MIGRATION PLAYBOOK · SERVERS AND CLOUD

How to move a Windows file server to Amazon FSx

Replace an ageing Windows file server with Amazon FSx for Windows File Server. Join FSx to your Active Directory, copy files with permissions intact, recreate the shares, and keep the old server name with a DNS alias so nobody remaps a drive.

Updated 4 Nov 2026 5 phases 10 detailed steps 6 official sources

START HERE

How do you move a Windows file server to Amazon FSx?

SHORT ANSWER

This moves the files and shares from a Windows file server into Amazon FSx for Windows File Server, a file server AWS runs for you. FSx joins your existing Active Directory, so permissions and groups stay the same. You copy the data in advance, recreate the shares, then at cutover stop changes on the old server, copy what changed, and point the old server name at FSx so mapped drives and shortcuts keep working.

- **Recommended route:** AWS DataSync from the existing file server into FSx joined to your own Active Directory, with the old server name as a DNS alias
- **Order:** Network and Active Directory come first, because FSx will not create without them.
- **5 phases:** Plan, Network and directory, Create FSx and copy, Recreate shares and Cut over.
- **You're done when:** Every share is on FSx with the same name and permissions.

RECOMMENDED ROUTE

AWS DataSync from the existing file server into FSx joined to your own Active Directory, with the old server name as a DNS alias

DataSync is what AWS recommends: it copies NTFS permissions and audit settings, runs on a schedule, and a final run catches changes after you stop writes.

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

- **Robocopy from a Windows server**
  : A small server, or you prefer a familiar command-line tool and can run it on a Windows machine near FSx.
- **AWS Managed Microsoft AD instead of your own AD**
  : You have no Active Directory reachable from AWS and are starting fresh.

TOOLS FOR THIS PLAN

Are you ready?
22-question readiness check

Plan your dates
Dated countdown you can add to your calendar

Check your DNS
MX, SPF, DKIM and DMARC lookup

New to the jargon?
Plain-English migration glossary

ORDER TO MIGRATE IN, AND WHY

Network and Active Directory come first, because FSx will not create without them. Copy the bulk of the data early, recreate shares, and keep the final copy and the name switch for a short window.

1. **Inventory of shares, sizes, permissions and the server name people use**
   Sizes decide storage and copy time; the name decides the DNS alias.
2. **Network from the VPC to your domain controllers, and the AD service account**
   FSx must reach writable domain controllers over the listed ports, and needs an account to join the domain.
3. **FSx file system created and joined to the domain**
   Everything else, from the copy to the alias, needs the file system to exist.
4. **Bulk copy with DataSync, repeated on a schedule**
   Running in advance moves most data before cutover, so the final run is short.
5. **Shares recreated on FSx**
   File data and share configuration are separate steps in AWS's plan.

6 Cutover: stop writes, final copy, DNS alias, retire the old server

AWS notes you must pause writes on the source for the final copy to be exact.

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)

- [ ] **Copy tool**

  DataSync or Robocopy.

  ▼ How each tool handles it

  Built-in method AWS recommends DataSync, which copies data and metadata including ownership, timestamps, NTFS ACLs and SACLs, and can run on a schedule. Robocopy with /copy:DATSOU copies data, attributes, timestamps, NTFS ACLs, owner and auditing information.

  Tip: Use DataSync for anything large or busy, because scheduled runs keep the copy close to current until cutover.

  AWS: Migrating existing files to FSx for Windows File Server using AWS DataSync

- [ ] **Active Directory**

  Join your own AD, or use AWS Managed Microsoft AD.

  ▼ How each tool handles it

  Built-in method FSx with self-managed AD: domain functional level Windows Server 2008 R2 or higher, writable domain controllers, at least one global catalog reachable, no single-label domain names, and the VPC subnets defined in an AD site. Single-AZ 2 and Multi-AZ need a domain name of 47 characters or fewer.

  Tip: Create an AD site and subnet for the AWS VPC before creating FSx, so it finds the nearest domain controllers.

  AWS: Using a self-managed Microsoft Active Directory

- [ ] **Service account**

  Which account FSx uses to join the domain.

  ▼ How each tool handles it

Built-in method FSx needs a service account with delegated permissions in the target OU: reset passwords, read and write account restrictions, validated write to DNS host name and service principal name. AWS recommends storing its password in AWS Secrets Manager.

Tip: Create a dedicated OU for FSx and do not move or delete the computer objects FSx creates there.

AWS: Using a self-managed Microsoft Active Directory

- [ ] **Storage type during the copy**

SSD or HDD storage.

▼ How each tool handles it

Built-in method AWS: to migrate quickly, use SSD storage, then move to HDD after migration by backing up and restoring to an HDD file system if HDD suits. HDD file systems have a minimum of 2 TB, and capacity cannot change when restoring from a backup.

Tip: Size the HDD file system correctly before restoring, because the restore cannot resize it.

AWS: Migrating existing file storage to FSx for Windows File Server

- [ ] **Keeping the server name**

Whether users keep the old UNC paths.

▼ How each tool handles it

Built-in method FSx: associate the old name as a DNS alias, formatted as a fully qualified domain name. Up to 50 aliases per file system; an alias becomes available within about 2.5 minutes.

Tip: List every name users and apps use, including old aliases, and add each one.

AWS: Migrating your on-premises DNS configuration to FSx for Windows File Server

- [ ] **Who can copy everything**

Which account runs the copy so locked-down folders are not skipped.

▼ How each tool handles it

Built-in method Robocopy: with /b, the source account must be in Backup Operators (or Domain Admins) and the destination account in the FSx administrators group (Domain Admins or the custom group you set).

Tip: Use a dedicated migration account in both groups, and remove it after cutover.

AWS: Migrating existing files to FSx for Windows File Server using Robocopy

THE PLAN, PHASE BY PHASE

1 Plan Week 1

List shares, sizes, share permissions and the names users connect to.

Choose the AWS region, deployment type and storage size.

Agree a cutover window when nobody needs to change files.

Watch out: Huge numbers of small files make copies slow.

WAYS AROUND IT

- Start the bulk copy early and schedule repeat runs.

Show the detailed steps (1) →

2 Network and directory

Weeks 1 to 2

Connect the VPC to your network with VPN or Direct Connect.

Open the required ports between the VPC and domain controllers.

Create the OU, service account and AD site subnet for FSx.

Watch out: FSx ignores domain controllers with port 389 blocked, and needs at least one reachable global catalog.

WAYS AROUND IT

- Check firewall rules on both sides, and mirror them on the domain controllers.

Show the detailed steps (2) →

3 Create FSx and copy Weeks 2 to 4

Create the FSx file system joined to your domain.

Deploy a DataSync agent, create the SMB source and FSx destination, and run the task.

Schedule the task to repeat until cutover.

Watch out: Without the right privileges, the copy skips folders whose permissions deny the copy account.

WAYS AROUND IT

- Use an account in Backup Operators on the source and the FSx administrators group on the destination.

Show the detailed steps (3) →

4 Recreate shares Week 4

Create each share on FSx with the same name and share permissions.

Test access from a client as a normal user.

Watch out: File data and share settings are migrated separately.

WAYS AROUND IT

- Export share names and permissions from the old server and recreate them on FSx.

Show the detailed steps (2) →

5 Cut over Planned window

Stop writes on

the old server, then run the final DataSync task.

Remove the old server's DNS record and associate its name as an alias on FSx.

Test mapped drives, then shut down the old server after a quiet period.

> ⚠ **Watch out:** Changes made on the old server after the final copy are not on FSx.
>
> **WAYS AROUND IT**

- Make the old shares read-only before the final run.

Turn this phase into dated tasks with the cutover planner

Check your DNS records before and after the change

Show the detailed steps (2) →

You are finished when

- Every share is on FSx with the same name and permissions.
- Users open mapped drives by the old server name and reach FSx.
- The final copy shows no errors, and file counts match the source.
- The old server is read-only or shut down, and backups run on FSx.

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 −

Amazon FSx for Windows File Server is a managed Windows file server in AWS. It joins your Active Directory, serves SMB shares with NTFS permissions, and AWS handles the Windows patching, hardware and backups. AWS sets the migration out in four steps: copy the files, recreate the share configuration, associate the old server name as a DNS alias, then cut over.
AWS recommends DataSync for the copy, run in advance and topped up at cutover; Robocopy works too. If your servers are moving to AWS as well, see VMware to AWS. For Microsoft 365 instead, see file server to SharePoint.

RECOMMENDED COPY TOOL	PERMISSIONS KEPT	IDENTITY
AWS DataSync; Robocopy as an alternative	**NTFS ACLs, owner and auditing (SACL) information**	**Your own Active Directory, or AWS Managed Microsoft AD**
KEEP THE OLD NAME	COPY SPEED TIP	HDD MINIMUM
		2 TB storage capacity

DNS aliases: up to 50 per file system

Migrate onto SSD storage, then move to HDD by backup and restore if you want

1 What do you need before you move a Windows file server to Amazon FSx?

Need	Details	Where to get it
AWS account and VPC	In the region closest to your users.	AWS console
Network link to your domain controllers	VPN, Direct Connect, peering or Transit Gateway, with the FSx ports open.	Your network team
AD service account and OU	Delegated rights to join computers in one OU.	Active Directory Users and Computers
Migration account	In Backup Operators on the source and the FSx administrators group.	Active Directory
Share inventory	Share names, paths, sizes, permissions, and server names in use.	Server Manager on the file server

2 Inventory the file server

1 step

1

List shares and sizes

Where: PowerShell (as administrator) on the existing file server

Export each share with its path and permissions, and note folder sizes. Put the results in the network and DNS worksheet alongside the server names users connect to.

```
Get-SmbShare | Where-Object {$_.Special -eq $false} | Select Name, Path, Description | Export-Csv C:\temp\shares.csv -NoTypeInformation
Get-SmbShare | Where-Object {$_.Special -eq $false} | ForEach-Object { Get-SmbShareAccess -Name $_.Name } | Export-Csv C:\temp\share-access.csv -NoTypeInformation
```

✓ **You should see:** Two CSV files listing shares and their access entries.

3 Prepare the network and Active Directory

2 steps

1

Open the required ports

Where: AWS VPC security groups and network ACLs, and the firewalls in front of your domain controllers

Allow DNS 53, Kerberos 88, 464, LDAP 389 and 636, NTP 123, RPC 135, SMB 445, global catalog 3268 and 3269, WinRM 5985, AD Web Services 9389, and RPC ports 49152 to 65535, plus ICMP. AWS says the same rules must apply on the domain controllers' firewalls.

✓ **You should see:** A test VM in the VPC can resolve and reach a domain controller.

2

Create the OU, service account and AD site subnet

Where: Active Directory Users and Computers, and Active Directory Sites and Services

Create an OU for FSx and a service account, then use Delegate Control on the OU to grant reset passwords, read and write account restrictions, and validated write to DNS host name and service principal name. Add the VPC subnets to an AD site.

✓ **You should see:** The service account has delegated rights on the OU, and the VPC subnets appear in Sites and Services.

4 Create FSx and copy the files

3 steps

1

Create the file system

Where: Amazon FSx console > Create file system > Amazon FSx for Windows File Server

Choose the deployment type and SSD storage for the migration, select the VPC and subnets, and under Windows authentication choose **Self-managed Microsoft Active Directory** with your domain, DNS server IPs, OU and service account.

✓ **You should see:** The file system shows as Available and a computer object appears in the OU.

2

Copy with DataSync

Where: AWS DataSync console

Deploy and activate a DataSync agent near the file server, create an SMB location for the old share using the migration account, create an FSx for Windows location, then create and start a task. Schedule it to repeat until cutover.

✓ **You should see:** The task completes and the files appear on FSx with their permissions.

3

Or copy with Robocopy

Where: Command Prompt on a Windows server near FSx, as the migration account

Map the source share and the FSx share, then run AWS's Robocopy command. Use `/zb` instead of `/b` on slow or unreliable links.

```
robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
```

✓ **You should see:** Robocopy's summary shows files copied and no failures.

5 Recreate the shares

2 steps

1

Create shares on FSx

Where: Shared Folders (fsmgmt.msc) on a Windows machine, connected to the FSx file system's DNS name, as an FSx administrator

Create each share with the same name, path and share permissions as in your export.

✓ **You should see:** Every share from the export exists on FSx.

2

Test access

Where: A user's PC

Open each share by the FSx DNS name as a normal user and check they can read and write only where they should.

✓ **You should see:** Access matches the old server.

6 Cut over and keep the old name

2 steps −

1

Stop writes and run the final copy

Where: The old file server, then the DataSync console

Make the old shares read-only, then run the DataSync task one last time. Follow the cutover runsheet.

✓ **You should see:** The final task completes with no errors.

2

Move the server name to FSx

Where: DNS Manager, then Amazon FSx console > the file system > Network & security > DNS aliases > Manage

Remove the old server's DNS record and rename or shut down the old server, then associate its fully qualified name (for example `files.corp.contoso.com`) as an alias on FSx.

```
aws fsx associate-file-system-aliases --file-system-id fs-0123456789abcdef0 --aliases
files.corp.contoso.com
```

✓ **You should see:** The alias shows as Available, and \\files.corp.contoso.com opens the FSx shares.

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 2 options −

AWS DataSync — MEDIUM EFFORT

Best for: Most file servers, especially large or busy ones

- + Recommended by AWS
- + Copies NTFS ACLs and SACLs
- + Scheduled runs and a short final sync
- – Needs a DataSync agent deployed near the source
- – Another AWS service to set up

Read more →

Robocopy — LOW EFFORT

Best for: Smaller servers and admins who prefer the command line

- + Built into Windows
- + Copies data, ACLs, owner and auditing
- + Restartable mode for poor links
- – You run and re-run it yourself
- – Needs a Windows server near FSx

Read more →

OUR ADVICE

Use DataSync unless the server is small enough to copy in one evening, in which case Robocopy with AWS's flags is simpler. Either way, keep the old server name as a DNS alias.

AWS recommends DataSync

SAVES TIME —

DataSync copies NTFS ACLs and SACLs, runs on a schedule, and a final run after stopping writes makes the destination an exact copy.

WHAT TO DO

Start DataSync runs weeks ahead so the final run is short.

AWS: Migrating existing files to FSx for Windows File Server using AWS DataSync

Active Directory requirements are strict

REDUCES RISK —

FSx needs writable domain controllers, a reachable global catalog, a functional level of Windows Server 2008 R2 or higher, and the VPC subnets in an AD site. Single-label domains are not supported.

WHAT TO DO

Check each requirement before creating the file system; a failure means recreating it.

AWS: Using a self-managed Microsoft Active Directory

Third-party DNS needs manual records

SAVES TIME

FSx only registers its DNS records if you use Microsoft DNS. With third-party DNS you create them yourself after the file system is created.

WHAT TO DO

If your DNS is not Microsoft DNS, add the records for the file system and each alias by hand.

AWS: Using a self-managed Microsoft Active Directory

Keep the old name, avoid remapping

USER IMPACT

Associating the old name as a DNS alias lets users and apps keep the same UNC paths.

WHAT TO DO

List every name in use, including old aliases, and associate each one at cutover.

AWS: Migrating your on-premises DNS configuration to FSx for Windows File Server

Copy onto SSD, settle on HDD later

COST LEVER

AWS suggests SSD for a fast migration, then a backup and restore to HDD. HDD has a 2 TB minimum and restores cannot change capacity.

WHAT TO DO

Decide the final storage type and size before you start, and plan the restore window.

AWS: Migrating existing file storage to FSx for Windows File Server

FINISH SAFELY

How do you check it worked, or roll back?

Full validation checklist

5 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
All files copied	Compare file and folder counts and total size between source and FSx, and read the DataSync task report or Robocopy summary.	Counts match and no errors are reported.
Permissions match	Compare the Security tab on a sample of folders on both sides, and test as a normal user.	Users have the same access as before.
Shares exist with the same names	Compare the share list on FSx with your export.	Every share exists with matching share permissions.
Old name works	From a client, open \\oldname\share and run `nslookup oldname.corp.contoso.com`.	The name resolves to FSx and the share opens.
Backups run on FSx	Check automatic daily backups are enabled on the file system.	A backup completed after cutover.

Rollback plan

If it goes wrong

ROLL BACK IF

- Users cannot reach shares through the old name after cutover
- Permissions are wrong on FSx and cannot be fixed in the window
- The final copy fails or misses data

POINT OF NO RETURN

As long as the old server and its data are unchanged and only read-only, you can go back by restoring its DNS record. Once users have written new files to FSx, going back means copying those files back to the old server.

1

Remove the alias from FSx

Where: Amazon FSx console > the file system > Network & security > DNS aliases > Manage

Disassociate the old server name from FSx.

✓ **You should see:** The alias no longer appears on FSx.

2

Restore the old server

Where: DNS Manager and the old file server

Recreate the old server's DNS record, bring it back online and make its shares writable again.

✓ **You should see:** Users reach the old server by its name.

3

Copy back new files

Where: A Windows server with both shares mapped

Copy any files changed on FSx since cutover back to the old server with Robocopy, preserving permissions.

✓ **You should see:** No work done on FSx is lost.

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

Common problems and fixes

4 errors −

`File system creation fails to join the domain`

Cause: Blocked ports, unreachable or read-only domain controllers, wrong service account rights, or subnets not in an AD site.

Fix: Check the port list, domain controller reachability and the delegated permissions on the OU.

`Copy skips folders with access denied`

Cause: The copy account cannot read or write folders whose ACLs deny it.

Fix: Use an account in Backup Operators on the source and the FSx administrators group, with /b in Robocopy.

`Users cannot open \\oldname after cutover`

Cause: The old DNS record still exists, or the alias is not yet available.

Fix: Remove the old record, check the alias shows Available, and clear client DNS caches.

`FSx name does not resolve`

Cause: Third-party DNS is in use and records were not created.

Fix: Create the DNS records for the file system manually.

Search the full error library →

FAQ

Frequently asked questions

Does Amazon FSx keep NTFS permissions? –

Yes. DataSync copies NTFS ACLs and SACLs, and Robocopy with /copy:DATSOU copies ACLs, owner and auditing information.

Can users keep the same server name? –

Yes. Associate the old fully qualified name as a DNS alias on FSx, up to 50 aliases per file system.

Do I need AWS Managed Microsoft AD?

No. FSx can join your own Active Directory if it is reachable from the VPC and meets AWS's requirements.

Which tool should I use to copy?

AWS recommends DataSync; Robocopy is an alternative.

Can I start on SSD and move to HDD?

Yes, by backing up the SSD file system and restoring it to HDD. HDD needs at least 2 TB, and capacity cannot change on restore.

SOURCES

Official sources

6 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.

- AWS: Migrating existing file storage to Amazon FSx
- AWS: Migrating existing file storage to FSx for Windows File Server
- AWS: Migrating existing files to FSx for Windows File Server using AWS DataSync
- AWS: Migrating existing files to FSx for Windows File Server using Robocopy
- AWS: Using a self-managed Microsoft Active Directory
- AWS: Migrating your on-premises DNS configuration to FSx for Windows File Server