TRAINEE HANDBOOK

SERVER+

Practical Training

Build the environment.
Operate the services.
Prove the result.

28-29 October 2026

YOUR TRAINER

Ahmed Farouk Ismail

Microsoft Certified Trainer

Windows Server 2019 | Windows 10 / 11 | VMware

From knowledge to a working environment.

This handbook accompanies a practical follow-up to the CompTIA Server+ course. You will act as the administrator of a small company: build its Windows domain, connect employee workstations, publish internal services and demonstrate recovery when something goes wrong.

Each task gives you a requirement, an expected deliverable and a verification checklist. Attempt the work first, use the online hints when needed, and demonstrate the result to your trainer. Record observations and fixes, but never record passwords.

Overall topics

Day 1 / Build the foundation

01 / Build the virtual lab

02 / Connect the machines

03 / Create the company domain

04 / Organize people and access

05 / Join the workstations

06 / Verify and hand over Day 1

Day 2 / Operate the environment

07 / Administer passwords

08 / Provision a data volume

09 / Publish departmental storage

10 / Launch the company intranet

11 / Back up and recover a Finance file

12 / Resolve the service incident

Continue your practice

E1 / Automate client addressing

E2 / Make Documents follow the user

E3 / Observe an unattended deployment

Trainee / pair: _____

SECTION 01 / 28 October 2026

01

Day 1

Build the foundation. Connect the people and machines.

One company. One connected lab.

Component	Reference configuration
Domain / NetBIOS	askfarouk.local / ASKFAROUK
Server / DNS	Windows Server 2019 | 192.168.77.129
Windows 10 client	192.168.77.130
Windows 11 client	Suggested 192.168.77.131; confirm actual address
Subnet / NAT gateway	255.255.255.0 / 192.168.77.2
C: / D:	Windows / VMware DVD drive
E: / F:	CompanyData (20 GB) / Backup (30 GB)

> Different private IP addresses or subnets are okay. Use unique addresses, the correct subnet mask and a fixed domain-controller address. Point domain members to the domain DNS server, and update DNS records, commands, DHCP ranges and firewall scopes consistently. The addresses here match the demonstrated setup; they are examples, not mandatory values.

Demonstrated setup: Windows Server 2019, domain askfarouk.local, server/DNS 192.168.77.129, Windows 10 client 192.168.77.130, subnet mask 255.255.255.0 and VMware NAT gateway 192.168.77.2. The Windows 11 client is now shown in the domain-join walkthrough; 192.168.77.131 is its suggested course address, so confirm the actual address before testing it. DC01 is the course server name; if your existing domain controller has a different hostname, substitute its actual name in DNS lookups, UNC paths and management commands. Do not rename an existing domain controller just to match a caption. Drive assignments: C: Windows, D: VMware DVD drive, E: CompanyData and F: Backup.

Before working

- Use the same VMware lab network for all machines; avoid bridging lab services onto the venue network.
- Disable VMware DHCP before activating Windows DHCP in the optional extension.
- Keep the firewall enabled and allow the required lab traffic.
- Use E: for company files and F: for backups. A disk on the same host does not protect against host failure.

DAY 1 / TASK 01

Build the virtual lab

Prepare an isolated virtual environment with one Windows Server and two Windows workstations. You will use these three machines throughout the course.

> Your deliverable: Three named, working virtual machines connected to the same private lab network.

Before you begin

• Installation media and VMware installer are available locally.

• Host virtualization is enabled; you have permission to install software.

• Use Pro, Enterprise or Education client editions that support domain join.

Assignment

1. Install VMware Workstation and connect the lab VMs to the same VMware NAT lab network (192.168.77.0/24 in this setup). Keep the lab off the venue's bridged network. Identify VMware's DHCP service; disable it on the chosen lab network before deploying Windows DHCP in the optional extension.

2. Create DC01 using Windows Server 2019 Standard Evaluation with Desktop Experience.

3. Create PC10 using Windows 10 and PC11 using Windows 11. Assign each VM to the same lab network. Windows 11 domain joining is demonstrated in Task 05.

4. Install VMware Tools, set the agreed computer names, and check the date and time.

Verification checklist

□ VMware starts and can run the lab VMs.

□ DC01 boots into Windows Server 2019 Desktop Experience.

□ PC10 and PC11 boot into domain-capable Windows editions.

□ Computer names are DC01, PC10 and PC11.

□ All three virtual adapters use the same intended lab network; its NAT and DHCP settings are understood.

□ VMware Tools is installed and local administrator sign-in works.

Evidence: Show the VMware library, each computer name, and the virtual network settings. Do not capture passwords.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

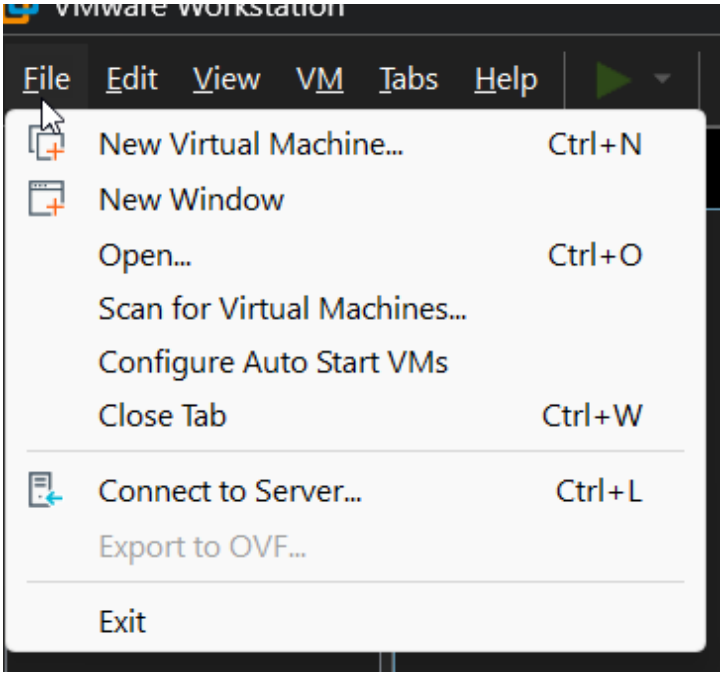
TASK 01 / SCREENSHOT WALKTHROUGH

Visual reference

These walkthrough images use Windows Server 2019 and Windows 10, matching the current setup. VMware labels may vary. Select the guest version matching your actual installation media. DC01, PC10 and PC11 are the course machine labels; The Windows 11 client's domain-join screenshots appear in Task 05.

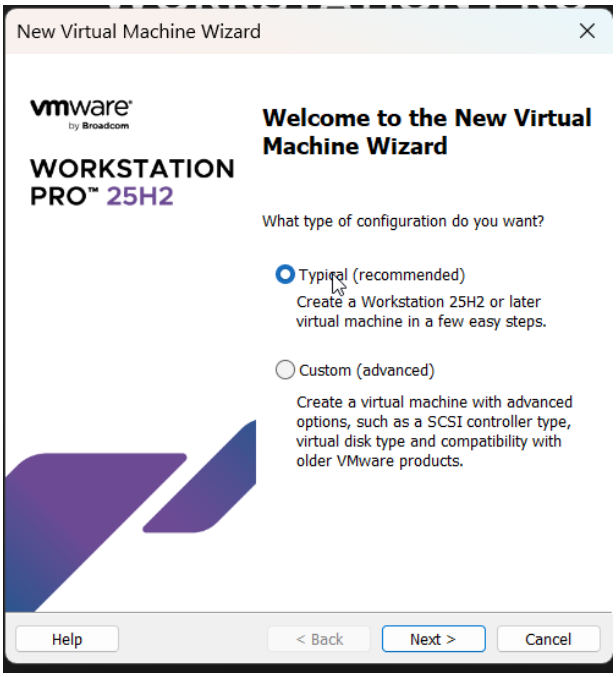
1 / Create the virtual machine

Start a new virtual machine



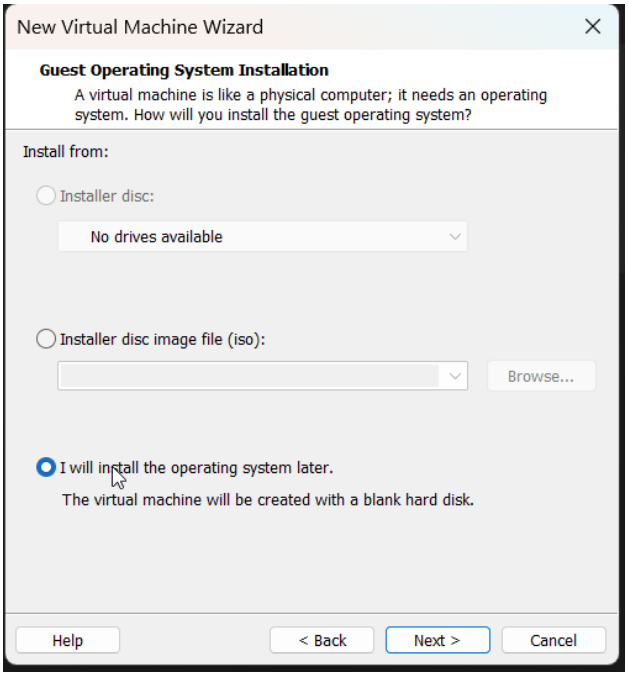
Open File → New Virtual Machine in VMware Workstation. This begins VM creation; VMware itself must already be installed.

Choose the wizard type



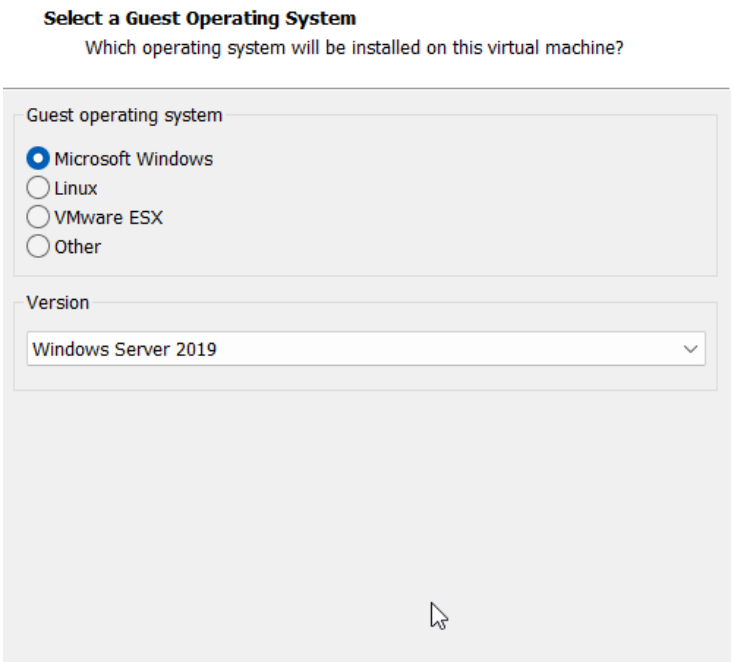
Select Typical for the standard classroom setup.

Install the operating system later



Choose this option to create the VM first and attach the intended ISO manually.

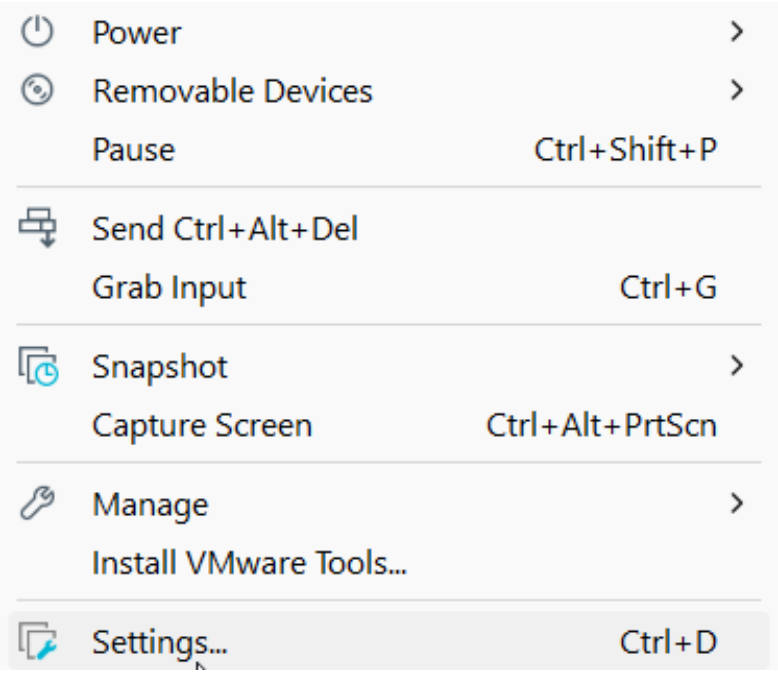
Match the guest operating system



Choose Microsoft Windows and Windows Server 2019 for the server VM. Choose the matching Windows client version when creating a workstation.

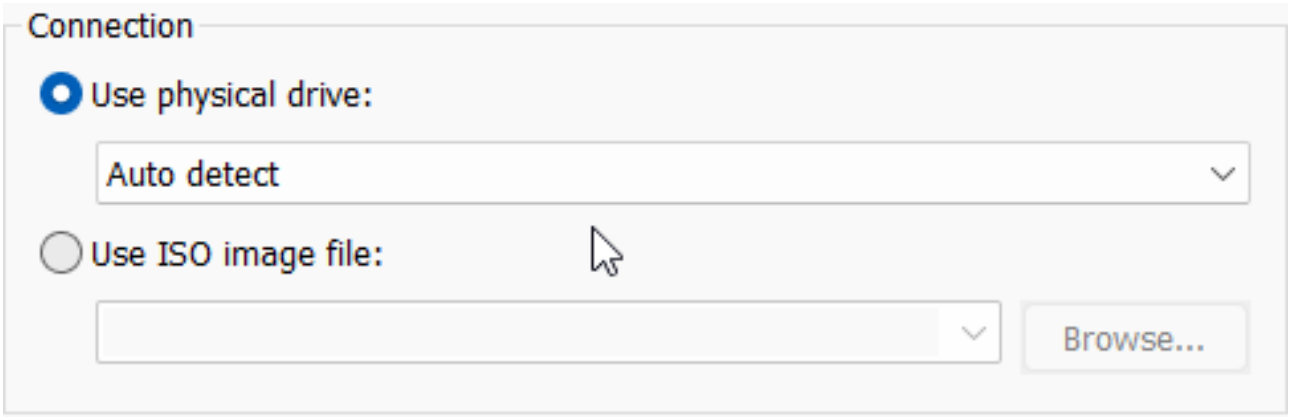
2 / Attach media and install Windows

Open VM settings



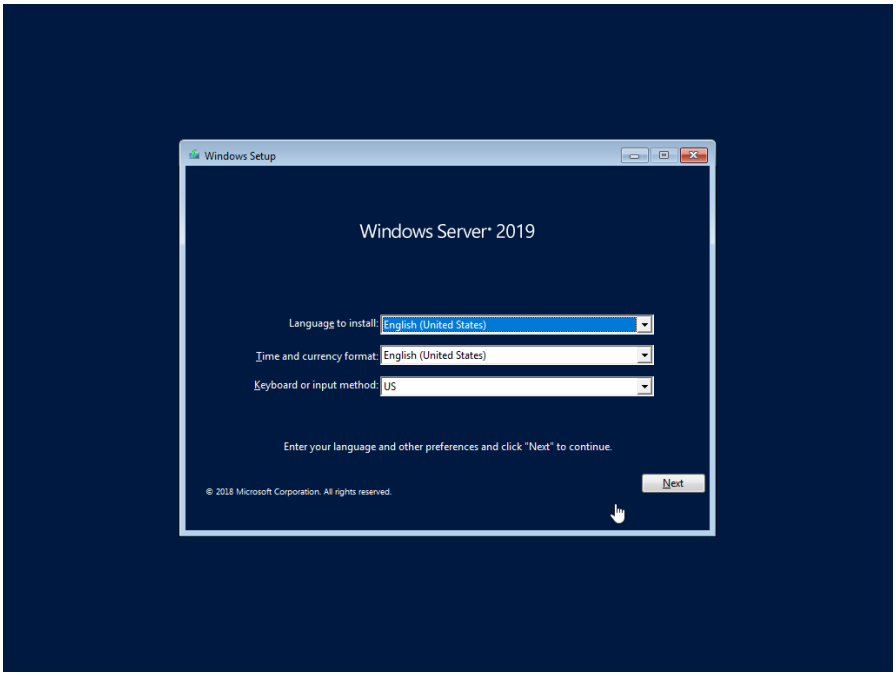
Use VM → Settings to review hardware and attach the installation media.

Attach the ISO image



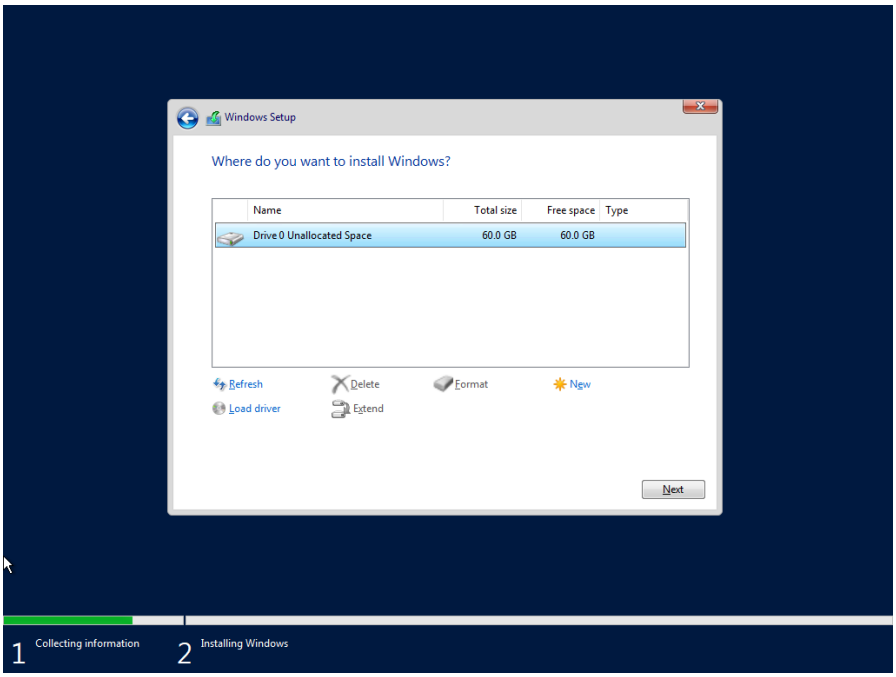
Under CD/DVD, choose Use ISO image file and Browse to your intended ISO. Ensure the virtual drive connects when the VM starts.

Start Windows Setup



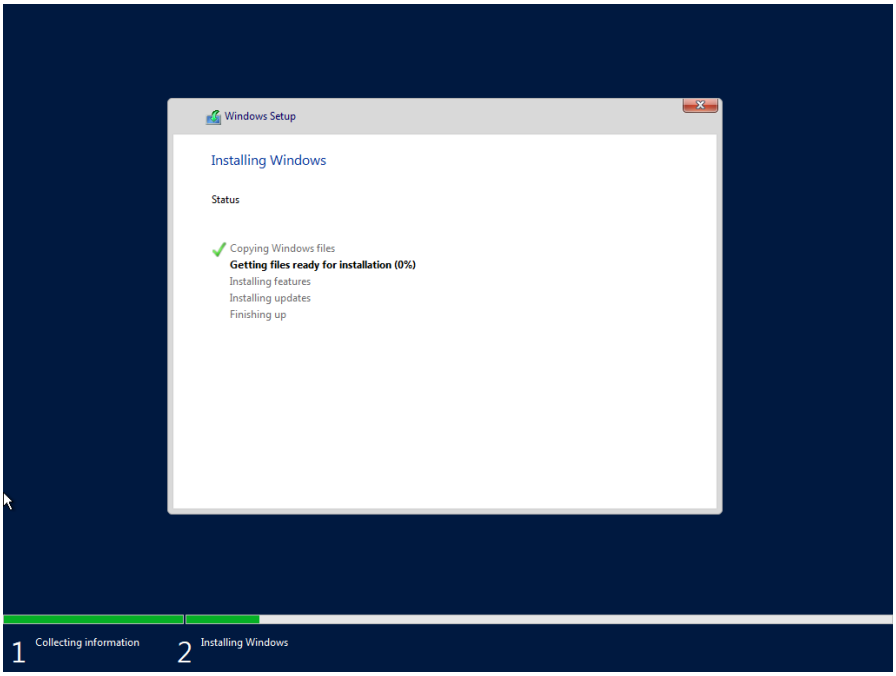
Select the language, time and keyboard for Windows Server 2019. When choosing the server edition, select Desktop Experience for the graphical administration interface used in this course.

Choose the installation disk



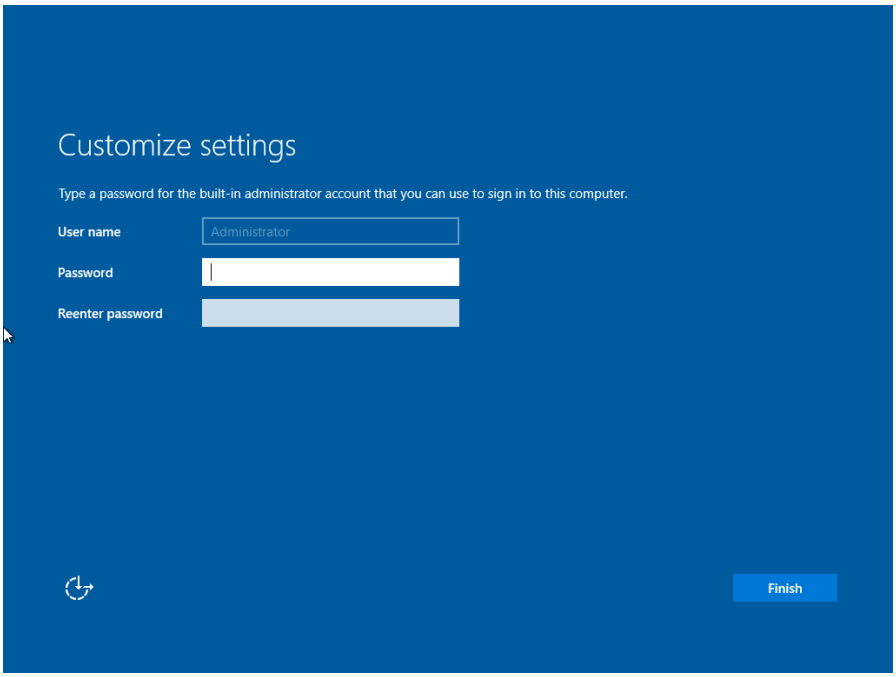
Select the new VM's empty OS disk. The captured example has 60 GB; provision at least 64 GB for the course VMs, including Windows 11. Do not format an existing data disk.

Allow installation to finish



Windows copies files and installs the operating system. Allow the VM to restart as required.

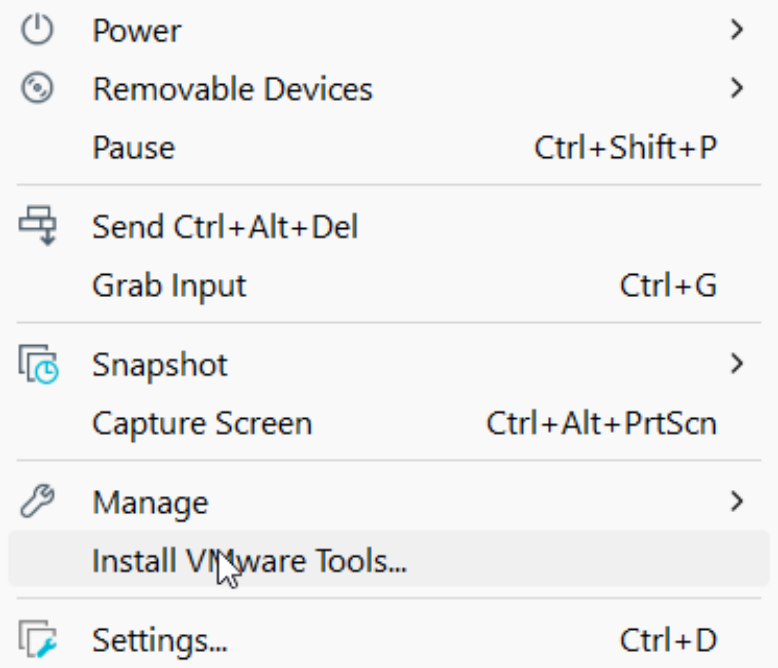
Set the local administrator password



Set and confirm the local Administrator password securely. This is the local account setup, not domain creation.

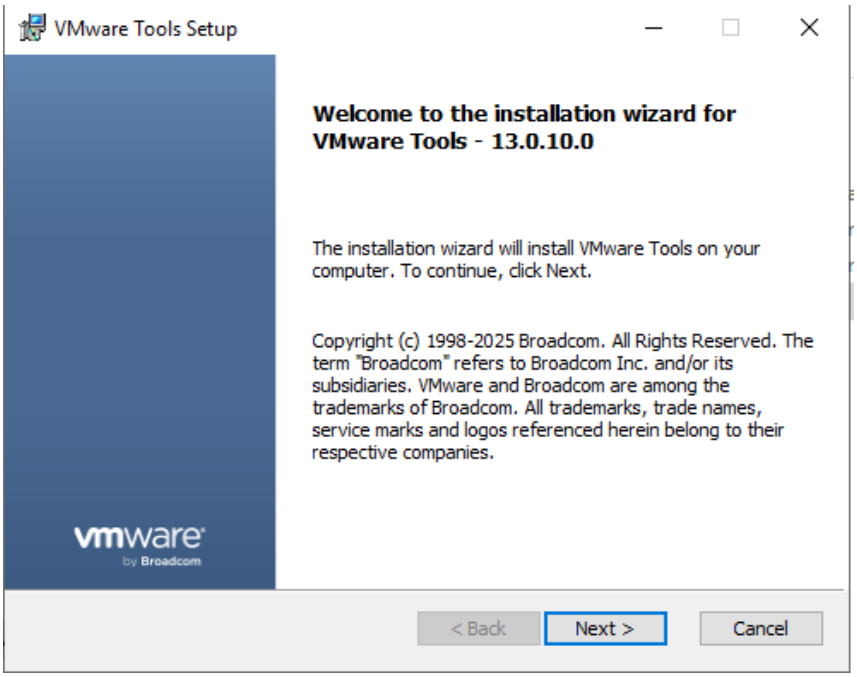
3 / Install VMware Tools

Mount VMware Tools



After Windows is installed, use VM → Install VMware Tools to mount the installer in the guest.

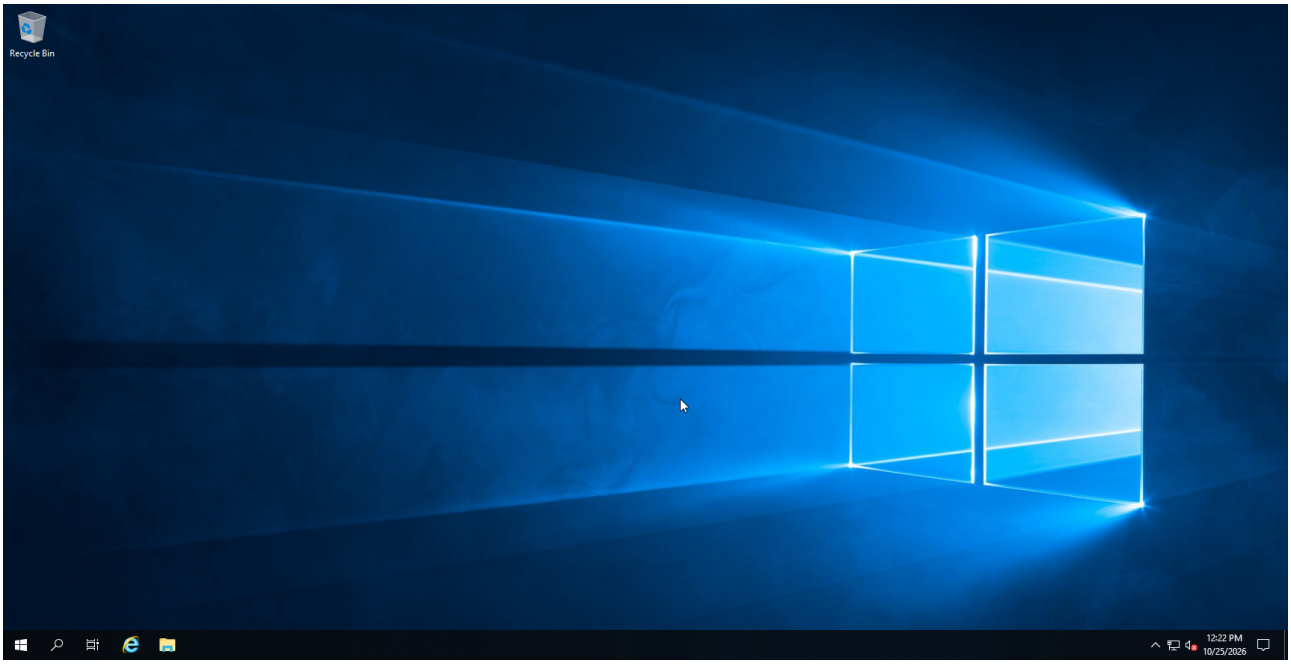
Run the Tools installer



Run VMware Tools Setup inside Windows, finish the wizard and restart if prompted.

Expected results

A working guest desktop



The guest reaches the desktop after installation. Also verify VMware Tools, the agreed computer name and the correct Windows edition; a desktop screenshot alone does not prove every checkpoint.

DAY 1 / TASK 02

Connect the machines

Give every machine a unique address and prepare clients to find the future domain controller.

> Your deliverable: A working 192.168.77.0/24 lab network with clients using DC01 for DNS.

Before you begin

• All three VMs are installed and connected to the same isolated network.

Assignment

1. Set DC01 to 192.168.77.129/24, PC10 to 192.168.77.130/24 and PC11 to 192.168.77.131/24.

2. Set DNS on all machines to 192.168.77.129. Use gateway 192.168.77.2 for the demonstrated VMware NAT network. On a host-only network without a router, leave the gateway blank instead.

3. Verify addresses and connectivity. Name resolution will be tested after the DNS role is installed.

Verification checklist

□ Each VM has the correct unique address and 255.255.255.0 subnet mask.

□ DC01 has a static address of 192.168.77.129.

□ Both clients use 192.168.77.129 for DNS, without a public alternate.

□ ipconfig /all confirms the intended configuration.

□ Both clients can reach DC01 using an appropriate connectivity test.

□ Windows Firewall stays enabled; any ICMP rule is limited to the lab network.

Evidence: Show ipconfig /all on each machine and a successful client-to-server test.

Verification commands

```
ipconfig /all

ping 192.168.77.129
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

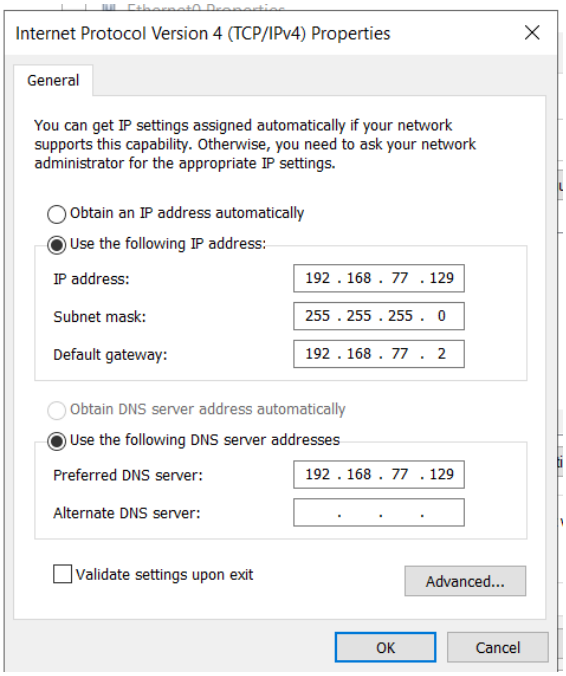
TASK 02 / SCREENSHOT WALKTHROUGH

Visual reference

These screenshots use the current 192.168.77.0/24 setup: server/DNS .129, Windows 10 .130 and VMware NAT gateway .2. The suggested Windows 11 address is .131; verify its actual configuration. The ipconfig captures show basic address information; run ipconfig /all to check DNS too. Different private IP addresses or subnets are okay. Use unique addresses, the correct subnet mask and a fixed domain-controller address. Point domain members to the domain DNS server, and update DNS records, commands, DHCP ranges and firewall scopes consistently. The addresses here match the demonstrated setup; they are examples, not mandatory values.

Configure a static server address

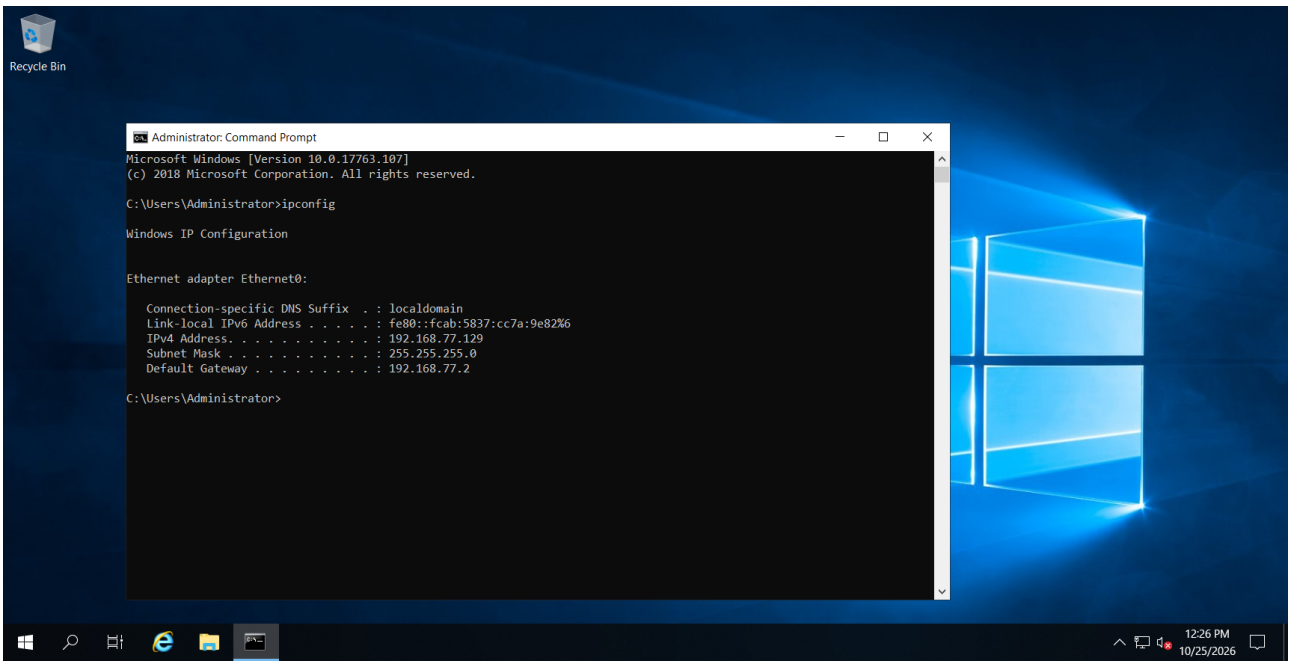
Static IPv4 and the domain DNS server



The corrected server configuration uses static IPv4 address 192.168.77.129, mask 255.255.255.0, gateway 192.168.77.2 and Preferred DNS 192.168.77.129. With AD DS and DNS installed, the server points to its own domain DNS service. Domain clients use that same DNS address.

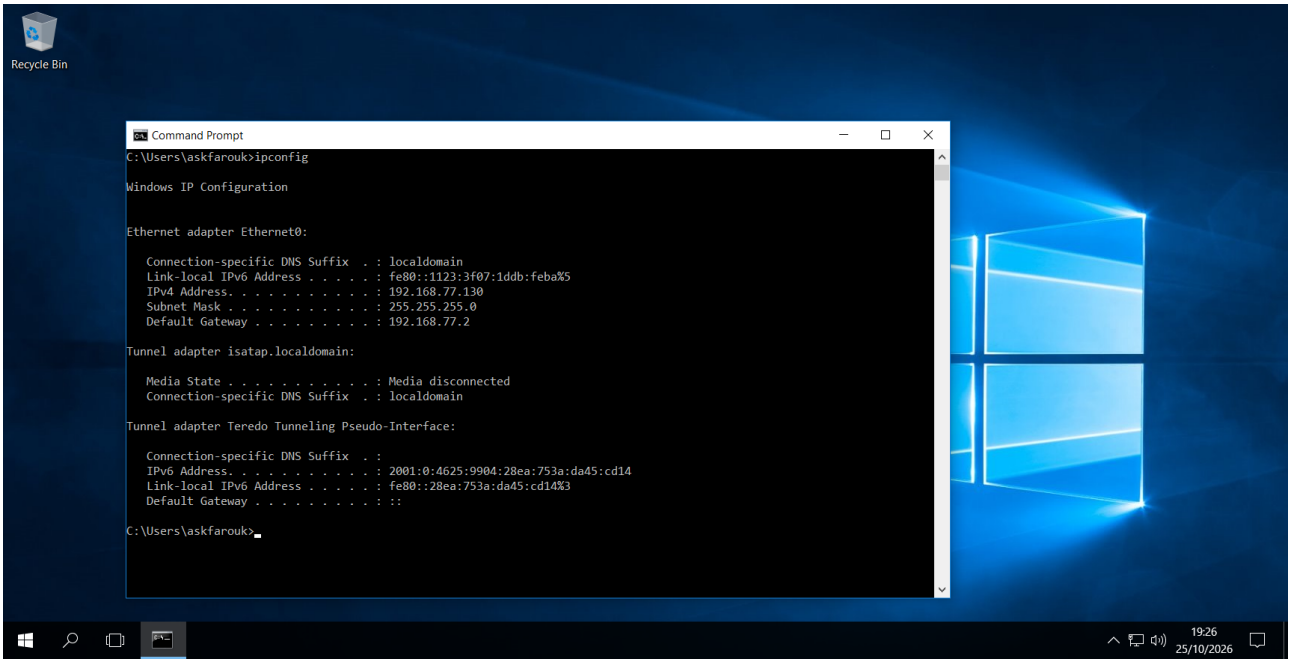
1 / Read the address configuration

Read the server IPv4 configuration



Read the Ethernet IPv4 address 192.168.77.129 and subnet mask 255.255.255.0. This earlier capture shows the address but does not prove it is static or show the DNS setting; use the corrected NIC image and ipconfig /all for those checks.

Read the client IPv4 configuration



The demonstrated Windows 10 client uses 192.168.77.130 with mask 255.255.255.0 and gateway 192.168.77.2. Use ipconfig /all to confirm Preferred DNS is the domain server at 192.168.77.129.

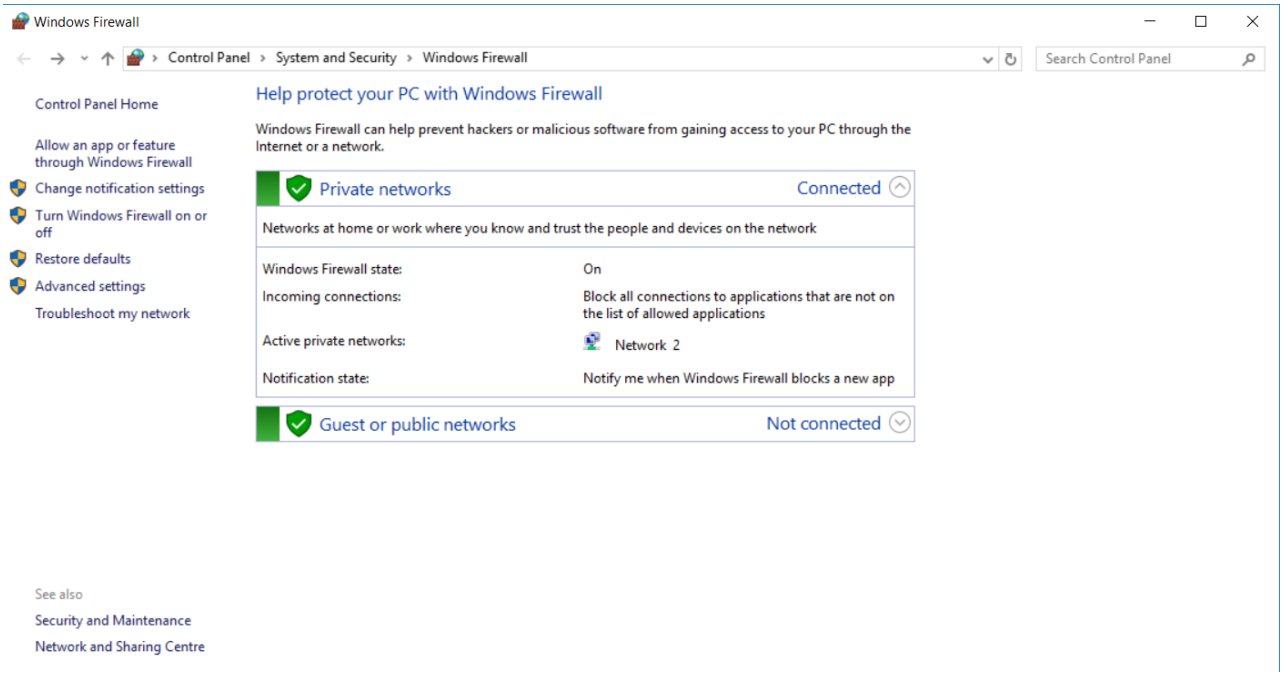
2 / Diagnose a one-way ping

Inspect the inbound echo-request rule

Name	Group	Profile	Enabled
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
Distributed Transaction Co-ordinator (RPC)	Distributed Transaction Co-...	Private...	No
Distributed Transaction Co-ordinator (RPC)	Distributed Transaction Co-...	Domain	No
Distributed Transaction Co-ordinator (RPC-EPMAP)	Distributed Transaction Co-...	Domain	No
Distributed Transaction Co-ordinator (RPC-EPMAP)	Distributed Transaction Co-...	Private...	No
Distributed Transaction Co-ordinator (TCP-In)	Distributed Transaction Co-...	Domain	No
Distributed Transaction Co-ordinator (TCP-In)	Distributed Transaction Co-...	Private...	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	No

This captured rule list shows ICMPv4 Echo Request rules disabled. If ping works in one direction only, inspect the receiving machine's firewall. Enable the appropriate inbound Echo Request rule for the active profile and limit its scope to the lab subnet.

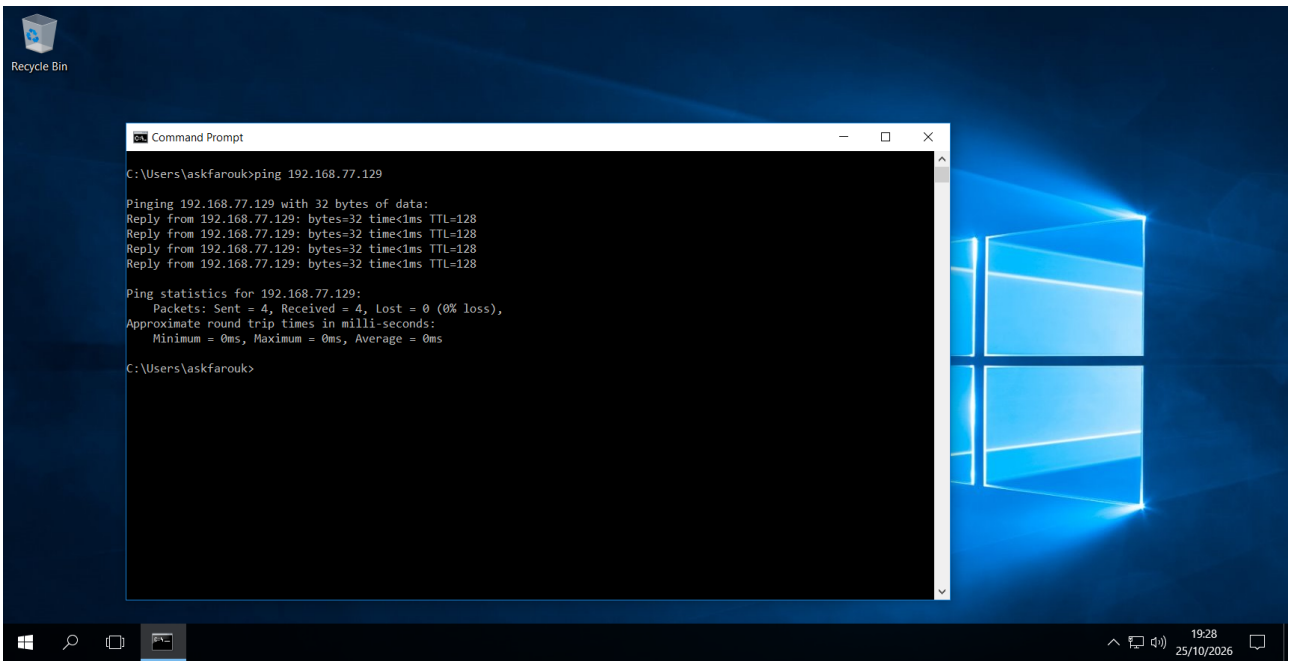
Confirm the firewall is on



The active Private profile in this example shows Windows Firewall state: On. Keep the firewall enabled and allow the specific lab traffic. Repeat the tests after changing the rule; success while the firewall was off does not verify the final configuration.

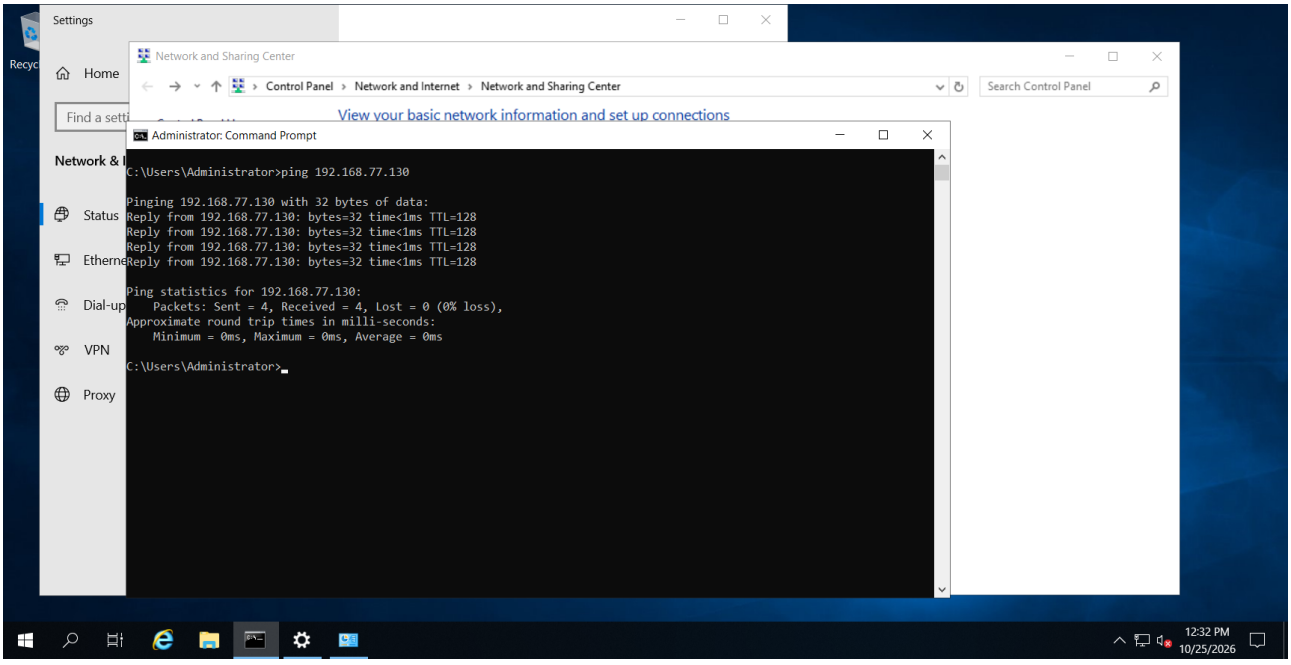
Expected results

Client → server: replies received



Windows 10 receives all four replies from server 192.168.77.129 with 0% loss. Repeat the test from each available client using the address assigned to your own server.

Server → client: replies received



The server receives all four replies from Windows 10 at 192.168.77.130 with 0% loss. Repeat with the firewall enabled and the intended ICMP rule applied. When PC11 is added, also test its assigned address (192.168.77.131 in the course plan).

DAY 1 / TASK 03

Create the company domain

Turn DC01 into the first domain controller for askfarouk.local and verify the directory and DNS services.

> Your deliverable: A functioning Active Directory forest with DNS and the standard domain shares.

Before you begin

• DC01 is renamed, has a static address, and its time is correct.

Assignment

1. Install Active Directory Domain Services and its management tools.

2. Promote DC01 into a new forest named askfarouk.local. Install DNS and securely record the DSRM password.

3. Restart, sign in as the domain administrator and verify services from the server and a client.

Verification checklist

□ AD DS and DNS roles are installed.

□ DC01 is promoted into askfarouk.local and restarts successfully.

□ Domain administrator sign-in succeeds.

□ Active Directory Users and Computers and DNS Manager open.

□ The askfarouk.local forward lookup zone exists.

□ A client resolves DC01.askfarouk.local to 192.168.77.129.

□ SYSVOL and NETLOGON shares exist.

Evidence: Show the domain in ADUC, the DNS zone, a successful client lookup and the domain shares.

Verification commands

```
nslookup DC01.askfarouk.local

net share
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

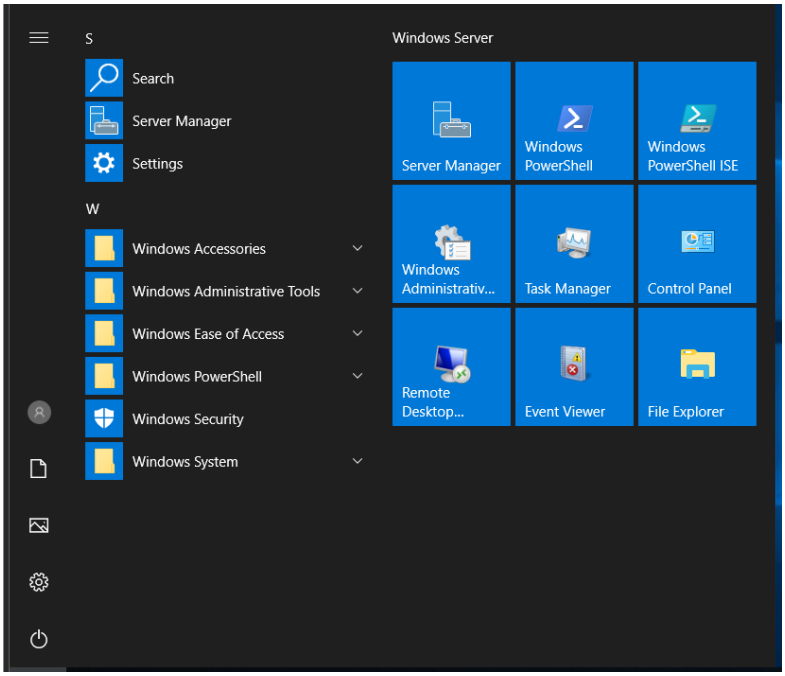
TASK 03 / SCREENSHOT WALKTHROUGH

Visual reference

These examples use Windows Server 2019, domain askfarouk.local and NetBIOS name ASKFAROUK, matching the current course setup. The captured server retains its original automatic hostname; DC01 is the course label. Use your actual server hostname in lookups and UNC paths if it differs. Role installation and domain-controller promotion are separate steps.

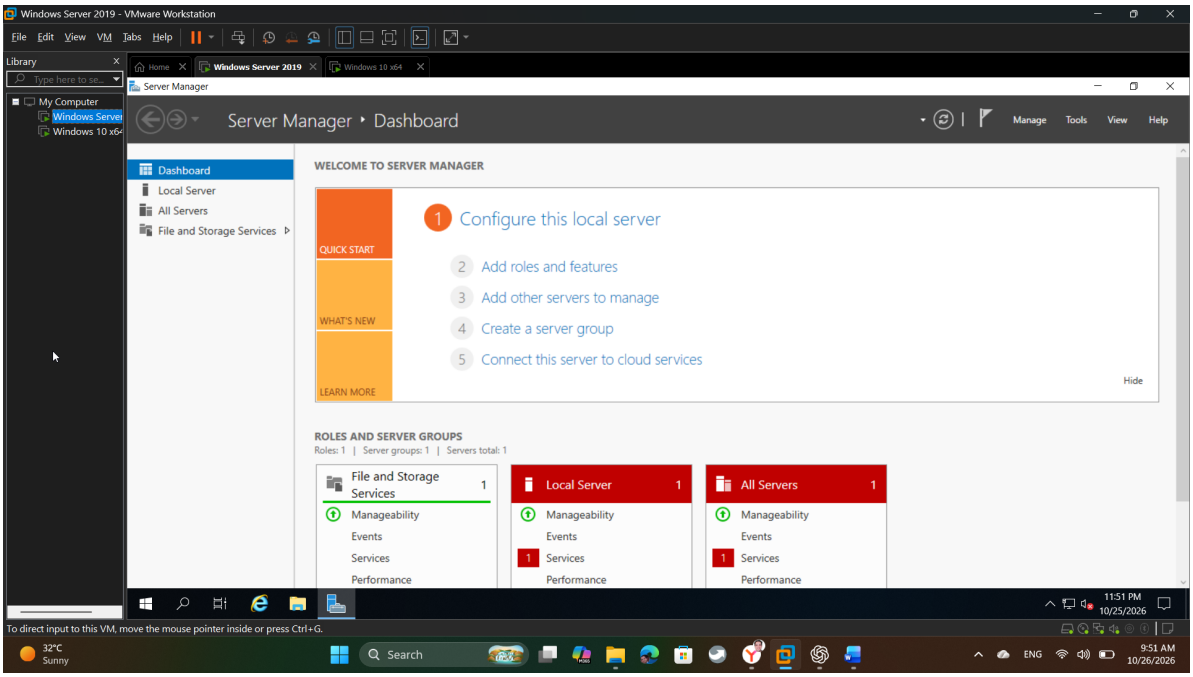
1 / Install Active Directory Domain Services

Open Server Manager



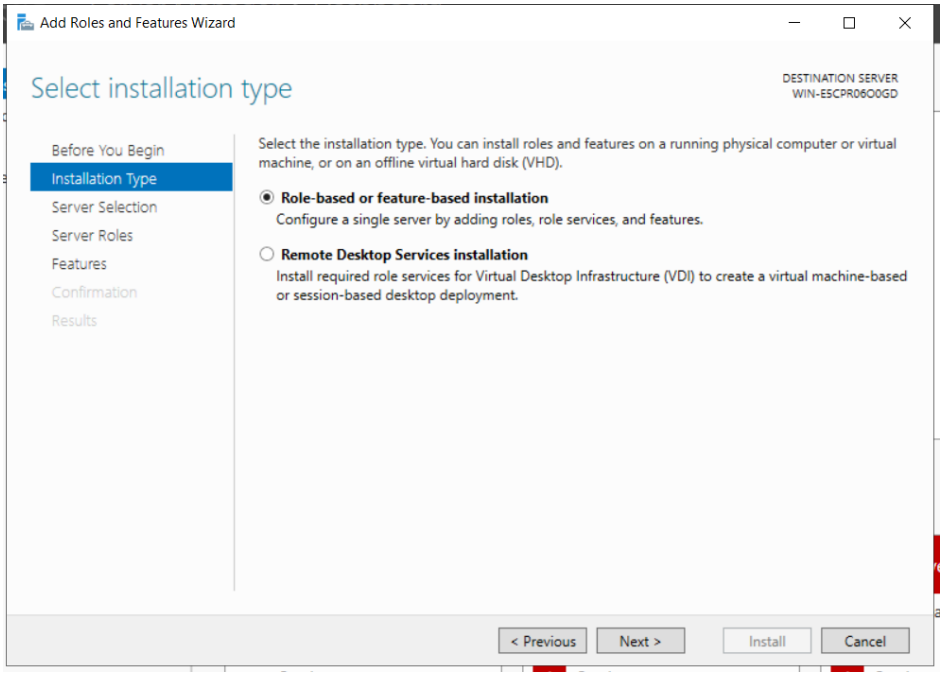
Start Server Manager from the Windows Start menu.

Start the role wizard



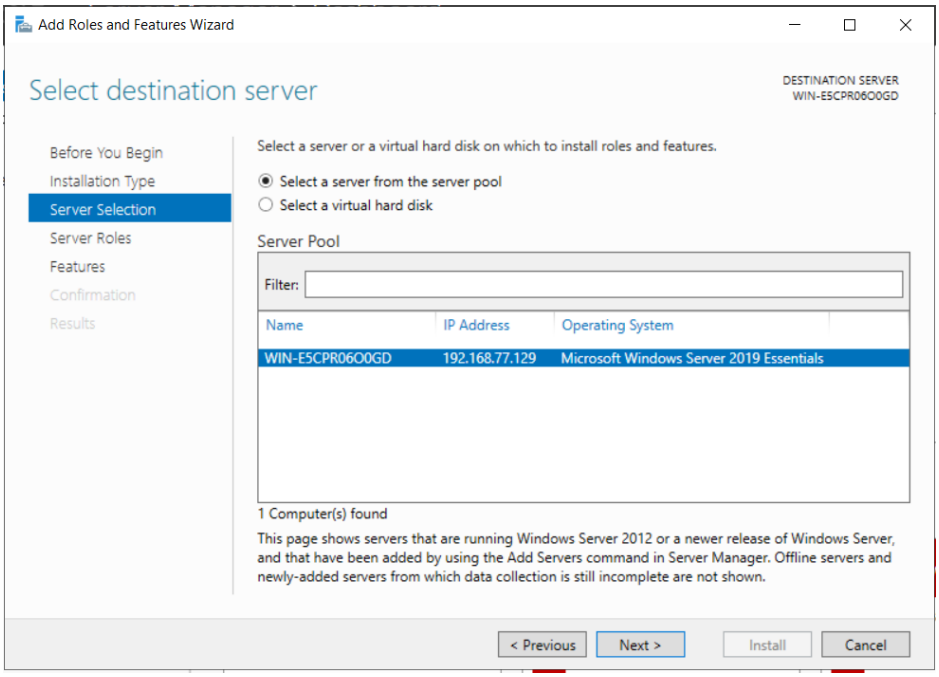
On the dashboard choose Add roles and features, or use Manage → Add Roles and Features.

Choose role-based installation



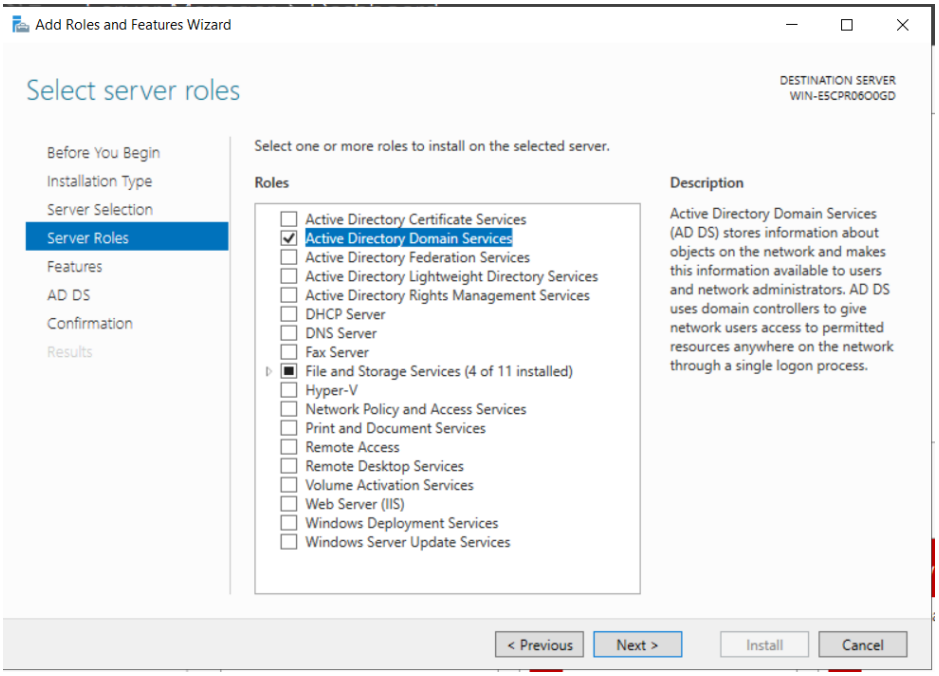
Select Role-based or feature-based installation.

Choose the destination server



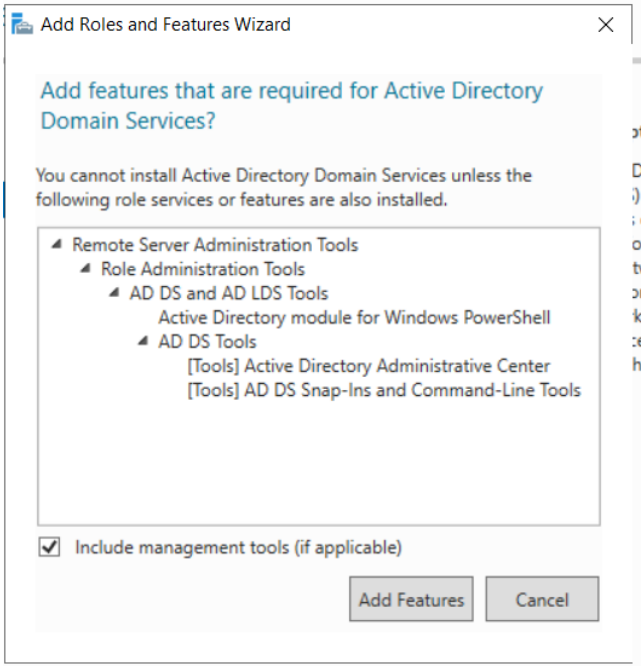
Select the intended local server. Verify its identity and static address before installing the role.

Select AD DS



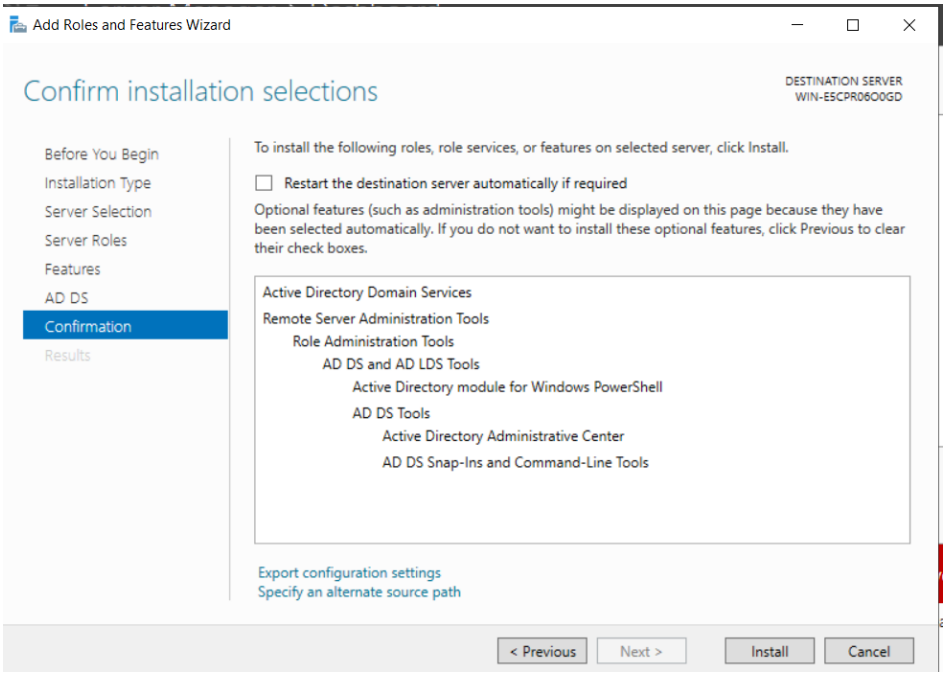
Select Active Directory Domain Services. This installs the role; it does not yet make the machine a domain controller.

Include the management tools



Accept the required features and include the management tools for AD DS.

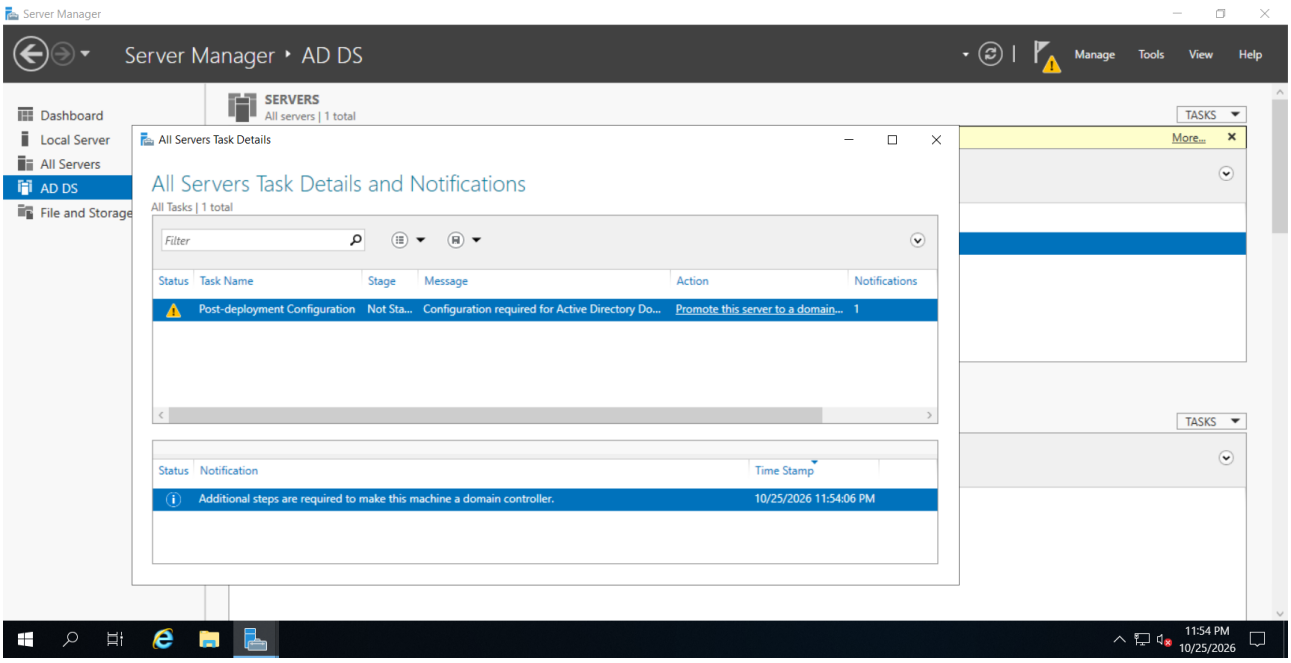
Review and install the role



Review the AD DS and management-tool selections, then install. Continue to promotion after role installation finishes.

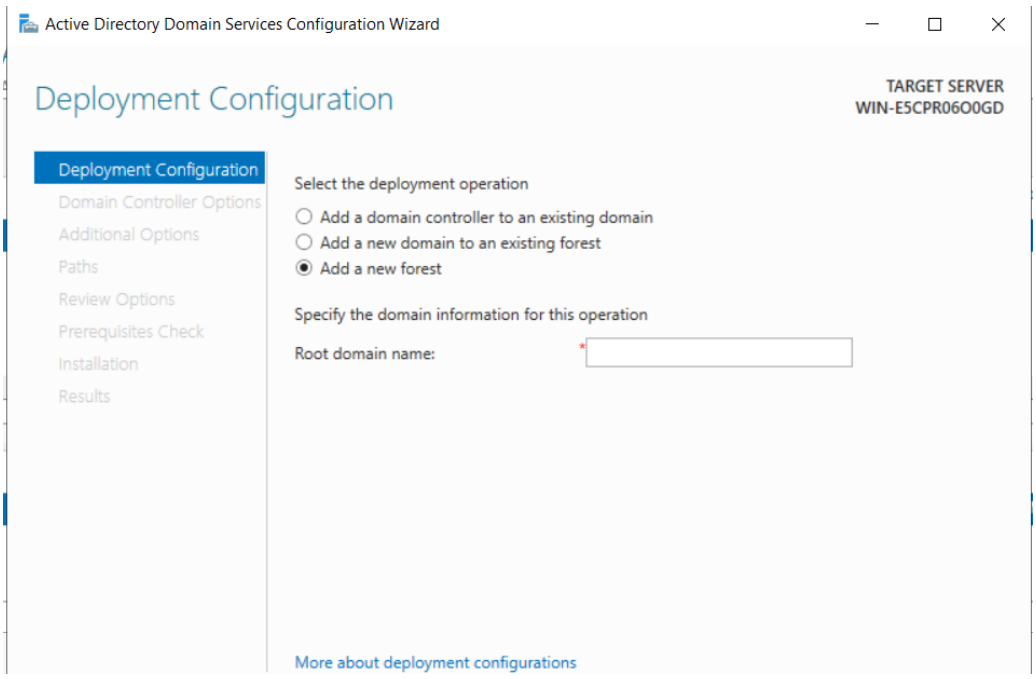
2 / Promote the first domain controller

Start the promotion wizard



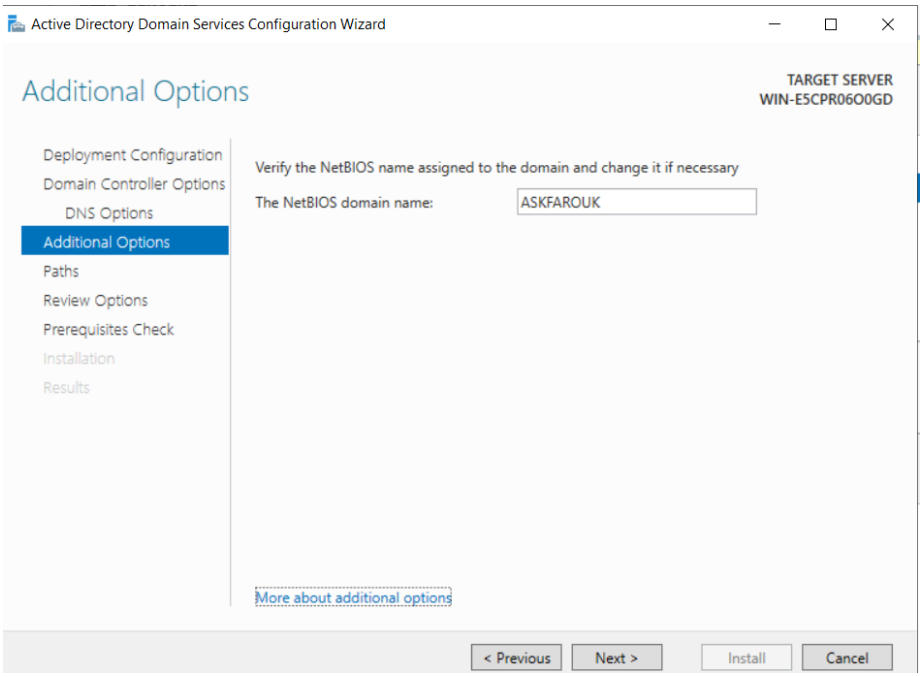
Open the notification flag and choose Promote this server to a domain controller.

Create a new forest



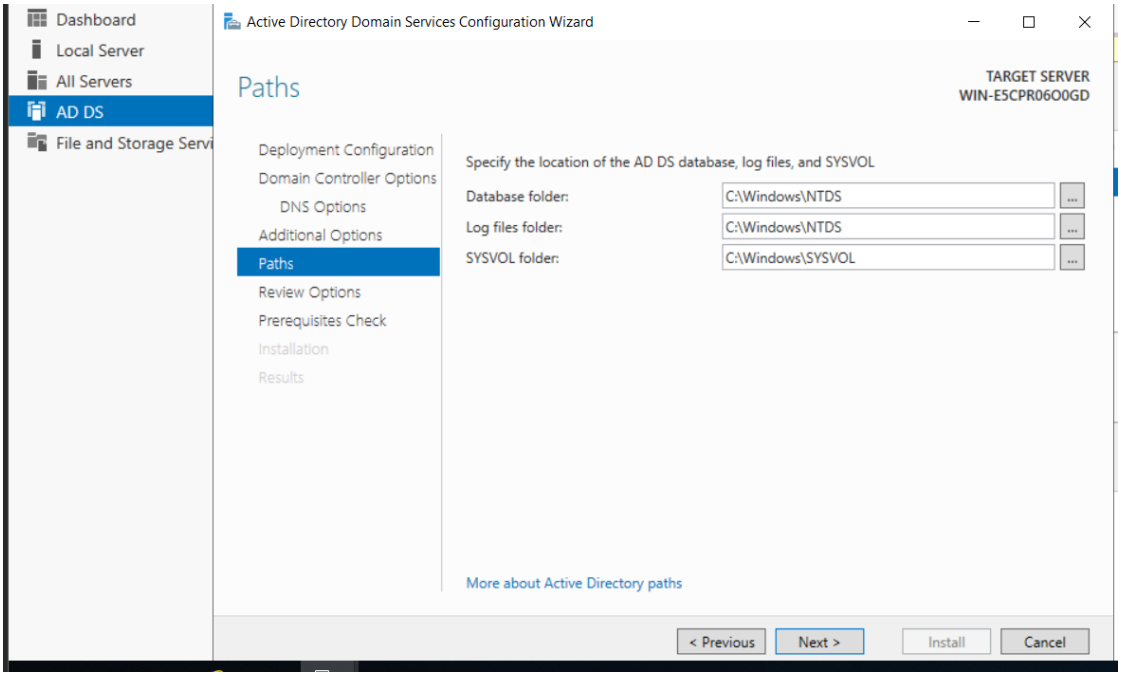
Select Add a new forest and enter askfarouk.local as the root domain name. The captured field is still blank; fill it before continuing. On the following Domain Controller Options page, keep DNS and Global Catalog selected, review functional levels and set a secure DSRM password.

Confirm the NetBIOS name



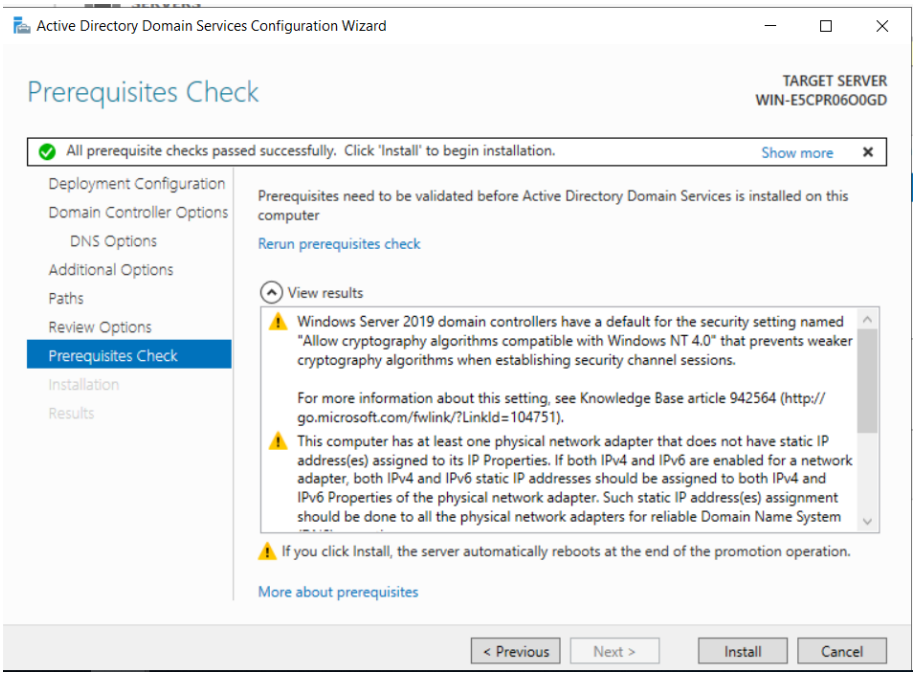
The practice domain uses ASKFAROUK. This is the short domain name used in sign-in identities such as ASKFAROUK\Administrator.

Review directory paths



Review the database, log and SYSVOL locations. The default paths are sufficient for this classroom exercise.

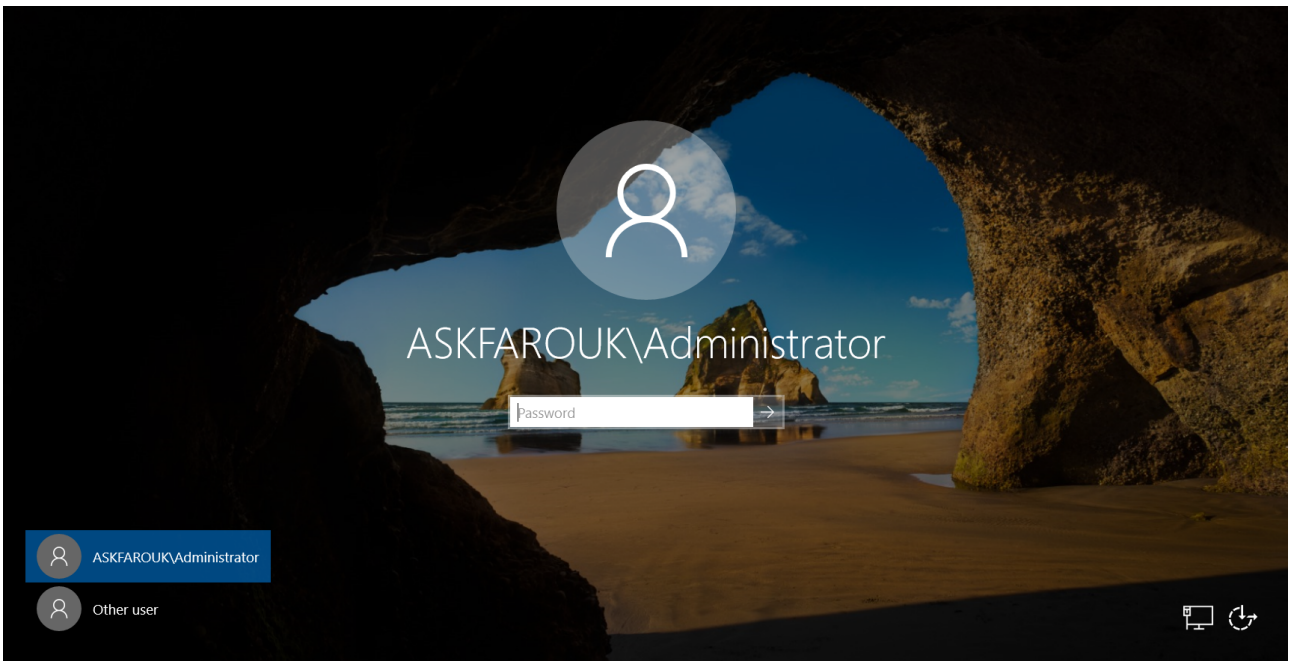
Read the prerequisite results



This is the Prerequisites Check page, not completed installation. Review warnings even when checks pass. This capture contains a non-static-address warning; verify the intended lab adapter is static and uses the domain DNS server before continuing. Use the corrected static-NIC example in Lab 02. Click Install only after reviewing the configuration; the server restarts after promotion.

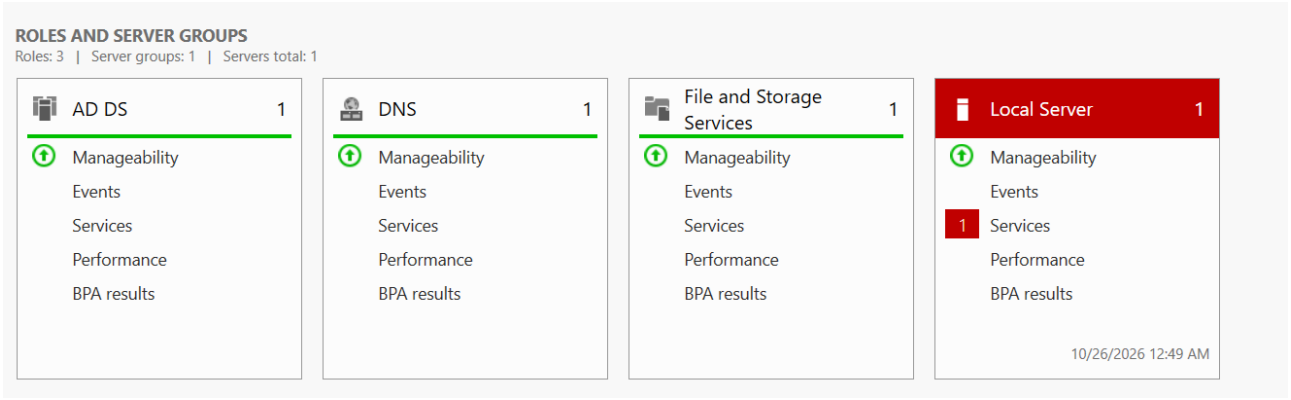
Expected results

Domain sign-in is available



The sign-in screen displays ASKFAROUK\Administrator after promotion. Enter the domain administrator credentials and verify sign-in succeeds; this screen alone does not demonstrate a completed sign-in.

AD DS and DNS appear in Server Manager



The AD DS and DNS role cards are visible. Finish the task checks by opening ADUC and the DNS zone, resolving the server name from a client, and checking SYSVOL and NETLOGON with net share. The cards alone do not prove all directory services are healthy.

DAY 1 / TASK 04

Organize people and access

Create the employee accounts and groups that will later control access to departmental data.

> Your deliverable: Two users, two departmental security groups and a clean OU structure.

Before you begin

• The domain and AD management tools are working.

Assignment

1. Create Lab Users and Lab Workstations OUs at the domain root.

2. Create finance.user and hr.user inside Lab Users.

3. Create GG_Finance and GG_HR as global security groups. Add each employee to the correct group.

4. Keep these users as standard users. Do not enable Password never expires.

Verification checklist

□ Lab Users and Lab Workstations OUs exist.

□ finance.user and hr.user exist in Lab Users.

□ GG_Finance and GG_HR are global security groups.

□ Each user belongs to the correct departmental group.

□ Neither employee has administrative group membership.

□ Both accounts are enabled and Password never expires is off.

Evidence: Show the OU structure, account properties and the Members tab of both security groups.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

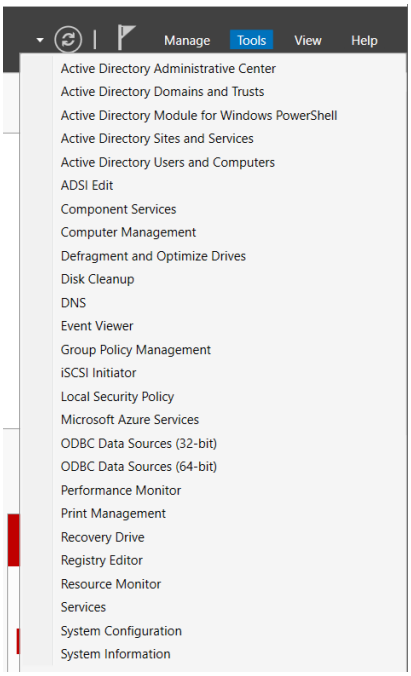
TASK 04 / SCREENSHOT WALKTHROUGH

Visual reference

These screenshots use askfarouk.local and the same Lab Users, Lab Workstations, finance.user, hr.user, GG_Finance and GG_HR names as this course. “Right-click” means opening an object’s context menu; the Tools menu in Server Manager opens with a normal click. Passwords shown in setup are masked; keep actual passwords out of notes and evidence.

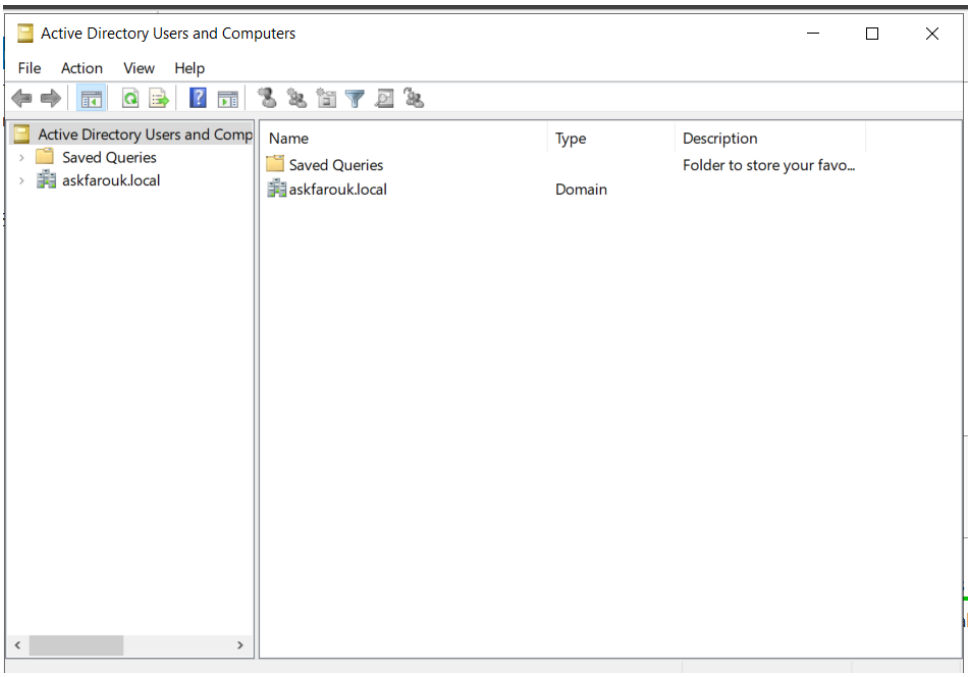
1 / Open the directory management console

Open Active Directory Users and Computers



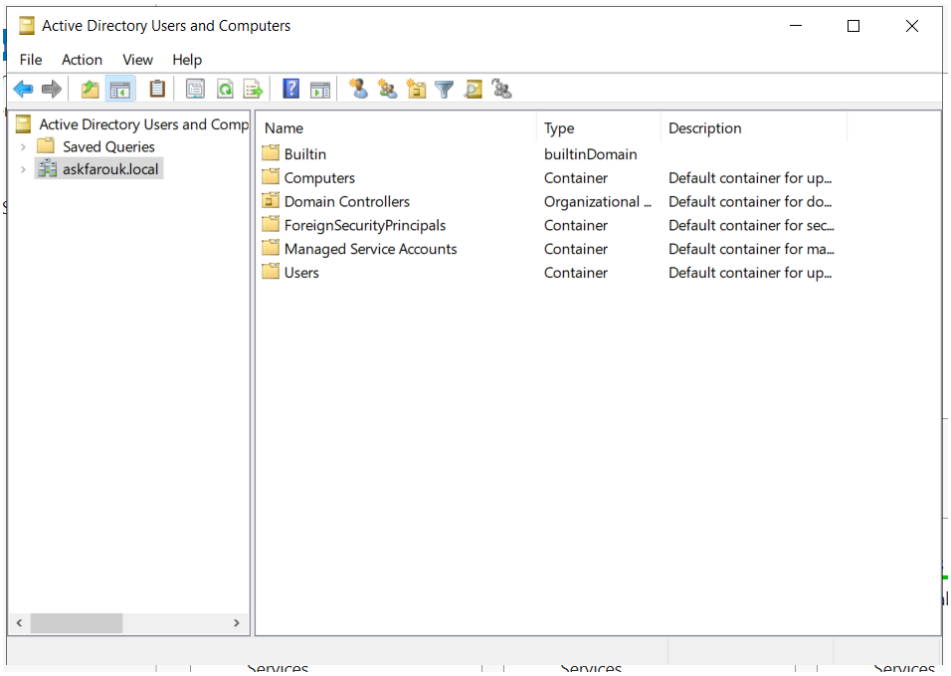
In Server Manager, click Tools → Active Directory Users and Computers. This menu opens with a normal click, not a right-click.

Find the domain



Locate askfarouk.local in the left pane of Active Directory Users and Computers.

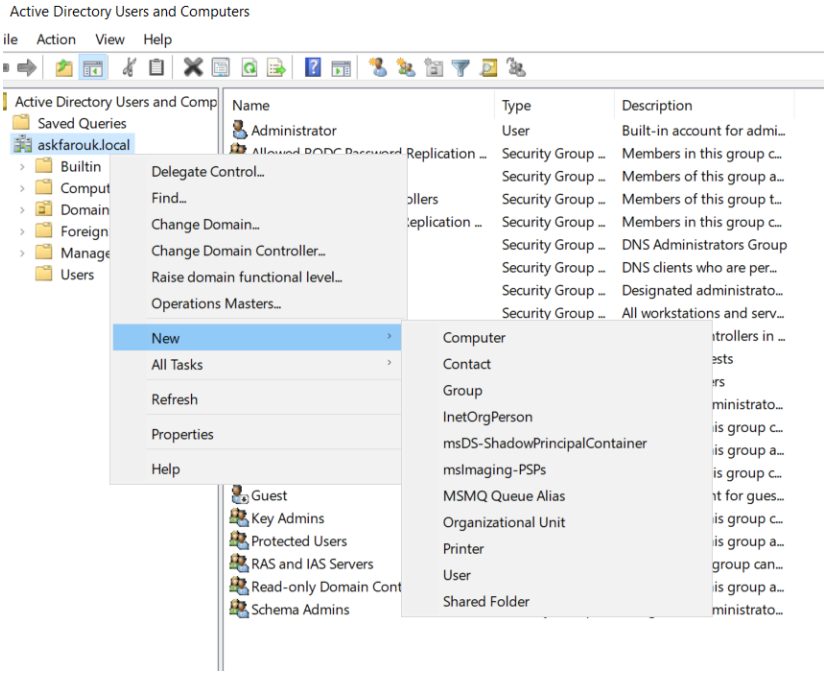
Inspect the domain root



Select or expand askfarouk.local. Builtin, Computers and Users are existing containers; create the course OUs at the domain root.

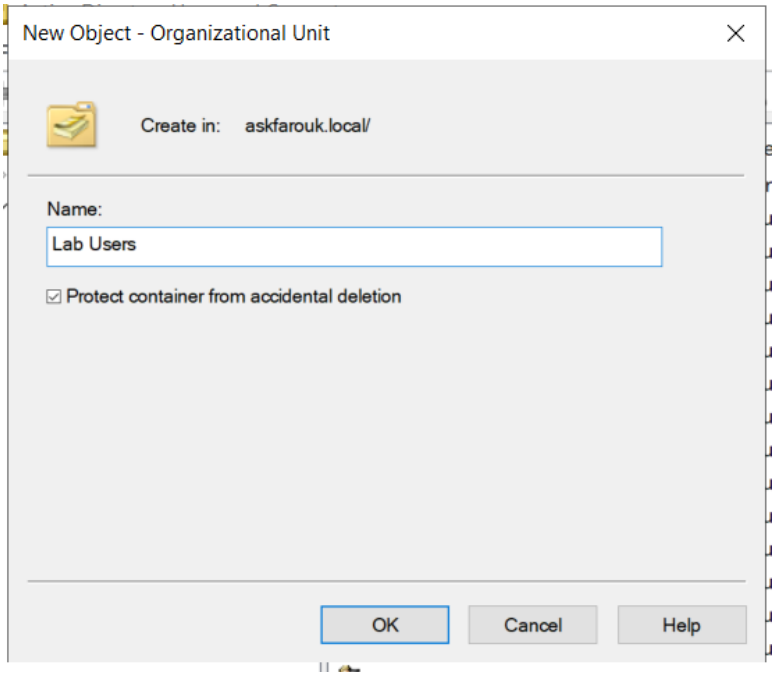
2 / Create the organizational units

Right-click the domain to create an OU



Right-click askfarouk.local → New → Organizational Unit. Do not create the lab OUs inside the default Users container.

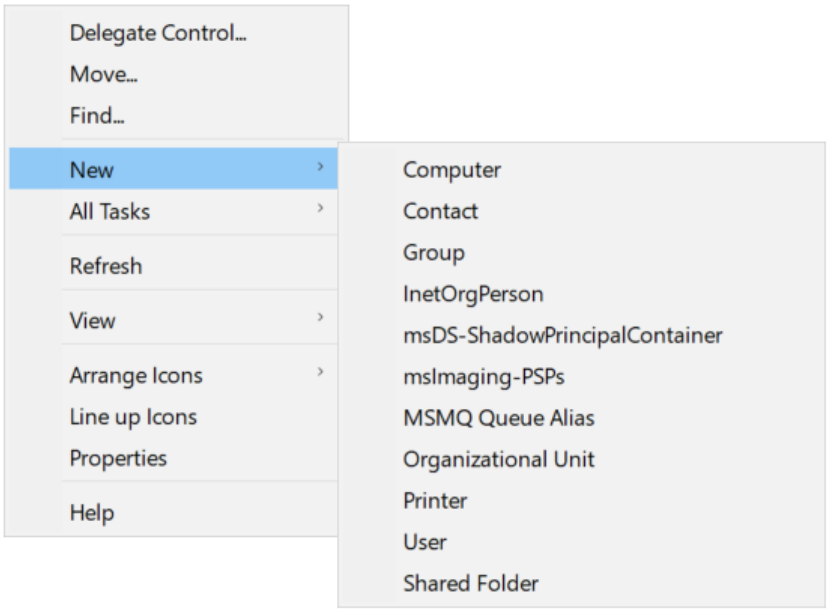
Name and protect the OU



Enter Lab Users and keep Protect container from accidental deletion selected. Repeat at the domain root to create Lab Workstations.

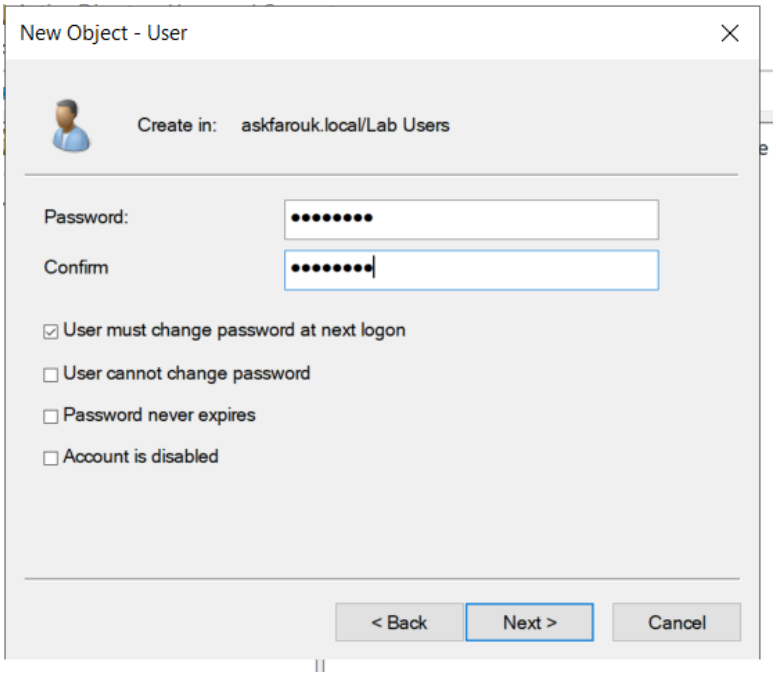
3 / Create the employee accounts

Right-click Lab Users to create a user



Right-click Lab Users → New → User. Enter the user details and logon name for finance.user, then repeat for hr.user.

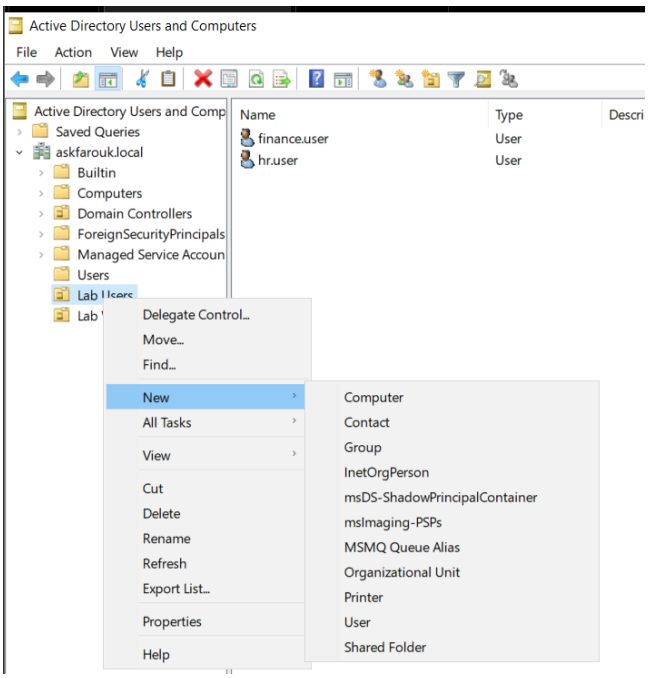
Set a temporary password and review the flags



Set and confirm a secure temporary password. Password never expires stays unchecked and Account is disabled stays unchecked. This capture requires a password change at next logon; if you retain it, complete that change during the first client sign-in. Task 07 will demonstrate a fresh administrator reset and next-sign-in change.

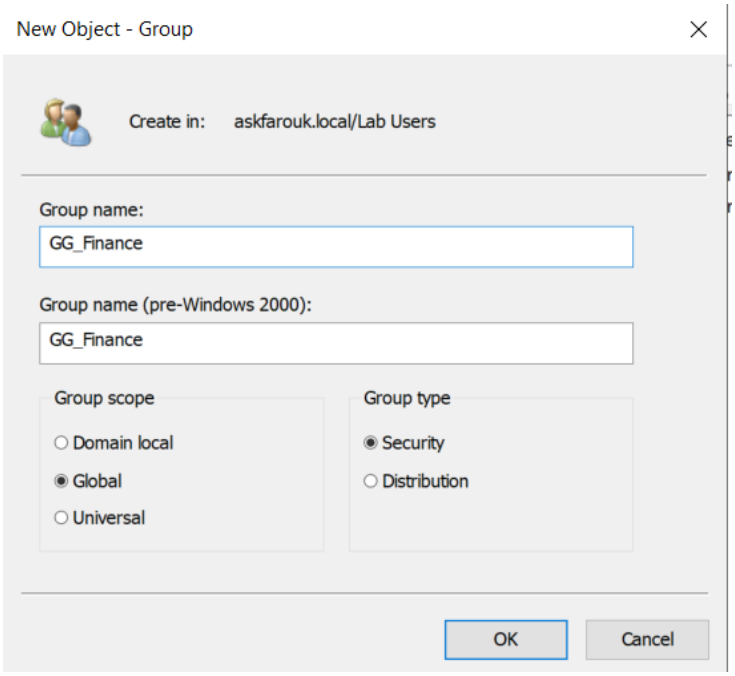
4 / Create departmental security groups

Right-click Lab Users to create a group



Right-click Lab Users → New → Group. Create GG_Finance, then repeat for GG_HR.

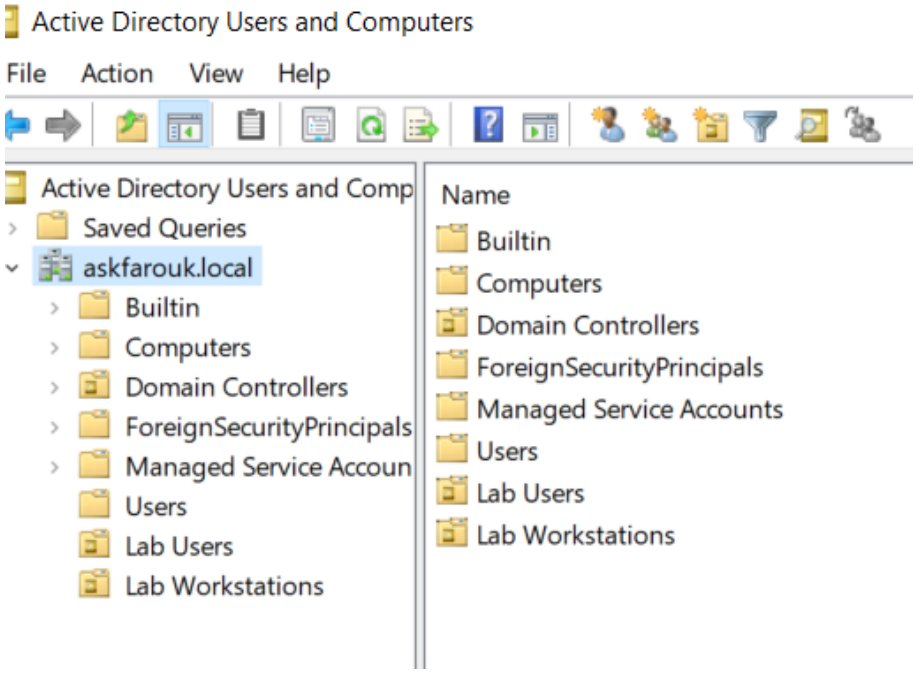
Choose Global and Security



For GG_Finance, set Group scope to Global and Group type to Security. Use the same scope and type for GG_HR. Open each group → Members → Add to assign the matching employee.

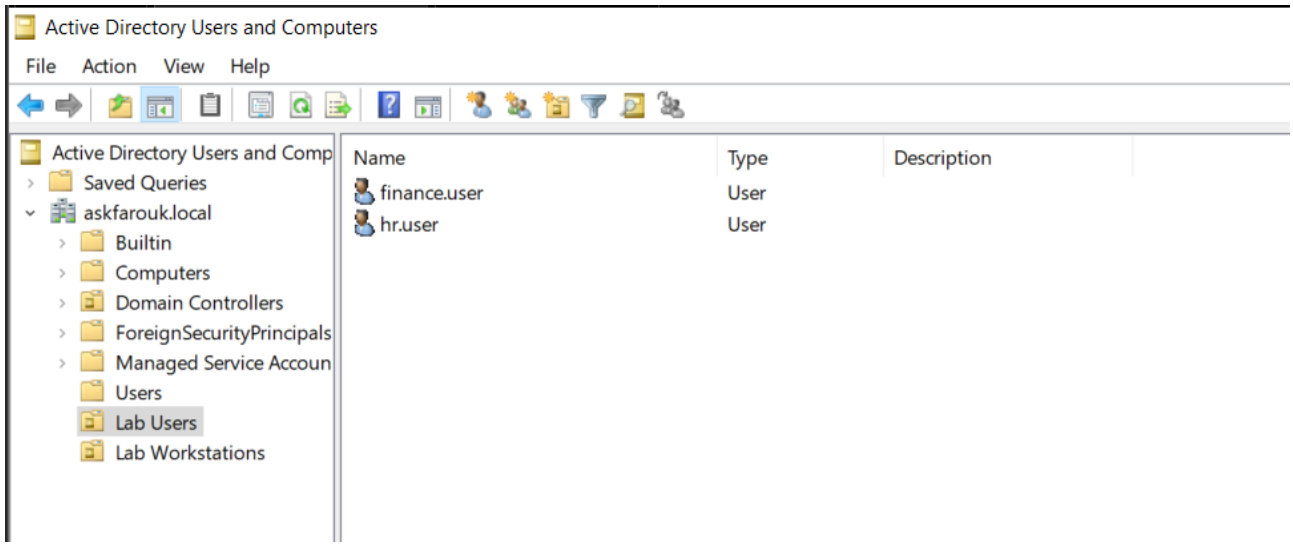
Expected results

Both organizational units exist



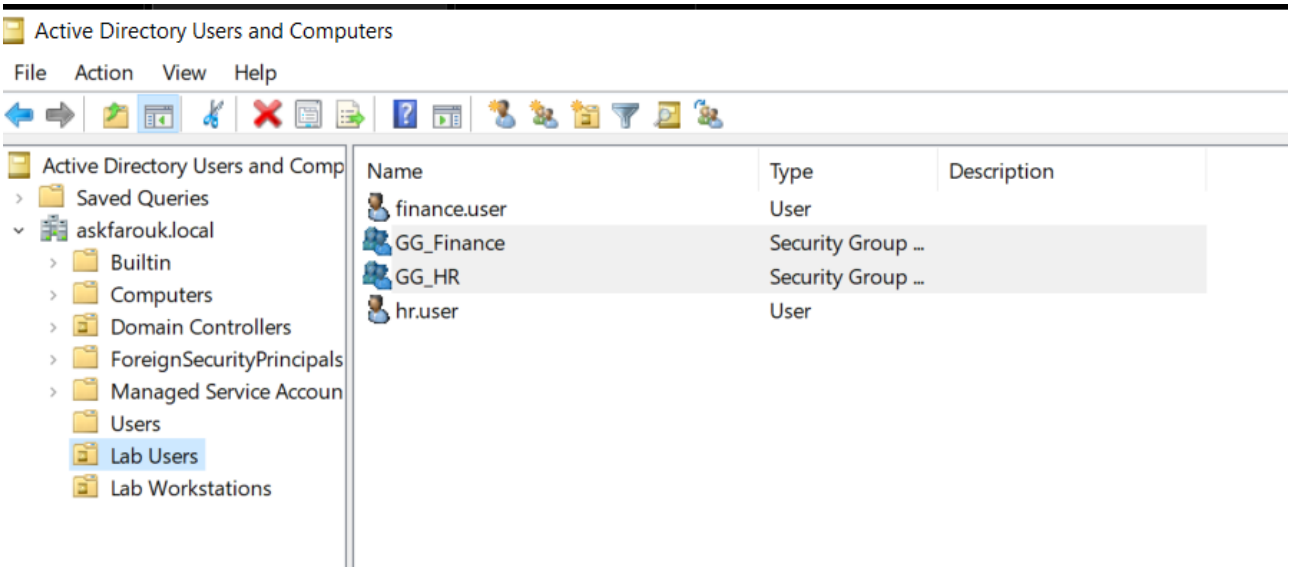
Lab Users and Lab Workstations appear at the root of askfarouk.local. User accounts belong in Lab Users; domain-joined computer objects will be moved into Lab Workstations in the next lab.

Both employees are in Lab Users



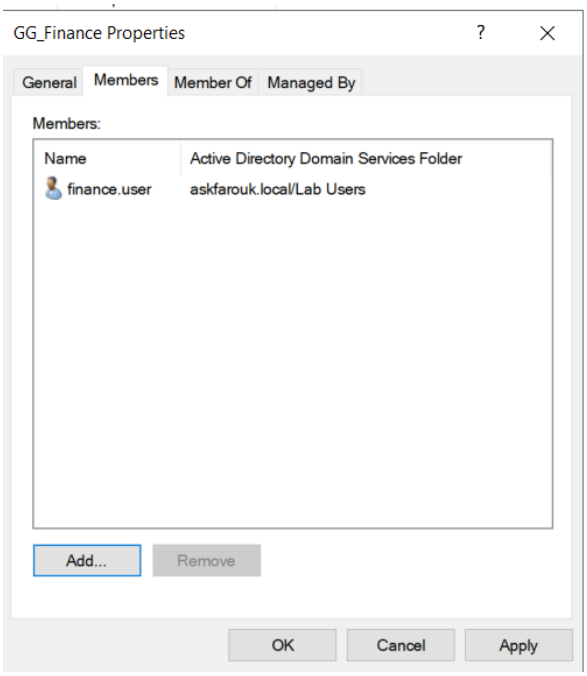
finance.user and hr.user appear as User objects in Lab Users. A similar display name alone is not enough; verify each account's logon name and enabled state.

Two users and two security groups



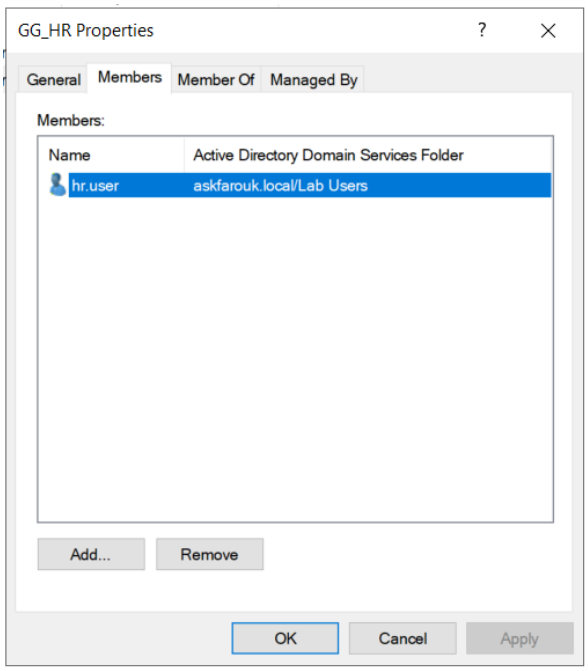
Lab Users now contains finance.user, hr.user, GG_Finance and GG_HR. Group creation does not automatically create shared folders.

Finance membership is assigned



The Members tab of GG_Finance contains finance.user. Repeat the operation for GG_HR with hr.user, and show its Members tab to verify the second group as well.

HR membership is assigned



The Members tab of GG_HR contains hr.user in askfarouk.local/Lab Users. Together with the GG_Finance membership example, this verifies that each employee belongs to the correct departmental security group.

DAY 1 / TASK 05

Join the workstations

Connect both workstations to the company directory and prove employees can sign in with domain accounts.

> Your deliverable: Two domain-joined clients with their computer objects in Lab Workstations.

Before you begin

• Clients resolve DC01 through the domain DNS server.

• Employee accounts exist and the client time is in sync.

Assignment

1. Join PC10 and PC11 to askfarouk.local and restart both.

2. Move their computer objects from Computers into Lab Workstations.

3. Sign in on each client using an employee domain account and verify the identity.

Verification checklist

□ PC10 and PC11 are members of askfarouk.local.

□ Both clients restart after joining.

□ Both computer objects exist inside Lab Workstations.

□ A domain employee successfully signs in on each client.

□ whoami shows ASKFAROUK and the expected user.

□ Trainee can distinguish a local account from a domain account.

Evidence: Show the computer objects in the OU and whoami after employee sign-in on each client.

Verification commands

```
nslookup DC01.askfarouk.local

whoami
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

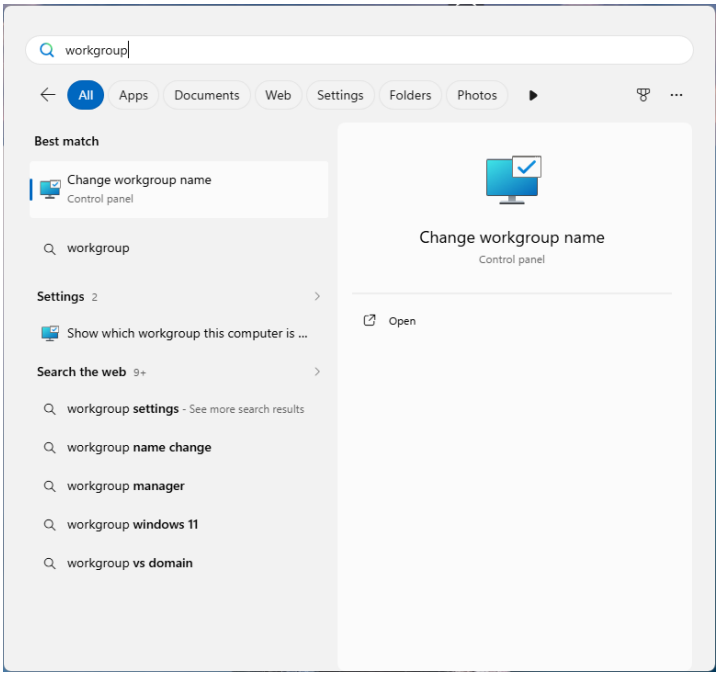
TASK 05 / SCREENSHOT WALKTHROUGH

Visual reference

This walkthrough shows Windows 11 joining askfarouk.local. Windows 10 can use the same System Properties method: run sysdm.cpl → Computer Name → Change. The screenshots retain the client's automatic hostname; use your actual client name when checking its AD computer object. Before joining, set client DNS to 192.168.77.129 and check name resolution. A credential prompt is progress, not proof that joining finished.

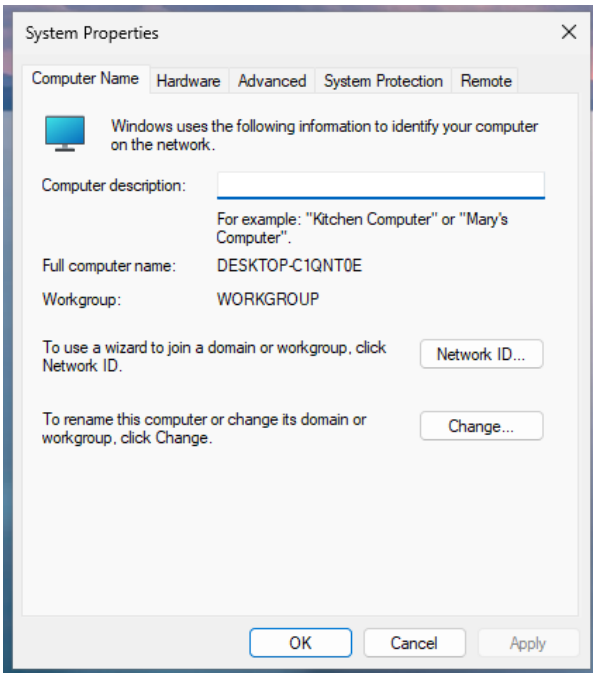
1 / Open computer domain membership

Open the computer membership settings



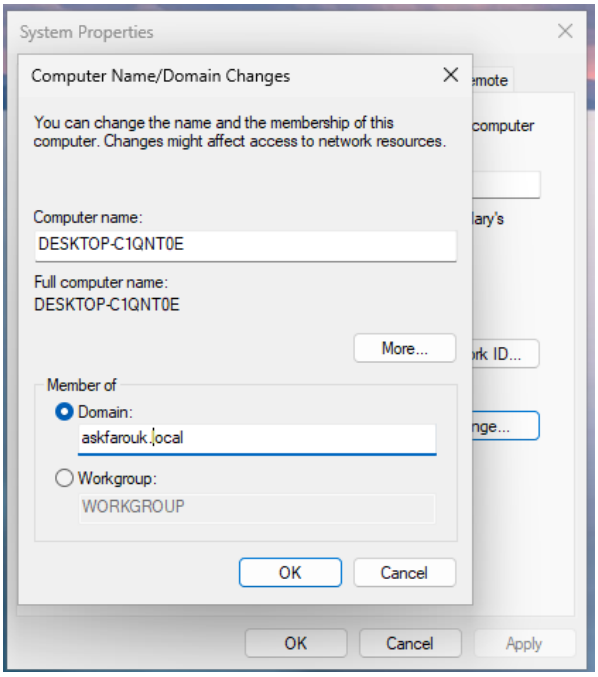
Search for Change workgroup name, or run sysdm.cpl to open System Properties. This method also works on domain-capable Windows 10 editions.

Choose Change on the Computer Name tab



System Properties currently shows WORKGROUP membership. Select Change to choose a domain.

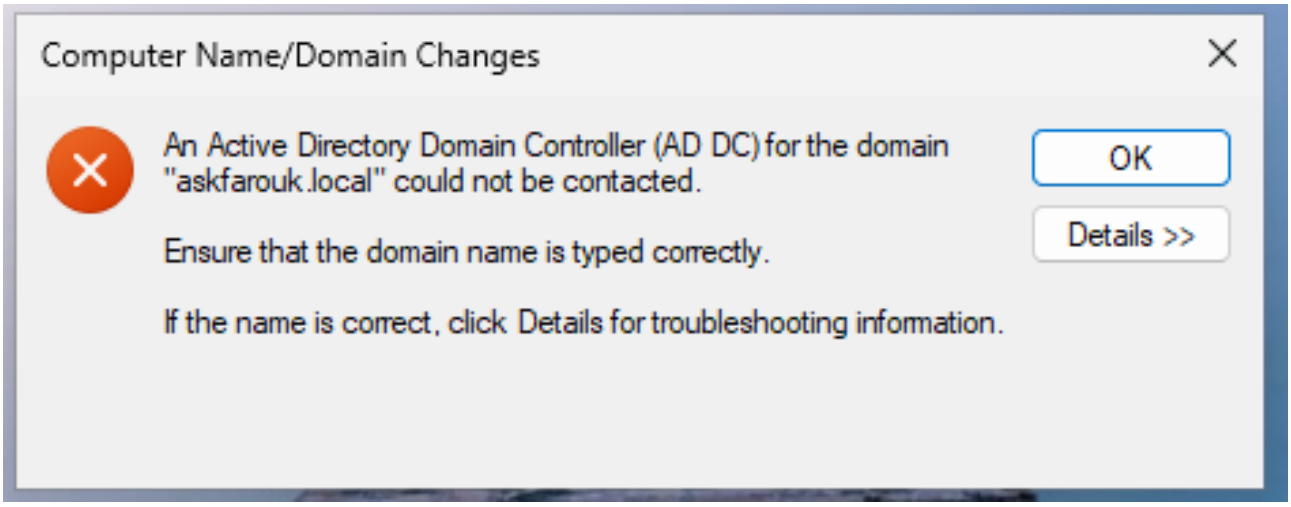
Enter the Active Directory domain



Select Domain, enter askfarouk.local and select OK. Use the on-premises AD domain, not Microsoft Entra ID enrollment.

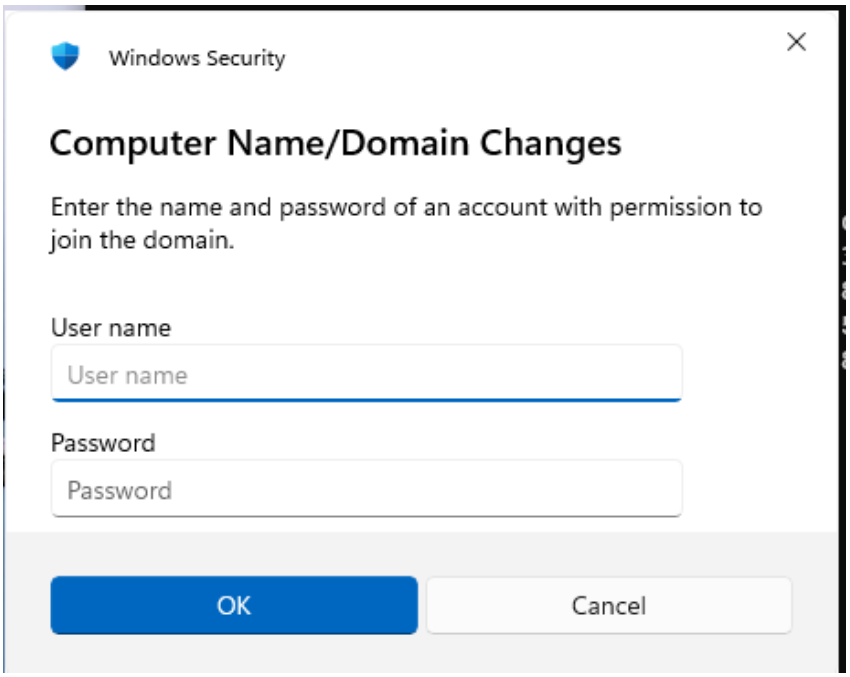
2 / Diagnose DNS and authorize the join

Investigate the domain-controller lookup failure



This error states that a domain controller could not be contacted. Check the exact error, server availability, DNS and time. In this example, correcting client DNS resolved discovery. Use 192.168.77.129 for domain DNS, then verify the server name with nslookup before retrying.

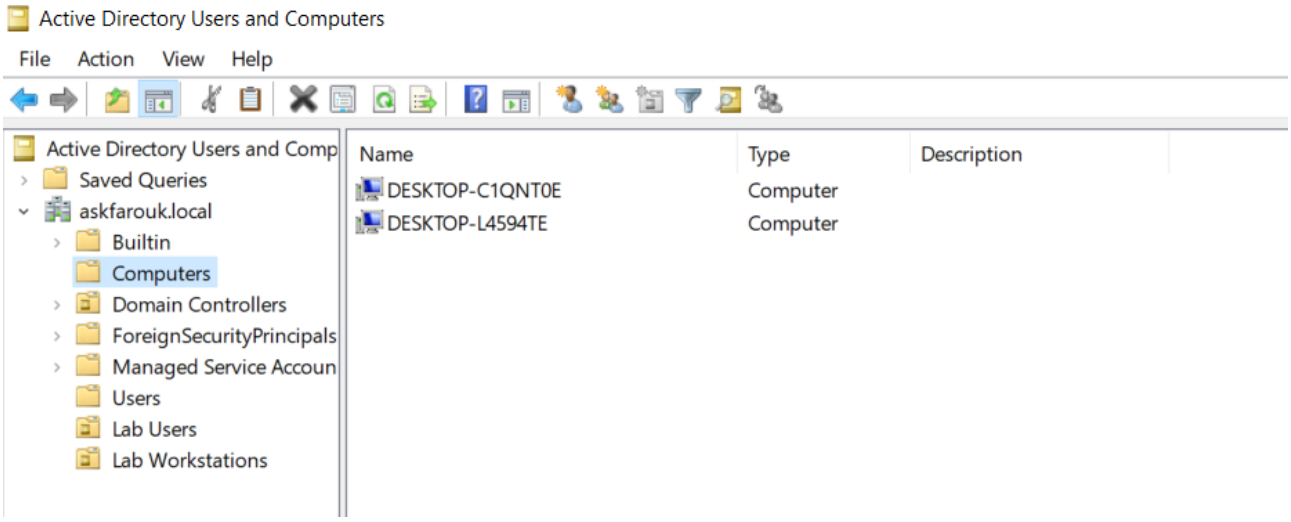
Provide authorized domain-join credentials



After DNS correction the join reaches a credential prompt. Enter an authorized account such as ASKFAROUK\Administrator securely. Continue until the domain welcome message appears, then restart. This prompt alone does not prove that domain joining completed.

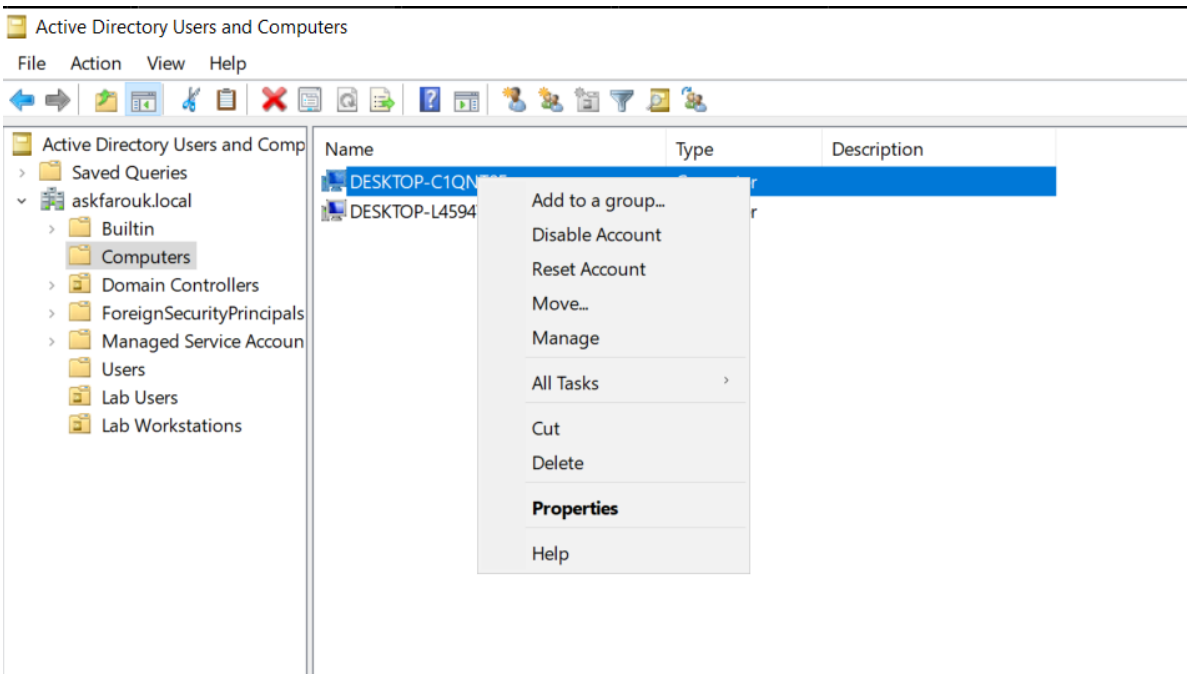
3 / Move computer accounts into the workstation OU

Before the move: the default Computers container



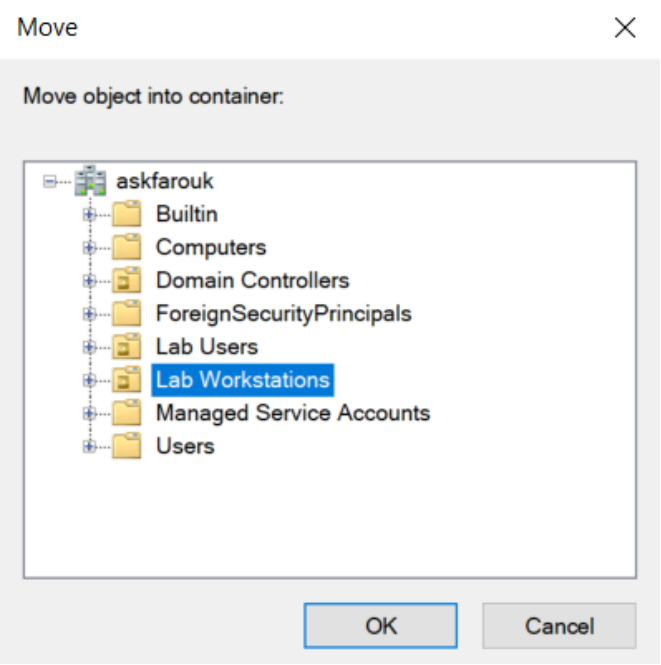
Both client computer accounts appear in the default Computers container after domain joining. This is the starting location, not the required final OU. Computers is a container, not a security group; GPOs cannot be linked directly to it.

Right-click the computer account and choose Move



In ADUC, select a client computer account, right-click it and choose Move. Repeat for the other client. Moving the object does not rename the workstation or change its domain membership.

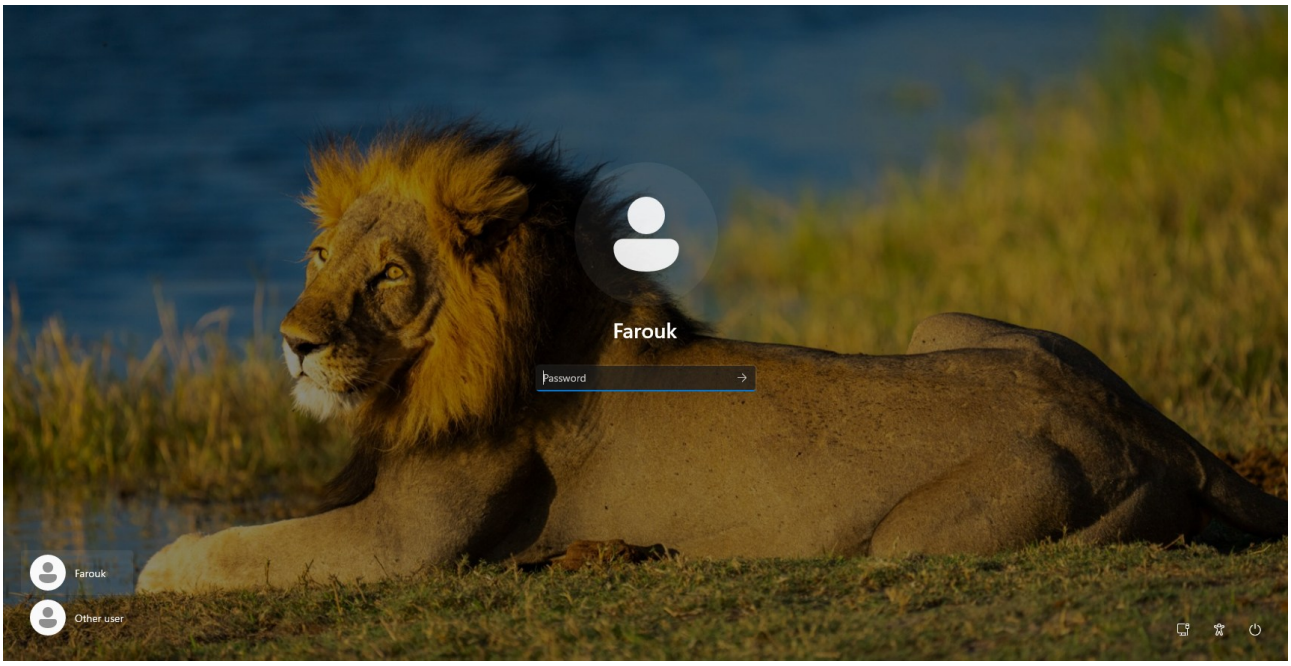
Choose Lab Workstations as the destination



Select the Lab Workstations organizational unit and confirm with OK. This moves the computer object into the OU; it does not add the computer to a security group.

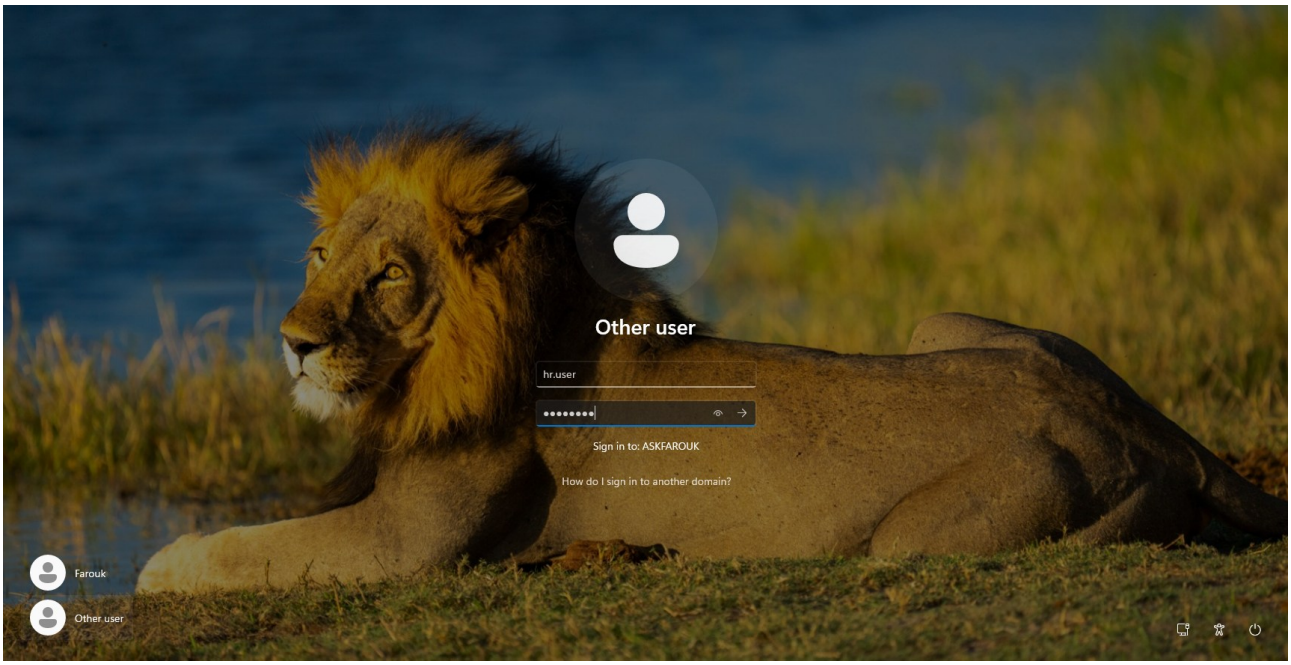
Expected results

Choose Other user after restarting



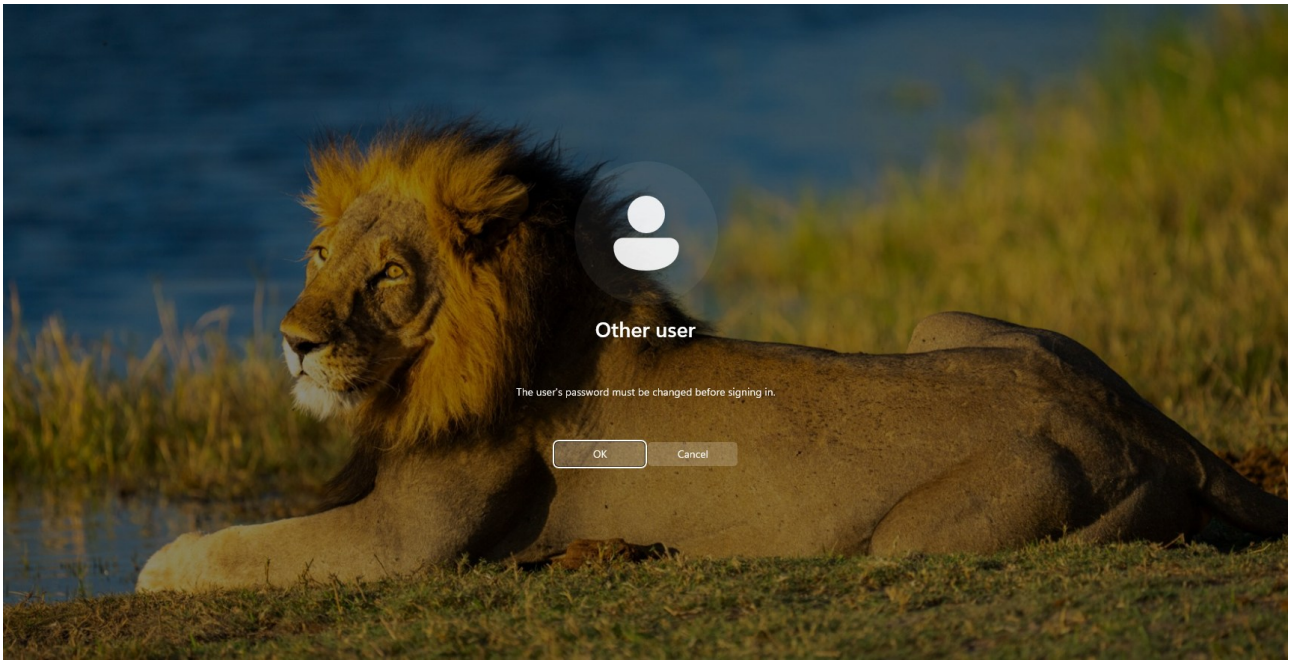
Select Other user rather than signing into the existing local account. The sign-in screen is not proof of a successful domain-user session.

Check the domain sign-in context



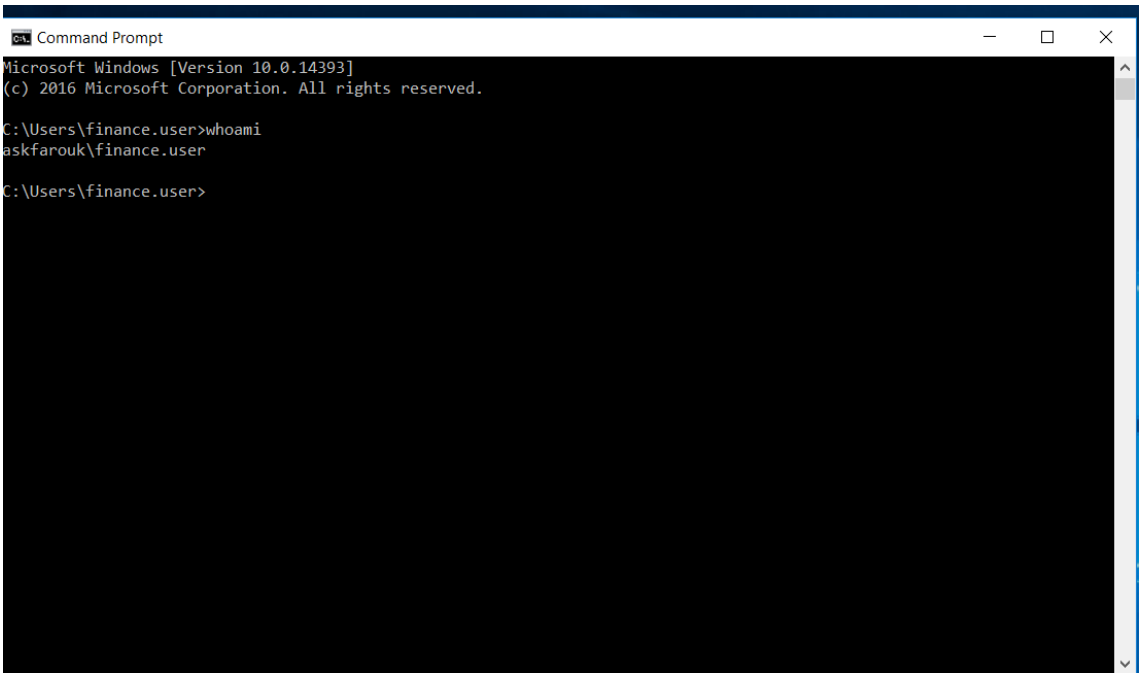
The Other user screen displays ASKFAROUK as the sign-in domain. Use ASKFAROUK\hr.user or hr.user@askfarouk.local, then sign in. Once at the desktop, run whoami to prove which account is active.

Complete the required first-sign-in password change



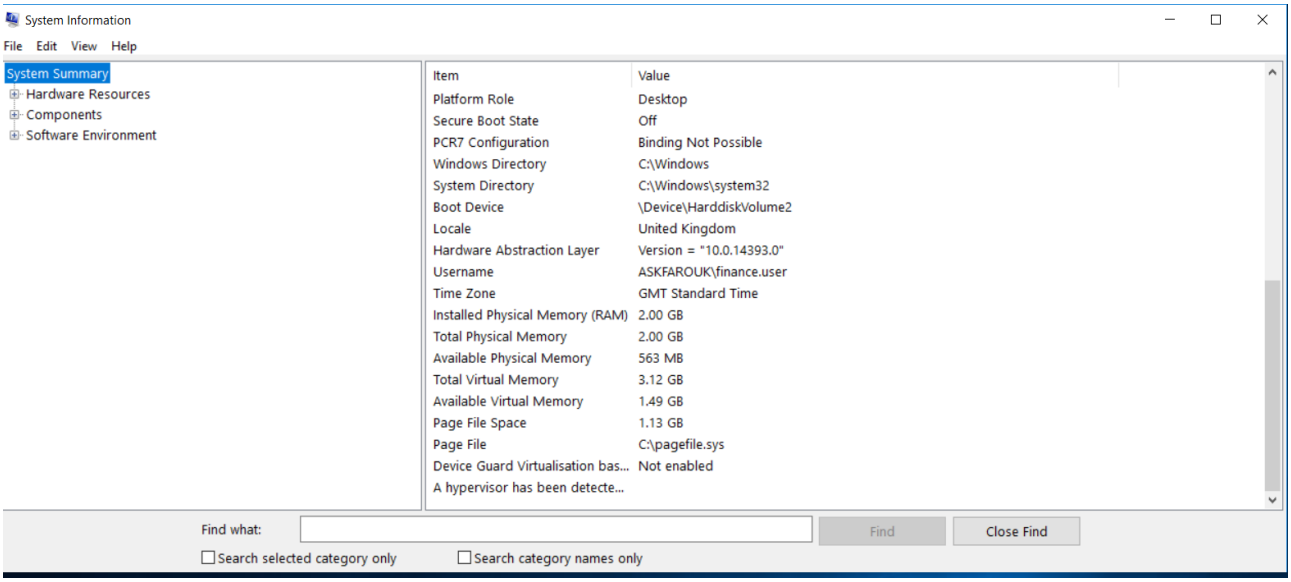
The domain account requests a password change, matching the flag selected when hr.user was created. Complete the change and reach the desktop. This first-sign-in step does not replace Task 07's separate password-reset and policy exercise.

Windows 10: domain-user sign-in verified



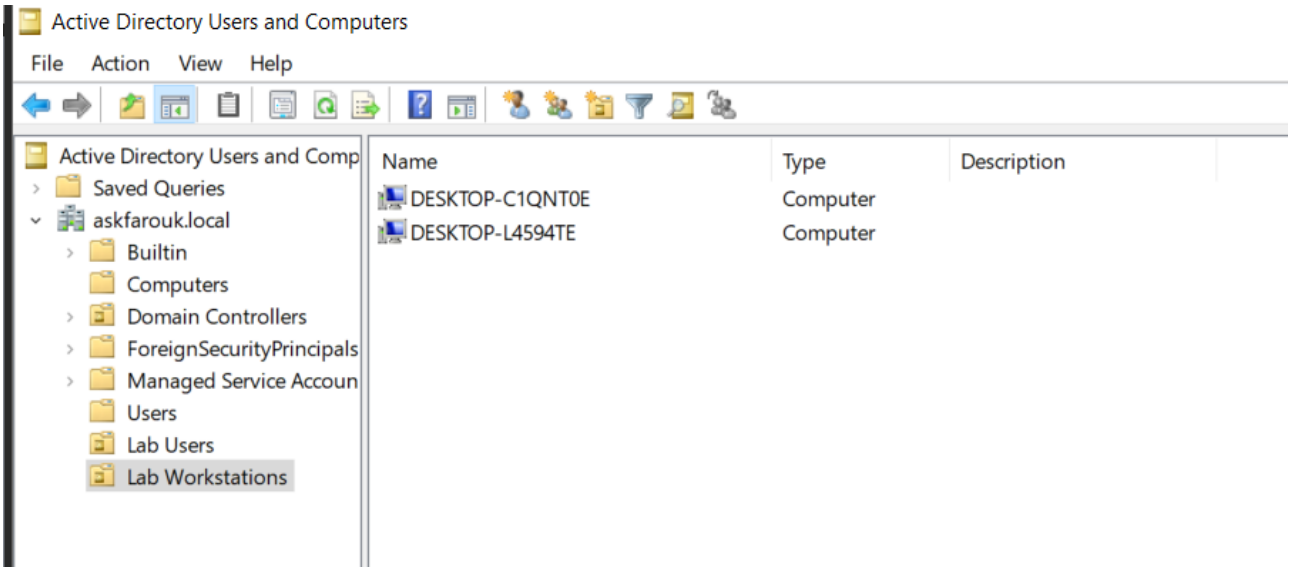
After signing into Windows 10 as finance.user, whoami returns askfarouk\finance.user. This confirms that the active session uses the domain employee account, rather than a similarly named local account.

Windows 10: confirm the signed-in identity



System Information shows Username ASKFAROUK\finance.user, corroborating the domain-user session. This part of System Information does not display computer domain membership; verify that separately in System Properties or by checking the computer object in ADUC.

Both clients are in Lab Workstations



ADUC shows both Computer objects inside the Lab Workstations OU under askfarouk.local. The screenshots retain the clients' automatic DESKTOP names rather than the course labels PC10 and PC11. Verify which object belongs to each workstation using its actual computer name.

DAY 1 / TASK 06

Verify and hand over Day 1

Demonstrate that your environment is ready for administration work on Day 2. Record the configuration so another administrator could continue.

> Your deliverable: A verified network, directory, account and workstation baseline.

Before you begin

• Tasks 01-05 have been attempted. Use this slot to finish essential dependencies.

Assignment

1. Demonstrate the environment to the trainer and resolve any remaining dependency failures.

2. Record server/client names, addresses, domain and OU structure in your handover notes.

3. Shut down the lab VMs cleanly at the end of the session, unless the trainer instructs otherwise.

Verification checklist

□ All three machines start and communicate on the intended network.

□ Client DNS lookups return the correct server address.

□ ADUC shows the expected OUs, users, groups and computer objects.

□ Employee domain sign-in succeeds.

□ The configuration and any outstanding issue are recorded in notes.

□ Trainer has observed the working Day 1 baseline.

Evidence: Use the task notes below for the handover. Show live results rather than relying only on screenshots.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

SECTION 02 / 29 October 2026

02

Day 2

Operate the environment. Protect data and restore service.

DAY 2 / TASK 07

Administer passwords

An employee needs a password reset. Require a change at the next sign-in, then enforce a minimum password standard for domain users.

> Your deliverable: A demonstrated next-sign-in password change and a tested domain password policy.

Before you begin

• Day 1 baseline works and both employee accounts are available.

Assignment

1. Reset finance.user's password and select User must change password at next logon.

2. Sign in as that user on a client and complete the required change.

3. Configure a dedicated domain-root GPO for a minimum password length of 12 characters and enabled complexity. Ensure its link precedence makes those settings effective.

4. Show the effective domain policy. Try changing a test user password to a noncompliant value, then a compliant value.

Troubleshooting tip / Link Order

> If the effective minimum password length still shows the old value, open GPMC and select askfarouk.local → Linked Group Policy Objects. Select your passwordlevel (or Lab Domain Password Policy) link and use the up-arrow control to move it to Link Order 1, above Default Domain Policy. Link Order 1 has the highest precedence among these domain-root links when neither is Enforced. Keep Link Enabled set to Yes and Enforced set to No for this lab. On the domain controller, run gpupdate /force and wait until it finishes. Then run Get-ADDefaultDomainPasswordPolicy | Select-Object MinPasswordLength, ComplexityEnabled separately. Confirm 12 and True; the settings shown inside the GPO editor alone are not proof of the effective domain policy.

Verification checklist

□ The correct employee password is reset.

□ Next-sign-in change is enabled and the client prompts for it.

□ Employee completes the password change successfully.

□ Password policy GPO is linked at the domain root with appropriate precedence.

□ Effective domain policy shows a minimum length of 12 and complexity enabled.

□ A noncompliant password change is rejected.

□ A compliant password change succeeds.

Evidence: Show the effective policy and successful user workflow. Never record or screenshot the actual passwords.

Verification commands

```
Get-ADDefaultDomainPasswordPolicy | Select-Object MinPasswordLength,ComplexityEnabled,MinPasswordAge,MaxPasswordAge
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

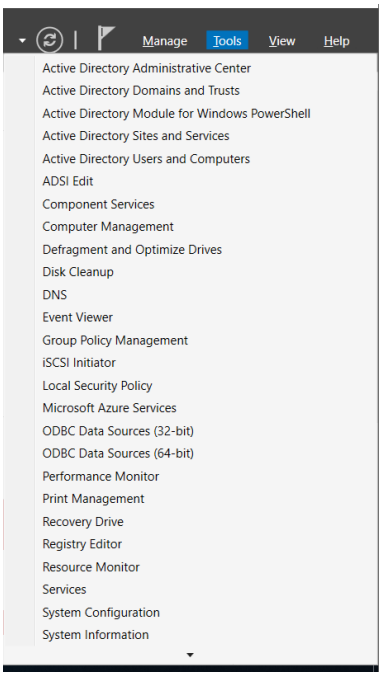
TASK 07 / SCREENSHOT WALKTHROUGH

Visual reference

These images show password-policy settings and a rejected password change. To enforce the default domain-user password policy, link the GPO at the askfarouk.local domain root, not Lab Users, and check effective settings on the domain controller. The GPO name in the images is passwordlevel; the course calls it Lab Domain Password Policy. Either descriptive name is fine, but scope and precedence determine the result. The two captures showing the OU link are excluded from the walkthrough.

1 / Open Group Policy Management and scope the policy

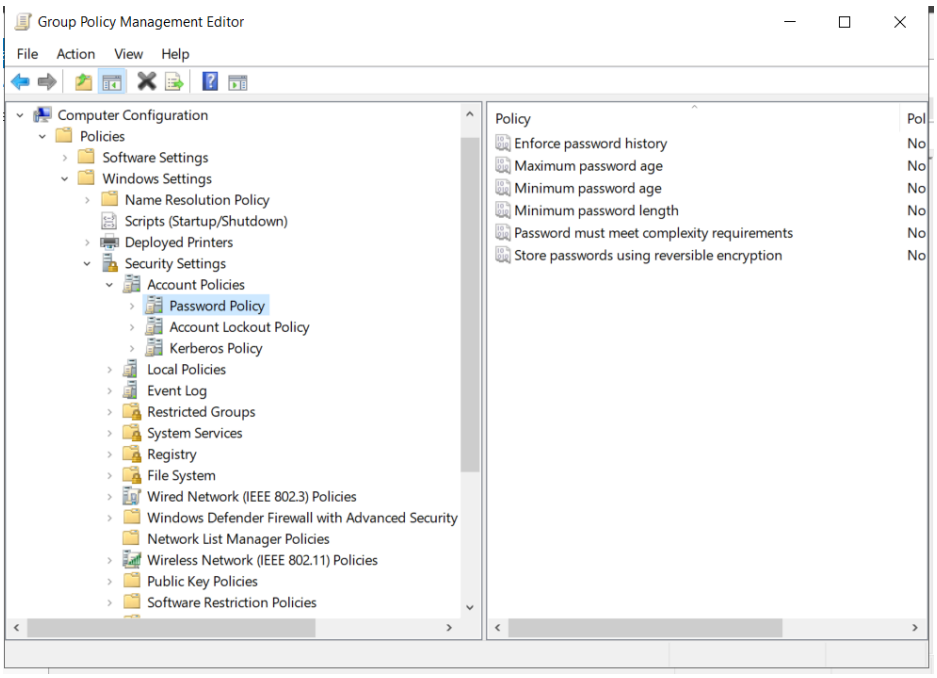
Open Group Policy Management



In Server Manager, click Tools → Group Policy Management. Right-click askfarouk.local itself, then create and link a dedicated password-policy GPO, or link your existing passwordlevel GPO there. Do not link the domain-user password policy only to Lab Users. Review domain-root link precedence and refresh policy on DC01.

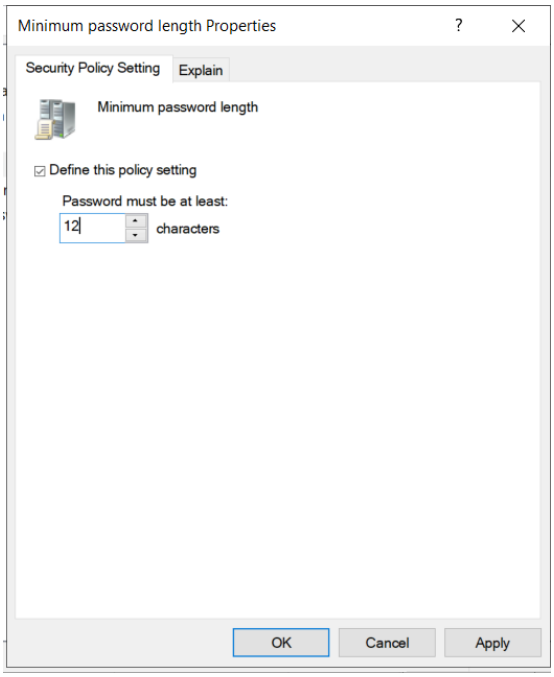
2 / Configure the password requirements

Find the computer password-policy settings



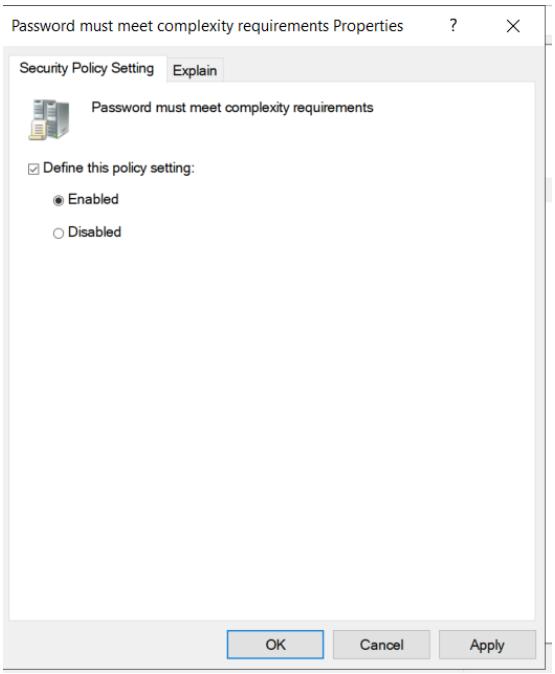
Edit the GPO and open Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy. The settings are under Computer Configuration even though they govern domain-user passwords.

Define a minimum length of 12 characters



Open Minimum password length, select Define this policy setting, set 12 characters and confirm. This configures the GPO; verify the effective domain policy separately.

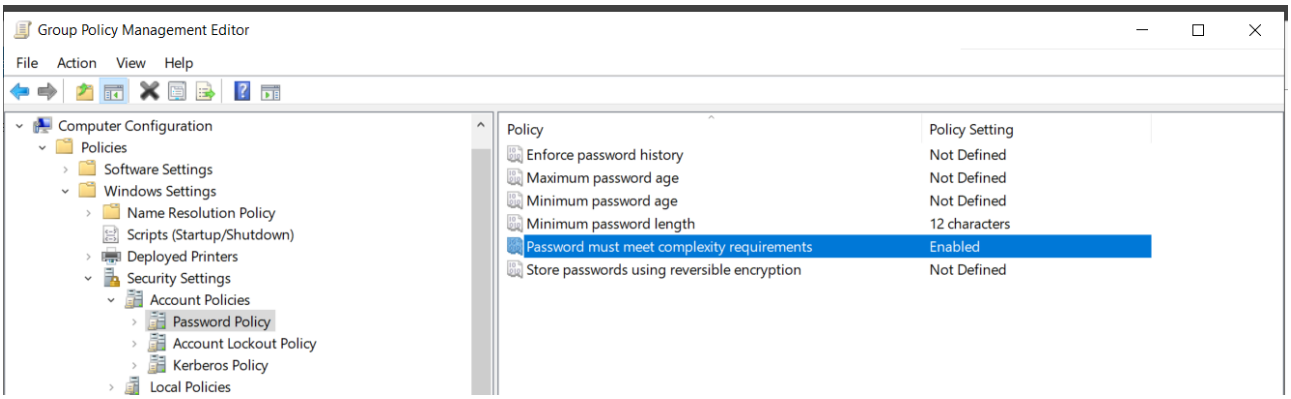
Enable password complexity



Open Password must meet complexity requirements, define the setting and select Enabled. Confirm the change, then verify that the domain-root policy is effective. Passwords should be kept out of screenshots and notes.

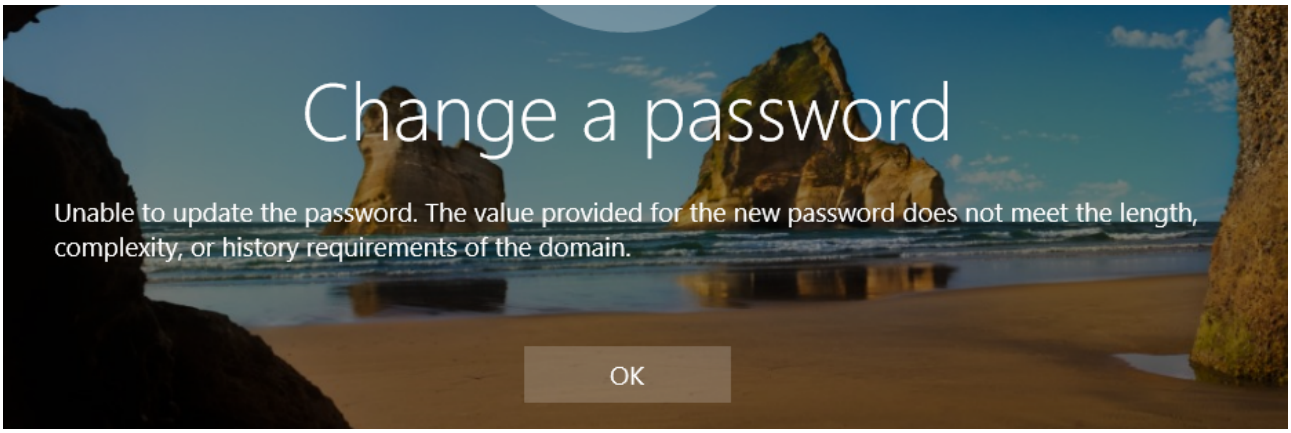
Expected results

The GPO contains the requested settings



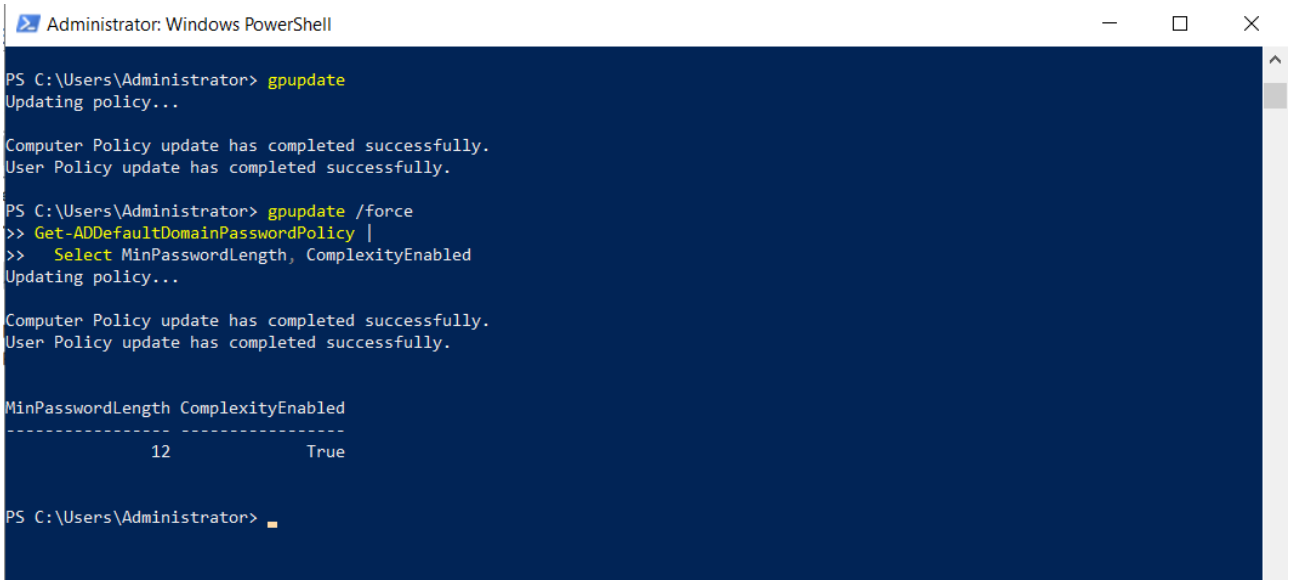
The editor shows Minimum password length: 12 characters and Password must meet complexity requirements: Enabled. This proves what the GPO contains, not that it is applied. On DC01, use Get-ADDefaultDomainPasswordPolicy to confirm MinPasswordLength and ComplexityEnabled.

A noncompliant password change is rejected



Windows reports that the new password does not meet length, complexity or history requirements. This is a useful negative test, but it does not identify which GPO is effective. Verify the domain policy first, then demonstrate an accepted compliant password change and successful sign-in.

Effective domain password policy verified



After policy refresh, Get-ADDefaultDomainPasswordPolicy returns MinPasswordLength 12 and ComplexityEnabled True. This confirms the effective default domain password settings. If the old length appears, check the domain-root link and set the intended policy to Link Order 1 before refreshing and testing again.

DAY 2 / TASK 08

Provision a data volume

Company files need their own data volume. Add storage without modifying the operating system disk.

> Your deliverable: A new NTFS data volume ready to hold departmental files.

Before you begin

• DC01 is working. Save work and shut it down before adding the virtual disk.

Assignment

1. Add a new 20 GB virtual disk to DC01, then start the server.

2. Identify the new disk by its capacity. Bring it online and initialize it as GPT.

3. Create an NTFS volume, assign drive letter E: and label it CompanyData. Leave D: assigned to the VMware DVD drive. Use the separate F: volume for backups.

4. Create E:\Company. Inside it create test.txt, write a short sentence and save. Restart the server, reopen E:\Company\test.txt and confirm the saved content is unchanged.

Verification checklist

□ A separate 20 GB virtual disk is attached to DC01.

□ Trainee correctly distinguishes the data disk from the OS disk.

□ New disk is online and initialized as GPT.

□ Volume uses NTFS, drive letter E: and the CompanyData label.

□ E:\Company exists and accepts a test file.

□ Test data remains accessible after restarting DC01.

Evidence: Show VMware disk configuration, Disk Management and the test file after restarting.

Verification commands

```
Get-Disk

Get-Volume
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

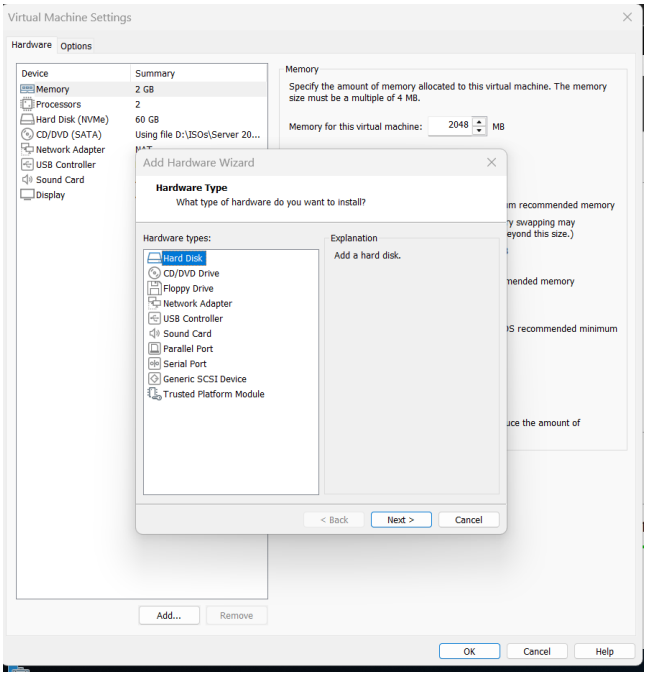
TASK 08 / SCREENSHOT WALKTHROUGH

Visual reference

The screenshots demonstrate a new 20 GB SATA data disk, initialized as GPT and formatted as NTFS. CompanyData uses E:, the VMware DVD drive uses D:, and backups use a separate F: volume. Earlier screenshots show the default label New Volume; the final screenshot confirms CompanyData. Disk numbers change between captures: identify the new disk by capacity and contents, never by assuming Disk 0 or Disk 1 is always the OS disk.

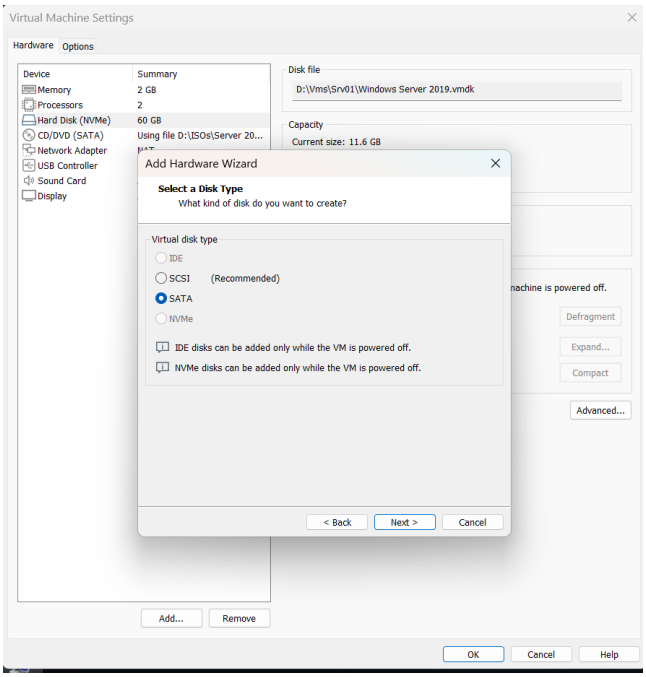
1 / Attach a new virtual data disk

Add a hard disk to the server VM



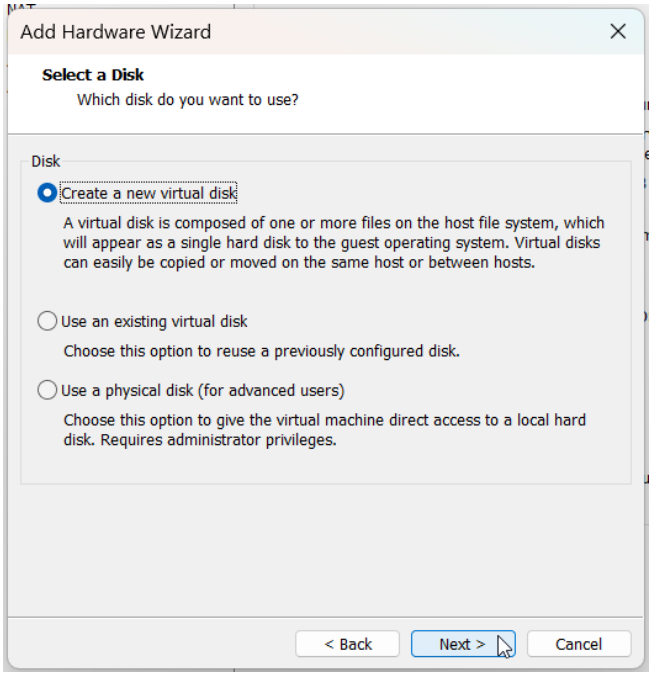
Shut down the server first. Open VMware settings → Add → Hard Disk. Add a separate disk rather than replacing or resizing the existing OS disk.

Choose the virtual disk controller



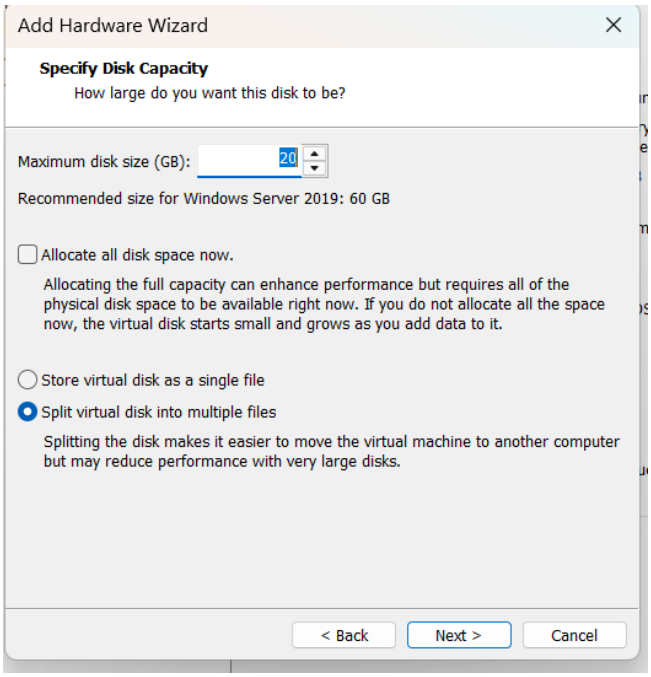
The captured example selects SATA. This is the controller choice, not Windows Basic/Dynamic disk type or GPT/MBR partition style.

Create a new virtual disk



Select Create a new virtual disk. Keep the existing Windows system disk intact.

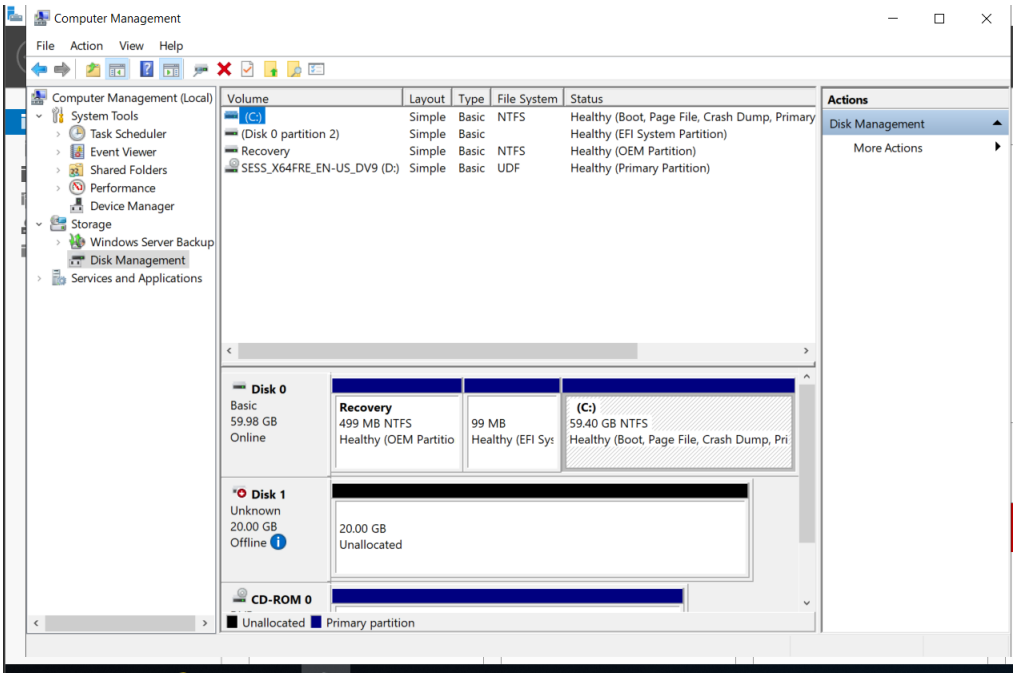
Allocate 20 GB for the data disk



Set Maximum disk size to 20 GB. This is an additional data disk; the wizard's recommended OS disk capacity is not the requirement for this data-only volume.

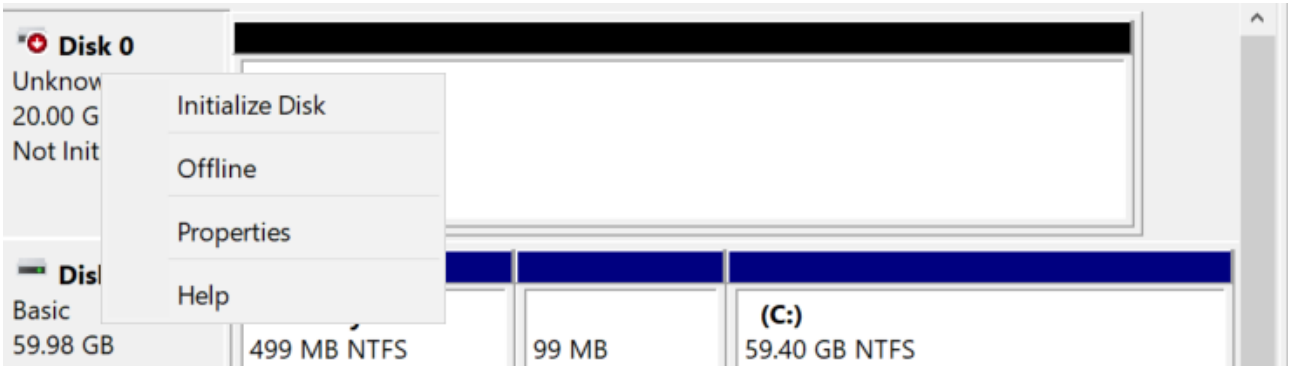
2 / Identify and initialize the disk

Find the new 20 GB disk in Disk Management



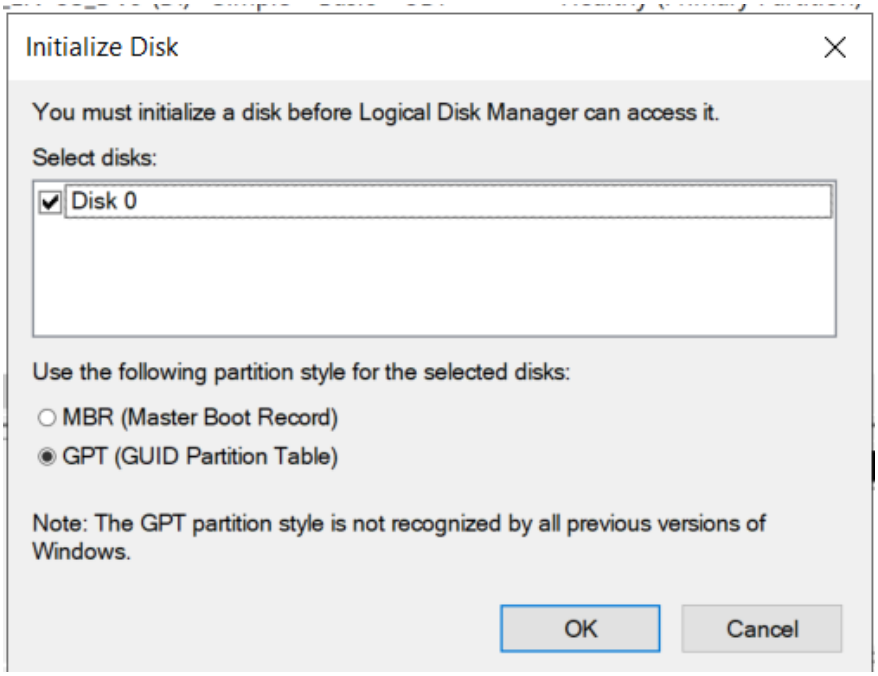
Start the server, open Computer Management → Storage → Disk Management and identify the new 20 GB disk. Here it appears as Disk 1; later captures show it as Disk 0, so always check capacity and existing partitions.

Initialize only the new empty disk



Bring the new disk online if necessary. Right-click its disk label and choose Initialize Disk. The selected 20 GB empty disk is distinct from the roughly 60 GB disk containing C:.

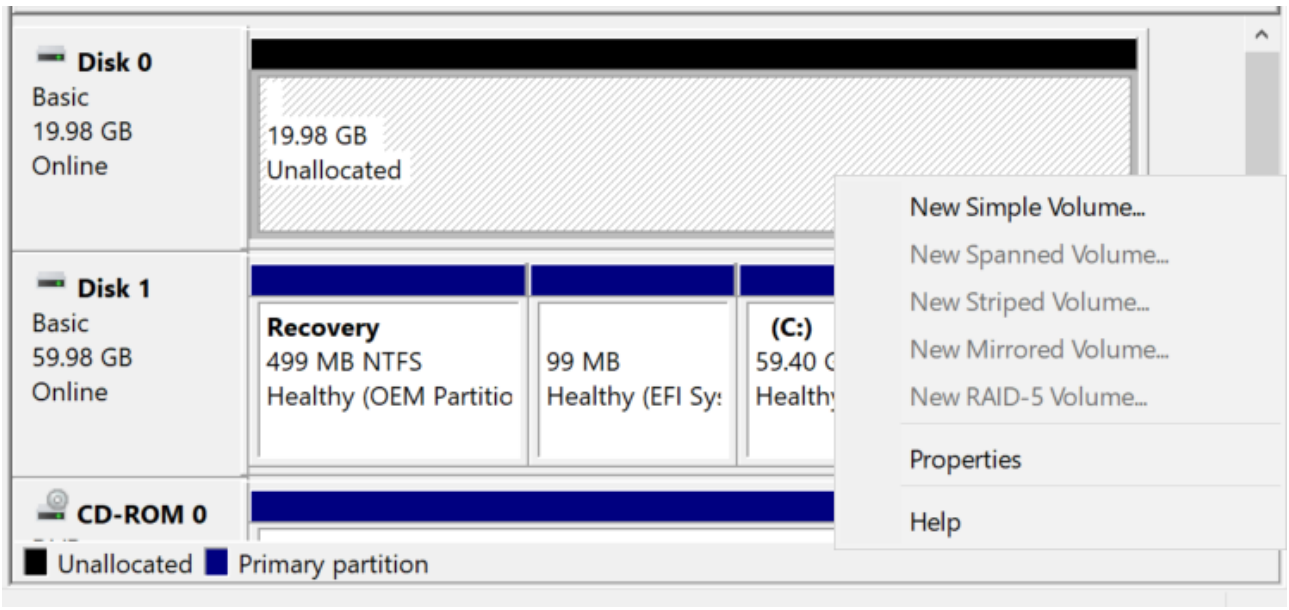
Choose GPT partition style



Select GPT (GUID Partition Table) for the new data disk. Keep the disk Basic; no Dynamic conversion is needed.

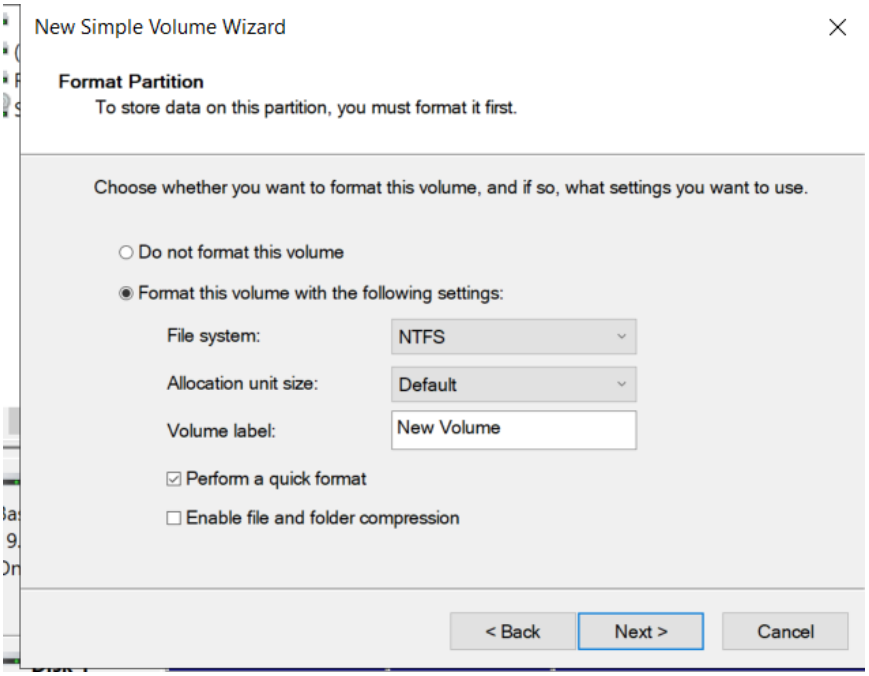
3 / Create and format the volume

Create a New Simple Volume



Right-click the unallocated space on the new 20 GB disk → New Simple Volume. Use the intended capacity and assign E:. Do not select the partitions containing C:.

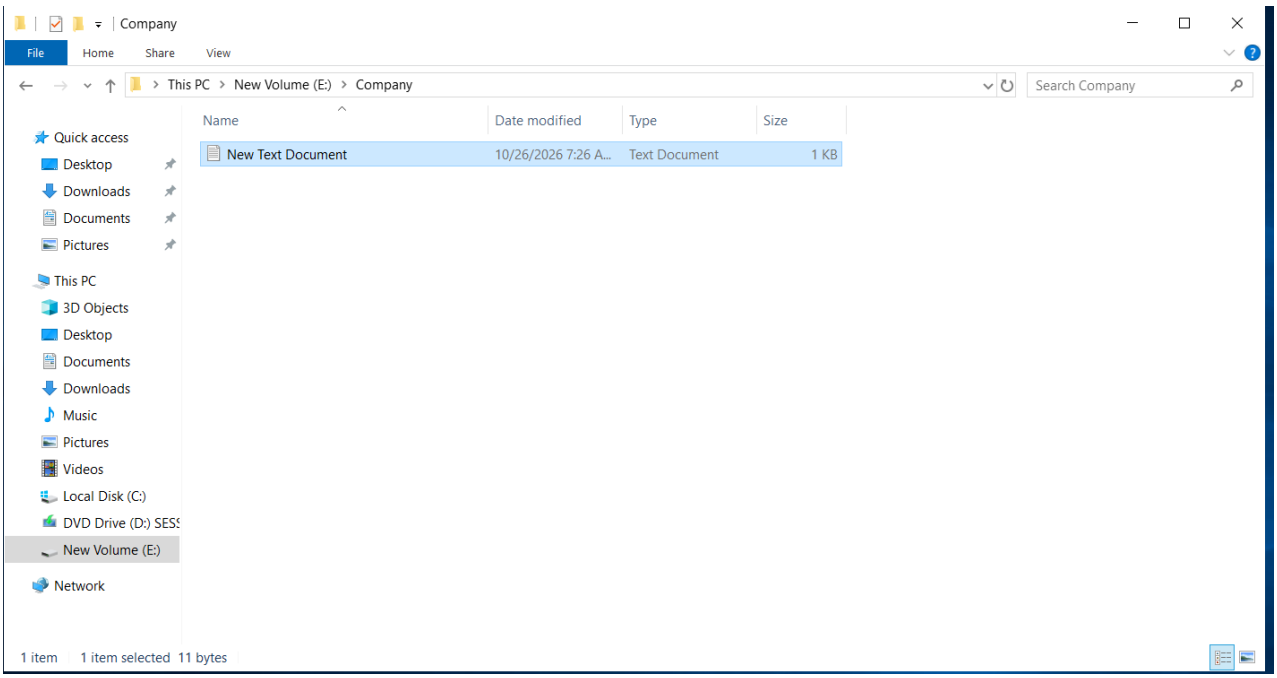
Format as NTFS and set the label



Choose NTFS with the default allocation unit size and quick format. Replace the captured default label New Volume with CompanyData before finishing. The demonstration assigns E: because D: is already occupied.

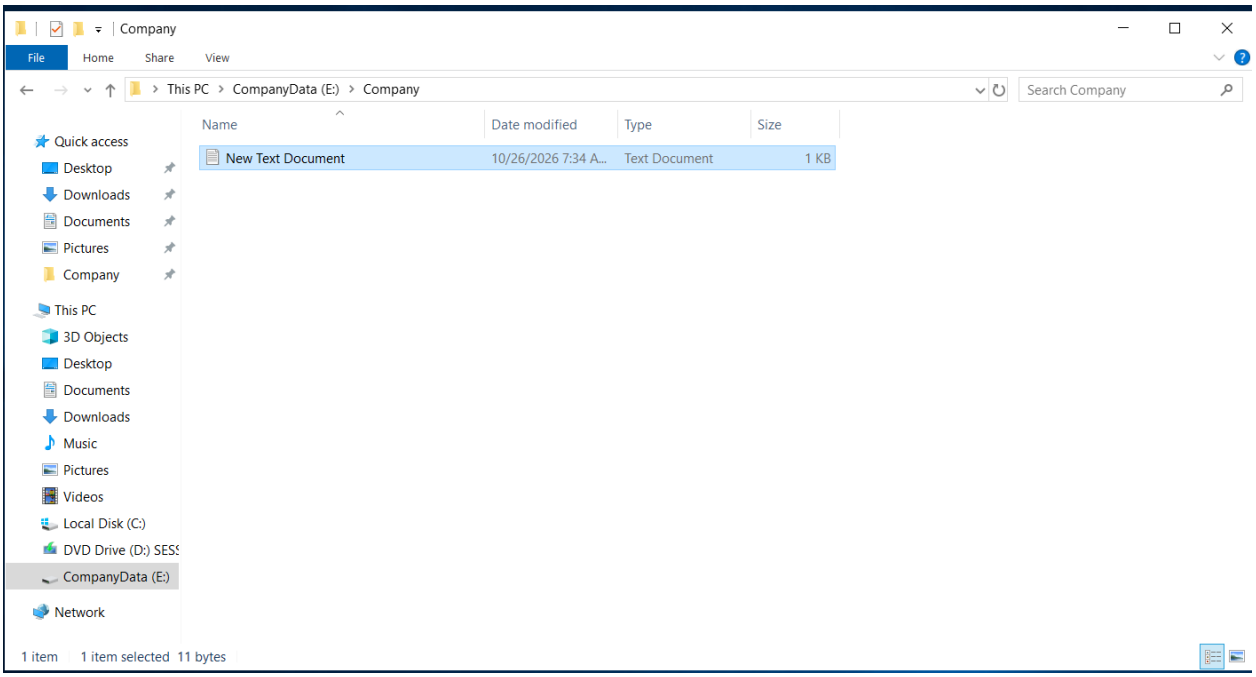
Expected results

Create Company and a saved test file



File Explorer shows E:\Company with a text document on the new data volume. Put a recognizable sentence in the file and save it. Restart the server, reopen it and confirm the text remains. This screenshot proves the folder/file exist, but does not by itself prove the post-restart check.

CompanyData and a non-empty test file



File Explorer shows E:\Company on CompanyData (E:) with a saved text document. The status bar reports 11 bytes, confirming the file is no longer empty. Reopen it after restarting the server and confirm that the saved sentence is unchanged; this screenshot alone does not establish that a restart occurred.

DAY 2 / TASK 09

Publish departmental storage

Finance employees must edit their departmental files. HR employees must not access them. Prove both outcomes from a client.

> Your deliverable: A Finance share with tested group-based access control.

Before you begin

• CompanyData volume exists and GG_Finance/GG_HR contain the correct users.

Assignment

1. Create E:\Company\Finance and share it as Finance.

2. Set share permissions to allow GG_Finance Change and Administrators Full Control. Remove broad unintended access.

3. Set NTFS permissions to allow GG_Finance Modify, while retaining SYSTEM and Administrators Full Control. Review inherited access.

4. Test file creation, editing and deletion as finance.user. Sign out and test denied access as hr.user.

Verification checklist

□ The Finance folder and \\DC01\Finance share exist.

□ Share and NTFS permissions are both reviewed.

□ Departmental access is assigned through GG_Finance.

□ SYSTEM and Administrators retain required NTFS access.

□ No unintended broad group grants HR access.

□ finance.user creates, edits and deletes a test file from a client.

□ hr.user receives access denied in a separate sign-in session.

□ Trainee explains how share and NTFS permissions combine for network access.

Evidence: Show both permission layers and demonstrate allowed and denied access using standard employee accounts.

Verification commands

```
Get-SmbShareAccess -Name Finance

icacls E:\Company\Finance
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

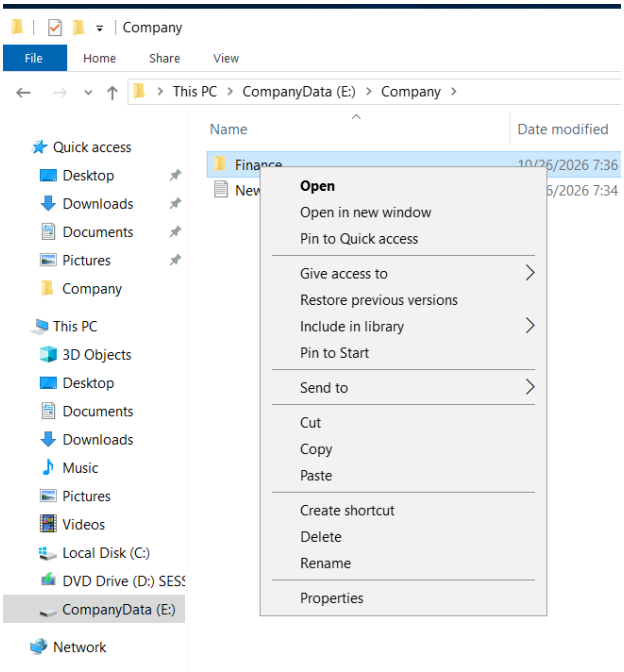
TASK 09 / SCREENSHOT WALKTHROUGH

Visual reference

The demonstration uses E:\Company\Finance, shared as Finance, and the server address 192.168.77.129. The updated share-permission screenshots confirm GG_Finance Change and Read, and Administrators Full Control. The NTFS screenshots show a separate layer: verify GG_Finance Modify, SYSTEM and Administrators Full Control, and review the remaining Users entry for unintended access. Check both layers separately.

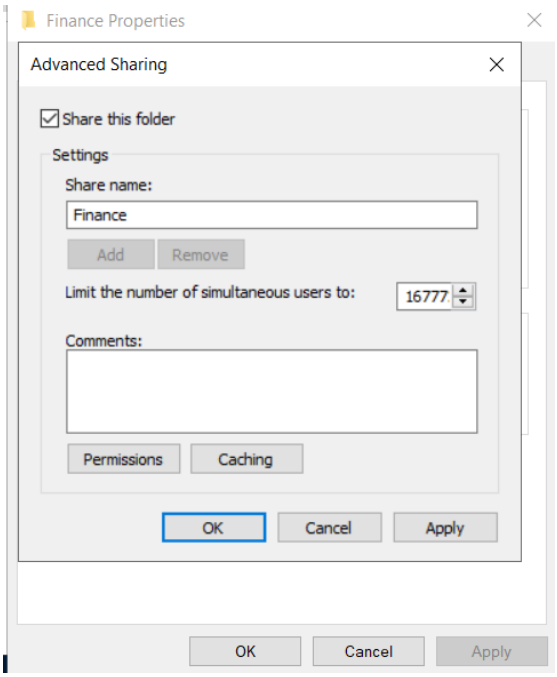
1 / Publish the Finance share

Open the Finance folder properties



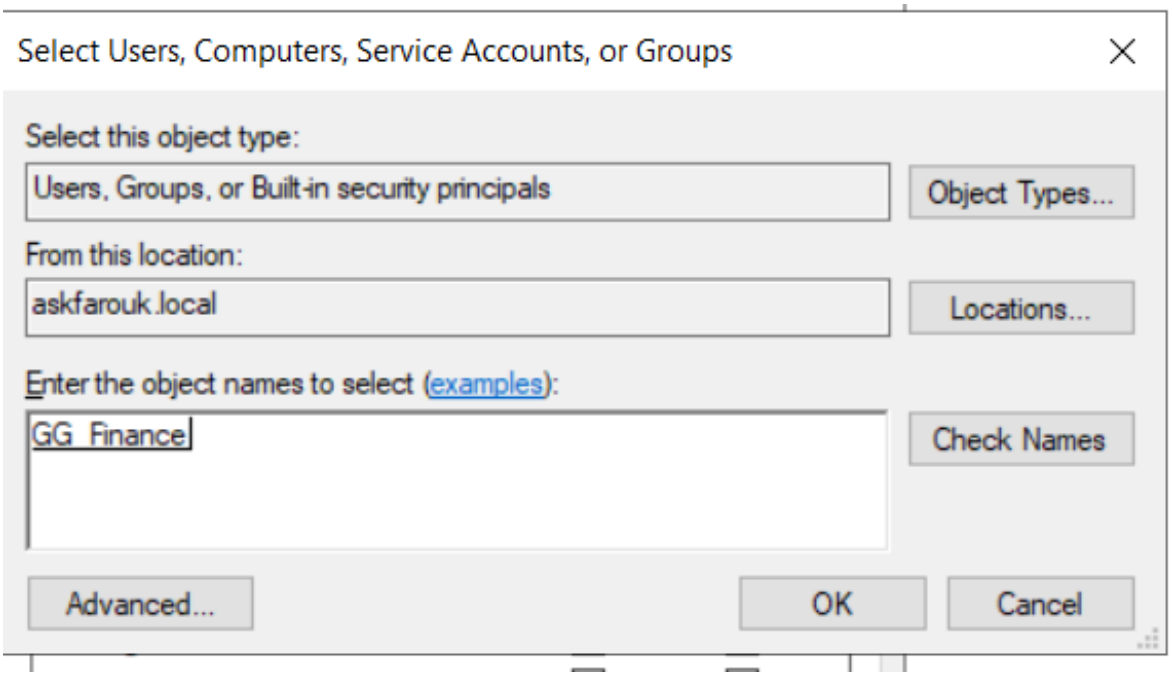
Create Finance inside E:\Company. Right-click Finance and select Properties.

Enable Advanced Sharing



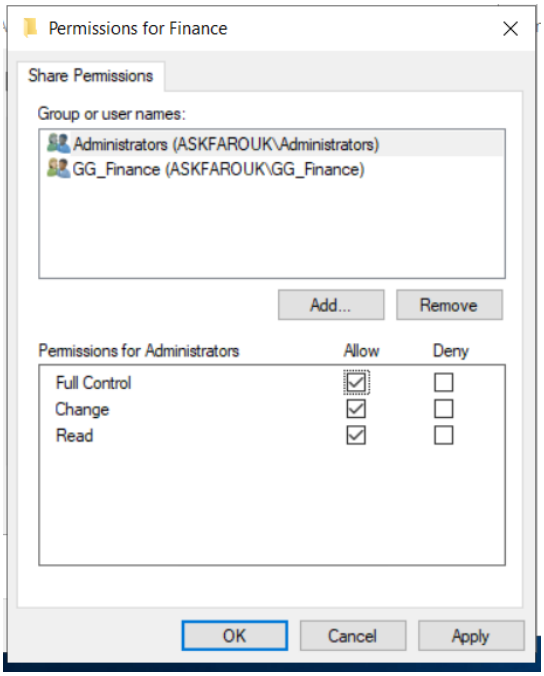
On the Sharing tab choose Advanced Sharing, select Share this folder and set the share name to Finance.

Add the domain security group



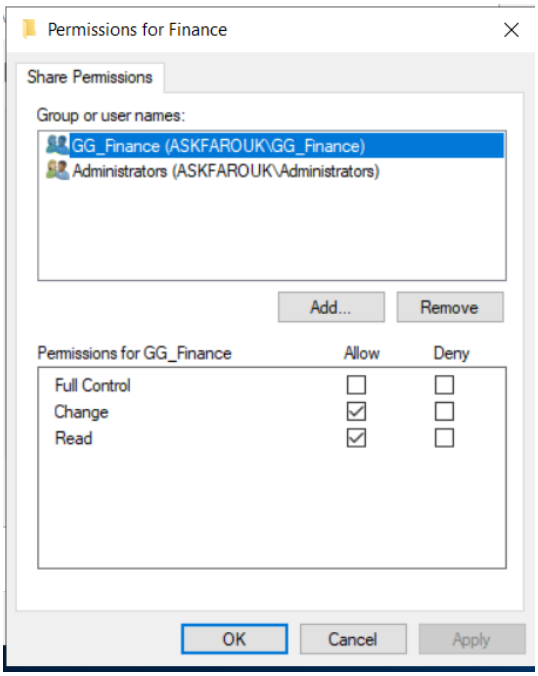
In share Permissions choose Add, enter GG_Finance and use Check Names. Confirm the location is askfarouk.local.

Share permissions: Administrators Full Control



Administrators is selected and Allow Full Control, Change and Read are checked. GG_Finance is also present. This verifies the administrative share-permission entry; select Finance separately to inspect its permissions.

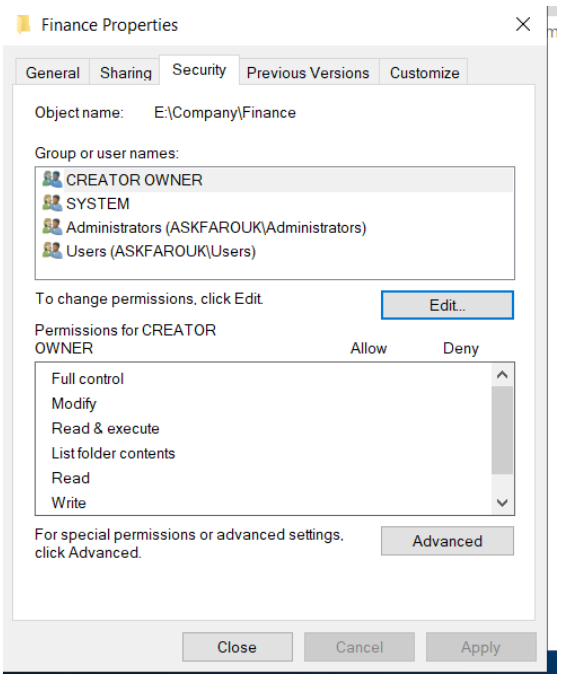
Share permissions: Finance Change and Read



GG_Finance is selected. Allow Change and Read are checked, while Full Control is unchecked. Alongside the Administrators screenshot, this confirms the requested share ACL. NTFS permissions remain a separate layer and still need their own review.

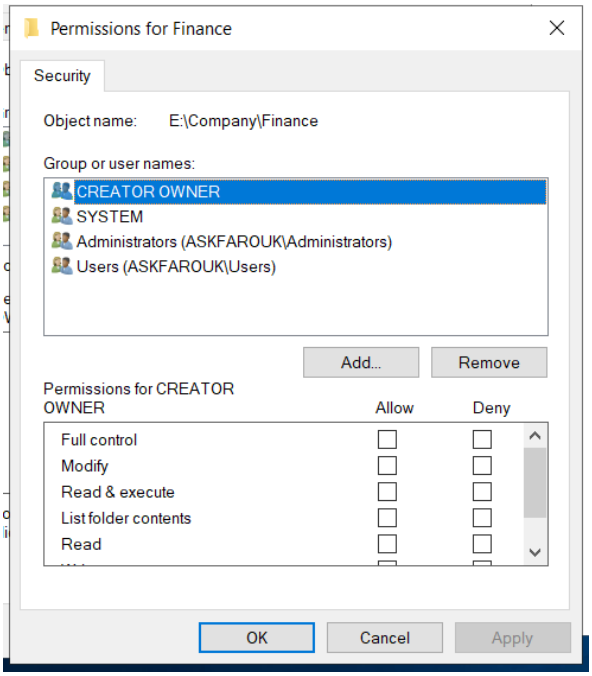
2 / Configure NTFS permissions

Inspect the Security tab



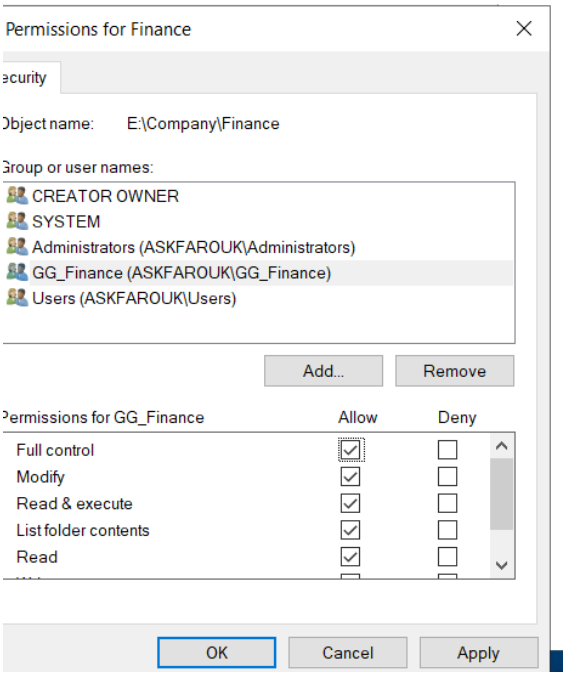
This is the NTFS permission layer. Review inherited permissions and retain SYSTEM and Administrators. Inspect the remaining Users entry for unintended broad access.

Edit the NTFS ACL



Choose Edit → Add and add GG_Finance. If entries are inherited, use Advanced to review inheritance and remove unintended access while preserving SYSTEM and Administrators.

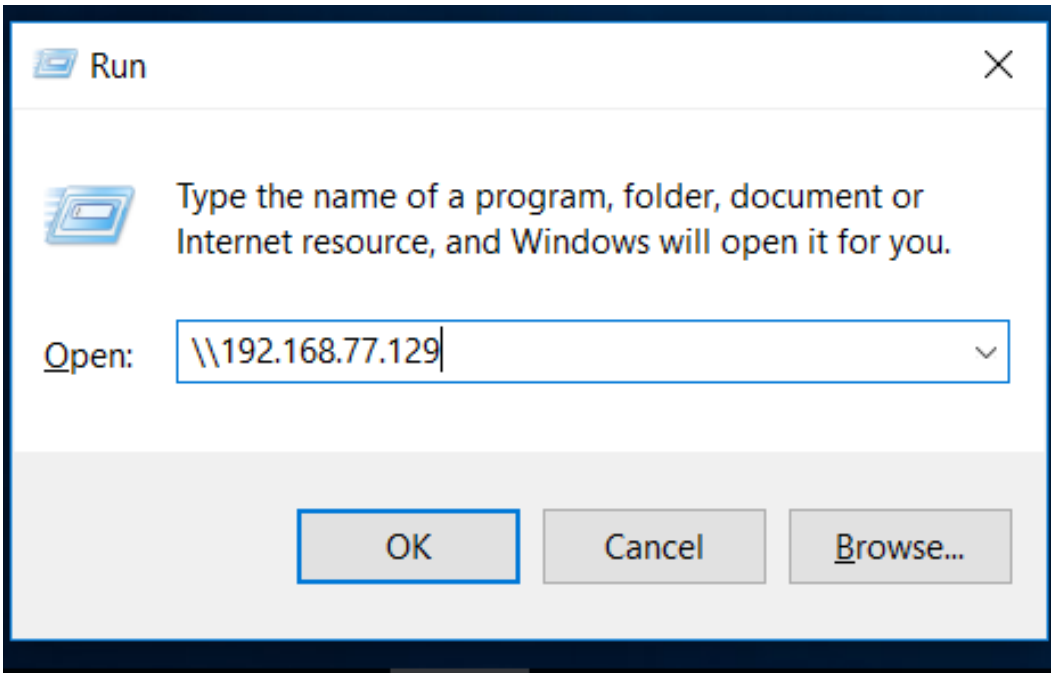
Assign GG_Finance Modify



Modify is selected for GG_Finance. Keep SYSTEM and Administrators Full Control. Review the separate Users entry; Finance's correct entry does not prove that other groups lack access. Prefer removing an unintended Allow over adding an explicit Deny.

3 / Test from an employee client

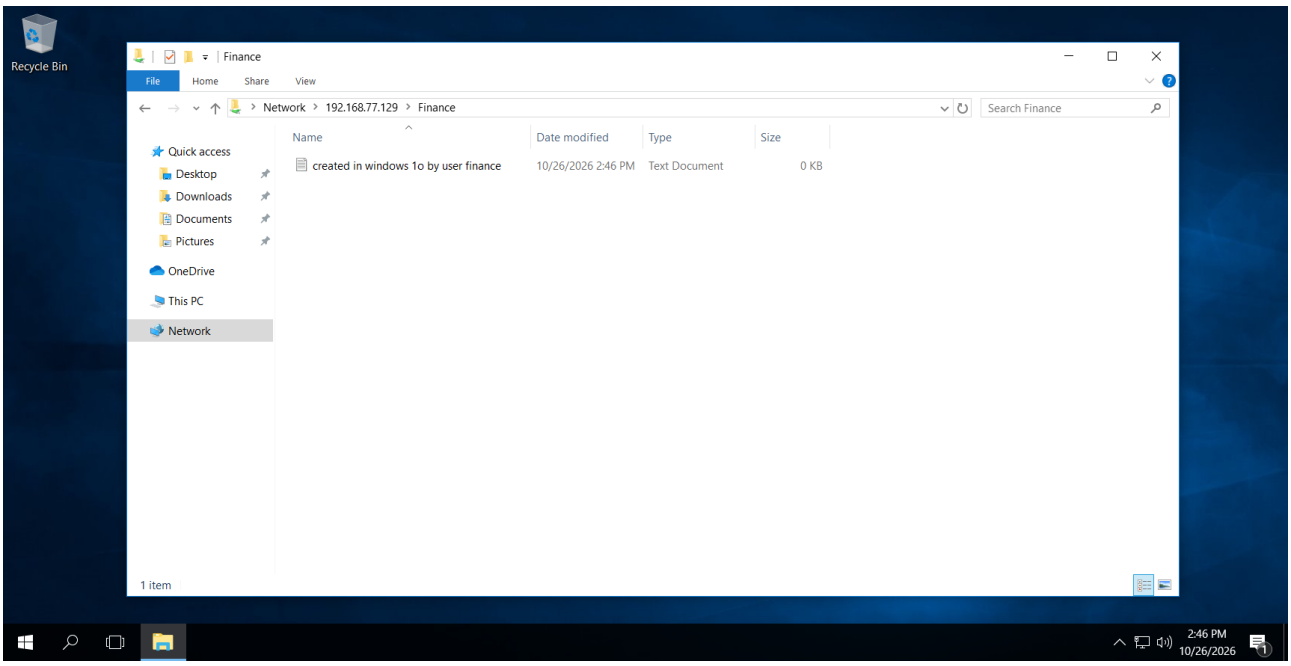
Open the server shares



Use Win + R and enter \\192.168.77.129, then open Finance; or open \\192.168.77.129\Finance directly. Confirm the active employee identity with whoami.

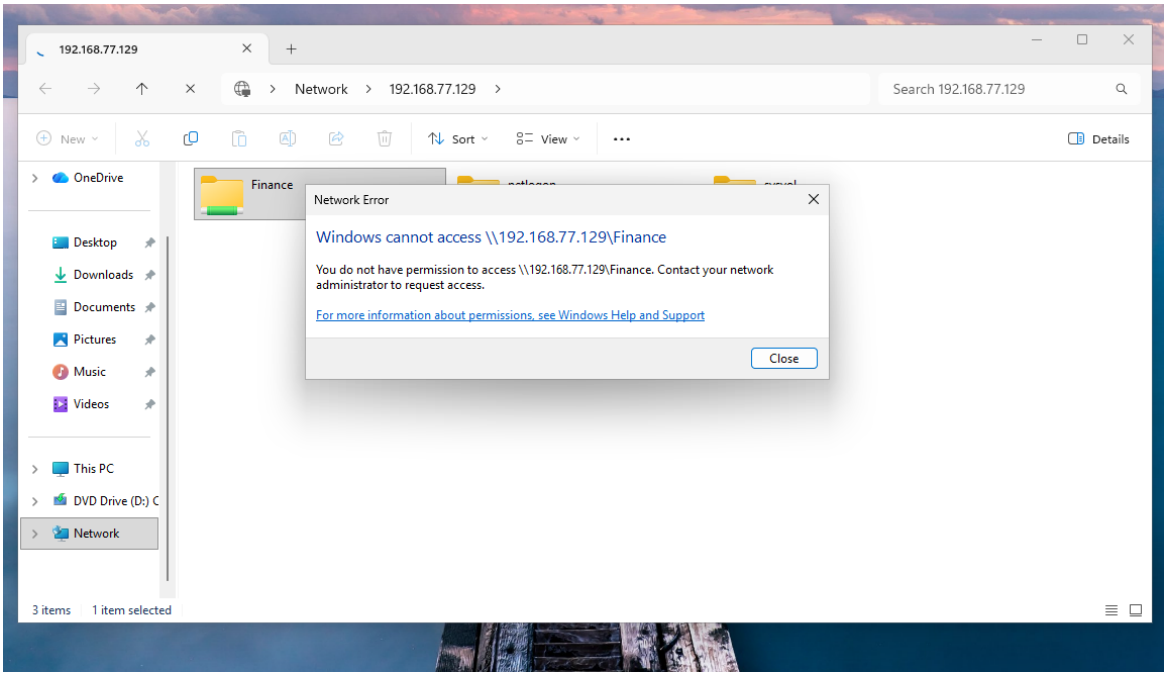
Expected results

Finance-user test: create a file



The Finance share contains the file created during the Finance-user test. Also edit, save and delete a designated test file to verify Modify access. Establish the employee identity with whoami; File Explorer alone does not show it.

HR-user test: access denied



The HR-user test receives a permission-denied error for the Finance share. Use a separate employee sign-in session to avoid cached SMB credentials. This confirms denied network access in this test, but does not prove that each permission layer independently excludes HR.

DAY 2 / TASK 10

Launch the company intranet

Publish a simple internal website that employees can open by name from either workstation. Make it recognizably yours.

> Your deliverable: A custom intranet at http://askfarouk.local:8080/, accessible from both clients with the firewall enabled.

Before you begin

• Domain DNS and client connectivity work. The data volume is ready.

Assignment

1. Install Web Server (IIS), including Static Content, Default Document and the IIS Management Console.

2. Create E:\Intranet on CompanyData. Download the index.html starter into it, then edit the team name and welcome message. Confirm the file is index.html, not index.html.txt.

3. In IIS create a site named companyportal, physical path E:\Intranet, type HTTP, IP All Unassigned, port 8080 and a blank Host name. Keep this binding unique among running sites. The port-80 Default Web Site can remain separate.

4. Give the web server the required read access to the content folder. Confirm index.html is an enabled Default Document, the site is started, and askfarouk.local resolves to 192.168.77.129.

5. Allow inbound TCP 8080 from 192.168.77.0/24 on the server. Keep Windows Firewall enabled. Test http://askfarouk.local:8080/ from each client, then edit the page and confirm the updated result.

Download index.html starter from the online course

Recorded fix / site opens on server but not on clients

Observed: the client could ping 192.168.77.129 but its TCP 8080 test failed. The server showed a listener on :: and successfully connected to its own IPv4 address on 8080. That local IPv4 test confirmed the listener accepted IPv4. Creating an inbound Allow rule for TCP 8080, restricted to the lab subnet and covering all firewall profiles, restored client access. A profile switched off earlier may not be the active Domain profile. Keep the firewall enabled with this specific rule; Enforced GPO settings are not part of this fix.

```
Get-NetTCPConnection -State Listen -LocalPort 8080

Test-NetConnection 192.168.77.129 -Port 8080

New-NetFirewallRule -DisplayName "Lab IIS TCP 8080" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 8080 -RemoteAddress 192.168.77.0/24 -Profile Any
```

Run the listener check and rule creation in elevated PowerShell on Server 2019. Run the TCP test first on the server and then on each client. After applying the rule, confirm TcpTestSucceeded is True from the client and browse http://askfarouk.local:8080/. Profile Any covers Domain, Private and Public; RemoteAddress limits the rule to this lab subnet. Create the named rule once; if it already exists, inspect it instead of adding duplicates.

Verification checklist

□ IIS role, Static Content, Default Document and management tools are installed.

□ companyportal points to the intended Intranet folder and is started.

□ HTTP binding uses All Unassigned (or the server address), port 8080 and a blank host name.

□ index.html is present, loads as the default document and displays a custom company or team name.

□ The web server has the required NTFS read access to the content folder.

□ askfarouk.local resolves to 192.168.77.129 from the clients.

□ PC10 and PC11 load http://askfarouk.local:8080/ successfully.

□ An edited page is visible after refresh; Windows Firewall is enabled and the lab TCP 8080 rule allows client access.

Evidence: Show the IIS binding, DNS lookup and your custom intranet open on both clients.

Verification commands

```
nslookup askfarouk.local

Test-NetConnection 192.168.77.129 -Port 8080

Get-NetTCPConnection -State Listen -LocalPort 8080
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

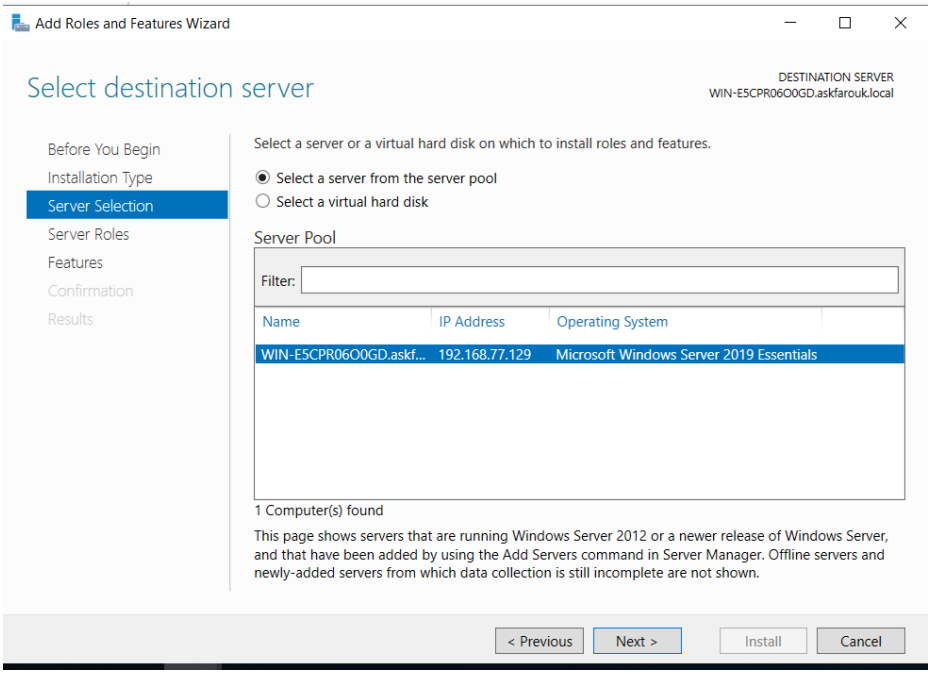
TASK 10 / SCREENSHOT WALKTHROUGH

Visual reference

These screenshots match the demonstrated Server 2019 IIS setup: site companyportal, physical path E:\Intranet, HTTP port 8080, IP All Unassigned and a blank host name. The client uses http://askfarouk.local:8080/. The data folder is E:\Intranet. If using another subnet, update the address and firewall scope consistently. The starter is now supplied directly as index.html.

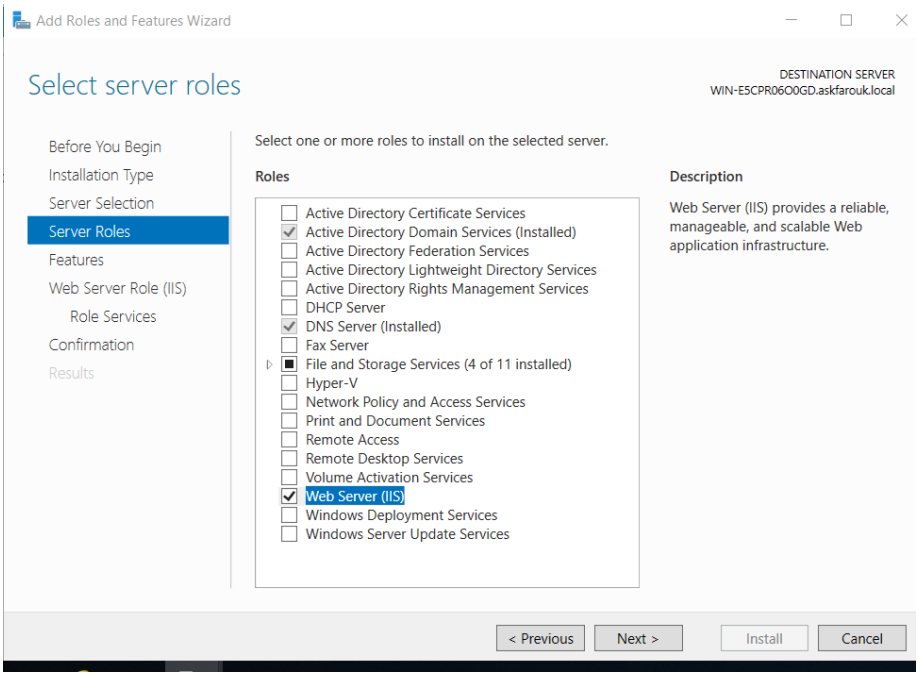
1 / Install and open IIS

Select the destination server



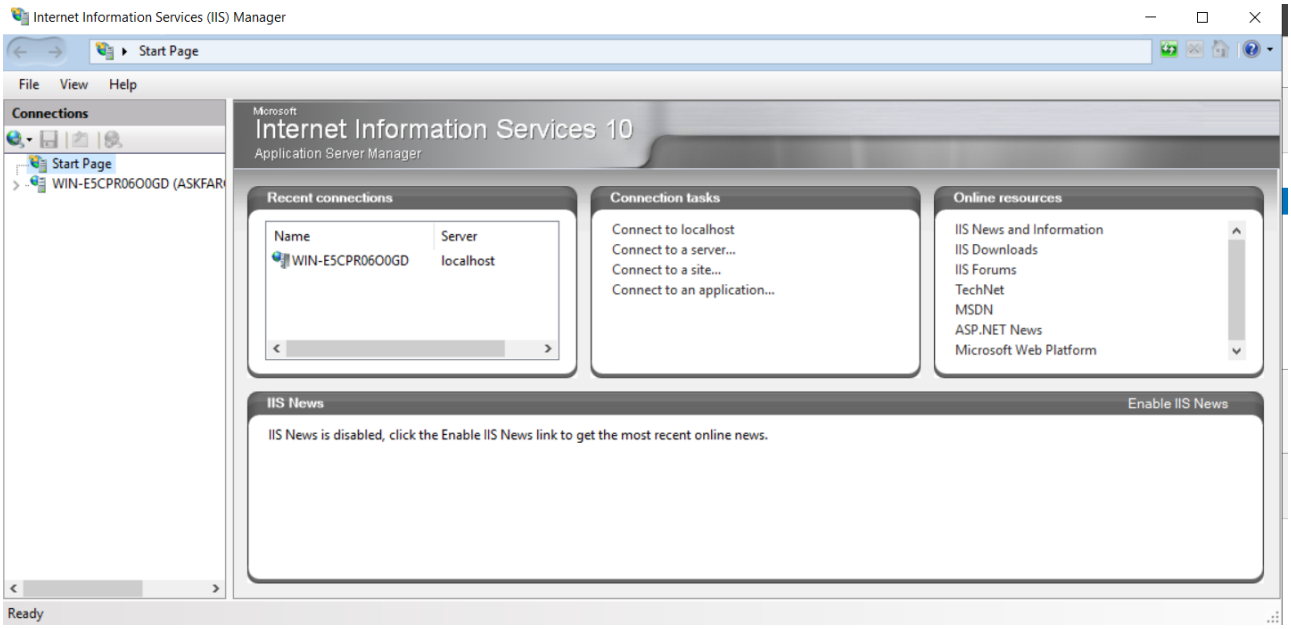
In Add Roles and Features, select the intended Server 2019 machine at 192.168.77.129. Its actual hostname may differ from the course label DC01.

Install Web Server (IIS)



Select Web Server (IIS) and include its management tools. Ensure Static Content and Default Document are installed, then complete installation.

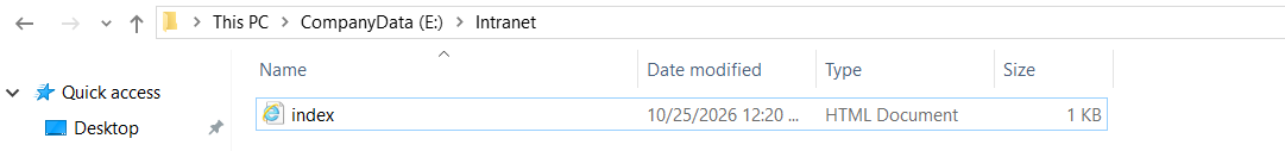
Open Internet Information Services Manager



Open IIS Manager from Server Manager → Tools and expand the server in the Connections pane.

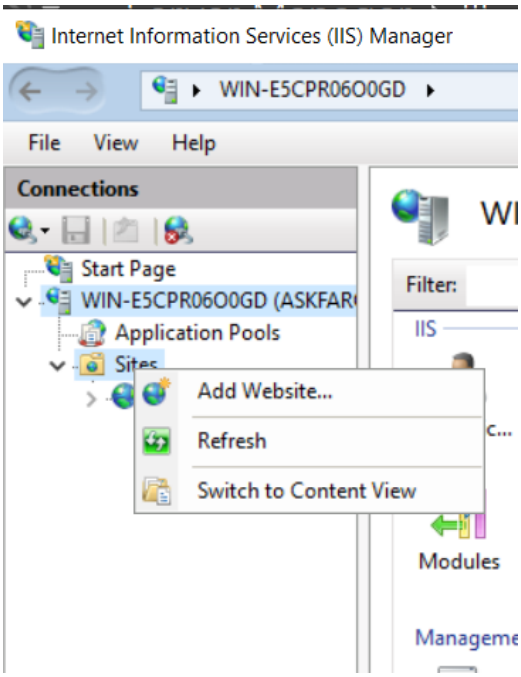
2 / Prepare content and configure the site

Place index.html in the Intranet folder



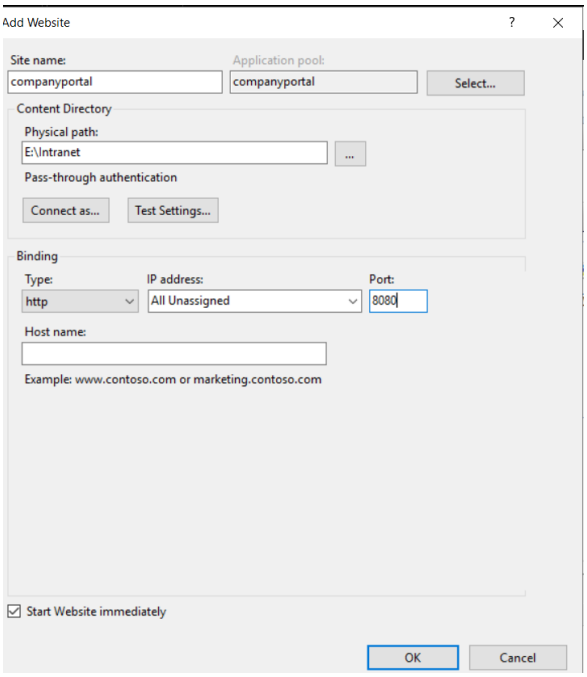
The screenshot shows index in E:\Intranet with file type HTML Document. The download is named index.html. Confirm the full extension and keep it in the folder configured as the IIS physical path.

Right-click Sites and add a website



In IIS Manager right-click Sites → Add Website.

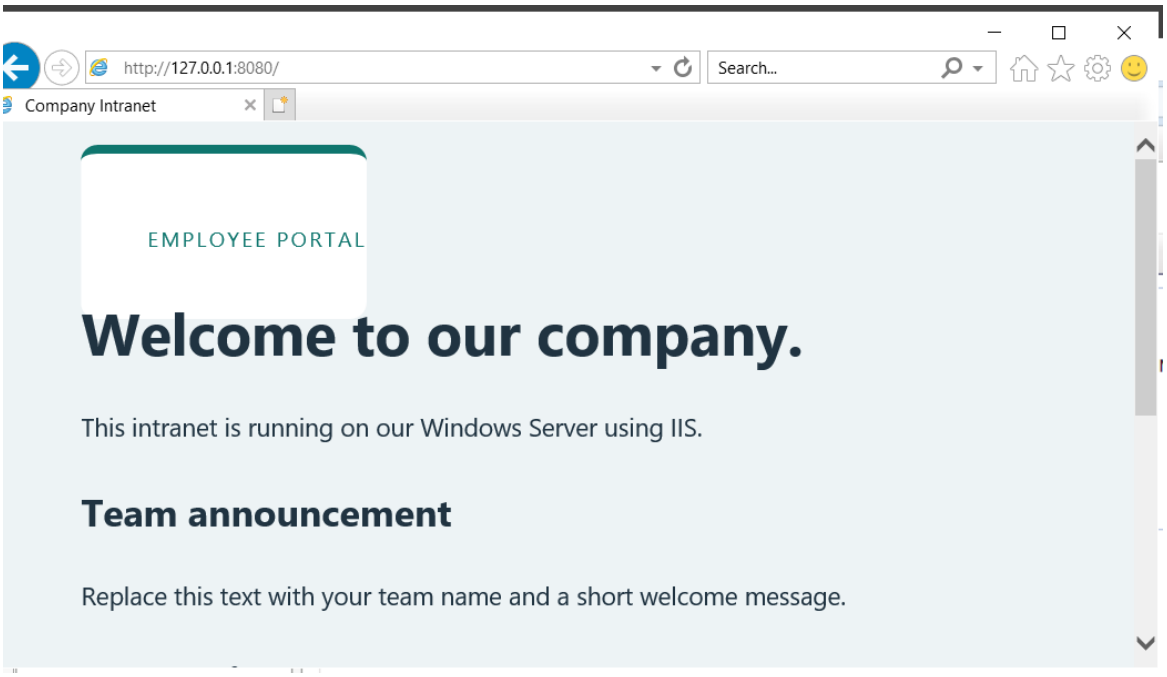
Use the demonstrated HTTP 8080 binding



Set site name companyportal, physical path E:\Intranet, HTTP, All Unassigned and port 8080. Leave Host name blank and start the site. A blank host name allows requests to this binding using the server IP or an appropriate DNS name.

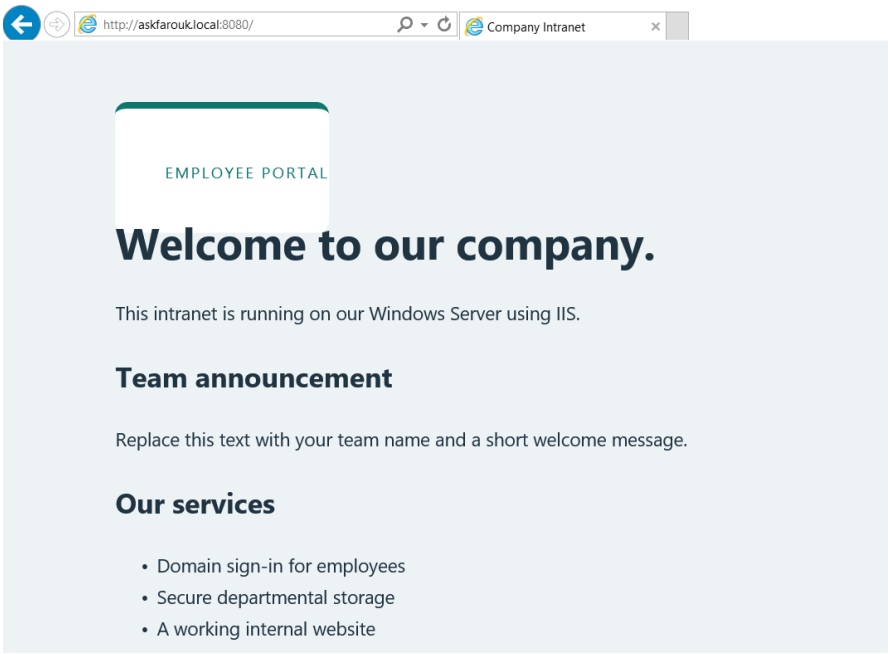
Expected results

Server-local website test



The server opens http://127.0.0.1:8080/ and loads the starter page. This proves local serving, but a client test is also needed. If remote TCP 8080 fails, use the recorded firewall diagnostic sequence.

Client website test succeeds



The client loads http://askfarouk.local:8080/ successfully. Repeat on the second client with Windows Firewall enabled and the lab TCP 8080 rule in place. Customize the team text before completing the task; the captured page still contains the supplied starter wording.

DAY 2 / TASK 11

Back up and recover a Finance file

Protect a Finance document with Windows Server Backup, recover its backed-up version and prove the content and employee access are correct. The demonstrated method creates a restored copy while preserving the original.

> Your deliverable: A successful Finance-folder backup on F: and a recovered file with matching content, accessible to the Finance employee.

Before you begin

• Finance share works. A separate backup disk is available or can be added.

Assignment

1. Prepare a separate 30 GB backup disk, formatted as NTFS and assigned F: with label Backup. Keep CompanyData (E:) separate. Confirm Windows Server Backup is installed; install it through Server Manager → Add Roles and Features → Features if needed.

2. Create E:\Company\Finance\Recovery-Test.txt. Enter a recognizable sentence, save and close it, then reopen it to confirm the content was saved.

3. Open Windows Server Backup → Local Backup → Backup Once → Different options → Custom → Add Items. Select E:\Company\Finance, choose Local drives and destination Backup (F:), review the summary and run the backup. Confirm Successful before attempting recovery.

4. Choose Recover → This server → the successful backup date/time → Files and folders. Browse to CompanyData (E:) → Company → Finance and select Recovery-Test.txt. Verify the file is available in the backup.

5. For the demonstrated non-destructive method, keep the original file, select Original location and Create copies so that you have both versions. Keep Restore ACL permissions selected. Review the summary, recover and open the new dated copy. Compare its content with the original saved sentence.

6. Alternatively, to simulate accidental deletion, delete only the designated Recovery-Test.txt after verifying it exists in the backup, then recover it to its original location. Do not delete the Finance folder or unrelated data. Use either recovery method and record which one you tested.

7. Sign into a client as finance.user and open the recovered file through the Finance share. Verify its text and permissions. Explain why F: on the same physical host is sufficient for this exercise but does not protect against host failure.

Verification checklist

□ Backup (F:) is a separate volume from CompanyData (E:) and has sufficient free space.

□ Windows Server Backup is installed and its Local Backup console opens.

□ Recovery-Test.txt contains identifiable saved text before backup.

□ A completed successful backup includes E:\Company\Finance and the test file.

□ The chosen recovery method is recorded: preserved-original copy recovery or deletion of only the designated test file.

□ The recovered file opens and contains the same text as the backed-up version.

□ finance.user can open the recovered file through the Finance share.

□ Trainee explains why a backup disk on the same host does not protect against host failure.

Evidence: Show the successful backup result, restored file content and client access.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

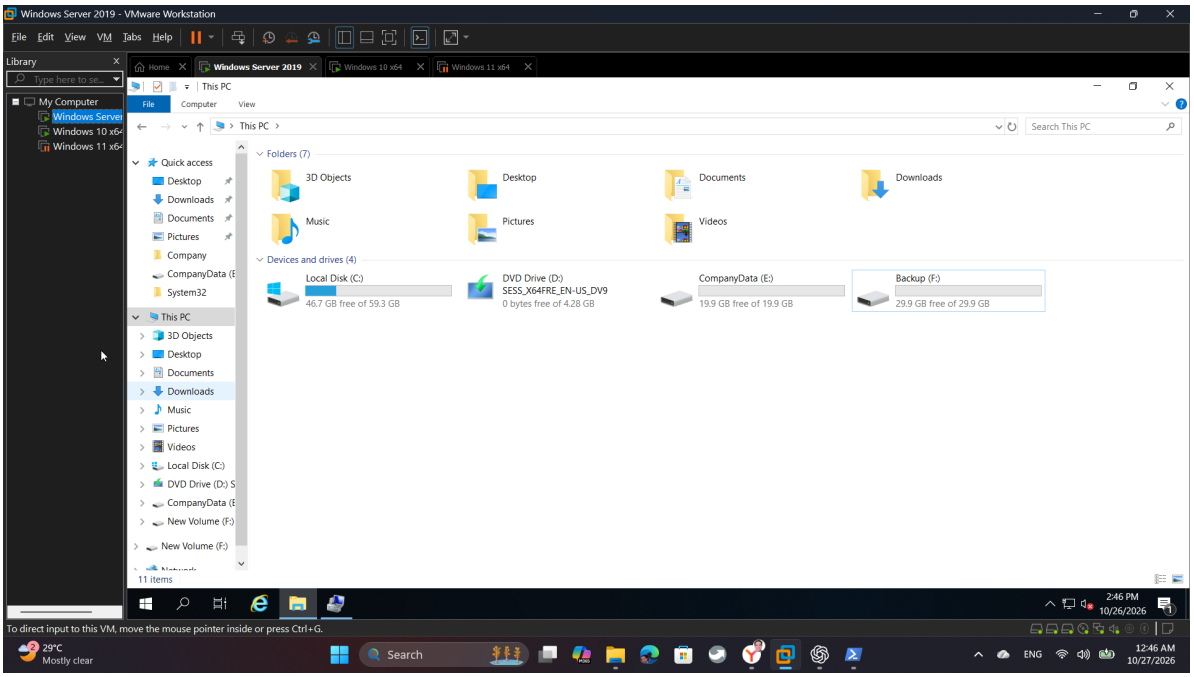
TASK 11 / SCREENSHOT WALKTHROUGH

Visual reference

The demonstrated setup uses CompanyData (E:) for source data and a separate roughly 30 GB Backup (F:) volume for the backup. The recovery creates a copy because the original file remains. This demonstrates recovering a backed-up file, not deletion recovery. The course also offers deletion of only the designated test file as an alternative exercise after verifying the backup.

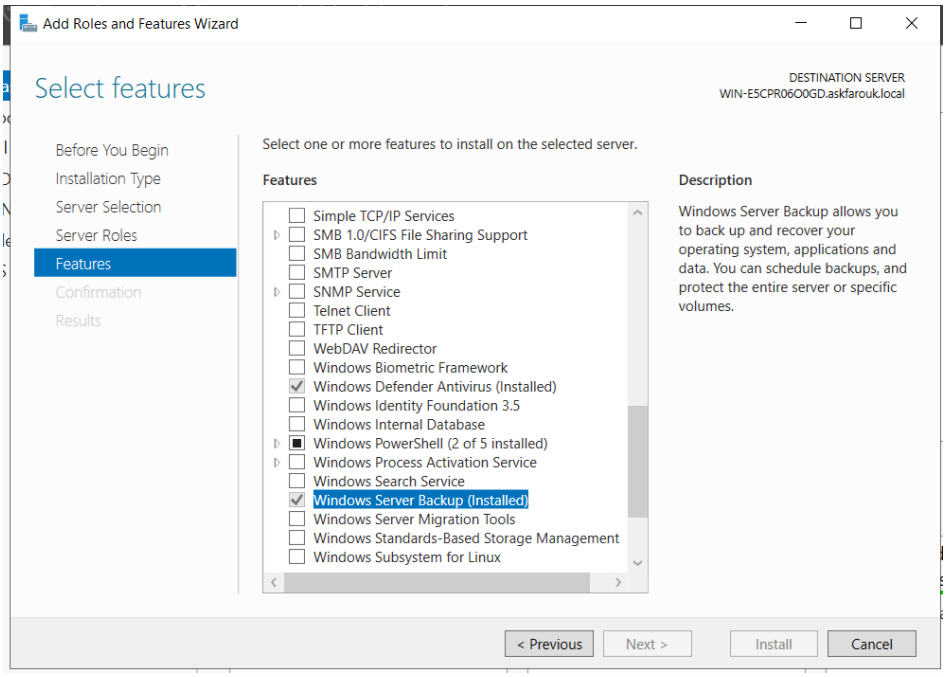
1 / Prepare the destination and source file

Separate backup volume is available



File Explorer shows CompanyData (E:) and Backup (F:) with approximately 30 GB available on the backup volume. The label Backup is acceptable.

Windows Server Backup is installed



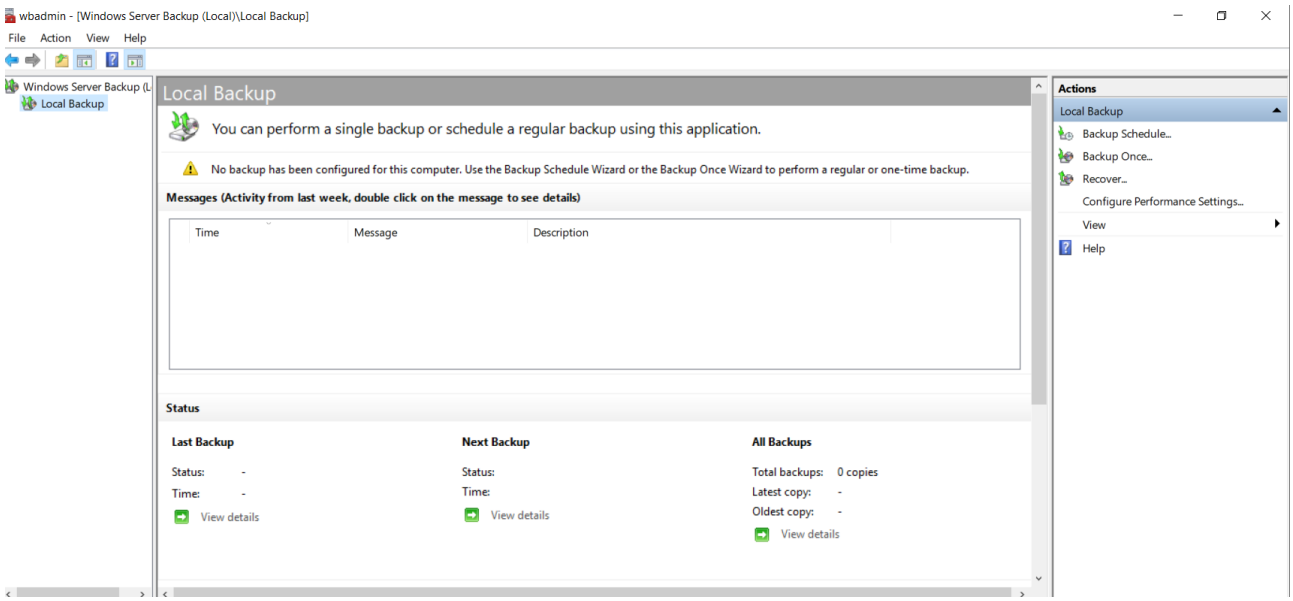
The Features wizard marks Windows Server Backup as Installed. If already present, close the wizard and open the backup console; no reinstall is required.

Save distinctive test content



Recovery-Test contains the text Finance recovery test - this file must be restored. Save it in E:\Company\Finance\Recovery-Test.txt before backup. The wording lets you verify the recovered version later.

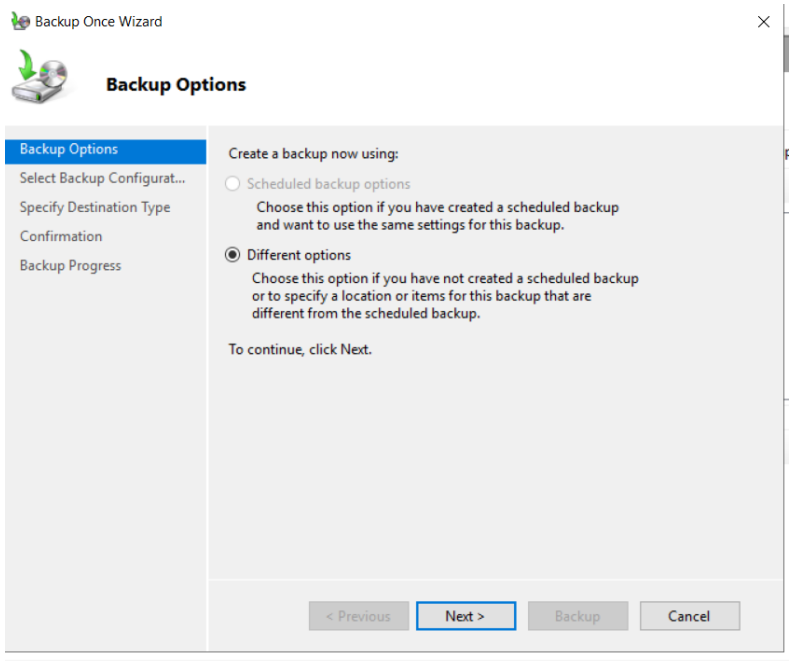
Open Local Backup



Open Server Manager → Tools → Windows Server Backup → Local Backup. Choose Backup Once to create the classroom folder backup.

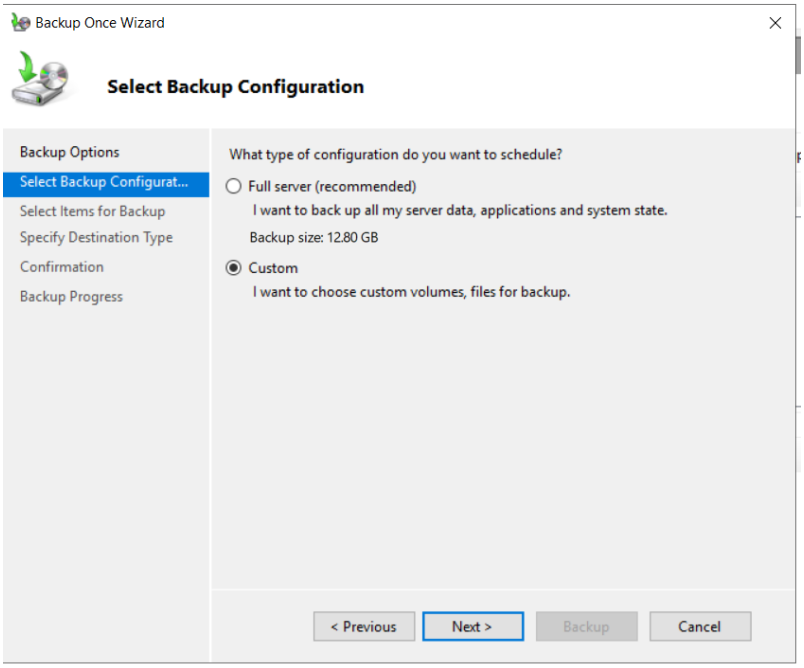
2 / Create a custom folder backup

Choose Different options



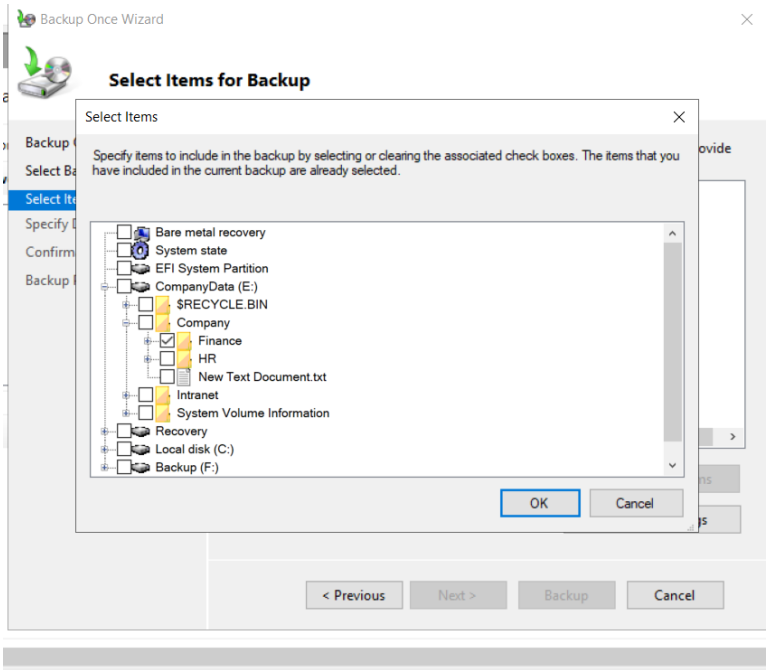
In Backup Once, select Different options to configure this one-time job.

Select Custom



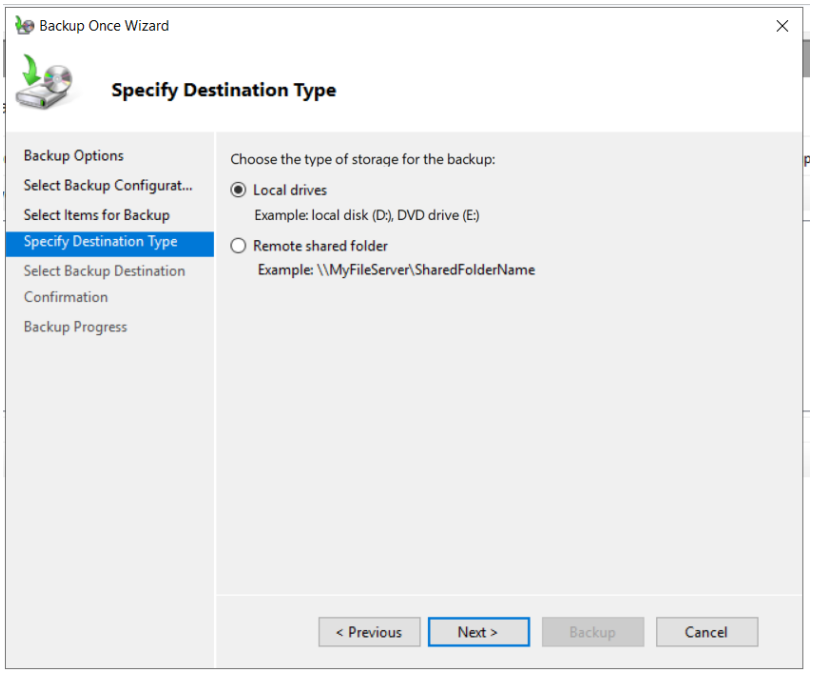
Choose Custom so you can select Finance rather than backing up the whole server.

Select the Finance folder



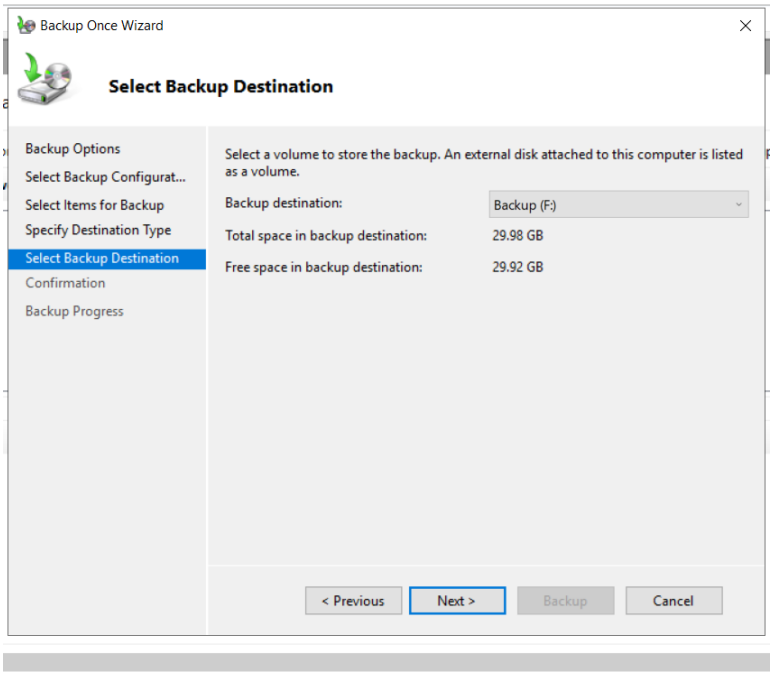
Expand CompanyData (E:) → Company and select Finance. Confirm Recovery-Test.txt was saved inside this folder.

Choose a local-drive destination



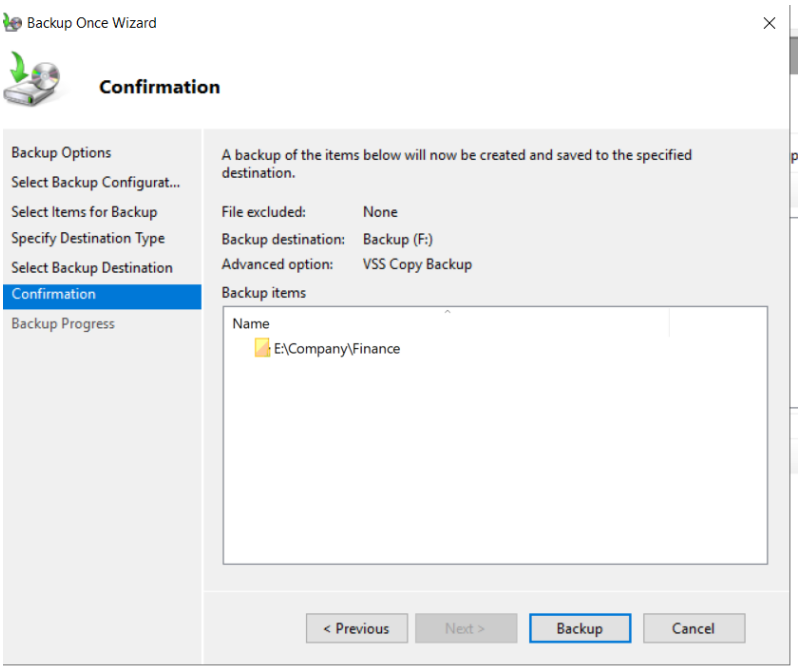
Select Local drives. The backup destination must be separate from the selected source volume.

Select Backup (F:)



Choose Backup (F:) and confirm it has sufficient space. The source is on E:, not F:.

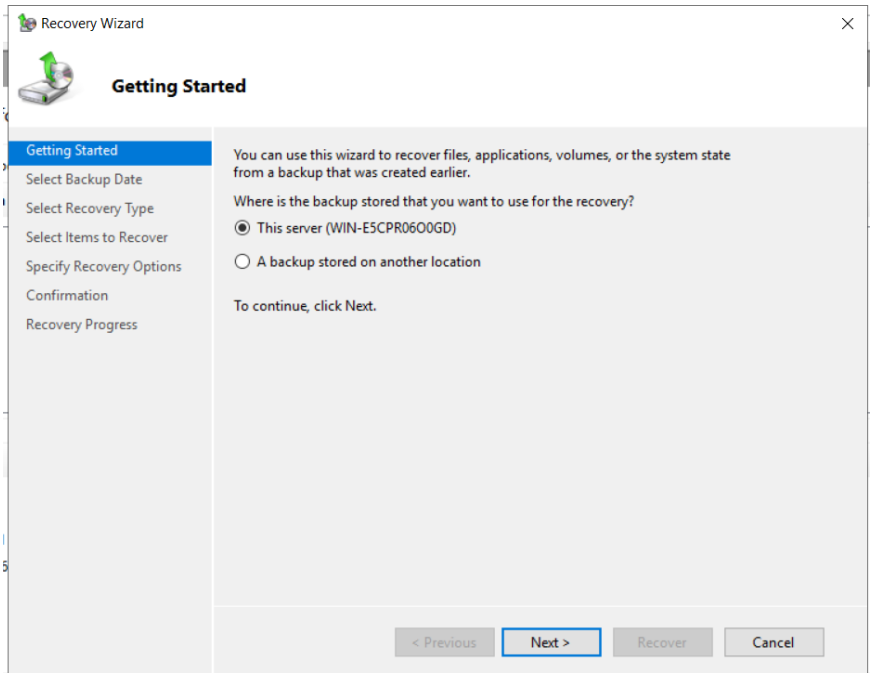
Review before starting



The confirmation shows E:\Company\Finance as the backup item, Backup (F:) as the destination and VSS Copy Backup. Start the job and wait for the outcome.

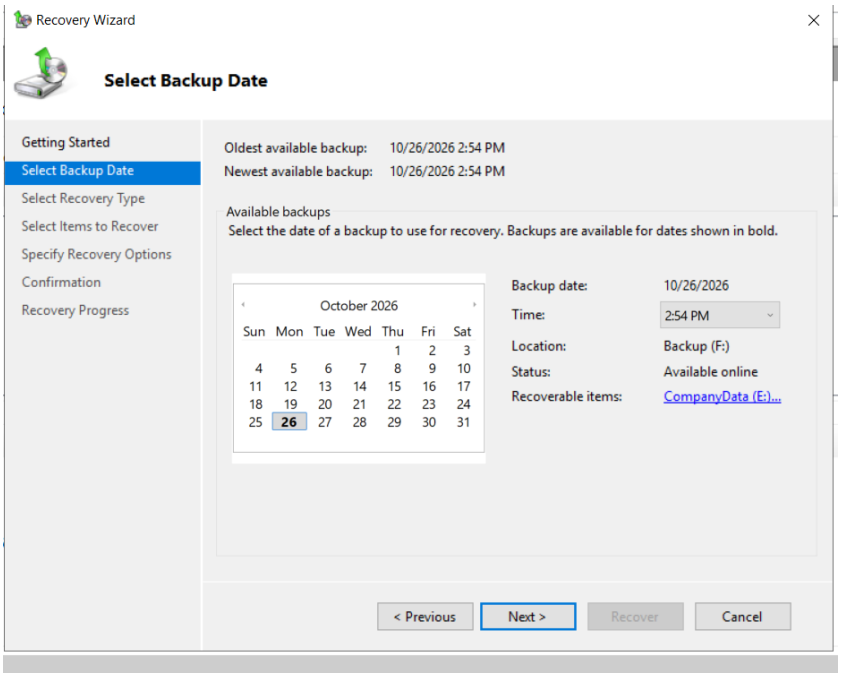
3 / Select and recover the backed-up file

Start recovery from this server



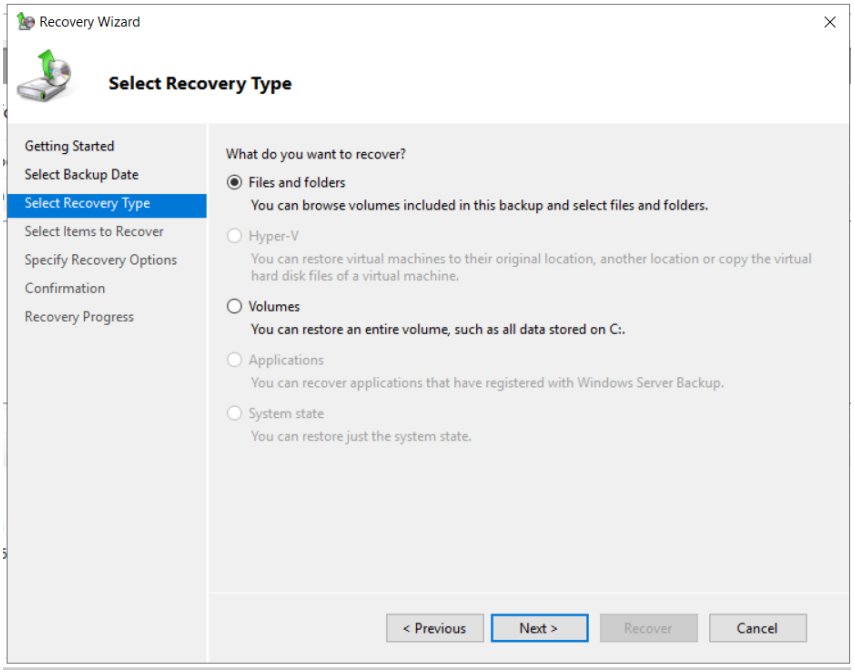
Choose Recover, then This server because the job was created on this server and its backup is available locally.

Select the successful backup version



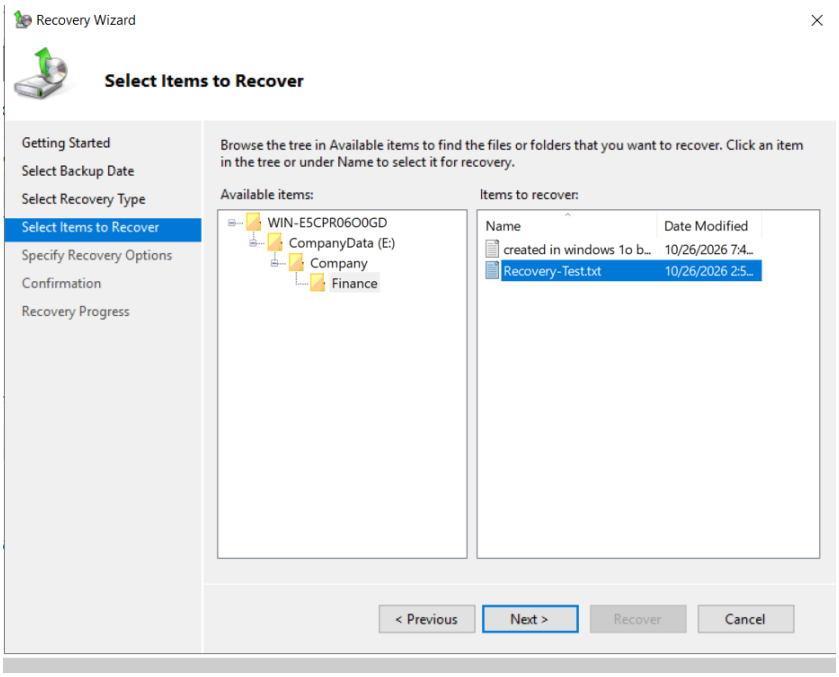
Select the date and time of the successful backup. The displayed recoverable item is CompanyData (E:), with the backup stored on F:.

Choose Files and folders



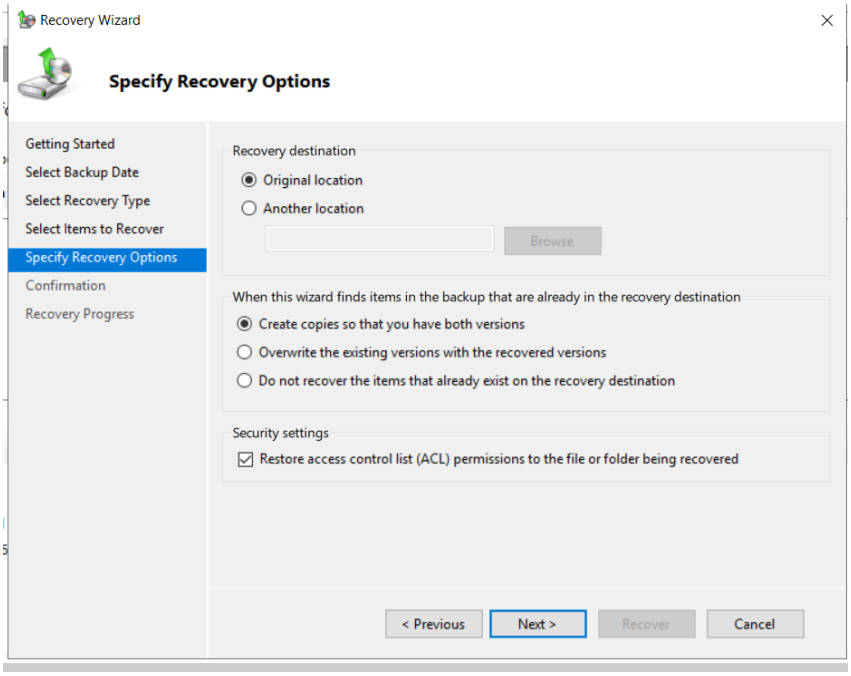
Select Files and folders to recover the individual test document.

Confirm the test file is in the backup



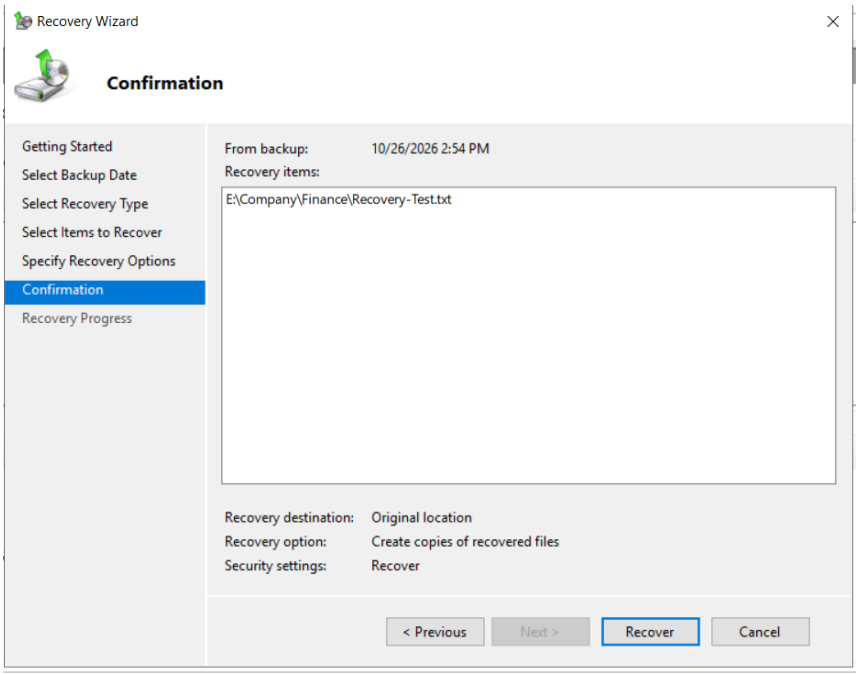
Expand CompanyData (E:) → Company → Finance and select Recovery-Test.txt. This confirms the backup contains the file before any optional deletion exercise.

Keep both versions and restore ACLs



Choose Original location and Create copies so that you have both versions. Keep Restore access control list (ACL) permissions selected. This demonstrated method preserves the existing original.

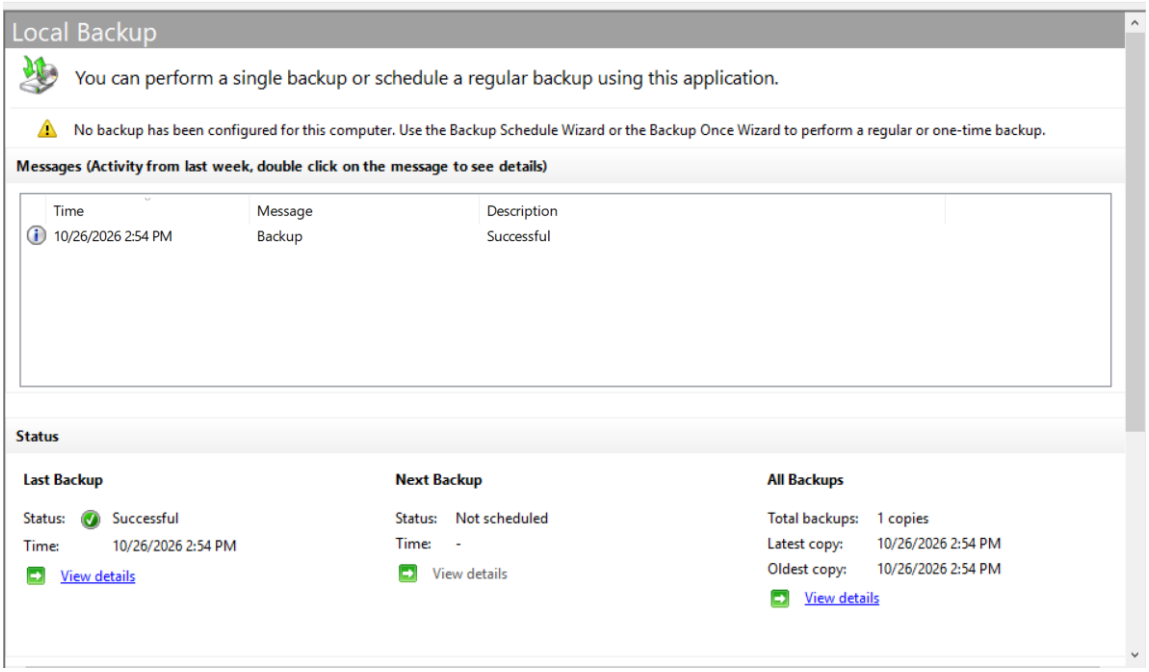
Review the recovery plan



The summary shows E:\Company\Finance\Recovery-Test.txt, Original location and Create copies of recovered files. Click Recover and wait for completion; this summary alone is not a success result.

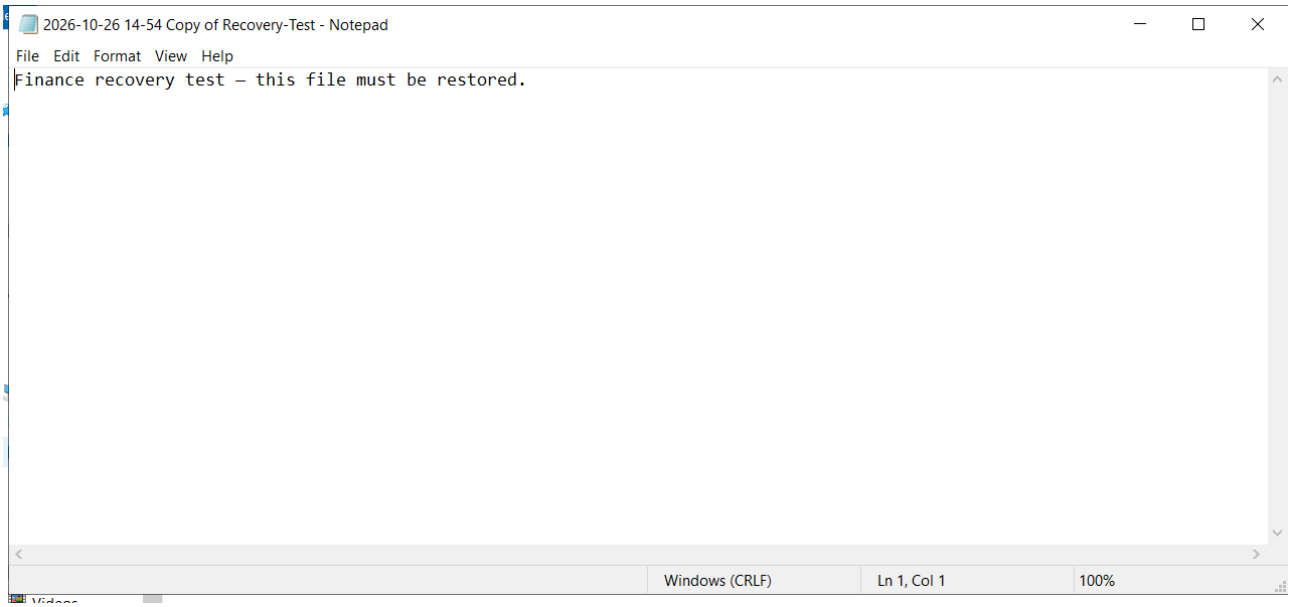
Expected results

The backup job succeeded



Last Backup shows Successful and All Backups shows one copy. The warning about no configured backup schedule refers to scheduling; the on-demand backup has succeeded.

The recovered copy contains the expected text



Notepad opens a dated Copy of Recovery-Test with the same Finance recovery-test sentence. This supports successful copy recovery. Finish by checking the recovery job outcome and opening this recovered file from a client signed in as finance.user.

DAY 2 / TASK 12

Resolve the service incident

The trainer will introduce one fault. Reproduce the user complaint, collect evidence, fix the cause and demonstrate recovery.

> Your deliverable: A restored service and a short incident record that another administrator can understand.

Before you begin

• The relevant service worked before the trainer introduced the fault.

Assignment

1. Write down the symptom and reproduce it as the affected employee.

2. Check the most relevant dependencies and record the evidence before making a change.

3. Identify the cause, make a targeted correction and repeat the original failed action.

4. Verify a related function still works. Record symptom, cause, fix and verification in your notes.

Verification checklist

□ The original complaint is reproduced.

□ Relevant evidence is collected before settings are changed.

□ The actual cause is identified.

□ A targeted correction restores the intended configuration.

□ The original failed action succeeds after the fix.

□ A related service or function still works.

□ Notes contain the symptom, cause, correction and verification.

Evidence: Demonstrate the recovered service live and complete the incident notes below.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

DAY 2 / FINAL DEMONSTRATION

Hand over a working environment.

□ Sign in as a domain employee.

□ Show the effective password policy.

□ Demonstrate Finance access and denied HR access.

□ Open the intranet by name.

□ Show the recovered file and successful backup.

□ Explain a fault: symptom, evidence, cause, correction and verification.

Outstanding issues / handover

SECTION 03 /

03

Continue your practice.

Extend the lab. Build independence, one verified change at a time.

BEYOND THE CORE LABS

Make the next change with a clear purpose.

Choose an extension, define what success should look like and record the change. Verify that the services built earlier still work afterward.

- Automate client addressing with DHCP.
- Redirect Documents so employee files are available from either workstation.
- Observe a prepared unattended deployment and distinguish network boot from complete automation.

> Document the starting configuration → make one change → test the intended result → check a related service → record what you learned.

Automate client addressing

Replace the static client addresses with leases from an authorized DHCP server.

> Your deliverable: Both clients receive correct addresses and DNS settings automatically.

Before you begin

- Core labs are complete. All machines use the same lab network. Disable VMware DHCP on that network before activating Windows DHCP to avoid competing address offers.

Assignment

1. Install DHCP on DC01 and complete authorization in Active Directory.

2. Create and activate a scope from 192.168.77.160 to 192.168.77.190 with mask 255.255.255.0. This avoids the server and planned static client addresses .129-.131; check for other occupied addresses before activation.

3. Set scope DNS server to 192.168.77.129 and DNS suffix to askfarouk.local. Set router option 003 to 192.168.77.2 for the demonstrated NAT network; omit it on a host-only network without a router.

4. Change both clients to automatic IP and DNS settings. Renew their leases and retest the domain, share and intranet.

Verification checklist

□ DHCP is installed and authorized.

□ Scope range and mask are correct and scope is active.

□ DNS options point to DC01 and the domain suffix.

□ Both clients receive addresses in the scope.

□ ipconfig /all identifies DC01 as DHCP and DNS server.

□ Both leases appear in DHCP Manager.

□ Domain services, Finance access and intranet still work.

Evidence: Show client configuration, server leases and a successful service test.

Verification commands

```
ipconfig /release

ipconfig /renew

ipconfig /all
```

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

CONTINUE YOUR PRACTICE / TASK E2

Make Documents follow the user

Store employee Documents folders centrally so a user can access the same documents from either workstation.

> Your deliverable: Documents redirected through a user GPO, with cross-client access and per-user privacy verified.

Before you begin

• Domain users, both clients and the data volume work. Review the linked Microsoft permission recipe before configuring the share.

Assignment

1. Create E:\Redirect and share it as Redirect$. Configure the documented folder-redirection permissions for the participating users, SYSTEM, Administrators and CREATOR OWNER.

2. Create Lab Documents Redirection and link it to Lab Users. Under User Configuration → Policies → Windows Settings → Folder Redirection → Documents, choose Basic and Create a folder for each user under the root path.

3. Set the root path to \\DC01\Redirect$. Do not append %username% when using that target option.

4. Refresh policy and sign out/in. Save a document on PC10, then sign into PC11 as the same user and verify it. Test another user's access is denied.

Verification checklist

□ The redirection share exists before the GPO is applied.

□ Share and NTFS permissions follow the documented per-user design.

□ The user GPO is linked to Lab Users.

□ The root path and per-user target option are correct.

□ Documents resolves to the expected per-user server location.

□ A document saved on PC10 is available on PC11 for the same user.

□ A different ordinary user cannot open the first user's private folder.

Evidence: Show Documents location, the same file on both clients and the privacy test.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

Observe an unattended deployment

Observe a pre-tested deployment workflow and identify which steps are automated. Building the deployment platform is outside this course's core course.

> Your deliverable: An observed deployment and an accurate explanation of PXE, unattended setup and zero-touch outcomes.

Before you begin

- Trainer has a tested deployment solution, image and answer configuration compatible with the target Windows version.
- Use a new disposable VM on the isolated deployment network.

Assignment

1. Observe the blank target VM start the prepared workflow.

2. Identify how the image, installation answers and final configuration are selected.

3. Review the resulting machine and deployment status or logs. Installation may continue in the background.

4. Explain why PXE boot alone does not demonstrate complete zero-touch deployment.

Verification checklist

□ The target VM starts the prepared workflow.

□ The intended OS image and configuration are selected.

□ Expected setup stages proceed without manual answers.

□ The final state or current deployment status is verified honestly.

□ Trainee distinguishes PXE boot, unattended setup and zero-touch deployment.

Evidence: Record the automation observed and whether the final intended state was reached.

Assessment

□ Independent □ Prompted □ Assisted □ Incomplete

Notes / evidence

KEEP LEARNING

References and online companion.

askfarouk.net/server-plus

Official references

CompTIA Server+ SK0-005 objectives

Scope reference: web roles, storage, unattended installation, security and troubleshooting.

Install Active Directory Domain Services

Microsoft guidance for installing AD DS and creating a forest.

Join a computer to a domain

Microsoft domain-join guidance and requirements.

Domain password policy

Domain-level password policy settings and scope.

Deploy Folder Redirection

Use the documented share and NTFS permission recipe for the optional lab.

WDS boot-image support

Check support limitations before preparing a Windows deployment demonstration.

Windows 10 support information

Windows 10 is retained here as an isolated legacy-client exercise. Use a supported or appropriately covered system outside this lab.