MIGRATION PLAYBOOK · SERVERS AND CLOUD

How to move remote desktops from Remote Desktop Services to Azure Virtual Desktop

Replace your on-premises RDS servers, gateway and broker with Azure Virtual Desktop. Check who is already licensed, build a host pool and a golden image, move user profiles into FSLogix containers, and switch users over a group at a time.

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

START HERE

How do you move remote desktops from Remote Desktop Services to Azure Virtual Desktop?

SHORT ANSWER

This replaces on-premises Remote Desktop Services (RDS) servers with Azure Virtual Desktop, where Microsoft runs the connection services and you run virtual machines in Azure that users sign in to. You build an image with your apps, create a host pool (a group of identical session hosts), copy each user's profile into an FSLogix container file, and move users a group at a time while the old RDS farm keeps running as a fallback.

- **Recommended route:** Pooled host pool of Windows 11 Enterprise multi-session session hosts, FSLogix profiles on Azure Files, joined to your existing Active Directory
- **Order:** Settle licences and identity first, because they decide the operating system and how session hosts join.
- **5 phases:** Assess the RDS farm, Build the foundation, Image and host pool, Profiles and pilot and Move everyone and retire RDS.
- **You're done when:** Every user signs in to AVD with their profile, apps and printers working.

RECOMMENDED ROUTE

Pooled host pool of Windows 11 Enterprise multi-session session hosts, FSLogix profiles on Azure Files, joined to your existing Active Directory

Multi-session cuts the number of VMs, most Microsoft 365 business and enterprise plans already licence it, and keeping AD join means file shares and group policies keep working.

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

- **Windows Server session hosts**
  : An app only supports Windows Server, or you already own RDS CALs with Software Assurance.
- **Personal (persistent) host pool**
  : Users need their own desktop with local admin rights or software installed just for them.
- **Microsoft Entra joined session hosts**
  : You are cloud-only, with no Active Directory, and apps do not need Kerberos to on-premises servers.

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

Settle licences and identity first, because they decide the operating system and how session hosts join. Then build the image and storage, prove it with a pilot group, and move users by group. Keep RDS running until the last group has used AVD for a few weeks.

1. **Inventory of users, apps, printers and peak concurrent sessions on the RDS farm**
   This sizes the host pool and lists everything the image must contain.
2. **Licence and identity decision**
   Windows 11 multi-session needs qualifying Microsoft 365 or Windows licences, Windows Server needs RDS CALs with Software Assurance, and user accounts must

exist in Microsoft Entra ID.

3 **Network, storage and the profile share**

Session hosts need a virtual network in the same region and a route to domain controllers and file shares; FSLogix needs an SMB share with the right permissions.

4 **Golden image and host pool**

Every session host starts from the image, so apps and settings are fixed once rather than per server.

5 **Profiles copied and a pilot group moved**

The pilot shows profile, app and printer problems while only a few people are affected.

6 **Remaining groups moved, then the RDS farm retired**

Group-by-group moves keep the old farm as a fallback until AVD is proven.

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)

- [ ] **Licensing**

  Which operating system the session hosts run, based on what users are already licensed for.

  ▼ How each tool handles it

Built-in method	Azure Virtual Desktop: Windows 11 or 10 Enterprise (including multi-session) for internal users is covered by Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Windows Enterprise E3 or E5, Windows Education A3 or A5, or Windows VDA per user. Windows Server session hosts need RDS CALs with Software Assurance or RDS User Subscription Licences.

  Tip: Check your Microsoft 365 licences first: many businesses already own AVD access rights and only pay for the Azure VMs and storage.

  Microsoft Learn: Prerequisites for Azure Virtual Desktop

- [ ] **Identity and domain join**

  Whether session hosts join Active Directory, Microsoft Entra Domain Services or Microsoft Entra ID.

▼ How each tool handles it

Built-in method Azure Virtual Desktop: users always sign in with Microsoft Entra ID. Session hosts can join AD DS, Microsoft Entra Domain Services or Microsoft Entra ID. With hybrid identities the UPN or SID must match across both. Personal Microsoft accounts are not supported, and the account used to join the domain cannot have MFA.

Tip: Create a dedicated domain join account without MFA and with rights only to join computers to one OU.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

- [ ] **Operating system and VM choices**
Which images and VM options to use.

▼ How each tool handles it

Built-in method Azure Virtual Desktop: 64-bit Windows 11 or 10 Enterprise (single or multi-session) and Windows Server 2016 to 2025. Not supported: 32-bit, N, KN and LTSC editions, ephemeral OS disks, Virtual Machine Scale Sets and Arm64 Azure VMs.

Tip: Start from the Windows 11 Enterprise multi-session image with Microsoft 365 Apps from the Azure gallery and add your apps on top.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

- [ ] **User profiles**
Where profiles live and how existing profiles are moved.

▼ How each tool handles it

Built-in method FSLogix: profile containers on an SMB share, set with the registry values Enabled=1 and VHDLocations (the share path), VHDX recommended. The frx copy-profile command copies a local profile into a VHD or VHDX; for profiles over 5 GB add -size-mbs with a size above 5000.

Tip: Copy only active users' profiles, and let others start fresh with their files on OneDrive or a file share.

Microsoft Learn: frx command-line utility

- [ ] **Applications**
Which apps go in the image and which are delivered separately.

▼ How each tool handles it

Built-in method Azure Virtual Desktop: install Win32, MSIX and Appx apps in the image, or use App Attach to attach MSIX, Appx or App-V packages to a user session from an SMB share, assigned per application per user.

Tip: Put common apps in the image and use App Attach for apps only a few users need, so one image serves everyone.

Microsoft Learn: App Attach overview for Azure Virtual Desktop

- [ ] **Network and latency**

Which Azure region hosts the session hosts, and how they reach on-premises servers.

▼ How each tool handles it

Built-in method Azure Virtual Desktop: users make a reverse connection over TCP 443, so no inbound ports are needed, and Microsoft recommends not opening 3389. The virtual network must be in the session hosts' region, and round-trip latency from users to the region should be under 150 ms.

Tip: For Australian users, use Australia East or Australia Southeast session hosts, and connect the virtual network to the office by VPN for domain controllers and file shares.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

- [ ] **Client apps**

What users install to connect.

▼ How each tool handles it

Built-in method Azure Virtual Desktop: Windows App or the Remote Desktop client on Windows, macOS, iOS, iPadOS, Android and ChromeOS, or a web browser. The built-in Remote Desktop Connection (MSTSC) and RemoteApp and Desktop Connections clients are not supported.

Tip: Deploy Windows App to managed PCs before each group moves, and give users the web client address as a fallback.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

THE PLAN, PHASE BY PHASE

1 Assess the RDS farm Weeks 1 to 2

List users, collections, published apps, printers and peak concurrent sessions.

Record profile type (local, roaming or user profile disks) and size per user.

Check which Microsoft 365 or Windows licences users already have.

> **Watch out:** Apps that only run on Windows Server, or need licence dongles or local hardware.
>
> **WAYS AROUND IT**
>
> - Use Windows Server session hosts for those apps, or keep them on-premises.

Show the detailed steps (2) →

2 Build the foundation

Weeks 2 to 3

- Register the Microsoft.DesktopVirtualization resource provider in the subscription.
- Create a virtual network in the chosen region with a route to domain controllers.
- Create the Azure Files share for FSLogix profiles and set permissions.

> **Watch out:** Session hosts cannot join the domain if they cannot reach a domain controller or DNS.
>
> **WAYS AROUND IT**

- Point the virtual network DNS at your domain controllers, or place a domain controller in Azure.

Show the detailed steps (2) →

3 Image and host pool

Weeks 3 to 4

Build a golden image with Microsoft 365 Apps, FSLogix settings and your apps.

Create a pooled host pool, workspace and desktop application group.

Add session hosts from the image and set up autoscale.

> **Watch out:** Apps that only some users need make the image bigger and harder to update.
>
> **WAYS AROUND IT**
>
> - Deliver those apps with App Attach from an SMB share instead.

Show the detailed steps (2) →

4 Profiles and pilot Week 5

Copy pilot users' profiles into FSLogix containers with frx copy-profile.

Assign the pilot group to the desktop application group.

Have pilot users work in AVD for a full week and

log every problem.

> **Watch out:** Large or corrupt old profiles copy slowly or bring problems with them.
>
> **WAYS AROUND IT**
>
> - Start large or problem profiles fresh, with files kept on OneDrive or a share.

Show the detailed steps (2) →

5 Move everyone and retire RDS

Weeks 6 to 10

Move users group by group, copying profiles the night before.

Install Windows App on their devices and send the connection steps.

After a quiet fortnight, shut down the

RDS servers and remove the gateway from DNS and the firewall.

> **Watch out:** Users who keep using the old RDS farm create profile changes that are not copied.
>
> **WAYS AROUND IT**
>
> - Remove each moved group from the RDS collection on the day it moves.

Check your DNS records before and after the change

Show the detailed steps (2) →

You are finished when

- Every user signs in to AVD with their profile, apps and printers working.
- Autoscale runs, and session hosts are not overloaded at peak.
- No user has signed in to the RDS farm for two weeks.
- RDS servers are shut down, and the RD Gateway is removed from DNS and the firewall.

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 —

Azure Virtual Desktop (AVD) replaces the infrastructure side of Remote Desktop Services. Microsoft runs the gateway, broker and web access parts; you manage only the session host virtual machines and their image. Users connect with Windows App or the Remote Desktop client, and you do not open any inbound ports.

The decisions that shape the project are licensing (many Microsoft 365 plans already include the right to use AVD with Windows 11 multi-session), identity (session hosts joined to your Active Directory or to Microsoft Entra ID), profiles (FSLogix containers), and how apps get to the session hosts. For the file shares your users rely on, see NAS or file server to Azure Files.

WHAT GOES AWAY
The RD Gateway, Connection Broker and Web Access servers: Microsoft runs those parts

SESSION HOST OS
Windows 11 Enterprise multi-session, Windows 11 Enterprise, or Windows Server 2016 to 2025

LICENCES
Windows 11 multi-session: Microsoft 365 E3, E5, Business Premium and similar; Windows Server: RDS CALs with Software Assurance

USER PROFILES
FSLogix profile containers on an SMB share such as Azure Files

NETWORK
No inbound ports; under 150 ms round trip to the Azure region recommended

CLIENTS
Windows App or the Remote Desktop client; not the built-in Remote Desktop Connection (MSTSC)

1 What do you need before you move remote desktops from Remote Desktop Services to Azure Virtual Desktop?

Need	Details	Where to get it
Azure subscription	Contributor or Owner, to register the resource provider and create resources.	Azure portal
Qualifying licences	Microsoft 365 or Windows licences for Windows client hosts, or RDS CALs with Software Assurance for Windows Server.	Microsoft 365 admin center or your licensing partner

Need	Details	Where to get it
Users in Microsoft Entra ID	Synced from AD or cloud-only; personal Microsoft accounts are not supported.	Microsoft Entra admin center
Domain join account	An account without MFA that can join computers to an OU.	Active Directory Users and Computers
Network path to on-premises	VPN or ExpressRoute from the Azure virtual network to domain controllers and file servers.	Your network team or provider
RDS farm inventory	Users, apps, printers, profile sizes and peak sessions.	RD Connection Broker and Server Manager

2 Assess the RDS farm

2 steps

1

List collections, apps and users

Where: Server Manager on the RD Connection Broker > Remote Desktop Services > Collections

For each collection, record the published desktops or RemoteApps, the user groups, and the session hosts. Add each app to the application inventory with its licensing and any hardware it needs.

✓ **You should see:** A list of every app and user group, with notes on special requirements.

2

Measure peak sessions and profile sizes

Where: RD Connection Broker connection reports, and the profile share or local C:\Users folders

Note the highest number of concurrent sessions over a normal week and the size of each user's profile. These size the host pool and decide which profiles to copy.

✓ **You should see:** Peak concurrent users and a profile size per user.

3 Build the network and profile storage

2 steps

1

Register the resource provider

Where: Azure portal > Subscriptions > your subscription > Resource providers

Search for `Microsoft.DesktopVirtualization`, select it and select **Register**.

✓ **You should see:** Status shows Registered.

2

Create the profile share

Where: Azure portal > Storage accounts > Create, then File shares > + File share

Create a storage account in the same region as the session hosts and a file share for profiles. Join it to your Active Directory for identity-based access and set share and NTFS permissions so each user can create and use only their own profile folder.

✓ **You should see:** A share path such as \\storageaccount.file.core.windows.net\profiles that a test user can open.

4 Build the image and host pool

2 steps

1

Build the golden image

Where: An Azure VM created from the Windows 11 Enterprise multi-session image with Microsoft 365 Apps

Install your apps and the FSLogix settings below, apply updates, then capture the VM to an Azure Compute Gallery image.

```
$VHDLocations = "\\storageaccount.file.core.windows.net\profiles"
New-ItemProperty -Path HKLM:\SOFTWARE\FSLogix\Profiles\ -Name Enabled -PropertyType dword -Value 1
-Force
New-ItemProperty -Path HKLM:\SOFTWARE\FSLogix\Profiles\ -Name VHDLocations -PropertyType string -
Value $VHDLocations -Force
New-ItemProperty -Path HKLM:\SOFTWARE\FSLogix\Profiles\ -Name VolumeType -PropertyType string -
Value VHDX -Force
```

✓ **You should see:** An image version in the gallery.

2

Create the host pool

Where: Azure portal > Azure Virtual Desktop > Host pools > Create

Choose **Pooled**, set the load balancing and maximum sessions, add session hosts from your image, join them to your domain OU, and create a workspace with a desktop application group.

✓ **You should see:** Session hosts show as Available in the host pool.

5 Copy profiles and run a pilot

2 steps

1

Copy pilot profiles into FSLogix

Where: An RDS session host where the user's local profile exists, in an elevated Command Prompt, with the user signed out

Run `frx copy-profile` for each pilot user, then copy the VHDX into their folder on the profile share. For profiles over 5 GB add `-size-mbs` above 5000.

```
cd "C:\Program Files\FSLogix\Apps"
frx copy-profile -filename C:\Temp\msmith\Profile_msmith.vhdx -username CONTOSO\msmith -size-mbs
30000
```

✓ **You should see:** A VHDX for each pilot user on the share.

2

Assign the pilot group

Where: Azure portal > Azure Virtual Desktop > Application groups > your desktop group > Assignments

Add the pilot user group. Have them install Windows App and subscribe with their work account. Use the pilot test plan to record results.

✓ **You should see:** Pilot users see the desktop in Windows App and sign in with their old settings.

6 Move everyone and retire RDS

2 steps −

1

Move users by group

Where: AVD application group assignments, and the RDS collection user groups

The evening before each group moves, copy their profiles. On the day, add them to the AVD assignment and remove them from the RDS collection so they cannot use both.

✓ **You should see:** Each group works in AVD and no longer appears in RDS connection reports.

2

Retire the RDS farm

Where: The RDS servers, your public DNS, and the firewall

After two quiet weeks, shut down the session hosts, broker, web access and gateway, remove the gateway DNS record and close its firewall rule. Keep backups for your retention period.

✓ **You should see:** No RDS server is running and the gateway address no longer resolves.

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 3 options −

Pooled Windows 11 multi-session

MEDIUM EFFORT

Best for: Most office users who run the same set of apps

+ Fewer VMs for the same users
+ Often covered by existing Microsoft 365 licences
+ Autoscale reduces cost out of hours
– Users share hosts, so no per-user software installs
– Needs FSLogix profiles

Read more →

Personal desktops

MEDIUM EFFORT

Best for: Developers or power users who need their own machine

+ Each user keeps their own VM
+ Local admin and custom software possible
– One VM per user costs more
– Each VM is patched separately

Read more →

Windows Server session hosts

MEDIUM EFFORT

Best for: Apps that only support Windows Server, with existing RDS CALs and Software Assurance

+ Familiar to RDS admins
+ Uses existing RDS CALs with Software Assurance
– Needs RDS CALs with Software Assurance
– Not available for external users

Read more →

OUR ADVICE

Start with a pooled Windows 11 multi-session host pool for most users, add a small personal pool only for people who genuinely need one, and keep Windows Server hosts for apps that will not run on Windows 11.

You may already own the licences

COST LEVER –

Microsoft 365 E3, E5, Business Premium, F3 and several Windows and education licences include the right to use AVD with Windows client session hosts. Windows Server hosts need RDS CALs with Software Assurance instead.

WHAT TO DO

Check user licences before choosing the operating system; most businesses can use Windows 11 multi-session without new licences.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

Latency decides the experience

PERFORMANCE

Microsoft recommends a round trip under 150 ms from users' networks to the Azure region hosting the session hosts.

WHAT TO DO

Pick the region closest to your users, and test from each office before the pilot.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

No more inbound ports

REDUCES RISK

AVD uses a reverse connection over TCP 443, so you do not open inbound ports, and Microsoft recommends not opening 3389 on session hosts.

WHAT TO DO

Close the old RD Gateway's inbound rule once the last group has moved.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

Old Remote Desktop Connection will not work

USER IMPACT

AVD does not support the built-in Remote Desktop Connection (MSTSC) or the RemoteApp and Desktop Connections client. Users need Windows App, the Remote Desktop client or a browser.

WHAT TO DO

Deploy Windows App before each group moves and include the web address in user instructions.

Microsoft Learn: Prerequisites for Azure Virtual Desktop

Plan the Kerberos encryption change for profile shares

REDUCES RISK

Microsoft warns that a Windows Server update changes the default Kerberos encryption from RC4 to AES-SHA1, and FSLogix shares not upgraded to AES-SHA1 might have access issues.

WHAT TO DO

Configure the profile storage account for AES-SHA1 Kerberos encryption when you set it up.

Microsoft Learn: Create a profile container for a host pool using a file share

Keep one image, and attach the odd apps

SAVES TIME

App Attach delivers MSIX, Appx or App-V packages to a session from a file share, assigned per user, so apps for a few users do not need their own image.

WHAT TO DO

Package rarely used apps for App Attach and keep the image to common apps.

Microsoft Learn: App Attach overview for Azure Virtual Desktop

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
Users sign in with their profile	Sign in as a sample user and check desktop, browser favourites and Outlook settings.	Settings are present and no temporary profile message appears.
Apps and printers work	Users run their main apps and print from AVD during the pilot week.	Every app in the inventory works or has a fix.

Check	How to check	What good looks like
Host pool handles the peak	Check host pool sessions and CPU at the busiest time of day.	Sessions fit within the maximum per host with CPU headroom.
Autoscale works	Check that session hosts start before working hours and stop after.	Hosts follow the schedule.
Nobody still uses RDS	Check RD Connection Broker connection reports for the last two weeks.	No sessions since the last group moved.

Rollback plan

If it goes wrong

ROLL BACK IF

- Users cannot get their profiles or key apps in AVD
- Performance is poor because of latency or undersized hosts
- A group cannot work in AVD on its move day

POINT OF NO RETURN

As long as the RDS farm is running and users are still in its collections, rollback is putting the group back. Once you shut down the RDS servers and remove the gateway, going back means rebuilding them, so keep RDS running until every group has worked in AVD for at least two weeks.

1

Put the group back on RDS

Where: Server Manager > Remote Desktop Services > the collection > User groups

Add the group back to the RDS collection and tell users to use their old connection.

✓ **You should see:** Users sign in to RDS again.

2

Remove the AVD assignment

Where: Azure portal > Azure Virtual Desktop > Application groups > Assignments

Remove the group so it does not use both systems.

✓ **You should see:** The desktop no longer appears in Windows App for that group.

3

Copy back changed files

Where: The user's FSLogix VHDX and OneDrive or file shares

Files saved to OneDrive or shares are unaffected. Help users move anything saved only inside their AVD profile.

✓ **You should see:** No user loses work from their time in AVD.

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

Common problems and fixes

5 errors

`Session hosts fail to join the domain`

Cause: The domain join account has MFA, or the virtual network cannot reach a domain controller or DNS.

Fix: Use an account without MFA, and point the virtual network DNS at your domain controllers.

`Users get a temporary profile`

Cause: FSLogix cannot open the profile share: wrong path, permissions, or Kerberos settings.

Fix: Check VHDLocations, share and NTFS permissions, and the storage account's identity-based access.

`User cannot see the desktop`

Cause: The user is not assigned to the application group, or is signing in with a personal Microsoft account.

Fix: Assign the user's work account to the desktop application group.

`Connection fails from Remote Desktop Connection`

Cause: The built-in MSTSC client is not supported for AVD.

Fix: Install Windows App or use the web client.

`frx copy-profile fails for a large profile`

Cause: Profiles over 5 GB need a larger disk size.

Fix: Add -size-mbs with a value above 5000.

Search the full error library →

FAQ

Frequently asked questions

Do I still need RD Gateway and Connection Broker servers?

No. Microsoft runs the gateway, broker and web access parts of Azure Virtual Desktop; you manage the session hosts.

Which licences cover Azure Virtual Desktop?

For Windows 11 or 10 Enterprise session hosts, Microsoft 365 E3, E5, A3, A5, F3, Business Premium and Windows Enterprise or VDA licences, among others. Windows Server hosts need RDS CALs with Software Assurance.

Can users keep their existing profiles?

Yes. FSLogix frx copy-profile copies a local profile into a VHDX profile container.

Do I need to open port 3389?

No. Users connect through a reverse connection over TCP 443, and Microsoft recommends not opening 3389.

Can session hosts stay joined to our Active Directory?

Yes. Session hosts can join AD DS, Microsoft Entra Domain Services or Microsoft Entra ID, while users always authenticate with Microsoft Entra ID.

SOURCES

Official sources

5 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: Prerequisites for Azure Virtual Desktop
- Microsoft Learn: Move on-premises Remote Desktop Services to Azure Virtual Desk...
- Microsoft Learn: Create a profile container for a host pool using a file share
- Microsoft Learn: frx command-line utility
- Microsoft Learn: App Attach overview for Azure Virtual Desktop