درس ۵ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

مدیریت Active Directory: کاربران، گروه‌ها، OU ها و تفویض

دوره کامل · Windows Server 2025 (build 26100)



در درس پنجم چه یاد می‌گیرید

- ابزارهای مدیریت AD: ADAC، ADUC و ماژول ActiveDirectory
- طراحی organizational unit ها
- کاربران: ساختن، پیدا کردن، تغییر، غیرفعال کردن، باز کردن قفل و ری‌سِت
- ساختن گروهی کاربران از یک فایل CSV
- گروه‌ها: محدوده‌ها، انواع و استراتژی AGDLP
- حساب‌های کمپیوتر و پاک‌سازی حساب‌های کهنه
- تفویض، AD Recycle Bin، پالیسی‌های رمز و Windows LAPS

ابزارهای مدیریت Active Directory

ابزار	فرمان	بهترین برای
AD Users and Computers	dsa.msc	کار روزانه کلاسیک؛ ویزارد Delegation
AD Administrative Center	dsac.exe	Recycle Bin، پالیسی‌های رمز، تاریخچه PowerShell
ماژول ActiveDirectory	Get-ADUser، New-ADUser ...	خودکارسازی و تغییرات گروهی
Windows Admin Center	مرورگر	کارهای سریع کاربر و گروه
Sites and Services / Domains and Trusts	dssite.msc / domain.msc	Replication، trust ها

طراحی Organizational Unit ها

چرا	شامل	مسیر OU
پالیسی‌های استادان، تفویض به مدیر مکتب	حساب‌های استادان	LAB > Staff > Teachers
پشتیبانی می‌تواند این جا رمز را ری‌سِت کند	حساب‌های محصلان	LAB > Staff > Students
GPO های ورک‌استیشن، LAPS	کمپیوترهای صنف و دفتر	LAB > Computers > Workstations
GPO های امنیتی سرور	سرورهای عضو	LAB > Computers > Servers
پیدا کردن و مدیریت آسان	گروه‌های امنیتی و توزیع	LAB > Groups
محافظت بیشتر	حساب‌های admin جداگانه	LAB > Admins

ساختن ساختار OU

```
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
```

کاربران: ساختن، پیدا کردن، تغییر

```
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'
```

کارهای روزانه پشتیبانی

```
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
```

کاربران گروهی از یک فایل CSV

```
# 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
```

گروه‌ها: محدوده‌ها، انواع و AGDLP

مفهوم	معنی
Security group	برای اجازه‌ها استفاده می‌شود (و ایمیل اگر mail-enabled باشد)
Distribution group	فقط لست ایمیل — بدون اجازه
Global	اعضا از domain خودش؛ برای گروه‌بندی افراد بر اساس نقش
Domain local	برای دادن اجازه روی منابع در domain خودش
Universal	اعضا از هر domain در forest؛ forest های چند domain
AGDLP	Accounts ← Global groups ← Domain Local groups ← Permissions

گروه‌ها با 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')
```

تفویض، Recycle Bin، پالیسی‌های رمز، LAPS

چگونه	ویژگی
dsa.msc > کلیک راست روی OU > Delegate Control (مثلاً ری‌سِت رمز در Students)	تفویض کنترل
Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet	AD Recycle Bin
Get-ADObject -Filter … -IncludeDeletedObjects | Restore-ADObject	بازیابی یک object
New-ADFineGrainedPasswordPolicy برای admin ها یا حساب‌های سرویس	رمزهای دقیق
رمزهای admin محلی منحصربه‌فرد و چرخشی، ذخیره در AD	Windows LAPS
حساب‌های سرویس مدیریت‌شده: ویندوز رمزهای سرویس را عوض می‌کند	dMSA / gMSA

لابراتوار: Recycle Bin و 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
```

خلاصه و کارخانگی

- OU ها را برای تفویض و Group Policy طراحی کنید
- New-ADUser، Set-ADUser، Search-ADAccount، Unlock-ADAccount
- تغییرات گروهی: Import-Csv | ForEach-Object { ... -WhatIf }
- AGDLP: حساب‌ها ← domain local ← global ← اجازه‌ها
- کارخانگی: OU های LAB را بسازید و ۱۰ محصل را از CSV وارد کنید
- کارخانگی: Recycle Bin را فعال کنید و یک کاربر حذف‌شده را بازیابی کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید