درس ۱۱ از ۱۲

Windows 10 & 11

Desktop · Workstation · Laptop

ذخیره‌سازی، امنیت، آپدیت‌ها و بکاپ

دوره کامل · Windows 10 22H2 · Windows 11 26H2



در درس یازدهم چه یاد می‌گیرید

- دیسک‌ها، پارتیشن‌ها و volume ها در GUI و PowerShell
- اجازه‌های NTFS با icacls و Get-Acl
- BitLocker و device encryption — و کلید بازیابی
- Windows Security: memory integrity، SmartScreen، Defender Antivirus
- مدیریت Windows Update مانند یک مدیر سیستم
- بکاپ: قانون ۳-۲-۱، restore point، Windows Backup، File History
- یک لابراتوار که یک فولدر واقعی را کاملاً محافظت می‌کند

دیسک‌ها و volume ها با PowerShell

```
PS C:\> Get-PhysicalDisk | Select-Object FriendlyName, MediaType, HealthStatus,
          @{n='GB'; e={[int]($_.Size/1GB)}}
PS C:\> Get-Disk ; Get-Partition ; Get-Volume

# Prepare a NEW empty disk (check the number twice!)
PS C:\> Initialize-Disk -Number 1 -PartitionStyle GPT
PS C:\> New-Partition -DiskNumber 1 -UseMaximumSize -AssignDriveLetter |
          Format-Volume -FileSystem NTFS -NewFileSystemLabel Data

PS C:\> Optimize-Volume -DriveLetter C -ReTrim -Verbose    # SSD TRIM
```

GUI: diskmgmt.msc، یا Settings > System > Storage > Advanced storage settings > Disks & volumes

اجازه‌های NTFS

اجازه می‌دهد	اجازه
همه چیز، از جمله تغییر اجازه‌ها و گرفتن مالکیت	Full control
خواندن، نوشتن و حذف فایل‌ها و فولدرها	Modify
باز کردن فایل‌ها و اجرای برنامه‌ها	Read & execute
دیدن محتوا / ساختن و تغییر محتوا	Read / Write
فولدرهای فرزند اجازه‌های والد را می‌گیرند مگر اینکه متوقف کنید	Inheritance
اجازه‌های share و NTFS هر دو اعمال می‌شوند — سخت‌گیرترین برنده است	با اشتراک‌ها

اجازه‌ها با icacls و Get-Acl

```
C:\> icacls C:\Lab                                  # who has what
C:\> icacls C:\Lab /grant student:(OI)(CI)M         # Modify, inherited by all
C:\> icacls C:\Lab /remove student
C:\> icacls C:\Lab /save C:\Backup\lab-acl.txt /T   # back up permissions
C:\> takeown /f C:\Old\locked.txt                   # take ownership (admin)

PS C:\> (Get-Acl C:\Lab).Access | Select-Object IdentityReference, FileSystemRights, IsInherited
#  (OI) object inherit  (CI) container inherit  F=Full  M=Modify  RX=Read&Execute
```

BitLocker و Device Encryption

ویژگی	نکات
Device encryption	بسیاری از کمپیوترهای Home: با حساب Microsoft خودکار روشن می‌شود
BitLocker	Pro و بالاتر: کنترل کامل، TPM + PIN، پالیسی‌ها
BitLocker To Go	رمزگذاری فلش‌های USB با رمز
محافظت در برابر	لپ‌تاپ‌های دزدیده‌شده یا گم‌شده و دیسک‌های بیرون‌شده
کلید بازیابی	۴۸ رقم — حساب Microsoft، حساب کاری (Entra ID)، یا چاپ کنید
قبل از تغییرات BIOS/سخت‌افزار	BitLocker را موقتاً متوقف کنید، یا کلید بازیابی را آماده داشته باشید

BitLocker از خط فرمان

```
C:\> manage-bde -status                          # every volume: encrypted? method?
C:\> manage-bde -protectors -get C:              # shows the recovery password ID

PS C:\> Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, EncryptionPercentage,
ProtectionStatus
PS C:\> Enable-BitLocker -MountPoint D: -EncryptionMethod XtsAes256 -RecoveryPasswordProtector
PS C:\> (Get-BitLockerVolume D:).KeyProtector     # save this recovery password!
PS C:\> Suspend-BitLocker -MountPoint C: -RebootCount 1     # before a BIOS update
PS C:\> Resume-BitLocker -MountPoint C:
```

نگاهی به Windows Security

چه چیزی بررسی کنیم	بخش
Microsoft Defender Antivirus روشن، زنده، آپدیت	Virus & threat protection
Controlled folder access؛ بازیابی فایل در OneDrive	محافظت از باج‌افزار
Windows Hello، Dynamic lock	Account protection
همه profile ها روشن (درس ۱۰)	Firewall & network protection
SmartScreen؛ Smart App Control در نصب‌های جدید	App & browser control
Core isolation (memory integrity)، TPM، Secure Boot	Device security

Microsoft Defender از PowerShell

```
PS C:\> Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled,
          AntivirusSignatureLastUpdated, QuickScanEndTime
PS C:\> Update-MpSignature                          # get the newest definitions
PS C:\> Start-MpScan -ScanType QuickScan
PS C:\> Start-MpScan -ScanType CustomScan -ScanPath D:\Downloads
PS C:\> Get-MpThreatDetection                       # what was found and when
PS C:\> Set-MpPreference -EnableControlledFolderAccess Enabled   # ransomware shield
```

مدیریت Windows Update

کجا / چرا	تنظیم
آپدیت‌های امنیتی در سه‌شنبه دوم هر ماه	Patch Tuesday
از ری‌استارت در زمان کار شما جلوگیری می‌کند	Active hours
تا چند هفته — بعد آپدیت‌ها قبل از توقف دوباره نصب می‌شوند	Pause updates
Advanced options > Optional updates: درایورها، پیش‌نمایش‌ها	Optional updates
ببینید چه نصب شده؛ یک آپدیت مشکل‌دار را حذف کنید	Update history
Get-HotFix | winget upgrade --all برای برنامه‌ها	خط فرمان

بکاپ: قانون ۳-۲-۱

نکات	محافظت می‌کند	ابزار
۳ کاپی، ۲ نوع رسانه متفاوت، ۱ خارج از محل (ابر)	همه چیز	**قانون ۳-۲-۱**
به OneDrive؛ هنگام نصب کمپیوتر جدید بازیابی می‌شود	تنظیمات، لست برنامه‌ها، فولدرها	**برنامه Windows Backup**
تاریخچه نسخه‌ها، بازیابی از باج‌افزار	Desktop، Documents، Pictures	**بکاپ فولدر OneDrive**
به یک دیسک بیرونی یا اشتراک شبکه	فایل‌های شما، نسخه‌های زیاد	**File History**
قدیمی اما قبل از تغییرات بزرگ مفید	کل درایو C:	**System image (wbadmin)**
بکاپ اسناد شما نیست	فایل‌های سیستم، درایورها، registry	**Restore point ها**

لابراتوار: محافظت کامل از یک فولدر

```
PS C:\> Checkpoint-Computer -Description 'Before Lesson 11 lab' -RestorePointType MODIFY_SETTINGS
PS C:\> icacls C:\Lab /save C:\Backup\lab-acl.txt /T
PS C:\> robocopy C:\Lab E:\Backup\Lab /E /R:1 /W:1 /LOG:C:\Backup\robocopy.log
PS C:\> Get-BitLockerVolume E: | Select-Object VolumeStatus, ProtectionStatus
PS C:\> Start-MpScan -ScanType CustomScan -ScanPath C:\Lab
# Test the restore: delete one file in C:\Lab, then copy it back from E:\Backup\Lab
C:\> wbadmin start backup -backupTarget:E: -include:C: -allCritical -quiet   # system image
```

خلاصه و کارخانگی

- سلامت Get-PhysicalDisk، Get-Volume، Optimize-Volume -ReTrim
- icacls: grant (OI)(CI)M، قبل از تغییرات بزرگ /save
- BitLocker همه جا؛ بدانید هر کلید بازیابی کجا است
- Windows Security همه سبز؛ Patch Tuesday؛ winget upgrade برای برنامه‌ها
- بکاپ: ۳-۲-۱، و یک بازیابی را آزمایش کنید
- کارخانگی: همین حالا کلید بازیابی BitLocker خود را آنلاین پیدا 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