درس ۶ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

Group Policy در domain

دوره کامل · Windows Server 2025 (build 26100)



در درس ششم چه یاد می‌گیرید

- Group Policy Object ها: تنظیمات کمپیوتر در برابر کاربر، policy در برابر preference
- GPO ها کجا اعمال می‌شوند: site ها، OU، domain ها — و ترتیب LSDOU
- Enforced، Block Inheritance، Inheritance و security filtering
- ساختن و وصل کردن GPO ها در GPMC و PowerShell
- GPO های مفید: امنیت، drive map، آپدیت‌ها، LAPS، USB
- عیب‌یابی با gpresult و RSoP
- بکاپ‌ها، central store و بهترین روش‌ها

مفاهیم Group Policy

مفهوم	معنی
GPO	یک Group Policy Object: مجموعه‌ای نام‌دار از تنظیمات
Computer Configuration	به کمپیوترها اعمال می‌شود، هنگام شروع و هر تازه‌سازی
User Configuration	به کاربران اعمال می‌شود، هنگام ورود و هر تازه‌سازی
Policies	تنظیمات اجباری؛ کاربران نمی‌توانند تغییر دهند
Preferences	تنظیمات پیش‌فرض که کاربران می‌توانند تغییر دهند: درایوها، پرینترها، میانبرها
Administrative Templates	فایل‌های ADMX که تنظیمات مبتنی بر registry را توصیف می‌کنند
Link	یک GPO را به یک domain، site یا OU وصل می‌کند

ترتیب اجرا: LSDOU

ترتیب	سطح	مثال
۱	Local	پالیسی محلی خود کمپیوتر
۲	Site	به ندرت استفاده می‌شود؛ تنظیمات بر اساس موقعیت
۳	Domain	Default Domain Policy: رمزها، قفل شدن
۴	OU (والد ← فرزند)	LAB ← Computers ← Workstations
قانون	آخرین اعمال‌شده برنده است	تنظیم OU فرزند تنظیم domain را لغو می‌کند
استثناها	Enforced؛ Block Inheritance	Enforced از Block Inheritance قوی‌تر است

فیلتر و تازه‌سازی

چه چیزی بدانید	موضوع
یک GPO را فقط به اعضای یک گروه اعمال کنید (پیش‌فرض Authenticated Users)	Security filtering
فقط اگر یک کوئری درست باشد اعمال شود، مثلاً فقط لپ‌تاپ‌ها یا فقط Windows 11	WMI filtering
فقط preference ها: هدف قرار دادن گروه، سیستم عامل، محدوده IP و غیره	Item-level targeting
هر ۹۰ دقیقه ± ۳۰ برای اعضا؛ هر ۵ دقیقه روی DC ها	فاصله تازه‌سازی
نصب نرم‌افزار، folder redirection: فقط هنگام ری‌استارت یا ورود	بعضی تنظیمات
gpupdate /force، یا Invoke-GPUpdate از سرور	همین حالا اجرا کنید

ساختن و وصل کردن GPO ها با PowerShell

```
PS C:\> Import-Module GroupPolicy                    # gpmc.msc is the GUI
PS C:\> $ws = 'OU=Workstations,OU=Computers,OU=LAB,DC=lab,DC=mywebuniversity,DC=local'
PS C:\> New-GPO -Name 'WS - Windows Update' -Comment 'Update settings for workstations'
PS C:\> Set-GPRegistryValue -Name 'WS - Windows Update' `
           -Key 'HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' `
           -ValueName NoAutoRebootWithLoggedOnUsers -Type DWord -Value 1
PS C:\> New-GPLink -Name 'WS - Windows Update' -Target $ws

PS C:\> Get-GPInheritance -Target $ws        # which GPOs apply, in what order
PS C:\> Get-GPO -All | Select-Object DisplayName, GpoStatus, ModificationTime
```

GPO های مفید برای یک مکتب یا دفتر

GPO	کجا در ویرایشگر
رمز و قفل شدن	Default Domain Policy > Computer > Policies > Windows Settings > Security
Map کردن درایو S:	User > Preferences > Windows Settings > Drive Maps (هدف: یک گروه)
مسدود کردن USB	Computer > Admin Templates > System > Removable Storage Access
Windows Update	Computer > Admin Templates > Windows Components > Windows Update
Windows LAPS	Computer > Admin Templates > System > LAPS
Defender، فایروال، BitLocker	Computer > Admin Templates > Windows Components / Windows Settings > Security

لابراتوار: Central Store، پالیسی LAPS و یک Drive Map

```
# 1. Central store: one shared copy of the ADMX templates in SYSVOL
PS C:\> Copy-Item C:\Windows\PolicyDefinitions `
          \\lab.mywebuniversity.local\SYSVOL\lab.mywebuniversity.local\Policies\ -Recurse

# 2. New GPO 'WS - LAPS' linked to Workstations, then in gpmc.msc edit:
#    Computer > Policies > Admin Templates > System > LAPS >
#    'Configure password backup directory' = Enabled: Active Directory

# 3. New GPO 'USR - Teachers Drive' linked to Staff OU:
#    User > Preferences > Windows Settings > Drive Maps > New > S: \\SRV01\Teachers
#    Common tab > Item-level targeting > Security Group = LAB\GG_Teachers
PS C:\> Invoke-GPUpdate -Computer CL01 -Force
```

عیب‌یابی Group Policy

```
C:\> gpresult /r                                        # summary: applied and filtered GPOs
C:\> gpresult /h C:\Reports\gp-CL01.html /f              # full HTML report (admin)
C:\> gpupdate /force

PS C:\> Get-GPResultantSetOfPolicy -Computer CL01 -User LAB\mahmadi `
           -ReportType Html -Path C:\Reports\rsop.html
PS C:\> Get-WinEvent -LogName 'Microsoft-Windows-GroupPolicy/Operational' -MaxEvents 20

# Checklist: Is the GPO linked? Enabled? Right OU? Security filter? WMI filter?
#            Computer vs User half? Replicated to all DCs? Needs a restart?
```

بکاپ، گزارش و بازیابی GPO ها

```
PS C:\> New-Item C:\GPOBackups -ItemType Directory
PS C:\> Backup-GPO -All -Path C:\GPOBackups
PS C:\> Get-GPOReport -All -ReportType Html -Path C:\Reports\all-gpos.html

PS C:\> Restore-GPO -Name 'WS - Windows Update' -Path C:\GPOBackups
PS C:\> Copy-GPO -SourceName 'WS - Windows Update' -TargetName 'TEST - Windows Update'

PS C:\> Get-GPO -All | Where-Object {                    # GPOs with no links
            -not ([xml](Get-GPOReport -Guid $_.Id -ReportType Xml)).GPO.LinksTo } |
            Select-Object DisplayName
```

بهترین روش‌های Group Policy

- Default Domain Policy را فقط برای رمزها و قفل شدن بگذارید
- یک هدف برای هر GPO، با نام‌های واضح: 'SRV - ...'، 'USR - ...'، 'WS - ...'
- هر وقت ممکن است به OU ها وصل کنید، نه به domain
- اول روی یک OU آزمایشی امتحان کنید، بعد به محیط واقعی وصل کنید
- از Block Inheritance و Enforced اجتناب کنید مگر اینکه مجبور باشید
- هفتگی بکاپ بگیرید؛ از خط پایه‌های امنیتی Microsoft شروع کنید

خلاصه و کارخانگی

- GPO = نیمه کمپیوتر + نیمه کاربر؛ policy اجبار می‌کند، preference پیشنهاد می‌دهد
- LSDOU: آخرین اعمال‌شده برنده است؛ Enforced و Block Inheritance استثنا هستند
- New-GPO، Set-GPRegistryValue، New-GPLink، Get-GPInheritance
- عیب‌یابی با gpresult /r، /h و لاگ GroupPolicy
- کارخانگی: GPO، central store برای LAPS و drive map درایو S: را بسازید
- کارخانگی: از همه GPO ها بکاپ بگیرید و یک گزارش HTML بسازید

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