

Active Directory Creation and Administration

Tutorial Number: 02

01 - Domain and Forest Creation

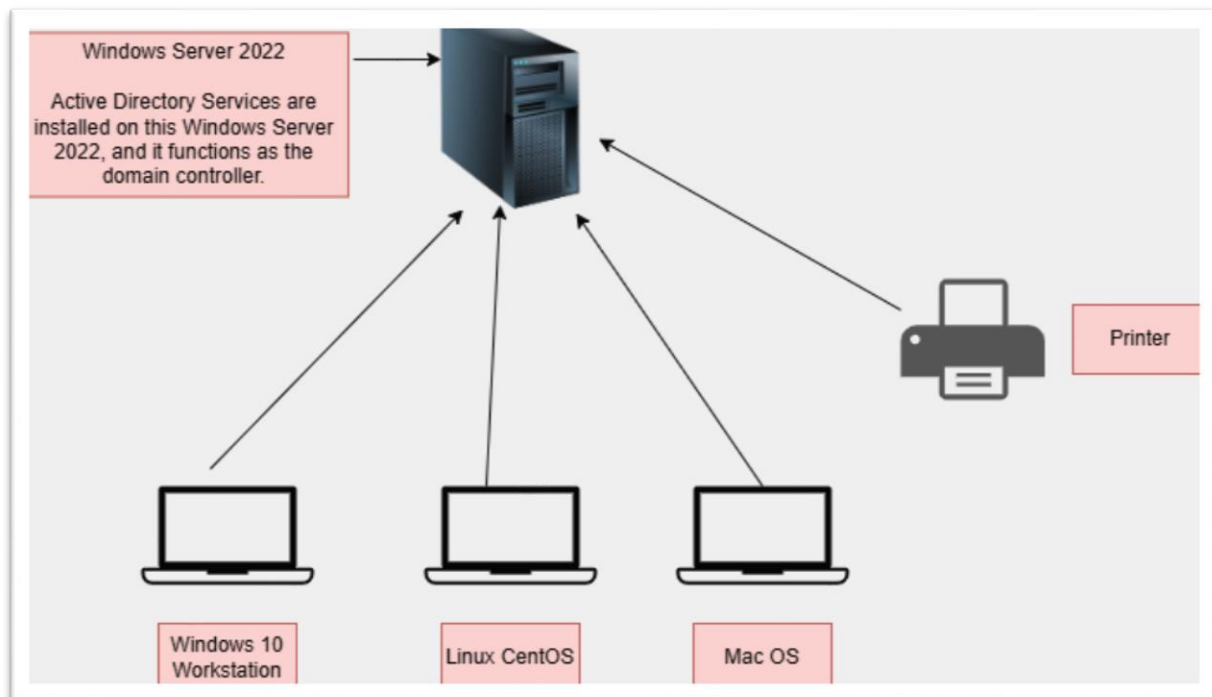
What is Active Directory (AD)?

Active Directory (AD) is a service that helps you manage users, computers, and resources in a centralized way in a network domain.

What is AD DS (Active Directory Domain Services)?

- AD DS is the Windows Server role that enables you to run Active Directory.
- Installing AD DS is just the first step — it does not yet configure AD.

It only installs the tools (like dcpromo.exe) needed to promote the server to become a Domain Controller.



LAB: Install and Configure AD on Windows Server 2022

➤ **Goal: Create a new forest and promote this server to the first domain controller.**

✓ **Step 1: Install AD DS Role**

- Open Server Manager
- Click Add Roles and Features
- Select:
 - Role-based or feature-based installation
 - Select your local server
- Under Server Roles → Check Active Directory Domain Services
- Click Next until Install

This installs the AD tools, not AD itself yet.

The process is shown in five sequential screenshots, connected by green arrows indicating the flow of the installation steps.

Screenshot 1: Windows Server Start Menu
The Start menu is open, showing various applications. The **Server Manager** icon is highlighted with a red box and a red arrow.

Screenshot 2: Server Manager Dashboard
The Server Manager application is open, showing the **Dashboard** tab. The **WELCOME TO SERVER MANAGER** section displays a **QUICK START** guide with three steps: 1. Configure this local server, 2. Add roles and features (highlighted with a red box and a red arrow), and 3. Add other servers to manage.

Screenshot 3: Add Roles and Features Wizard - Select installation type
The **Add Roles and Features Wizard** is open, showing the **Select installation type** screen. The **Before You Begin** section is active, and the **Installation Type** is set to **Role-based or feature-based installation** (highlighted with a red box and a red arrow).

Screenshot 4: Add Roles and Features Wizard - Select destination server
The **Add Roles and Features Wizard** is open, showing the **Select destination server** screen. The **Before You Begin** section is active, and the **Server Selection** step is highlighted with a red box and a red arrow. The **Server Pool** table lists the available servers:

Name	IP Address	Operating System
win-mmick-in	80.1.1.39	Microsoft Windows Server 2022 Datacenter

The **win-mmick-in** server is highlighted with a red box.

Screenshot 5: Add Roles and Features Wizard - Select server roles
The **Add Roles and Features Wizard** is open, showing the **Select server roles** screen. The **Before You Begin** section is active, and the **Server Roles** step is highlighted with a red box and a red arrow. The **Roles** list includes:

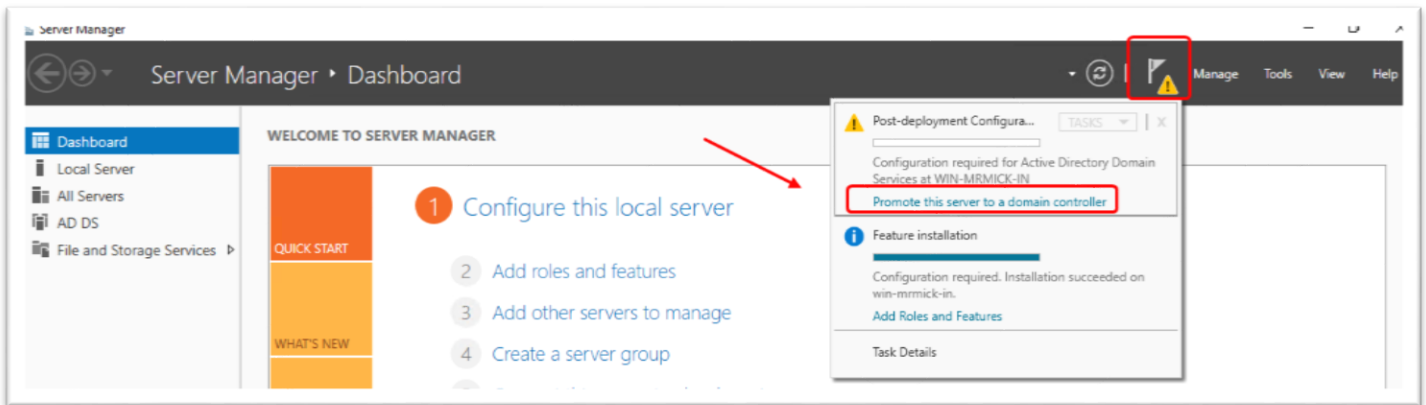
- ☐ Active Directory Certificate Services
- ☒ **Active Directory Domain Services** (highlighted with a red box and a red arrow)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server

Screenshot 6: Add Roles and Features Wizard - Installation progress
The **Add Roles and Features Wizard** is open, showing the **Installation progress** screen. The **Before You Begin** section is active, and the **Results** step is highlighted with a red box and a red arrow. The **View installation progress** section shows the **Feature installation** progress bar and the list of installed features:

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
- Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - AD DS Tools
 - Active Directory Administrative Center
 - AD DS Snap-Ins and Command-Line Tools

✓ Step 2: Promote the Server to Domain Controller

After AD DS is installed, you'll see a yellow exclamation ! in Server Manager. Click "Promote this server to a domain controller"



Concept:

1. Deployment Type: Create a New Forest

- Since this is your first domain controller, you must create a new forest.
- A forest is the topmost structure in AD — it contains one or more domains that trust each other and share a schema.

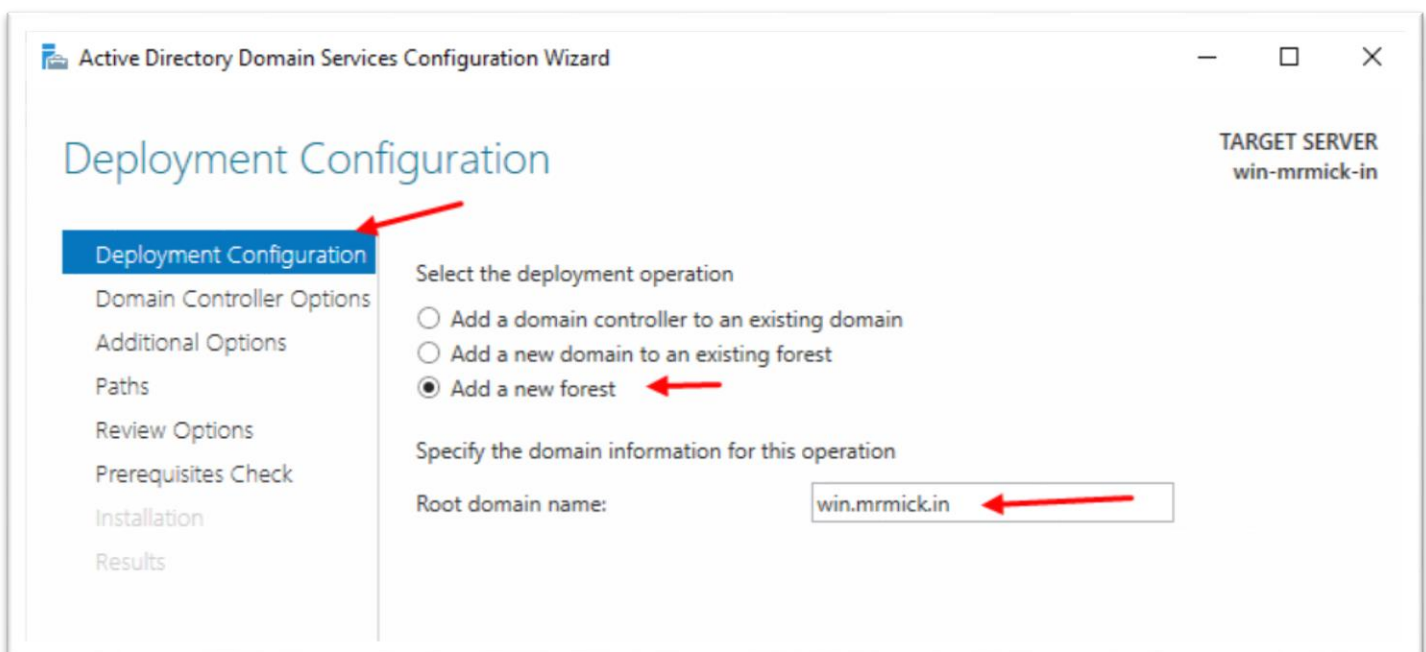
2. Root Domain Name

- You are asked to enter a fully qualified domain name (FQDN) like: corp.example.com
- It's recommended to use a domain you own publicly, like example.com.

Why choose a publicly owned domain?

- ✓ Prevents conflicts if your network connects to the internet or external services
- ✓ Avoids name resolution issues with non-routable domains like .local
- ✓ You can get SSL certificates, DNS records, email routing easier

Avoid made-up domains like `company.local`, especially with cloud integration.



3. Forest and Domain Functional Level

You must choose the lowest version of Windows Server you want to support.

- Forest Functional Level: Applies to the entire forest
- Domain Functional Level: Applies to the domain

4. Domain Controller Capabilities

- **DNS Server**
 - Yes – needed unless you already have a DNS setup
- **Global Catalog**
 - Yes – this DC will host full copy of AD
- **Read-only DC**
 - No – you need writable DC for first domain controller

5. Directory Services Restore Mode (DSRM) Password

- Set a strong password here.
- This is used when booting into DSRM mode to restore AD during disaster recovery.

This account is local to the server only, not a domain user.

6. NetBIOS Domain Name

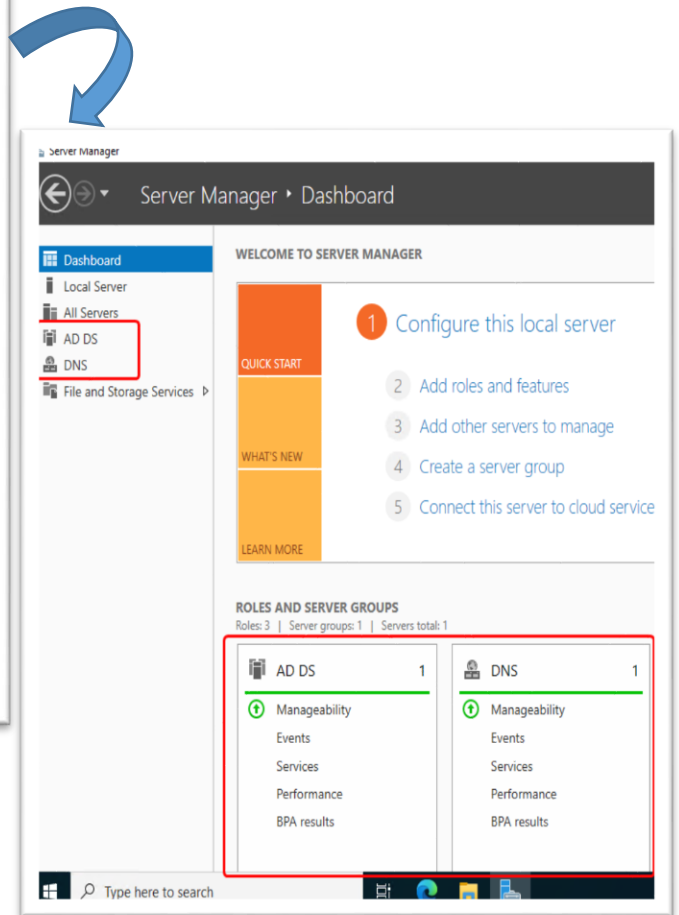
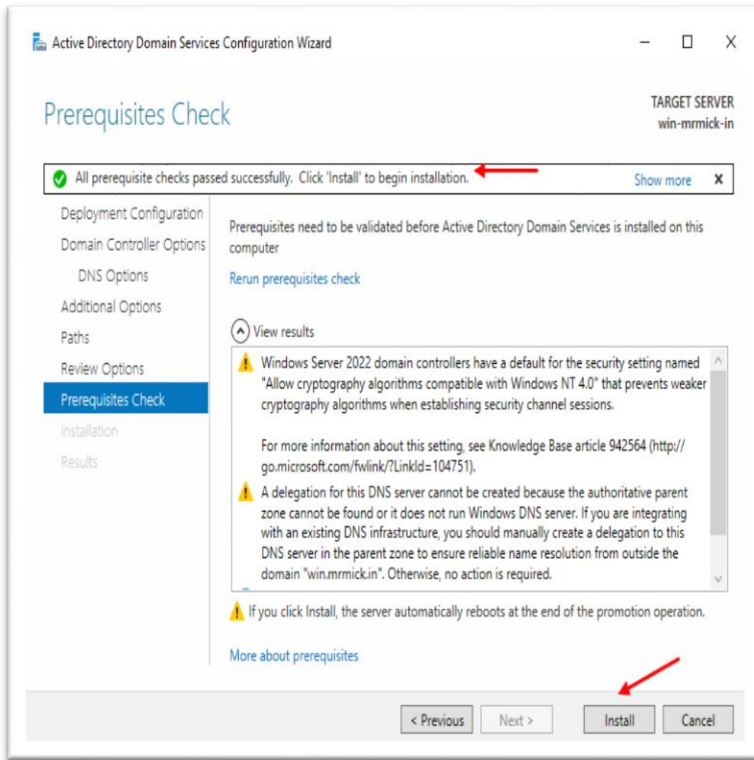
NetBIOS is an older naming system (used in legacy systems).

- Windows will automatically suggest a NetBIOS name based on your root domain.
 - E.g., corp.example.com → NetBIOS: CORP

You can change it if needed, but usually the default is fine.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Domain Controller Options' page. The window title is 'Active Directory Domain Services Configuration Wizard' and the target server is 'win-mrmick-in'. The left sidebar shows the navigation pane with 'Domain Controller Options' selected. The main content area is titled 'Domain Controller Options' and contains the following sections:

- Deployment Configuration:** A red box highlights the 'Domain Controller Options' link in the sidebar.
- Select functional level of the new forest and root domain:** Two dropdown menus are shown, both set to 'Windows Server 2016'. A red box highlights these dropdowns.
- Specify domain controller capabilities:** Three checkboxes are shown: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). A red box highlights the first two checked options.
- Type the Directory Services Restore Mode (DSRM) password:** Two password input fields are shown, both masked with dots. A red box highlights these fields.
- More about domain controller options:** A blue link is located at the bottom of the main content area.
- Navigation buttons:** At the bottom of the window are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. A red box highlights the 'Next >' button.



What is a Forest in Active Directory?

A Forest is the topmost container in Active Directory.

- It's like a whole company or organization.
- A forest can contain one or more domains.
- All domains in a forest trust each other automatically.
- All domains in a forest share the same schema and global catalog.

Forest = Security boundary + Logical container for domains.

Example:

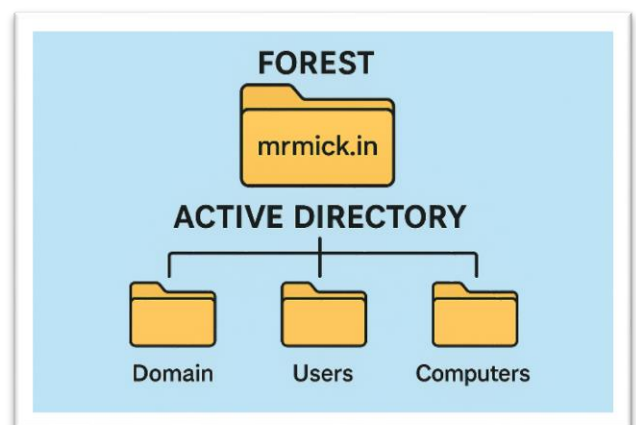
Imagine a company called TechWorld Inc.
They have multiple departments in different countries.

They might set up:
Forest Name: techworld.com

Domains under this forest:

- us.techworld.com (for USA)
- india.techworld.com (for India)
- uk.techworld.com (for UK)

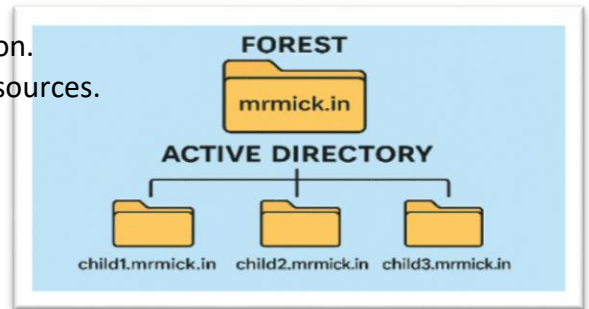
All domains are part of the same forest, share information, and trust each other.



What is a Domain in Active Directory?

A Domain is a group of objects (users, computers, printers, etc.) that are managed by the same security policies.

- It's like a department or branch within the organization.
- Domains are used to organize and secure network resources.
- Each domain has:
 - Its own Domain Controller(s)
 - A unique name (e.g., sales.techworld.com)
 - Its own Group Policies
 - Its own authentication

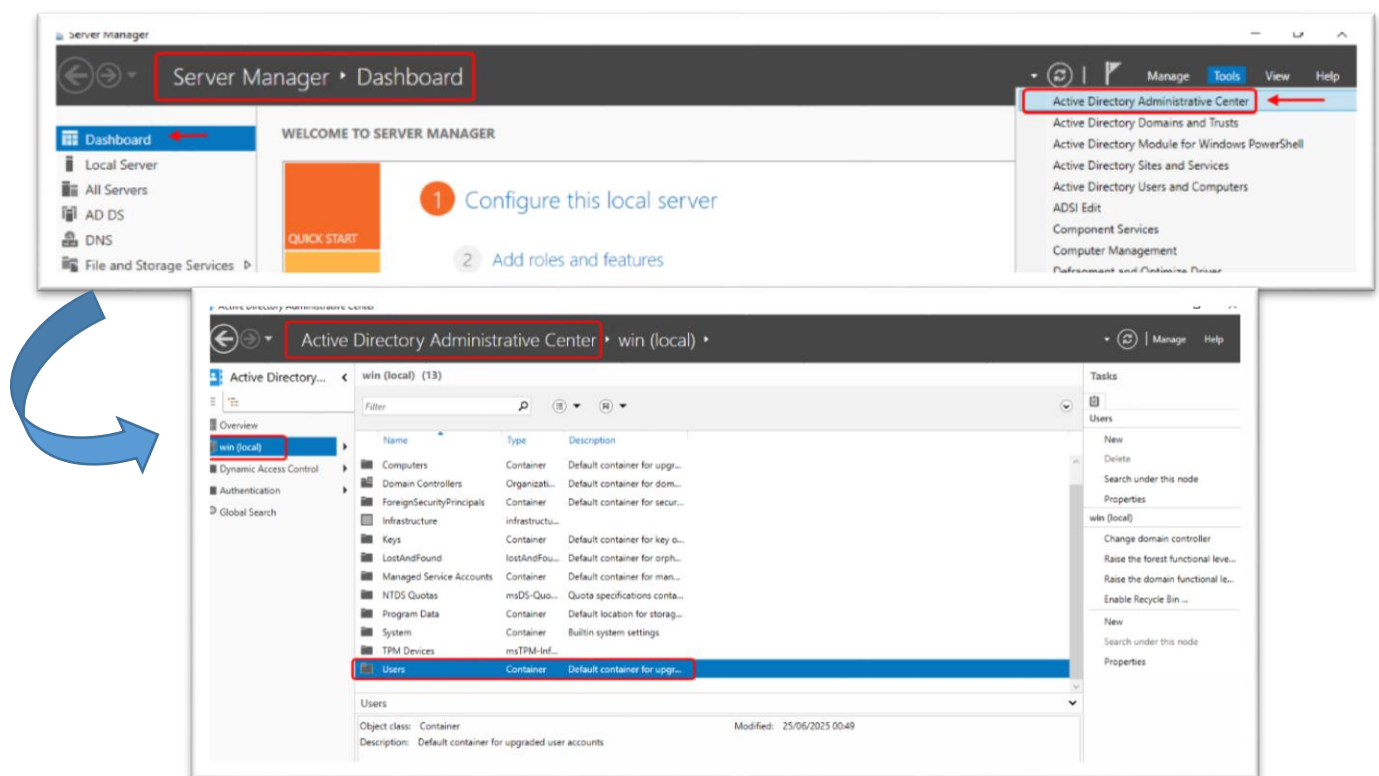


Domain = Unit inside a forest that holds users, computers, and resources.

02 Active Directory Management Tools

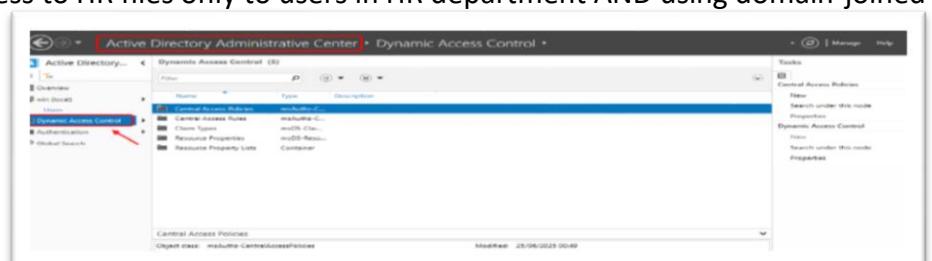
1. Active Directory Administrative Center (ADAC)

Tool to manage users, groups, OUs, GPOs, and advanced features in a modern interface.



a. Dynamic Access Control (DAC)

- DAC allows file/folder access based not only on users but also user claims, device claims, and resource properties.
- Example: "Give access to HR files only to users in HR department AND using domain-joined laptops."

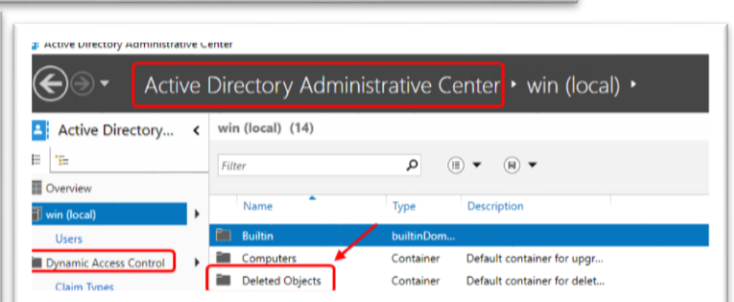
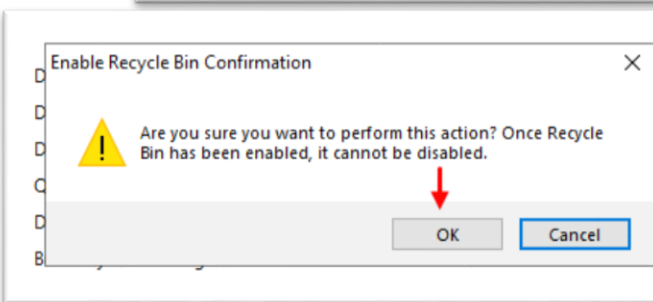
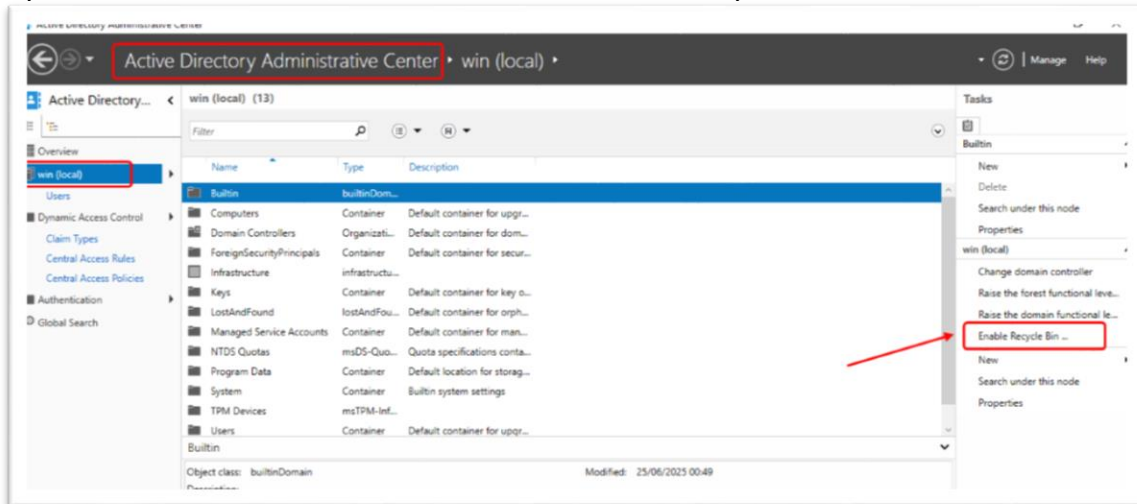


b. Enable Recycle Bin

- i. Allows recovery of deleted users, OUs, groups, etc. directly from the console.
- ii. Must be enabled per forest.
- iii. Once enabled, you can right-click → Restore deleted objects (before tombstone period ends).

Example Use Case:

Accidentally deleted a user account? Restore it in 1 click from Recycle Bin in ADAC.



2. Active Directory Domains and Trusts

Used to manage domain relationships and domain/forest functional levels.

a. Set Domain and Forest Functional Levels

- i. Define the lowest version of Windows Server allowed for DCs.
- ii. Example: Set Windows Server 2022 level to enable new security features.

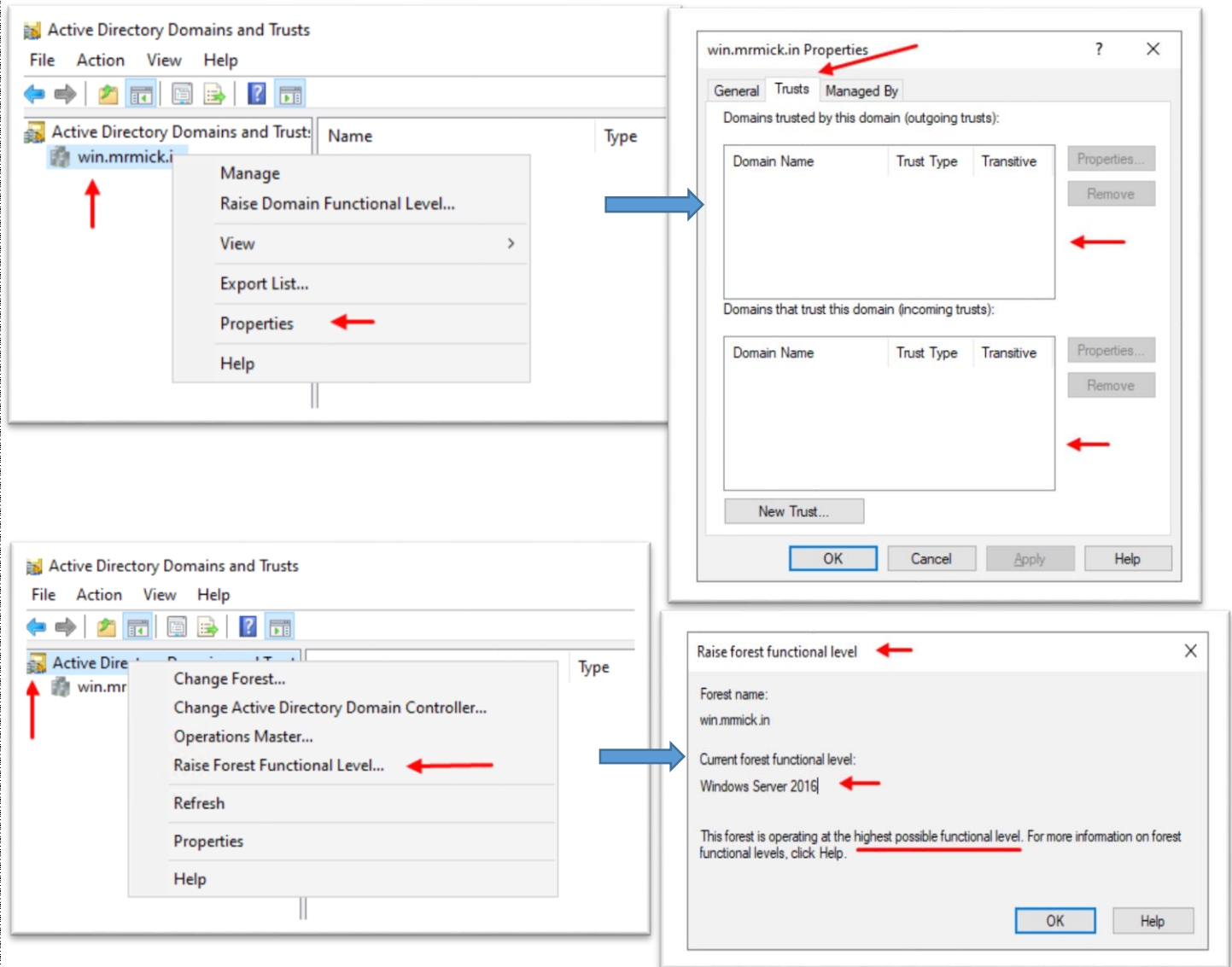
b. Create Trusts Between Domains/Forests

- i. Create trust relationships so users in one domain can access resources in another.
- ii. Example:
 - I. Trust between sales.example.com and hr.example.com → cross-domain access.

Example Use Case:

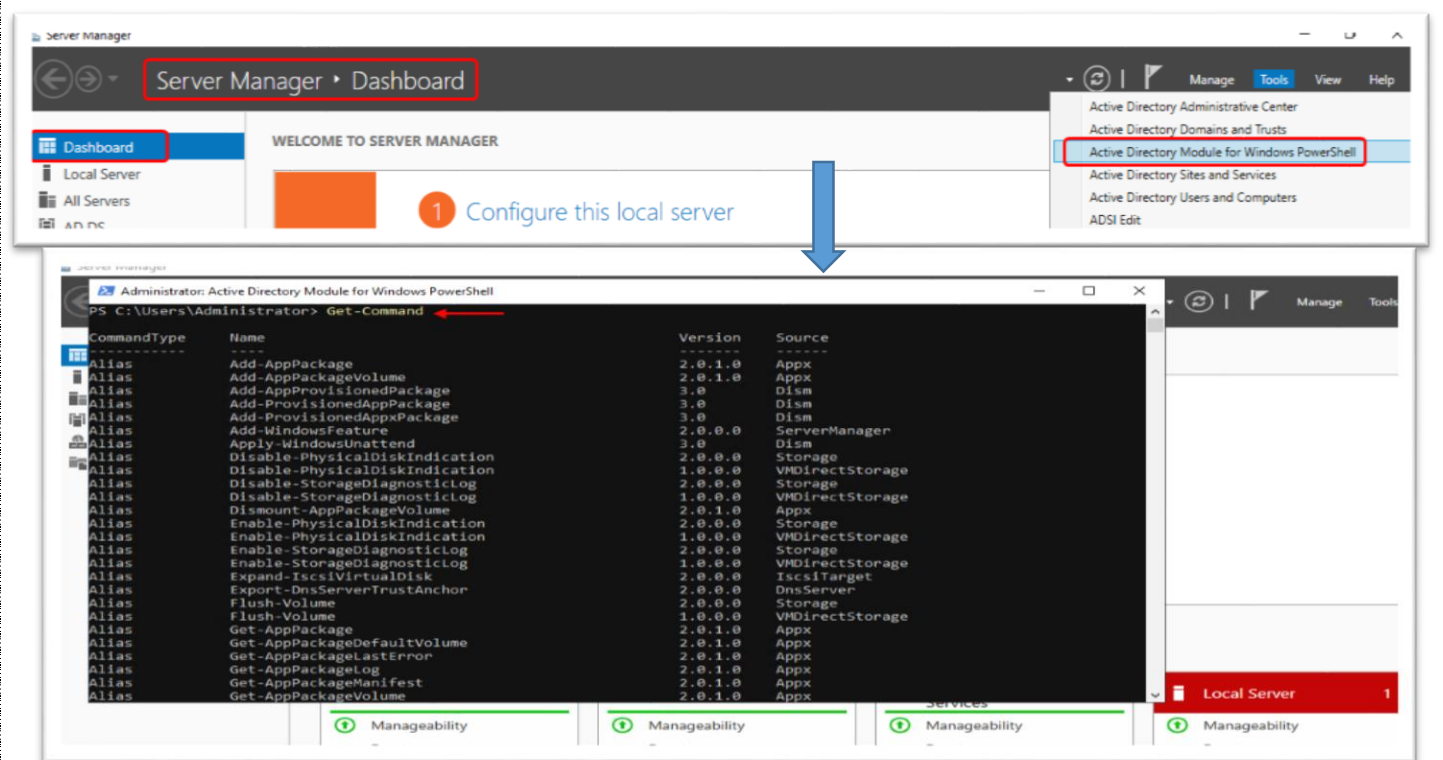
You want users in Domain A to access files in Domain B → create a two-way trust.





3. Active Directory Module for Windows PowerShell

It is a PowerShell extension that adds AD-specific cmdlets for scripting and automation.



4. Active Directory Sites and Services

Used to manage replication between domain controllers (DCs) across different physical locations (sites).

a. Replication

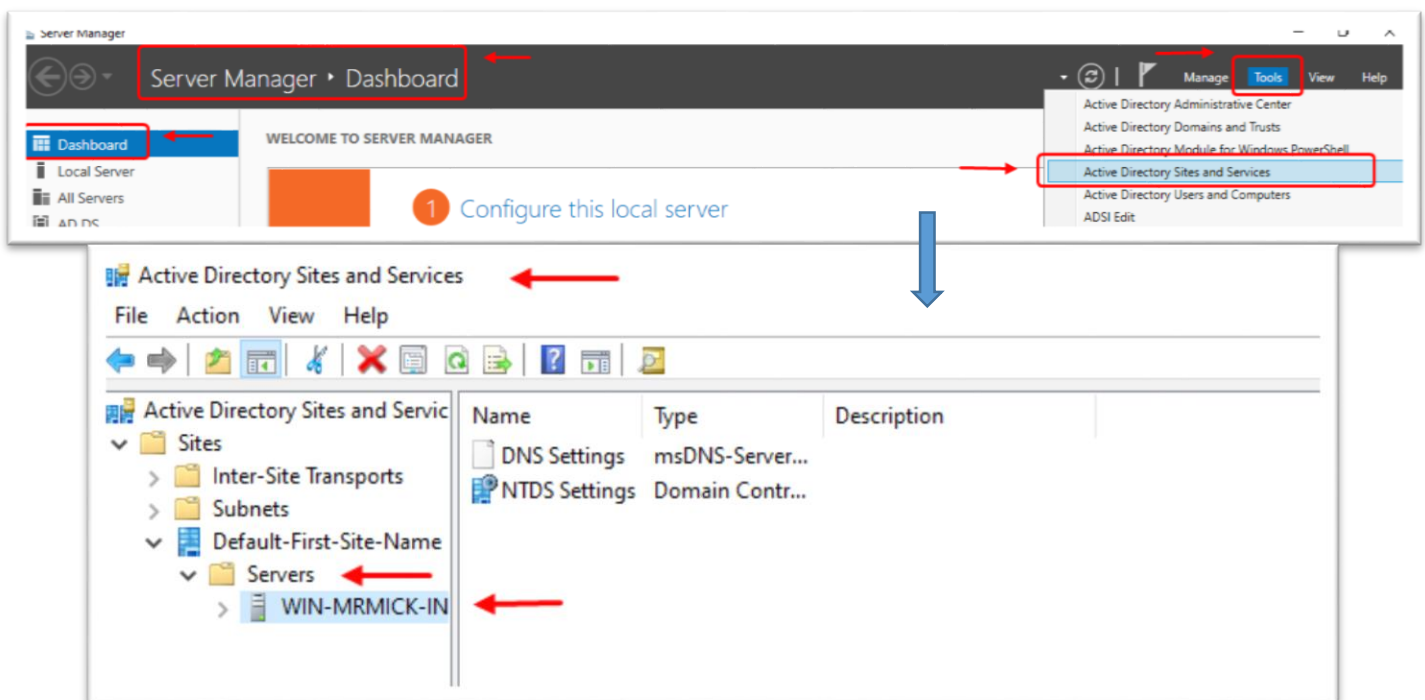
- i. AD replication is the process of copying data between domain controllers to keep them updated.
- ii. If you have multiple offices, you create sites to represent them.
- iii. Replication between DCs in the same site = fast
- iv. Replication between different sites = scheduled (to save bandwidth)

b. Components:

- i. Sites = Physical locations (e.g., New York, London)
- ii. Site Links = Define how sites talk to each other
- iii. Bridgehead Servers = Handle inter-site replication

Example Use Case:

You have DCs in India and UK. You want AD to replicate every 3 hours between them — configure this in Sites and Services.



5. Active Directory Users and Computers (ADUC)

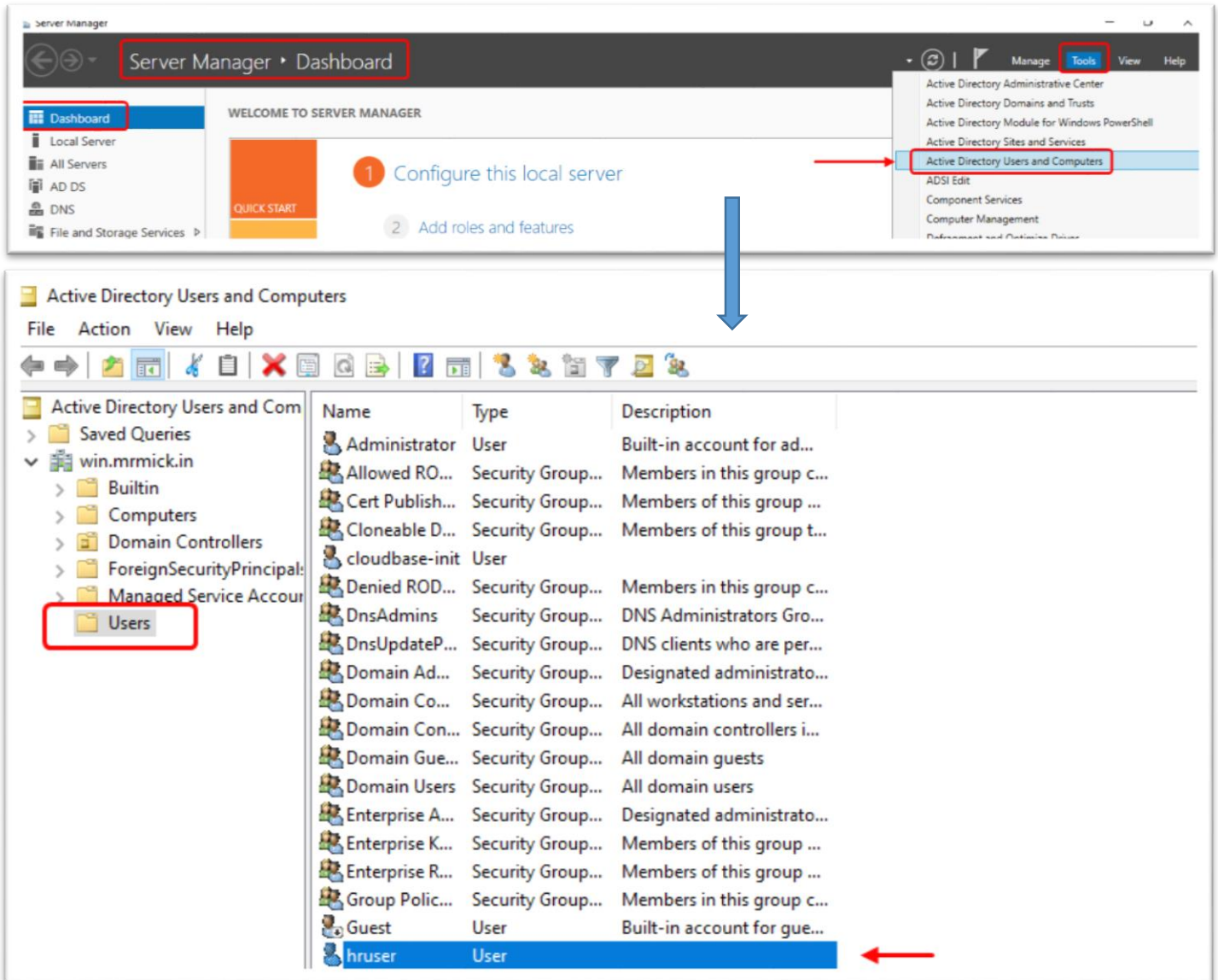
The most common and basic tool to manage users, groups, OUs, and computers.

a. Key Features:

- i. Create/modify users
- ii. Reset passwords
- iii. Move objects between OUs
- iv. Create security groups
- v. Delegate control
- vi. Set Group Memberships

Example Use Case:

HR requests creation of 5 new user accounts — do it via ADUC.
Reset a user's password or disable a leaving employee's account.



03 - Adding Second Domain Controller OR Child Domain

Why Add a Second Domain Controller?

Adding a second DC to your domain provides:

- Redundancy: If the first DC goes down, users can still log in and authenticate.
- Load Balancing: Authentication requests are split between DCs, improving performance.
- Replication: Both DCs share AD data — changes in one are replicated to the other.

Lab Setup Example

- First DC is: Server-01 (DC01) → Already a Domain Controller for domain: mrmick.in
- Now you want to make Server-02 a second Domain Controller in the same domain.

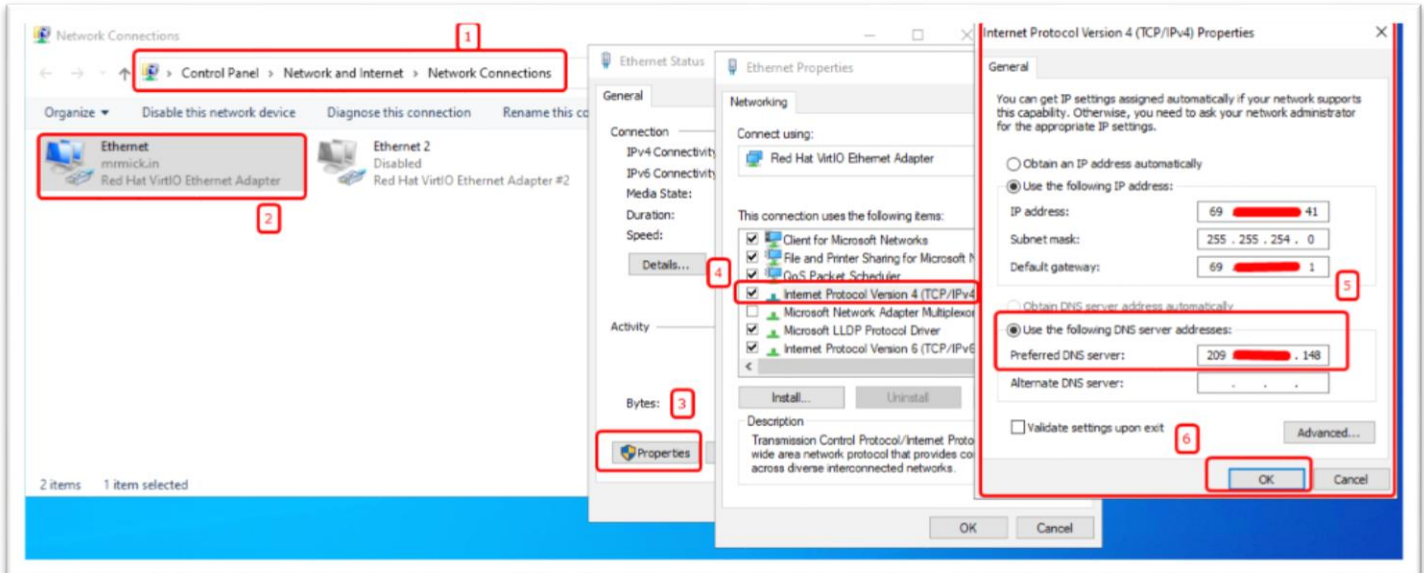
🚦 Step-by-Step Guide to Add a Second Domain Controller

✓ Step 1: Set Correct DNS on Server-02 (DC02)

- On Server-02 (DC02), go to:
 - Control Panel > Network Adapter Settings > IPv4
 - Set Preferred DNS = IP of Server 01 (your first DC – DC01)

Why?

Because Server-02 needs to contact Server-01 to find domain info and join the domain.



✓ Step 2: Join Server-02 (DC02) to the Domain (In tutorial this has been skipped)

- Right-click This PC > Properties > Rename this PC (advanced)
- Click Change and join domain: mrmick.in
- Reboot after successful domain join.

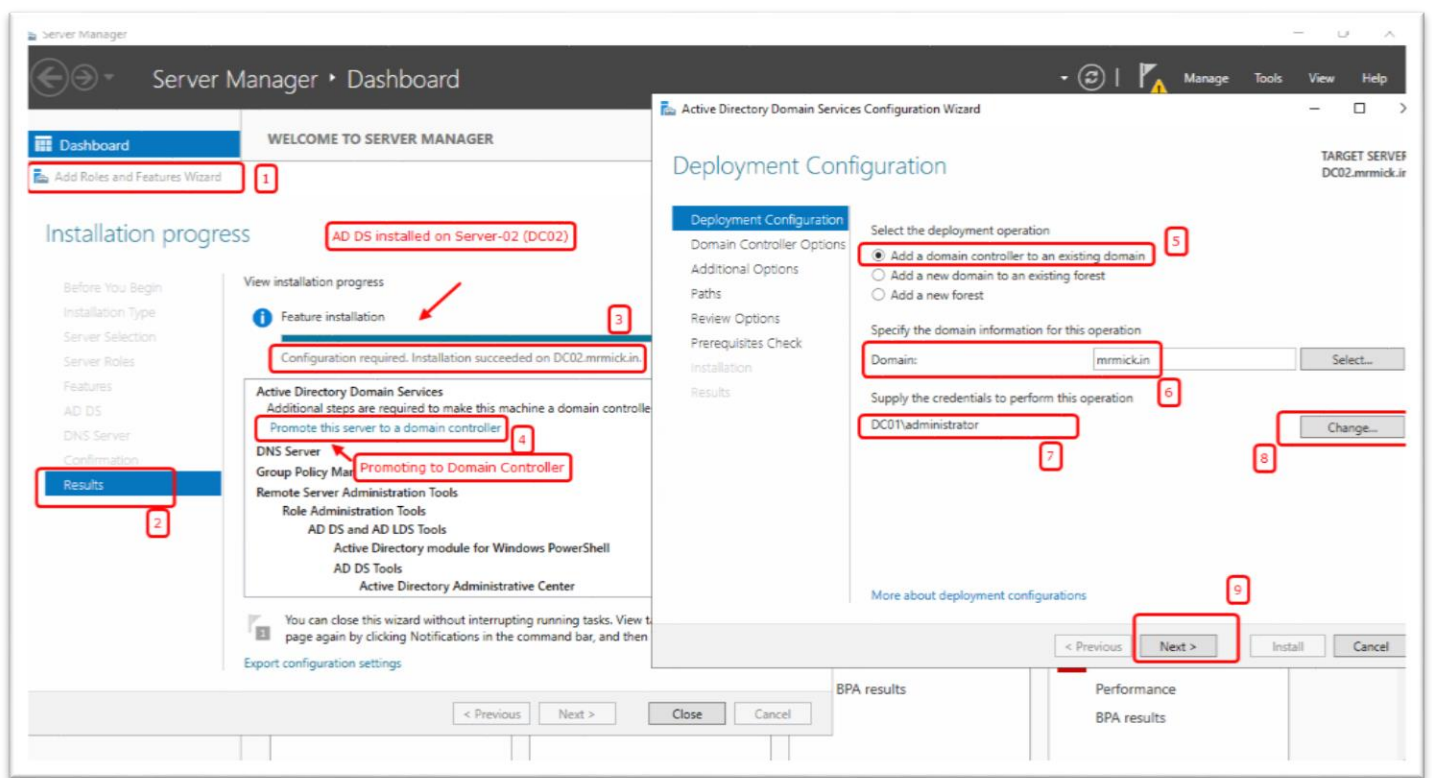
✓ Step 3: Install Active Directory Domain Services Role

- On Server-02 (DC02):
 - Open Server Manager
 - Click Add Roles and Features
 - Select Active Directory Domain Services
 - Click Next > Next > Install

[This has been showed above, check the steps to install Active Directory Domain Services]

✓ Step 4: Promote Server-02 to Domain Controller

- After install finishes, click Promote this server to a domain controller
- Choose:
 - Add a domain controller to an existing domain
- Enter:
 - Domain: mrmick.in
 - Credentials: Use Domain Admin account from Server-01



✓ Step 5: Choose Domain Controller Options

- DNS Server (Keep checked)
- Global Catalog (GC) (Keep checked)
- Read-only domain controller (RODC) (Leave unchecked for full DC)
- Set DSRM password (Directory Services Restore Mode password)

What Happens Now?

- Server02 becomes another DC for mrmick.in
- It starts replicating AD data with Server-01 (DC01)
- Both DCs can handle:
 - User logins
 - Group Policy
 - DNS queries (if DNS role is installed)

Real-World Example

Imagine your head office is in Delhi, and branch in Mumbai.

You already have DC in Delhi. You set up a second DC in Mumbai (connected via VPN).


Now users in Mumbai authenticate locally, not over slow WAN — and if Delhi DC fails, Mumbai still runs smoothly.

04 - Joining AD from a workstation

What Is Joining a Workstation to AD?

Joining a workstation (e.g. Windows 10/11 PC) to Active Directory allows:

- Centralized login using domain credentials
- Applying Group Policies
- Easier device and user management from the domain controller

 **Before You Start**

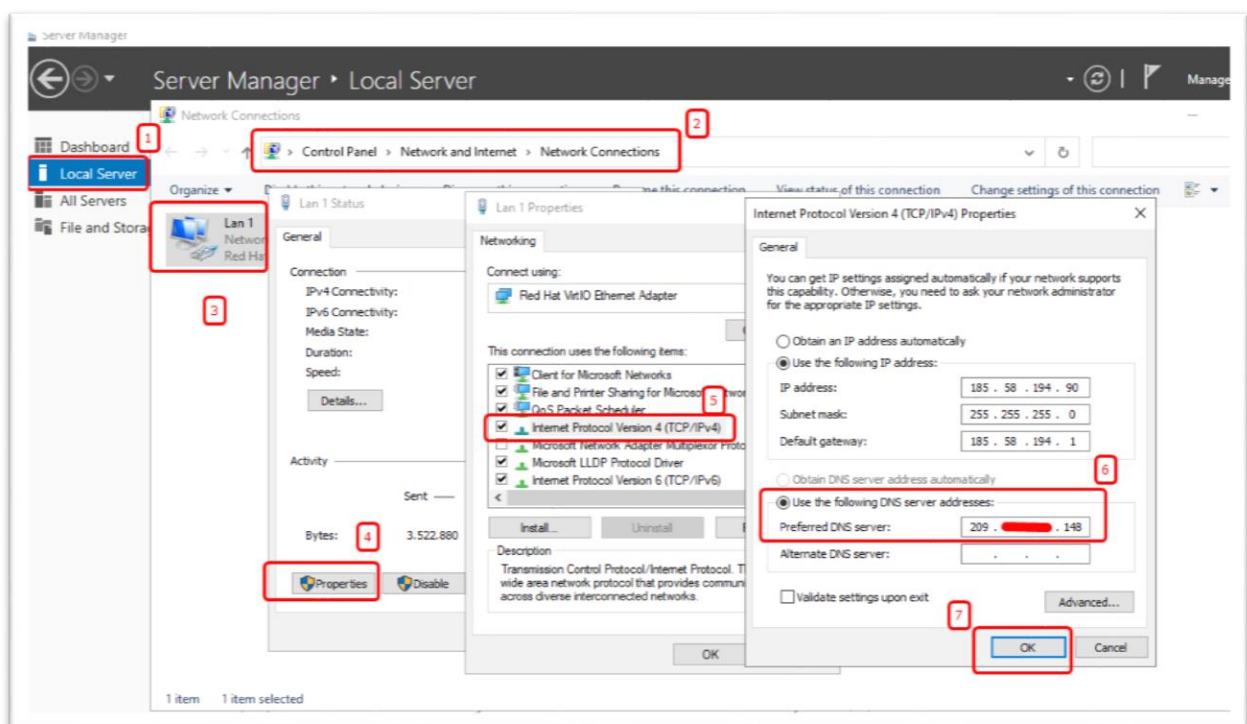
Make sure:

Requirement	Why?
PC is on the same network/subnet as the Domain Controller	So they can talk to each other
PC's DNS server is set to the Domain Controller's IP (e.g. 192.168.1.10)	So it can find the domain
You have Domain Admin credentials (e.g. admin@corp.local)	Required to join machines to domain

Steps to Join a Workstation to AD

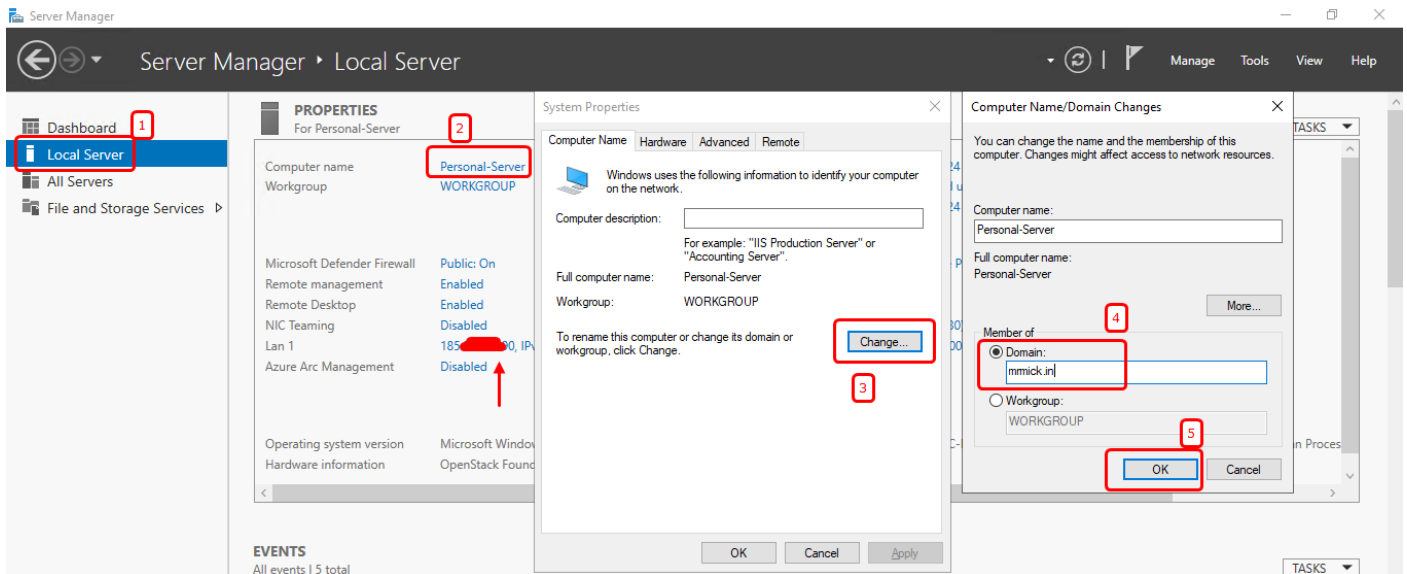
a. Step 1: Set DNS on Workstation

- Go to Control Panel > Network and Sharing Center
- Click your network > Properties > IPv4
- Set Preferred DNS to IP of Domain Controller (e.g., 192.168.1.10)
- Click OK



b. Step 2: Join the Domain

- i. Right-click This PC > Properties
- ii. Click Advanced system settings > Computer Name tab
- iii. Click Change
- iv. In Member of, select:
 - ✓ Domain, and enter: corp.local (or your domain name)
- v. Click OK
- vi. Enter Domain Admin credentials when prompted



Behind the scenes:

- The PC sends a request to the DC
- DC authenticates the credentials
- DC creates a computer object in AD

How to Verify in Active Directory

On Domain Controller:

1. Open Server Manager > Tools > Active Directory Users and Computers
2. Click on Computers container (left side panel)
3. You will see the workstation name listed there

05 - File Sharing and Drive Mapping

Part 1: Creating and Sharing a Folder

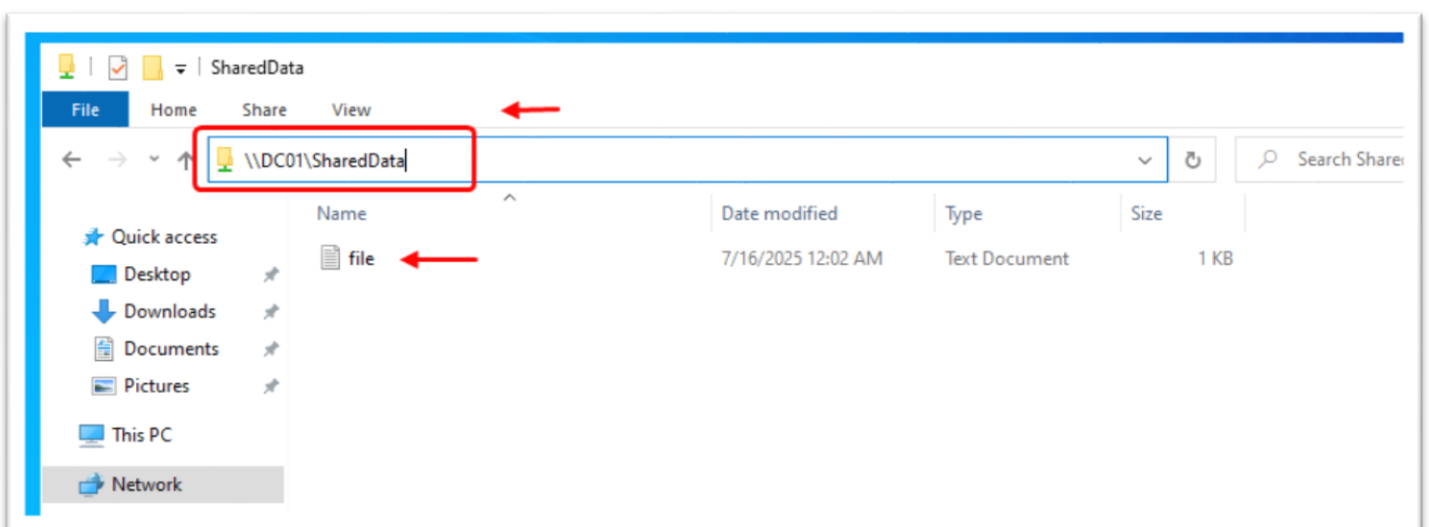
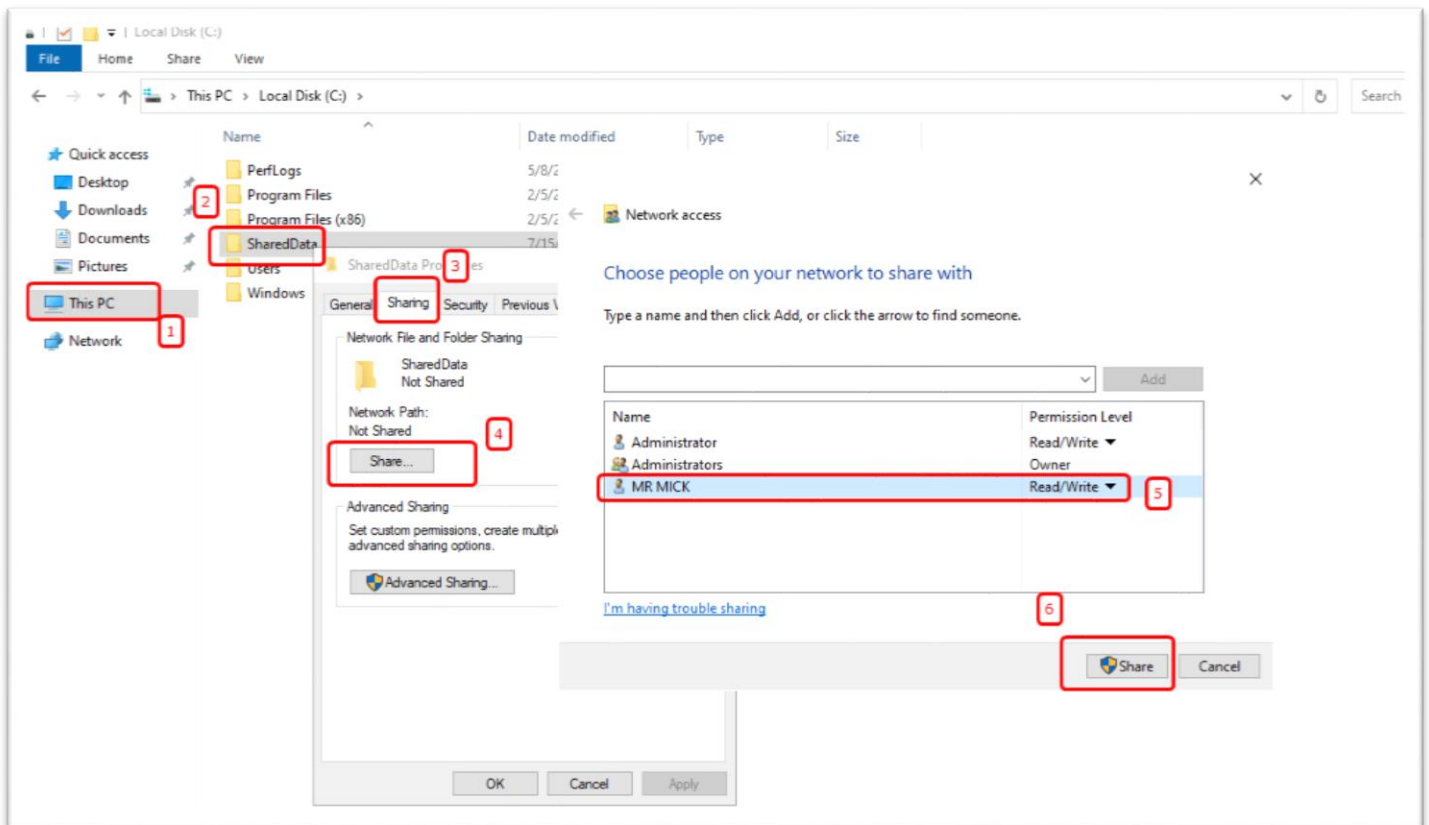
You want to share a folder from a server (e.g., Domain Controller or File Server) with domain users.

Steps to Share a Folder:

1. Create a folder, e.g.,
C:\SharedData
2. Right-click > Properties > Sharing tab

Option 1: Basic Sharing (Share Button)

- a) Click Share
- b) Add users or groups (e.g., HRGroup, Domain Users)
- c) Set permissions (Read / Read-Write)
- d) Click Share and then Done



Option 2: Advanced Sharing

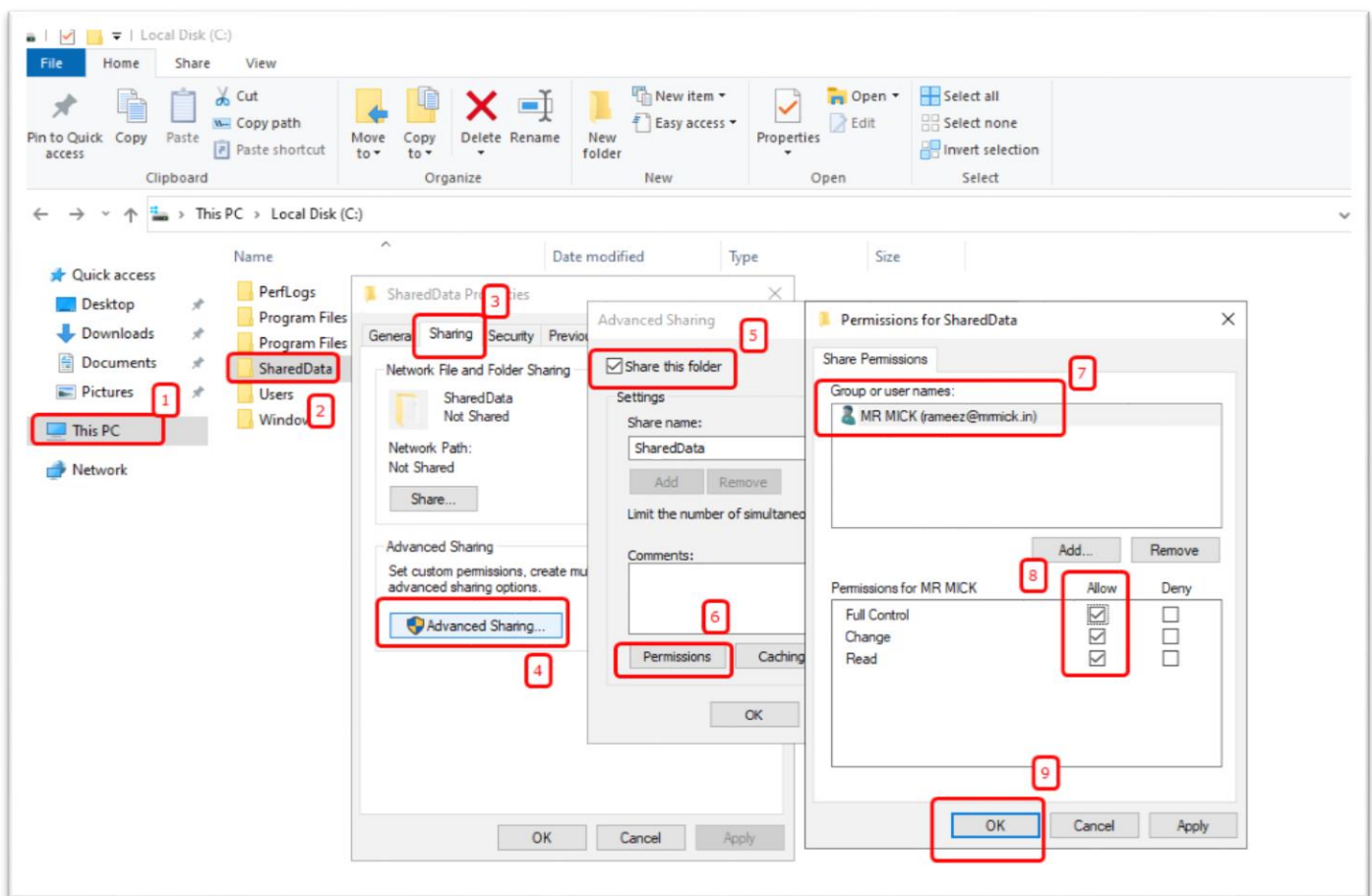
- Click Advanced Sharing
- Check: ✓ "Share this folder"
- Set Share Name (e.g., HRShare)
- Set Limit number of users if needed
- Click Permissions

Default has Everyone = Read

Remove Everyone group to avoid giving access to all users in the domain — it's not secure.

What is "Caching" in Advanced Sharing?

- Caching allows offline access to shared files
- If enabled, users can open/edit files without being connected, and files will sync when reconnected



Part 2: Security Tab – NTFS Permissions

Go to:

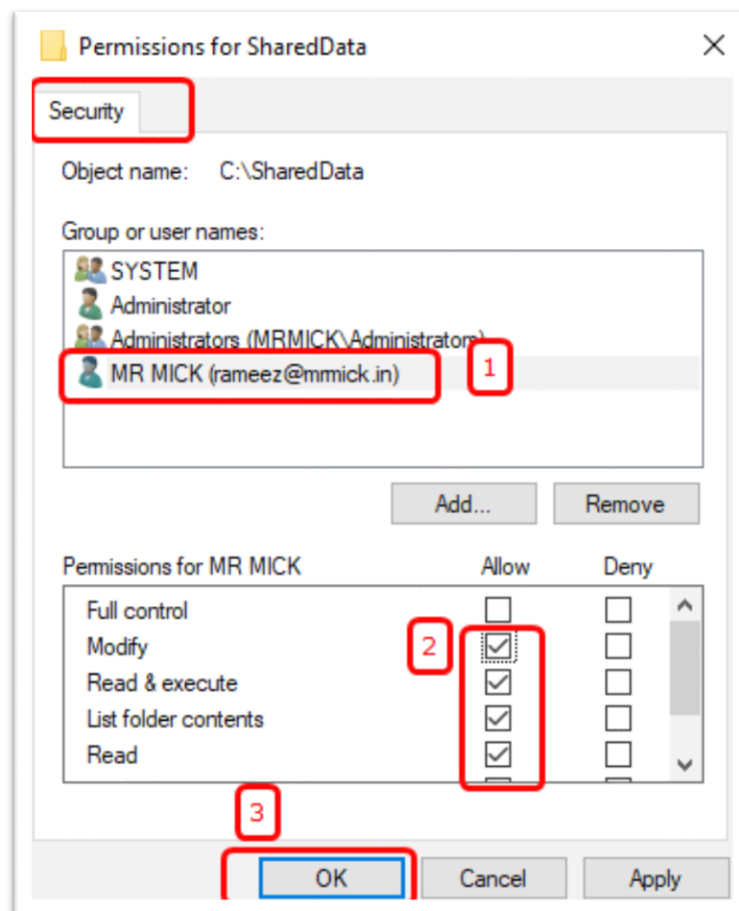
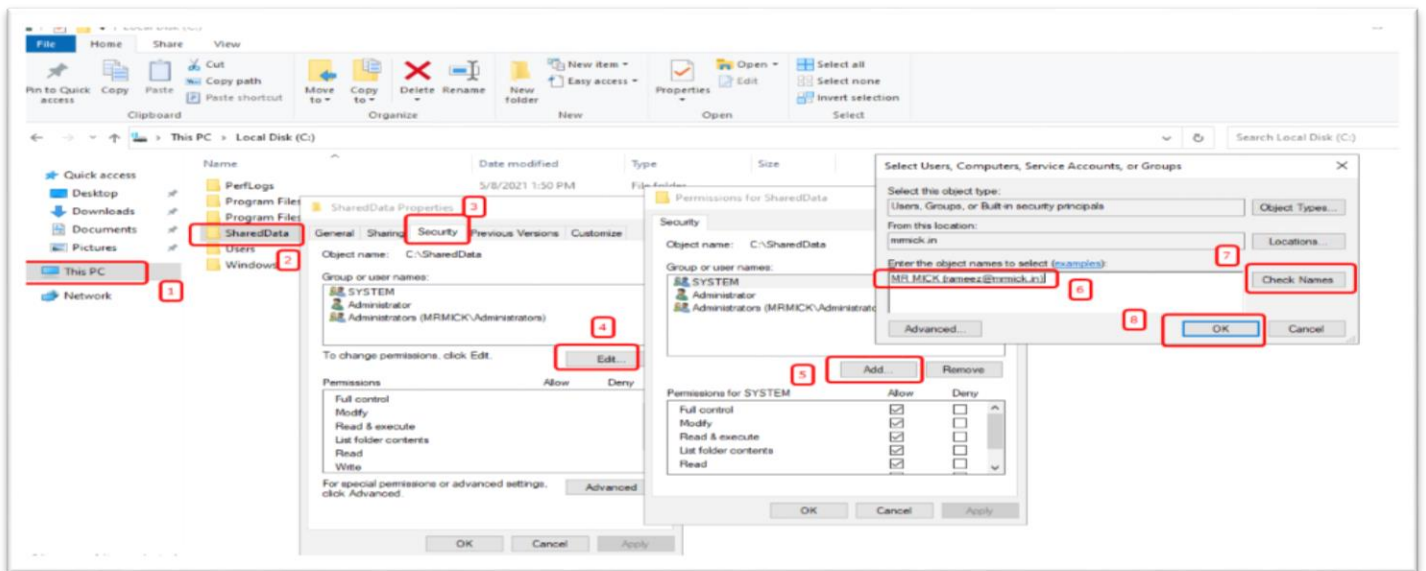
- Right-click folder > Properties > Security Tab

What You Do Here:

- Set actual permissions on the file system
- These are more detailed and secure

Steps:

- Click Edit
- Remove or modify CREATOR OWNER if needed
- Click Add to add users or groups (e.g., rameez)
- Set Permissions:



Important Concept: Share vs. NTFS Permissions

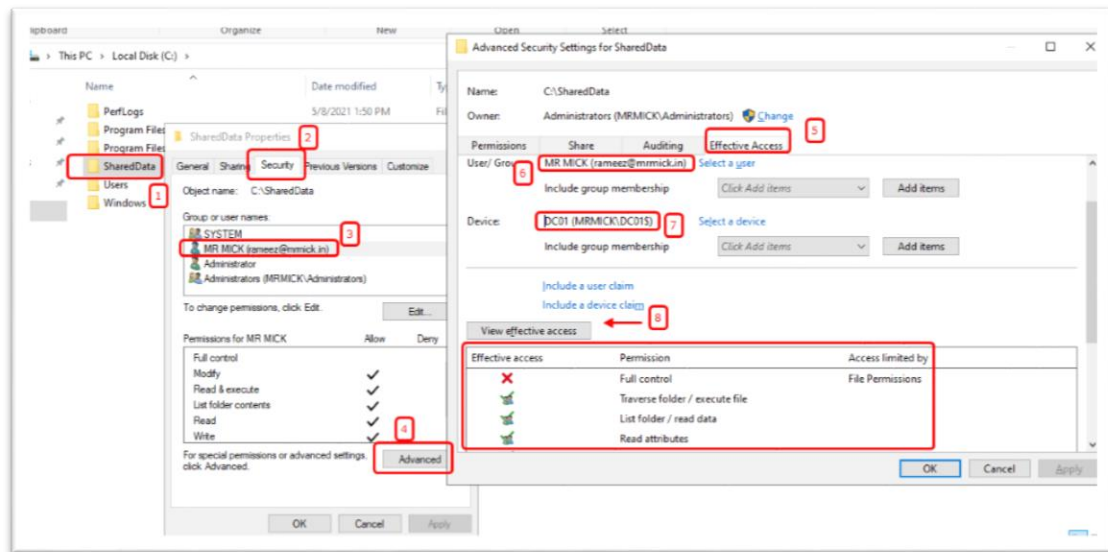
Type	Where	Controls
Share Permissions	Sharing tab	Who can access folder over the network
NTFS Permissions	Security tab	Who can access folder locally or via network

Most restrictive permission wins
If:

- "Share permission = Full Control"
- "NTFS = Read
→ User gets Read only"

Checking Access: "Effective Access"

1. Go to Security Tab > Advanced
2. Click Effective Access
3. Select a user or group
4. Click View effective access



This shows exactly what permissions that user has, considering both Share and NTFS.

File Sharing Using Server Manager

Instead of right-clicking a folder, you can use Server Manager > File and Storage Services for a more structured and scalable way to manage shared folders.

Steps to Create a Shared Folder

Step 1: Open Server Manager

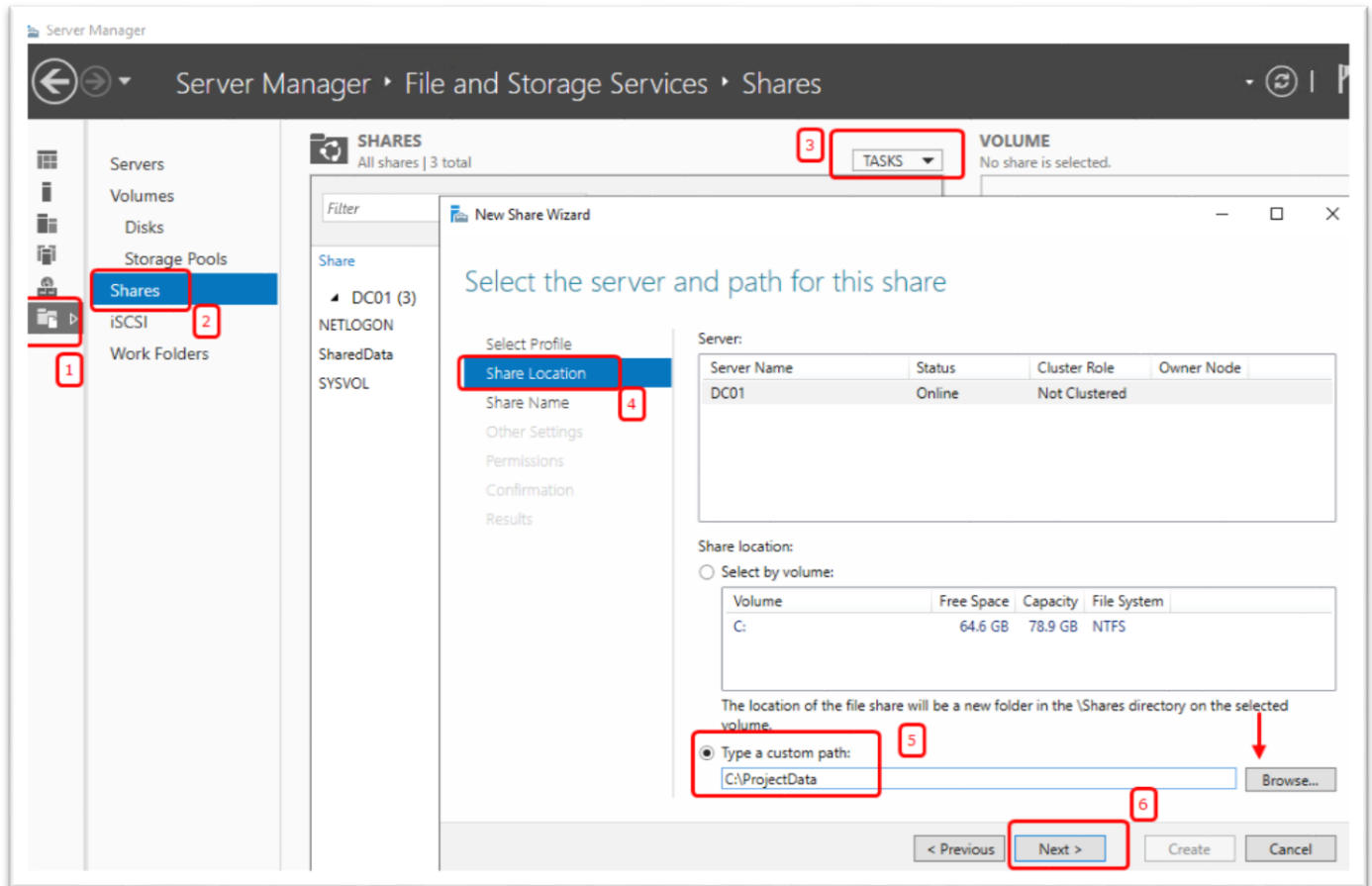
1. Open Server Manager
2. Click on File and Storage Services > Shares
3. On the top-right, click Tasks > New Share

Share Profile Types (Options You See)	
Option	Purpose
SMB Share - Quick	Basic, simple sharing
SMB Share - Advanced	Adds more controls like quotas, file screening via FSRM
SMB Share - Applications	For use with apps like Hyper-V or SQL (handles large files & metadata better)
NFS Share - Quick/Advanced	For Linux/Unix/Mac systems to connect to your Windows shares

Step-by-Step: Create SMB Share – Quick

1. Choose Profile
 - a. Select: SMB Share - Quick (simple folder sharing)
2. Select Share Location
 - a. Type or browse custom folder path

Example: C:\ProjectData



3. Configure Share Settings

Enable Access-Based Enumeration

- Only shows the files/folders a user is allowed to access
- Hides other files/folders from unauthorized users

Example:

User A only has access to Folder A — they won't even see Folder B in the same share

Allow Caching of Share

- Allows offline access
- Users can work with files while disconnected, and changes sync back when reconnected

Example:

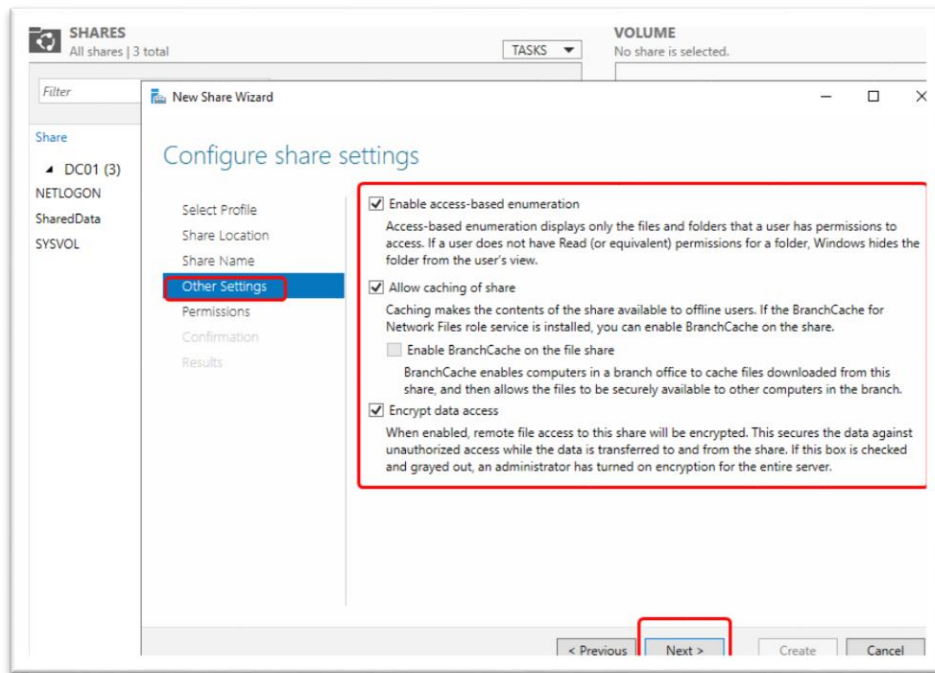
A laptop user goes out of office, edits a file offline → once they return and connect, changes sync

Encrypt data access

- Secures data while transferring over network
- Helps protect against sniffing/hacking

Example:

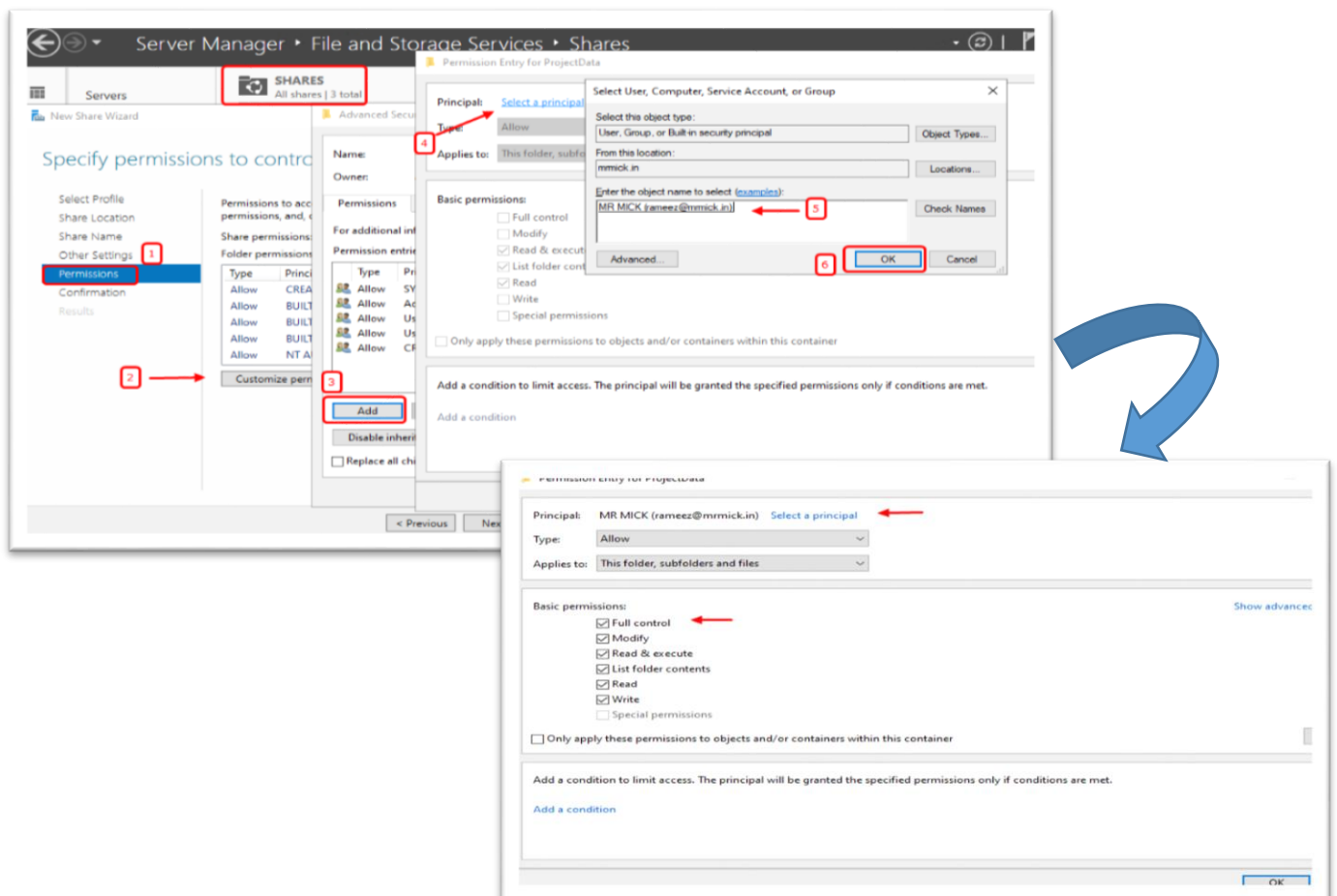
If user accesses share over Wi-Fi or public LAN, data is encrypted during transfer.

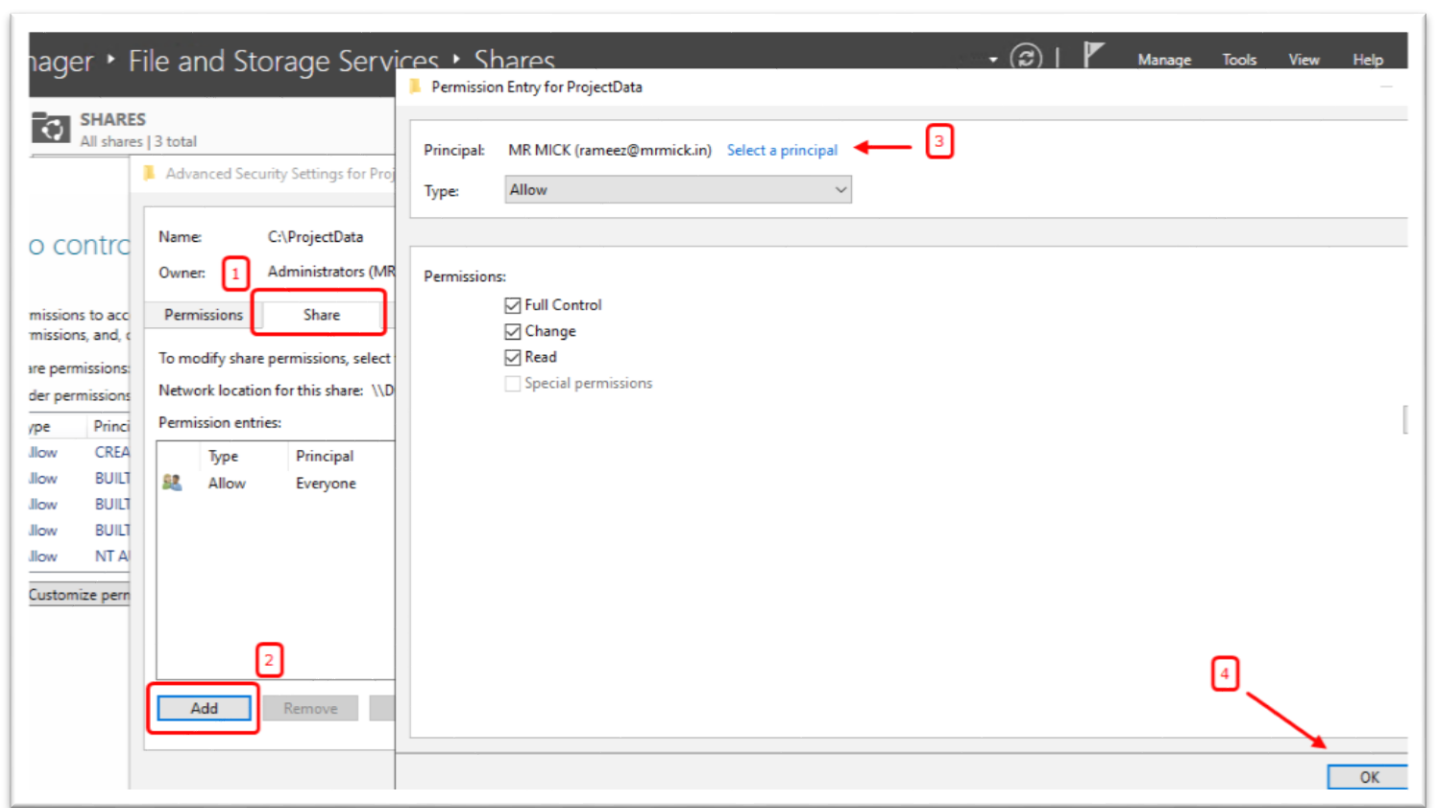


4. Customize Permissions

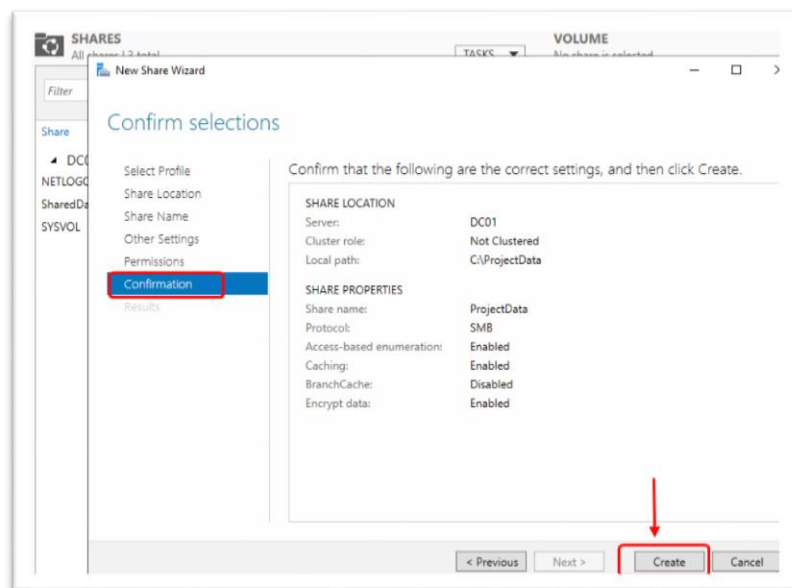
Click Customize permissions, then:

- Go to Permissions tab (same as NTFS Security tab)
- Add Domain Users group
- Give them Modify or Read access
- Remove "Everyone" (to avoid open access)
- On Share tab, also remove Everyone and give Full Control to desired group





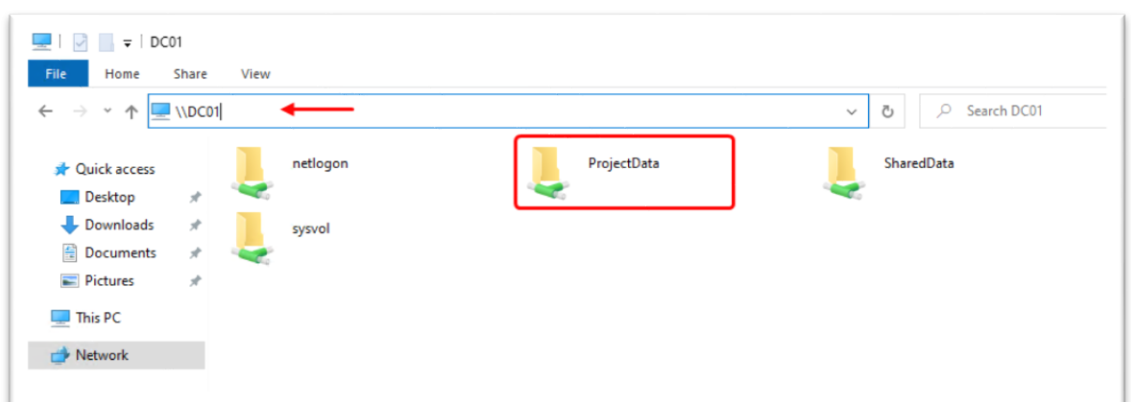
5. Create the Share



After Share Is Created

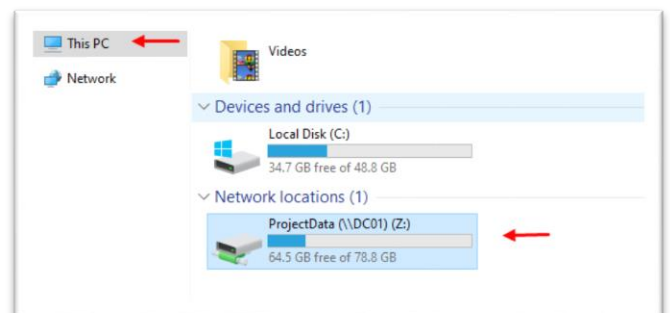
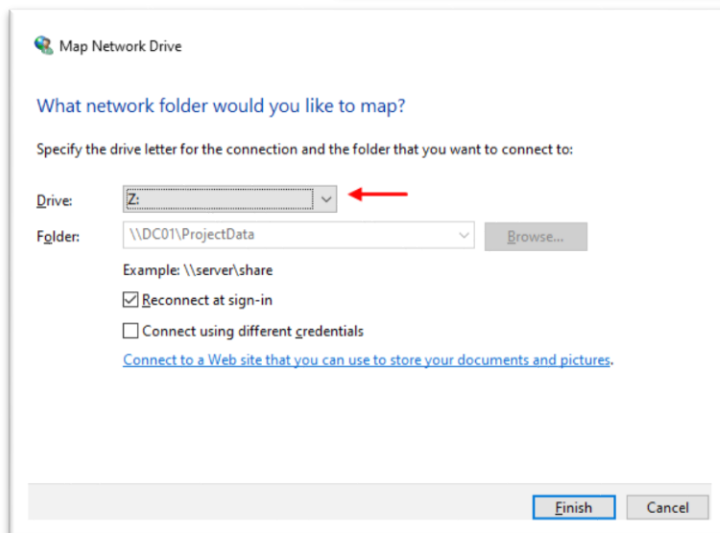
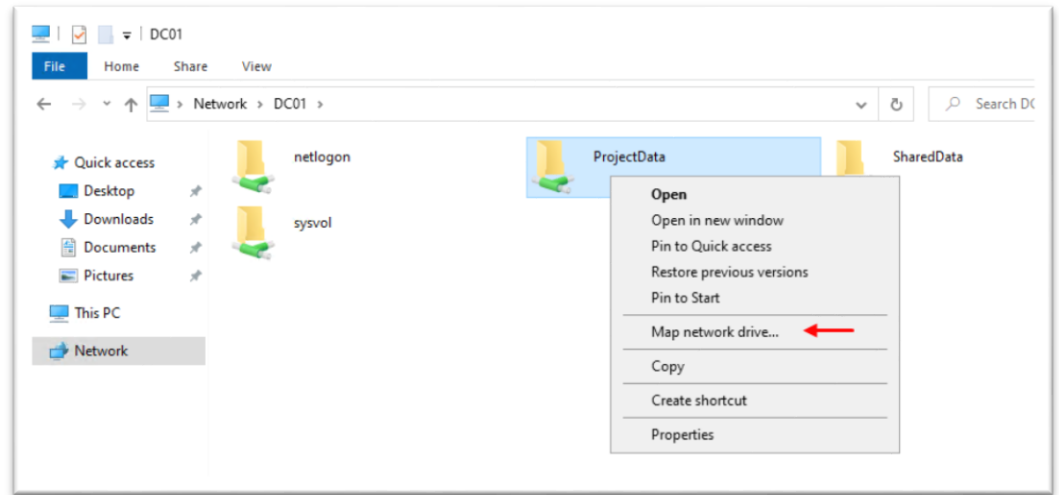
Access the Share from Client:

1. Open File Explorer
2. Type the UNC path in address bar:
 - a. [\\ServerName\ProjectData](#)



OR

3. Map a Drive (optional):
 - a. Right-click This PC > Map Network Drive
 - b. Choose Drive Letter (e.g., Z:)
 - c. Enter path: \\ServerName\ProjectData
 - d. Check Reconnect at logon
 - e. Done!



06 - Group Policy

Group Policy lets administrators control user and computer settings from a central place in Active Directory (AD).

Example: You want to hide the Recycle Bin from all users' desktops — instead of going to each PC, you do it once using Group Policy.

Tool Used: Group Policy Management Console (GPMC)

How to Open:

- Server Manager > Tools > Group Policy Management

Step-by-Step: Create a GPO to Hide Recycle Bin


Step 1: Create New Group Policy Object (GPO)

1. In Group Policy Management, right-click your domain name
Example: mycompany.local
2. Click: "Create a GPO in this domain and link it here"
3. Name it:
 - a. Hide Recycle Bin


This applies the policy at domain level (applies to all users). If you want it to apply only to some users, move it to a specific OU (Organizational Unit).

Step 2: Edit the GPO

1. Right-click your GPO (Hide Recycle Bin) → Click Edit
2. You'll see two main sections:

 **Group Policy Editor: Two Main Sections**

Section	Applies To	Example Settings
Computer Configuration	Affects the machine , no matter who logs in	Set password policies, disable USB
User Configuration	Affects the user , no matter which PC they log in from	Hide Recycle Bin, lock Control Panel

 Since we want to hide the **Recycle Bin** for users, we use **User Configuration**

Step 3: Hide Recycle Bin

Navigate to:

```
pgsql

User Configuration >
  Administrative Templates >
    Desktop >
      Hide and disable all items on the desktop
```

Or more directly:

```
pgsql

User Configuration >
  Administrative Templates >
    Desktop >
      Remove Recycle Bin icon from desktop
```


1. Double-click: Remove Recycle Bin icon from desktop
2. Set to: Enabled
3. Click Apply > OK

Now this setting will remove Recycle Bin from desktop for users affected by this GPO.

Step 4: Delegation (Optional)

You can control who can edit or manage this GPO.

- a. In GPMC, select the GPO
- b. Go to Delegation tab
- c. Click Add to give permission (Read / Edit / Full)
- d. Use this to restrict junior admins from editing critical GPOs

Applying the GPO

Once created, the GPO will apply automatically:

- At next login for user-based settings
- Or during background refresh (every 90-120 mins by default)

To apply immediately, you can:

- Go to a client PC → open Command Prompt
- Run:
 - gpupdate /force

Where Is the GPO Stored?

In GPMC, look under:

- Group Policy Objects → this contains the actual GPO "files"
- You can edit GPOs from here even if not yet linked

Example Lab Scenario

Goal: Hide Recycle Bin only for users in HR

- Create an Organizational Unit: HR
 - Move HR users into that OU
 - Create and link the Hide Recycle Bin GPO to the HR OU
 - Edit GPO → User Config → Desktop → Remove Recycle Bin icon
 - Apply GPO
 - Login as HR user on client → Recycle Bin should be gone
-

07 - DNS Management

What is DNS in Windows Server?

- DNS = Domain Name System
- It translates names (like server01.company.com) to IP addresses (like 192.168.1.10) so computers can talk to each other.

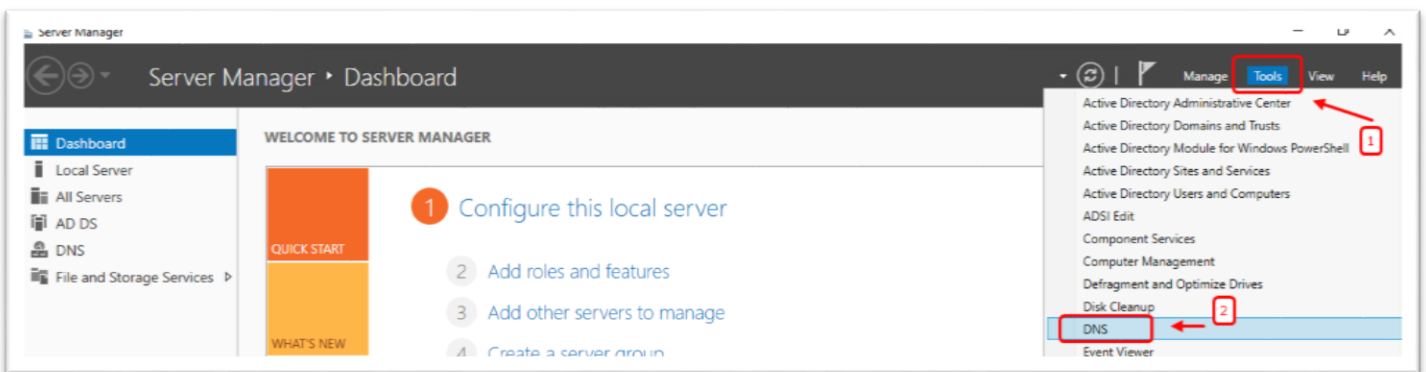
Why It Matters for AD?

Active Directory relies heavily on DNS:

- It uses DNS to locate domain controllers, services, and replicate data.
- If DNS is misconfigured, logins, Group Policy, and AD tools will fail.

Open DNS Manager

- Go to Server Manager > Tools > DNS

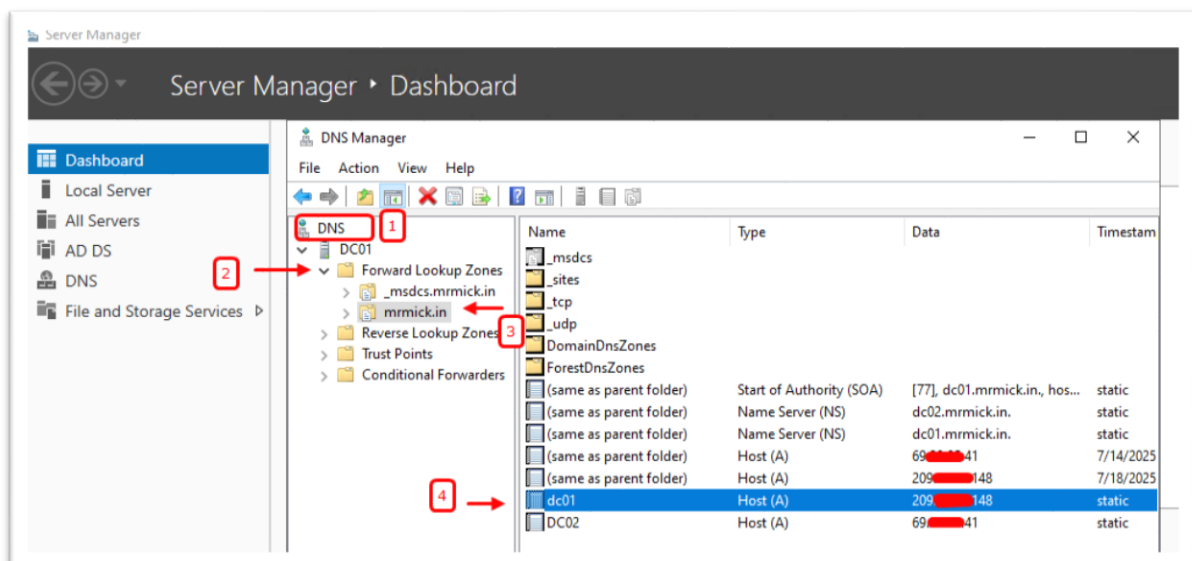


Default Zones Created with AD

When you install Active Directory Domain Services (ADDS) and promote to Domain Controller, Windows automatically sets up DNS and creates two zones:

1. Forward Lookup Zone (company.local)

- a. Translates name → IP
- b. Example record: server01.company.local → 192.168.1.10

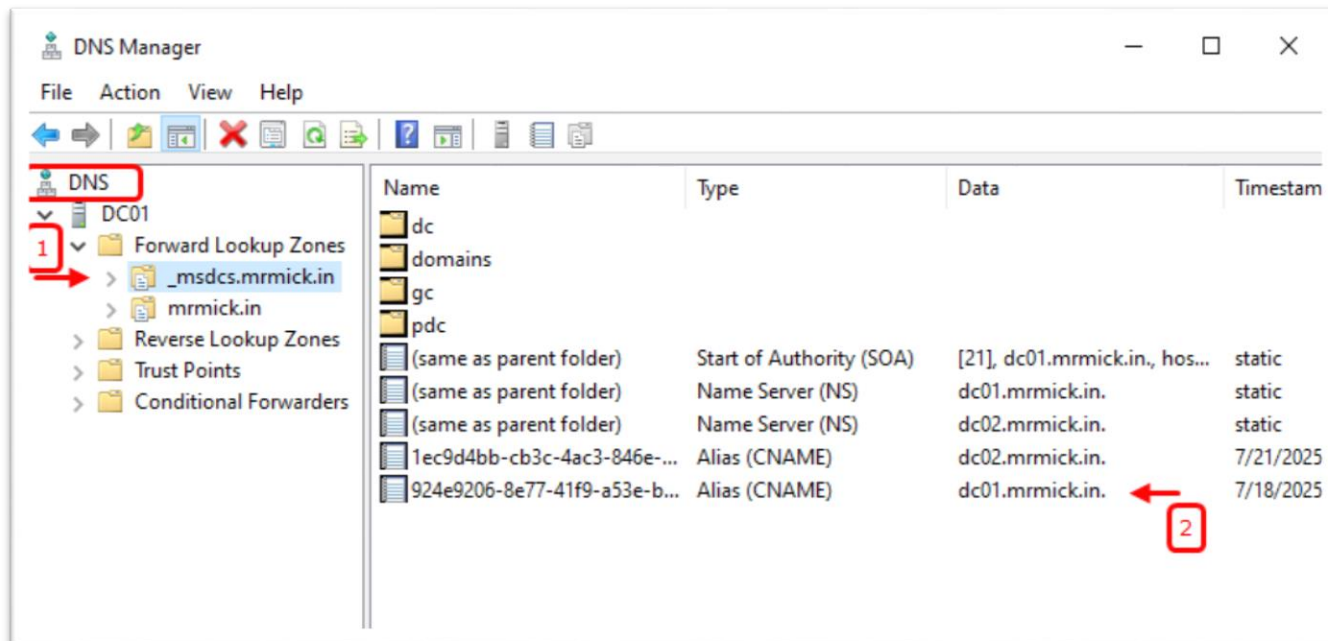


This is the working/production zone.

2. _msdcs.company.local

- a. _msdcs = Microsoft Domain Controller Services
- b. Contains records required for AD replication and locating domain controllers
- c. Includes:
 - i. SRV records for services like LDAP, Kerberos
 - ii. GUID-based entries for each DC

It is automatically replicated to other DNS servers when they are also domain controllers.



Creating a New Zone

Right-click Forward Lookup Zones > New Zone

You'll choose between:

1. Primary Zone

- a. Main writable copy
- b. Stored locally on the server
- c. Most commonly used for Active Directory

Example: You create dev.company.local for development servers

2. Secondary Zone

- a. Read-only copy of another DNS zone
- b. Gets data from a primary zone via zone transfer
- c. Used for redundancy and load balancing

Example: A second server in another office holds a copy of company.local as a secondary zone

3. Stub Zone

- a. Holds only minimal info: NS (Name Server), SOA (Start of Authority), and A records for another zone
- b. Used for faster lookups across different DNS namespaces

Example: You have sales.company.local and want your server to redirect queries there without holding full records

Reverse Lookup Zone

- Does the opposite of forward lookup
- Translates IP → name

How to Create:

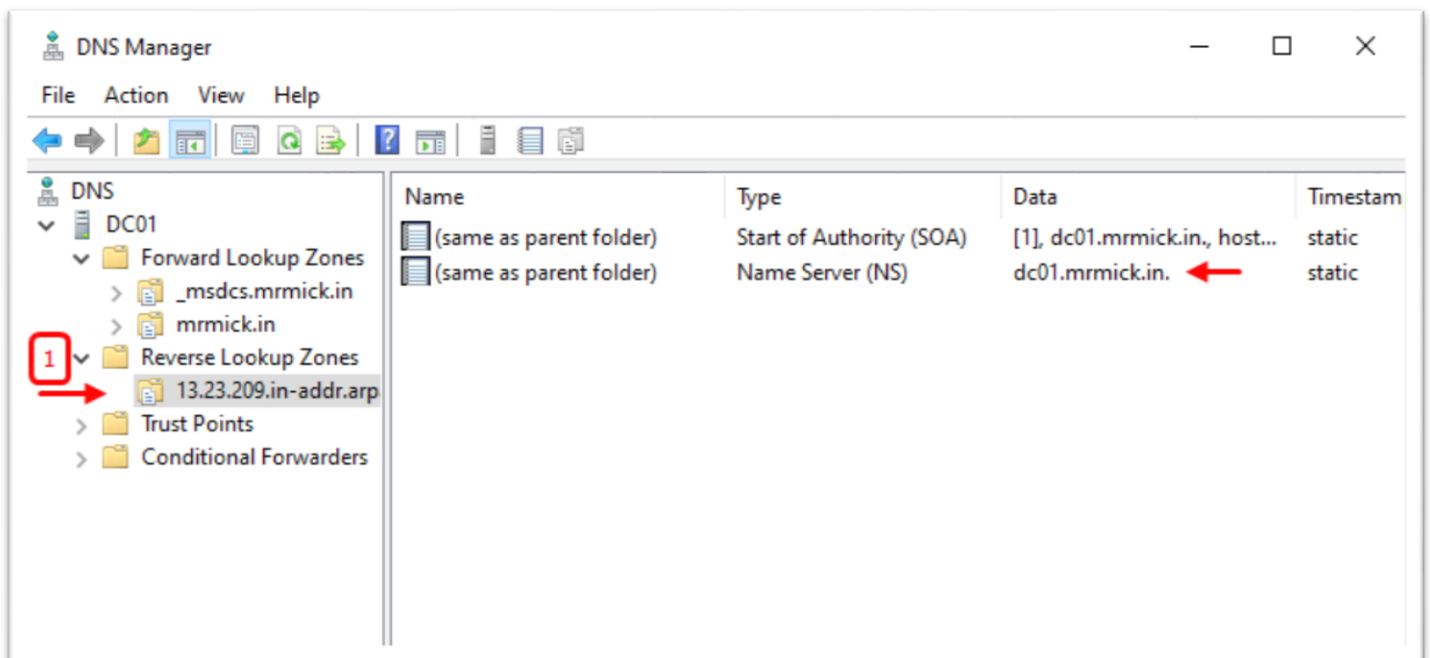
1. Right-click Reverse Lookup Zones > New Zone
2. Choose Primary Zone
3. Enter Network ID (based on subnet)
 - a. Example: If subnet is 192.168.1.0/24, enter 192.168.1
4. Now DNS can answer:
 - a. 192.168.1.10 → server01.company.local

Used in security audits, logging, and troubleshooting

Lab Scenario

Goal: Create a reverse lookup zone for your AD subnet

1. Open DNS Manager
2. Right-click Reverse Lookup Zones > New Zone
3. Choose:
 - a. Zone Type: Primary
 - b. Replication Scope: To all DNS servers in AD forest
 - c. Network ID: 192.168.1
 - d. Finish
4. Now your DNS can resolve IP → Name



08 - DHCP Installation

What is DHCP?

DHCP (Dynamic Host Configuration Protocol) automatically assigns:

- IP address
- Subnet mask
- Default gateway
- DNS server

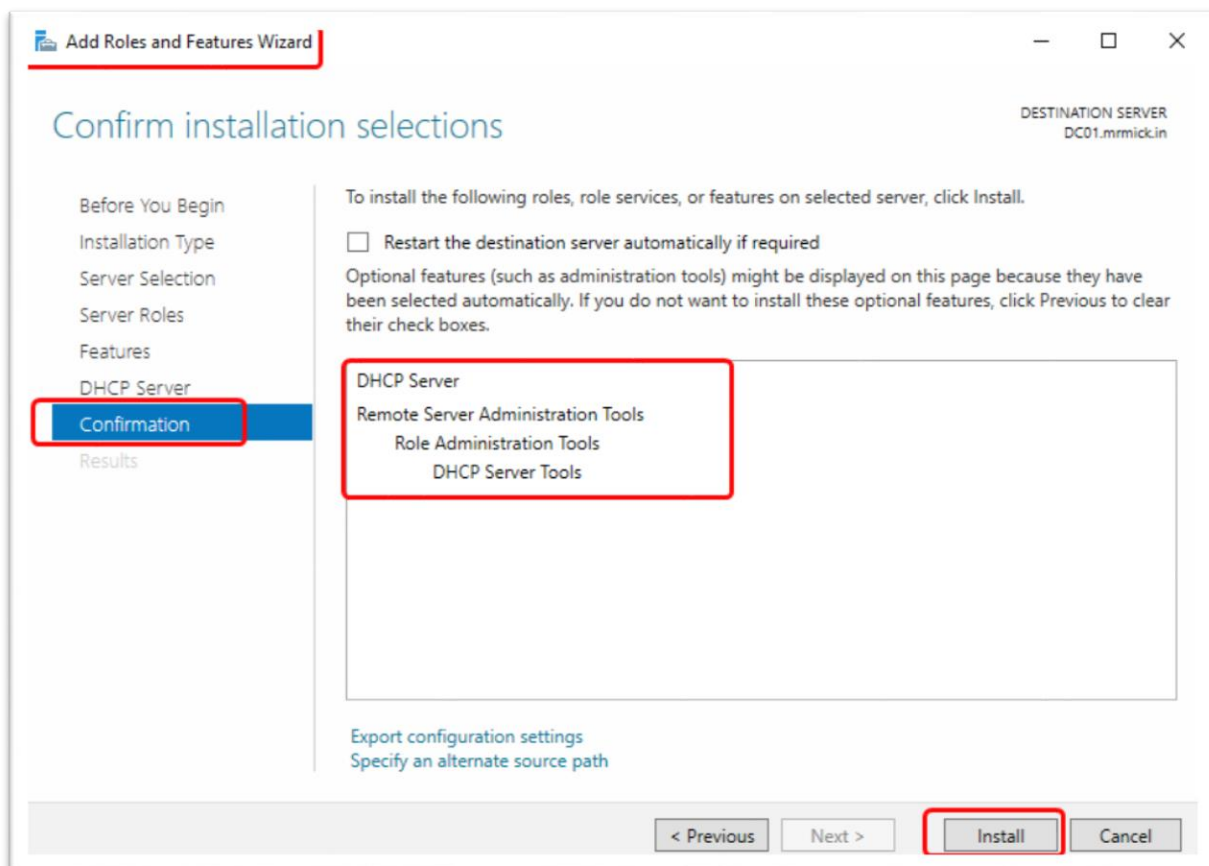
...to devices in a network.

So you don't need to set IP manually on each client PC.

Step-by-Step: DHCP in Windows Server

✓ Step 1: Install DHCP Role

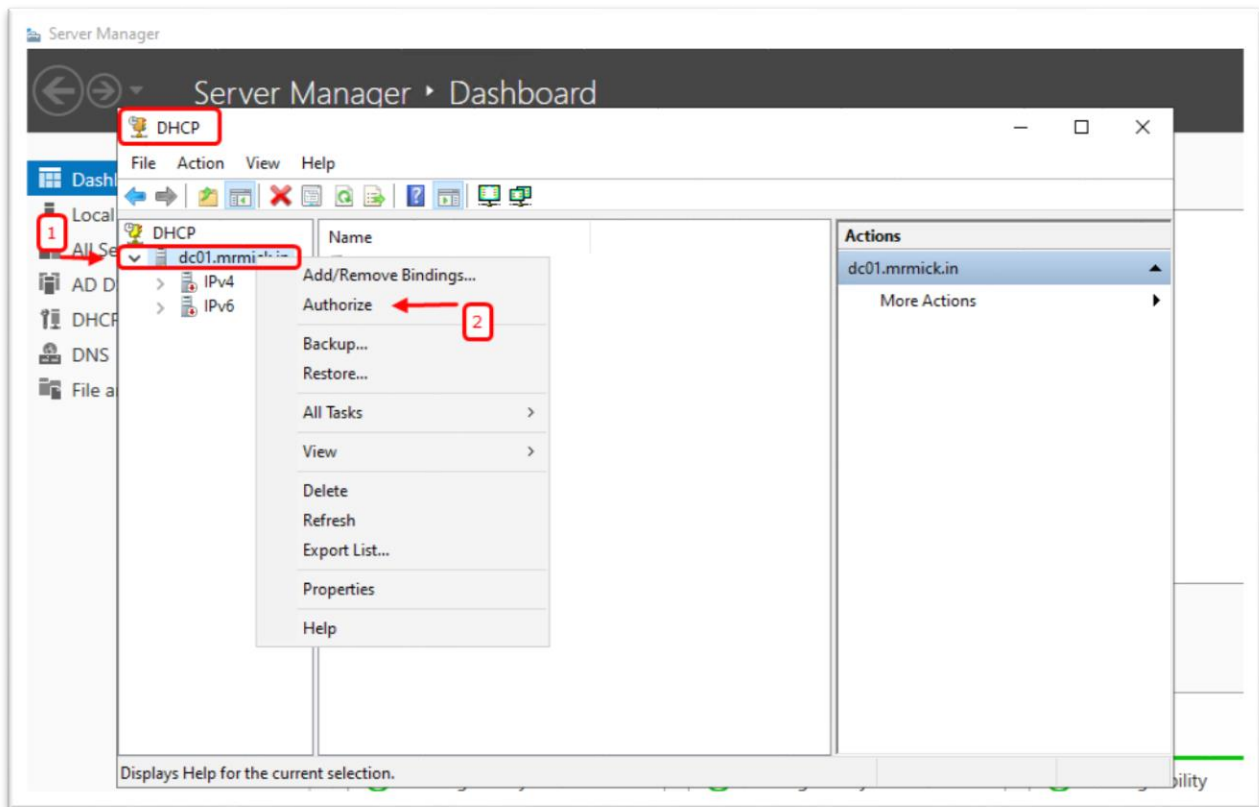
- Go to: Server Manager > Add Roles and Features
- Choose: DHCP Server
- Complete the wizard and Install
- After install, open:
 - Tools > DHCP



✓ Step 2: Authorize DHCP Server

Before the server can hand out IPs, it must be authorized in Active Directory.

- In DHCP Console, right-click your server name
- Click Authorize
- Wait a few seconds; it should show a green check mark



✓ Step 3: Create a New IPv4 Scope

- Expand: DHCP > IPv4
- Right-click IPv4 > New Scope
- Follow the wizard:

Field	Example
Scope Name	Office Network
Start IP	192.168.1.100
End IP	192.168.1.200
Subnet Mask	255.255.255.0
Lease Duration	8 days
Router (Default Gateway)	192.168.1.1
DNS Server	192.168.1.10 (your DC)

Once created, it's ready to assign IP addresses to clients.

Reservation

- ✓ Reservation is used to always assign the same IP to a specific device based on its MAC address.
- ✓ Useful for printers, servers, or any device that should always get the same IP.

How to Create:

- Right-click on the Reservations folder under your scope
- Click New Reservation
- Fill:
 - Reservation Name
 - IP Address (pick from inside the range or outside)
 - MAC Address (can be found using ipconfig /all on client)

Server Options

- Server Options are global settings (apply to all scopes on that DHCP server).

You can set:

- DNS Server IP
- Default Gateway
- Domain Name
- WINS Server (if used)

How to Configure:

- Right-click Server Options under IPv4
- Click Configure Options
- Check required options like:
 - 003 Router
 - 006 DNS Server
 - 015 DNS Domain Name

You can also set these on a per-scope basis if needed.

Important Notes

You can't have two DHCP servers active in same network unless they are in failover mode.

- Otherwise, Windows DHCP will shut down the second server to avoid IP conflicts.

Example Lab Scenario

Goal: Set up a DHCP server that assigns IPs to client PCs from 192.168.10.100–192.168.10.200.

- Install DHCP Role on Domain Controller
- Authorize DHCP
- Create scope named OfficeNetwork
- Set range: 192.168.10.100 to 192.168.10.200
- Add router: 192.168.10.1
- Add DNS: 192.168.10.10
- Create reservation for printer (MAC: A0-B1-C2-D3-E4-F5) → Assign IP: 192.168.10.150
- On client PC: Set to Obtain IP automatically
- Check IP using:
 - ipconfig /all