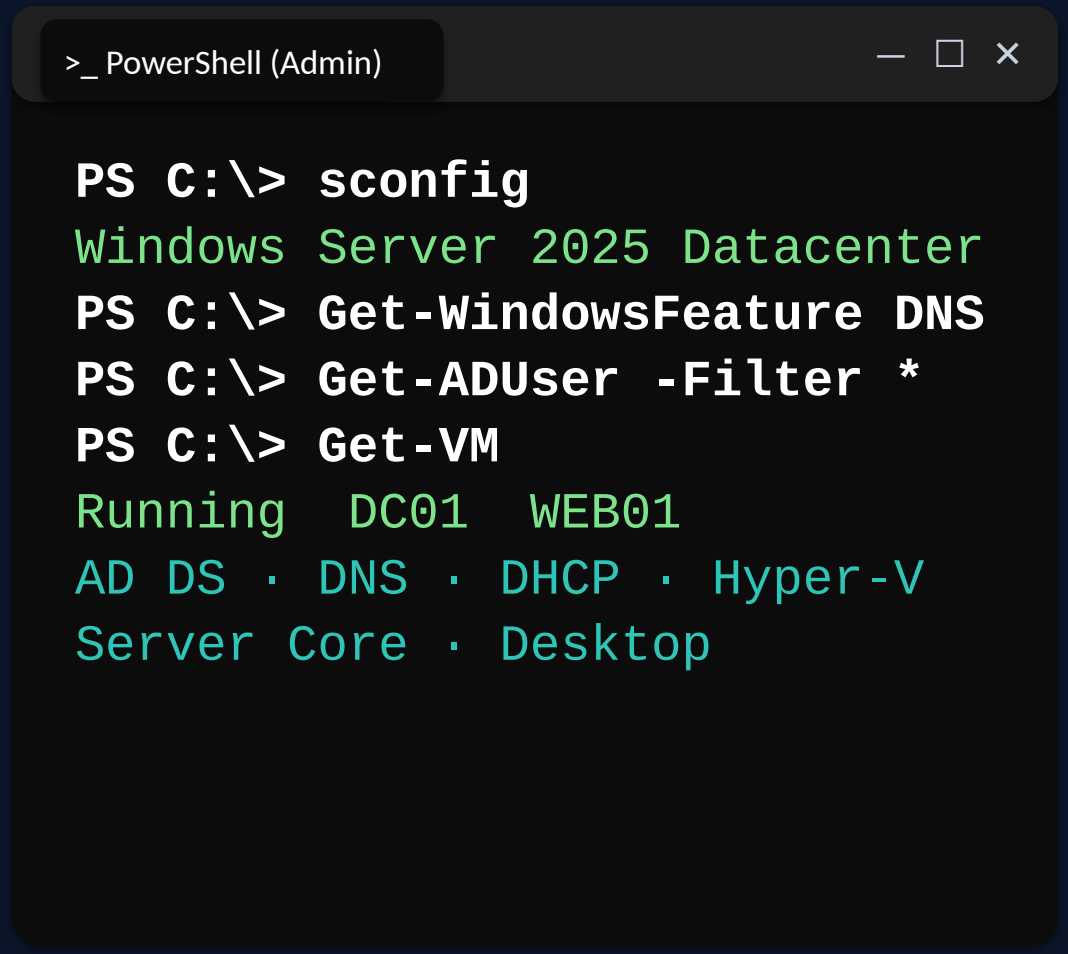


LESSON 5 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Managing Active Directory: Users, Groups, OUs & Delegation

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 5

- The AD management tools: ADUC, ADAC and the ActiveDirectory module
- Designing organizational units
- Users: create, find, change, disable, unlock and reset
- Bulk user creation from a CSV file
- Groups: scopes, types and the AGDLP strategy
- Computer accounts and stale-account cleanup
- Delegation, the AD Recycle Bin, password policies and Windows LAPS

Active Directory Management Tools

Tool	Command	Best for
AD Users and Computers	dsa.msc	Classic daily work; Delegation wizard
AD Administrative Center	dsac.exe	Recycle Bin, password policies, PowerShell history
ActiveDirectory module	Get-ADUser, New-ADUser …	Automation and bulk changes
Windows Admin Center	Browser	Quick user and group tasks
Sites and Services / Domains and Trusts	dssite.msc / domain.msc	Replication, trusts

Designing Organizational Units

OU path	Contains	Why
LAB > Staff > Teachers	Teacher user accounts	Teacher policies, delegated to the principal
LAB > Staff > Students	Student accounts	Help desk can reset passwords here
LAB > Computers > Workstations	Classroom and office PCs	Workstation GPOs, LAPS
LAB > Computers > Servers	Member servers	Server security GPOs
LAB > Groups	Security and distribution groups	Easy to find and manage
LAB > Admins	Separate admin accounts	Extra protection

Create the OU Structure

```
PS C:\> $dc = 'DC=lab,DC=mywebuniversity,DC=local'
PS C:\> New-ADOrganizationalUnit -Name LAB -Path $dc
PS C:\> 'Staff','Computers','Groups','Admins','Disabled' | ForEach-Object {
          New-ADOrganizationalUnit -Name $_ -Path "OU=LAB,$dc" }
PS C:\> 'Teachers','Students' | ForEach-Object {
          New-ADOrganizationalUnit -Name $_ -Path "OU=Staff,OU=LAB,$dc" }
PS C:\> 'Workstations','Servers' | ForEach-Object {
          New-ADOrganizationalUnit -Name $_ -Path "OU=Computers,OU=LAB,$dc" }
PS C:\> Get-ADOrganizationalUnit -Filter * | Select-Object DistinguishedName
PS C:\> redircmp "OU=Workstations,OU=Computers,OU=LAB,$dc"   # new PCs land here
```

Users: Create, Find, Change

```
PS C:\> $ou = 'OU=Teachers,OU=Staff,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'
PS C:\> New-ADUser -Name 'Maryam Ahmadi' -GivenName Maryam -Surname Ahmadi `
           -SamAccountName mahmadi -UserPrincipalName mahmadi@lab.mywebuniversity.local `
           -Department Math -Path $ou -AccountPassword (Read-Host -AsSecureString) `
           -Enabled $true -ChangePasswordAtLogon $true

PS C:\> Get-ADUser mahmadi -Properties Department, LastLogonDate, Enabled
PS C:\> Get-ADUser -Filter "Department -eq 'Math'" | Select-Object Name, SamAccountName
PS C:\> Set-ADUser mahmadi -Title 'Math Teacher' -Office 'Room 12'
```

Daily Help-Desk Tasks

```
PS C:\> Unlock-ADAccount mahmadi
PS C:\> Set-ADAccountPassword mahmadi -Reset -NewPassword (Read-Host -AsSecureString)
PS C:\> Set-ADUser mahmadi -ChangePasswordAtLogon $true
PS C:\> Disable-ADAccount mahmadi                       # someone left
PS C:\> Move-ADObject (Get-ADUser mahmadi) -TargetPath
'OU=Disabled,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'

PS C:\> Search-ADAccount -LockedOut | Select-Object Name, LastLogonDate
PS C:\> Search-ADAccount -PasswordExpired
PS C:\> Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UsersOnly
```

Bulk Users from a CSV File

```
# students.csv
# First,Last,Username,Grade
# Ahmad,Rahimi,arahimi,10
# Zahra,Karimi,zkarimi,11

PS C:\> $ou = 'OU=Students,OU=Staff,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'
PS C:\> $pw = Read-Host -AsSecureString 'Initial password'
PS C:\> Import-Csv C:\Scripts\students.csv | ForEach-Object {
          New-ADUser -Name "$($_.First) $($_.Last)" -GivenName $_.First -Surname $_.Last `
            -SamAccountName $_.Username -UserPrincipalName "$
($_.Username)@lab.mywebuniversity.local" `
            -Description "Grade $($_.Grade)" -Path $ou -AccountPassword $pw -Enabled $true `
            -ChangePasswordAtLogon $true -WhatIf }      # remove -WhatIf to create
```

Groups: Scopes, Types and AGDLP

Concept	Meaning
Security group	Used for permissions (and email if mail-enabled)
Distribution group	Email lists only — no permissions
Global	Members from its own domain; used to group people by role
Domain local	Used to grant permissions on resources in its domain
Universal	Members from any domain in the forest; multi-domain forests
AGDLP	Accounts → Global groups → Domain Local groups → Permissions

Groups with PowerShell

```
PS C:\> $g = 'OU=Groups,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'
PS C:\> New-ADGroup GG_Teachers -GroupScope Global -GroupCategory Security -Path $g
PS C:\> New-ADGroup DL_Share_Teachers_Modify -GroupScope DomainLocal -Path $g
PS C:\> Add-ADGroupMember GG_Teachers -Members mahmadi
PS C:\> Add-ADGroupMember DL_Share_Teachers_Modify -Members GG_Teachers   # AGDLP

PS C:\> Get-ADGroupMember DL_Share_Teachers_Modify -Recursive | Select-Object Name
PS C:\> Get-ADPrincipalGroupMembership mahmadi | Select-Object Name
PS C:\> Add-ADGroupMember GG_Teachers -Members (Get-ADUser -Filter * `
           -SearchBase 'OU=Teachers,OU=Staff,OU=LAB,DC=lab,DC=mywebuniversity,DC=local')
```

Delegation, Recycle Bin, Password Policies, LAPS

Feature	How
Delegate control	dsa.msc > right-click OU > Delegate Control (e.g., reset passwords in Students)
AD Recycle Bin	Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet
Restore an object	Get-ADObject -Filter … -IncludeDeletedObjects | Restore-ADObject
Fine-grained passwords	New-ADFineGrainedPasswordPolicy for admins or service accounts
Windows LAPS	Unique rotating local admin passwords, stored in AD
dMSA / gMSA	Managed service accounts: Windows rotates service passwords

Lab: Recycle Bin and Windows LAPS

```
PS C:\> Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet `
          -Target lab.mywebuniversity.local
PS C:\> Remove-ADUser arahimi -Confirm:$false                    # oops!
PS C:\> Get-ADObject -Filter "samAccountName -eq 'arahimi'" -IncludeDeletedObjects |
          Restore-ADObject                                       # restored

# Windows LAPS (built into Windows Server 2025 and Windows 11)
PS C:\> Update-LapsADSchema
PS C:\> Set-LapsADComputerSelfPermission -Identity
'OU=Workstations,OU=Computers,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'
# Turn on the LAPS policy with a GPO (Lesson 6), then:
PS C:\> Get-LapsADPassword CL01 -AsPlainText
```

Summary & Homework

- Design OUs for delegation and Group Policy
- New-ADUser, Set-ADUser, Search-ADAccount, Unlock-ADAccount
- Bulk changes: Import-Csv | ForEach-Object { … -WhatIf }
- AGDLP: accounts → global → domain local → permissions
- Homework: build the LAB OUs and import 10 students from CSV
- Homework: enable the Recycle Bin and restore a deleted user

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.