MCSA End-to-End Project

Project Title: Active Directory Enterprise Deployment

Microsoft Certified Solutions Associate

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)
Course: Microsoft Certified Solutions Associate
Date: 2025-09-15

Project Overview

Goal: Deploy a reliable Active Directory Domain Services (AD DS) domain with OU design, user/group provisioning, Group Policies, and advanced security hardening.

Why this matters:

- Centralized identity & scalable administration
- OU delegation for clear separation of tasks
- Consistent security baselines with Group Policy
- Modern hardening features like LAPS, fine-grained password policies, LDAP signing, and NTLM restrictions

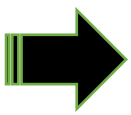
---

Module 1: Build the AD DS Domain

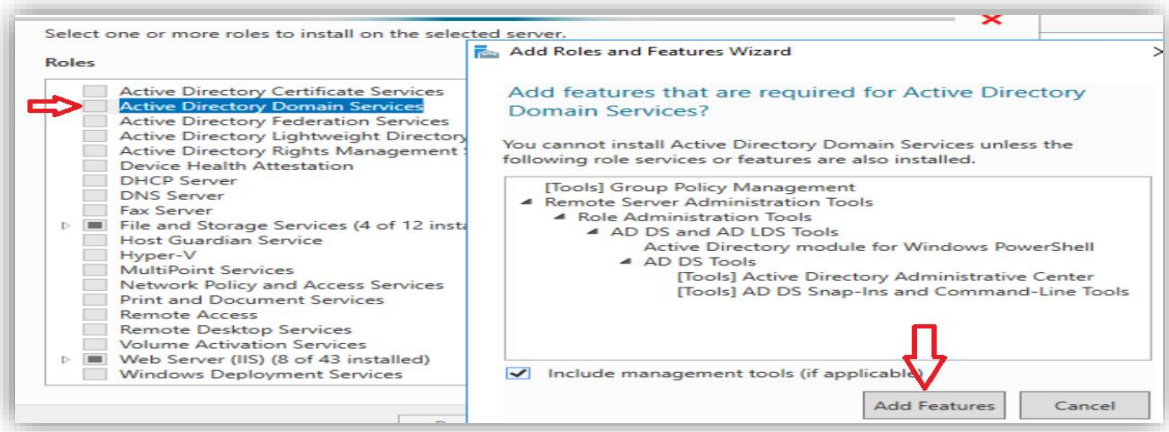
Objective: Install AD DS, create a new forest/domain, and add a secondary domain controller for resiliency.

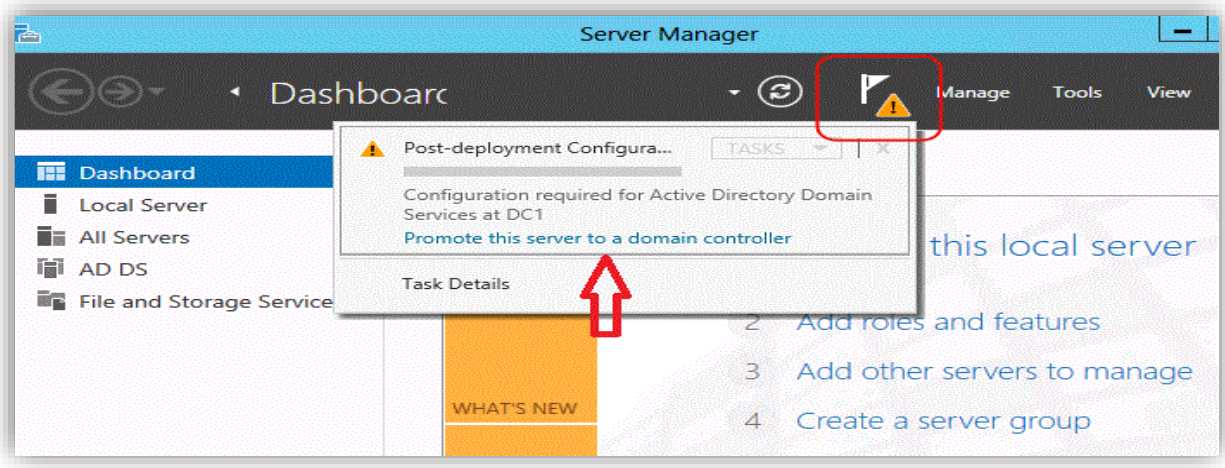
Steps (GUI):

1. **Add AD DS Role**
    - Open **Server Manager > Manage > Add Roles and Features**
    - Select **Active Directory Domain Services**
    - Complete the wizard
2. **Promote to Domain Controller**
    - In Server Manager, click **Notification > Promote this server to a domain controller**
    - Select **Add a new forest**, enter root domain (e.g., microsoft.com)

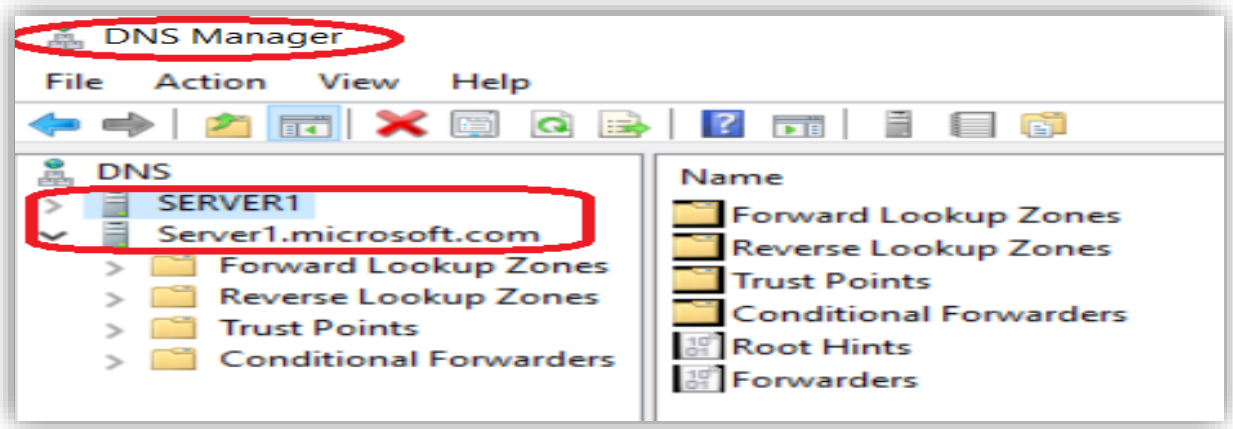


- Configure DSRM password > Finish and reboot





3. **Verify Services**
   - Log in as domain admin
   - Open **Active Directory Users and Computers (ADUC)** → confirm domain tree
   - Open **DNS Manager** → check _msdcs and domain records

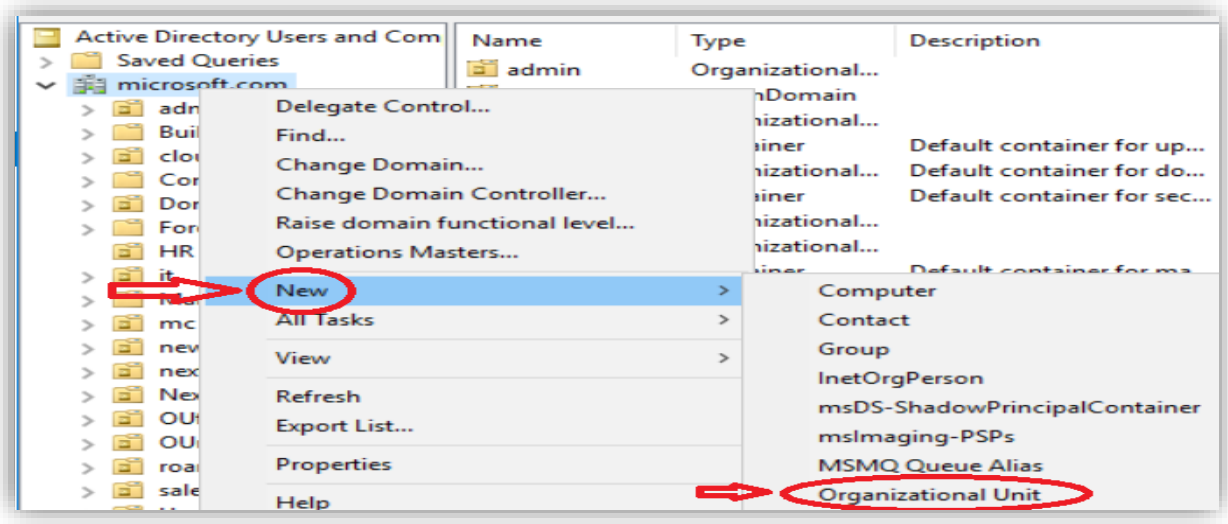


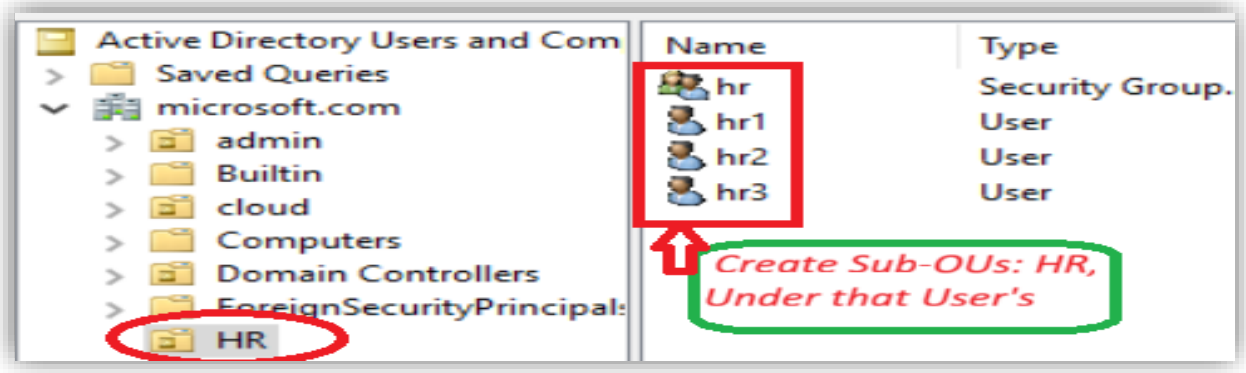
Module 2: OU Design and Creation

Objective: Create a clean OU hierarchy for delegation and Group Policy scoping.

Steps (GUI):

1. Open **ADUC > Right-click domain > New > Organizational Unit**
2. Create top-level OUs: **Servers, Workstations, Admin, Service Accounts**
3. Inside Corp, create sub-OUs: **HR, Finance, IT**
4. Redirect default “Users” and “Computers” containers into purpose-built Ous





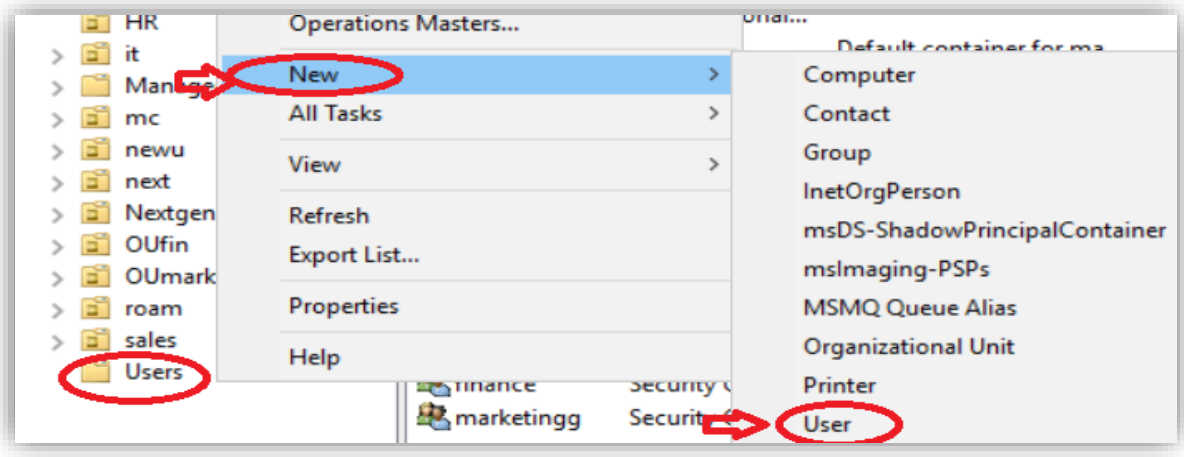
Module 3: Users, Groups, and Access Model

Objective: Provision users, create security groups, and apply AGDLP model.

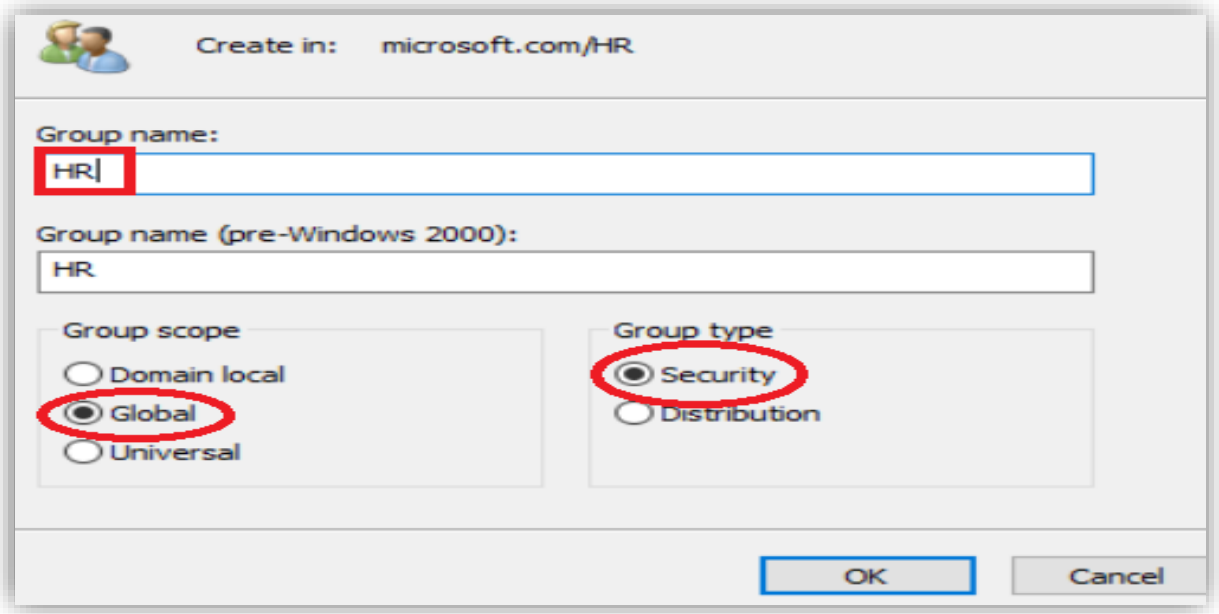
Steps (GUI):

1. **Create User**
    - In ADUC, go to **OU=HR** → Right-click → **New > User**

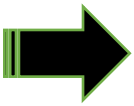
- Enter user details → Set initial password → Enable account

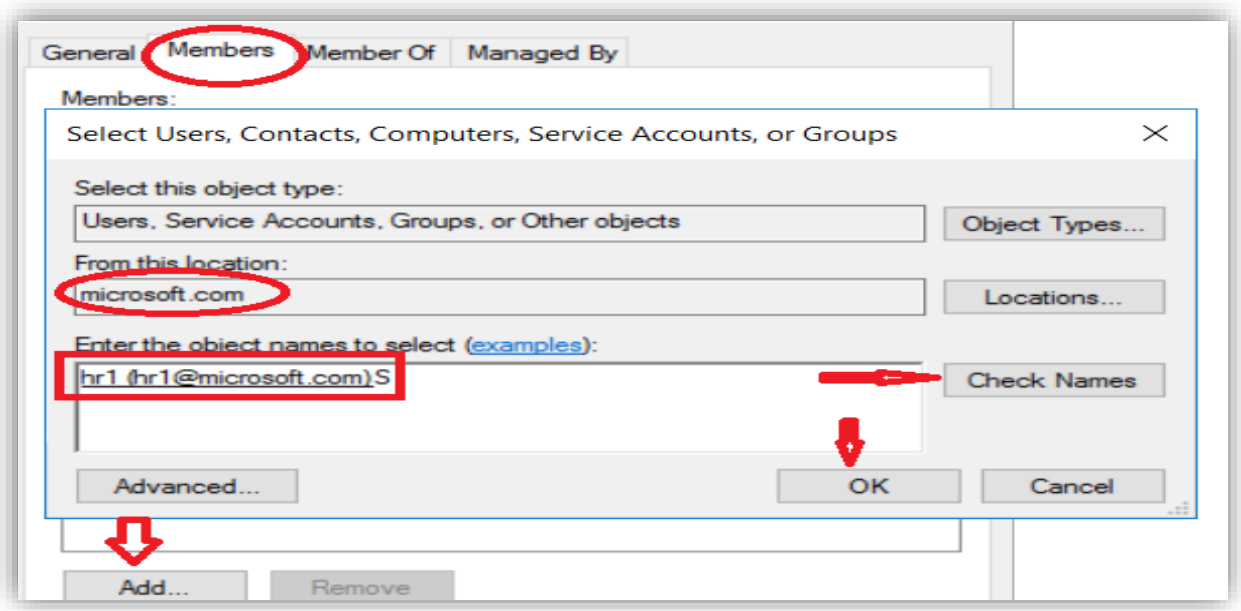


2. **Create Group**
   - In ADUC, go to **OU=Groups** → Right-click → **New > Group**
   - Choose **Global Security Group** (e.g., HR-Staff)



3. **Add Members**
   - Right-click group → **Properties > Members > Add**
   - Select HR users and apply



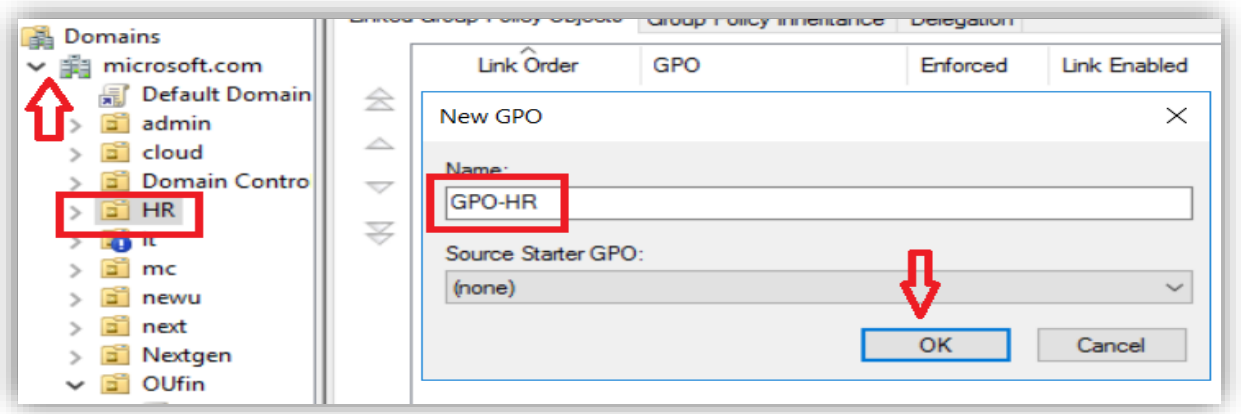


Module 4: Group Policy Strategy and Deployment

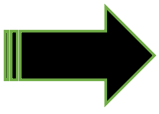
Objective: Apply baseline GPOs for workstations, servers, and domain controllers. Configure LAPS, password policies, LDAP signing, and NTLM restrictions.

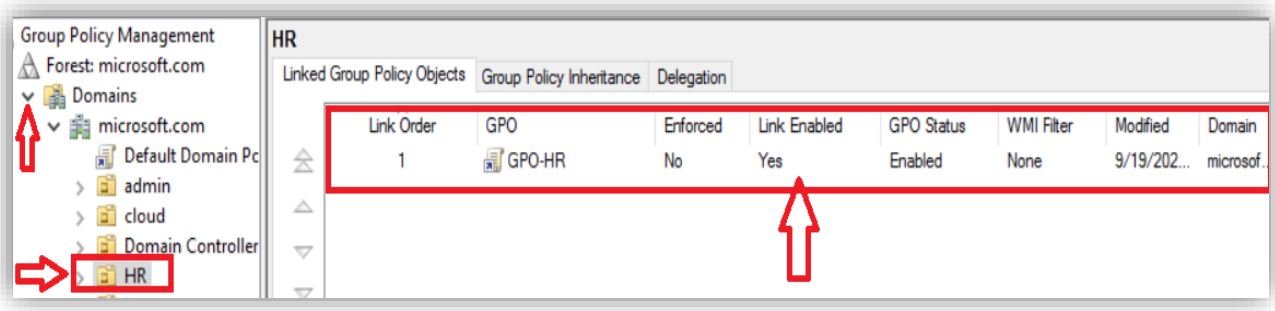
Steps (GUI):

1. **Create GPOs**
    - Open **Group Policy Management Console (GPMC)**
    - Right-click domain/OU → **Create a GPO in this domain, and Link it here**
    - Name examples: Workstation_Baseline, Server_Baseline

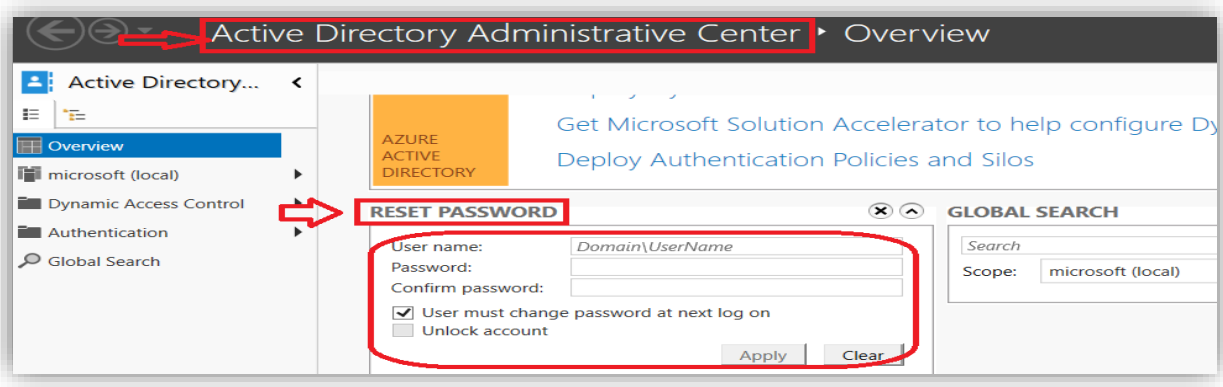


2. **Link GPOs**
    - Right-click target OU (e.g., Workstations) → **Link Existing GPO**

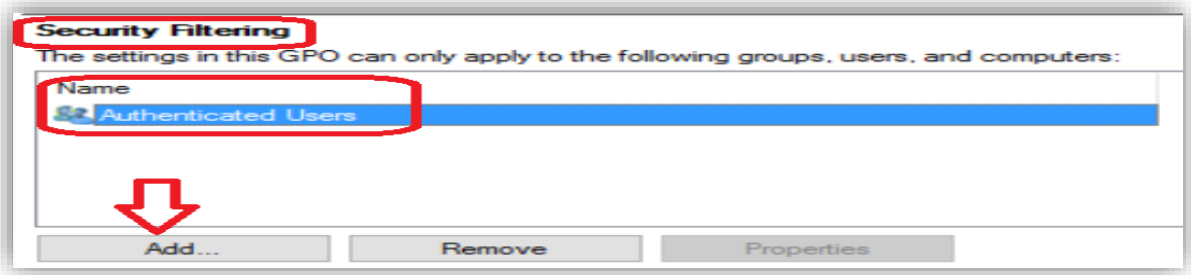




3. **Fine-Grained Password Policies**
    - Open **Active Directory Administrative Center (ADAC)**
    - Go to **Password Settings Container > New > Password Settings**
    - Apply to high-privileged groups



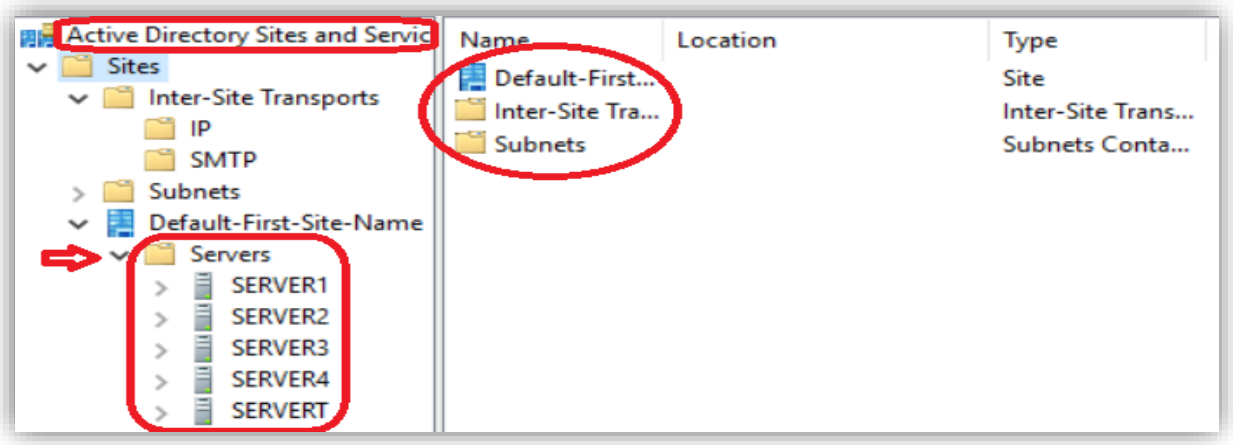
4. **LDAP Signing & NTLM Restrictions**
    - In GPMC, create GPO linked to **Domain Controllers OU**
    - Configure:
        - *Domain controller: LDAP server signing requirements = Require signing*
        - *Network security: Restrict NTLM in this domain*

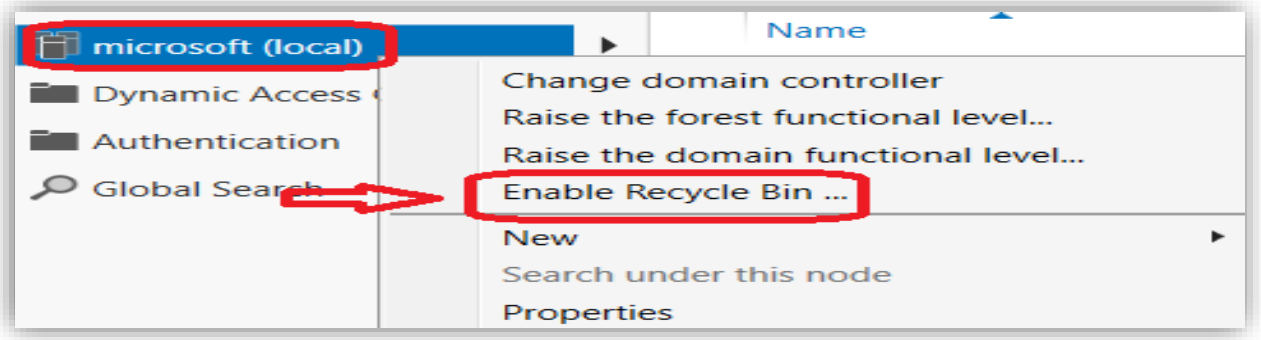


Module 5: Reliability, Security & Enhancements

Steps (GUI):

- Deploy **2+ DCs** for redundancy
- Configure **Active Directory Sites and Services** → map subnets correctly
- Enable **Active Directory Recycle Bin** in ADAC
- Maintain a **Central Store** for ADMX templates
- Apply **tiered baseline GPOs** (Domain, Workstation, Server, DCs)





Validation Checklist

✓ Domain online, sign-in verified
✓ OU structure created and visible in ADUC
✓ Users & groups provisioned, memberships assigned
✓ GPOs created, linked, and applied
✓ LAPS working (local admin passwords rotating)
✓ Fine-grained password policy active
✓ LDAP/NTLM restrictions applied successfully
✓ AD Recycle Bin enabled

Troubleshooting Guide

- **DC promotion fails:** Verify DNS configuration and credentials
- **GPO not applying:** Check link order, inheritance, security filtering, and WMI filter evaluation
- **LAPS not working:** Ensure schema extended and OU permissions configured
- **Protocol hardening breaks apps:** Start with audit mode before enforcing

---

Conclusion :

This project successfully built a **production-style Active Directory environment** with a secure, scalable, and well-structured design. By combining **OU design, Group Policies, LAPS, password tiering, and authentication hardening**, this lab mirrors real enterprise IT practices. It provides a strong baseline for administrators to manage identities, policies, and security in a modern infrastructure.

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)
Course: Microsoft Certified Solutions Associate
Date: 2025-09-15