FileStorage storage accounts. The two storage tiers have the attributes described in the following table.

Storage tier	Performance	Storage account type	Redundancy options	Billing model	Use cases
Premium	SSD-backed, consistent low latency	FileStorage	LRS, ZRS	Provisioned (pay for capacity reserved)	High-performance workloads requiring low latency
Transaction Optimized	HDD-backed, standard performance	General-purpose v2 (GPv2)	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Pay-as-you-go	High-transaction workloads,

Storage tier	Performance	Storage account type	Redundancy options	Billing model	Use cases
					frequently accessed data
Hot	HDD-backed, standard performance	General-purpose v2 (GPv2)	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Pay-as-you-go	General-purpose team shares and collaborative workloads
Cool	HDD-backed, standard performance	General-purpose v2 (GPv2)	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Pay-as-you-go	Cost-efficient online archive and backup scenarios

Note

Transaction Optimized, Hot, and Cool are all Standard (HDD-based) tiers with different pricing structures optimized for specific access patterns. Premium tier uses SSD storage with provisioned billing (you pay for the capacity you reserve), while Standard tiers use pay-as-you-go billing.

Types of authentication

There are three main authentications methods that Azure Files supports.

Authentication method	Description
Identity-based authentication over SMB	SMB identity-based authentication supports three Active Directory sources: On-premises AD DS, Microsoft Entra Domain Services, and Microsoft Entra Kerberos. Once your Active Directory source is selected, assign Azure RBAC roles to users who need access to the file share.
Access key	An access key is an older and less flexible option. An Azure storage account has two access keys that can be used when making a request to the storage account, including to Azure Files. Access keys are static and provide full control access to Azure Files. Access keys should be secured and not shared with users, because they bypass all access control restrictions. A best practice is to avoid sharing storage account keys and use identity-based authentication whenever possible.
A Shared Access Signature (SAS) token	SAS is a dynamically generated Uniform Resource Identifier (URI) that's based on the storage access key. SAS provides restricted access rights to an Azure storage account. Restrictions include allowed permissions, start and expiry time, allowed IP addresses from where requests can be sent, and allowed protocols. With Azure Files, a SAS token is only used to provide REST API access from code.

Creating SMB Azure file shares (classic)

Classic Azure file shares live inside a storage account, so they follow the same limits as that account. You can choose between two storage tiers: SSD (premium) and HDD (standard).

SSD file shares are great when you need fast, consistent performance with low latency—usually in the single digit milliseconds. HDD shares are more budget friendly and work well for general purpose storage.

If you need SMB access, make sure to create your file share inside a storage account. SMB file shares let you pick from several access tiers, including transaction optimized, hot, and cool.

Home > Storage center | File shares

New file share ...

Basics Backup Review + create

Name *

Access tier *

Transaction optimized



Premium

Premium file shares are only available for premium file storage accounts.

Transaction optimized

Lowest transaction cost pricing for transaction-heavy workloads that don't need the low latency offered by premium file shares. Recommended while migrating data to Azure Files.

Hot

Balanced storage and transaction pricing for workloads that have a good measure of both.

Cool

Most cost-efficient storage pricing for storage-intensive workloads.

Performance

Maximum IO/s ⓘ 20000

Maximum capacity 100 TiB

Note

When connecting over SMB, don't forget that traffic uses port 445. Many ISPs block port 445 outbound, which is the most common connectivity issue when mounting Azure file shares from on-premises environments.

Important

[File shares \(preview\)](#) are now generally available that don't require an Azure storage account. This option provides simplified management for scenarios where you only need file shares without other storage services.

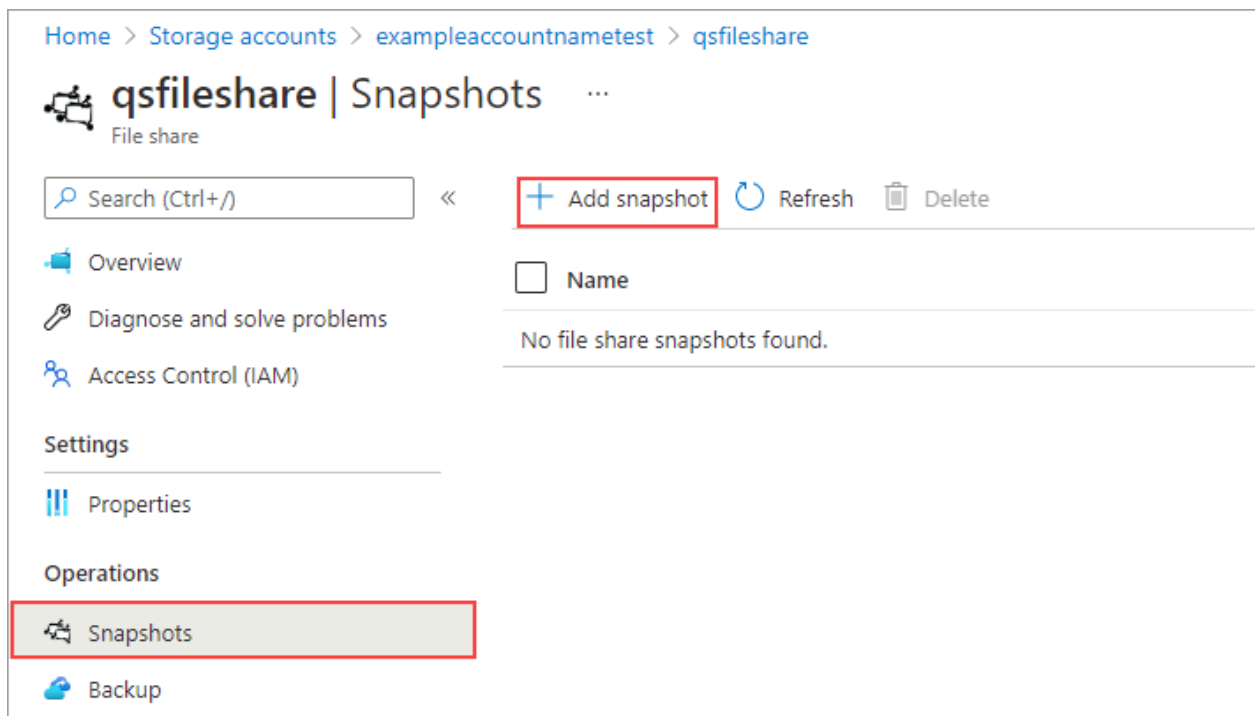
4. Create file share snapshots

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/4-create-file-share-snapshots>

Create file share snapshots

Completed

Azure Files provides the capability to take share [snapshots of file shares](#). Share snapshots provide point-in-time copies of your Azure file shares that protect against accidental deletion and enable recovery from application errors.



Things to know about file share snapshots

- Snapshots are incremental, read-only point-in-time copies at the share level.
- To reduce time and cost only captures from the last snapshot.
- Same experience for SMB and NFS shares in all Azure public regions.

- Snapshot adds a unique timestamp to the share URI.
- Uses the shares redundancy settings.
- Up to 200 snapshots per file share for low-RPO recovery points.
- Snapshots persist until deleted. Deleting the share deletes all snapshots.
- Azure Backup can lease snapshots to help prevent accidental deletion.
- Restore a file, folder, or full share; full restore requires only the latest snapshot.

Things to consider when using file share snapshots

File share snapshots can help you protect and recover your data. As you review the benefits, consider where snapshots fit into your Azure Files setup.

Benefit	Description
Protect against application error and data corruption	File-share workloads constantly read and write data. If a misconfiguration, bad deployment, or software bug overwrites or corrupts data, a snapshot lets you roll the share back to a known-good point in time. Take a snapshot before releasing new code so you have a clean restore point if something goes wrong.
Protect against accidental deletions or unintended changes	If a file is changed, snapshots give you a quick way to restore an earlier version. Use snapshots to roll back to the last good copy when something unexpected happens.
Support backup and recovery	Create snapshots on a schedule to build a backup history for your file share. Keeping prior versions makes it easier to meet audit needs and recover data after mistakes or a broader outage.

For automated snapshot creation or integration with existing scripts, PowerShell and Azure CLI provide programmatic access to snapshot operations. Both tools support adding metadata to snapshots and can be scheduled through Azure Automation, GitHub Actions, or any continuous integration system.

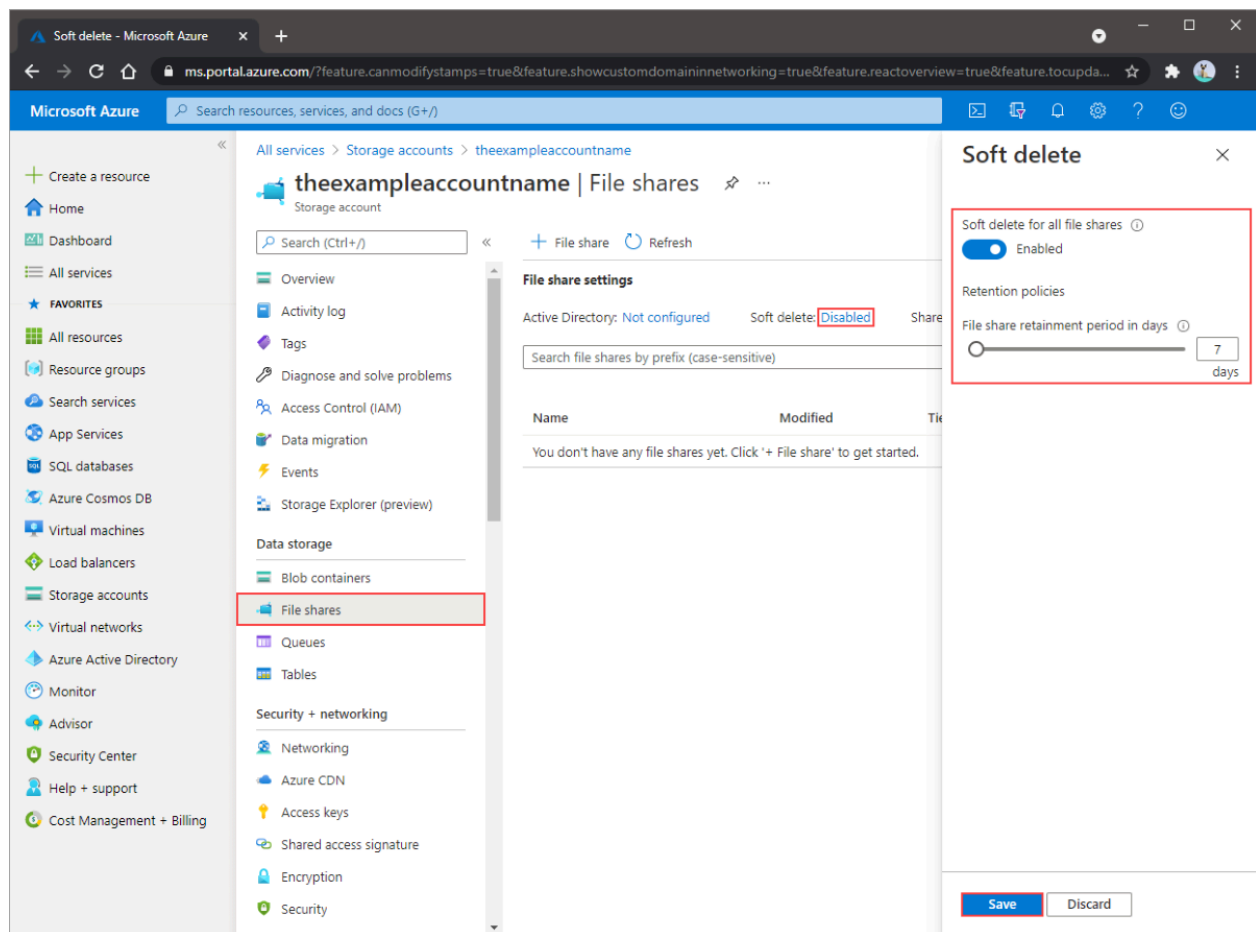
5. Implement soft delete for Azure Files

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/5-implement-file-sync>

Implement soft delete for Azure Files

Completed

Azure Files offers [soft delete for file shares](#). Soft delete lets you recover deleted files and file shares.



Things to know about soft delete for Azure Files

Let's take a look at the characteristics of soft delete for Azure Files.

- Soft delete for file shares is enabled at the storage account level.
- Soft delete transitions content to a soft deleted state instead of being permanently erased.
- Soft delete lets you configure the retention period. The retention period is the amount of time that soft deleted file shares are stored and available for recovery.
- Soft delete provides a retention period between 1 and 365 days.
- Soft delete can be enabled on either new or existing file shares.

Things to consider when using soft delete for Azure Files

There are many advantages to using soft delete for Azure Files. Consider the following scenarios, and think about how you can use soft delete.

- **Recover from accidental data loss.** You can recover deleted or corrupted data with soft delete.

- **Upgrade scenarios.** Use soft delete to restore to a known good state after a failed upgrade attempt.
- **Ransomware protection.** Use soft delete to recover data without paying ransom to cybercriminals.
- **Long-term retention.** Use soft delete to comply with data retention requirements.
- **Business continuity.** Use soft delete to prepare your infrastructure to be highly available for critical workloads.

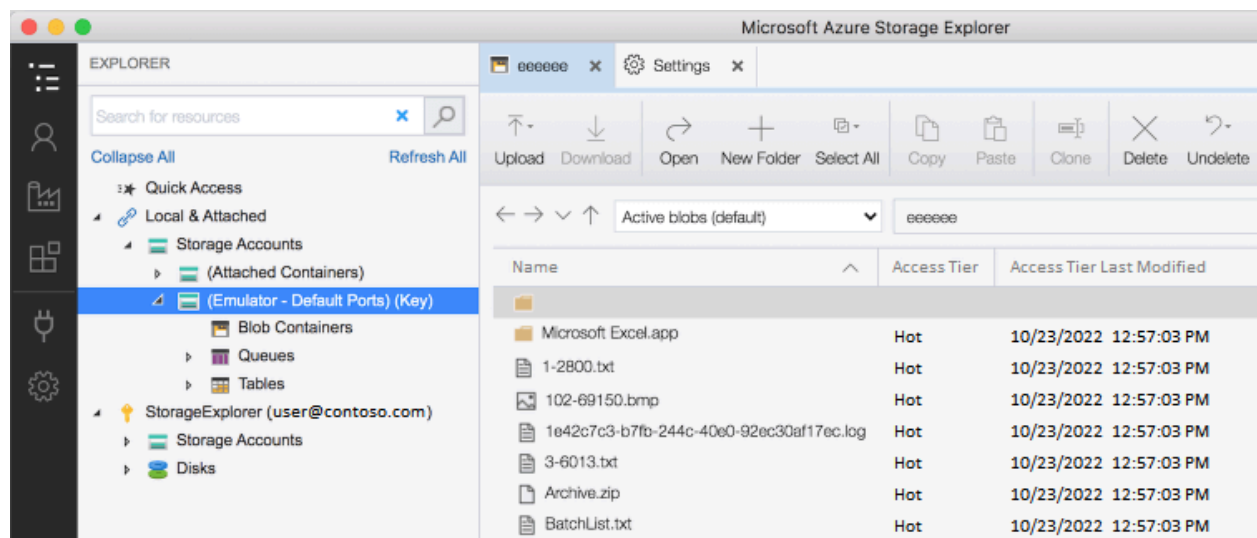
6. Use Azure Storage Explorer

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/6-identify-components>

Use Azure Storage Explorer

Completed

[Azure Storage Explorer](#) is a standalone application that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. With Azure Storage Explorer, you can access multiple accounts and subscriptions, and manage all your Storage content.



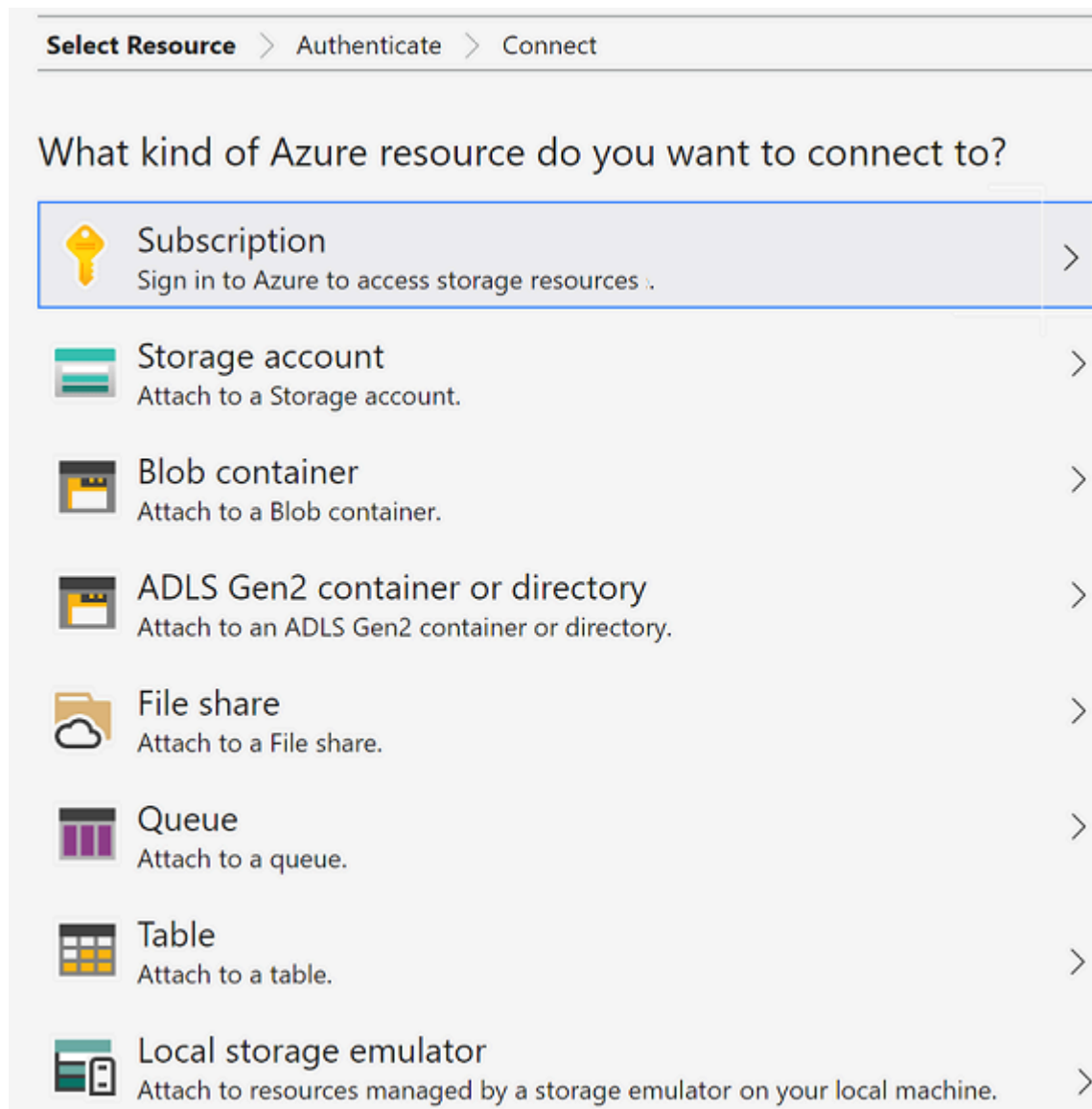
Things to know about Azure Storage Explorer

Azure Storage Explorer has the following characteristics.

- Azure Storage Explorer requires both management (Azure Resource Manager) and data layer permissions to allow full access to your resources. You need Microsoft Entra ID permissions to

access your storage account, the containers in your account, and the data in the containers.

- Azure Storage Explorer lets you connect to different storage accounts.
 - Connect to storage accounts associated with your Azure subscriptions.
 - Connect to storage accounts and services that are shared from other Azure subscriptions.
 - Connect to and manage local storage by using the Azure Storage Emulator.



Things to consider when using Azure Storage Explorer

Azure Storage Explorer supports many scenarios for working with storage accounts in Azure. As you review these options, think about which scenarios apply to your Azure Storage implementation.

Scenario	Description
Connect to an Azure subscription	Manage storage resources that belong to your Azure subscription.

Scenario	Description
Work with local development storage	Manage local storage by using the Azure Storage Emulator.
Attach to external storage	Manage storage resources that belong to another Azure subscription or that are under national Azure clouds by using the storage account name, key, and endpoints. This scenario is described in more detail in the next section.
Attach a storage account with a SAS	Manage storage resources that belong to another Azure subscription by using a shared access signature (SAS).
Attach a service with a SAS	Manage a specific Azure Storage service (blob container, queue, or table) that belongs to another Azure subscription by using a SAS.

Attach to external storage account

Azure Storage Explorer lets you attach to external storage accounts so storage accounts can be easily shared.

To create the connection, you need the external storage **Account name** and **Account key**. In the Azure portal, the account key is called **key1**.

Attach using Name and Key

Enter information to connect to the Microsoft Azure storage account

Account name:

Account key:

Storage endpoints domain:

Azure
▼

☐ Use HTTP (Not recommended)

[Online privacy statement](#)

Back
Next
Connect
Cancel

To use a storage account name and key from a national Azure cloud, use the **Storage endpoints domain** drop-down menu to select **Other**, and then enter the custom storage account endpoint domain.

Access keys

Access keys provide access to the entire storage account. You're provided two access keys so you can maintain connections by using one key while regenerating the other.

Important

Store your access keys securely. We recommend regenerating your access keys regularly.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action doesn't interrupt access to disks from your virtual machines.

7. Consider Azure File Sync

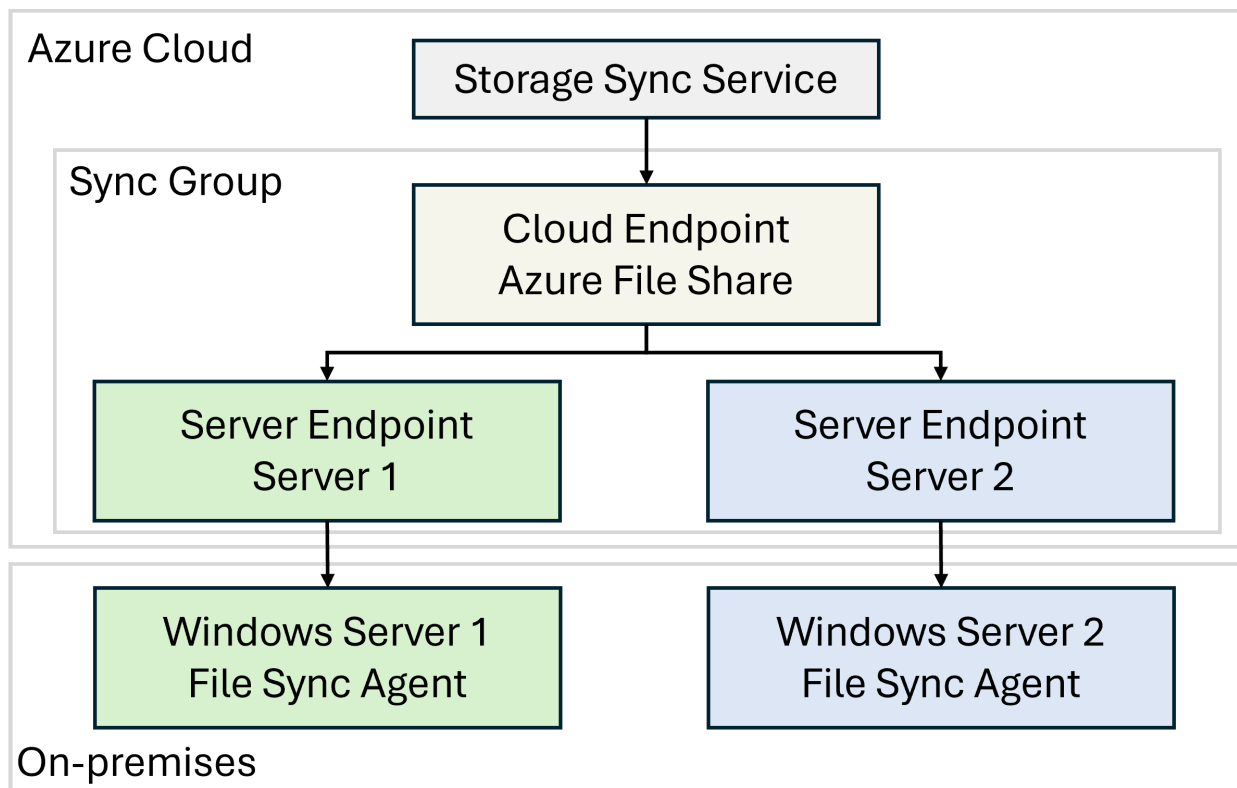
<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/7-deploy-azure-file-sync>

Consider Azure File Sync

Completed

[Azure File Sync](#) enables you to cache several Azure Files shares on an on-premises Windows Server or cloud virtual machine. You can use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server.

Azure File Sync consists of five main components that work together to synchronize files between on-premises Windows Servers and Azure file shares.



- The **Storage Sync Service** is the primary Azure resource responsible for managing file synchronization. It can support up to 100 sync groups, operates within a single Azure region, and allows for up to 99 registered Windows Servers.
- The **sync group** establishes the synchronization setup, containing one cloud endpoint (Azure file share) and up to 50 server endpoints. Server endpoints are specific NTFS paths on registered Windows Servers, but cannot be on the system volume, and cloud tiering is not supported there.
- The **cloud endpoint** is an Azure file share that participates in the sync group. Only one cloud endpoint is allowed per sync group.
- The **server endpoint** is a path on a registered Windows Server that syncs with the cloud endpoint. The server endpoint must be an NTFS-formatted volume, and can't be a system volume.
- The **Azure File Sync Agent** is installed on each Windows Server. The agent is a background Windows service for sync operations and management tasks.

Things to know about Azure File Sync

Let's take a look at the characteristics of Azure File Sync.

- Azure File Sync transforms Windows Server into a quick cache of your Azure Files shares.
- You can use any protocol that's available on Windows Server to access your data locally with Azure File Sync, including SMB, NFS, and FTPS.

- Azure File Sync supports as many caches as you need around the world.
- There is a maximum of 100 sync groups per Storage Sync Service, and 50 server endpoints per sync group.

Things to consider when using Azure File Sync

There are many advantages to using Azure File Sync. Consider the following scenarios, and think about how you can use Azure File Sync with your Azure Files shares.

- **Consider application lift and shift.** Use Azure File Sync to move applications that require access between Azure and on-premises systems. Provide write access to the same data across Windows Servers and Azure Files.
- **Consider support for branch offices.** Support your branch offices that need to back up files by using Azure File Sync. Use the service to set up a new server that connects to Azure storage.
- **Consider backup and disaster recovery.** After you implement Azure File Sync, Azure Backup backs up your on-premises data. Restore file metadata immediately and recall data as needed for rapid disaster recovery.
- **Consider file archiving with cloud tiering.** Azure File Sync stores only recently accessed data on local servers. Implement cloud tiering so older data moves to Azure Files.

8. Knowledge check

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/8-knowledge-check>

Knowledge check

Completed

9. Summary and resources

<https://learn.microsoft.com/en-us/training/modules/configure-azure-files-file-sync/9-summary-resources>

Summary and resources

Completed

Azure Administrators are familiar with Azure Files and the Azure File Sync agent. They know how to implement fully managed file shares in the cloud by using industry standard protocols. They understand how to use Azure File Sync to cache Azure Files shares on an on-premises Windows Server or cloud virtual machine.

In this module, you learned when to use Azure Files and how the service compares to Azure Blob Storage. You also reviewed Azure Files features such as snapshots and soft delete. You learned how Azure File Sync can be used with on-premises data stores. You also were introduced to Azure Storage Explorer.

The main takeaways for this module are:

- Azure Files provides the SMB and NFS protocols, client libraries, and a REST interface that allows access from anywhere to stored files.
- Azure Files is ideal to lift and shift an application to the cloud that already uses the native file system APIs. Share data between the app and other applications running in Azure.
- Azure Files offers two industry-standard file system protocols for mounting Azure file shares: the Server Message Block (SMB) protocol and the Network File System (NFS) protocol.
- Azure Files offers two types of file shares: standard and premium. The premium tier stores data on modern solid-state drives (SSDs), while the standard tier uses hard disk drives (HDDs).
- File share snapshots capture a point-in-time, read-only copy of your data.
- Soft delete allows you to recover your deleted file share.
- Azure Storage Explorer is a standalone application that makes it easy to work with stored data on Windows, macOS, and Linux.
- Azure File Sync enables you to cache file shares on an on-premises Windows Server or cloud virtual machine.

Learn more with Copilot

Copilot can assist you in configuring Azure infrastructure solutions. Copilot can compare, recommend, explain, and research products and services where you need more information. Open a Microsoft Edge browser and choose Copilot (top right) or navigate to copilot.microsoft.com. Take a few minutes to try these prompts and extend your learning with Copilot.

- What are Azure Files and how are they different from Azure blob storage?
- What are some common configuration and administration tasks for Azure Files?

Learn more with documentation

- [Azure Files documentation](#). This page is your starting point for all things related to Azure Files.
- [Azure File Sync documentation](#). This page is your starting point for all things related to Azure File Sync.

Learn more with self-paced training

- [Implement a hybrid file server infrastructure](#). In this module, you learn to deploy Azure File Sync and use Storage Migration Services to migrate file servers to Azure.
- [Guided Project - Azure Files and Azure Blobs](#). In this module, you practice storing business data securely by using Azure Blob Storage and Azure Files. The lab combines both learning and practical experience.