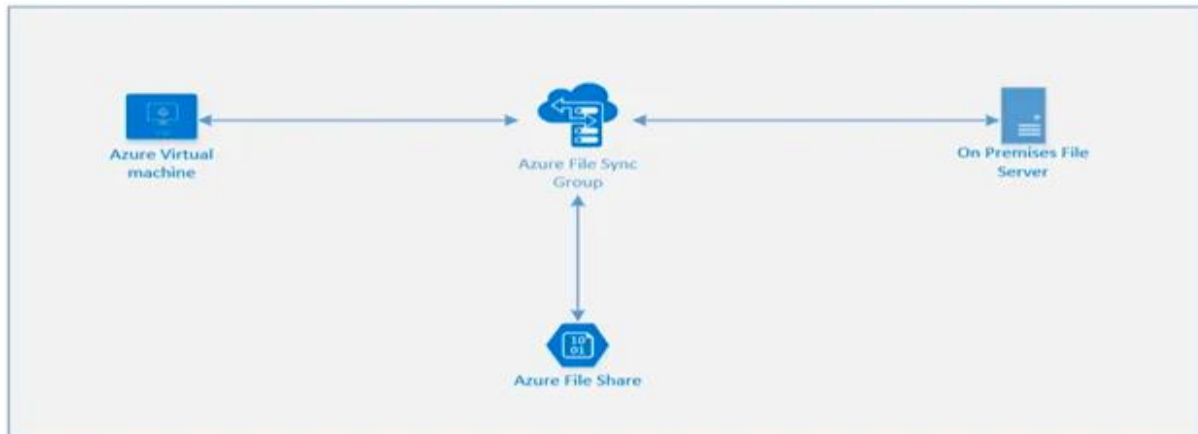


Azure File share



Azure Files fully managed file shares in the Azure cloud that are accessible via the industry standard Server Message Block (SMB 3.0) protocol or Network File System (NFS) protocol.

It can concurrently mounted by cloud VM or on-premises Systems.

Azure Files SMB file shares are accessible from Windows, Linux, and macOS clients and NFS file shares are accessible from Linux or macOS clients.

A file share account quota of maximum of 5 TiB by default, but you can increase the share limit to 100 TiB. To increase your share limit, enable Large file share on your storage account. Premium storage accounts (FileStorage storage accounts) don't have the large file share feature flag as all premium file shares are already enabled for provisioning up to the full 100-TiB capacity.

To enable large file shares on an existing storage account, navigate to File shares in the storage account's table of contents. On this blade, select Share capacity, change the share capacity to 100 TiB and select Save.

Azure Files provides two distinct billing models: provisioned and pay-as-you-go. The provisioned model is only available for premium file shares, which are file shares deployed in the FileStorage storage account kind. The pay-as-you-go model is only available for standard file shares, which are file shares deployed in the general purpose version 2 (GPV2) storage account kind.

Create a storage account

On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. Select Storage Accounts.

On the Storage Accounts window that appears, choose Add.

On the Basics tab, select the subscription in which to create the storage account.

Create storage account ...

[Basics](#) [Networking](#) [Data protection](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.

[Learn more about Azure storage accounts](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Pay-As-You-Go"/>
Resource group *	<input type="text" value="(New) rg-asegk-00"/>

[Create new](#)

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name * ⓘ	<input type="text" value="strasegkstd00"/>
Location *	<input type="text" value="(Asia Pacific) South India"/>
Performance ⓘ	<input checked="" type="radio"/> Standard <input type="radio"/> Premium
Account kind ⓘ	<input type="text" value="StorageV2 (general purpose v2)"/>
Replication ⓘ	<input type="text" value="Read-access geo-redundant storage (RA-GRS)"/>

Under the Resource group field, select resource group, or create a new resource group.
Next, enter a name for your storage account. The name you choose must be unique across Azure. The name also must be between 3 and 24 characters in length, and may include only numbers and lowercase letters.
Select a location for your storage account, or use the default location.
Select a performance tier. The default tier is Standard.
Set the Account kind field to Storage V2 (general-purpose v2).
Specify how the storage account will be replicated. The default replication option is Read-access geo-redundant storage (RA-GRS). For more information about available replication options, see [Azure Storage redundancy](#).

Additional options are available on the Networking, Data protection, Advanced, and Tags tabs.

Create storage account ...

Basics Networking **Data protection** Advanced Tags Review + create

Recovery

- Turn on point-in-time restore for containers
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)
- Turn on soft delete for blobs
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
- Turn on soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
Sign up is required on a per-subscription basis to use container soft delete. [Sign up for container soft delete](#)
- Turn on soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)
Keep deleted file shares for (in days)

Tracking

- Turn on versioning for blobs
Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. [Learn more](#)
- Turn on blob change feed
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

Create storage account ...

- Secure transfer required Disabled Enabled
- Allow shared key access Disabled Enabled
- Minimum TLS version
- Infrastructure encryption Disabled Enabled
Sign up is currently required to enable infrastructure encryption on a per-subscription basis. [Sign up for infrastructure encryption](#)
- Blob storage**
- Allow Blob public access Disabled Enabled
- Blob access tier (default) Cool Hot
- NFS v3 Disabled Enabled
Sign up is currently required to utilize the NFS v3 feature on a per-subscription basis. [Sign up for NFS v3](#)
- Data Lake Storage Gen2**
- Hierarchical namespace Disabled Enabled
- Azure Files**
- Large file shares Disabled Enabled
The current combination of storage account kind, performance, replication and location does not support large file shares.
- Tables and Queues**
- Customer-managed keys support Disabled Enabled
Sign up is currently required to enable customer-managed keys support for tables and queues on a per-subscription basis. [Sign up for CMK support](#)

To use Azure Data Lake Storage, choose the Advanced tab, and then set Hierarchical namespace to Enabled.

Select Review + Create to review your storage account settings and create the account.

Select Create.

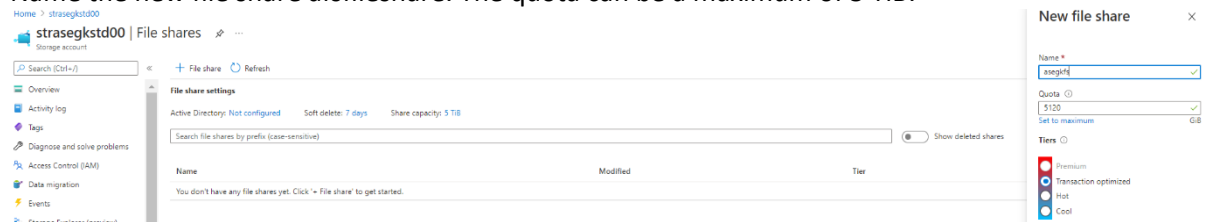
Create a file share

After you deploy an Azure storage account, you create a file share.

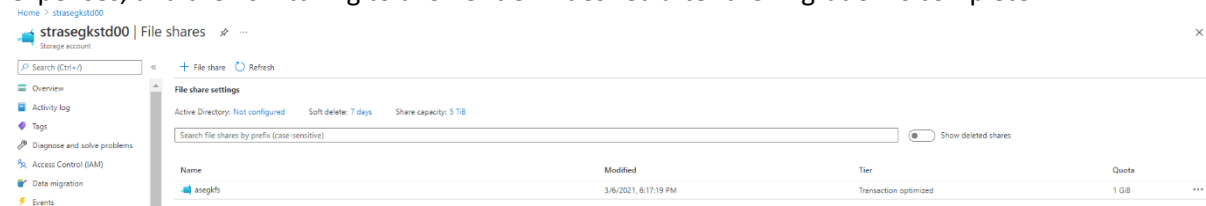
In the Azure portal, select Go to resource.

Select Files from the storage account pane.

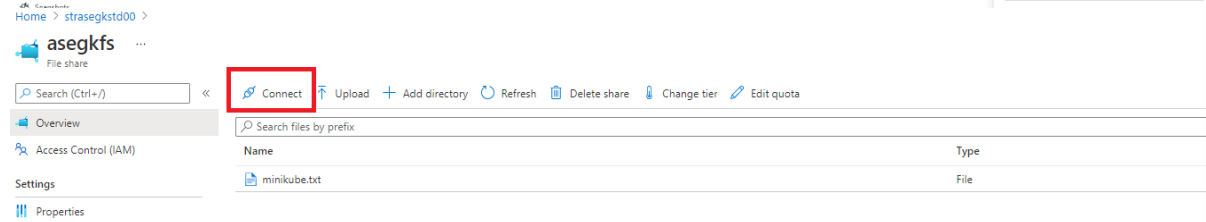
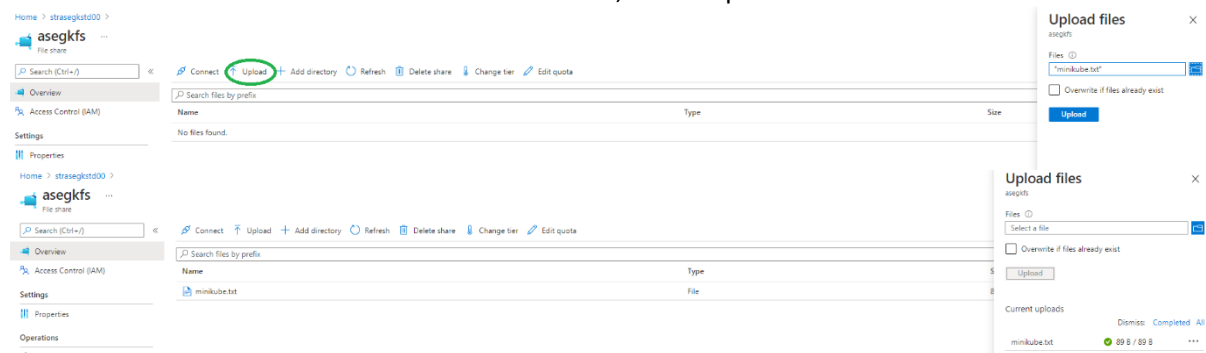
Name the new file share afileshare. The quota can be a maximum of 5 TiB.



Tiers: the selected tier for a file share. This field is only available in a general purpose (GPv2) storage account. You can choose transaction optimized, hot, or cool. The share's tier can be changed at any time. recommend picking the hottest tier possible during a migration, to minimize transaction expenses, and then switching to a lower tier if desired after the migration is complete.



Select the new file share. On the file share location, select Upload.



Map the Azure file share to a Windows drive

In the Azure portal, navigate to the fileshare and select Connect.

Copy the contents to a Notepad.

Connect ✕

asegkfs

⚠ 'Secure transfer required' is enabled on the storage account. SMB clients connecting to this share must support SMB protocol version 3 or higher in order to handle the encryption requirement. [Click here to learn more.](#)

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

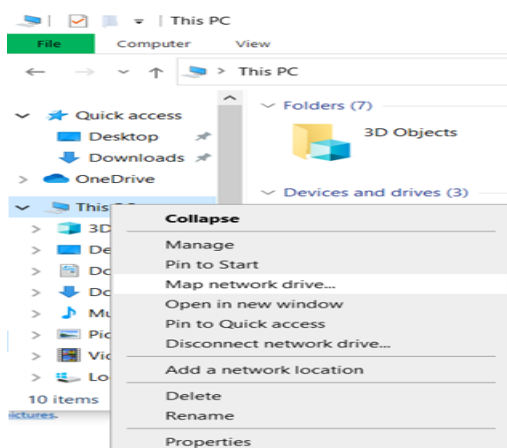
i Connecting to a share using the storage account key is only appropriate for admin access. Utilizing Active Directory allows to differentiate file and folder access, per AD account, within a share. [Learn more](#)

```

$connectTestResult = Test-NetConnection -ComputerName
strasegkstd00.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:"strasegkstd00.file.core.windows.net"
    /user:"Azure\strasegkstd00"
    /pass:"Uu/xknX4ARoQyrhX2KwQlj7JijXJurNmLuQS8MUtAnhu3ssiFMY1ZV5R1Uf9xJc"
  }
  
```

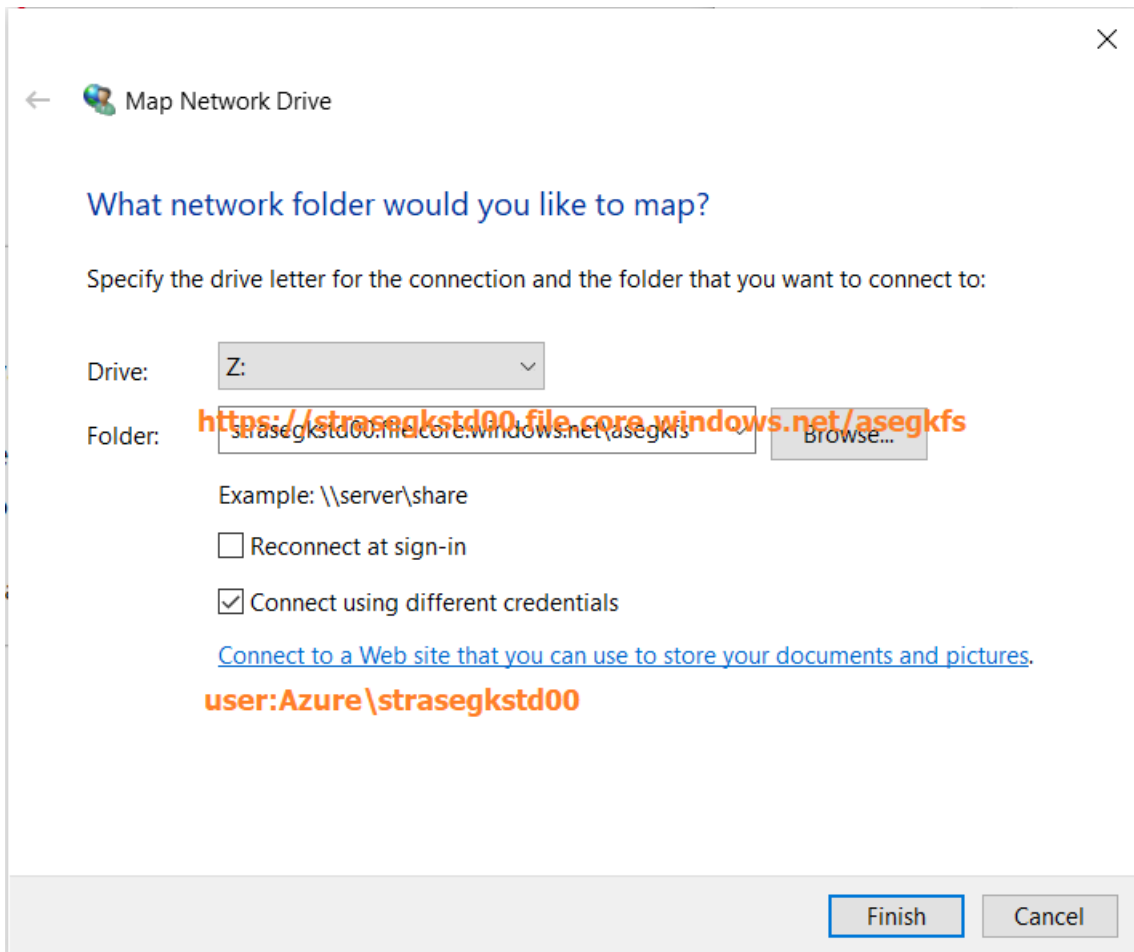
This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site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

On the Computer menu, select Map network drive.



Select the drive letter and enter the UNC path.

UNC path format is \\<storageAccountName>.file.core.windows.net\<fileShareName>.



In the Windows Security dialog box, copy the storage account name in the Windows Security dialog box as the username AZURE\strasegkstd00.

From Notepad, copy the storage account key and paste it in the Windows Security dialog box as the password.

Performance requirements for your Azure file share

Azure Files offers standard file shares which are hosted on hard disk-based (HDD-based) hardware, and premium file shares, which are hosted on solid-state disk-based (SSD-based) hardware.

Redundancy requirements for Azure file share

Standard file shares offer locally-redundant (LRS), zone redundant (ZRS), geo-redundant (GRS), or geo-zone-redundant (GZRS) storage, however the large file share feature is only supported on locally redundant and zone redundant file shares. Premium file shares do not support any form of geo-redundancy.

File share size

In local and zone redundant storage accounts, Azure file shares can span up to 100 TiB, however in geo- and geo-zone redundant storage accounts, Azure file shares can span only up to 5 TiB.