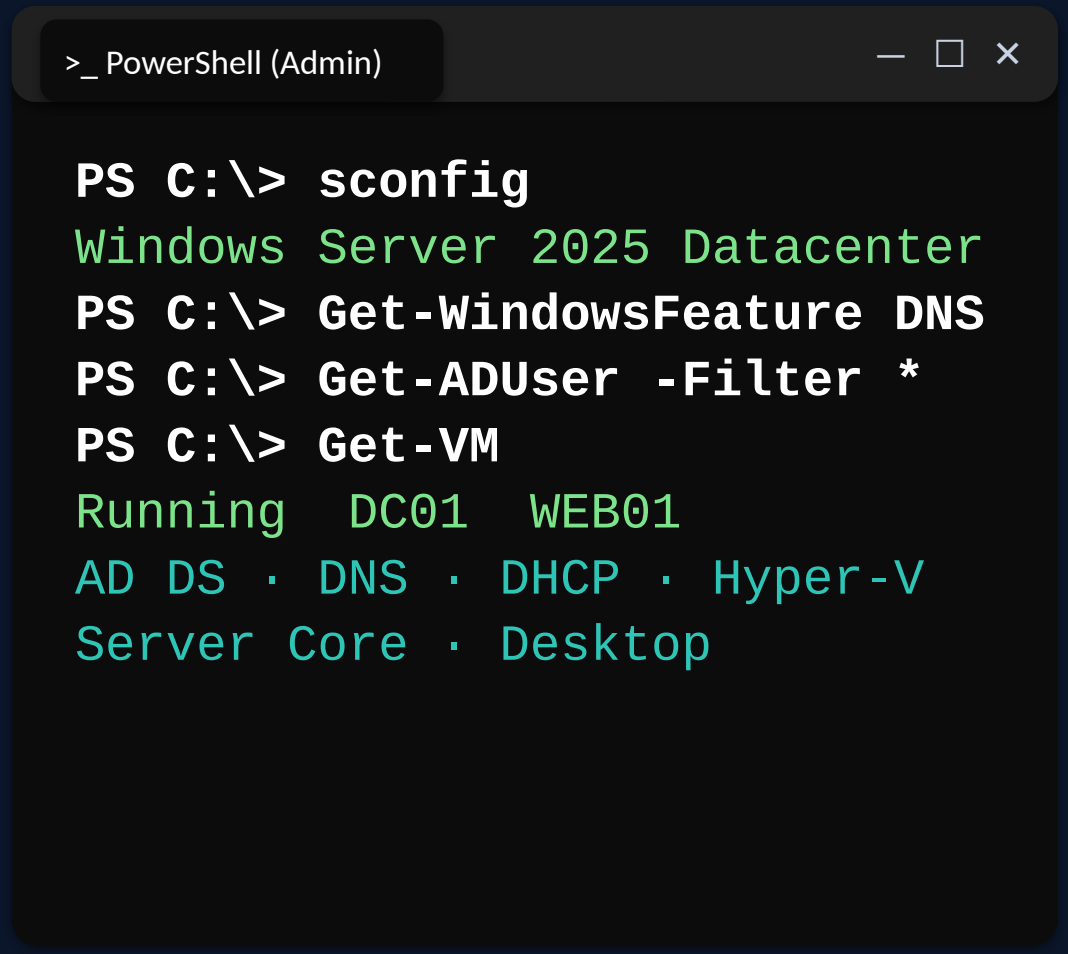


LESSON 4 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Active Directory Domain Services: Concepts & Your First Domain

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 4

- Active Directory concepts: forest, domain, OU, domain controller
- What AD gives you: single sign-on, Kerberos, Group Policy, DNS
- Planning: domain name, number of DCs, functional levels
- Promoting DC01: Install-ADDSForest
- Checking health: dcdiag, FSMO roles, DNS records
- Joining SRV01 and CL01 to the domain
- A second domain controller, replication and AD safety

Active Directory Concepts

Term	Meaning
Domain	A security boundary: users, groups and computers sharing one directory
Forest	One or more domains with a shared schema; the top of AD
Organizational Unit (OU)	A folder inside a domain for delegation and Group Policy
Domain controller (DC)	A server that holds a copy of the directory and signs users in
Global catalog	A searchable index of every object in the forest
Sites	Physical locations; control replication and which DC clients use
Schema	The definition of every object type and attribute

What Active Directory Gives You

Feature	Benefit
Single sign-on	One account opens computers, file shares, email and apps
Kerberos and LDAP	Secure authentication; a directory any app can query
Group Policy	Configure thousands of computers from one place (Lesson 6)
Central control	Disable one account and access ends everywhere
DNS integration	Clients find DCs automatically through DNS records
Hybrid identity	Sync to Microsoft Entra ID for Microsoft 365 and cloud apps

Planning Your Domain

Decision	Recommendation
Domain name	Production: a subdomain you own, e.g. ad.mywebuniversity.com
Lab name	lab.mywebuniversity.local is fine for this course
NetBIOS name	Short, 15 characters max: LAB
Domain controllers	At least two per domain, on different hosts
DNS	AD-integrated DNS on the DCs
Functional level	Highest level all your DCs support

Functional Levels

Level	Requires	Notes
Windows Server 2016	All DCs 2016 or newer	Most common today; many mixed environments
Windows Server 2025	All DCs Windows Server 2025	Newest level in 2025
32k database pages	2025 forest functional level	Optional feature; larger objects, cannot be undone
Raising levels	Set-ADDomainMode / Set-ADForestMode	One way — plan and back up first

Promote DC01: Your First Domain

```
# 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
```

Check the Health of Your Domain

```
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
```

FSMO Roles (Operations Masters)

Role	Scope	Job
Schema master	Forest	Changes to the schema
Domain naming master	Forest	Adding or removing domains
PDC emulator	Domain	Time source, password changes, account lockout
RID master	Domain	Hands out ID pools for new objects
Infrastructure master	Domain	Cross-domain references

Join SRV01 and the Windows 11 Client

```
# 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)
```

A Second Domain Controller and 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
```

Keeping Active Directory Safe

- Two or more DCs on different hosts; never a single point of failure
- Store the DSRM password in a safe, offline place
- Back up the System State of a DC regularly (Lesson 11)
- Do not restore old VM snapshots of DCs; use proper AD restore
- Only a few people in Domain Admins; use separate admin accounts
- Enable the AD Recycle Bin (Lesson 5)

Summary & Homework

- Forest > domain > OU; domain controllers hold and replicate the directory
- Install-WindowsFeature AD-Domain-Services, then Install-ADDSForest
- Check with Get-ADDomain, dcdiag /q, netdom query fsmo
- Clients must use the DC for DNS before Add-Computer
- Homework: build lab.mywebuniversity.local on DC01
- Homework: join SRV01 and CL01, and run dcdiag

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.