درس ۱۰ از ۱۲

Windows Server 2025

Install · AD · Hyper-V · Admin

سرور وب (IIS)، Remote Desktop Services و دسترسی از راه دور

دوره کامل · Windows Server 2025 (build 26100)



در درس دهم چه یاد می‌گیرید

- مفاهیم IIS: site ها، binding ها، application pool ها، لاگ‌ها
- نصب IIS و ساختن یک ویب‌سایت با PowerShell
- binding های HTTPS و سرتیفیکیت‌ها
- Application pool ها و امنیت IIS
- Remote Desktop Services: نقش‌ها، collection ها و RemoteApp
- دسترسی از راه دور: VPN، RD Gateway و SMB over QUIC
- یک چک‌لست امنیتی برای هر چیزی که رو به انترنت است

مفاهیم IIS

اصطلاح	معنی
Site	یک وب‌سایت با فولدر، binding ها و تنظیمات خودش
Binding	پروتوکول + IP + پورت + نام میزبان، مثلاً https *:443 intranet.lab...
Application pool	یک پروسه کارگر جدا (w3wp.exe) که یک یا چند برنامه را اجرا می‌کند
Virtual directory / application	یک فولدر یا برنامه داخل یک site
Physical path	جایی که فایل‌ها قرار دارند، مثلاً C:\inetpub\intranet
لاگ‌ها	C:\inetpub\logs\LogFiles — هر درخواست، کد وضعیت، زمان

نصب IIS و ساختن سایت Intranet

```
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
```

اضافه کردن 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 Pool ها و امنیت IIS

چرا	روش
جداسازی: یک crash یا نفوذ محدود می‌ماند	یک app pool برای هر برنامه
هر pool با حساب مجازی کم‌دسترسی خودش اجرا می‌شود	ApplicationPoolIdentity
رمزها و دیتا را در مسیر محافظت می‌کند	فقط HTTPS؛ HTTP را redirect کنید
ماژول‌های کمتر = سطح حمله کوچک‌تر	فقط ویژگی‌های لازم را نصب کنید
درخواست‌های بد را مسدود کنید؛ مشکلات را بررسی کنید	Request filtering، لاگ‌گیری
ASP.NET Core Hosting Bundle؛ PHP/Python از طریق FastCGI یا HttpPlatformHandler	برنامه‌ها

App Pool ها و لاگ‌ها با 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
```

(RDS) Remote Desktop Services

وظیفه	نقش
دسکتاپ‌ها و برنامه‌هایی را اجرا می‌کند که کاربران زیاد شریک هستند	RD Session Host
کاربران را به میزبان درست می‌فرستد؛ جلسات را دوباره وصل می‌کند	RD Connection Broker
صفحه ویبی که دسکتاپ‌ها و RemoteApp های منتشرشده را لست می‌کند	RD Web Access
ورود امن HTTPS از انترنت — بدون باز کردن پورت 3389	RD Gateway
RDS CAL ها را صادر می‌کند (۱۲۰ روز مهلت برای شروع)	RD Licensing
هر کاربر به جای جلسه مشترک، VM خودش را می‌گیرد	VDI (جایگزین)

نصب سریع RDS و یک 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
```

دسترسی از راه دور: گزینه‌های امن

گزینه	بهترین برای	نکات
VPN (RRAS / Always On VPN)	دسترسی کامل شبکه برای لپ‌تاپ‌های مدیریت‌شده	IKEv2 یا SSTP؛ سرتیفیکیت‌ها؛ MFA
RD Gateway	دسکتاپ‌ها و RemoteApp های از راه دور	HTTPS 443؛ MFA اضافه کنید
SMB over QUIC	اشتراک‌های فایل از هر جا	بدون VPN؛ بر اساس سرتیفیکیت؛ همه نسخه‌ها
برنامه‌های وب پشت reverse proxy	سایت‌های intranet	HTTPS، MFA، WAF
هرگز	باز کردن RDP (3389) یا SMB (445) به انترنت	حمله‌کنندگان دائماً جستجو می‌کنند

چک‌لست برای هر چیزی که رو به انترنت است

- HTTPS در همه جا، با سرتیفیکیت از یک CA مطمئن
- احراز هویت چندمرحله‌ای در هر نقطه ورود بیرونی
- فقط پورت 443 (و پورت‌های VPN) باز؛ هیچ چیز دیگر
- آپدیت ماهانه — اول سرورهای رو به انترنت
- کمترین دسترسی: هویت‌های app pool، هیچ domain admin روی سرورهای وب
- لاگ‌ها به صورت مرکزی جمع و مرور شوند (درس ۱۲)

خلاصه و کارخانگی

- IIS: site ها، binding های نام میزبان، یک app pool برای هر برنامه، لاگ‌ها
- New-IISSite، New-IISSiteBinding -Protocol https، Get-IISAppPool
- RDS: Licensing، Gateway، Web Access، Broker، Session Host
- New-RDSessionDeployment، New-RDSessionCollection، New-RDRemoteApp
- کارخانگی: سایت intranet با HTTPS و app pool خودش را بسازید
- کارخانگی: یک RemoteApp منتشر کنید و آن را از CL01 باز 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