MIGRATION PLAYBOOK · SERVERS AND CLOUD

How to migrate a NAS to Azure Files

Move SMB shares from a NAS appliance to Azure file shares with their NTFS permissions and timestamps intact, set up identity-based access, and switch users over with DFS Namespaces or the old server name.

Updated 4 Nov 2026 6 phases 30 detailed steps 12 official sources

START HERE

How do you migrate a NAS to Azure Files?

SHORT ANSWER

This moves shared folders from a NAS (network storage box) to Azure Files, Microsoft's managed file shares in the cloud, keeping folder permissions and timestamps. You copy the data ahead of time, top it up each night, then switch users over in a short outage while the old \\server\share paths keep working.

- **Recommended route:** Cloud-only Azure file shares, copied with Robocopy or Azure Storage Mover
- **Order:** Clean up the NAS and set up storage, sign-in and root permissions first, then seed each share, top it up nightly, and switch users in one short outage.
- **6 phases:** List the shares, Create the storage, Set up sign-in and permissions, Copy and top up, Keep the old paths and Cut over.
- **You're done when:** Each share has the same file count and size as the NAS, and the final pass shows no failed items.

The time is driven by the first full copy over your internet link; the outage is only as long as the last top-up copy.

RECOMMENDED ROUTE

Cloud-only Azure file shares, copied with Robocopy or Azure Storage Mover

Both keep permissions, timestamps and attributes, and repeat runs copy only what changed. Robocopy is built into Windows; Storage Mover suits many shares.

▼ **Other options and when to use them**

- **Azure File Sync (hybrid)**
  : Offices need local speed, have slow internet, or cannot reach Azure on port 445. Data goes to a Windows Server first.
- **Azure Data Box seed**
  : Very large data on a slow link. The bulk copy travels offline and Robocopy catches up the changes.
- **AzCopy**
  : Data where permissions do not matter, because AzCopy may lose some file details.

TOOLS FOR THIS PLAN

Not sure which route? Answer 5 quick questions	**Are you ready?** 22-question readiness check	**Plan your dates** Dated countdown you can add to your calendar
Compare options Cloud platforms compared	**Check your DNS** MX, SPF, DKIM and DMARC lookup	**New to the jargon?** Plain-English migration glossary

ORDER TO MIGRATE IN, AND WHY

Clean up the NAS and set up storage, sign-in and root permissions first, then seed each share, top it up nightly, and switch users in one short outage. Each step depends on the one before: permissions only work once Azure Files can recognise your domain accounts, and fixes made after the big copy have to be copied again.

1. **Inventory and clean-up: share sizes, local NAS accounts, stale data**
   Every file you delete or archive now is a file you never copy or top up, and NAS-local accounts must be replaced before they are copied.
2. **Storage account, network path (port 445 or a private link) and sign-in setup**
   The copy and the users both need to reach the share and be recognised by it.
3. **Share-level roles and root folder permissions on each Azure file share**
   Microsoft says root permission changes after a large copy take a long time to spread, so set them first.
4. **Seed copy of each share, largest first**
   The first full copy takes longest, so the biggest shares start earliest.

5 **Pilot users from each team on the Azure shares**

Finds permission, sign-in and path problems while the NAS is still the live copy.

6 **Nightly top-ups, then cutover: NAS read-only, final top-up, old name or drive maps switched**

Each top-up copies only changes, so the final one fits in a short outage.

7 **Azure Backup on, then retire the NAS**

The read-only NAS is your rollback and restore point until the first Azure backups succeed.

SETTINGS CHECKLIST: DECIDE THESE BEFORE YOU COPY

Built-in and third-party tools treat these differently. Tick each one off once you have decided.

Download this checklist (Excel)

☐ **Folder permissions (ACLs) and owners**

Which permissions must survive, and which tool keeps them.

▼ How each tool handles it

Built-in method	Robocopy: /COPY:DATSO and /DCOPY:DAT keep NTFS permissions and owner on files and folders. Azure Storage Mover: keeps ACLs (permission lists) from an SMB source. Microsoft lists both as full fidelity, and says owner SID, group SID, DACLs and SACLs must be preserved.
Azure File Sync	Microsoft lists it as full fidelity, natively integrated with Azure file shares.
AzCopy	Microsoft lists it as supported but not fully recommended: some file fidelity might be lost because it copies through the Azure Files REST API.
Azure Data Box	Preserves ACLs, timestamps and attributes when seeding SMB shares.

Tip: Set up identity-based sign-in before the pilot, so Azure Files can check the domain accounts in those permissions.

Microsoft Learn: Migrate to SMB Azure file shares

☐ **Local NAS users and groups**

Which NAS-local accounts are replaced by domain groups before the first copy.

▼ **How each tool handles it**

Built-in method	Every tool copies permissions as they are. A permission granted to a NAS-local account arrives as an unresolved SID (an ID nothing recognises), and those people lose access.
Komprise Elastic Data Migration	Not stated in Komprise's documentation: test it in your pilot.

Tip: Replace local accounts with domain groups on the NAS itself, so every copy and top-up carries the fix.

Microsoft Learn: Migrate to SMB Azure file shares

- [ ] **Root folder permissions**

The permissions on each share's top folder.

▼ **How each tool handles it**

Built-in method	Microsoft: set the root directory ACLs before copying a large number of files, because changes to root permissions after a large migration can take a long time to spread.

Tip: Mount each share as an admin and set its root permissions to match the NAS before the seed copy.

Microsoft Learn: Migrate to SMB Azure file shares

- [ ] **Timestamps and file attributes**

Whether created and modified dates and attributes such as read-only and hidden must survive.

▼ **How each tool handles it**

Built-in method	Robocopy: /COPY:DATSO and /DCOPY:DAT keep timestamps and attributes. Storage Mover: keeps file and folder timestamps and attributes from an SMB source. Azure Files does not support the last access time, whichever tool you use.
AzCopy	Some file fidelity might be lost, according to Microsoft.
Azure Data Box	Preserves timestamps and attributes.

Tip: Compare the modified date on a sample of files at the NAS and the share after the pilot copy.

Microsoft Learn: Migrate to SMB Azure file shares

- [ ] **Alternate data streams**

Whether any application relies on alternate data streams (hidden extra data attached to a file).

▼ **How each tool handles it**

Built-in method	Azure file shares cannot store alternate data streams, whichever tool copies the files.
Azure File Sync	Keeps alternate data streams on the on-premises Windows Server cache, not in the Azure file share.

Tip: Ask application owners about alternate data streams before choosing cloud-only shares.

Microsoft Learn: Migrate to SMB Azure file shares

- [ ] **Copy mode and deletes in the target**

Whether the target mirrors the NAS exactly or keeps extra files.

▼ **How each tool handles it**

Built-in method	Robocopy /MIR: deletes anything in the target that is not on the source. Storage Mover: Mirror deletes target files not in the source; Merge keeps them, and a rename between copies creates duplicate content. Microsoft advises not renaming folders during a migration.
Azure File Sync	Robocopy fills the Azure File Sync server folder, which then syncs to Azure, so the Robocopy options decide deletes.

Tip: Double-check the target path before each /MIR run, and do not rename top-level folders between passes.

Microsoft Learn: Define and start an Azure Storage Mover migration job

- [ ] **Top-up copies (delta passes) and scheduling**

How often top-ups run before cutover, and when.

▼ **How each tool handles it**

Built-in method	Robocopy: rerunning /MIR copies only what changed since the last run. Storage Mover: jobs run manually, once

	or on a daily, weekly or monthly schedule, with start times in UTC.
Azure Data Box	Seeds the bulk offline; Robocopy /MIR then catches up the changes.
AzCopy	Its sync command handles up to 10 million files per job.

Tip: Record how long each nightly top-up takes; the last one before cutover sets the outage length.

Microsoft Learn: Define and start an Azure Storage Mover migration job

- [ ] **File size and share size**

Which shares need their own storage account, and which files are too large for a tool.

▼ **How each tool handles it**

Built-in method	Storage Mover: Microsoft tested it with 500 million files and folders. Robocopy: Microsoft states no file count limit. Azure Files has its own size limits per file and per share, which depend on the billing model.
Azure Data Box	Files must be 4 TiB or smaller, and Data Box cannot import into NFS shares.
Komprise Elastic Data Migration	Analyses data type, ownership, usage, age and growth per share to decide what goes where.

Tip: Check Microsoft's current Azure Files scale targets for your billing model during inventory.

Microsoft Learn: Migrate to Azure file shares using Azure Storage Mover

- [ ] **Network path and ports**

Whether the copy and the users reach Azure over the internet, a VPN or ExpressRoute.

▼ **How each tool handles it**

Built-in method	Robocopy: copies over SMB, which needs TCP port 445 to the storage account. Storage Mover: its agent VM needs outbound port 443, and Microsoft says it is faster than Robocopy because it uses the FileREST API rather than SMB.

Azure File Sync	Users reach a local Windows Server, so they do not need port 445 to Azure.

Tip: Test port 445 from each office and a remote user before choosing cloud-only shares.

Microsoft Learn: Migrate to Azure file shares using Azure Storage Mover

- [ ] **Copy credentials**

Which account reads the NAS for the copy, and where its password is kept.

▼ **How each tool handles it**

Built-in method	Robocopy: /B (backup mode) needs an elevated window and an account with backup rights. Storage Mover: for SMB sources, the username and password are stored as two secrets in Azure Key Vault.

Tip: Use a dedicated migration account, and disable it after cutover.

Microsoft Learn: Migrate to Azure file shares using Azure Storage Mover

- [ ] **Share-level access**

Which share-level role users get, and when it is assigned.

▼ **How each tool handles it**

Built-in method	Azure Files: the default share-level permission is None, so users get Access denied until a role such as Storage File Data SMB Share Contributor is assigned. Roles can take 30 minutes or more to apply.

Tip: Assign roles at least a day before the pilot, and let folder permissions do the fine-grained control.

- [ ] **NAS snapshots and backup**

How users restore files after cutover, and how long the NAS keeps old versions.

▼ **How each tool handles it**

Built-in method	None of the copy tools brings NAS snapshots (the previous versions users restore from), because they are not part of the live share. Azure file shares have no backup until you turn on Azure Backup.

Tip: Keep the NAS read-only until the first Azure backups succeed, and tell users how restores work now.

THE PLAN, PHASE BY PHASE

1 List the shares

Before you create anything

- Export the NAS share list with each share's path and permissions.
- Measure size and file count per share, and archive or delete what nobody needs.
- Check the permissions on each share root and top-level folders with icacls.

List drive maps, login scripts, applications and scheduled tasks that use each path.

Map each NAS share to an Azure file share, storage account and region near your users.

> **Watch out:** Permissions granted to NAS-local users or groups mean nothing to Azure Files, so those people lose access.
>
> **WAYS AROUND IT**
>
> - Replace them with domain groups on the NAS itself before the first copy, so every top-up carries the fix.

> **Watch out:** Azure Files has size limits per share, and with Azure File Sync one Windows Server can sync at most 30 shares.
>
> **WAYS AROUND IT**

- Give large or busy shares their own storage account, and check Microsoft's current limits for your billing model.

TOOLS THAT CAN DO IT

Komprise Elastic Data Migration
Analyses data type, ownership, usage, age and growth per share to decide what goes where, then runs the NAS migration.

Show the detailed steps (4) →

2 Create the storage

Create the storage account, choosing the performance and redundancy your owners agreed.

Set up networking (private endpoint, firewall rules) before you turn on AD DS sign-in.

Create one file

share per NAS share, with a quota of its size plus growth.

Test TCP port 445 (the port Windows file sharing uses) to the storage account from each office and a remote user.

> ⚠ **Watch out:** SMB file sharing needs port 445, which many internet providers and firewalls block.
>
> **WAYS AROUND IT**
>
> - Use a VPN or ExpressRoute (a private link to Azure) with a private endpoint.
> - Or use Azure File Sync, so users reach a local Windows Server instead.

Show the detailed steps (3) →

3 Set up sign-in and permissions

Choose one sign-in source: AD DS (your on-premises Active Directory) for domain-joined PCs, or Microsoft Entra Kerberos for Entra-joined PCs.

Join the storage account to AD DS with AzFilesHybrid, or enable Entra Kerberos

and grant admin consent.

Assign a share-level role such as Storage File Data SMB Share Contributor, at least a day before the pilot.

Give IT admins the Storage File Data SMB Share Elevated Contributor role.

Mount each share as

an admin and set its root permissions to match the NAS, before the big copy.

> **Watch out:** The default share-level permission is None, so users get Access denied until a role is assigned, and roles can take 30 minutes or more to apply.
>
> **WAYS AROUND IT**
>
> - Set a default role for all authenticated users and let folder permissions do the real control.

> **Watch out:** With AD DS, shares stop working if the storage account's AD password passes its maximum age.
>
> **WAYS AROUND IT**
>
> - Put a dated password rotation task in your operations runbook.

> **Watch out:** Entra Kerberos does not support MFA for Azure Files access.
>
> **WAYS AROUND IT**
>
> - Check how your Conditional Access MFA policies apply to the storage account app before the pilot.

Show the detailed steps (5) →

4 Copy and top up

Weeks before cutover, then nightly

Use one copy

tool per share: Storage Mover or Robocopy for cloud-only, Azure File Sync for hybrid.

Robocopy: run Microsoft's command with /MIR, /COPY:DATSO and /DCOPY:DAT from a server near the NAS.

Storage Mover: deploy the agent VM, store NAS credentials in Key

Vault, and check the copy mode before running.

Hybrid: Robocopy the NAS into the Azure File Sync server folder, with cloud tiering at 99% free space.

Rerun the copy nightly and record how long each top-up takes.

> **Watch out:** The first full copy can take too long over a slow internet link.
>
> **WAYS AROUND IT**

- Start the seed weeks ahead and run top-ups nightly.

TOOLS THAT CAN DO IT

Azure Data Box
Seeds Azure file shares offline with ACLs and timestamps, then Robocopy /MIR catches up changes. Files must be 4 TiB or smaller.

Watch out: Robocopy /MIR, and Storage Mover in Mirror mode, delete anything in the target that is not on the source.

WAYS AROUND IT

- Double-check the target folder, and do not rename top-level folders between passes.

Watch out: Large permission changes on the NAS between passes cascade down the tree and every changed item copies again.

WAYS AROUND IT

- Make permission fixes before the seed, not between top-ups.

Show the detailed steps (7) →

5 Keep the old paths

Decide: a stand-alone DFS namespace with root consolidation keeps the NAS name, or a domain namespace gives a

new path.

Install DFS Namespaces (a Windows feature that redirects share paths) on a domain-joined member server, not a domain controller.

For root consolidation, set Microsoft's registry value and restart the DFS service.

Create a folder per share with

exactly the old share name, pointing at the Azure file share.

> **Watch out:** A stand-alone namespace cannot have a second namespace server.
>
> **WAYS AROUND IT**
>
> - Use a failover cluster for the namespace server if you need high availability.

Show the detailed steps (4) →

6 Cut over In the planned outage

Pilot with a few users from each team, fixing permission or sign-in issues first.

Set the NAS shares to

read-
only,
then
run
the
final
top-
up
and
check
it
shows
no
failures.

Take
the
NAS
off
the
network,
then
give
its
name
to
the
namespace
server
with
netdom
and
a
DNS
CNAME
record.

Or,
if
not
keeping
the
old

name, update drive maps in Group Policy.

Turn on Azure Backup for each share, and set Azure File Sync tiering back to its long-term value.

> **Watch out:** Azure file shares have no backup until you set it up, unlike the NAS snapshots users restored from.
>
> **WAYS AROUND IT**
>
> - Keep the NAS read-only until the first Azure backups succeed, and tell users how restores work now.

> **Watch out:** Once users save work to Azure Files, rolling back means copying changes back to the NAS.
>
> **WAYS AROUND IT**
>
> - Copy back with Robocopy /E /XO, not /MIR, then give the old name back to the NAS.

Turn this phase into dated tasks with the cutover planner

Check your DNS records before and after the change

Show the detailed steps (5) →

You are finished when

- Each share has the same file count and size as the NAS, and the final pass shows no failed items.
- Sample folders show the same permissions with no unresolved SIDs, and test users get the right access.
- Old paths and mapped drives open the Azure file shares, and every listed application still works.
- Every share has a completed backup, and no files on the NAS changed after cutover.

Tools named in this plan are independent third-party products, not endorsed by the platform vendor and not paid placements. Check the tool's own documentation and run a pilot first.

CLICK BY CLICK

What does each step involve?

Open a part when you reach it in the plan. Each step says where to go, what to do and what you should see.

About this migration What it covers, limits at a glance −

Most NAS appliances serve Windows clients over SMB with NTFS-style permissions. Azure Files can take over that role as a managed SMB share, either on its own (cloud-only) or with Azure File Sync caching hot files on a Windows Server in the office (hybrid). The move is mostly a copy job, but three things decide whether users notice: permissions surviving the copy, Kerberos sign-in working against the new share, and the old UNC paths still resolving on cutover day.
This guide follows the order the work is done: inventory, choose cloud-only or hybrid and a copy tool, create the storage, set up identity and share-level

permissions, set root ACLs, seed the data with delta passes, publish the new paths through DFS Namespaces and cut over.
If the files are documents that belong in Microsoft 365 rather than on a mapped drive, the file server to SharePoint guide is the better fit.

CLOUD-ONLY TOOLS MICROSOFT LISTS
Azure Storage Mover, Azure Data Box, or Robocopy to a mounted share

HYBRID (CACHE ON-PREMISES)
Azure File Sync on Windows Server; NAS data is first copied to the server

FIDELITY
Storage Mover, Robocopy and Azure File Sync keep ACLs, timestamps and attributes; AzCopy may lose some

IDENTITY
On-premises AD DS, or Microsoft Entra Kerberos for hybrid identities

NETWORK
SMB needs TCP 445 open from clients to the storage account, or a VPN or ExpressRoute

KEEP THE OLD PATH
DFS Namespaces, including root consolidation to keep \\OldServer\share

1 What you need before step one

Need	Details	Where to get it
Azure roles	Contributor on the storage account and Reader on its resource group to join it to AD DS; Owner or User Access Administrator to assign share-level roles; Contributor on the resource group for Storage Mover or Azure File Sync.	Azure portal (https://portal.azure.com) > Subscriptions > Access control (IAM)
Active Directory rights	An account that can create a computer or service logon account in the target OU (for AD DS authentication) and edit DNS.	Your domain admins
Directory sync	Users and groups synced to Microsoft Entra ID with Entra Connect Sync or Entra Cloud Sync. Needed for granular share-level roles and Entra Kerberos.	Install Entra Connect Sync
NAS admin access	An account that can read every file (backup operator rights or equivalent) and change share permissions on the NAS.	Your NAS management console

Need	Details	Where to get it
Azure PowerShell and AzFiles Hybrid	Az.Storage 8.1.0 or higher, and the AzFilesHybrid module, on a domain-joined Windows PC running PowerShell 5.1.	Install Azure PowerShell; AzFilesHybrid from https://github.com/Azure-Samples/azure-files-samples/releases
Azure CLI (optional)	For creating storage accounts and shares from the command line.	Install the Azure CLI
Copy tool host	Robocopy: a Windows Server 2022 or later machine near the NAS. Storage Mover: a Hyper-V or VMware host for the agent VM. Azure File Sync: a Windows Server 2016 or later with direct-attached storage and the agent from https://aka.ms/AFS/agent.	Your virtualisation platform
Network	TCP 445 from clients to *.file.core.windows.net, or a VPN or ExpressRoute; outbound 443 for Storage Mover and Azure File Sync.	Your firewall and network team
DFS Namespaces server	A domain-joined Windows Server member server (not a domain controller) with the DFS Namespaces role, if you will keep old paths.	Server Manager > Add Roles and Features

2 Inventory the NAS shares

4 steps

1

List shares, size and item counts

Where: The NAS management console (shares list), then PowerShell on a domain-joined admin PC

Export the share list with each share's path and share-level permissions from the NAS console. Then measure size and file count per share from the admin PC and record both in your **Mailbox and data inventory** (one row per share).

```
Get-ChildItem -Path \\nas01\finance -Recurse -File -Force -ErrorAction SilentlyContinue | Measure-Object -Property Length -Sum | Select-Object Count,@{n="GB";e={[math]::Round($_.Sum/1GB,1)}}
```

✓ **You should see:** A row per share with item count and size in GB.

2

Check root and top-level ACLs

Where: Command Prompt on a domain-joined admin PC

Show the ACL on each share root and its first-level folders. Look for entries that are not domain accounts (NAS-local users, unresolved SIDs, Everyone with Full control). Fix them on the NAS by replacing them with domain groups before the copy.

```
icacls \\nas01\finance
icacls \\nas01\finance\*
```

✓ **You should see:** Every entry is a CONTOSO\ domain group or a built-in account such as CREATOR OWNER or SYSTEM.

3

Find who and what uses each share

Where: Group Policy Management (drive mapping preferences), login scripts, and the NAS console (open sessions)

List drive maps, login scripts, applications and scheduled tasks that use each UNC path, and any DFS namespace that already points at the NAS. Record the old path and the owner in your **Application inventory and dependency map**.

✓ **You should see:** Every share has a business owner and a list of the paths and systems that reference it.

4

Map shares to Azure file shares

Where: Your Target-state architecture document

Decide one Azure file share per NAS share where you can, which storage account each goes in (busy shares on their own account), the region close to users, and whether each share is cloud-only or synced with Azure File Sync.

✓ **You should see:** A table of NAS share, target storage account, target share name and access model, signed off by the owner.

3 Create the storage account and shares

3 steps −

1

Create the storage account

Where: Azure portal (https://portal.azure.com) > Storage accounts > Create, or the Azure CLI

Choose the subscription, resource group, a globally unique name and the region from Step 1. Pick the performance and redundancy your owners agreed, and check the vendor's current pricing for that choice. Complete any networking (private endpoint, firewall rules) now, because Microsoft says to configure networking before enabling AD DS authentication.

```
az storage account create --name stcontosofiles --resource-group rg-files --location <region> --kind StorageV2 --sku Standard_ZRS --enable-large-file-share
```

✓ **You should see:** The account shows in Storage accounts with Provisioning state Succeeded.

2

Create the file shares

Where: Azure portal (https://portal.azure.com) > the storage account > Data storage > Classic file shares > + File share, or the Azure CLI

Create one share per row of your mapping table, using lower-case names. Set the quota to the share's size plus growth.

```
az storage share-rm create --resource-group rg-files --storage-account stcontosofiles --name finance --quota 2048
```

✓ **You should see:** Each share appears in the Classic file shares list with its quota.

3

Test SMB connectivity

Where: PowerShell on a PC at each site and on a remote user's PC

Check TCP 445 to the storage account. If it fails, fix the firewall or plan VPN, ExpressRoute or Azure File Sync before going further.

```
Test-NetConnection -ComputerName stcontosofiles.file.core.windows.net -Port 445
```

✓ **You should see:** TcpTestSucceeded : True

4 Set up identity-based access

5 steps

Choose one identity source per storage account: on-premises AD DS for domain-joined clients that reach a domain controller, or Microsoft Entra Kerberos for Entra joined or hybrid joined clients. Both keep existing Windows ACLs.

1

Option A: join the storage account to AD DS

Where: Windows PowerShell 5.1 on a domain-joined PC, signed in as an account that can create computer accounts in the target OU

Download and unzip AzFilesHybrid, run `CopyToPSPath.ps1` from its folder, then run the commands below. `Join-AzStorageAccount` performs the equivalent of an offline domain join and creates a computer account (default) or service logon account for the storage account.

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
.\CopyToPSPath.ps1
Import-Module -Name AzFilesHybrid
Connect-AzAccount
Select-AzSubscription -SubscriptionId "<subscription-id>"
Join-AzStorageAccount -ResourceGroupName "rg-files" -StorageAccountName "stcontosofiles" -
SamAccountName "stcontosofiles" -DomainAccountType "ComputerAccount" -
OrganizationalUnitDistinguishedName "OU=AzureFiles,DC=contoso,DC=com"
Debug-AzStorageAccountAuth -StorageAccountName "stcontosofiles" -ResourceGroupName "rg-files" -
Verbose
```

✓ **You should see:** Debug-AzStorageAccountAuth passes its checks, and (Get-AzStorageAccount -ResourceGroupName rg-files -Name stcontosofiles).AzureFilesIdentityBasedAuth.DirectoryServiceOptions returns AD.

2

Option A: plan the account password

Where: Active Directory Users and Computers (the OU you chose), and your operations calendar

Check the password policy on the OU. Microsoft says you must update the password of the storage account identity in AD DS before the maximum password age, or access to the shares fails. Put the rotation in the operations runbook.

✓ **You should see:** The storage account object is in the OU and a dated password rotation task is in the runbook.

3

Option B: enable Microsoft Entra Kerberos

Where: Azure portal (https://portal.azure.com) > the storage account > Data storage > Classic file shares > Identity-based access

Select the status next to **Identity-based access** (for example **Not configured**). Under **Microsoft Entra Kerberos** select **Set up**, tick **Microsoft Entra Kerberos**, optionally enter the domain name and domain GUID (needed only to set permissions from File Explorer) and select **Save**.

✓ **You should see:** Identity-based access shows Microsoft Entra Kerberos as configured.

4

Option B: grant admin consent and configure clients

Where: Microsoft Entra admin center > App registrations > All applications, then Intune > Devices > Configuration (Settings catalog)

Open the app named **[Storage Account] stcontosofiles.file.core.windows.net**, select **API permissions** > **Grant admin consent for** your directory and confirm. Do not edit this service principal otherwise. Then deploy a Settings catalog policy that sets **Kerberos** > **Cloud Kerberos Ticket Retrieval Enabled** to enabled on the clients; it applies after a policy refresh or reboot.

✓ **You should see:** API permissions shows Granted for your directory, and the policy reports Succeeded on pilot devices.

5

Assign share-level permissions

Where: Azure portal (https://portal.azure.com) > the storage account > Data storage > Classic file shares > Identity-based access, or the Azure CLI

For a default for everyone, under **Step 2: Set share-level permissions** select **Enable permissions for all authenticated users and groups**, choose **Storage File Data SMB Share Contributor** and select **Save**. For granular control, assign roles to synced groups on each share instead. Give migration and IT admins **Storage File Data SMB Share Elevated Contributor** so they can change ACLs.

```
az role assignment create --role "Storage File Data SMB Share Contributor" --assignee-object-id <group-object-id> --assignee-principal-type Group --scope "/subscriptions/<subscription-id>/resourceGroups/rg-files/providers/Microsoft.Storage/storageAccounts/stcontosofiles/fileServices/default/fileshares/finance"
```

✓ **You should see:** The role assignment appears on the share's Access control (IAM) blade. Allow up to 30 minutes, sometimes longer, before testing.

5 Set the root permissions on each share

2 steps −

1

Mount the share with admin access

Where: Command Prompt on a domain-joined Windows PC (not PowerShell, so the drive is visible to File Explorer and icacls)

Microsoft recommends mounting with identity-based access and an admin-level RBAC role. If you must use the storage account key (Storage account > Security + networking > Access keys), use the second form, and keep the key out of scripts and tickets.

```
net use Z: \\stcontosofiles.file.core.windows.net\finance
net use Z: \\stcontosofiles.file.core.windows.net\finance /user:localhost\stcontosofiles <storage-account-key>
```

✓ **You should see:** The command completed successfully, and Z: shows the empty share in File Explorer.

2

Apply the root ACL from the NAS share

Where: Command Prompt on the same PC, with Z: mounted

Match the root permissions of the NAS share. Remove the default `Authenticated Users` Modify entry if the NAS root did not grant it, and grant the share's domain groups. Inheritance then carries these down as files arrive.

```
icacls Z:\
icacls Z:\ /remove "NT AUTHORITY\Authenticated Users"
icacls Z:\ /grant "CONTOSO\Finance-Modify:(OI)(CI)(M)" "CONTOSO\Finance-Read:(OI)(CI)(RX)"
```

✓ **You should see:** icacls Z:\ lists the same domain groups and rights as icacls \\nas01\finance.

Robocopy brings the rest. You only set the root by hand. The copy tools carry the ACLs on every folder and file below it, as long as you use the fidelity switches in Step 5.

6 Seed the data and run delta passes

7 steps

Use 5a (Storage Mover) or 5b (Robocopy) for cloud-only shares, or 5c for hybrid with Azure File Sync. Do not mix tools on the same share.

1

5a. Deploy and register a Storage Mover agent

Where: Azure portal (https://portal.azure.com) > Storage movers > Create; then your Hyper-V or VMware host

Create a Storage Mover resource. Deploy the agent VM on a host close to the NAS from the image linked in Microsoft's agent deployment article, and register it with the Storage Mover resource (Microsoft prefers SSH for the registration). Allow outbound 443 to the endpoints the agent's connectivity checker lists.

✓ **You should see:** The agent appears as registered and online in the Storage mover resource in the portal.

2

5a. Create the endpoints

Where: Azure portal (https://portal.azure.com) > your Storage mover > Storage endpoints > Create endpoint

Store the NAS username and password as two secrets in an Azure Key Vault. Select **Create source endpoint**, choose SMB, enter **Host name or IP** and **Share name**, select the **Key vault** and the **Select secret for username** and **Select secret for password** secrets, then **Create**. Then select **Create target endpoint**, pick the **Subscription**, **Storage account**, a file share **Target type** and the **File share**, and select **Create**.

✓ **You should see:** Both endpoints appear under Storage endpoints, and the source shows the Full source path \\nas01\finance.

3

5a. Create a project and job, and run it

Where: Azure portal (https://portal.azure.com) > your Storage mover > Projects

Create a project per group of shares, then a job definition. On the **Source** and **Target** tabs choose the endpoints, and on the **Settings** tab review the copy mode and migration outcome carefully before you save. Start the job. Rerun it for each delta pass.

✓ **You should see:** Projects > your project > the job > Run history shows the run Succeeded and the Monitoring tab shows no Failed items.

4

5b. Run the initial Robocopy

Where: An elevated Command Prompt or PowerShell on a Windows Server near the NAS, with the target share mounted as Z: (Step 4)

Run Microsoft's recommended command. `/B` needs an elevated window; `/COPY:DATSO` and `/DCOPY:DAT` keep data, attributes, timestamps, NTFS ACLs and owner; `/MIR` mirrors and deletes target items not on the source. Microsoft found 8 to 20 threads gives balanced performance for the first run. Auditing information (`U`) cannot be stored in Azure Files.

```
robocopy \\nas01\finance Z:\ /MT:20 /R:2 /W:1 /B /MIR /IT /COPY:DATSO /DCOPY:DAT /NP /NFL /NDL /XD
"System Volume Information" /UNILOG:C:\migration\finance-pass1.log
```

✓ **You should see:** The summary at the end of finance-pass1.log shows FAILED 0 (or only files that were locked) for Files and Dirs.

5

5b. Run delta passes

Where: The same Windows Server, as a scheduled task

Run the same command nightly with a new log name. Each pass copies only changes. Record the duration of each pass in your runsheet; the last one sets your outage length.

```
robocopy \\nas01\finance Z:\ /MT:20 /R:2 /W:1 /B /MIR /IT /COPY:DATSO /DCOPY:DAT /NP /NFL /NDL /XD "System Volume Information" /UNILOG:C:\migration\finance-pass2.log
```

✓ **You should see:** Later passes finish much faster and copy only the files changed since the previous pass.

6

5c. Set up Azure File Sync (hybrid)

Where: Azure portal (https://portal.azure.com) > Storage Sync Services > Create; then the Windows Server (agent from https://aka.ms/AFS/agent)

Create one Storage Sync Service in the same region as the storage accounts. Install the agent on the Windows Server and register the server. In the Storage Sync Service create a **sync group** per share (the share becomes the cloud endpoint), then **Add server endpoint** with the local folder. If the server has less disk than the NAS data, turn on cloud tiering and set volume free space to 99% during the migration.

✓ **You should see:** The server shows under Registered servers, and each sync group shows a healthy cloud and server endpoint.

7

5c. Copy NAS to the Windows Server

Where: An elevated Command Prompt on the Azure File Sync server

Azure File Sync cannot sync from a NAS directly, so Robocopy the NAS share into the server endpoint folder with the same switches, then run delta passes. If Robocopy stops with Volume full, wait for cloud tiering to free space and rerun.

```
robocopy \\nas01\finance D:\Shares\Finance /MT:20 /R:2 /W:1 /B /MIR /IT /COPY:DATSO /DCOPY:DAT /NP
/NFL /NDL /XD "System Volume Information" /UNILOG:C:\migration\finance-afs-pass1.log
```

✓ **You should see:** The log summary shows no failures and the sync group shows files uploading to the Azure file share.

Match folder structures exactly with /MIR. Robocopy /MIR purges target items that do not exist on the source. Pointing it at the wrong target folder, or renaming top-level folders between passes, causes large deletions and recopies.

7 Publish the new paths with DFS Namespaces

4 steps

1

Choose the namespace type

Where: Your Target-state architecture document

To keep the NAS name (`\\nas01\finance`), use a stand-alone namespace with root consolidation. Otherwise use a domain-based namespace (`\\contoso.com\files\finance`) and update drive maps once. A stand-alone namespace keeps its metadata in the server registry and cannot have a second namespace server, so Microsoft recommends a failover cluster for high availability.

✓ **You should see:** The design records the namespace type, server name and the user-facing path for each share.

2

Install DFS Namespaces

Where: Server Manager on the domain-joined namespace server > Manage > Add Roles and Features

Under **File and Storage Services** > **File and iSCSI Services**, select **DFS Namespaces** and complete the wizard. Do not use a domain controller for a root consolidated namespace.

✓ **You should see:** DFS Management appears under Server Manager > Tools.

3

Enable root consolidation (only if keeping the NAS name)

Where: PowerShell as administrator on the namespace server

Set the registry value Microsoft documents and restart the DFS service. The service reads it only at start-up. The namespace is then named after the old server with a `#` prefix, for example `#nas01`.

```
New-Item -Path "HKLM:SYSTEM\CurrentControlSet\Services\Dfs\Parameters\Replicated" -Force
Set-ItemProperty -Path "HKLM:SYSTEM\CurrentControlSet\Services\Dfs\Parameters\Replicated" -Name
"ServerConsolidationRetry" -Value 1
Restart-Service -Name "Dfs"
```

✓ **You should see:** Get-ItemProperty on the key shows ServerConsolidationRetry 1 and the Dfs service is Running.

4

Create the namespace and folder targets

Where: DFS Management on the namespace server > Namespaces > New Namespace, then the namespace > New Folder

Create the namespace (`#nas01` for root consolidation, or your chosen name). For each share select **New Folder**, use exactly the old share name, select **Add** and enter `\\stcontosofiles.file.core.windows.net\finance`. If the console warns the path cannot be contacted, Microsoft says this is expected; select **Yes**. For a pre-cutover test, add the folders now but do not take over the old name yet.

✓ **You should see:** Each folder lists the Azure file share as its target.

8 Cut over

5 steps

1

Pilot with a few users

Where: Pilot users' PCs, through the DFS path or a direct mapping to the Azure share

Ask pilot users from each team to open, edit and save files, check they cannot reach folders they should not, and open a file from a line-of-business app. Fix permission or sign-in issues before the cutover date.

✓ **You should see:** Pilot sign-off recorded in your Pilot test plan.

2

Remove user access to the NAS

Where: The NAS management console > shares > permissions

At the start of the outage, set the NAS shares to read-only (or change the root ACLs) so no new changes land on the source. Microsoft gives pointing the DFS namespace at a non-existent location or changing root ACLs as examples.

✓ **You should see:** A test user can read but not save a file on \\nas01\finance.

3

Run the final pass

Where: The Robocopy server, the Storage Mover portal job, or the Azure File Sync server

Run one last delta pass and check its log or run history for failures. Its duration is your downtime.

✓ **You should see:** The final pass shows no failed items.

4

Take over the old name (root consolidation)

Where: Command Prompt as administrator on the namespace server, then DNS Manager (dnsmgmt.msc) on a DNS server

Take the NAS off the network or rename it first. Remove its service principal names, add the old name as an alternate computer name of the namespace server with `netdom` (Microsoft says not to hand-build SPNs with setspn instead), then create a CNAME for the old name pointing at the namespace server's FQDN. If you are not keeping the old name, update drive maps in Group Policy to the new path instead.

```
setspn -L nas01
setspn -D HOST/nas01 nas01
netdom computername dfsn01.contoso.com /add:nas01.contoso.com
```

✓ **You should see:** Test-Path -Path "\\nas01\finance" returns True and the folder opens the Azure file share contents.

5

Turn on backup and finish hybrid settings

Where: Azure portal (https://portal.azure.com) > Azure Backup for the file share (a Recovery Services vault), and Storage Sync Services > each sync group

Enable Azure Backup for each share in a Recovery Services vault and run a first backup. For Azure File Sync, change the cloud tiering volume free space back from 99% to your long-term value on every server endpoint on the volume.

✓ **You should see:** Each share shows a successful backup job, and each server endpoint shows the new tiering policy.

WORTH KNOWING

What can go wrong, and how do you avoid it?

The detail behind the plan: options compared, and what experienced engineers check first. Tap any item.

Compare all the ways to do this

4 options –

Azure Storage Mover (cloud-only)

MEDIUM EFFORT

Best for: Many shares or large namespaces moved to cloud-only Azure file shares, managed from the Azure portal

+ Full fidelity for SMB: timestamps, ACLs and attributes
+ Agent VM runs on Hyper-V or VMware near the NAS
+ Projects, job runs and copy logs in the portal; Microsoft says it is tested with 500 million namespace items
– Needs an agent VM, Key Vault for the NAS credentials and outbound 443
– Read the copy mode on the job Settings tab carefully before you start

Read more →

Robocopy to a mounted share (cloud-only)

LOW EFFORT

Best for: Smaller estates, or admins who want a scriptable copy from a Windows machine

+ Built into Windows
+ Full fidelity with /COPY:DATSO and /DCOPY:DAT
+ Repeatable delta passes with /MIR
– Runs over SMB, so it needs port 445 and is slower than Storage Mover's REST-based copy
– /MIR deletes target items if the folder structures do not match
– You run and monitor each job yourself

Read more →

Azure File Sync (hybrid)

MEDIUM EFFORT

Best for: Offices that need LAN-speed access or have slow internet, keeping a Windows Server cache with cloud tiering

+ Users keep a local SMB server; cold files tier to Azure
+ Natively integrated with Azure file shares, full fidelity
+ Avoids opening port 445 to the internet for users
– Cannot sync from a NAS directly: data is copied NAS to Windows Server first
– A Windows Server to patch and back up
– Limits per server and per share to plan around

Read more →

AzCopy

LOW EFFORT

Best for: Data where ACLs do not matter, or one-off copies of specific folders

+ Single executable, fast REST transfers
+ Sync command for deltas
– Microsoft lists it as supported but not fully recommended for Azure Files because some fidelity may be lost
– Microsoft gives a limit of 10 million files per AzCopy job

Read more →

OUR ADVICE

If users will connect to Azure directly and port 445 or a VPN is available, use Storage Mover for anything beyond a handful of shares and Robocopy for small jobs. If offices need local speed or cannot reach Azure on 445, go hybrid with Azure File Sync. For very large data on a slow link, Microsoft also documents Azure Data Box as the seed. Keep AzCopy for data without permissions that matter.

Find ACL entries that belong to the NAS, not the domain

USER IMPACT –

Many NAS appliances let admins grant access to local NAS users and groups. Those security identifiers mean nothing to Azure Files or Active Directory, so after the copy they show as unresolved SIDs and the people who relied on them lose access.

WHAT TO DO

Before you copy, check the root and top-level folders of each share with `icacls` from a domain-joined PC (Step 1). Replace any NAS-local user or group with a

domain group on the NAS itself, then copy. Fixing it on the source means every delta pass carries the correct ACL.

Set the root ACL before the big copy

SAVES TIME

Microsoft advises setting the ACLs for the root directory of a file share before copying a large number of files, because root ACL changes can take a long time to propagate after a large migration.

WHAT TO DO

Mount each new share with admin access and set the root permissions (Step 5) before the first Robocopy or Storage Mover run. Avoid large permission changes on the NAS between delta passes; they cascade down the tree and every changed item is copied again.

Microsoft Learn: Migrate to SMB Azure file shares

Pick the copy tool for fidelity, not familiarity

REDUCES RISK

Microsoft rates Storage Mover, Robocopy, Data Box and Azure File Sync as full fidelity. AzCopy is "supported but not fully recommended" because it uses the REST APIs and some file fidelity might be lost; Storage Explorer loses ACLs and Azure Data Factory does not copy metadata.

WHAT TO DO

Use Storage Mover or Robocopy for a cloud-only target, and Azure File Sync for hybrid. Use AzCopy only for data where ACLs do not matter or after you have tested its `--preserve-permissions` result on a sample folder. See copy files with AzCopy.

Microsoft Learn: Migrate to SMB Azure file shares

Use delta passes so the outage is only the last pass

SAVES TIME

The first copy takes the longest. Later Robocopy runs with `/MIR` copy only what changed, and Microsoft says the final pass after you remove user access is your downtime.

WHAT TO DO

Seed weeks ahead, then run delta passes nightly and note how long each scan takes. Schedule cutover when the last delta fits your outage. Keep source and

target folder structures identical, because `/MIR` deletes target items that are not on the source.

TOOLS THAT CAN GET AROUND THIS

When the seed would take too long over the internet link, Azure Data Box carries the bulk copy offline and Robocopy then catches up only the changes, so the delta passes and the final outage work the same way.

Azure Data Box

Microsoft documents seeding Azure file shares with Data Box Disk, which preserves ACLs, timestamps and attributes, or next-generation Data Box loaded with RoboCopy or the data copy service, then RoboCopy /MIR catch-up passes. Files must be 4 TiB or smaller and Data Box cannot import into NFS shares.

Third-party tools, not endorsed by the platform vendor. Confirm in the tool's documentation and run a pilot first.

Microsoft Learn: Use Robocopy to migrate to Azure file shares

Check port 445 from every site before you design the network

USER IMPACT

SMB needs TCP port 445. Microsoft notes connections fail if it is blocked and that your firewall or ISP may block it. Many home and some business internet services block it outbound, which breaks remote users who are not on the VPN.

WHAT TO DO

Run `Test-NetConnection -ComputerName stcontosofiles.file.core.windows.net -Port 445` from each office and from a remote user. If it fails and you cannot open it, plan a VPN or ExpressRoute connection (and usually a private endpoint), or use Azure File Sync so users reach a local Windows Server.

Microsoft Learn: Mount SMB Azure file share on Windows

Choose AD DS or Entra Kerberos by how your devices are joined

USER IMPACT

Only one identity source can be enabled per storage account. AD DS needs clients with network connectivity to a domain controller. Microsoft Entra Kerberos suits Entra joined or hybrid joined Windows clients, but it does not support MFA for Azure Files access and setting Windows ACLs for hybrid identities still needs connectivity to a domain controller.

WHAT TO DO

If PCs are domain joined and on the corporate network or VPN, use AD DS (Step 4). If they are Entra joined and roam, use Entra Kerberos and set the client policy

`CloudKerberosTicketRetrievalEnabled` . Check the supported Windows builds in Microsoft's article before you choose. Microsoft says Entra Kerberos does not support MFA for Azure Files access, so check how your Conditional Access MFA policies apply to the storage account app before the pilot.

Microsoft Learn: Enable Microsoft Entra Kerberos for hybrid identities on Azure Files

Remember share-level permissions are a second gate

USER IMPACT

Azure Files checks an Azure RBAC role at share level before NTFS ACLs. The default share-level permission is None, so users with perfect NTFS rights still get access denied if no role is assigned. Role changes usually take effect within 30 minutes but can take longer.

WHAT TO DO

Either set a default share-level permission for all authenticated users (typically Storage File Data SMB Share Contributor) and let NTFS ACLs do the real control, or assign roles to synced groups per share. Do this at least a day before pilot users test.

Microsoft Learn: Assign share-level permissions for Azure file shares

Keep the old UNC paths with DFS Namespaces

USER IMPACT

Mapped drives, shortcuts, Office recent files, scripts and line-of-business apps all hold `\\nas01\share` paths. Changing every one is the slowest part of a file migration.

WHAT TO DO

If you already use DFS-N, change the folder targets at cutover. If not, use a stand-alone namespace with root consolidation to answer on the old NAS name, as Microsoft documents (Step 7). The namespace server must be a domain-joined Windows Server, not a domain controller.

Microsoft Learn: How to use DFS Namespaces with Azure Files

Size shares and accounts for the limits, then clean up

COST LEVER

Microsoft documents per-share size limits that depend on the billing model, recommends one busy share per storage account, and for Azure File Sync caps a server at 30 synced shares with a best practice of staying under 20 to 30 million items per share. Old project folders and duplicate copies count towards storage and copy time.

WHAT TO DO

Report size and item count per share (Step 1), archive or delete what nobody needs before the seed, and map large or busy shares to their own storage account. Check the current limits in Microsoft's planning articles and the vendor's current pricing for the billing model you choose.

TOOLS THAT CAN GET AROUND THIS

Instead of building size and age reports per share by hand, a data management tool can analyse the NAS first and show which data is worth moving and where it should land.

Komprise Elastic Data Migration

Komprise analytics show data type, ownership, usage, age and growth per share to decide what goes to Azure Files, Azure Blob Storage or Azure NetApp Files, and it then runs the NAS migration.

Third-party tools, not endorsed by the platform vendor. Confirm in the tool's documentation and run a pilot first.

Microsoft Learn: Migrate from NAS to a hybrid deployment with Azure File Sync

Plan backup and snapshots before go-live

REDUCES RISK

The NAS probably had snapshots users restore from with Previous Versions. Azure file shares have no backup until you configure it, and Microsoft's Storage Mover guidance ends by telling you to enable Azure Backup for the shares.

WHAT TO DO

Configure Azure Backup for each share in a Recovery Services vault before cutover, and tell users how restores work now. Keep the NAS read-only until the first backups have succeeded.

Microsoft Learn: Use Azure Storage Mover to migrate to SMB Azure file shares

FINISH SAFELY

How do you check it worked, or roll back?

Full validation checklist

8 checks

Run these before you declare the migration complete. Record the results in the data validation report.

Check	How to check	What good looks like
File counts and size match per share	Run the Step 1 `Get-ChildItem ... | Measure-Object` command against `\\nas01\finance` and against the mounted Azure share, and read the totals in the final Robocopy log or the Storage Mover Monitoring tab.	Same file count and size, allowing only for files you deliberately excluded.
No failed items in the final pass	Check the summary at the end of the last Robocopy log, or Storage mover > Projects > the job > Run history and Monitoring, or the Azure File Sync sync group health.	FAILED 0 in the Robocopy summary, no Failed items in Storage Mover, and no per-item sync errors.
ACLs match on sample folders	Compare `icacls \\nas01\finance\Payroll` with `icacls Z:\Payroll` for the root and several deep folders per share, including ones with broken inheritance.	Identical entries and no unresolved SIDs.
Users get the right access	Sign in as a test user from each permission group and open, edit and save a file, then try a folder they should not reach.	Allowed actions succeed with no credential prompt; denied folders return Access is denied.
Old paths resolve to the new share	Run `Test-Path -Path "\\nas01\finance"` (root consolidation) or open the domain namespace path, and check a mapped drive and a desktop shortcut on a user PC.	The paths open the Azure file share contents.
Applications and scheduled jobs still work	Run each app and job from the Step 1 dependency list that reads or writes the shares and check its output or log.	Every listed dependency runs without path or permission errors.
Backups run	In the Recovery Services vault, open Backup jobs and check the first job for each share, then restore one file to an alternate location.	Completed backup jobs for every share and a successful test restore.

Check	How to check	What good looks like
The NAS is no longer written to	Check open sessions and recently modified files on the NAS console a day after cutover.	No user sessions and no files modified after the cutover time.

Rollback plan

If it goes wrong

ROLL BACK IF

- Users cannot sign in to the shares and the cause is not fixed inside the outage
- Permission checks show missing or wrong ACLs on a business-critical share
- A key application cannot read or write its files on Azure Files
- Port 445 or VPN connectivity fails for a whole site

POINT OF NO RETURN

Rollback is simple while the NAS is intact and read-only: users go back to it and lose nothing. Once users save work to Azure Files, those changes must be copied back to the NAS before you switch. After the NAS is wiped, returned or its old name is permanently taken over by DFS and the device decommissioned, rollback means a new migration.

1

Stop changes on Azure Files

Where: Azure portal (https://portal.azure.com) > the storage account > Data storage > Classic file shares > Identity-based access (share-level permissions)

Change the default share-level permission to **Storage File Data SMB Share Reader** (or remove group roles) so users can no longer save to the Azure shares.

✓ **You should see:** A test user can open but not save files on the Azure share.

2

Copy back changes made since cutover

Where: An elevated Command Prompt on the Robocopy server, with the Azure share mounted as Z:

Make the NAS share writable for the admin account, then copy new and changed files back. Do not use `/MIR` in this direction unless you are sure, because it deletes NAS files not present in Azure.

```
robocopy Z:\ \\nas01\finance /E /XO /MT:20 /R:2 /W:1 /B /IT /COPY:DATSO /DCOPY:DAT /NP /NFL /NDL
/UNILOG:C:\migration\finance-rollback.log
```

✓ **You should see:** The log summary shows the changed files copied and FAILED 0.

3

Give the old name back to the NAS

Where: Command Prompt on the namespace server, DNS Manager, and the NAS console

Remove the alternate computer name from the namespace server, delete the CNAME for the old name, and bring the NAS back on its original name and address. If you used a domain namespace, point the folder targets back at the NAS shares instead.

```
netdom computername dfsn01.contoso.com /remove:nas01.contoso.com
```

✓ **You should see:** nslookup nas01 returns the NAS address and \\nas01\finance opens the NAS share.

4

Restore NAS write access

Where: The NAS management console > shares > permissions

Set the share permissions back to the values recorded in Step 1 and ask a pilot user to save a test file.

✓ **You should see:** Users can save files on the NAS again.

5

Log the cause and plan again

Where: Your Issue and decision log and Cutover runsheet

Record what failed, keep the Azure shares for diagnosis, and schedule a new cutover after a fresh delta pass.

✓ **You should see:** A recorded root cause and a new cutover date agreed with the share owners.

Agree the triggers and who decides before the go / no-go meeting. Use the rollback plan template.

Common problems and fixes

7 errors

`System error 53 has occurred. The network path was not found.`

Cause: TCP 445 is blocked between the client and *.file.core.windows.net.

Fix: Run Test-NetConnection on port 445, open it on the firewall or use VPN, ExpressRoute, a private endpoint or Azure File Sync.

`Access is denied when mapping the share with a domain account`

Cause: No share-level RBAC role (the default is None) or the role has not propagated yet.

Fix: Assign a Storage File Data SMB Share role or a default share-level permission, wait up to 30 minutes and try again.

`Users prompted for credentials on Entra joined PCs`

Cause: Cloud Kerberos ticket retrieval not enabled on the client, or admin consent not granted for the storage account app.

Fix: Set CloudKerberosTicketRetrievalEnabled through the Settings catalog, reboot, and grant admin consent on the [Storage Account] app.

`Unresolved SIDs in folder permissions after the copy`

Cause: NAS-local users or groups were granted access on the source.

Fix: Replace them with domain groups on the NAS and run another delta pass with /IT so the ACL change is carried over.

`Robocopy ERROR 5 (0x00000005) Access is denied`

Cause: The window is not elevated for /B, or the share was not mounted with admin-level access.

Fix: Run Robocopy elevated and mount the share with an admin-level role or, as Microsoft suggests if errors persist, the storage account key.

`Shares stop working weeks after go-live (AD DS)`

Cause: The password of the storage account identity in AD DS expired.

Fix: Update the password as Microsoft documents and schedule it before the maximum password age.

`DFS folder target warning: path cannot be contacted`

Cause: DFS Management cannot query the Azure file share as a server.

Fix: Microsoft says this is expected for Azure Files targets; select Yes and test access through the namespace.

Search the full error library →

FAQ

Frequently asked questions

What is the best way to migrate a NAS to Azure Files?

For cloud-only shares Microsoft lists Azure Storage Mover, Azure Data Box and Robocopy to a mounted share. For a hybrid set-up with a local cache, copy to a Windows Server and use Azure File Sync.

Do NTFS permissions survive the move?

Yes, with a full-fidelity tool such as Storage Mover, Robocopy with /COPY:DATSO or Azure File Sync, and identity-based access configured so Azure Files can evaluate domain SIDs.

Can Azure File Sync sync directly from my NAS?

No. Microsoft says Azure File Sync does not support NAS locations, so copy the data to direct-attached storage on a Windows Server first.

Can users keep the same \\server\share path?

Yes. A stand-alone DFS namespace with root consolidation can answer on the old server name and redirect to the Azure file share.

Do I need a domain controller for Azure Files?

For AD DS authentication, clients need connectivity to a domain controller. Microsoft Entra Kerberos removes that need for sign-in from Entra joined or hybrid joined clients, but setting ACLs for hybrid identities still needs domain controller connectivity.

Why does AzCopy lose permissions?

AzCopy uses the REST APIs, and Microsoft notes some file fidelity might be lost. Use its preserve options and test, or choose a full-fidelity tool for shares where

permissions matter.

SOURCES

Official sources

12 official pages this guide is based on

Vendors change limits and features, so confirm details on the source before you rely on them. Last checked 4 Nov 2026.

- Microsoft Learn: Migrate to SMB Azure file shares
- Microsoft Learn: Use Azure Storage Mover to migrate to SMB Azure file shares
- Microsoft Learn: Manage Azure Storage Mover endpoints
- Microsoft Learn: Use Robocopy to migrate to Azure file shares
- Microsoft Learn: Migrate from NAS to a hybrid deployment with Azure File Sync
- Microsoft Learn: Overview of AD DS authentication for Azure file shares
- Microsoft Learn: Enable AD DS authentication for Azure file shares
- Microsoft Learn: Enable Microsoft Entra Kerberos for hybrid identities on Azure Files
- Microsoft Learn: Assign share-level permissions for Azure file shares
- Microsoft Learn: Configure directory and file-level permissions for Azure file shares
- Microsoft Learn: How to use DFS Namespaces with Azure Files
- Microsoft Learn: Mount SMB Azure file share on Windows