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**