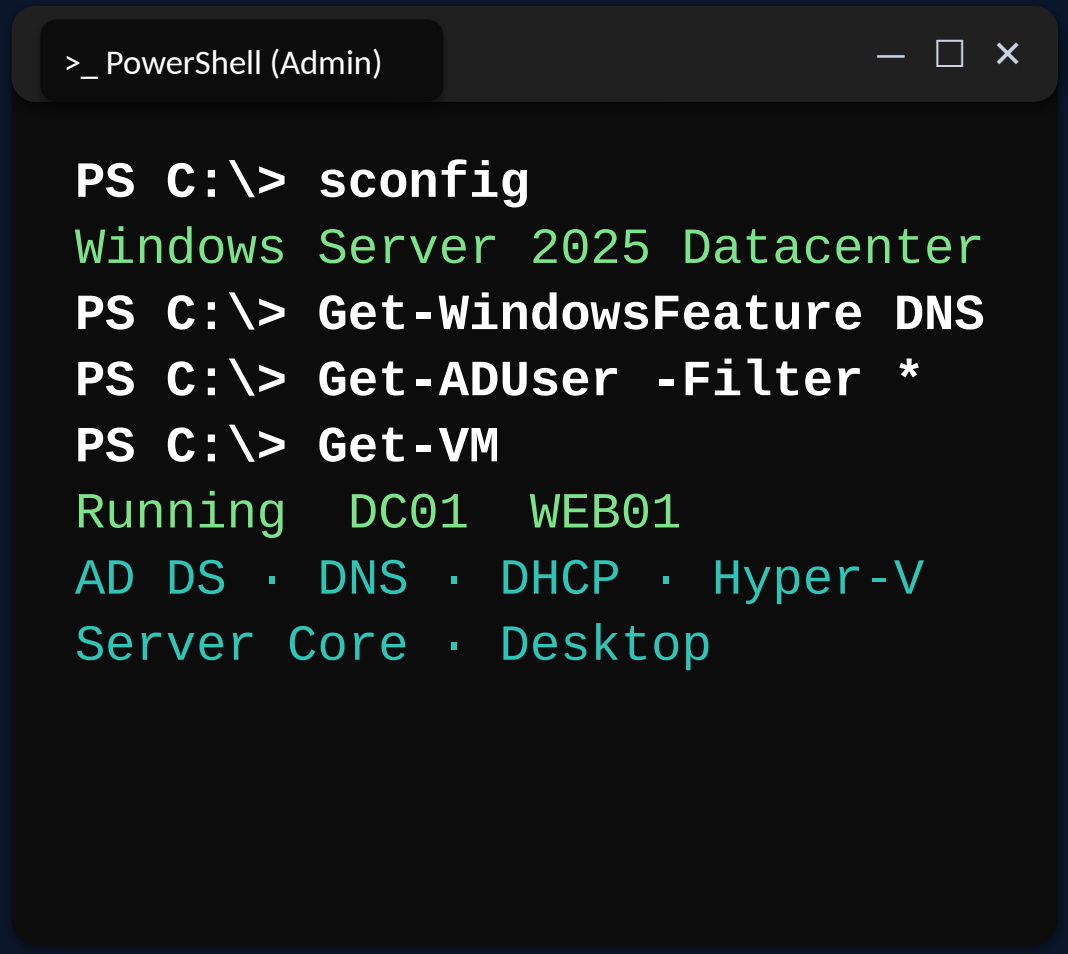


LESSON 11 OF 12

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.