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**