دوره کامل · ۱۲ درس

Windows Server 2025

Install · AD · Hyper-V · Admin

Active Directory، Group Policy، DNS، DHCP، Hyper-V، IIS و Azure Arc

دوره کامل · Windows Server 2025 (build 26100)



درس ۱ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

Windows Server 2025: نسخه‌ها، لایسنس، دوره پشتیبانی و لابراتوار

دوره کامل · Windows Server 2025 (build 26100)



در درس اول چه یاد می‌گیرید

- یک سرور چه کار می‌کند، و تاریخچه کوتاه Windows Server
- دوره پشتیبانی: 2025 در برابر 2022، 2019 و 2016
- چه چیزی در Windows Server 2025 جدید است
- نسخه‌ها: Essentials، Datacenter: Azure Edition، Datacenter، Standard
- اصول لایسنس: core ها، CAL ها و پرداخت ماهانه
- نیازمندی‌های سخت‌افزاری؛ Server Core در برابر Desktop Experience
- لابراتوار دوره: سه ماشین مجازی روی Hyper-V

یک Windows Server چه کار می‌کند؟

درس	چه چیزی فراهم می‌کند	نقش
۴ تا ۶	ورود مرکزی، کاربران، گروه‌ها، کمپیوترها	Active Directory (AD DS)
۷	نام‌ها و آدرس‌های IP برای شبکه	DNS و DHCP
۸	فولدرهای مشترک، اجازه‌ها، سهمیه‌ها، DFS	File server
۹	ماشین‌های مجازی	میزبان Hyper-V
۱۰	وب‌سایت‌ها و برنامه‌های وب	سرور وب (IIS)
۱۰	دسکتاپ‌ها و برنامه‌ها برای کاربران زیاد	Remote Desktop Services
۱۱ و ۱۲	آپدیت‌ها، محافظت، سلامت	WSUS / بکاپ / نظارت

تاریخچه کوتاه Windows Server

۱۹۹۳	Windows NT 3.1 Advanced Server
۲۰۰۰	Windows 2000 Server: Active Directory می‌آید
۲۰۰۸	Server Core و Hyper-V
R2 2012	Storage Spaces، PowerShell در همه جا، آماده ابر
۲۰۱۶	کانتینرها، Nano Server، Shielded VM ها
۲۰۱۹	Windows Admin Center، ترکیب با Azure
۲۰۲۲	Secured-core server، TLS 1.3 به طور پیش‌فرض
۲۰۲۵	Hotpatch، بهبودهای AD، تقسیم GPU

دوره پشتیبانی (Long-Term Servicing Channel)

نسخه	پایان پشتیبانی اصلی	پایان پشتیبانی تمدیدی
Windows Server 2025	۱۳ نوامبر ۲۰۲۹	۱۴ نوامبر ۲۰۳۴
Windows Server 2022	پایان یافت ۱۳ اکتوبر ۲۰۲۶	۱۴ اکتوبر ۲۰۳۱
Windows Server 2019	پایان یافت جنوری ۲۰۲۴	جنوری ۲۰۲۹
Windows Server 2016	پایان یافت جنوری ۲۰۲۲	جنوری ۲۰۲۷ (بعد فقط ESU پولی)
پشتیبانی اصلی	اصلاحات امنیتی و غیرامنیتی، ویژگی‌ها	
پشتیبانی تمدیدی	فقط آپدیت‌های امنیتی	

چه چیزی در Windows Server 2025 جدید است

نکات برجسته	بخش
Hotpatch: آپدیت‌های امنیتی بدون ری‌استارت (Azure Arc)	آپدیت‌ها
ارتقای در جا از 2012 R2 و بعد؛ همچنین از طریق Windows Update	ارتقا
سطح عملکرد جدید، صفحه‌های اختیاری 32k دیتابیس، امنیت قوی‌تر LDAP	Active Directory
(dMSA) Delegated Managed Service Accounts	حساب‌ها
SMB over QUIC در همه نسخه‌ها؛ SMB signing به طور پیش‌فرض لازم	فایل‌ها
تقسیم GPU، VM های بزرگ‌تر، ذخیره‌سازی سریع‌تر NVMe	Hyper-V و ذخیره‌سازی

مقایسه نسخه‌ها

نسخه	بهترین برای	نکات کلیدی
Standard	سرورهای فزیکی یا کم‌مجازی	حق ۲ VM برای هر میزبان کاملاً لایسنس‌شده
Datacenter	دیتاسنترهای پرمجازی	VM نامحدود؛ SDN، Storage Spaces Direct
Datacenter: Azure Edition	Azure و Azure Local	ویژگی‌های ابری مانند hotpatch در Azure
Essentials	کسب و کارهای کوچک (از سازندگان کمپیوتر)	تا ۲۵ کاربر ۵۰ / دستگاه؛ سرورهای کوچک

اصول لایسنس

چه چیزی بدانید	مفهوم
core های فزیکی را لایسنس کنید: حداقل ۸ برای هر پروسسور، ۱۶ برای هر سرور	بر اساس core
هر کاربر یا دستگاهی که از سرور استفاده می‌کند یک Client Access License لازم دارد	CAL ها
لایسنس اضافی برای کاربران Remote Desktop Services	RDS CAL ها
Standard: ۲ VM برای هر میزبان لایسنس‌شده؛ Datacenter: نامحدود	مجازی‌سازی
پرداخت ماهانه از طریق Azure Arc به جای خرید لایسنس	پرداخت ماهانه
ISO آزمایشی رایگان ۱۸۰ روزه برای یادگیری و آزمایش	آزمایشی

نیازمندی‌های سخت‌افزاری (حداقل)

مورد	حداقل	توصیه برای لابراتوار
پروسسور	۱٫۴ گیگاهرتز ۶۴ بیتی، SSE4.2 و POPCNT	۲ CPU مجازی یا بیشتر
حافظه	۵۱۲ مگابایت (Server Core)، ۲ گیگابایت (Desktop Experience)	۴ گیگابایت برای هر VM
ذخیره‌سازی	۳۲ گیگابایت	۶۰ تا ۸۰ گیگابایت برای هر VM
شبکه	کارت Ethernet گیگابیتی	یک switch داخلی لابراتوار
Firmware	UEFI؛ TPM 2.0 و Secure Boot برای ویژگی‌های امنیتی	VM های Generation 2

Server Core در برابر Desktop Experience

Desktop Experience	Server Core	
دسکتاپ کامل، Server Manager	خط فرمان، sconfig، PowerShell	**رابط**
بزرگ‌تر	کوچک‌تر، آپدیت و ری‌استارت کمتر	**اندازه و آپدیت‌ها**
بزرگ‌تر	کوچک‌تر — امن‌تر	**سطح حمله**
محلی یا از راه دور	از راه دور: Windows Admin Center، RSAT، PowerShell	**مدیریت با**
یادگیری، برنامه‌هایی که GUI لازم دارند	Domain controller ها، DNS، Hyper-V، file server	**انتخاب برای**
نه	نه — هنگام نصب انتخاب کنید	**بعداً عوض شود؟**

لابراتوار دوره شما

VM	سیستم عامل	نقش در دوره
DC01	Windows Server 2025، Server Core	Domain controller، DNS، DHCP
SRV01	Windows Server 2025، Desktop Experience	File server، IIS، WSUS، ابزارهای مدیریت
CL01	Windows 11 Pro یا Enterprise (آزمایشی)	کلاینت domain برای آزمایش
میزبان	Windows 11 Pro/Enterprise یا Windows Server با Hyper-V	۱۶ گیگابایت RAM یا بیشتر توصیه می‌شود
شبکه	switch داخلی 'LabNet'، 10.0.0.0/24	Domain: lab.mywebuniversity.local

لابراتوار: ساختن شبکه و VM ها با PowerShell

```
# On the Hyper-V host, PowerShell as Administrator
PS C:\> New-VMSwitch -Name LabNet -SwitchType Internal
PS C:\> $iso = 'C:\ISO\WindowsServer2025_Eval.iso'          # your downloaded file
PS C:\> foreach ($n in 'DC01','SRV01') {
          New-VM -Name $n -Generation 2 -MemoryStartupBytes 4GB -SwitchName LabNet `
                 -NewVHDPath "C:\VMs\$n.vhdx" -NewVHDSizeBytes 80GB
          Set-VMProcessor $n -Count 2
          Add-VMDvdDrive $n -Path $iso
          Set-VMFirmware $n -FirstBootDevice (Get-VMDvdDrive $n) }
PS C:\> Get-VM
```

ISO آزمایشی ۱۸۰ روزه را از Microsoft Evaluation Center دانلود کنید؛ نام فایل شما فرق دارد.

خلاصه و کارخانگی

- Windows Server 2025: منتشرشده ۱ نوامبر ۲۰۲۴؛ پشتیبانی تا ۱۴ نوامبر ۲۰۳۴
- Standard (۲ VM) در برابر Datacenter (VM نامحدود)؛ Essentials برای کسب و کار کوچک
- لایسنس: core ها + CAL ها؛ نسخه آزمایشی رایگان ۱۸۰ روزه برای یادگیری
- Server Core برای بیشتر نقش‌های زیربنایی؛ Desktop Experience برای یادگیری
- کارخانگی: ISO آزمایشی و یک نسخه آزمایشی Windows 11 را دانلود کنید
- کارخانگی: DC01، LabNet و SRV01 را در Hyper-V 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

درس ۲ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

نصب و تنظیمات اولیه: Desktop Experience و Server Core

دوره کامل · Windows Server 2025 (build 26100)



در درس دوم چه یاد می‌گیرید

- نصب Windows Server 2025 قدم به قدم
- Server Core: منوی sconfig
- تنظیم اولیه با PowerShell: نام، DNS ،IP، منطقه زمانی
- آپدیت‌ها، فعال‌سازی و تبدیل نسخه آزمایشی
- ارتقای در جای سرورهای قدیمی
- زندگی با Server Core: چه چیزی هست (و نیست)
- لابراتوار: تنظیم DC01 و SRV01 روی شبکه LabNet

نصب Windows Server، قدم به قدم

چه کار می‌کنید	قدم
از ISO یا USB (VM نسل ۲: اول DVD)	۱. بوت
زبان، زمان و کیبورد، بعد 'Install Windows Server'	۲. زبان
Standard یا Datacenter — با یا بدون 'Desktop Experience'	۳. نسخه
شرایط را قبول کنید؛ نسخه آزمایشی کلید لازم ندارد	۴. لایسنس
دیسک را انتخاب کنید؛ Setup پارتیشن‌ها را می‌سازد	۵. دیسک
یک رمز قوی برای Administrator محلی تنظیم کنید	۶. رمز

Server Core: منوی sconfig

```
===============================================================
            Welcome to Windows Server 2025 Datacenter
===============================================================
 1) Domain/workgroup:                Workgroup: WORKGROUP
 2) Computer name:                   WIN-8K2L0A1B2C3
 3) Add local administrator
 4) Remote management:               Enabled
 6) Update setting:                  Download only
 7) Install updates
 8) Remote desktop:                  Disabled
 9) Network settings
10) Date and time
13) Restart          14) Shut down          15) Exit to PowerShell
```

تنظیم اولیه با PowerShell

```
PS C:\> Get-NetAdapter                                  # note the adapter name
PS C:\> New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.10 -PrefixLength 24
PS C:\> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.0.0.10
PS C:\> Set-TimeZone -Id 'Pacific Standard Time'        # Get-TimeZone -ListAvailable
PS C:\> Rename-Computer -NewName DC01 -Restart

PS C:\> Get-ComputerInfo -Property CsName, WindowsProductName, OsBuildNumber
CsName WindowsProductName                    OsBuildNumber
DC01   Windows Server 2025 Datacenter Evaluation 26100
```

چک‌لست تنظیم اولیه

چرا مهم است	مورد
DC01، FS01، WEB01 — هرگز نام تصادفی WIN-xxxx	نام معنی‌دار
کلاینت‌ها و سرورهای دیگر باید همیشه آن را پیدا کنند	IP ثابت + DNS درست
اگر ساعت‌ها بیشتر از ۵ دقیقه فرق کنند Kerberos ناکام می‌شود	منطقه زمانی و هماهنگی زمان
قبل از رفتن به محیط واقعی	همه آپدیت‌ها نصب‌شده
نسخه آزمایشی بعد از ۱۸۰ روز منقضی می‌شود	فعال‌سازی
بدون نشستن کنار کنسول آن را مدیریت کنید	مدیریت از راه دور + فایروال
نام، IP، نقش‌ها، مسئول، هدف	مستند کنید

آپدیت‌ها، فعال‌سازی و تبدیل نسخه آزمایشی

```
# Updates: sconfig option 6 (setting) and 7 (install), or Settings > Windows Update (Desktop)
PS C:\> Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 3

C:\> slmgr /dlv                         # license status, evaluation days left
C:\> slmgr /ipk <your-product-key>      # install a key
C:\> slmgr /ato                         # activate

# Convert evaluation to a licensed edition (keeps your data):
C:\> DISM /Online /Get-CurrentEdition
C:\> DISM /Online /Get-TargetEditions
C:\> DISM /Online /Set-Edition:ServerStandard /ProductKey:<key> /AcceptEula
```

ارتقای سرورهای قدیمی

نکات	مسیر
ارتقای در جا: تا چهار نسخه یک‌جا	2012 ← 2016، 2019، 2022، R2 2025
پیشنهاد ارتقا برای سرورهای واجد شرایط و مدیریت‌شده	از طریق Windows Update
ISO را mount کنید، setup.exe را اجرا کنید، 'Keep files, settings and apps' را انتخاب کنید	از طریق setup.exe
بهترین روش: یک DC جدید 2025 اضافه کنید، نقش‌ها را منتقل کنید، قدیمی را بازنشسته کنید	Domain controller ها
بکاپ کامل، بررسی پشتیبانی برنامه‌ها، آزمایش در لابراتوار، پلان برگشت	قبل از هر ارتقا
ارتقا همان نوع نصب را نگه می‌دارد	Core در برابر Desktop

زندگی با Server Core

ندارید	هنوز دارید
منوی Start، File Explorer، پنجره Server Manager	PowerShell، cmd، sconfig
بیشتر کنسول‌های msc. به صورت محلی (از راه دور استفاده کنید)	notepad، regedit، taskmgr، msinfo32
مرورگر	سرور OpenSSH (از قبل نصب‌شده)
یک دسکتاپ برای کلیک کردن	ابزارهای از راه دور: Windows Admin Center، RSAT
— mmc، File Explorer و ابزارهای بیشتر را اضافه می‌کند	App Compatibility FOD (اختیاری)

فرمان‌های مفید Server Core

```
PS C:\> sconfig                                      # back to the menu
PS C:\> Get-WindowsFeature | Where-Object Installed   # roles and features present
PS C:\> Get-NetIPConfiguration
PS C:\> Get-Service sshd ; Start-Service sshd ; Set-Service sshd -StartupType Automatic
PS C:\> Enable-NetFirewallRule -DisplayGroup 'Remote Event Log Management'
PS C:\> taskmgr ; notepad C:\Windows\System32\drivers\etc\hosts
PS C:\> Restart-Computer ; Stop-Computer
PS C:\> logoff
```

لابراتوار: تنظیم DC01 (Core) و SRV01 (Desktop)

```
# DC01 — install Datacenter (or Standard) WITHOUT Desktop Experience, then:
PS C:\> New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.10 -PrefixLength 24
PS C:\> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 127.0.0.1
PS C:\> Set-TimeZone -Id 'Pacific Standard Time' ; Rename-Computer DC01 -Restart

# SRV01 — install WITH Desktop Experience, then:
PS C:\> New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.20 -PrefixLength 24
PS C:\> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.0.0.10
PS C:\> Rename-Computer SRV01 -Restart
PS C:\> Test-Connection 10.0.0.10 -Count 2          # can SRV01 reach DC01?
```

از منطقه زمانی خودتان استفاده کنید؛ DNS سرور DC01 به خودش اشاره می‌کند چون در درس ۴ سرور DNS می‌شود.

خلاصه و کارخانگی

- نسخه و نوع نصب را با دقت انتخاب کنید — بعداً نمی‌توانید عوض کنید
- sconfig یا PowerShell: نام، IP ثابت، DNS، منطقه زمانی، آپدیت‌ها
- slmgr /dlv برای وضعیت لایسنس؛ DISM /Set-Edition نسخه آزمایشی را تبدیل می‌کند
- ارتقای در جا از 2012 R2 به بعد؛ DC های جدید به جای ارتقای قدیمی‌ها
- کارخانگی: DC01 (Core) و SRV01 (Desktop) را نصب و تنظیم کنید
- کارخانگی: قدم‌های تنظیم اولیه خود را به صورت یک اسکریپت ps1. بنویسید

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

درس ۳ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

Server Manager، Windows PowerShell و Admin Center Remoting

دوره کامل · Windows Server 2025 (build 26100)



در درس سوم چه یاد می‌گیرید

- جعبه ابزار مدیریت: محلی، از راه دور، گرافیکی و خط فرمان
- Server Manager: داشبورد، گروه‌های سرور، نقش‌ها و ویژگی‌ها
- نصب نقش‌ها و ویژگی‌ها با PowerShell
- Windows Admin Center: مدیریت از طریق مرورگر
- RSAT: ابزارهای سرور روی ورک‌استیشن Windows 11 شما
- PowerShell Remoting: session، Invoke-Command، Enter-PSSession ها
- Remoting در لابراتوار workgroup، remoting با SSH و روش‌های امن

جعبه ابزار مدیریت

ابزار	نوع	بهترین برای
Server Manager	GUI، در Desktop Experience	نقش‌ها، ویژگی‌ها، مدیریت چند سرور
Windows Admin Center	از طریق مرورگر، رایگان	Server Core و مدیریت مدرن از راه دور
RSAT (روی Windows 11)	کنسول‌های MMC + ماژول‌های PowerShell	AD، DNS، DHCP، GPO از ورک‌استیشن شما
PowerShell Remoting	خط فرمان، WinRM	خودکارسازی، سرورهای زیاد همزمان
OpenSSH	خط فرمان، SSH	مدیران چندپلتفرمی، عادت‌های لینوکس
Remote Desktop	جلسه دسکتاپ کامل	وقتی واقعاً GUI لازم دارید

گردشی در Server Manager

چه کار می‌کند	بخش
کاشی‌های سلامت: رویدادها، سرویس‌ها، کارایی، بهترین روش‌ها	Dashboard
نام، IP، آپدیت‌ها، فایروال، Remote Desktop، منطقه زمانی	Local Server
هر سروری که اضافه کردید؛ برای مدیریت کلیک راست کنید	All Servers
DC01 و سرورهای دیگر را برای مدیریت از راه دور اضافه کنید	Manage > Add Servers
ویزارد نصب	Manage > Add Roles and Features
هر کنسول: AD، DNS، DHCP، Hyper-V، IIS، Event Viewer	منوی Tools

نقش‌ها و ویژگی‌ها با PowerShell

```
PS C:\> Get-WindowsFeature | Where-Object Installed | Select-Object Name, DisplayName
PS C:\> Get-WindowsFeature *web*                          # search by name

PS C:\> Install-WindowsFeature Web-Server -IncludeManagementTools -WhatIf
PS C:\> Install-WindowsFeature Web-Server -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
True    No             Success   {Web Server (IIS), ...}

PS C:\> Install-WindowsFeature DHCP -ComputerName DC01 -IncludeManagementTools  # remote!
PS C:\> Uninstall-WindowsFeature Web-Server -Remove        # also delete the payload
```

Windows Admin Center

موضوع	چه چیزی بدانید
چیست	مدیریت رایگان از طریق مرورگر برای Windows Server و Windows 11
نصب	روی یک Windows Server (gateway) یا ورک‌استیشن Windows 11 شما
اتصال	https://<gateway> — سرورها را با نام اضافه کنید؛ از credential شما استفاده می‌کند
ابزارها	Overview، Files، Events، Services، Updates، Firewall، Certificates، PowerShell
نقش‌ها	Hyper-V، Storage، Active Directory، DNS، DHCP و غیره با extension ها
Azure	اتصال به Azure Monitor، Azure Backup، Azure Arc

RSAT روی Windows 11

```
# Windows 11: Settings > System > Optional features > View features > search 'RSAT'
PS C:\> Get-WindowsCapability -Online -Name RSAT* |
          Select-Object Name, State
PS C:\> Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
PS C:\> Add-WindowsCapability -Online -Name Rsat.Dns.Tools~~~~0.0.1.0
PS C:\> Add-WindowsCapability -Online -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0

# Then: dsa.msc (AD Users and Computers), dnsmgmt.msc, gpmc.msc, dhcpmgmt.msc
PS C:\> Get-Module -ListAvailable ActiveDirectory, DnsServer, GroupPolicy
```

PowerShell Remoting چگونه کار می‌کند

جزئیات	موضوع
WinRM (WS-Management): HTTP 5985، HTTPS 5986	پروتوکول
به طور پیش‌فرض فعال؛ Enable-PSRemoting روی کلاینت‌ها	روی سرورها
احراز هویت Kerberos — با نام فوراً کار می‌کند	در یک domain
سرورها را به TrustedHosts اضافه کنید، از Credential- استفاده کنید	در یک workgroup
ترافیک رمزگذاری‌شده است؛ به طور پیش‌فرض فقط admin ها وصل می‌شوند	امنیت
PowerShell 7 از طریق SSH: Enter-PSSession -HostName	جایگزین

PowerShell Remoting در عمل

```
PS C:\> Test-WSMan DC01                                  # is WinRM answering?
PS C:\> Enter-PSSession -ComputerName DC01               # interactive remote prompt
[DC01]: PS C:\> Get-Service WinRM ; exit

PS C:\> Invoke-Command -ComputerName DC01, SRV01 -ScriptBlock {
           Get-CimInstance Win32_OperatingSystem | Select-Object CSName, Caption, LastBootUpTime }

PS C:\> $s = New-PSSession -ComputerName DC01          # a reusable session
PS C:\> Copy-Item C:\Scripts\setup.ps1 -Destination C:\Temp\ -ToSession $s
PS C:\> Invoke-Command -Session $s -FilePath C:\Scripts\audit.ps1
PS C:\> Remove-PSSession $s
```

لابراتوار: Remoting قبل از ساختن domain

```
# On SRV01 (workgroup lab), PowerShell as Administrator
PS C:\> Set-Item WSMan:\localhost\Client\TrustedHosts -Value 'DC01,10.0.0.10' -Force
PS C:\> Add-Content C:\Windows\System32\drivers\etc\hosts '10.0.0.10  DC01'
PS C:\> $cred = Get-Credential DC01\Administrator
PS C:\> Invoke-Command -ComputerName DC01 -Credential $cred -ScriptBlock { hostname; Get-TimeZone }

# In Server Manager: Manage > Add Servers > DNS tab > 10.0.0.10
# then right-click DC01 > Manage As... > DC01\Administrator

PS C:\> ssh Administrator@10.0.0.10                # if you started sshd in Lesson 2
```

مدیریت امن از راه دور

چرا	روش
حساب روزانه شما domain admin نیست	حساب‌های admin جداگانه
نه از همان کمپیوتری که با آن مرور و ایمیل می‌کنید	مدیریت از یک ورک‌استیشن امن
Just Enough Administration محدود می‌کند کاربر از راه دور چه چیزی اجرا کند	کمترین دسترسی JEA /
script block logging و transcript های PowerShell را روشن کنید	لاگ‌گیری
WinRM، RDP و SSH را فقط از شبکه‌های admin اجازه دهید	محدوده فایروال
از VPN، Azure Bastion یا یک gateway استفاده کنید	هیچ RDP از انترنت

خلاصه و کارخانگی

- Server Manager برای چند سرور؛ Windows Admin Center برای Core و مرورگر
- Install-WindowsFeature -IncludeManagementTools [-ComputerName]
- RSAT ابزارهای DHCP، DNS، AD و GPO را به Windows 11 می‌آورد
- Enter-PSSession برای یک سرور؛ Invoke-Command برای سرورهای زیاد
- کارخانگی: DC01 را به Server Manager روی SRV01 اضافه کنید
- کارخانگی: یک Invoke-Command را روی هر دو سرور اجرا 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

درس ۴ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

Active Directory Domain Services: مفاهیم و اولین domain شما

دوره کامل · Windows Server 2025 (build 26100)



در درس چهارم چه یاد می‌گیرید

- مفاهیم Active Directory: forest، domain، OU، domain controller
- AD به شما چه می‌دهد: DNS، Group Policy، Kerberos، single sign-on
- پلان: نام domain، تعداد DC ها، سطح عملکرد
- ارتقای DC01: Install-ADDSForest
- بررسی سلامت: dcdiag، نقش‌های FSMO، رکوردهای DNS
- پیوستن SRV01 و CL01 به domain
- یک domain controller دوم، replication و امنیت AD

مفاهیم Active Directory

اصطلاح	معنی
Domain	یک مرز امنیتی: کاربران، گروه‌ها و کمپیوترهایی که یک دایرکتوری را شریک هستند
Forest	یک یا چند domain با یک schema مشترک؛ بالاترین سطح AD
Organizational Unit (OU)	یک فولدر داخل domain برای تفویض و Group Policy
Domain controller (DC)	سروری که یک کاپی از دایرکتوری را دارد و کاربران را وارد می‌کند
Global catalog	یک فهرست قابل جستجو از هر object در forest
Sites	موقعیت‌های فزیکی؛ replication و DC مورد استفاده کلاینت‌ها را کنترل می‌کنند
Schema	تعریف هر نوع object و ویژگی

Active Directory به شما چه می‌دهد

فایده	ویژگی
یک حساب کمپیوترها، اشتراک فایل، ایمیل و برنامه‌ها را باز می‌کند	Single sign-on
احراز هویت امن؛ دایرکتوری که هر برنامه می‌تواند از آن بپرسد	Kerberos و LDAP
تنظیم هزاران کمپیوتر از یک جا (درس ۶)	Group Policy
یک حساب را غیرفعال کنید و دسترسی همه جا پایان می‌یابد	کنترل مرکزی
کلاینت‌ها DC ها را از طریق رکوردهای DNS خودکار پیدا می‌کنند	ادغام با DNS
همگام‌سازی با Microsoft Entra ID برای Microsoft 365 و برنامه‌های ابری	هویت ترکیبی

پلان domain شما

توصیه	تصمیم
Production: یک زیر domain که مالک آن هستید، مثلاً ad.mywebuniversity.com	نام domain
lab.mywebuniversity.local برای این دوره خوب است	نام لابراتوار
کوتاه، حداکثر ۱۵ حرف: LAB	نام NetBIOS
حداقل دو برای هر domain، روی میزبان‌های مختلف	Domain controller ها
DNS ادغام‌شده با AD روی DC ها	DNS
بالاترین سطحی که همه DC های شما پشتیبانی می‌کنند	سطح عملکرد

سطوح عملکرد

سطح	لازم دارد	نکات
Windows Server 2016	همه DC ها 2016 یا جدیدتر	امروز رایج‌ترین؛ محیط‌های مختلط زیاد
Windows Server 2025	همه DC ها Windows Server 2025	جدیدترین سطح در 2025
صفحه‌های 32k دیتابیس	سطح عملکرد forest نسخه 2025	ویژگی اختیاری؛ object های بزرگ‌تر، برگشت‌ناپذیر
بالا بردن سطح	Set-ADDomainMode / Set-ADForestMode	یک‌طرفه — اول پلان و بکاپ کنید

ارتقای DC01: اولین domain شما

```
# On DC01 (Server Core), PowerShell as Administrator
PS C:\> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

PS C:\> Install-ADDSForest -DomainName 'lab.mywebuniversity.local' `
          -DomainNetbiosName 'LAB' -InstallDns `
          -SafeModeAdministratorPassword (Read-Host -AsSecureString 'DSRM password')
# Accept the restart. After reboot, sign in as LAB\Administrator

PS C:\> Test-ADDSForestInstallation -DomainName 'lab.mywebuniversity.local'   # optional pre-check
```

بررسی سلامت domain شما

```
PS C:\> Get-ADDomain | Select-Object DNSRoot, NetBIOSName, DomainMode, PDCEmulator
PS C:\> Get-ADForest | Select-Object Name, ForestMode, SchemaMaster
PS C:\> Get-ADDomainController -Filter * | Select-Object Name, IPv4Address, IsGlobalCatalog
PS C:\> Get-Service NTDS, DNS, Netlogon, Kdc | Select-Object Name, Status

C:\> dcdiag /q                      # no output = no errors
C:\> netdom query fsmo              # which DC holds each FSMO role
PS C:\> Resolve-DnsName _ldap._tcp.dc._msdcs.lab.mywebuniversity.local -Type SRV
```

نقش‌های FSMO (Operations Masters)

نقش	محدوده	وظیفه
Schema master	Forest	تغییرات در schema
Domain naming master	Forest	اضافه یا حذف کردن domain ها
PDC emulator	Domain	منبع زمان، تغییر رمز، قفل شدن حساب
RID master	Domain	دادن مجموعه ID برای object های جدید
Infrastructure master	Domain	ارجاع‌های بین domain ها

پیوستن SRV01 و کلاینت Windows 11

```
# DNS on each machine must point to DC01 (10.0.0.10) first!
PS C:\> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.0.0.10
PS C:\> Add-Computer -DomainName lab.mywebuniversity.local `
           -Credential LAB\Administrator -Restart

# After the restart, sign in as LAB\Administrator and check:
PS C:\> Test-ComputerSecureChannel              # True = trusted by the domain
C:\> nltest /dsgetdc:lab.mywebuniversity.local  # which DC answered
C:\> whoami /fqdn
# GUI: Settings > System > About > Domain or workgroup (Windows 11: Access work or school)
```

یک domain controller دوم و replication

```
# On a new server DC02 (DNS -> 10.0.0.10), as a domain admin:
PS C:\> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
PS C:\> Install-ADDSDomainController -DomainName lab.mywebuniversity.local -InstallDns `
          -Credential (Get-Credential LAB\Administrator) `
          -SafeModeAdministratorPassword (Read-Host -AsSecureString)

C:\> repadmin /replsummary              # replication health, all DCs
C:\> repadmin /showrepl DC02
C:\> dssite.msc                         # Active Directory Sites and Services
```

امن نگه داشتن Active Directory

- دو DC یا بیشتر روی میزبان‌های مختلف؛ هرگز یک نقطه خرابی
- رمز DSRM را در یک جای امن و آفلاین نگه دارید
- به طور منظم از System State یک DC بکاپ بگیرید (درس ۱۱)
- snapshot های کهنه VM ها را برای DC ها بازیابی نکنید؛ از بازیابی درست AD استفاده کنید
- فقط چند نفر در Domain Admins؛ از حساب‌های admin جداگانه استفاده کنید
- AD Recycle Bin را فعال کنید (درس ۵)

خلاصه و کارخانگی

- Forest > domain > OU؛ domain controller ها دایرکتوری را نگه می‌دارند و کاپی می‌کنند
- Install-WindowsFeature AD-Domain-Services، بعد Install-ADDSForest
- بررسی با netdom query fsmo، dcdiag /q، Get-ADDomain
- کلاینت‌ها قبل از Add-Computer باید از DC برای DNS استفاده کنند
- کارخانگی: lab.mywebuniversity.local را روی DC01 بسازید
- کارخانگی: SRV01 و CL01 را وصل کنید و dcdiag را اجرا 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

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

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

درس ۷ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

سرورهای DNS و DHCP

دوره کامل · Windows Server 2025 (build 26100)



در درس هفتم چه یاد می‌گیرید

- مفاهیم DNS: zone ها، رکوردها، forwarder ها و DNS ادغام‌شده با AD
- مدیریت DNS با PowerShell: zone ها، رکوردهای A، PTR، CNAME
- عیب‌یابی تبدیل نام
- امن کردن DNS
- مفاهیم DHCP: scope، DORA، option ها، reservation ها
- نصب، مجاز کردن و تنظیم DHCP
- DHCP failover و عیب‌یابی

مفاهیم DNS

اصطلاح	معنی
Forward lookup zone	نام ← IP، مثلاً lab.mywebuniversity.local
Reverse lookup zone	IP ← نام، مثلاً 10.0.0.in-addr.arpa
Zone ادغام‌شده با AD	در AD ذخیره می‌شود؛ به DC ها کاپی می‌شود؛ آپدیت‌های پویای امن
رکوردها	A / AAAA (IP)، CNAME (نام مستعار)، MX (ایمیل)، PTR (معکوس)، SRV (سرویس‌ها)، TXT
Forwarder ها	سرور سوال‌های انترنتی را که نمی‌تواند جواب دهد به کجا می‌فرستد
Conditional forwarder	سوال‌های یک domain را به یک سرور خاص بفرستید (شرکت همکار)
Scavenging	رکوردهای پویای کهنه را خودکار حذف می‌کند

مدیریت DNS با PowerShell

```
PS C:\> Get-DnsServerZone -ComputerName DC01
PS C:\> Add-DnsServerPrimaryZone -NetworkId 10.0.0.0/24 -ReplicationScope Domain   # reverse zone
PS C:\> Add-DnsServerResourceRecordA -ZoneName lab.mywebuniversity.local -Name web `
           -IPv4Address 10.0.0.20 -CreatePtr
PS C:\> Add-DnsServerResourceRecordCName -ZoneName lab.mywebuniversity.local `
           -Name intranet -HostNameAlias srv01.lab.mywebuniversity.local
PS C:\> Set-DnsServerForwarder -IPAddress 1.1.1.1, 8.8.8.8
PS C:\> Get-DnsServerResourceRecord -ZoneName lab.mywebuniversity.local -RRType A
PS C:\> Set-DnsServerScavenging -ScavengingState $true -ScavengingInterval 7.00:00:00 -
ApplyOnAllZones
```

عیب‌یابی تبدیل نام

```
PS C:\> Resolve-DnsName srv01.lab.mywebuniversity.local
PS C:\> Resolve-DnsName srv01 -Server 10.0.0.10 -DnsOnly       # ask DC01 directly
PS C:\> Resolve-DnsName 10.0.0.20                              # reverse (PTR)
C:\> nslookup -type=SRV _ldap._tcp.dc._msdcs.lab.mywebuniversity.local

C:\> ipconfig /flushdns & ipconfig /registerdns     # client: clear cache, re-register
PS C:\> Clear-DnsServerCache -ComputerName DC01 -Force
C:\> dcdiag /test:dns /v                            # AD-specific DNS tests
# Golden rule: domain members use ONLY your DCs as DNS servers
```

امن کردن DNS

چرا	روش
فقط اعضای domain می‌توانند رکورد ثبت کنند	فقط آپدیت‌های پویای امن
هرگز به سوال‌های بازگشتی از انترنت جواب ندهید	open resolver نباشید
رکوردهای کهنه جواب‌های اشتباه و سردرگمی ایجاد می‌کنند	Scavenging روشن
zone ها را امضا می‌کند تا جواب‌ها جعل نشوند	DNSSEC (جایی که لازم است)
لاگ‌های analytical/audit را برای بررسی مشکلات فعال کنید	لاگ‌گیری
فقط به سرورهای secondary لست‌شده	محدود کردن zone transfer

مفاهیم DHCP

اصطلاح	معنی
DORA	Discover، Offer، Request، Acknowledge — کلاینت چگونه آدرس می‌گیرد
Scope	محدوده‌ای از آدرس‌ها برای یک subnet، مثلاً 10.0.0.100-200
Exclusions	آدرس‌هایی در محدوده که DHCP نباید بدهد
Reservations	همیشه یک IP ثابت به یک دستگاه بدهید (با آدرس MAC)
Options	003 روتر، 006 سرورهای DNS، 015 نام domain برای DNS
Lease	کلاینت چه مدت آدرس خود را نگه دارد (پیش‌فرض ۸ روز)
Authorization	در یک domain، سرور DHCP باید در AD مجاز شود تا کار کند

نصب، مجاز کردن و تنظیم DHCP

```
PS C:\> Install-WindowsFeature DHCP -IncludeManagementTools -ComputerName DC01
PS C:\> Invoke-Command DC01 { netsh dhcp add securitygroups ; Restart-Service DHCPServer }
PS C:\> Add-DhcpServerInDC -DnsName dc01.lab.mywebuniversity.local -IPAddress 10.0.0.10

PS C:\> Add-DhcpServerv4Scope -ComputerName DC01 -Name LabNet -StartRange 10.0.0.100 `
            -EndRange 10.0.0.200 -SubnetMask 255.255.255.0 -LeaseDuration 1.00:00:00
PS C:\> Add-DhcpServerv4ExclusionRange -ComputerName DC01 -ScopeId 10.0.0.0 `
            -StartRange 10.0.0.100 -EndRange 10.0.0.109
PS C:\> Set-DhcpServerv4OptionValue -ComputerName DC01 -ScopeId 10.0.0.0 `
            -DnsServer 10.0.0.10 -DnsDomain lab.mywebuniversity.local -Router 10.0.0.1
PS C:\> Add-DhcpServerv4Reservation -ComputerName DC01 -ScopeId 10.0.0.0 `
            -IPAddress 10.0.0.150 -ClientId '00-15-5D-01-02-03' -Name Printer01
```

آزمایش با کلاینت و دیدن lease ها

```
# On CL01: switch the adapter to automatic (DHCP)
PS C:\> Set-NetIPInterface -InterfaceAlias Ethernet -Dhcp Enabled
PS C:\> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ResetServerAddresses
C:\> ipconfig /release & ipconfig /renew & ipconfig /all

# On the server:
PS C:\> Get-DhcpServerv4Lease -ComputerName DC01 -ScopeId 10.0.0.0
PS C:\> Get-DhcpServerv4ScopeStatistics -ComputerName DC01      # free / in use / %
PS C:\> Get-DhcpServerv4OptionValue -ComputerName DC01 -ScopeId 10.0.0.0
```

DHCP Failover برای دسترسی بالا

```
# Requires a second DHCP server, e.g. DC02 (authorized in AD)
PS C:\> Add-DhcpServerv4Failover -ComputerName DC01 -Name LabFailover `
          -PartnerServer dc02.lab.mywebuniversity.local -ScopeId 10.0.0.0 `
          -LoadBalancePercent 50 -SharedSecret (Read-Host 'Shared secret') -AutoStateTransition
$true
PS C:\> Get-DhcpServerv4Failover -ComputerName DC01

# Modes: Load balance (both answer) or Hot standby (partner waits)
# Backup: Backup-DhcpServer -ComputerName DC01 -Path C:\DhcpBackup
#         Export-DhcpServer -ComputerName DC01 -File C:\DhcpBackup\dhcp.xml -Leases
```

عیب‌یابی DHCP

علامت	علت احتمالی و راه حل
کلاینت x.x.169.254 دارد	جوابی از DHCP نیامد: سرور خاموش، مجاز نشده، scope پر، شبکه/VLAN
سرور آدرس نمی‌دهد	در AD مجاز نشده (Add-DhcpServerInDC)؛ سرویس متوقف است
DNS یا روتر اشتباه	option های scope/سرور را بررسی کنید؛ کلاینت را renew کنید
کلاینت‌ها در subnet دیگر	روتر یک DHCP relay (IP helper) به سمت سرور لازم دارد
تداخل آدرس	IP ثابت داخل scope — آن را exclude کنید یا conflict detection را تنظیم کنید
سرور DHCP ناشناخته	روتر یا دستگاه غیرمجاز در شبکه — پیدا و حذف کنید

خلاصه و کارخانگی

- Zone های ادغام‌شده با AD، آپدیت‌های پویای امن، forwarder ها، scavenging
- Add-DnsServerResourceRecordA -CreatePtr؛ Resolve-DnsName -Server
- اعضای domain فقط از DC های شما برای DNS استفاده می‌کنند
- DHCP: مجاز کردن، exclusion، scope ها، option های 003/006/015، reservation ها
- کارخانگی: reverse zone، رکورد A برای web و CNAME برای intranet را بسازید
- کارخانگی: scope دی‌اچ‌سی‌پی LabNet را بسازید و به CL01 یک آدرس بدهید

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

درس ۸ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

خدمات فایل و ذخیره‌سازی: SMB، Storage Spaces، DFS و ReFS

دوره کامل · Windows Server 2025 (build 26100)



در درس هشتم چه یاد می‌گیرید

- نقش‌ها و ویژگی‌های سرور فایل
- ساختن اشتراک‌های SMB، و مدل اجازه share + NTFS
- امنیت SMB در Windows Server 2025
- DFS Namespaces و DFS Replication
- File Server Resource Manager: سهمیه‌ها و file screen ها
- Shadow copy ها (Previous Versions)
- ReFS، Storage Spaces و data deduplication

نقش‌ها و ویژگی‌های سرور فایل

هدف	نام برای Install-WindowsFeature	ویژگی
اشتراک‌های SMB	FS-FileServer	**File Server**
یک مسیر برای اشتراک‌ها روی سرورهای زیاد	FS-DFS-Namespace	**DFS Namespaces**
همگام نگه داشتن فولدرها بین سرورها	FS-DFS-Replication	**DFS Replication**
سهمیه‌ها، file screen ها، گزارش‌ها	FS-Resource-Manager	**File Server Resource Manager**
دیتای تکراری را فقط یک بار ذخیره کنید	FS-Data-Deduplication	**Data Deduplication**
ارائه دیسک‌ها از طریق شبکه	FS-iSCSITarget-Server	**iSCSI Target Server**

ساختن اشتراک‌های Teachers و Students

```
# On SRV01 (a second data disk D: is recommended)
PS C:\> Install-WindowsFeature FS-FileServer, FS-Resource-Manager, FS-DFS-Namespace `
            -IncludeManagementTools
PS C:\> New-Item D:\Shares\Teachers, D:\Shares\Students -ItemType Directory

PS C:\> New-SmbShare -Name Teachers -Path D:\Shares\Teachers `
            -FullAccess 'LAB\Domain Admins' -ChangeAccess 'LAB\Domain Users' `
            -FolderEnumerationMode AccessBased
PS C:\> New-SmbShare -Name Students -Path D:\Shares\Students `
            -FullAccess 'LAB\Domain Admins' -ChangeAccess 'LAB\Domain Users' -FolderEnumerationMode
AccessBased
PS C:\> Get-SmbShare | Where-Object Special -eq $false
```

اجازه‌های NTFS با AGDLP

```
PS C:\> icacls D:\Shares\Teachers /inheritance:r                    # stop inheriting
PS C:\> icacls D:\Shares\Teachers /grant 'SYSTEM:(OI)(CI)F' 'LAB\Domain Admins:(OI)(CI)F'
PS C:\> icacls D:\Shares\Teachers /grant 'LAB\DL_Share_Teachers_Modify:(OI)(CI)M'
PS C:\> icacls D:\Shares\Teachers

PS C:\> Get-SmbShareAccess Teachers
# Effective access = the MORE RESTRICTIVE of share and NTFS permissions
# Check one user: folder Properties > Security > Advanced > Effective Access
```

امنیت SMB در Windows Server 2025

چه کار می‌کند	ویژگی
به طور پیش‌فرض روشن: محافظت در برابر دستکاری و حملات relay	SMB signing لازم
یک share یا کل سرور را رمزگذاری کنید (SMB 3)	رمزگذاری SMB
دسترسی امن به فایل از طریق انترنت بدون VPN — در همه نسخه‌ها	SMB over QUIC
حذف‌شده — هرگز دوباره نصب نکنید	SMB1
کاربران فقط فولدرهایی را می‌بینند که می‌توانند باز کنند	Access-based enumeration
دنبال کنید چه کسی فایل‌ها را باز، تغییر یا حذف کرد	Auditing

بررسی و محکم کردن SMB

```
PS C:\> Get-SmbServerConfiguration |
          Select-Object RequireSecuritySignature, EncryptData, EnableSMB1Protocol
PS C:\> Set-SmbShare -Name Teachers -EncryptData $true -Force

PS C:\> Get-SmbSession | Select-Object ClientComputerName, ClientUserName, NumOpens
PS C:\> Get-SmbOpenFile | Select-Object ClientUserName, Path
PS C:\> Get-SmbOpenFile | Where-Object Path -like '*report.docx' | Close-SmbOpenFile -Force

# On CL01 as a teacher:  net use S: \\SRV01\Teachers   (or the GPO drive map from Lesson 6)
```

DFS Namespaces: یک مسیر برای همه چیز

```
PS C:\> New-Item C:\DFSRoots\Shares -ItemType Directory
PS C:\> New-SmbShare -Name Shares -Path C:\DFSRoots\Shares -ReadAccess 'LAB\Domain Users'
PS C:\> New-DfsnRoot -Path \\lab.mywebuniversity.local\Shares `
           -TargetPath \\SRV01\Shares -Type DomainV2
PS C:\> New-DfsnFolder -Path \\lab.mywebuniversity.local\Shares\Teachers -TargetPath \\SRV01\Teachers
PS C:\> New-DfsnFolder -Path \\lab.mywebuniversity.local\Shares\Students -TargetPath \\SRV01\Students
PS C:\> Get-DfsnFolder -Path '\\lab.mywebuniversity.local\Shares\*'

# Users map \\lab.mywebuniversity.local\Shares — move data to new servers without changing paths
# DFS Replication (FS-DFS-Replication) keeps copies in sync for branch offices
```

سهمیه‌های FSRM، File Screen ها و Shadow Copy ها

```
PS C:\> New-FsrmQuota -Path D:\Shares\Students -Size 5GB -Description 'Student share limit'
PS C:\> New-FsrmAutoQuota -Path D:\Shares\Students\Home -Template '200 MB Limit Reports to User'
PS C:\> New-FsrmFileScreen -Path D:\Shares\Students -Template 'Block Executable Files'
PS C:\> Get-FsrmQuota | Select-Object Path, Size, Usage

# Shadow copies (Previous Versions) on the data volume:
C:\> vssadmin add shadowstorage /for=D: /on=D: /maxsize=10%
C:\> vssadmin create shadow /for=D:
# GUI: D: Properties > Shadow Copies > Enable (twice a day by default)
# Users: right-click a file > Restore previous versions
```

Storage Spaces، ReFS و Deduplication

چه چیزی به شما می‌دهد	ویژگی
ترکیب دیسک‌های فزیکی زیاد در یک pool	Storage pool
Simple (بدون محافظت)، Mirror (کاپی‌ها)، Parity (صرفه‌جو در فضا)	مقاومت virtual disk
Resilient File System: بررسی سلامت دیتا، عالی برای Hyper-V و دیتای بکاپ	ReFS
۳۰ تا ۹۰ درصد صرفه‌جویی در اشتراک فایل، VDI و بکاپ‌ها	Data Deduplication
Datacenter: جمع کردن دیسک‌های محلی یک cluster (hyper-converged)	Storage Spaces Direct
کارایی سریع‌تر ذخیره‌سازی NVMe در 2025	NVMe

لابراتوار: یک volume آینه‌ای ReFS با Deduplication

```
# On the Hyper-V host: give SRV01 two extra disks
PS C:\> 1..2 | ForEach-Object { New-VHD C:\VMs\SRV01-Data$_.vhdx -SizeBytes 40GB -Dynamic |
          Out-Null; Add-VMHardDiskDrive SRV01 -Path C:\VMs\SRV01-Data$_.vhdx }

# On SRV01:
PS C:\> New-StoragePool -FriendlyName Pool1 -StorageSubSystemFriendlyName 'Windows Storage*' `
          -PhysicalDisks (Get-PhysicalDisk -CanPool $true)
PS C:\> New-VirtualDisk -StoragePoolFriendlyName Pool1 -FriendlyName Data `
          -ResiliencySettingName Mirror -UseMaximumSize |
        Get-Disk | Initialize-Disk -PassThru | New-Partition -DriveLetter E -UseMaximumSize |
        Format-Volume -FileSystem ReFS -NewFileSystemLabel Data
PS C:\> Install-WindowsFeature FS-Data-Deduplication ; Enable-DedupVolume E: -UsageType Default
```

خلاصه و کارخانگی

- اجازه‌های share گسترده؛ کنترل واقعی با NTFS و گروه‌های AGDLP
- SMB signing به طور پیش‌فرض روشن؛ اشتراک‌های حساس را رمزگذاری کنید؛ SMB1 هرگز
- DFS Namespaces: یک مسیر domain؛ سرورها می‌توانند پشت آن عوض شوند
- سهمیه‌ها و file screen های FSRM؛ shadow copy برای بازیابی خودکار کاربران
- Storage Spaces mirror + ReFS + deduplication برای ذخیره‌سازی مقاوم
- کارخانگی: اشتراک‌های DFS، Teachers/Students و یک سهمیه را 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

درس ۹ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

Hyper-V در Windows Server

دوره کامل · Windows Server 2025 (build 26100)



در درس نهم چه یاد می‌گیرید

- مفاهیم Hyper-V: نسل‌ها، دیسک‌های VHDX، switch ها، حافظه پویا
- چه چیزی در Hyper-V ویندوز سرور 2025 جدید است
- نصب Hyper-V (و nested virtualization برای لابراتوار)
- virtual switch ها و ساختن VM ها با PowerShell
- تمپلیت‌ها با sysprep و دیسک‌های differencing
- Checkpoint ها، export/import و PowerShell Direct
- Hyper-V Replica، Live migration و clustering

مفاهیم Hyper-V

اصطلاح	معنی
Hypervisor (نوع ۱)	مستقیم روی سخت‌افزار اجرا می‌شود؛ ویندوز parent partition می‌شود
VM نسل ۲	UEFI، Secure Boot، TPM مجازی — برای همه مهمان‌های مدرن استفاده کنید
VHDX	دیسک مجازی: ثابت، پویا یا differencing
Virtual switch	External (شبکه فزیکی)، Internal (میزبان + VM ها)، Private (فقط VM ها)
حافظه پویا	حافظه را به اندازه نیاز بین یک حداقل و حداکثر به VM ها می‌دهد
Checkpoint	وضعیت یک VM در یک لحظه — بکاپ نیست
Integration services	درایورها برای هماهنگی زمان، خاموش کردن، بکاپ، کاپی فایل

Hyper-V در Windows Server 2025

ویژگی	نکات برجسته
مقیاس	تا ۲,۰۴۸ CPU مجازی و ۲۴۰ ترابایت حافظه برای هر VM نسل ۲
تقسیم GPU	یک GPU را بین چند VM شریک کنید، با live migration و clustering
Workgroup cluster ها	Failover cluster بدون Active Directory (بر اساس سرتیفیکیت)
Dynamic processor compatibility	Live migration بین میزبان‌هایی با نسل‌های مختلف CPU
پیش‌فرض	VM های جدید به طور پیش‌فرض نسل ۲ هستند
یادآوری لایسنس	Standard: ۲ VM ویندوز سرور برای هر میزبان لایسنس‌شده؛ Datacenter: نامحدود

نصب Hyper-V (و Nested Virtualization برای لابراتوار)

```
# LAB ONLY: SRV01 is itself a VM, so first allow nested virtualization
# On the physical host, with SRV01 turned off:
PS C:\> Stop-VM SRV01
PS C:\> Set-VMProcessor SRV01 -ExposeVirtualizationExtensions $true
PS C:\> Set-VMMemory SRV01 -DynamicMemoryEnabled $false -StartupBytes 8GB
PS C:\> Get-VMNetworkAdapter SRV01 | Set-VMNetworkAdapter -MacAddressSpoofing On
PS C:\> Start-VM SRV01

# On SRV01 (or any physical server):
PS C:\> Install-WindowsFeature Hyper-V -IncludeManagementTools -Restart
PS C:\> Get-VMHost | Select-Object Name, LogicalProcessorCount, MemoryCapacity, VirtualHardDiskPath
```

Virtual Switch ها و یک VM جدید

```
PS C:\> New-VMSwitch -Name External -NetAdapterName Ethernet -AllowManagementOS $true
PS C:\> New-VMSwitch -Name Isolated -SwitchType Private
PS C:\> Get-VMSwitch

PS C:\> New-VM -Name WEB01 -Generation 2 -MemoryStartupBytes 2GB -SwitchName External `
           -NewVHDPath D:\VMs\WEB01.vhdx -NewVHDSizeBytes 60GB
PS C:\> Set-VMMemory WEB01 -DynamicMemoryEnabled $true -MinimumBytes 1GB -MaximumBytes 4GB
PS C:\> Set-VMProcessor WEB01 -Count 2
PS C:\> Add-VMDvdDrive WEB01 -Path D:\ISO\WindowsServer2025_Eval.iso
PS C:\> Set-VMFirmware WEB01 -FirstBootDevice (Get-VMDvdDrive WEB01)
PS C:\> Start-VM WEB01 ; vmconnect localhost WEB01
```

تمپلیت‌ها: sysprep و دیسک‌های Differencing

```
# Inside a fully updated 'golden' VM:
C:\> C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown

# On the host: keep the generalized disk as a read-only template
PS C:\> Move-Item D:\VMs\Golden.vhdx D:\Templates\WS2025-Base.vhdx
PS C:\> Set-ItemProperty D:\Templates\WS2025-Base.vhdx -Name IsReadOnly -Value $true

PS C:\> New-VHD -Path D:\VMs\APP01.vhdx -ParentPath D:\Templates\WS2025-Base.vhdx -Differencing
PS C:\> New-VM -Name APP01 -Generation 2 -MemoryStartupBytes 2GB -VHDPath D:\VMs\APP01.vhdx `
            -SwitchName External ; Start-VM APP01        # ready in about a minute
```

Checkpoint ها، Export و PowerShell Direct

```
PS C:\> Checkpoint-VM WEB01 -SnapshotName 'Before IIS'
PS C:\> Get-VMSnapshot WEB01
PS C:\> Restore-VMSnapshot -VMName WEB01 -Name 'Before IIS' -Confirm:$false
PS C:\> Remove-VMSnapshot -VMName WEB01 -Name 'Before IIS'      # merge when done

PS C:\> Export-VM WEB01 -Path E:\Exports ; Import-VM -Path (Get-Item E:\Exports\WEB01\*\*.vmcx) -Copy
-GenerateNewId

# PowerShell Direct: manage a VM from its host, even with no network
PS C:\> Enter-PSSession -VMName WEB01 -Credential (Get-Credential)
PS C:\> Invoke-Command -VMName WEB01 -Credential $c -ScriptBlock { Get-NetIPAddress -AddressFamily
IPv4 }
PS C:\> Copy-VMFile WEB01 -SourcePath C:\Scripts\setup.ps1 -DestinationPath C:\Temp\setup.ps1 -
FileSource Host -CreateFullPath
```

دسترسی بالا برای VM ها

چه کار می‌کند	ویژگی
یک VM در حال اجرا را بدون توقف به میزبان دیگر منتقل کنید	Live migration
دیسک‌های یک VM در حال اجرا را به ذخیره‌سازی جدید منتقل کنید	Storage migration
کاپی ناهمزمان یک VM در میزبان یا محل دیگر، برای بازیابی از فاجعه	Hyper-V Replica
وقتی یک میزبان خراب شود VM ها خودکار روی node دیگر شروع می‌شوند	Failover clustering
Datacenter: ذخیره‌سازی hyper-converged برای cluster	Storage Spaces Direct
از بکاپ آگاه از Hyper-V استفاده کنید (درس ۱۱)، نه checkpoint ها	بکاپ

Live Migration، Replica و نظارت

```
# Between two domain-joined Hyper-V hosts (HV01, HV02):
PS C:\> Enable-VMMigration ; Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
PS C:\> Move-VM WEB01 -DestinationHost HV02 -IncludeStorage -DestinationStoragePath D:\VMs\WEB01

PS C:\> Enable-VMReplication WEB01 -ReplicaServerName HV02 -ReplicaServerPort 80 `
          -AuthenticationType Kerberos ; Start-VMInitialReplication WEB01

PS C:\> Get-VM | Select-Object Name, State, CPUUsage, @{n='MemGB';e={$_.MemoryAssigned/1GB}}, Uptime
PS C:\> Enable-VMResourceMetering WEB01 ; Measure-VM WEB01
```

خلاصه و کارخانگی

- VM های نسل ۲، دیسک‌های VHDX، نوع درست switch، حافظه پویا
- Install-WindowsFeature Hyper-V؛ nested virtualization برای لابراتوار
- vmconnect، Start-VM، Set-VMProcessor، Set-VMMemory، New-VM
- sysprep + تمپلیت‌ها؛ checkpoint ها بکاپ نیستند
- PowerShell Direct: Enter-PSSession -VMName
- کارخانگی: WEB01 را روی SRV01 بسازید و قبل از درس ۱۰ یک checkpoint بگیرید

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

درس ۱۰ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

سرور وب (IIS)، Remote Desktop Services و دسترسی از راه دور

دوره کامل · Windows Server 2025 (build 26100)



در درس دهم چه یاد می‌گیرید

- مفاهیم IIS: site ها، binding ها، application pool ها، لاگ‌ها
- نصب IIS و ساختن یک ویب‌سایت با PowerShell
- binding های HTTPS و سرتیفیکیت‌ها
- Application pool ها و امنیت IIS
- Remote Desktop Services: نقش‌ها، collection ها و RemoteApp
- دسترسی از راه دور: VPN، RD Gateway و SMB over QUIC
- یک چک‌لست امنیتی برای هر چیزی که رو به انترنت است

مفاهیم IIS

اصطلاح	معنی
Site	یک وب‌سایت با فولدر، binding ها و تنظیمات خودش
Binding	پروتوکول + IP + پورت + نام میزبان، مثلاً https *:443 intranet.lab...
Application pool	یک پروسه کارگر جدا (w3wp.exe) که یک یا چند برنامه را اجرا می‌کند
Virtual directory / application	یک فولدر یا برنامه داخل یک site
Physical path	جایی که فایل‌ها قرار دارند، مثلاً C:\inetpub\intranet
لاگ‌ها	C:\inetpub\logs\LogFiles — هر درخواست، کد وضعیت، زمان

نصب IIS و ساختن سایت Intranet

```
PS C:\> Install-WindowsFeature Web-Server -IncludeManagementTools    # inetmgr is the GUI
PS C:\> New-Item C:\inetpub\intranet -ItemType Directory
PS C:\> Set-Content C:\inetpub\intranet\index.html `
           '<h1>MyWebUniversity Lab Intranet</h1><p>Served by IIS on Windows Server 2025</p>'

PS C:\> Import-Module IISAdministration
PS C:\> New-IISSite -Name Intranet -PhysicalPath C:\inetpub\intranet `
           -BindingInformation '*:80:intranet.lab.mywebuniversity.local'
PS C:\> Get-IISSite
PS C:\> Invoke-WebRequest http://intranet.lab.mywebuniversity.local -UseBasicParsing |
           Select-Object StatusCode, Content
```

اضافه کردن HTTPS

```
# LAB: a self-signed certificate.  PRODUCTION: a certificate from AD CS or a public CA
PS C:\> $cert = New-SelfSignedCertificate -DnsName intranet.lab.mywebuniversity.local `
           -CertStoreLocation Cert:\LocalMachine\My
PS C:\> New-IISSiteBinding -Name Intranet -Protocol https `
           -BindingInformation '*:443:intranet.lab.mywebuniversity.local' `
           -CertificateThumbPrint $cert.Thumbprint -CertStoreLocation 'Cert:\LocalMachine\My' -
SslFlag Sni
PS C:\> Get-IISSiteBinding -Name Intranet
PS C:\> Get-NetFirewallRule -DisplayGroup 'World Wide Web Services*' | Select-Object DisplayName,
Enabled
```

Application Pool ها و امنیت IIS

چرا	روش
جداسازی: یک crash یا نفوذ محدود می‌ماند	یک app pool برای هر برنامه
هر pool با حساب مجازی کم‌دسترسی خودش اجرا می‌شود	ApplicationPoolIdentity
رمزها و دیتا را در مسیر محافظت می‌کند	فقط HTTPS؛ HTTP را redirect کنید
ماژول‌های کمتر = سطح حمله کوچک‌تر	فقط ویژگی‌های لازم را نصب کنید
درخواست‌های بد را مسدود کنید؛ مشکلات را بررسی کنید	Request filtering، لاگ‌گیری
ASP.NET Core Hosting Bundle؛ PHP/Python از طریق FastCGI یا HttpPlatformHandler	برنامه‌ها

App Pool ها و لاگ‌ها با PowerShell

```
PS C:\> Import-Module WebAdministration
PS C:\> New-WebAppPool -Name IntranetPool
PS C:\> Set-ItemProperty IIS:\Sites\Intranet -Name applicationPool -Value IntranetPool
PS C:\> Get-IISAppPool | Select-Object Name, State, ManagedRuntimeVersion
PS C:\> Restart-WebAppPool IntranetPool

PS C:\> icacls C:\inetpub\intranet /grant 'IIS AppPool\IntranetPool:(OI)(CI)RX'

PS C:\> Get-ChildItem C:\inetpub\logs\LogFiles -Recurse -File |
           Sort-Object LastWriteTime | Select-Object -Last 1 | Get-Content -Tail 10
```

(RDS) Remote Desktop Services

وظیفه	نقش
دسکتاپ‌ها و برنامه‌هایی را اجرا می‌کند که کاربران زیاد شریک هستند	RD Session Host
کاربران را به میزبان درست می‌فرستد؛ جلسات را دوباره وصل می‌کند	RD Connection Broker
صفحه ویبی که دسکتاپ‌ها و RemoteApp های منتشرشده را لست می‌کند	RD Web Access
ورود امن HTTPS از انترنت — بدون باز کردن پورت 3389	RD Gateway
RDS CAL ها را صادر می‌کند (۱۲۰ روز مهلت برای شروع)	RD Licensing
هر کاربر به جای جلسه مشترک، VM خودش را می‌گیرد	VDI (جایگزین)

نصب سریع RDS و یک RemoteApp

```
# All roles on SRV01 for the lab (production: separate servers)
PS C:\> $s = 'srv01.lab.mywebuniversity.local'
PS C:\> New-RDSessionDeployment -ConnectionBroker $s -WebAccessServer $s -SessionHost $s
#       (the server restarts; sign in again as LAB\Administrator)
PS C:\> New-RDSessionCollection -CollectionName Staff -SessionHost $s -ConnectionBroker $s
PS C:\> Set-RDSessionCollectionConfiguration -CollectionName Staff -UserGroup 'LAB\GG_Teachers'
PS C:\> New-RDRemoteApp -CollectionName Staff -DisplayName 'Notepad' `
          -FilePath 'C:\Windows\System32\notepad.exe' -ConnectionBroker $s

# On CL01 as a teacher:  https://srv01.lab.mywebuniversity.local/RDWeb
```

دسترسی از راه دور: گزینه‌های امن

گزینه	بهترین برای	نکات
VPN (RRAS / Always On VPN)	دسترسی کامل شبکه برای لپ‌تاپ‌های مدیریت‌شده	IKEv2 یا SSTP؛ سرتیفیکیت‌ها؛ MFA
RD Gateway	دسکتاپ‌ها و RemoteApp های از راه دور	HTTPS 443؛ MFA اضافه کنید
SMB over QUIC	اشتراک‌های فایل از هر جا	بدون VPN؛ بر اساس سرتیفیکیت؛ همه نسخه‌ها
برنامه‌های وب پشت reverse proxy	سایت‌های intranet	HTTPS، MFA، WAF
هرگز	باز کردن RDP (3389) یا SMB (445) به انترنت	حمله‌کنندگان دائماً جستجو می‌کنند

چک‌لست برای هر چیزی که رو به انترنت است

- HTTPS در همه جا، با سرتیفیکیت از یک CA مطمئن
- احراز هویت چندمرحله‌ای در هر نقطه ورود بیرونی
- فقط پورت 443 (و پورت‌های VPN) باز؛ هیچ چیز دیگر
- آپدیت ماهانه — اول سرورهای رو به انترنت
- کمترین دسترسی: هویت‌های app pool، هیچ domain admin روی سرورهای وب
- لاگ‌ها به صورت مرکزی جمع و مرور شوند (درس ۱۲)

خلاصه و کارخانگی

- IIS: site ها، binding های نام میزبان، یک app pool برای هر برنامه، لاگ‌ها
- New-IISSite، New-IISSiteBinding -Protocol https، Get-IISAppPool
- RDS: Licensing، Gateway، Web Access، Broker، Session Host
- New-RDSessionDeployment، New-RDSessionCollection، New-RDRemoteApp
- کارخانگی: سایت intranet با HTTPS و app pool خودش را بسازید
- کارخانگی: یک RemoteApp منتشر کنید و آن را از CL01 باز 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

درس ۱۱ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

امنیت، آپدیت‌ها، Hotpatch و بکاپ

دوره کامل · Windows Server 2025 (build 26100)



در درس یازدهم چه یاد می‌گیرید

- خط پایه‌های امنیتی و محافظت‌های داخلی
- محافظت از حساب‌های privileged: tier ها، LAPS، Protected Users
- آدیت ورودها و تغییرات
- گزینه‌های آپدیت: Azure Update Manager، WSUS، Windows Update
- Hotpatch: آپدیت‌های امنیتی بدون ری‌استارت
- Windows Server Backup: کامل، Hyper-V، system state
- بکاپ مقاوم در برابر باج‌افزار و پلان بازیابی

محافظت‌های داخلی که باید بدانید

چه کار می‌کند	محافظت
داخلی و به طور پیش‌فرض در Windows Server روشن	Microsoft Defender Antivirus
رازها را در امنیت مبتنی بر مجازی‌سازی جدا می‌کند	Credential Guard / VBS
ابزارها را از بیرون کشیدن رمزها از حافظه منع می‌کند	LSA protection
دستکاری و حملات relay را مسدود می‌کند	SMB و LDAP signing
احراز هویت ضعیف و قدیمی را حذف می‌کند	Kerberos AES، بدون NTLMv1
شروع مطمئن؛ محافظت در برابر بدافزار سطح بوت	Secure Boot، TPM 2.0

اعمال یک خط پایه امنیتی

```
# Option 1 (Windows Server 2025): the OSConfig baseline module
PS C:\> Install-Module Microsoft.OSConfig -Scope AllUsers
PS C:\> Set-OSConfigDesiredConfiguration -Scenario SecurityBaseline/WS2025/MemberServer -Default
PS C:\> Get-OSConfigDesiredConfiguration -Scenario SecurityBaseline/WS2025/MemberServer |
          Select-Object Name, @{n='Status';e={$_.Compliance.Status}} | Select-Object -First 10
#   Scenarios also exist for DomainController and WorkgroupMember

# Option 2: Microsoft Security Compliance Toolkit GPO baselines (import into GPMC)

PS C:\> Get-MpComputerStatus | Select-Object AMServiceEnabled, RealTimeProtectionEnabled,
AntivirusSignatureAge
```

خط پایه‌ها را اول روی یک سرور لابراتوار آزمایش کنید — ممکن است برنامه‌های قدیمی را مسدود کنند.

محافظت از حساب‌های Privileged

جزئیات	روش
Tier 0 = DC ها و admin های AD؛ هرگز با حساب tier 0 به ورک‌استیشن وارد نشوید	مدل tier
mahmadi برای ایمیل؛ adm-mahmadi برای مدیریت	حساب‌های admin جداگانه
محافظت قوی‌تر فقط با Kerberos برای admin ها	گروه Protected Users
یک کمپیوتر قفل‌شده فقط برای مدیریت	Privileged Access Workstation
رمزهای admin محلی منحصربه‌فرد روی هر سرور و کمپیوتر	Windows LAPS
حساب‌های سرویس با رمزهای خودکار	gMSA / dMSA

آدیتینگ: چه کسی چه کاری کرد؟

```
C:\> auditpol /get /category:*                    # current audit policy
C:\> auditpol /set /subcategory:"Logon" /success:enable /failure:enable
C:\> auditpol /set /subcategory:"User Account Management" /success:enable
C:\> auditpol /set /subcategory:"Security Group Management" /success:enable
# Domain-wide: GPO > Computer > Windows Settings > Security > Advanced Audit Policy

PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 10   # failed sign-ins
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4720,4728,4732} -MaxEvents 10
#   4720 user created   4728/4732 member added to a security group
```

گزینه‌های آپدیت برای سرورها

گزینه	بهترین برای	نکات
Windows Update	محیط‌های کوچک	sconfig، Settings؛ زمان‌های نگهداری را زمان‌بندی کنید
WSUS	تأیید و گزارش داخلی	هنوز موجود، اما منسوخ‌شده — بدون ویژگی جدید
Azure Update Manager	سرورهای ترکیبی از طریق Azure Arc	زمان‌بندی، گزارش انطباق، سرورهای زیاد
Hotpatch	ری‌استارت کمتر	آپدیت امنیتی بدون ری‌استارت (Azure Arc)
Patch Tuesday	همه	سه‌شنبه دوم هر ماه؛ آزمایش کنید، بعد اجرا کنید

Hotpatch در Windows Server 2025

چه چیزی بدانید	موضوع
کود در حال اجرا را در حافظه اصلاح می‌کند — برای بیشتر آپدیت‌های امنیتی ری‌استارت لازم نیست	چیست
Datacenter: Azure Edition؛ Standard و Datacenter وصل به Azure Arc	کجا
بدون هزینه اضافی همراه Azure Arc (از ۲۰۲۶)	هزینه
آپدیت baseline سه‌ماهه ری‌استارت لازم دارد؛ ماه‌های بین آن‌ها نه	چرخه
حدود ۴ ری‌استارت پلان‌شده در سال به جای ۱۲	نتیجه
Azure Arc > Azure portal > سرور شما > Hotpatch	فعال کردن

WSUS در ده خط

```
# On SRV01
PS C:\> Install-WindowsFeature UpdateServices -IncludeManagementTools
PS C:\> New-Item E:\WSUS -ItemType Directory
PS C:\> & 'C:\Program Files\Update Services\Tools\wsusutil.exe' postinstall CONTENT_DIR=E:\WSUS
# Then: Windows Server Update Services console > configuration wizard
#       (products: Windows Server 2025, Windows 11; classifications: Security, Critical)

# GPO 'SRV - WSUS' > Computer > Admin Templates > Windows Components > Windows Update >
#   Manage updates offered from Windows Server Update Service >
#   Specify intranet Microsoft update service location = http://srv01.lab.mywebuniversity.local:8530
C:\> usoclient StartScan          # or wait for the next detection cycle
```

Windows Server Backup

```
PS C:\> Install-WindowsFeature Windows-Server-Backup

# Domain controller: back up the System State (AD, SYSVOL, registry, boot files)
C:\> wbadmin start systemstatebackup -backupTarget:E: -quiet

# Full server (bare-metal recovery) and a Hyper-V VM:
C:\> wbadmin start backup -backupTarget:E: -allCritical -include:C:,D: -vssFull -quiet
C:\> wbadmin start backup -backupTarget:E: -hyperv:WEB01 -quiet

C:\> wbadmin get versions                # list backups
C:\> wbadmin start recovery -version:11/22/2026-02:00 -itemType:File -items:D:\Shares\Teachers -
recursive
```

بکاپ و بازیابی مقاوم در برابر باج‌افزار

چرا	روش
۳ کاپی، ۲ رسانه، ۱ خارج از محل، ۱ آفلاین یا تغییرناپذیر	قانون ۳-۲-۱-۱
نه domain admin؛ حمله‌کنندگان اول بکاپ‌ها را حذف می‌کنند	credential جداگانه برای بکاپ
کاپی‌هایی که حمله‌کنندگان نمی‌توانند تغییر یا حذف کنند	ذخیره‌سازی Azure Backup / تغییرناپذیر
یک بکاپ فقط بعد از یک بازیابی موفق واقعی است	بازیابی را به طور منظم آزمایش کنید
رمز DSRM، بکاپ‌های system state، AD Recycle Bin	پلان بازیابی AD
چه کسی چه کاری، به چه ترتیبی، در بدترین روز	دستورالعمل نوشته‌شده

لابراتوار: محکم کردن، آدیت، بکاپ، بازیابی

```
PS C:\> Add-ADGroupMember 'Protected Users' -Members adm-mahmadi      # an admin account
C:\> auditpol /set /subcategory:"Security Group Management" /success:enable
PS C:\> Add-ADGroupMember GG_Teachers -Members arahimi                 # generate an event
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4728,4756} -MaxEvents 3

# DC01: system state backup to a second disk (E:)
PS C:\> Install-WindowsFeature Windows-Server-Backup
C:\> wbadmin start systemstatebackup -backupTarget:E: -quiet
# SRV01: back up D:\Shares, delete a test file, restore it with wbadmin start recovery
```

خلاصه و کارخانگی

- خط پایه‌ها: OSConfig یا Security Compliance Toolkit؛ اول آزمایش کنید
- حساب‌های admin جداگانه، جداسازی LAPS، Protected Users، tier 0
- auditpol + رویدادهای لاگ 4732، 4728، 4720، 4625: Security
- آپدیت‌ها: WSUS، Windows Update (منسوخ)، Azure Update Manager
- Hotpatch با Azure Arc: حدود ۴ ری‌استارت در سال
- بکاپ‌ها: system state برای DC ها، ۳-۲-۱-۱، بازیابی را آزمایش 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

درس ۱۲ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

نظارت، عیب‌یابی، Azure Arc و مهاجرت

دوره کامل · Windows Server 2025 (build 26100)



در درس دوازدهم چه یاد می‌گیرید

- ابزارهای نظارت و counter های کارایی که مهم هستند
- خط پایه با Performance Monitor و logman
- جمع‌آوری مرکزی رویدادها و یک بررسی سلامت روزانه
- یک روش عیب‌یابی — و جعبه ابزار برای هر لایه
- Azure Arc: مدیریت سرورهای داخلی از Azure
- مهاجرت از نسخه‌های قدیمی Windows Server
- خلاصه دوره، پروژه نهایی و قدم‌های بعدی

ابزارهای نظارت

برای چه	ابزار
سلامت سریع نقش‌ها، رویدادها، سرویس‌ها	Server Manager / Windows Admin Center
counter های زنده و data collector set های طولانی‌مدت	Performance Monitor (perfmon)
کدام پروسه همین حالا از CPU، دیسک، شبکه استفاده می‌کند	Resource Monitor (resmon)
خطاها و هشدارها، جمع‌شده از سرورهای زیاد	Event Viewer + subscription ها
اسکریپت‌ها، گزارش‌ها، هشدارها	PowerShell (Get-، Get-Counter (WinEvent
داشبوردها و هشدارها برای سرورهای ترکیبی	Azure Monitor از طریق Azure Arc

Counter های کارایی که مهم هستند

Counter	مراقب باشید
Processor(_Total)\% Processor Time	به طور مداوم بالای ۸۰٪
Memory\Available MBytes	کمتر از حدود ۱۰٪ RAM
Memory\Pages/sec	مقادیر بالای مداوم همراه با حافظه کم
LogicalDisk\Avg. Disk sec/Transfer	بالای 0.020 (۲۰ میلی‌ثانیه) یعنی ذخیره‌سازی کُند
LogicalDisk\% Free Space	کمتر از ۱۵٪
Network Interface\Bytes Total/sec	نزدیک به سرعت لینک

Counter های زنده و یک خط پایه

```
PS C:\> $c = '\Processor(_Total)\% Processor Time', '\Memory\Available MBytes',
            '\LogicalDisk(_Total)\Avg. Disk sec/Transfer'
PS C:\> Get-Counter -Counter $c -ComputerName DC01, SRV01 -SampleInterval 5 -MaxSamples 3

# Record a 7-day baseline, one sample per minute:
C:\> logman create counter ServerBaseline -c "\Processor(_Total)\% Processor Time" ^
      "\Memory\Available MBytes" "\LogicalDisk(*)\Avg. Disk sec/Transfer" ^
      -si 00:01:00 -rf 168:00:00 -o C:\PerfLogs\ServerBaseline
C:\> logman start ServerBaseline
C:\> logman query ServerBaseline
# Open the .blg file in Performance Monitor to see the graphs
```

رویدادهای مرکزی و یک بررسی سلامت روزانه

```
C:\> wecutil qc                                          # on the collector (SRV01)
# Event Viewer > Subscriptions > Create: source DC01, Errors+Warnings, System+Application

PS C:\> $servers = 'DC01', 'SRV01'
PS C:\> Invoke-Command -ComputerName $servers -ScriptBlock {
    [pscustomobject]@{
      Server   = $env:COMPUTERNAME
      Uptime   = (Get-Date) - (Get-CimInstance Win32_OperatingSystem).LastBootUpTime
      FreeC_GB = [int]((Get-Volume C).SizeRemaining / 1GB)
      Errors24h = (Get-WinEvent -FilterHashtable @{LogName='System'; Level=2;
                   StartTime=(Get-Date).AddDays(-1)} -ErrorAction SilentlyContinue).Count
      StoppedAuto = (Get-Service | Where-Object {$_.StartType -eq 'Automatic' -and $_.Status -ne
'Running'}).Count
    } } | Format-Table Server, Uptime, FreeC_GB, Errors24h, StoppedAuto
```

یک روش آرام عیب‌یابی

چه کار می‌کنید	قدم
دقیقاً چه چیزی خراب است؟ برای چه کسی؟ از کی؟ پیام‌های خطا؟	۱. تعریف
یک کاربر، یک کمپیوتر، یک محل، یا همه؟	۲. محدوده
اخیراً چه چیزی تغییر کرد؟ آپدیت‌ها، GPO ها، سرتیفیکیت‌ها، رمزها	۳. تغییرات
شبکه ← DNS ← احراز هویت ← سرویس ← برنامه	۴. لایه‌ها
یک چیز را تغییر دهید، آزمایش کنید، نتیجه را بنویسید	۵. هر بار یک فرضیه
با کاربر تأیید کنید؛ لاگ‌ها را زیر نظر داشته باشید	۶. اصلاح و تأیید
علت، راه حل، پیشگیری — برای دفعه بعد	۷. مستند کنید

جعبه ابزار، لایه به لایه

ابزارها	لایه
Test-NetConnection -Port، Get-NetIPConfiguration، Get-NetTCPConnection	شبکه
Resolve-DnsName -Server، dcdiag /test:dns، ipconfig /flushdns	DNS
dcdiag، repadmin /replsummary، nltest /dsgetdc، Test-ComputerSecureChannel	Active Directory
gpresult /r، /h، Get-GPResultantSetOfPolicy	Group Policy
Get-WinEvent، Get-Service، لاگ‌های IIS، Restart-Service	سرویس‌ها و برنامه‌ها
Get-Counter، Get-HotFix، Reliability Monitor، sfc /scannow، DISM	سیستم

Azure Arc: مدیریت ترکیبی

چه چیزی بدانید	موضوع
سرورهای داخلی شما را به عنوان منابع قابل مدیریت در Azure نشان می‌دهد	چیست
ویزارد Azure Arc Setup در Windows Server 2025، یا azcmagent connect	اتصال
Azure Update Manager و Hotpatch (درس ۱۱)	آپدیت‌ها
Microsoft Defender for Cloud، Azure Policy، guest configuration	امنیت
Azure Monitor: معیارها، لاگ‌ها، هشدارها	نظارت
لایسنس اختیاری Windows Server با پرداخت ماهانه	لایسنس

اتصال یک سرور به Azure Arc

```
# Option 1: Windows Server 2025 – Azure Arc Setup (system tray icon or Server Manager)

# Option 2: the Connected Machine agent (values come from your Azure subscription)
C:\> azcmagent connect --resource-group "rg-lab-servers" --location "westus2" ^
      --subscription-id "<subscription-id>" --tenant-id "<tenant-id>"
C:\> azcmagent show                    # status: Connected
C:\> azcmagent check                   # network connectivity to Azure

# Then in the Azure portal > Azure Arc > Machines > SRV01:
#   Updates (Azure Update Manager), Hotpatch, Insights, Defender for Cloud
```

Resource group و region مثال هستند؛ از مقادیر subscription خودتان استفاده کنید.

مهاجرت از Windows Server قدیمی

سرویس	مسیر توصیه‌شده
Active Directory	DC های 2025 اضافه کنید ← نقش‌های FSMO را منتقل کنید ← DC های قدیمی را تنزل دهید ← سطح‌ها را بالا ببرید
File server ها	Storage Migration Service (در Windows Admin Center)؛ مسیرهای DFS
DHCP	Export-DhcpServer روی قدیمی ← Import-DhcpServer روی جدید ← مجاز کنید
DNS (ادغام‌شده با AD)	خودکار به DC های جدید کاپی می‌شود
سایت‌های IIS	Web Deploy، یا با اسکریپت دوباره بسازید و محتوا را کاپی کنید
VM های Hyper-V	Live migration یا export/import به میزبان‌های جدید
هر چیز دیگر	ارتقای در جا از 2012 R2 به بعد وقتی پشتیبانی می‌شود — بعد از بکاپ

مهاجرت در عمل: AD و DHCP

```
# New DC02 (2025) is already a DC (Lesson 4). Move all five FSMO roles to it:
PS C:\> Move-ADDirectoryServerOperationMasterRole -Identity DC02 -OperationMasterRole 0,1,2,3,4
C:\> netdom query fsmo

# Demote the old DC (run on the old DC):
PS C:\> Uninstall-ADDSDomainController -LocalAdministratorPassword (Read-Host -AsSecureString)

# DHCP: old server -> new server
PS C:\> Export-DhcpServer -ComputerName OLDDC -File C:\Migrate\dhcp.xml -Leases
PS C:\> Import-DhcpServer -ComputerName DC02 -File C:\Migrate\dhcp.xml -BackupPath C:\Migrate\Bak -
Leases
PS C:\> Add-DhcpServerInDC -DnsName dc02.lab.mywebuniversity.local ; Remove-DhcpServerInDC -DnsName
olddc.lab.mywebuniversity.local

# When ALL DCs run 2025:  Set-ADDomainMode / Set-ADForestMode (one way — back up first)
```

خلاصه دوره، پروژه نهایی و قدم‌های بعدی

- درس‌های ۱ تا ۳: نسخه‌ها، نصب، Server Core، مدیریت از راه دور
- درس‌های ۴ تا ۷: DNS، Group Policy، Active Directory و DHCP
- درس‌های ۸ تا ۱۰: خدمات فایل، ذخیره‌سازی، IIS، Hyper-V و RDS
- درس‌های ۱۱ و ۱۲: امنیت، آپدیت‌ها، بکاپ، نظارت، Azure Arc، مهاجرت
- پروژه نهایی: کل لابراتوار را با اسکریپت‌های خودتان دوباره بسازید و مستند کنید
- بعدی: امتحان AZ-802 (Windows Server Administrator Associate)؛ دوره‌های لینوکس ما

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