MIGRATION PLAYBOOK · AZURE

Azure migration: how to move servers, databases and files to Azure

A start-to-finish plan for moving on-premises workloads to Azure: assess, choose a route for each workload, build the landing zone, connect network and identity, replicate, test, cut over and optimise.

Updated 4 Nov 2026 7 phases 33 detailed steps 12 official sources

START HERE

How does an Azure migration work?

SHORT ANSWER

This moves on-premises workloads into Azure in planned waves. Azure Migrate (Microsoft's migration hub) discovers your servers, databases and web apps, checks readiness and suggests sizes. You then pick a route for each workload: rehost (lift and shift) servers to Azure VMs, move SQL Server databases to Azure SQL, move file shares to Azure Files, and move suitable web apps to App Service.

- **Recommended route:** Azure Migrate assessment, then rehost servers and replatform databases, files and web apps where it is low effort
- **Order:** Assess first, build the foundation second, and move workloads last in small waves, simple and non-production systems before critical ones.
- **7 phases:** Assess, Build the landing zone, Connect network and identity, Pilot, Migrate in waves, Cut over and Optimise and clean up.
- **You're done when:** Every workload in the wave plan is migrated, retired or recorded as retained, with owner sign-off.

The time depends on how many workloads you have, how long you collect performance data and how fast your link to Azure is. The copies run in the background; each outage is only the final switch.

RECOMMENDED ROUTE

Azure Migrate assessment, then rehost servers and replatform databases, files and web apps where it is low effort

One Microsoft project covers discovery, sizing, cost and server replication, and rehosting is the lowest-risk way to leave a data centre. Managed services remove patching work where the change is small.

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

- **Rehost everything to Azure VMs, modernise later**
  : You have a hard deadline such as a data centre exit or hardware end of life, and little time for testing application changes.
- **Azure VMware Solution**
  : You must keep vSphere, vCenter tooling or VMware-only appliances, or need to move faster than you can convert VMs.
- **A migration partner or a third-party tool listed by Microsoft**
  : You lack in-house Azure skills, or need features outside Azure Migrate. Partner tools may charge for their services.

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

Assess first, build the foundation second, and move workloads last in small waves, simple and non-production systems before critical ones. Each step depends on the one before: sizing needs performance data, and a migrated server only works if the network, DNS and sign-in it depends on already exist in Azure.

1 **Discovery and assessment in an Azure Migrate project**
Readiness, size and dependencies decide the route and the wave for every workload. Without them every later step is a guess.

2 **Business case and route per workload (rehost, replatform, retire, replace, retain)**
Retiring or replacing workloads early means less to copy, test and pay for.

3 **Landing zone: subscriptions, policies, budgets and admin access**

Microsoft says to set subscription boundaries before workloads move. Moving resources between subscriptions later is extra work.

4 **Hybrid network, DNS and identity reachable from Azure**

Microsoft calls hybrid connectivity one of the few prerequisites that can block every workload at once. Servers also need DNS and domain sign-in after cutover.

5 **Pilot: development, test and low-risk internal workloads**

Microsoft recommends non-production and low-complexity workloads first, to prove the process before production.

6 **Production waves, each application with its servers, databases and shares together**

Microsoft warns that dependent workloads cause outages if they are not migrated together.

7 **Critical systems last, then optimisation and decommissioning**

Critical systems move once the team has proven the method. Source servers go only after the rollback window closes.

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)

- [ ] **Route for each workload**

  Whether each workload is retired, rehosted, replatformed, refactored, rearchitected, rebuilt, replaced or retained.

  ▼ How each tool handles it

Built-in method	Azure Migrate assessment: reports readiness and recommended targets for servers (Azure VMs), SQL Server (Azure SQL Database, Managed Instance or SQL Server on Azure VMs) and web apps (App Service, Azure Spring Apps or AKS). The business case maps workloads to migration strategies. It does not decide for you.

  Tip: Record the route and the reason for each workload in a 7R decision matrix, and get the application owner to agree it.

  Microsoft Learn: Select your cloud migration strategies

- [ ] **Sizing method and buffer**

Whether Azure sizes come from real usage (performance-based) or from what each server has allocated today (as-is), and how much buffer to add.

▼ **How each tool handles it**

Built-in method	Azure Migrate assessment: offers as-is or performance-based sizing. The comfort factor adds a buffer to CPU, memory, disk and network sizing. Microsoft's example: a 10-core VM at 20% use normally becomes a 2-core VM, or 4 cores with a comfort factor of 2.0.

Tip: Collect performance data over a full business cycle, including month-end, before you trust a performance-based size.

Microsoft Learn: Azure Migrate assessment overview

- [ ] **Project geography and target region**

Where Azure Migrate stores its discovery records, and which Azure region each workload lands in.

▼ **How each tool handles it**

Built-in method	Azure Migrate: the project geography stores discovered metadata only, and you can migrate to other regions. For agent-based (physical) migration, the target region cannot be changed after you select Create resources, and all later migrations in that project go to that region.

Tip: Agree the region against your data residency rules first, and use a separate project for a second region.

Microsoft Learn: Migrate machines as physical servers to Azure

- [ ] **Network link to Azure**

Whether your sites connect to Azure over VPN Gateway (an encrypted tunnel over the internet) or ExpressRoute (a private circuit from a connectivity provider).

▼ **How each tool handles it**

Built-in method	Microsoft: choose on throughput, latency, compliance, lead time and routing, not on how new you are to Azure. VPN Gateway is often the fastest path; avoid the Basic SKU for production migrations. ExpressRoute depends on a provider and can take weeks or months.

Tip: If ExpressRoute will not be ready in time, start with VPN Gateway and keep it as the backup path later.

Microsoft Learn: Azure landing zones for on-premises experts

Sign-in and domain controllers

Whether migrated servers still need Active Directory (for Kerberos, LDAP or Group Policy) and where their domain controllers live.

▼ How each tool handles it

Built-in method	Microsoft: workloads that need LDAP, Kerberos or Group Policy need an early decision on domain controllers or Active Directory sites in Azure before cutover. Admins need Microsoft Entra ID groups and an emergency access path first.

Tip: Test domain sign-in from a VM in the Azure network during the pilot, before any production wave.

Microsoft Learn: Azure landing zones for on-premises experts

Disks Azure Migrate cannot copy

Which servers need agent-based replication or a separate data move because of how their disks are attached.

▼ How each tool handles it

Built-in method	Azure Migrate agentless (VMware): independent disks and iSCSI targets are not supported, and RDM (raw device) or passthrough disks are not replicated. Encrypted disks, shared disk clusters and NFS volumes mounted inside the guest are not supported by agentless or agent-based. Hyper-V: passthrough, shared, FC and iSCSI disks are not supported, and BitLocker must be turned off first.
Azure Migrate agent-based migration (VMware)	Supports independent disks, passthrough disks and iSCSI targets, up to 63 disks per VM. Needs a replication appliance and the Mobility service on each VM.

Tip: Add disk type, encryption and clustering columns to the inventory and flag servers before you plan waves.

Microsoft Learn: Support for Hyper-V migration

Disk sizes

Which disks are too large to move as they are.

▼ How each tool handles it

Built-in method	Azure Migrate (VMware agentless and agent-based, and Hyper-V): OS disks up to 2 TB for Generation 1 VMs and data disks up to 32 TB. Generation 2 OS disks up to 4 TB, but Microsoft's Hyper-V page also lists 2,048 GB, so

check before you rely on it. Hyper-V: up to 16 disks per VM.

Tip: Shrink or split oversized disks, or move that data separately, before the server's wave.

Microsoft Learn: Support for Hyper-V migration

- [ ] **SQL Server target and copy method**

Whether each database goes to Azure SQL Database, Azure SQL Managed Instance or SQL Server on an Azure VM, and whether the copy must stay in sync (online) or can be a one-time copy (offline).

▼ **How each tool handles it**

Built-in method	Azure Database Migration Service: offline only to Azure SQL Database; online or offline to Managed Instance and SQL Server on Azure VMs. Managed Instance link (needs Azure Arc on the SQL Server): replicates in near real time, so downtime is the final cutover only.

Tip: Use the decision helper and the SQL Server playbook for each instance; logins and SQL Agent jobs need separate handling.

Microsoft Learn: Migrate from SQL Server overview

- [ ] **File permissions, timestamps and attributes**

Which copy tool keeps NTFS permissions (ACLs), timestamps and attributes for each share.

▼ **How each tool handles it**

Built-in method	Microsoft rates Azure File Sync, Azure Storage Mover, Robocopy and Azure Data Box as full fidelity for Azure file shares. AzCopy may lose some fidelity and is limited to 10 million files per job. Azure Files cannot store alternate data streams, and LastAccessTime always equals CreationTime.
Azure Storage Mover	Keeps folder structure, timestamps, ACLs and attributes for SMB shares, and re-runs copy only what changed.

Tip: Set the permissions on the root of each Azure file share before the bulk copy; Microsoft warns root changes made afterwards can take a long time.

Microsoft Learn: Migration overview for SMB Azure file shares

- [ ] **Keep a local file server or not**

Whether users keep a local cache of the shares (hybrid) or use Azure file shares directly (cloud-only).

▼ **How each tool handles it**

Built-in method	Azure File Sync: syncs a Windows Server 2016 or later NTFS volume to an Azure file share and can tier cold files to the cloud. It skips hard links, symbolic links and junctions, never syncs files such as thumbs.db or *.tmp, and Microsoft says databases are not a good workload for it.
Azure Storage Mover	Copies straight from NAS or Linux SMB 2 and 3 shares, and NFS 3 and 4 shares, to Azure Files when there is no Windows server to run Azure File Sync.

Tip: Keep around 20 to 30 million items or fewer per share, as Microsoft suggests for Azure File Sync.

Microsoft Learn: Plan an Azure File Sync deployment

☐ **Windows Server licences**

Which VMs use Azure Hybrid Benefit (reusing Windows Server licences you already own) and how many core licences each needs.

▼ **How each tool handles it**

Built-in method	Azure Hybrid Benefit: needs core licences with active Software Assurance or qualifying subscription licences, and at least 8 core licences per VM. Standard licences can run on-premises and in Azure at the same time only once, for up to 180 days, while you migrate.

Tip: Count licences with your licensing partner before you tick Azure Hybrid Benefit in Azure Migrate.

Microsoft Learn: Azure Hybrid Benefit for Windows Server

☐ **Old operating systems**

Which servers to upgrade, rebuild or cover with Extended Security Updates (ESU: paid security-only patches after end of support).

▼ **How each tool handles it**

Built-in method	Windows Server 2016 reaches end of support on 12 January 2027. ESU for it can be set up through Azure Arc, with billing from 13 January 2027. Microsoft says Azure VMware Solution machines and VMs on Azure Local are

eligible for free ESU and should not enrol through Azure Arc.

Tip: Flag every 2016 server in the assessment and decide its path before you place it in a wave.

Microsoft Learn: Prepare to deliver ESUs through Azure Arc

- [ ] **Rollback window**

How long each wave keeps the source systems intact before you complete the migration and decommission.

▼ **How each tool handles it**

Built-in method	Microsoft: set rollback criteria and procedures before any migration starts, test rollback in a non-production environment, and get written approval from stakeholders for the plan and the rollback procedure.

Tip: Write the rollback triggers into the cutover runsheet and name who can call a rollback.

Microsoft Learn: Plan your migration

THE PLAN, PHASE BY PHASE

1 Assess — Over a full business cycle

- [ ] Create an Azure Migrate project in the geography that suits your data residency rules.
- [ ] Deploy the Azure Migrate

appliance (a discovery VM) and let it collect performance and dependency data.

Create assessments for servers, SQL Server and web apps, then a business case.

Pick a route for every workload: retire, rehost, replatform, replace or retain.

Group dependent workloads

into waves, with development and test systems first.

> **Watch out:** Azure Migrate appliance: one appliance discovers up to 10,000 VMware servers, 5,000 Hyper-V servers or 1,000 physical servers, and registers with one project only.
>
> **WAYS AROUND IT**
>
> - Deploy more appliances in the same project for larger estates.

> **Watch out:** Azure Migrate business case: available in public cloud regions only, not Azure Government.
>
> **WAYS AROUND IT**
>
> - In Azure Government, use the assessments for size and cost estimates instead.

Show the detailed steps (5) →

2 Build the landing zone

Before the pilot

Decide your subscriptions and management groups (folders for subscriptions), keeping shared services separate from workloads.

- Deploy a landing zone, starting from a Microsoft accelerator where you can.
- Apply a small policy baseline: allowed regions, no unmanaged public exposure, central logging.
- Set budgets and cost alerts with a named owner.

Show the detailed steps (3) →

3 Connect network and identity

- Connect your sites

to Azure with VPN Gateway or ExpressRoute, avoiding the Basic VPN SKU for production.

Check Azure address ranges do not overlap your on-premises ranges.

Make on-premises names and Azure private DNS zones resolve from an Azure test network.

Decide whether migrated servers need domain controllers in Azure, and set up admin groups in Entra ID.

> **Watch out:** ExpressRoute depends on a connectivity provider, and Microsoft says to plan in weeks or months.
>
> **WAYS AROUND IT**
>
> - Start with VPN Gateway and keep it as the backup path once ExpressRoute is live.

Check your DNS records before and after the change

Show the detailed steps (4) →

4 Pilot

Replicate one or two low-risk servers, plus one database and one

share, from the first wave.

Run a test migration into an isolated test network and check each application works.

Record copy times over your link and every fix needed, then update the wave plan.

> **Watch out:** Azure Migrate agentless replication (VMware) does not copy RDM, passthrough or independent disks, or in-guest iSCSI targets.
>
> **WAYS AROUND IT**
>
> - Test-migrate every flagged server and check each volume is there.
>
> **TOOLS THAT CAN DO IT**

Azure Migrate agent-based migration (VMware)
Supports independent disks, passthrough disks and iSCSI targets. Needs a replication appliance and the Mobility service on each VM.

Show the detailed steps (3) →

5 Migrate in waves

Servers: replicate with Azure Migrate, using agentless for VMware, the host provider for Hyper-V, and agent-based for physical servers.

Databases: copy SQL Server with Managed Instance link, Azure Database Migration Service

or backup and restore.

File shares: copy to Azure Files with Azure File Sync, Storage Mover or Robocopy, then run top-up copies.

Web apps: move ASP.NET apps to App Service with Azure Migrate or the App Service Migration Assistant.

Tick Azure Hybrid Benefit only for servers covered by eligible licences.

Watch out: Azure Migrate: you select up to 10 machines at a time for replication (stated for Hyper-V).

WAYS AROUND IT

- Split each wave into batches of 10 in the wave plan.

Watch out: AzCopy may lose some file fidelity because it uses the Azure Files REST API, and handles up to 10 million files per job.

WAYS AROUND IT

- Use AzCopy for small or simple shares only, and check permissions after the copy.

TOOLS THAT CAN DO IT

Azure Storage Mover
Full-fidelity SMB copies with ACLs, timestamps and attributes; re-runs copy only changes.

Watch out: Azure Database Migration Service: migration to Azure SQL Database is offline only, so writes stop for the whole copy.

WAYS AROUND IT

- Choose Azure SQL Managed Instance with Managed Instance link if the database cannot stop for long.

Show the detailed steps (3) →

6 Cut over

In each planned change window

Lower DNS TTLs

(how long other systems cache a record) a few days before.

Stop the application, run the final copy and start the Azure copy.

Point DNS, connection strings, drive mappings and firewall rules at Azure.

Run acceptance tests with each owner

and record sign-off or roll back.

> **Watch out:** Azure Migrate (servers): migrated VMs take new private IP addresses, so hard-coded IPs and cached DNS keep clients on the old server.
>
> **WAYS AROUND IT**
>
> - Search application settings for IP addresses during the test migration, and lower TTLs first.

Turn this phase into dated tasks with the cutover planner

Show the detailed steps (3) →

7 Optimise and clean up

After the rollback window

Complete the migration in Azure Migrate so replication stops.

Turn on backup, update management and Defender for Cloud for every

migrated workload.

Review Azure Advisor cost recommendations and resize or shut down idle VMs.

Decommission the source servers and update your documentation.

> **Watch out:** Azure Advisor: looks at 7 days of data by default, so a new VM's resize advice can miss month-end peaks.
>
> **WAYS AROUND IT**
>
> - Change the lookback period to 30, 60 or 90 days before you act on resize advice.

Show the detailed steps (3) →

You are finished when

- Every workload in the wave plan is migrated, retired or recorded as retained, with owner sign-off.
- Applications work from Azure, and names, drive mappings and connection strings point at Azure.
- Every migrated workload has backup, updates and security monitoring, and a budget with alerts.

- Source servers are off, no client still connects to them, and replication is completed.

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 —

An Azure migration moves the servers, databases, file shares and web apps you run on your own hardware into Microsoft Azure. Most organisations do not move everything the same way. Some servers are rehosted (lift and shift: copied to Azure virtual machines with as few changes as possible). Others are replatformed onto services Microsoft runs for you, such as Azure SQL Managed Instance, Azure Files and Azure App Service. Some are retired, replaced by software as a service, or kept where they are.

Azure Migrate is the starting point. It finds what you have, checks whether each workload is ready for Azure, suggests sizes and estimated running costs, builds a business case and then copies servers across. Before anything moves, you build a landing zone (the governed Azure foundation of subscriptions, policies, networks and access that workloads land in) and connect it to your network and directory.

This page is the hub. Each workload type has a deeper playbook: VMware, Hyper-V and physical servers to Azure, SQL Server to Azure SQL, NAS and file servers to Azure Files and Active Directory to Microsoft Entra ID. Still choosing a cloud? See cloud platforms compared.

HUB TOOL	SERVERS	SQL SERVER
Azure Migrate: discovery, assessment, business case and migration in	**VMware: agentless replication. Hyper-V: provider on each host. Physical, other**	**Azure SQL Database, Azure SQL Managed Instance or SQL Server on an Azure VM, using**

one project (Microsoft says the service itself is free; partner tools may charge)

hypervisors and other clouds: agent-based with a replication appliance

Managed Instance link, Azure Database Migration Service or backup and restore

FILE SHARES

Azure Files, with Azure File Sync, Azure Storage Mover, Robocopy, Azure Data Box or AzCopy

WEB APPS

ASP.NET apps to Azure App Service with Azure Migrate or the App Service Migration Assistant

FOUNDATION

An Azure landing zone from the Cloud Adoption Framework, connected by VPN Gateway or ExpressRoute

1 What you need before step one

Need	Details	Where to get it
Azure subscription and roles	Owner or Contributor on the subscription that holds the Azure Migrate project, plus rights to create networks and resource groups.	Azure portal, https://portal.azure.com
Admin access to the sources	vCenter, Hyper-V host or server admin credentials for discovery, SQL Server credentials for SQL discovery, and share-level admin on file servers or NAS.	Your hypervisor, server and NAS consoles
Appliance machine	A VM or server for the Azure Migrate appliance. Microsoft lists 32 GB RAM, 8 vCPUs and about 80 GB of disk for VMware and physical, with internet access.	Set up the Azure Migrate appliance
Azure CLI (optional)	For the network, storage and Advisor commands in this guide. Azure Cloud Shell in the portal already has it.	Install the Azure CLI
AzCopy (optional)	For small file copies to Azure Files or Blob storage.	Copy files with AzCopy

Need	Details	Where to get it
Licence records	Windows Server and SQL Server licences, with Software Assurance or subscription status, for Azure Hybrid Benefit.	Your licensing partner or Microsoft licensing portal
Templates	Application inventory and dependency map, Workload 7R decision matrix, Business case and ROI, Migration wave plan, Network and DNS worksheet, Cutover runsheet.	Templates linked at the end of this guide

2 Discover and assess with Azure Migrate

5 steps

Azure Migrate discovery is agentless: you install nothing on the servers. One appliance collects configuration, performance, installed software, SQL Server and dependency data and sends it to your project.

1

Create the project

Where: Azure portal (https://portal.azure.com) > search Azure Migrate > Get started

Create a project in a resource group, and choose the geography where its discovered metadata is stored. Microsoft says the geography is only for metadata: you can still assess and migrate to other regions. Full steps are in set up the Azure Migrate appliance.

✓ **You should see:** The project opens with Azure Migrate: Discovery and assessment available.

2

Deploy the appliance and start discovery

Where: Azure Migrate project > Discover, then vSphere Client, a Hyper-V host or a Windows Server 2022/2025 machine, then https://appliance-name-or-IP-address:44368

Download the OVA (VMware), VHD (Hyper-V) or PowerShell installer (physical and other clouds). Register the appliance with the project key, add credentials for vCenter, hosts or servers, and add SQL Server credentials so databases are discovered too. Select **Start discovery**. One appliance discovers up to 10,000 VMware servers, 5,000 Hyper-V servers or 1,000 physical servers.

✓ **You should see:** Discovered servers, SQL Server instances and (for VMware and physical) ASP.NET web apps appear in the project.

3

Let performance data build up

Where: The appliance (leave it running) and the project in the Azure portal

Leave the appliance running over a representative period, including month-end or seasonal peaks. Assessments are a point-in-time snapshot, and performance-based sizing is only as good as the data behind it.

✓ **You should see:** Servers show performance data and the appliance stays connected.

4

Create assessments

Where: Azure Migrate project > Infrastructure tab > select workloads > Create assessment

Assess servers for Azure VMs, SQL Server for Azure SQL targets and web apps for App Service. Choose the target region, sizing (performance-based or as-is) and comfort factor (a buffer for peaks and growth). Microsoft calculates readiness first: a server that fails readiness is marked unsuitable and gets no size or cost.

✓ **You should see:** Each assessment lists readiness, a recommended size and an estimated monthly cost per workload.

5

Map dependencies

Where: Azure Migrate project > dependency analysis for the discovered servers

Use agentless dependency analysis to see which servers talk to each other. Microsoft says dependent workloads cause outages if they are not migrated together, and to group them when in doubt.

✓ **You should see:** Every server is assigned to an application group in your dependency map.

Discovery covers files too. Microsoft says Azure Migrate can also discover SMB and NFS shares on Windows and Linux servers and rate them ready, ready with conditions or not ready.

3 Build the business case and choose a route per workload

3 steps

Workload	Common route	Tool	Deeper guide
VMware VMs	Rehost to Azure VMs	Azure Migrate agentless replication	VMware to Azure
Hyper-V VMs	Rehost to Azure VMs	Azure Migrate with the Hyper-V Replication provider on each host	VMware to Azure (Hyper-V section)
Physical servers, Xen, KVM, AWS or Google Cloud VMs	Rehost to Azure VMs	Azure Migrate agent-based replication with a replication appliance	VMware to Azure (physical section)
SQL Server	Replatform to Azure SQL Managed Instance or Azure SQL Database, or rehost to SQL Server on an Azure VM	Managed Instance link, Azure Database Migration Service, backup and restore	SQL Server to Azure SQL
File servers and NAS shares	Replatform to Azure Files, optionally with a local cache	Azure File Sync, Azure Storage Mover, Robocopy, Azure Data Box, AzCopy	NAS to Azure Files
ASP.NET web apps on IIS	Replatform to Azure App Service	Azure Migrate web app migration or App Service Migration Assistant	This guide, step 8
Windows Server 2016 servers	Upgrade during or before the move, or cover with ESU	Azure Migrate, in-place upgrade, Azure Arc ESU	Windows Server 2016 end of support

Workload	Common route	Tool	Deeper guide
Active Directory	Keep domain controllers for legacy apps; move users and devices to Entra ID over time	Entra Connect, domain controllers on Azure VMs	Active Directory to Entra ID

1

Build the business case

Where: Azure Migrate project > Business case (preview) > Build business case

Choose **Modernize with PaaS** (prefers managed services) or **Migrate to all IaaS** (lift and shift). The business case compares on-premises and Azure total cost of ownership over several years and includes savings from Azure Hybrid Benefit and Extended Security Updates. Many on-premises costs are Microsoft defaults; replace them with your real figures in the assumptions. Check the vendor's current pricing for anything you quote.

✓ **You should see:** A business case with cost comparison, cash flow, support status of your operating systems and databases, and suggested quick wins.

2

Pick a route for each workload

Where: Your Workload 7R decision matrix, using the assessments and business case

Microsoft's strategies are: retire (switch off), rehost (move with minimal changes), replatform (move to a managed platform with minimal code changes), refactor, rearchitect, rebuild, replace (with software as a service) and retain (leave as is). Use the table below for the common routes, and the decision helpers for which Azure SQL target and which VMware exit path.

✓ **You should see:** Every workload has one route, a target service and an owner who agreed it.

3

Plan waves

Where: Your Migration wave plan

Put development, test and low-risk internal workloads in the first waves, and critical systems later. Microsoft suggests adding one or two complex workloads to early waves to expose problems, planning only the next wave in detail, and avoiding busy business periods such as financial close.

✓ **You should see:** A wave plan with dates, workloads, owners and change windows for at least the next wave.

4 Build the landing zone

3 steps

Microsoft defines an Azure landing zone as two parts: a platform landing zone (shared governance, security and services, usually one per Entra tenant) and a workload landing zone for each workload (its development, test and production environments).

1

Set subscription boundaries

Where: Azure portal > Management groups and Subscriptions, recorded in your Target-state architecture

Decide the management group hierarchy and which subscriptions hold shared services (connectivity, identity, management) and which hold workloads. Microsoft says this is the decision that matters before workloads migrate. A subscription per workload makes cost allocation easier but is not required.

✓ **You should see:** A documented hierarchy with platform and workload subscriptions created.

2

Deploy from an accelerator

Where: Microsoft Learn: Cloud Adoption Framework > Azure landing zone > implementation options

Microsoft says its accelerators (infrastructure as code templates for platform and workload landing zones) are the fastest path for most organisations. Deploy with Bicep, Terraform or another repeatable method rather than one-off portal changes, so the next environment matches.

✓ **You should see:** The landing zone deploys and its resources show in the platform subscriptions.

3

Apply a small policy baseline and budgets

Where: Azure portal > Policy > Assignments, and Cost Management > Budgets

Apply only the policies that prevent risk during migration: restrict allowed regions, deny unmanaged public internet exposure and require diagnostic settings for central logging. Set budgets and alerts with a named owner. Do not let a perfect tagging scheme delay the build.

```
az group create --name rg-migrate --location <region>
az consumption budget list --output table
```

✓ **You should see:** Policy compliance shows the baseline assigned, and each workload subscription has a budget with alerts.

5 Connect networking and identity

4 steps

1

Create the networks

Where: Azure Cloud Shell or a terminal with the Azure CLI signed in (install the Azure CLI)

Create a hub virtual network for shared connectivity and spoke virtual networks for workloads, with subnets per tier, plus an isolated network for test migrations. Microsoft warns against one network with one subnet holding everything. Check nothing overlaps your on-premises address ranges.

```
az network vnet create --resource-group rg-migrate --name vnet-workloads --address-prefix
10.20.0.0/16 --subnet-name snet-servers --subnet-prefix 10.20.1.0/24
az network vnet create --resource-group rg-migrate --name vnet-test --address-prefix 10.99.0.0/16
--subnet-name snet-test --subnet-prefix 10.99.1.0/24
```

✓ **You should see:** Each command returns JSON with "provisioningState": "Succeeded".

2

Connect your sites

Where: Azure portal > Virtual network gateways (VPN Gateway) or ExpressRoute circuits

Choose VPN Gateway or ExpressRoute on throughput, latency, compliance and lead time. Microsoft says not to use the Basic VPN SKU for production migrations, and that ExpressRoute can take weeks or months to arrange, so run a VPN in parallel if dates are fixed.

✓ **You should see:** From an on-premises server you can reach the private IP address of a test VM in Azure.

3

Make DNS work both ways

Where: Your DNS servers (DNS Manager on a domain controller) and Azure portal > Private DNS zones or DNS private resolvers

Make on-premises names, Azure private DNS zones and any private endpoints resolve from a spoke network, and name an owner for forwarders and zones.

```
Resolve-DnsName app01.contoso.com
```

✓ **You should see:** The same name resolves to the right address from on-premises and from a VM in Azure.

4

Decide on domain controllers and admin access

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Groups, and your Target-state architecture

Create Entra ID groups for platform admins and an emergency access account. For servers that still need Kerberos, LDAP or Group Policy, decide whether domain controllers and Active Directory sites must exist in Azure before cutover. The longer-term move of users and devices is in Active Directory to Entra ID.

✓ **You should see:** A test VM in Azure can join the domain and a domain user can sign in to it.

Run Microsoft's readiness gate first. Before the first workload moves, Microsoft's minimum checks include: an Azure private IP reachable from on-premises, DNS resolving from a spoke, a tested inbound path, policy compliance, Entra ID role-based access and logs flowing centrally.

6 Move servers: replicate, test and migrate

3 steps

Rehosting copies each server's disks to Azure in the background, lets you test a copy, then switches over in a short outage. The click-by-click steps are in the VMware, Hyper-V and physical servers to Azure playbook.

1

Start replication

Where: Azure Migrate project > Execute > Migration > Start execution

VMware: choose agentless migration through the discovery appliance. Hyper-V: install the Hyper-V Replication provider on every host or cluster node. Physical servers, other hypervisors and other clouds: build a separate replication appliance (not the discovery appliance and not a source server) and install the Mobility service on each server. Choose the size, disk type, network and Azure Hybrid Benefit for each VM.

✓ **You should see:** The servers appear under Execute > Migrations with initial replication in progress.

2

Run a test migration

Where: Azure Migrate project > Execute > Migrations > the server > Testing > Start test migration

Always test into the isolated test network, because the test VM is a full copy with the same name. Sign in, check services and run the application's smoke tests. Then select **Clean up test migration**.

✓ **You should see:** The test VM boots in the test network and the smoke tests pass, or you have a list of fixes.

3

Migrate in the change window

Where: Azure Migrate project > Execute > Migrations > the server > Completion > Migrate

Stop the application, choose to shut down the source so a final copy runs, and select **Migrate**. Then update DNS and firewall rules for the new private IP address.

✓ **You should see:** The server shows at the Completion stage and the application answers from Azure.

The target region is fixed per project. For agent-based migration Microsoft says the target region cannot be changed after you select Create resources, and all later migrations in that project go there.

7 Move SQL Server databases

3 steps

A SQL Server can move with its VM (rehost), or its databases can move to a managed Azure SQL service (replatform). The choice decides the tool. Use the Azure SQL target helper and the SQL Server to Azure SQL playbook for the full steps.

1

Confirm the target from the assessment

Where: Azure Migrate project > Assessments (SQL), or SQL Server enabled by Azure Arc > Migration assessment

Check readiness for Azure SQL Database, Azure SQL Managed Instance and SQL Server on Azure VMs, and the recommended service tier and size for each.

✓ **You should see:** Each database has a target and a size, and every blocker is recorded.

2

Choose the copy method

Where: Your Technical migration runbook, using Microsoft Learn: Migrate from SQL Server overview

Managed Instance link (needs Azure Arc on the SQL Server) replicates in near real time to Managed Instance, so downtime is only the final cutover. Azure Database Migration Service does offline copies to all three targets and online copies to Managed Instance and Azure VMs. Backup and restore to SQL Server on an Azure VM is offline: downtime lasts until the restore finishes.

✓ **You should see:** Each database has a copy method that fits its allowed downtime.

3

Move logins and jobs, then cut over

Where: SQL Server Management Studio connected to the target, then the application configuration

Recreate logins, SQL Agent jobs and other server-level objects on the target before cutover, then stop writes, complete the copy and change connection strings.

✓ **You should see:** The application connects to the Azure database and its smoke tests pass.

8 Move file shares to Azure Files

3 steps

Azure Files gives you SMB file shares in Azure. Decide first whether users keep a local cache (hybrid, with Azure File Sync) or connect to Azure directly (cloud-only). The NAS to Azure Files playbook has the full steps, including sign-in with Active Directory.

1

Pick the copy tool per source

Where: Microsoft Learn: Migration overview for SMB Azure file shares (tool table)

Windows Server 2016 or later: install Azure File Sync in place. NAS or Linux SMB shares: Azure Storage Mover (SMB 2 and 3; SMB 1 is not supported) or Robocopy. Very large data over a slow link: Azure Data Box (offline, by shipping a device). AzCopy suits small, simple copies only, because Microsoft says it may lose some file fidelity and handles up to 10 million files per job.

✓ **You should see:** Each share has a tool and a target Azure file share in your inventory.

2

Set root permissions, then copy

Where: Azure portal > Storage accounts > your account > File shares, then the tool you chose

Set the Windows ACLs on the root of each share before the bulk copy. Microsoft warns that root permission changes made after a large copy can take a long time to apply. For a quick one-off copy with AzCopy, see copy files with AzCopy.

```
azcopy copy 'C:\myDirectory' 'https://mystorageaccount.file.core.windows.net/myfileshare?<SAS-token>' --recursive --preserve-permissions=true --preserve-info=true
```

✓ **You should see:** Files appear in the Azure file share with their folders, timestamps and permissions.

3

Top up and switch

Where: The copy tool, then DFS Namespaces, Group Policy drive maps or your login scripts

Run repeat copies so only changes move (Robocopy /MIR, Storage Mover re-runs, or Azure File Sync), make the source read-only, run a final pass, then repoint drive mappings and paths.

✓ **You should see:** Users open their files from the Azure file share and the source share is read-only.

9 Move web apps to Azure App Service

3 steps

1

Assess the web apps

Where: Azure Migrate project > Infrastructure > web apps > Create assessment

The appliance discovers ASP.NET web apps on IIS (VMware and physical environments). Assess them for Azure App Service. Apps rated ready or ready with conditions can be migrated in bulk.

✓ **You should see:** Each web app shows a readiness rating and a recommended App Service plan.

2

Migrate with Azure Migrate or the migration assistant

Where: Azure Migrate project > Execute > Migration (web apps), or the App Service Migration Assistant from Microsoft Learn: Migrate .NET apps to Azure App Service

For many apps in a VMware estate, use Azure Migrate's at-scale web app migration, which Microsoft says handles up to five App Service plans per run. For apps on a single Windows server, use the App Service Migration Assistant or its PowerShell scripts, linked from Microsoft's page.

✓ **You should see:** The app runs on an azurewebsites.net address in App Service.

3

Test, then move the domain

Where: Azure portal > App Services > your app > Custom domains, then your DNS host

Test the app on its azurewebsites.net address, add your custom domain and certificate in App Service, then change the DNS record in the change window.

✓ **You should see:** The site answers on your own domain from App Service with a valid certificate.

Apps that need the operating system. Microsoft says .NET Framework apps that need operating system customisation, registry changes or storage mounts can target Managed Instance on Azure App Service. If an app needs more than that, rehost its server instead.

10 Cut over each wave

3 steps

1

Agree go/no-go and rollback

Where: Your Cutover runsheet and Rollback plan

Microsoft says to set rollback criteria and procedures before any migration, get written stakeholder approval and name who can decide on a rollback. Schedule cutovers in maintenance windows or off-peak hours.

✓ **You should see:** A signed runsheet with go/no-go criteria, rollback triggers and a named decision-maker.

2

Lower DNS TTLs

Where: Your DNS server or DNS host (lower DNS TTL before a migration)

Lower the TTL on every record you will change a few days before the window, so clients pick up the new addresses quickly.

✓ **You should see:** The records show the lower TTL when you query them.

3

Switch and test

Where: Azure Migrate, the database and file tools you chose, then DNS and application settings

Stop the application, run the final copy for each server, database and share in the wave, then repoint DNS, connection strings and drive mappings. Run acceptance tests with each owner.

✓ **You should see:** Every owner signs off, or the agreed rollback trigger is met and you roll back.

11 Optimise and decommission

3 steps

1

Protect and operate

Where: Azure portal: Backup center, Azure Update Manager, Microsoft Defender for Cloud

Turn on backup, update management and Defender for Cloud for every migrated VM, database and share, and confirm a first backup completes.

✓ **You should see:** Each workload shows a backup policy with a completed backup and appears in Update Manager.

2

Right-size with Azure Advisor

Where: Azure portal > Advisor > Cost, or Azure Cloud Shell

Advisor suggests resizing or shutting down underused VMs. It looks at 7 days of data by default; change the lookback to 30, 60 or 90 days under **Configuration > Resources > VM/Virtual Machine Scale Sets right sizing** so month-end peaks count. Its savings use retail rates and ignore reservations and savings plans.

```
az advisor recommendation list --category Cost --output table
```

✓ **You should see:** A list of cost recommendations you can action or dismiss with a reason.

3

Complete and decommission

Where: Azure Migrate project > Execute > Migrations > Complete migration, then your hypervisor, backup console and CMDB

After the rollback window, complete each migration so replication stops. Power off and remove source servers, remove them from backup jobs, and update documentation.

✓ **You should see:** No source server is running, and nothing in Azure Migrate still shows active replication.

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 −

Rehost with Azure Migrate (lift and shift)

MEDIUM EFFORT

Best for: Most servers, and any estate with a deadline such as a data centre exit or hardware end of life

+ Fast and low risk, with minimal changes to each server
+ One project covers discovery, sizing and replication, with a test migration before cutover
– You still patch and manage every operating system
– Some disk types and encrypted disks need another method or preparation

Read more →

Replatform to managed services (Azure SQL, Azure Files, App Service)

MEDIUM EFFORT

Best for: SQL Server databases, file shares and ASP.NET web apps that pass the assessment

+ Microsoft runs the platform, so there is less patching and maintenance
+ Online copy methods such as Managed Instance link keep downtime to the final switch
– Each service has features it does not support, found in assessment and testing
– Logins, jobs, drive mappings and connection strings must be changed

Read more →

Azure VMware Solution

HIGH EFFORT

Best for: VMware estates that must keep vSphere tooling or VMware-only appliances

+ VMs move without conversion and keep vCenter
+ Microsoft says its VMs are eligible for free Windows Server 2016 ESU
– Runs on dedicated hosts, a larger commitment than individual VMs
– Does not reduce your dependence on VMware

Read more →

OUR ADVICE

Rehost most servers with Azure Migrate, and replatform databases, file shares and web apps where the assessment shows they are ready, because that removes patching work for little change. Choose Azure VMware Solution only when you must keep vSphere; compare it in the VMware exit path helper.

Retire and replace before you migrate

COST LEVER –

Every server you move is copied, tested and paid for in Azure. Microsoft lists retire (switch off workloads with no business value) and replace (use a SaaS product) as strategies alongside rehost.

WHAT TO DO

Use the software inventory and dependency data from Azure Migrate to find servers nobody uses, and agree with owners which to switch off before wave planning.

Microsoft Learn: Select your cloud migration strategies

Size on performance over a full business cycle

COST LEVER –

On-premises servers are often given more CPU and memory than they use. As-is sizing carries that into Azure. Performance-based sizing is only as good as the data, and assessments are a point-in-time snapshot.

WHAT TO DO

Let the appliance run through month-end or seasonal peaks, use performance-based sizing with a comfort factor, and compare the result with known peaks before accepting it.

Microsoft Learn: Azure Migrate assessment overview

Replace the business case defaults with your own figures

COST LEVER

The Azure Migrate business case uses Microsoft default assumptions for on-premises hardware, storage, facilities and labour. It also assumes servers left on-premises are Azure Arc-enabled unless you turn that off.

WHAT TO DO

Open the assumptions and enter your real costs, migration cadence and region before you share the result. Treat it as an estimate and check the vendor's current pricing.

Microsoft Learn: Business case in Azure Migrate

Start the network link early

SAVES TIME

Microsoft calls hybrid connectivity one of the few prerequisites that can block every workload at once. ExpressRoute depends on a provider and can take weeks or months.

WHAT TO DO

Order ExpressRoute (if needed) when the project starts, and build a VPN Gateway (not the Basic SKU) so the pilot is not held up.

Microsoft Learn: Azure landing zones for on-premises experts

Move dependent systems in the same wave

REDUCES RISK

Microsoft says dependencies between workloads cause service disruptions if they are not migrated together. Splitting an application between your site and Azure adds delay to every call between its parts.

WHAT TO DO

Use dependency analysis to group servers, databases and shares by application. When unsure, group them, and include the load balancers, DNS records and caches

each group needs.

Microsoft Learn: Migration wave planning

Check disks before choosing a replication method

REDUCES RISK

Azure Migrate agentless replication does not support independent disks or iSCSI targets and does not replicate RDM or passthrough disks. A server can migrate and boot without one of its volumes.

WHAT TO DO

Record disk type, encryption and clustering for every server, and test-migrate any flagged server to check every volume is present. Encrypted disks and shared disk clusters are not supported by either method, so decrypt or rebuild them.

TOOLS THAT CAN GET AROUND THIS

The agent-based method installs the Mobility service in the guest, so it replicates the independent disks, passthrough disks and iSCSI targets that agentless replication cannot.

Azure Migrate agent-based migration

Microsoft lists independent disks, passthrough disks and iSCSI targets as supported. Needs a replication appliance and the Mobility service on each VM.

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

Microsoft Learn: Support for VMware vSphere migration

Use a full-fidelity tool for file shares

REDUCES RISK

File permissions (NTFS ACLs), timestamps and attributes are what make a share usable after the move. Microsoft says AzCopy may lose some file fidelity because it uses the Azure Files REST API, and is limited to 10 million files per job.

WHAT TO DO

Use Azure File Sync, Azure Storage Mover or Robocopy for production shares, and set root permissions on each Azure file share before the bulk copy.

TOOLS THAT CAN GET AROUND THIS

These Microsoft tools keep ACLs, timestamps and attributes, and their repeat runs copy only what changed.

Azure Storage Mover

SMB 2 and 3 and NFS sources to Azure Files with ACLs, timestamps and attributes; re-runs move only changes, or only new metadata.

Azure File Sync

Syncs a Windows file server to Azure Files in the background with permissions intact.

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

Microsoft Learn: Migration overview for SMB Azure file shares

Azure File Sync needs a Windows server with NTFS

SAVES TIME

Azure File Sync runs on Windows Server 2016 or later and supports only directly attached NTFS volumes. A NAS cannot run it, and it skips hard links, symbolic links and junctions.

WHAT TO DO

For a NAS, copy straight to Azure Files, or copy to a Windows server first and sync from there. Keep shares to around 20 to 30 million items, as Microsoft suggests.

TOOLS THAT CAN GET AROUND THIS

Storage Mover reads NAS and Linux shares directly, so no Windows server is needed in between.

Azure Storage Mover

Copies SMB 2 and 3 mounts to SMB Azure file shares and NFS 3 and 4 mounts to NFS Azure file shares. SMB 1 sources are not supported.

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

Microsoft Learn: Plan an Azure File Sync deployment

Plan for a slow link with offline transfer

SAVES TIME

The first full copy of servers and shares goes over your connection to Azure. Microsoft lists Azure Data Box (shipping a device) as an option that takes longest because of shipping, but does not use your link.

WHAT TO DO

Estimate total data against your upload speed in the pilot. For large file sets, seed with Data Box and top up online.

TOOLS THAT CAN GET AROUND THIS

Data Box carries the bulk copy offline, and Storage Mover then copies only what changed since the Data Box transfer.

Azure Data Box

Microsoft says Data Box and Data Box Disk preserve ACLs, timestamps and attributes for SMB Azure file shares.

Azure Storage Mover

Detects differences after a Data Box transfer and uploads only new and changed files.

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

Microsoft Learn: Plan your migration

Count licences before you tick Azure Hybrid Benefit

COMPLIANCE

Azure Hybrid Benefit needs Windows Server core licences with active Software Assurance or a qualifying subscription, at least 8 core licences per VM, and Microsoft can audit. Standard licences may run in both places only once, for up to 180 days, while you migrate.

WHAT TO DO

Check licence counts and coverage dates with your licensing partner, apply the benefit only to covered VMs, and switch the source off within the allowance.

Microsoft Learn: Azure Hybrid Benefit for Windows Server

Decide the path for Windows Server 2016

COMPLIANCE

Windows Server 2016 reaches end of support on 12 January 2027. ESU through Azure Arc is billed from 13 January 2027. Microsoft says Azure VMware Solution and Azure Local VMs are eligible for free ESU.

WHAT TO DO

Flag 2016 servers in the assessment and choose: upgrade before or during the move, rebuild, or cover with ESU. See the Windows Server 2016 end of support guide.

Microsoft Learn: Prepare to deliver ESUs through Azure Arc

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
Every workload in the wave is accounted for	Compare Azure Migrate > Execute > Migrations, your database and file copy logs, and App Service with the Migration wave plan.	Every workload is migrated, retired or recorded as retained; none is missing or still mid-copy.
Servers boot with all disks and the VM agent	In the Azure portal open each VM > Overview and Disks, then sign in with Bastion or RDP/SSH and check every volume is online.	The VM agent status is Ready and every disk from the inventory is present at the right size.
Names resolve to Azure	Run `Resolve-DnsName app01.contoso.com` from on-premises and from a VM in Azure for every changed record.	Every name returns the Azure address from both places.
Domain sign-in works on migrated servers	On each migrated Windows VM, run `Test-ComputerSecureChannel` in an elevated PowerShell window and sign in with a domain account.	The command returns True and domain users can sign in.
Databases match the source	Compare row counts for key tables and run the application's data checks against the Azure database, recording results in the Data validation report.	Counts match and the application owner signs off the data.

Check	How to check	What good looks like
File shares keep permissions	Open a sample of folders on the Azure file share from a user PC and check Properties > Security against the source.	Permissions, owners and timestamps match the source for the sample; users can open their files.
Protection and cost controls are on	Check Backup center for completed backups, Azure Update Manager for each VM, and Cost Management > Budgets for each subscription.	Every workload has a completed backup and every subscription has a budget with alerts.
Nothing still uses the source	Check firewall or server logs for connections to old server addresses and shares after cutover.	No client connects to the source systems.

Rollback plan

If it goes wrong

ROLL BACK IF

- A critical application fails acceptance tests after cutover and the fix is not found within the window
- A migrated server will not boot or is missing data
- Hybrid network or domain sign-in from Azure fails and cannot be fixed within the window
- Performance is well below the agreed baseline and resizing does not fix it

POINT OF NO RETURN

Rollback is simple while the source systems are intact and users have not written data in Azure: stop the Azure copy, start the source and revert DNS and connection strings. Once users write data in Azure, rolling back also means copying that data back. Completing a server migration in Azure Migrate stops replication, so migrating it again starts from scratch. Decommissioning or deleting a source server is the final point of no return.

1

Stop writes in Azure

Where: Azure portal: the VM, App Service app or database

Stop the application, then stop the VM or app so it cannot clash with the source. Note what data was written since cutover.

✓ **You should see:** The Azure resource shows Stopped and no users can write to it.

2

Start the source

Where: vSphere Client, Hyper-V Manager or the physical server, and SQL Server Management Studio

Power on the source servers, start their services and make any read-only source databases or shares writable again.

✓ **You should see:** The application answers on its original address.

3

Revert names and settings

Where: Your DNS server or host, application configuration, DFS Namespaces or drive mapping Group Policy

Point DNS records, connection strings and drive mappings back to the source.

✓ **You should see:** `Resolve-DnsName` returns the source address and users open files from the original share.

4

Repair domain trust if needed

Where: Elevated Windows PowerShell on the source server

If the Azure copy ran on the domain, run `Test-ComputerSecureChannel`. If it returns False, run `Test-ComputerSecureChannel -Repair -Credential (Get-Credential)`.

✓ **You should see:** The command returns True and domain users can sign in.

5

Copy back data and record the cause

Where: The application or database, then your Rollback plan

Copy data written in Azure since cutover back to the source, or get the data owner to accept the gap in writing. Record why you rolled back before rescheduling the wave.

✓ **You should see:** The source holds every change, or the gap is signed off, and the wave has a new date.

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

Common problems and fixes

7 errors

`Server marked not ready (unsuitable for Azure) in the assessment`

Cause: The server failed the readiness stage, for example an unsupported operating system or disk. Microsoft skips sizing and cost for such servers.

Fix: Open the readiness details, fix the issue (upgrade the OS, resize the disk) and recalculate, or choose another route for that server.

`Hyper-V VM cannot be selected for replication`

Cause: Microsoft says VMs already enabled for Azure Site Recovery or Hyper-V Replica cannot be replicated by Azure Migrate.

Fix: Turn off the existing replication for that VM, then select it again.

`Migrated VM boots but a drive is missing`

Cause: Agentless replication does not copy RDM or passthrough disks, and NFS volumes mounted in the guest are not replicated by either method.

Fix: Use agent-based replication for RDM, passthrough or iSCSI disks, and move NFS data separately.

`Cannot change the target region for the migration project`

Cause: For agent-based migration the region is fixed once you select Create resources.

Fix: Create a separate Azure Migrate project for workloads going to another region.

`Azure File Sync cannot create a server endpoint on a volume`

Cause: Azure File Sync supports only directly attached NTFS volumes; ReFS, FAT and FAT32 are not supported.

Fix: Move the data to an NTFS volume, or copy it with Azure Storage Mover or Robocopy instead.

`Files such as thumbs.db, desktop.ini or *.tmp are missing after Azure File Sync`

Cause: Azure File Sync never syncs a fixed list of files, including these.

Fix: Expected behaviour: no fix needed. Check Microsoft's list before you report missing files.

`Business case option missing in an Azure Government project`

Cause: Microsoft says the business case works only in public cloud regions.

Fix: Use the assessments for size and cost estimates in Azure Government.

Search the full error library →

FAQ

Frequently asked questions

What is the first step in an Azure migration?

Discover and assess. Create an Azure Migrate project, deploy the appliance and let it collect performance and dependency data, then build assessments and a business case before you choose routes.

Is Azure Migrate free?

Microsoft describes Azure Migrate as a free service. You pay for the Azure resources you migrate into, and partner tools used with it may charge for their services.

What does lift and shift mean in Azure?

Lift and shift (rehost) copies a server to an Azure VM with as few changes as possible. Microsoft describes it as fast and low risk, for when you need little disruption and no near-term modernisation.

What is an Azure landing zone and do I need one?

It is the governed Azure foundation that workloads land in: subscriptions, policies, networks, access and logging. Even a small migration needs subscriptions, a network, DNS and admin access set up before the first server moves.

Can Azure Migrate move databases and file shares?

Azure Migrate discovers and assesses SQL Server and can discover file shares. Databases usually move with Managed Instance link, Azure Database Migration Service or backup and restore; file shares with Azure File Sync, Storage Mover or Robocopy.

Can I migrate from AWS or Google Cloud to Azure?

Yes. Azure Migrate treats VMs in other public clouds as physical servers and moves them with agent-based replication and a replication appliance.

How long does an Azure migration take?

It depends on the number of workloads, how long you collect performance data, your link speed and testing. Microsoft suggests planning only the next wave in detail and adding contingency time.

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: About Azure Migrate
- Microsoft Learn: Azure Migrate support matrix
- Microsoft Learn: Azure Migrate appliance
- Microsoft Learn: Business case in Azure Migrate
- Microsoft Learn: Select your cloud migration strategies
- Microsoft Learn: Plan your migration (Cloud Adoption Framework)
- Microsoft Learn: What is an Azure landing zone?
- Microsoft Learn: Azure landing zones for on-premises experts
- Microsoft Learn: What is Azure Database Migration Service?
- Microsoft Learn: Migration overview for SMB Azure file shares
- Microsoft Learn: Migrate .NET apps to Azure App Service
- Microsoft Learn: Azure Advisor VM right-sizing