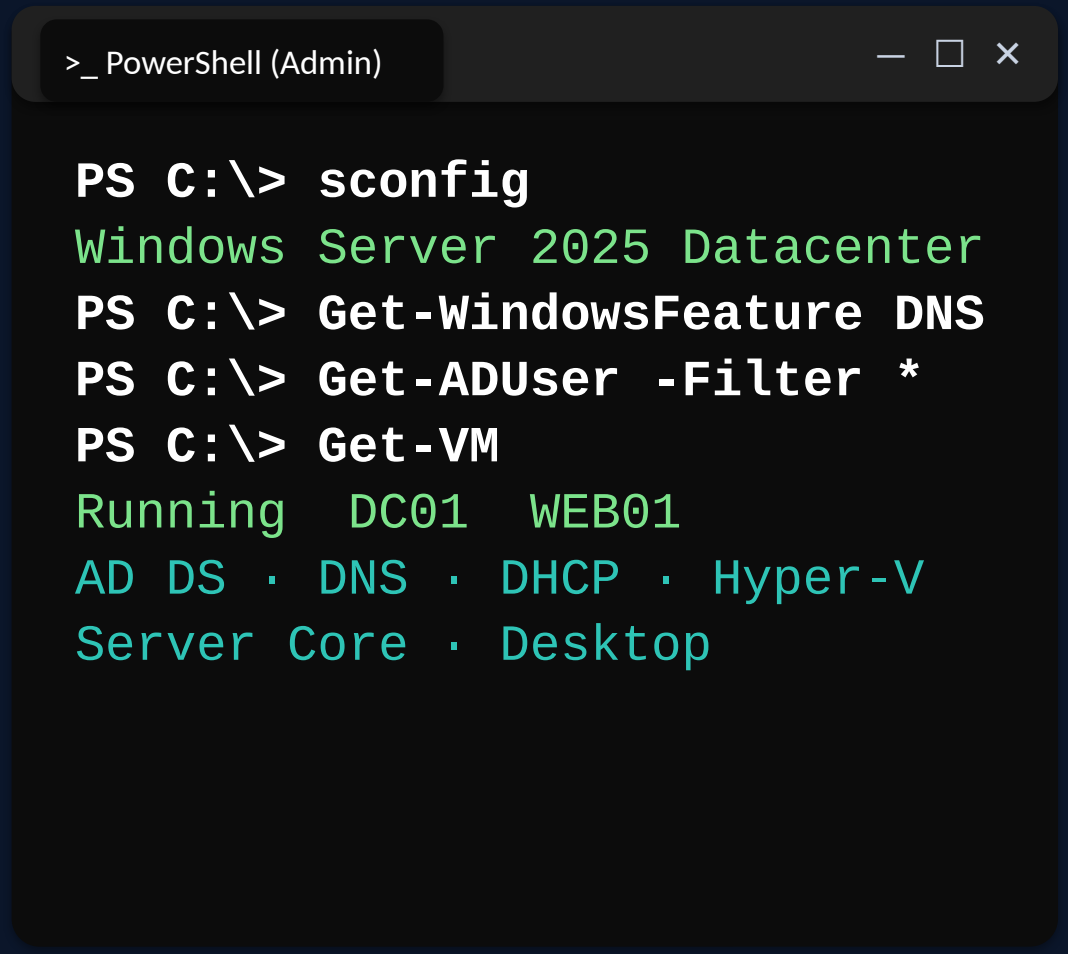


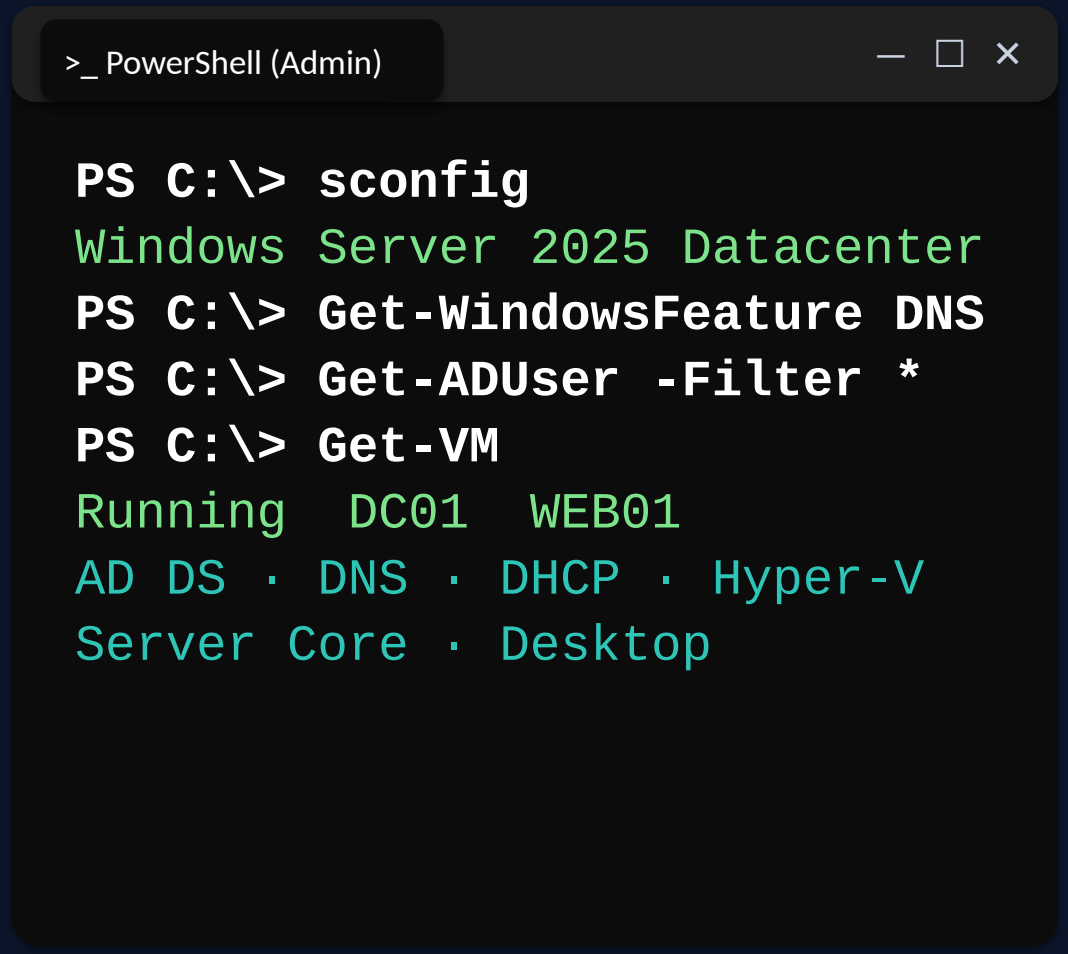
FULL COURSE · 12 LESSONS

Windows Server 2025

Install · AD · Hyper-V · Admin

Active Directory, Group Policy, DNS, DHCP, Hyper-V, IIS & Azure Arc

Full Course · Windows Server 2025 (build 26100)



LESSON 1 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Windows Server 2025: Editions, Licensing, Lifecycle & Lab

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 1

- What a server does, and a short history of Windows Server
- Support lifecycle: 2025 vs 2022, 2019 and 2016
- What's new in Windows Server 2025
- Editions: Standard, Datacenter, Datacenter: Azure Edition, Essentials
- Licensing basics: cores, CALs and pay-as-you-go
- Hardware requirements; Server Core vs Desktop Experience
- Your course lab: three virtual machines on Hyper-V

What Does a Windows Server Do?

Role	What it provides	Lesson
Active Directory (AD DS)	Central sign-in, users, groups, computers	4-6
DNS and DHCP	Names and IP addresses for the network	7
File server	Shared folders, permissions, quotas, DFS	8
Hyper-V host	Virtual machines	9
Web server (IIS)	Websites and web applications	10
Remote Desktop Services	Desktops and apps for many users	10
WSUS / Backup / Monitoring	Updates, protection, health	11-12

A Short History of Windows Server

1993	Windows NT 3.1 Advanced Server
2000	Windows 2000 Server: Active Directory arrives
2008	Server Core and Hyper-V
2012 R2	Storage Spaces, PowerShell everywhere, cloud-ready
2016	Containers, Nano Server, Shielded VMs
2019	Windows Admin Center, hybrid with Azure
2022	Secured-core server, TLS 1.3 by default
2025	Hotpatch, AD improvements, GPU partitioning

Support Lifecycle (Long-Term Servicing Channel)

Version	Mainstream support ends	Extended support ends
Windows Server 2025	Nov 13, 2029	Nov 14, 2034
Windows Server 2022	Ended Oct 13, 2026	Oct 14, 2031
Windows Server 2019	Ended Jan 2024	Jan 2029
Windows Server 2016	Ended Jan 2022	January 2027 (then paid ESU only)
Mainstream	Security + non-security fixes, features	
Extended	Security updates only	

What's New in Windows Server 2025

Area	Highlights
Updates	Hotpatch: security updates without restarts (Azure Arc)
Upgrades	In-place upgrade from 2012 R2 and later; also via Windows Update
Active Directory	New functional level, optional 32k database pages, stronger LDAP security
Accounts	Delegated Managed Service Accounts (dMSA)
Files	SMB over QUIC in all editions; SMB signing required by default
Hyper-V and storage	GPU partitioning, bigger VMs, faster NVMe storage

Editions Compared

Edition	Best for	Key points
Standard	Physical or lightly virtualized servers	Rights to 2 VMs per fully licensed host
Datacenter	Highly virtualized data centers	Unlimited VMs; Storage Spaces Direct, SDN
Datacenter: Azure Edition	Azure and Azure Local	Cloud-first features such as hotpatch on Azure
Essentials	Small businesses (from PC makers)	Up to 25 users / 50 devices; small servers

Licensing Basics

Concept	What to know
Core-based	License the physical cores: minimum 8 per processor, 16 per server
CALs	Each user or device that uses the server needs a Client Access License
RDS CALs	Extra licenses for Remote Desktop Services users
Virtualization	Standard: 2 VMs per licensed host; Datacenter: unlimited
Pay-as-you-go	Monthly billing through Azure Arc instead of buying licenses
Evaluation	Free 180-day evaluation ISO for learning and testing

Hardware Requirements (Minimum)

Item	Minimum	Recommended for the lab
Processor	1.4 GHz 64-bit, SSE4.2 and POPCNT	2+ virtual CPUs
Memory	512 MB (Server Core), 2 GB (Desktop Experience)	4 GB per VM
Storage	32 GB	60-80 GB per VM
Network	Gigabit Ethernet adapter	One internal lab switch
Firmware	UEFI; TPM 2.0 and Secure Boot for security features	Generation 2 VMs

Server Core vs Desktop Experience

	Server Core	Desktop Experience
Interface	Command line, sconfig, PowerShell	Full desktop, Server Manager
Size and updates	Smaller, fewer updates and restarts	Larger
Attack surface	Smaller — more secure	Larger
Managed by	Remotely: Windows Admin Center, RSAT, PowerShell	Locally or remotely
Choose it for	Domain controllers, DNS, Hyper-V, file servers	Learning, apps that need a GUI
Switch later?	No — choose at install time	No

Your Course Lab

VM	OS	Role in the course
DC01	Windows Server 2025, Server Core	Domain controller, DNS, DHCP
SRV01	Windows Server 2025, Desktop Experience	File server, IIS, WSUS, admin tools
CL01	Windows 11 Pro or Enterprise (evaluation)	Domain client for testing
Host	Windows 11 Pro/Enterprise or Windows Server with Hyper-V	16 GB RAM or more recommended
Network	Internal switch 'LabNet', 10.0.0.0/24	Domain: lab.mywebuniversity.local

Lab: Create the Network and VMs with 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
```

Download the 180-day evaluation ISO from the Microsoft Evaluation Center; your file name will differ.

Summary & Homework

- Windows Server 2025: released Nov 1, 2024; supported to Nov 14, 2034
- Standard (2 VMs) vs Datacenter (unlimited VMs); Essentials for small business
- Licensing: cores + CALs; free 180-day evaluation for learning
- Server Core for most infrastructure roles; Desktop Experience to learn
- Homework: download the evaluation ISO and a Windows 11 evaluation
- Homework: create LabNet, DC01 and SRV01 in Hyper-V

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

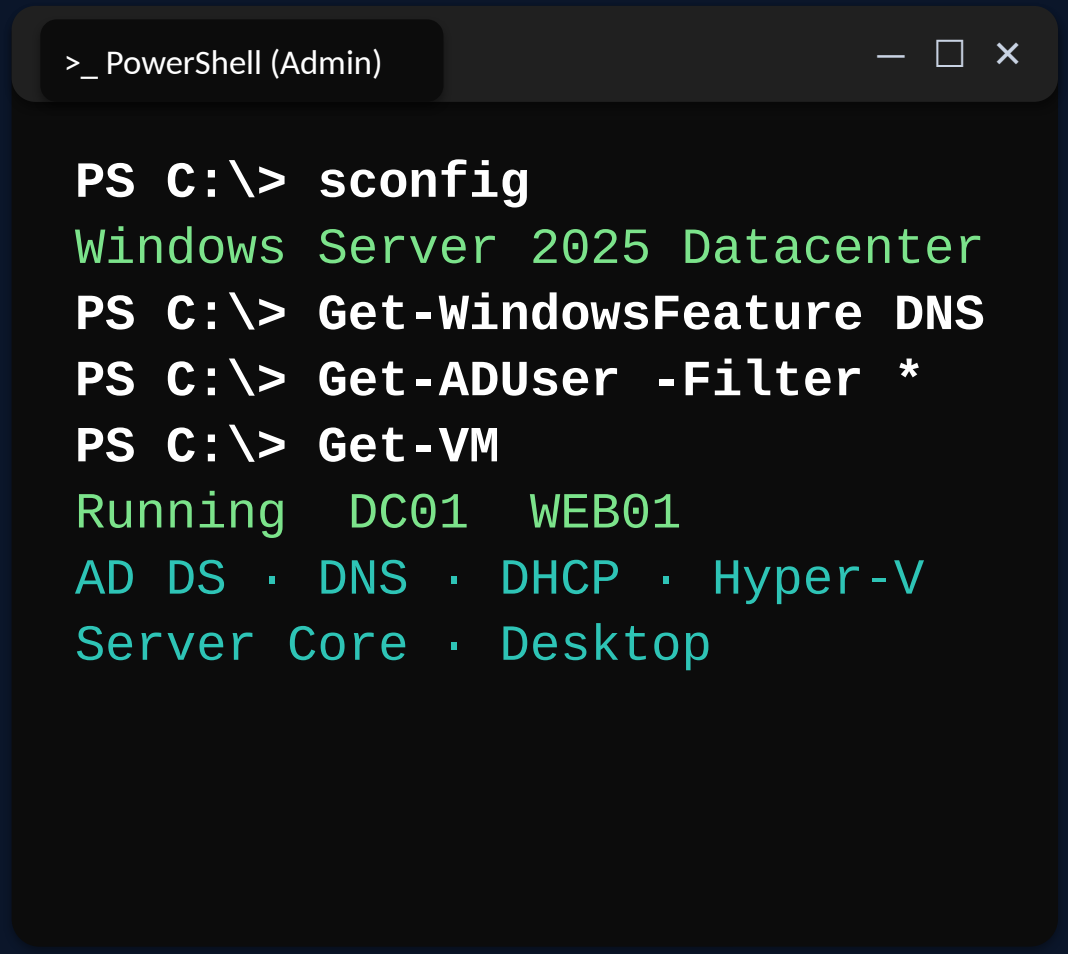
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 2 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Installing and First Configuration: Desktop Experience & Server Core

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 2

- Installing Windows Server 2025 step by step
- Server Core: the sconfig menu
- First configuration with PowerShell: name, IP, DNS, time zone
- Updates, activation, and converting an evaluation
- Upgrading older servers in place
- Living with Server Core: what is (and is not) there
- Lab: configure DC01 and SRV01 on the LabNet network

Installing Windows Server, Step by Step

Step	What you do
1. Boot	From the ISO or USB (generation 2 VM: DVD first)
2. Language	Language, time and keyboard, then 'Install Windows Server'
3. Edition	Standard or Datacenter — with or without 'Desktop Experience'
4. License	Accept the terms; evaluation needs no key
5. Disk	Choose the disk; Setup creates the partitions
6. Password	Set a strong password for the local Administrator

Server Core: The sconfig Menu

```
===============================================================
            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
```

First Configuration with 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
```

The First-Configuration Checklist

Item	Why it matters
Meaningful name	DC01, FS01, WEB01 — never the random WIN-xxxx name
Static IP + correct DNS	Clients and other servers must always find it
Time zone and time sync	Kerberos fails if clocks differ by more than 5 minutes
All updates installed	Before it goes into production
Activation	Evaluation expires after 180 days
Remote management + firewall	Manage it without sitting at the console
Document it	Name, IP, roles, owner, purpose

Updates, Activation and Converting an Evaluation

```
# 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
```

Upgrading Older Servers

Path	Notes
2012 R2, 2016, 2019, 2022 → 2025	In-place upgrade: up to four versions at once
Via Windows Update	Upgrade offer for eligible, managed servers
Via setup.exe	Mount the ISO, run setup.exe, choose 'Keep files, settings and apps'
Domain controllers	Best practice: add a NEW 2025 DC, move roles, retire the old one
Before any upgrade	Full backup, check app support, test in a lab, plan a rollback
Core vs Desktop	An upgrade keeps the same installation type

Living with Server Core

You still have	You do not have
PowerShell, cmd, sconfig	Start menu, File Explorer, Server Manager window
notepad, regedit, taskmgr, msinfo32	Most .msc consoles locally (use them remotely)
OpenSSH server (preinstalled)	Browser
Remote tools: Windows Admin Center, RSAT	A desktop to click around
App Compatibility FOD (optional)	— it adds Explorer, mmc and more tools

Handy Server Core Commands

```
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
```

Lab: Configure DC01 (Core) and 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?
```

Use your own time zone; DC01 points DNS to itself because it becomes the DNS server in Lesson 4.

Summary & Homework

- Choose the edition and installation type carefully — you cannot switch later
- sconfig or PowerShell: name, static IP, DNS, time zone, updates
- slmgr /dlv for license status; DISM /Set-Edition converts an evaluation
- In-place upgrade from 2012 R2+; new DCs instead of upgrading old ones
- Homework: install DC01 (Core) and SRV01 (Desktop) and configure both
- Homework: write your first-configuration steps as a .ps1 script

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

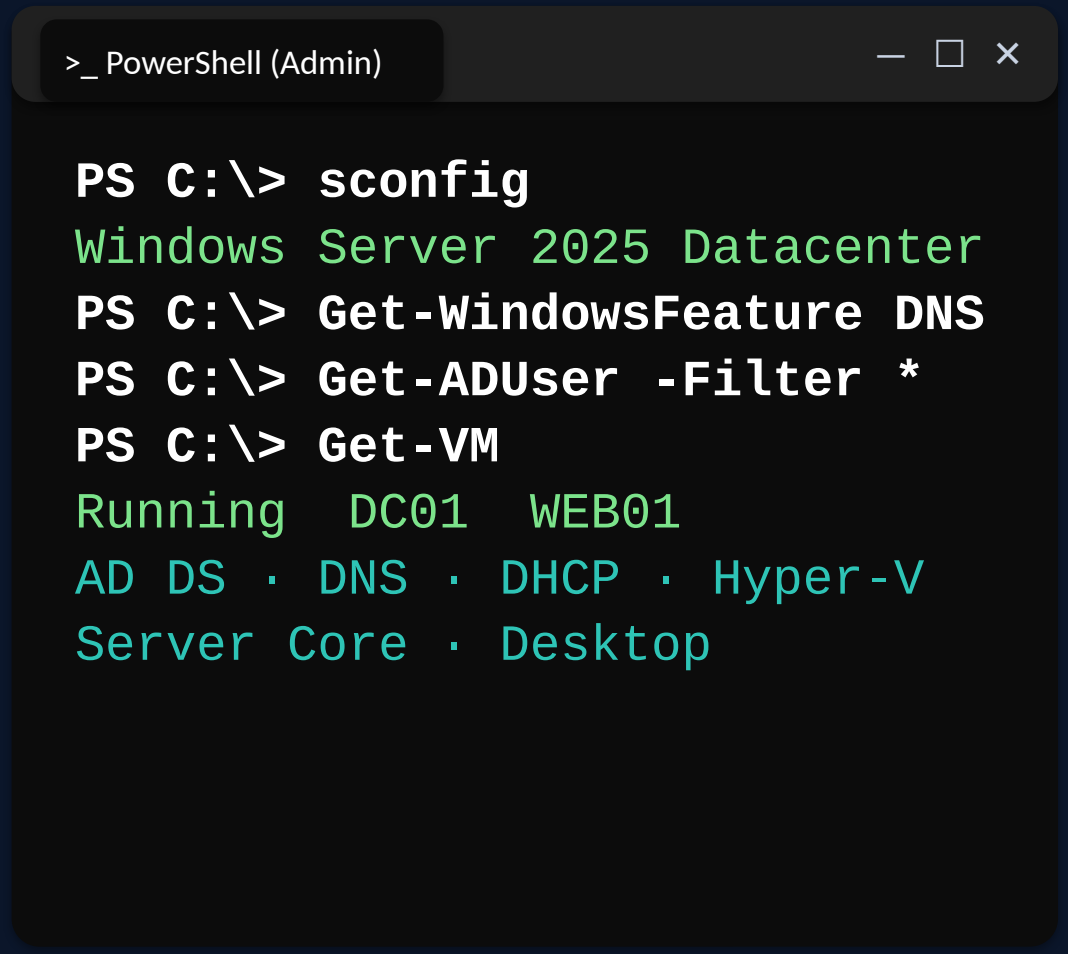
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 3 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Server Manager, Windows Admin Center & PowerShell Remoting

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 3

- The management toolbox: local, remote, graphical and command line
- Server Manager: dashboard, server groups, roles and features
- Installing roles and features with PowerShell
- Windows Admin Center: browser-based management
- RSAT: server tools on your Windows 11 workstation
- PowerShell Remoting: Enter-PSSession, Invoke-Command, sessions
- Remoting in a workgroup lab, SSH remoting and safe practices

The Management Toolbox

Tool	Type	Best for
Server Manager	GUI, on Desktop Experience	Roles, features, managing a few servers
Windows Admin Center	Browser-based, free	Server Core and modern remote management
RSAT (on Windows 11)	MMC consoles + PowerShell modules	AD, DNS, DHCP, GPO from your workstation
PowerShell Remoting	Command line, WinRM	Automation, many servers at once
OpenSSH	Command line, SSH	Cross-platform admins, Linux habits
Remote Desktop	Full desktop session	When you truly need the GUI

A Tour of Server Manager

Area	What it does
Dashboard	Health tiles: events, services, performance, best practices
Local Server	Name, IP, updates, firewall, Remote Desktop, time zone
All Servers	Every server you added; right-click to manage
Manage > Add Servers	Add DC01 and other servers to manage remotely
Manage > Add Roles and Features	The installation wizard
Tools menu	Every console: AD, DNS, DHCP, Hyper-V, IIS, Event Viewer

Roles and Features with 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

Topic	What to know
What	Free, browser-based management for Windows Server and Windows 11
Install	On a Windows Server (gateway) or your Windows 11 workstation
Connect	https://<gateway> — add servers by name; uses your credentials
Tools	Overview, Files, Events, Services, Updates, Firewall, Certificates, PowerShell
Roles	Hyper-V, Storage, Active Directory, DNS, DHCP and more with extensions
Azure	Connect to Azure Arc, Azure Backup, Azure Monitor

RSAT on 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
```

How PowerShell Remoting Works

Topic	Details
Protocol	WinRM (WS-Management): HTTP 5985, HTTPS 5986
On servers	Enabled by default; Enable-PSRemoting on clients
In a domain	Kerberos authentication — just works by name
In a workgroup	Add servers to TrustedHosts, use -Credential
Security	Traffic is encrypted; only administrators can connect by default
Alternative	PowerShell 7 over SSH: Enter-PSSession -HostName

PowerShell Remoting in Practice

```
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
```

Lab: Remoting Before the Domain Exists

```
# 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
```

Remote Management Safely

Practice	Why
Separate admin accounts	Your daily account is not a domain admin
Manage from a secure workstation	Not from the same PC you browse and email on
Least privilege / JEA	Just Enough Administration limits what a remote user can run
Logging	Turn on PowerShell script block logging and transcripts
Firewall scope	Allow WinRM, RDP and SSH only from admin networks
No RDP from the internet	Use a VPN, Azure Bastion or a gateway

Summary & Homework

- Server Manager for a few servers; Windows Admin Center for Core and the browser
- Install-WindowsFeature -IncludeManagementTools [-ComputerName]
- RSAT brings AD, DNS, DHCP and GPO tools to Windows 11
- Enter-PSSession for one server; Invoke-Command for many
- Homework: add DC01 to Server Manager on SRV01
- Homework: run one Invoke-Command against both servers

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

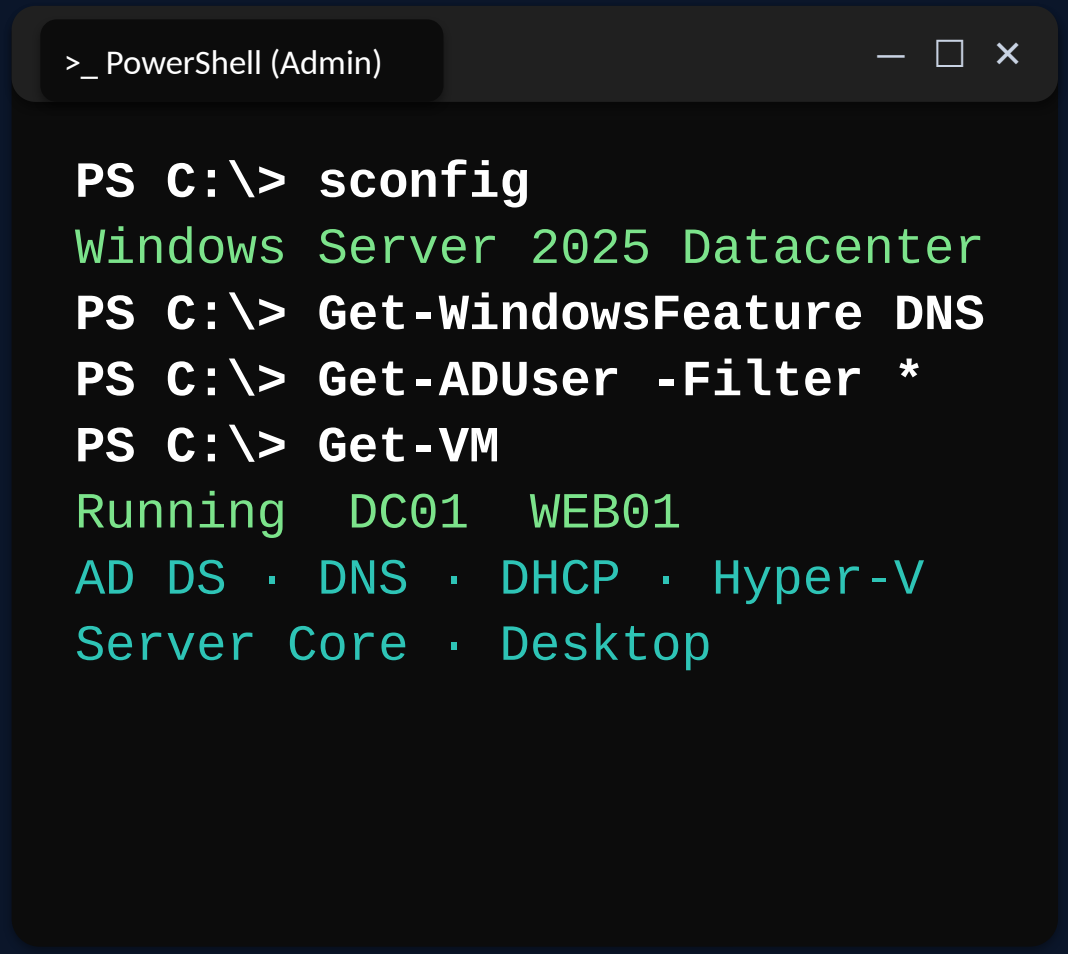
Slides for this lesson: MyWebUniversity.com/presentations

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.



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

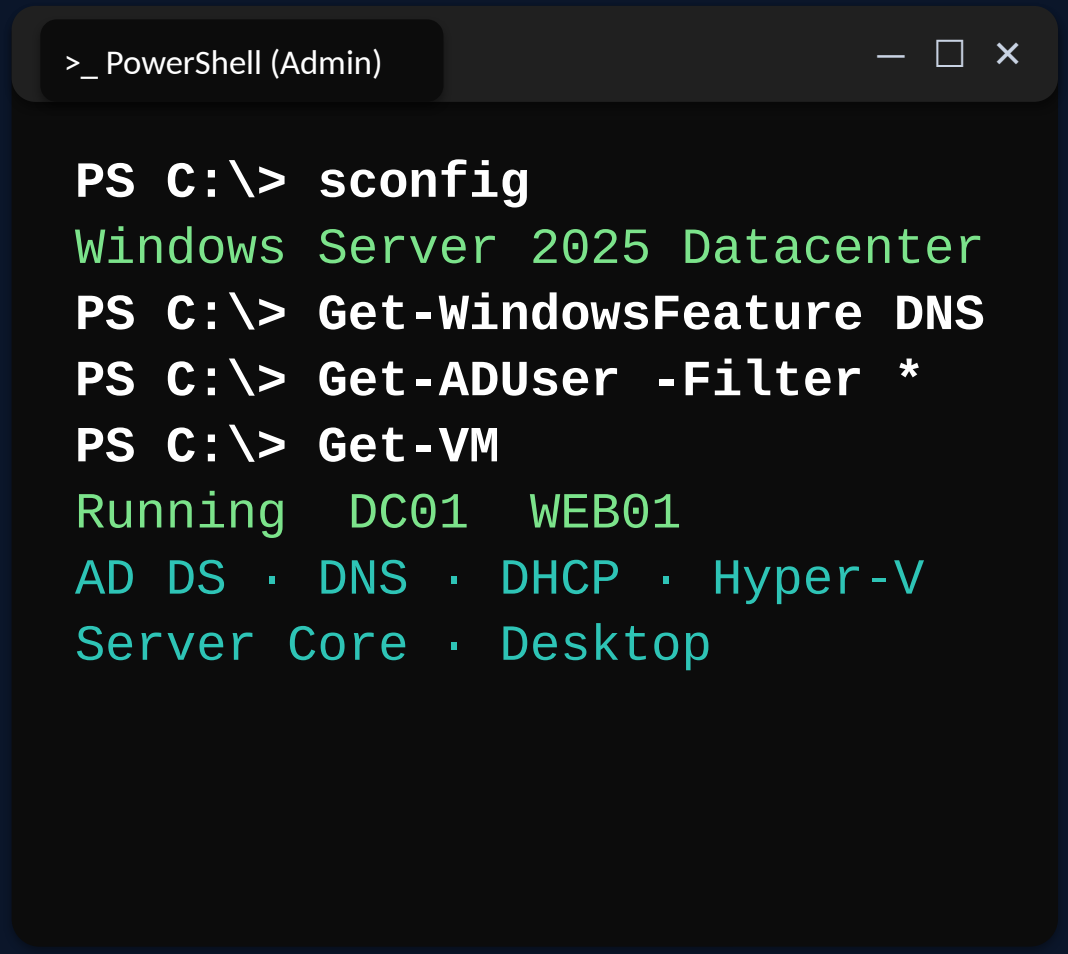
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 5 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Managing Active Directory: Users, Groups, OUs & Delegation

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 5

- The AD management tools: ADUC, ADAC and the ActiveDirectory module
- Designing organizational units
- Users: create, find, change, disable, unlock and reset
- Bulk user creation from a CSV file
- Groups: scopes, types and the AGDLP strategy
- Computer accounts and stale-account cleanup
- Delegation, the AD Recycle Bin, password policies and Windows LAPS

Active Directory Management Tools

Tool	Command	Best for
AD Users and Computers	dsa.msc	Classic daily work; Delegation wizard
AD Administrative Center	dsac.exe	Recycle Bin, password policies, PowerShell history
ActiveDirectory module	Get-ADUser, New-ADUser …	Automation and bulk changes
Windows Admin Center	Browser	Quick user and group tasks
Sites and Services / Domains and Trusts	dssite.msc / domain.msc	Replication, trusts

Designing Organizational Units

OU path	Contains	Why
LAB > Staff > Teachers	Teacher user accounts	Teacher policies, delegated to the principal
LAB > Staff > Students	Student accounts	Help desk can reset passwords here
LAB > Computers > Workstations	Classroom and office PCs	Workstation GPOs, LAPS
LAB > Computers > Servers	Member servers	Server security GPOs
LAB > Groups	Security and distribution groups	Easy to find and manage
LAB > Admins	Separate admin accounts	Extra protection

Create the OU Structure

```
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
```

Users: Create, Find, Change

```
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'
```

Daily Help-Desk Tasks

```
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
```

Bulk Users from a CSV File

```
# 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
```

Groups: Scopes, Types and AGDLP

Concept	Meaning
Security group	Used for permissions (and email if mail-enabled)
Distribution group	Email lists only — no permissions
Global	Members from its own domain; used to group people by role
Domain local	Used to grant permissions on resources in its domain
Universal	Members from any domain in the forest; multi-domain forests
AGDLP	Accounts → Global groups → Domain Local groups → Permissions

Groups with 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')
```

Delegation, Recycle Bin, Password Policies, LAPS

Feature	How
Delegate control	dsa.msc > right-click OU > Delegate Control (e.g., reset passwords in Students)
AD Recycle Bin	Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet
Restore an object	Get-ADObject -Filter … -IncludeDeletedObjects | Restore-ADObject
Fine-grained passwords	New-ADFineGrainedPasswordPolicy for admins or service accounts
Windows LAPS	Unique rotating local admin passwords, stored in AD
dMSA / gMSA	Managed service accounts: Windows rotates service passwords

Lab: Recycle Bin and 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
```

Summary & Homework

- Design OUs for delegation and Group Policy
- New-ADUser, Set-ADUser, Search-ADAccount, Unlock-ADAccount
- Bulk changes: Import-Csv | ForEach-Object { … -WhatIf }
- AGDLP: accounts → global → domain local → permissions
- Homework: build the LAB OUs and import 10 students from CSV
- Homework: enable the Recycle Bin and restore a deleted user

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

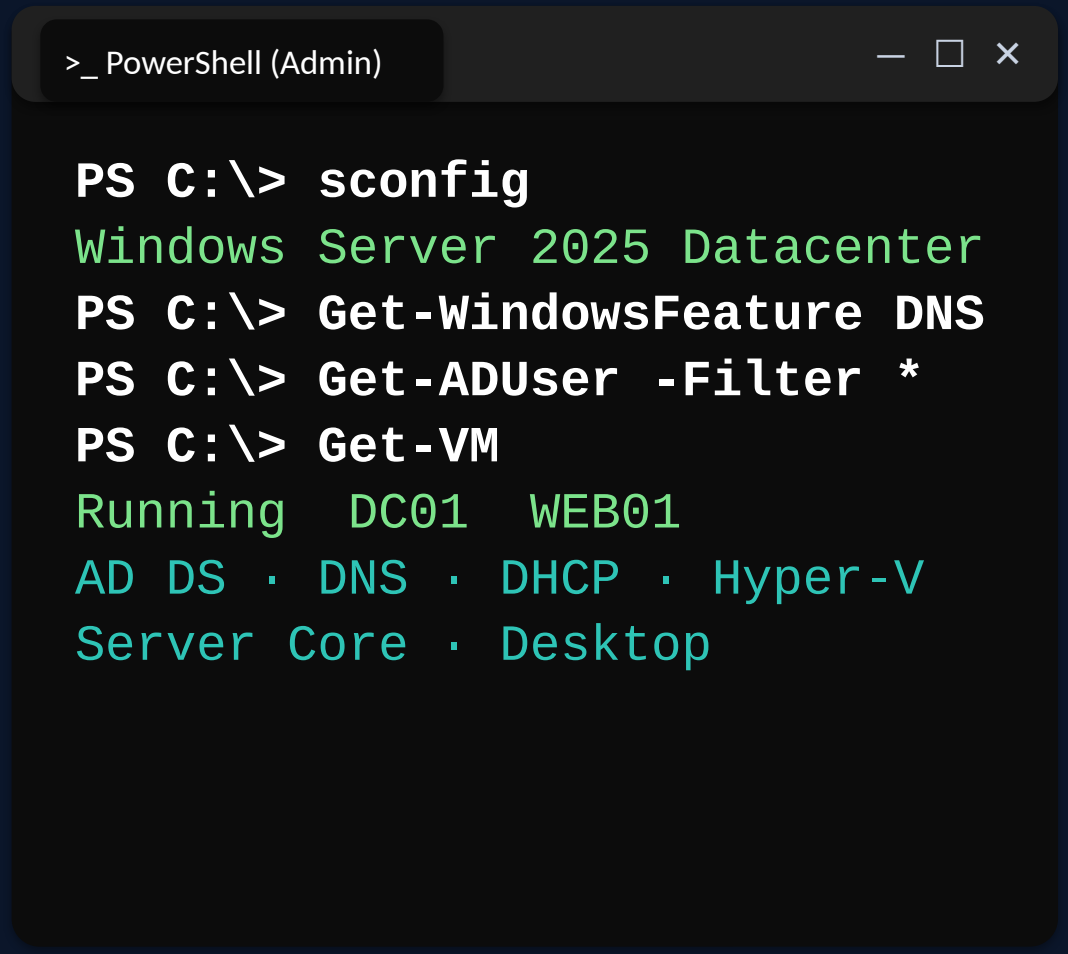
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 6 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Group Policy in the Domain

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 6

- Group Policy Objects: computer vs user settings, policies vs preferences
- Where GPOs apply: sites, domain, OUs — and the LSDOU order
- Inheritance, Block Inheritance, Enforced and security filtering
- Creating and linking GPOs in GPMC and PowerShell
- Useful GPOs: security, drive maps, updates, USB, LAPS
- Troubleshooting with gpresult and RSoP
- Backups, the central store and best practices

Group Policy Concepts

Concept	Meaning
GPO	A Group Policy Object: a named set of settings
Computer Configuration	Applies to computers, at startup and every refresh
User Configuration	Applies to users, at sign-in and every refresh
Policies	Enforced settings; users cannot change them
Preferences	Default settings users may change: drives, printers, shortcuts
Administrative Templates	ADMX files describing registry-based settings
Link	Connects a GPO to a site, the domain, or an OU

Order of Processing: LSDOU

Order	Level	Example
1	Local	The computer's own local policy
2	Site	Rarely used; location-based settings
3	Domain	Default Domain Policy: passwords, lockout
4	OU (parent → child)	LAB → Computers → Workstations
Rule	Last applied wins	A child OU setting overrides the domain setting
Exceptions	Enforced; Block Inheritance	Enforced beats Block Inheritance

Filtering and Refresh

Topic	What to know
Security filtering	Apply a GPO only to members of a group (Authenticated Users by default)
WMI filtering	Apply only if a query is true, e.g., only laptops or only Windows 11
Item-level targeting	Preferences only: target a group, OS, IP range, and more
Refresh interval	Every 90 minutes ± 30 for members; every 5 minutes on DCs
Some settings	Software install, folder redirection: only at restart or sign-in
Force now	gpupdate /force, or Invoke-GPUpdate from the server

Create and Link GPOs with 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
```

Useful GPOs for a School or Office

GPO	Where in the editor
Password and lockout	Default Domain Policy > Computer > Policies > Windows Settings > Security
Map drive S:	User > Preferences > Windows Settings > Drive Maps (target a group)
Block USB storage	Computer > Admin Templates > System > Removable Storage Access
Windows Update	Computer > Admin Templates > Windows Components > Windows Update
Windows LAPS	Computer > Admin Templates > System > LAPS
Defender, firewall, BitLocker	Computer > Admin Templates > Windows Components / Windows Settings > Security

Lab: Central Store, LAPS Policy and a 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
```

Troubleshooting 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?
```

Back Up, Report and Restore GPOs

```
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
```

Group Policy Best Practices

- Leave the Default Domain Policy for passwords and lockout only
- One purpose per GPO, with clear names: 'WS - …', 'USR - …', 'SRV - …'
- Link to OUs, not the domain, whenever possible
- Test on a TEST OU first, then link to production
- Avoid Block Inheritance and Enforced unless you must
- Back up weekly; start from Microsoft security baselines

Summary & Homework

- GPO = computer half + user half; policies enforce, preferences suggest
- LSDOU: last applied wins; Enforced and Block Inheritance are exceptions
- New-GPO, Set-GPRegistryValue, New-GPLink, Get-GPInheritance
- Troubleshoot with gpresult /r, /h and the GroupPolicy log
- Homework: create the central store, LAPS GPO and S: drive map
- Homework: back up all GPOs and create an HTML report

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

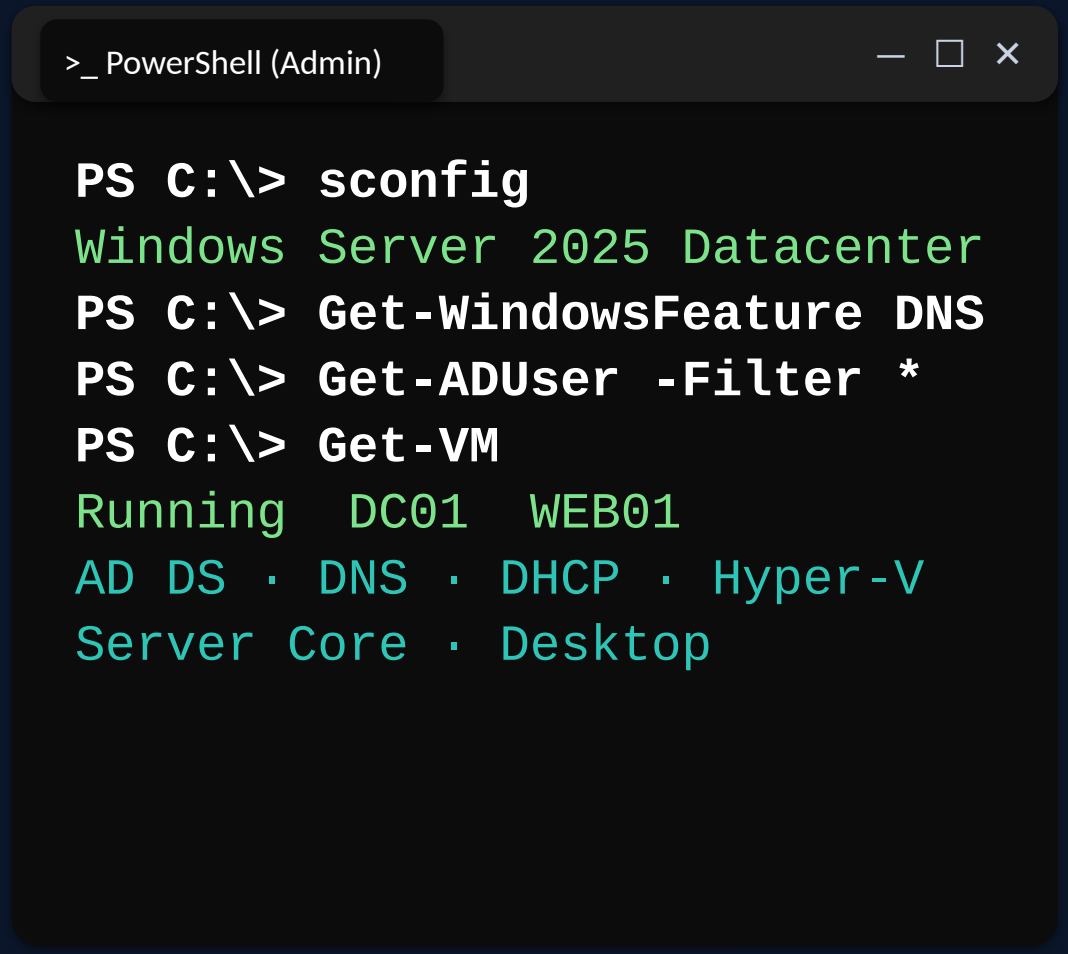
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 7 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

DNS and DHCP Servers

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 7

- DNS concepts: zones, records, forwarders and AD-integrated DNS
- Managing DNS with PowerShell: zones, A, PTR, CNAME records
- Troubleshooting name resolution
- Securing DNS
- DHCP concepts: DORA, scopes, options, reservations
- Installing, authorizing and configuring DHCP
- DHCP failover and troubleshooting

DNS Concepts

Term	Meaning
Forward lookup zone	Name → IP, e.g. lab.mywebuniversity.local
Reverse lookup zone	IP → name, e.g. 0.0.10.in-addr.arpa
AD-integrated zone	Stored in AD; replicated to DCs; secure dynamic updates
Records	A / AAAA (IP), CNAME (alias), MX (mail), PTR (reverse), SRV (services), TXT
Forwarders	Where the server sends internet queries it cannot answer
Conditional forwarder	Send one domain's queries to a specific server (partner company)
Scavenging	Removes stale dynamic records automatically

Manage DNS with 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
```

Troubleshooting Name Resolution

```
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
```

Securing DNS

Practice	Why
Secure dynamic updates only	Only domain members can register records
Do not be an open resolver	Never answer recursive queries from the internet
Scavenging on	Stale records cause wrong answers and confusion
DNSSEC (where needed)	Signs zones so answers cannot be forged
Logging	Enable analytical/audit logs to investigate problems
Limit zone transfers	Only to listed secondary servers

DHCP Concepts

Term	Meaning
DORA	Discover, Offer, Request, Acknowledge — how a client gets an address
Scope	A range of addresses for one subnet, e.g. 10.0.0.100-200
Exclusions	Addresses in the range that DHCP must not hand out
Reservations	Always give the same IP to one device (by MAC address)
Options	003 router, 006 DNS servers, 015 DNS domain name
Lease	How long a client may keep its address (default 8 days)
Authorization	In a domain, a DHCP server must be authorized in AD to run

Install, Authorize and Configure 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
```

Test with the Client, and Watch the Leases

```
# 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 for High Availability

```
# 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
```

Troubleshooting DHCP

Symptom	Likely cause and fix
Client has 169.254.x.x	No DHCP answer: server down, not authorized, scope full, network/VLAN
Server will not hand out	Not authorized in AD (Add-DhcpServerInDC); service stopped
Wrong DNS or router	Check scope/server options; renew the client
Clients on another subnet	Router needs a DHCP relay (IP helper) pointing to the server
Address conflicts	Static IP inside the scope — exclude it, or set conflict detection
Unknown DHCP server	Rogue router or device on the network — find and remove it

Summary & Homework

- AD-integrated zones, secure dynamic updates, forwarders, scavenging
- Add-DnsServerResourceRecordA -CreatePtr; Resolve-DnsName -Server
- Domain members use only your DCs for DNS
- DHCP: authorize, scope, exclusions, options 003/006/015, reservations
- Homework: create the reverse zone, web A record and intranet CNAME
- Homework: build the LabNet DHCP scope and get CL01 an address

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

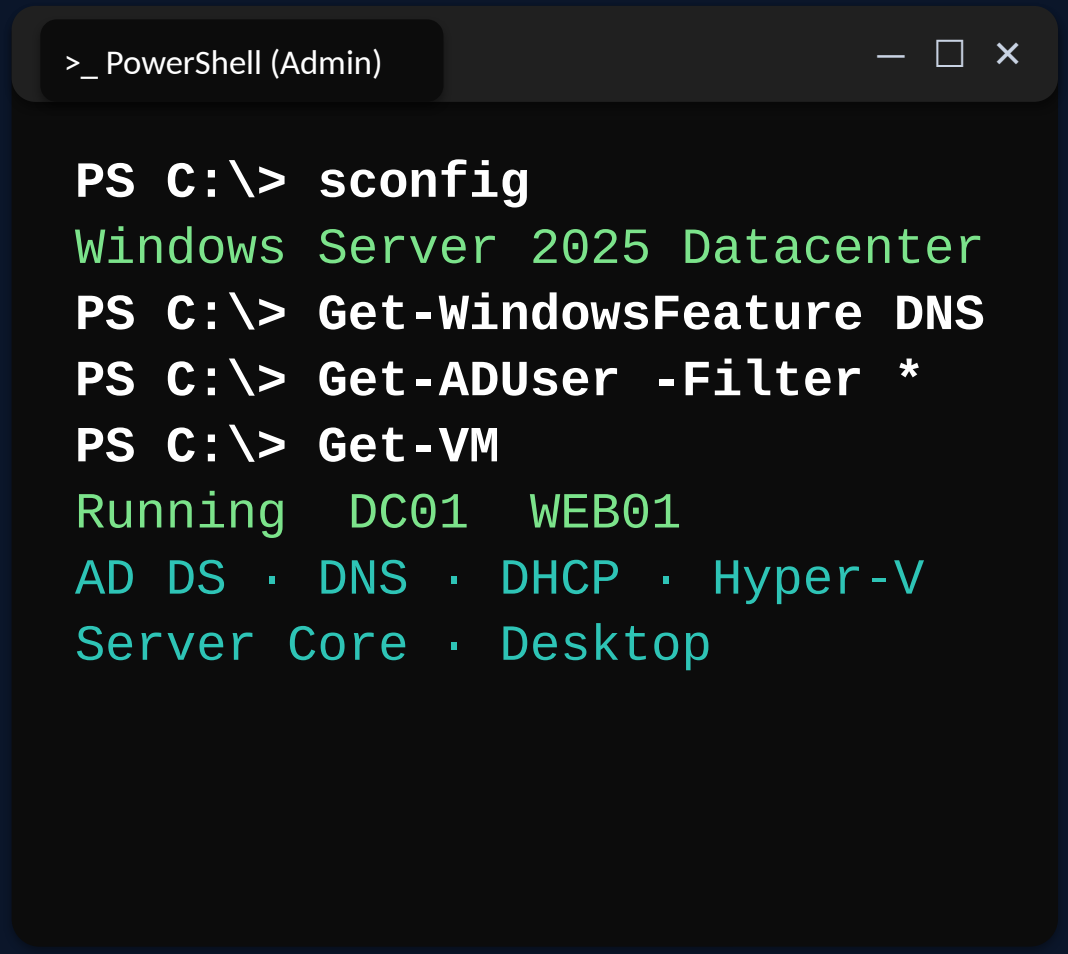
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 8 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

File Services and Storage: SMB, DFS, Storage Spaces & ReFS

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 8

- File server roles and features
- Creating SMB shares, and the share + NTFS permission model
- SMB security in Windows Server 2025
- DFS Namespaces and DFS Replication
- File Server Resource Manager: quotas and file screens
- Shadow copies (Previous Versions)
- Storage Spaces, ReFS and data deduplication

File Server Roles and Features

Feature	Name for Install-WindowsFeature	Purpose
File Server	FS-FileServer	SMB shares
DFS Namespaces	FS-DFS-Namespace	One path for shares on many servers
DFS Replication	FS-DFS-Replication	Keep folders in sync between servers
File Server Resource Manager	FS-Resource-Manager	Quotas, file screens, reports
Data Deduplication	FS-Data-Deduplication	Store repeated data only once
iSCSI Target Server	FS-iSCSITarget-Server	Offer disks over the network

Create the Teachers and Students Shares

```
# 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
```

NTFS Permissions with 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
```

SMB Security in Windows Server 2025

Feature	What it does
SMB signing required	On by default: protects against tampering and relay attacks
SMB encryption	Encrypt a share or the whole server (SMB 3)
SMB over QUIC	Secure file access over the internet without a VPN — in all editions
SMB1	Removed — never reinstall it
Access-based enumeration	Users see only folders they can open
Auditing	Track who opened, changed or deleted files

Inspect and Harden 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: One Path for Everything

```
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
```

FSRM Quotas, File Screens and Shadow Copies

```
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 and Deduplication

Feature	What it gives you
Storage pool	Combine many physical disks into one pool
Virtual disk resiliency	Simple (no protection), Mirror (copies), Parity (space-efficient)
ReFS	Resilient File System: integrity checks, great for Hyper-V and backup data
Data Deduplication	Saves 30-90% on file shares, VDI and backups
Storage Spaces Direct	Datacenter: pool local disks of a cluster (hyper-converged)
NVMe	Faster NVMe storage performance in 2025

Lab: A Mirrored ReFS Volume with 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
```

Summary & Homework

- Share permissions broad; real control with NTFS and AGDLP groups
- SMB signing on by default; encrypt sensitive shares; SMB1 never
- DFS Namespaces: one domain path; servers can change behind it
- FSRM quotas and file screens; shadow copies for self-service restore
- Storage Spaces mirror + ReFS + deduplication for resilient storage
- Homework: build the Teachers/Students shares, DFS and a quota

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

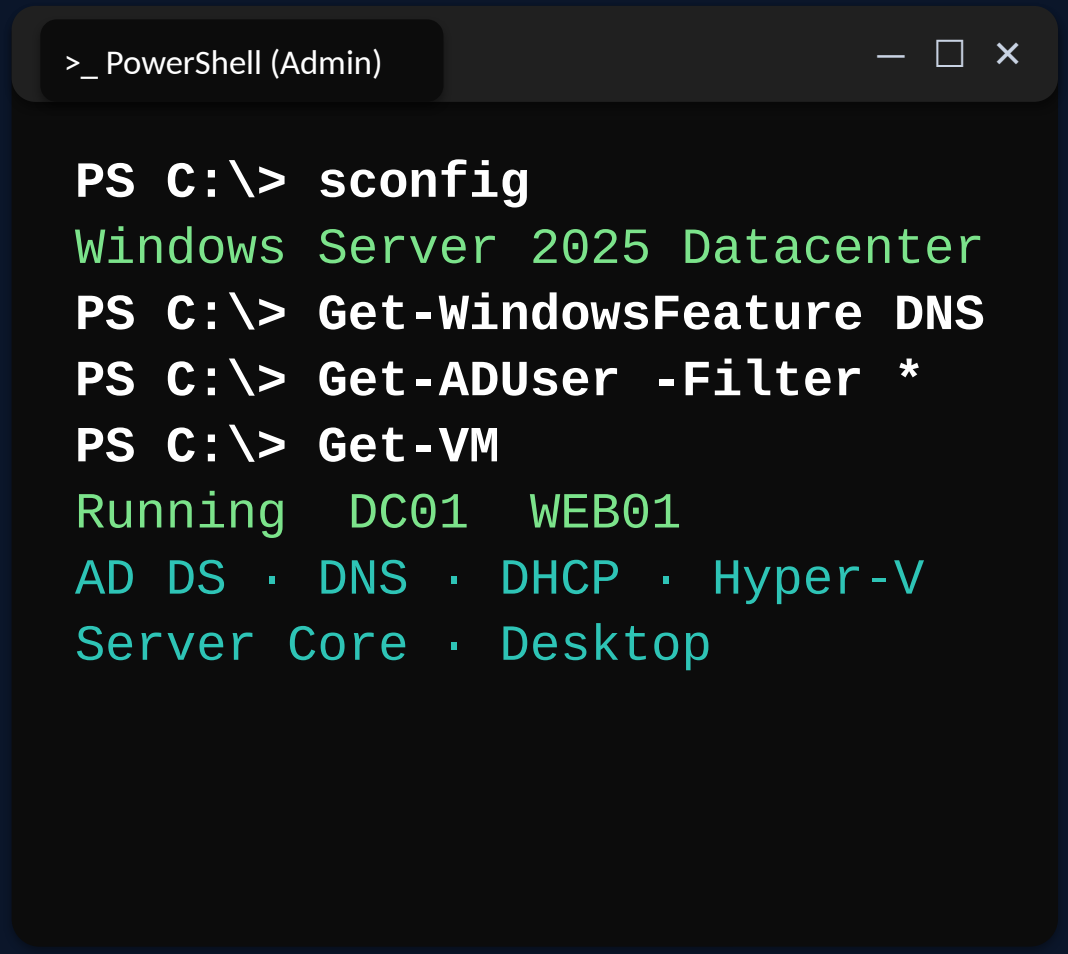
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 9 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Hyper-V on Windows Server

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 9

- Hyper-V concepts: generations, VHDX disks, switches, dynamic memory
- What's new in Hyper-V on Windows Server 2025
- Installing Hyper-V (and nested virtualization for the lab)
- Virtual switches and creating VMs with PowerShell
- Templates with sysprep and differencing disks
- Checkpoints, export/import and PowerShell Direct
- Live migration, Hyper-V Replica and clustering

Hyper-V Concepts

Term	Meaning
Hypervisor (type 1)	Runs directly on hardware; Windows becomes the parent partition
Generation 2 VM	UEFI, Secure Boot, virtual TPM — use it for all modern guests
VHDX	Virtual disk: fixed, dynamically expanding, or differencing
Virtual switch	External (physical network), Internal (host + VMs), Private (VMs only)
Dynamic memory	Gives VMs memory as needed, between a minimum and maximum
Checkpoint	A point-in-time state of a VM — not a backup
Integration services	Drivers for time sync, shutdown, backup, file copy

Hyper-V in Windows Server 2025

Feature	Highlights
Scale	Up to 2,048 virtual CPUs and 240 TB of memory per generation 2 VM
GPU partitioning	Share one GPU among several VMs, with live migration and clustering
Workgroup clusters	Failover clusters without Active Directory (certificate-based)
Dynamic processor compatibility	Live-migrate between hosts with different CPU generations
Default	New VMs are generation 2 by default
Licensing reminder	Standard: 2 Windows Server VMs per licensed host; Datacenter: unlimited

Install Hyper-V (and Nested Virtualization for the Lab)

```
# 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 Switches and a New VM

```
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
```

Templates: sysprep and Differencing Disks

```
# 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
```

Checkpoints, Export and 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
```

High Availability for VMs

Feature	What it does
Live migration	Move a running VM to another host with no downtime
Storage migration	Move a running VM's disks to new storage
Hyper-V Replica	Asynchronous copy of a VM to another host or site, for disaster recovery
Failover clustering	VMs restart automatically on another node when a host fails
Storage Spaces Direct	Datacenter: hyper-converged storage for the cluster
Backup	Use Hyper-V-aware backup (Lesson 11), not checkpoints

Live Migration, Replica and Monitoring

```
# 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
```

Summary & Homework

- Generation 2 VMs, VHDX disks, the right switch type, dynamic memory
- Install-WindowsFeature Hyper-V; nested virtualization for labs
- New-VM, Set-VMMemory, Set-VMProcessor, Start-VM, vmconnect
- sysprep + templates; checkpoints are not backups
- PowerShell Direct: Enter-PSSession -VMName
- Homework: build WEB01 on SRV01 and take a checkpoint before Lesson 10

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

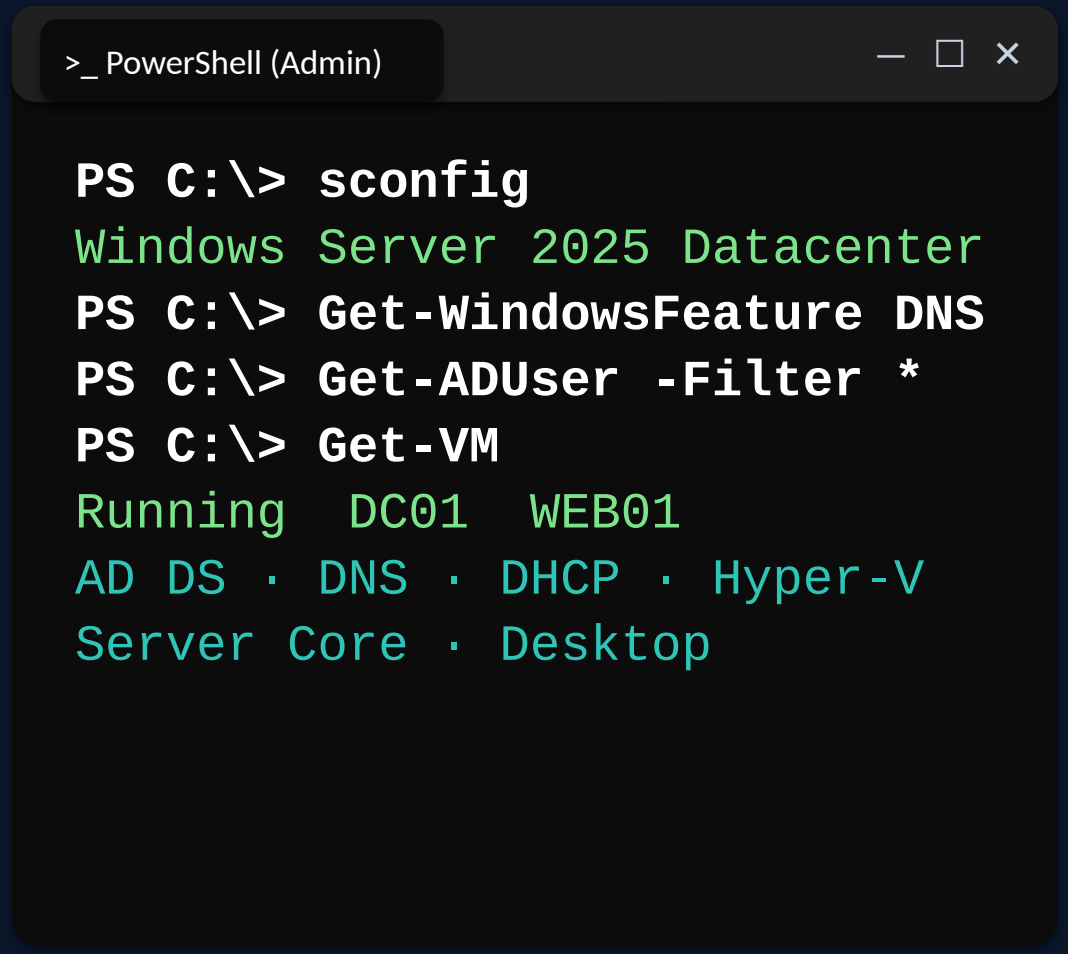
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 10 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Web Server (IIS), Remote Desktop Services & Remote Access

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 10

- IIS concepts: sites, bindings, application pools, logs
- Installing IIS and creating a website with PowerShell
- HTTPS bindings and certificates
- Application pools and IIS security
- Remote Desktop Services: roles, collections and RemoteApp
- Remote access: VPN, RD Gateway and SMB over QUIC
- A security checklist for anything facing the internet

IIS Concepts

Term	Meaning
Site	A website with its own folder, bindings and settings
Binding	Protocol + IP + port + host name, e.g. https *:443 intranet.lab…
Application pool	An isolated worker process (w3wp.exe) that runs one or more apps
Virtual directory / application	A folder or app inside a site
Physical path	Where the files live, e.g. C:\inetpub\intranet
Logs	C:\inetpub\logs\LogFiles — every request, status code, time

Install IIS and Create the Intranet Site

```
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
```

Add 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 Pools and IIS Security

Practice	Why
One app pool per application	Isolation: a crash or compromise stays contained
ApplicationPoolIdentity	Each pool runs as its own low-privilege virtual account
HTTPS only; redirect HTTP	Protects passwords and data in transit
Install only needed features	Fewer modules = smaller attack surface
Request filtering, logging	Block bad requests; investigate problems
Apps	ASP.NET Core Hosting Bundle; PHP/Python via FastCGI or HttpPlatformHandler

App Pools and Logs with 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
```

Remote Desktop Services (RDS)

Role	Job
RD Session Host	Runs the desktops and apps that many users share
RD Connection Broker	Sends users to the right host; reconnects sessions
RD Web Access	Web page listing published desktops and RemoteApps
RD Gateway	Secure HTTPS entry from the internet — no open port 3389
RD Licensing	Issues RDS CALs (120-day grace period to start)
VDI (alternative)	Each user gets their own VM instead of a shared session

Quick RDS Deployment and a 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
```

Remote Access: The Safe Options

Option	Best for	Notes
VPN (RRAS / Always On VPN)	Full network access for managed laptops	IKEv2 or SSTP; certificates; MFA
RD Gateway	Remote desktops and RemoteApps	HTTPS 443; add MFA
SMB over QUIC	File shares from anywhere	No VPN; certificate-based; all editions
Web apps behind a reverse proxy	Intranet sites	WAF, MFA, HTTPS
Never	Open RDP (3389) or SMB (445) to the internet	Attackers scan constantly

Checklist for Anything Facing the Internet

- HTTPS everywhere, with certificates from a trusted CA
- Multi-factor authentication on every external entry point
- Only ports 443 (and VPN ports) open; nothing else
- Patch monthly — internet-facing servers first
- Least privilege: app pool identities, no domain admins on web servers
- Logs collected centrally and reviewed (Lesson 12)

Summary & Homework

- IIS: sites, host-name bindings, one app pool per app, logs
- New-IISSite, New-IISSiteBinding -Protocol https, Get-IISAppPool
- RDS: Session Host, Broker, Web Access, Gateway, Licensing
- New-RDSessionDeployment, New-RDSessionCollection, New-RDRemoteApp
- Homework: build the HTTPS intranet site with its own app pool
- Homework: publish one RemoteApp and open it from CL01

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

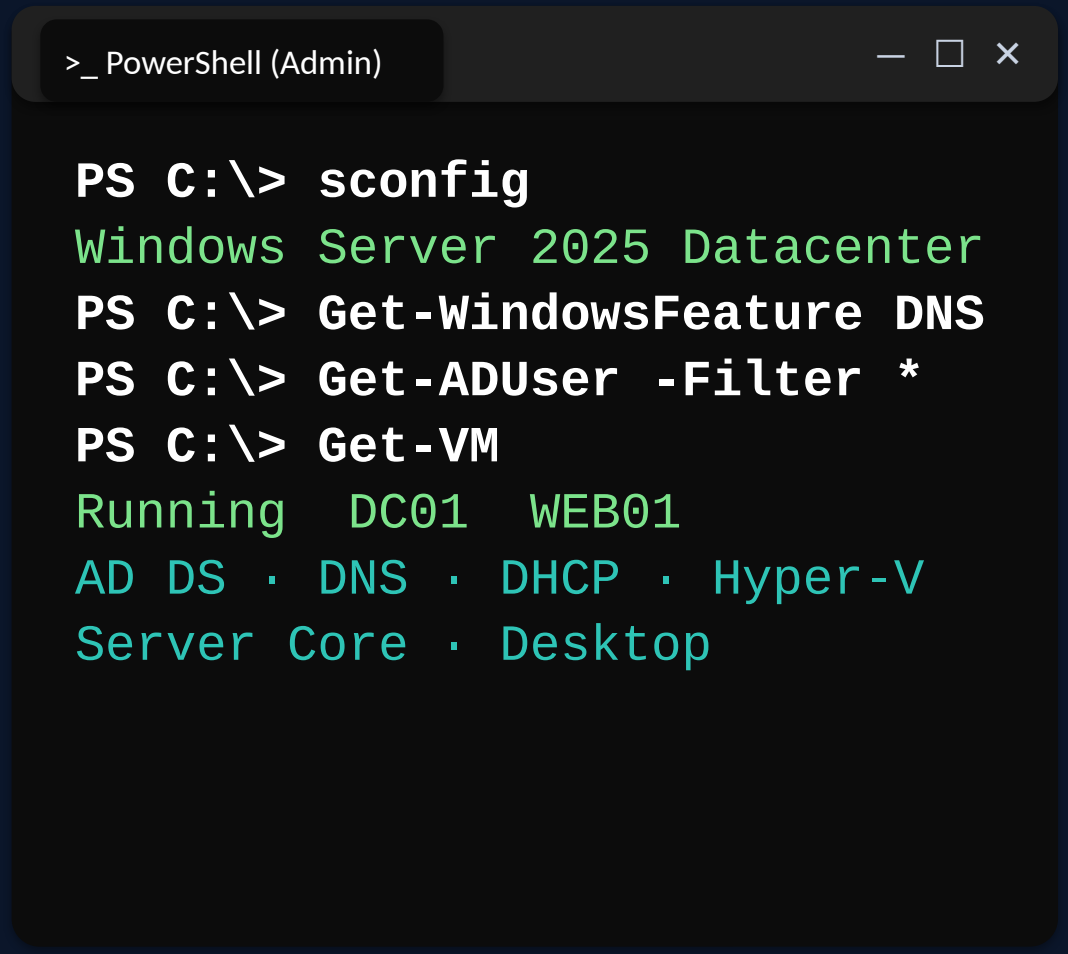
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 11 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Security, Updates, Hotpatch & Backup

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 11

- Security baselines and built-in protections
- Protecting privileged accounts: tiers, Protected Users, LAPS
- Auditing sign-ins and changes
- Update options: Windows Update, WSUS, Azure Update Manager
- Hotpatch: security updates without restarts
- Windows Server Backup: full, system state, Hyper-V
- Ransomware-resistant backup and recovery planning

Built-in Protections to Know

Protection	What it does
Microsoft Defender Antivirus	Built in and on by default on Windows Server
Credential Guard / VBS	Isolates secrets in virtualization-based security
LSA protection	Stops tools from dumping passwords from memory
SMB and LDAP signing	Blocks tampering and relay attacks
Kerberos AES, no NTLMv1	Removes weak, old authentication
Secure Boot, TPM 2.0	Trusted startup; protects against boot-level malware

Apply a Security Baseline

```
# 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
```

Test baselines on a lab server first — they can block older applications.

Protecting Privileged Accounts

Practice	Details
Tier model	Tier 0 = DCs and AD admins; never sign in to workstations with tier 0 accounts
Separate admin accounts	mahmadi for email; adm-mahmadi for administration
Protected Users group	Stronger Kerberos-only protection for admins
Privileged Access Workstation	A locked-down PC used only for administration
Windows LAPS	Unique local admin passwords on every server and PC
gMSA / dMSA	Service accounts with automatic passwords

Auditing: Who Did What?

```
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
```

Update Options for Servers

Option	Best for	Notes
Windows Update	Small environments	sconfig, Settings; schedule maintenance windows
WSUS	On-premises approval and reporting	Still available, but deprecated — no new features
Azure Update Manager	Hybrid servers via Azure Arc	Schedules, compliance reports, many servers
Hotpatch	Fewer restarts	Security updates without reboot (Azure Arc)
Patch Tuesday	All	Second Tuesday every month; test, then deploy

Hotpatch on Windows Server 2025

Topic	What to know
What	Patches running code in memory — no restart for most security updates
Where	Datacenter: Azure Edition; Standard and Datacenter connected to Azure Arc
Cost	Included with Azure Arc at no additional cost (since 2026)
Cycle	Quarterly baseline update needs a restart; the months between do not
Result	About 4 planned restarts a year instead of 12
Enable	Azure portal > Azure Arc > your server > Hotpatch

WSUS in Ten Lines

```
# 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
```

Ransomware-Resistant Backup and Recovery

Practice	Why
3-2-1-1 rule	3 copies, 2 media, 1 off-site, 1 offline or immutable
Separate backup credentials	Not domain admin; attackers delete backups first
Azure Backup / immutable storage	Copies attackers cannot change or delete
Test restores regularly	A backup is only real after a successful restore
AD recovery plan	DSRM password, system state backups, AD Recycle Bin
Written runbook	Who does what, in which order, on the worst day

Lab: Harden, Audit, Back Up, Restore

```
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
```

Summary & Homework

- Baselines: OSConfig or Security Compliance Toolkit; test first
- Separate admin accounts, tier 0 isolation, Protected Users, LAPS
- auditpol + Security log events 4625, 4720, 4728, 4732
- Updates: Windows Update, WSUS (deprecated), Azure Update Manager
- Hotpatch with Azure Arc: about 4 restarts a year
- Backups: system state for DCs, 3-2-1-1, test restores

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

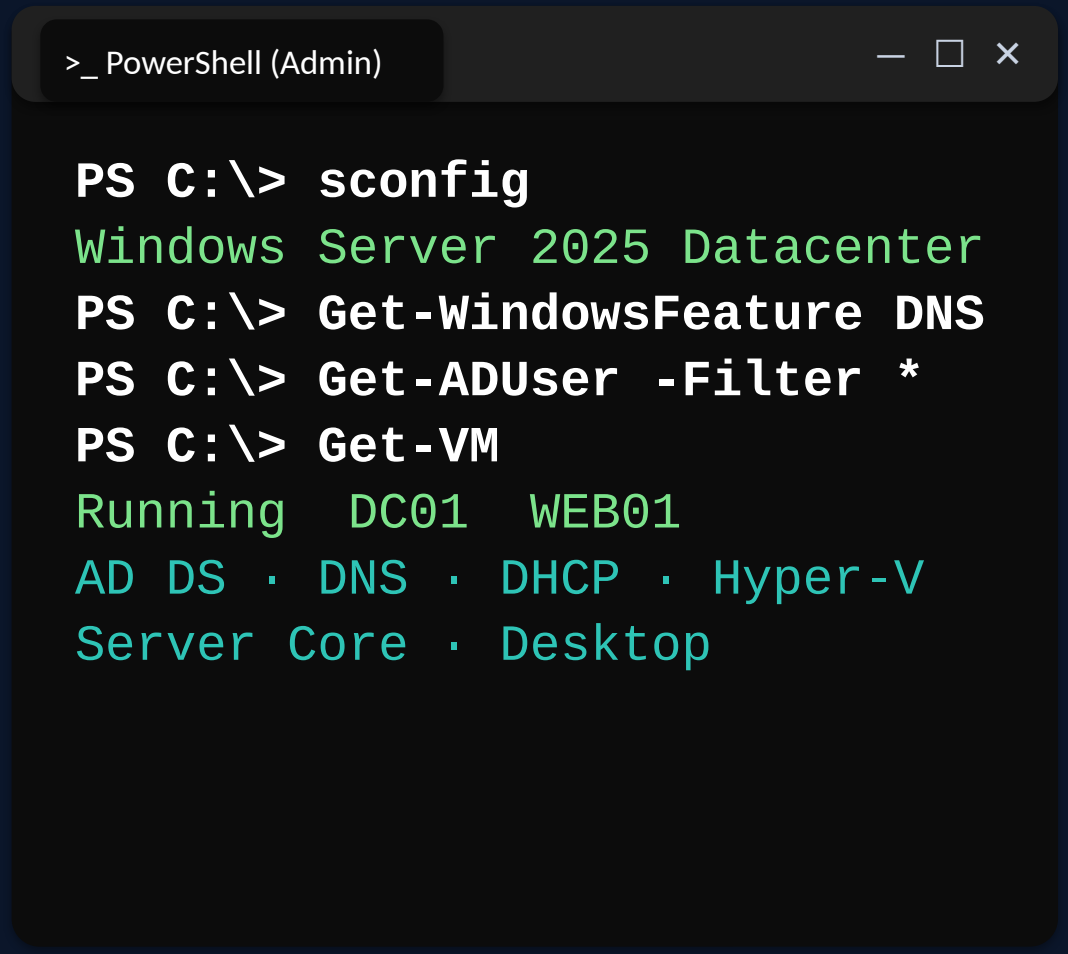
Slides for this lesson: MyWebUniversity.com/presentations

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.



LESSON 12 OF 12

Windows Server 2025

Install · AD · Hyper-V · Admin

Monitoring, Troubleshooting, Azure Arc & Migration

Full Course · Windows Server 2025 (build 26100)

What You Will Learn in Lesson 12

- Monitoring tools and the performance counters that matter
- Baselines with Performance Monitor and logman
- Central event collection and a daily health check
- A troubleshooting method — and the toolkit for each layer
- Azure Arc: managing on-premises servers from Azure
- Migrating from older Windows Server versions
- Course summary, final project and next steps

Monitoring Tools

Tool	Use it for
Server Manager / Windows Admin Center	Quick health of roles, events, services
Performance Monitor (perfmon)	Live counters and long-term data collector sets
Resource Monitor (resmon)	Which process uses CPU, disk, network right now
Event Viewer + subscriptions	Errors and warnings, collected from many servers
PowerShell (Get-Counter, Get-WinEvent)	Scripts, reports, alerts
Azure Monitor via Azure Arc	Dashboards and alerts for hybrid servers

Performance Counters That Matter

Counter	Watch for
Processor(_Total)\% Processor Time	Sustained above 80%
Memory\Available MBytes	Below about 10% of RAM
Memory\Pages/sec	Sustained high values together with low memory
LogicalDisk\Avg. Disk sec/Transfer	Above 0.020 (20 ms) means slow storage
LogicalDisk\% Free Space	Below 15%
Network Interface\Bytes Total/sec	Near the link speed

Live Counters and a Baseline

```
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
```

Central Events and a Daily Health Check

```
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
```

A Calm Troubleshooting Method

Step	What you do
1. Define	What exactly fails? For whom? Since when? Error messages?
2. Scope	One user, one PC, one site, or everyone?
3. Changes	What changed recently? Updates, GPOs, certificates, passwords
4. Layers	Network → DNS → authentication → service → application
5. Test one idea at a time	Change one thing, test, write down the result
6. Fix and verify	Confirm with the user; watch the logs
7. Document	Cause, fix, prevention — for next time

The Toolkit, Layer by Layer

Layer	Tools
Network	Test-NetConnection -Port, Get-NetIPConfiguration, Get-NetTCPConnection
DNS	Resolve-DnsName -Server, dcdiag /test:dns, ipconfig /flushdns
Active Directory	dcdiag, repadmin /replsummary, nltest /dsgetdc, Test-ComputerSecureChannel
Group Policy	gpresult /r, /h, Get-GPResultantSetOfPolicy
Services and apps	Get-Service, Get-WinEvent, IIS logs, Restart-Service
System	Get-Counter, Get-HotFix, Reliability Monitor, sfc /scannow, DISM

Azure Arc: Hybrid Management

Topic	What to know
What	Projects your on-premises servers into Azure as manageable resources
Connect	Azure Arc Setup wizard in Windows Server 2025, or azcmagent connect
Updates	Azure Update Manager and Hotpatch (Lesson 11)
Security	Microsoft Defender for Cloud, Azure Policy, guest configuration
Monitoring	Azure Monitor: metrics, logs, alerts
Licensing	Optional pay-as-you-go Windows Server licensing

Connect a Server to 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 and region are examples; use your own subscription values.

Migrating from Older Windows Server

Service	Recommended path
Active Directory	Add 2025 DCs → move FSMO roles → demote old DCs → raise levels
File servers	Storage Migration Service (in Windows Admin Center); DFS paths
DHCP	Export-DhcpServer on old → Import-DhcpServer on new → authorize
DNS (AD-integrated)	Replicates automatically to the new DCs
IIS sites	Web Deploy, or rebuild with scripts and copy content
Hyper-V VMs	Live migration or export/import to new hosts
Anything else	In-place upgrade from 2012 R2+ when supported — after a backup

Migration in Practice: AD and 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)
```

Course Summary, Final Project & Next Steps

- Lessons 1-3: editions, installation, Server Core, remote management
- Lessons 4-7: Active Directory, Group Policy, DNS and DHCP
- Lessons 8-10: file services, storage, Hyper-V, IIS and RDS
- Lessons 11-12: security, updates, backup, monitoring, Azure Arc, migration
- Final project: rebuild the whole lab from your own scripts, then document it
- Next: exam AZ-802 (Windows Server Administrator Associate); our Linux courses

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.