درس ۱۱ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

امنیت، آپدیت‌ها، Hotpatch و بکاپ

دوره کامل · Windows Server 2025 (build 26100)



در درس یازدهم چه یاد می‌گیرید

- خط پایه‌های امنیتی و محافظت‌های داخلی
- محافظت از حساب‌های privileged: tier ها، LAPS، Protected Users
- آدیت ورودها و تغییرات
- گزینه‌های آپدیت: Azure Update Manager، WSUS، Windows Update
- Hotpatch: آپدیت‌های امنیتی بدون ری‌استارت
- Windows Server Backup: کامل، Hyper-V، system state
- بکاپ مقاوم در برابر باج‌افزار و پلان بازیابی

محافظت‌های داخلی که باید بدانید

چه کار می‌کند	محافظت
داخلی و به طور پیش‌فرض در Windows Server روشن	Microsoft Defender Antivirus
رازها را در امنیت مبتنی بر مجازی‌سازی جدا می‌کند	Credential Guard / VBS
ابزارها را از بیرون کشیدن رمزها از حافظه منع می‌کند	LSA protection
دستکاری و حملات relay را مسدود می‌کند	SMB و LDAP signing
احراز هویت ضعیف و قدیمی را حذف می‌کند	Kerberos AES، بدون NTLMv1
شروع مطمئن؛ محافظت در برابر بدافزار سطح بوت	Secure Boot، TPM 2.0

اعمال یک خط پایه امنیتی

```
# 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
```

خط پایه‌ها را اول روی یک سرور لابراتوار آزمایش کنید — ممکن است برنامه‌های قدیمی را مسدود کنند.

محافظت از حساب‌های Privileged

جزئیات	روش
Tier 0 = DC ها و admin های AD؛ هرگز با حساب tier 0 به ورک‌استیشن وارد نشوید	مدل tier
mahmadi برای ایمیل؛ adm-mahmadi برای مدیریت	حساب‌های admin جداگانه
محافظت قوی‌تر فقط با Kerberos برای admin ها	گروه Protected Users
یک کمپیوتر قفل‌شده فقط برای مدیریت	Privileged Access Workstation
رمزهای admin محلی منحصربه‌فرد روی هر سرور و کمپیوتر	Windows LAPS
حساب‌های سرویس با رمزهای خودکار	gMSA / dMSA

آدیتینگ: چه کسی چه کاری کرد؟

```
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
```

گزینه‌های آپدیت برای سرورها

گزینه	بهترین برای	نکات
Windows Update	محیط‌های کوچک	sconfig، Settings؛ زمان‌های نگهداری را زمان‌بندی کنید
WSUS	تأیید و گزارش داخلی	هنوز موجود، اما منسوخ‌شده — بدون ویژگی جدید
Azure Update Manager	سرورهای ترکیبی از طریق Azure Arc	زمان‌بندی، گزارش انطباق، سرورهای زیاد
Hotpatch	ری‌استارت کمتر	آپدیت امنیتی بدون ری‌استارت (Azure Arc)
Patch Tuesday	همه	سه‌شنبه دوم هر ماه؛ آزمایش کنید، بعد اجرا کنید

Hotpatch در Windows Server 2025

چه چیزی بدانید	موضوع
کود در حال اجرا را در حافظه اصلاح می‌کند — برای بیشتر آپدیت‌های امنیتی ری‌استارت لازم نیست	چیست
Datacenter: Azure Edition؛ Standard و Datacenter وصل به Azure Arc	کجا
بدون هزینه اضافی همراه Azure Arc (از ۲۰۲۶)	هزینه
آپدیت baseline سه‌ماهه ری‌استارت لازم دارد؛ ماه‌های بین آن‌ها نه	چرخه
حدود ۴ ری‌استارت پلان‌شده در سال به جای ۱۲	نتیجه
Azure Arc > Azure portal > سرور شما > Hotpatch	فعال کردن

WSUS در ده خط

```
# 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
```

بکاپ و بازیابی مقاوم در برابر باج‌افزار

چرا	روش
۳ کاپی، ۲ رسانه، ۱ خارج از محل، ۱ آفلاین یا تغییرناپذیر	قانون ۳-۲-۱-۱
نه domain admin؛ حمله‌کنندگان اول بکاپ‌ها را حذف می‌کنند	credential جداگانه برای بکاپ
کاپی‌هایی که حمله‌کنندگان نمی‌توانند تغییر یا حذف کنند	ذخیره‌سازی Azure Backup / تغییرناپذیر
یک بکاپ فقط بعد از یک بازیابی موفق واقعی است	بازیابی را به طور منظم آزمایش کنید
رمز DSRM، بکاپ‌های system state، AD Recycle Bin	پلان بازیابی AD
چه کسی چه کاری، به چه ترتیبی، در بدترین روز	دستورالعمل نوشته‌شده

لابراتوار: محکم کردن، آدیت، بکاپ، بازیابی

```
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
```

خلاصه و کارخانگی

- خط پایه‌ها: OSConfig یا Security Compliance Toolkit؛ اول آزمایش کنید
- حساب‌های admin جداگانه، جداسازی LAPS، Protected Users، tier 0
- auditpol + رویدادهای لاگ 4732، 4728، 4720، 4625: Security
- آپدیت‌ها: WSUS، Windows Update (منسوخ)، Azure Update Manager
- Hotpatch با Azure Arc: حدود ۴ ری‌استارت در سال
- بکاپ‌ها: system state برای DC ها، ۳-۲-۱-۱، بازیابی را آزمایش کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید