

PowerShell v2.0 alapok

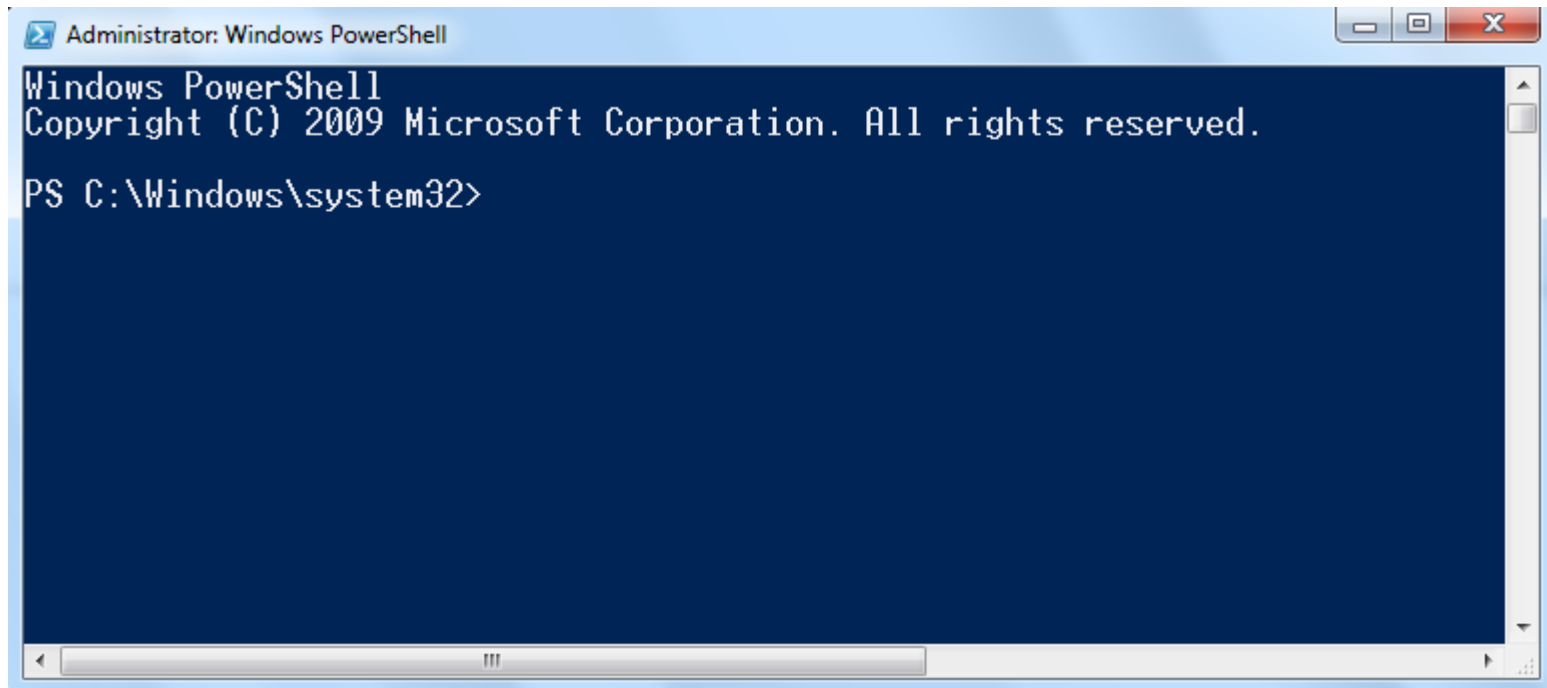
Nagy Miklós

Kezdetek, Felhasználás

- 2006-ban létrejött egy új script nyelv, mely Window Vista-ban, és Windows Server 2008-ban telepíthető opcióként jelenik meg. (PowerShell 1.0)
- Automatizáció alapvető eszköze.
- Legtöbb MS server támogatja: Exchange, SQL, Lync, SCOM.
- Nagy mennyiségű objektumon végzett műveletek hatékonysága (több ezer v. több tízezer objektum esetén drasztikusan csökken a műveleti idő).
- Szál kezelés támogatása (Job-ok)
- Script-írás, mely scriptek ütemezhetőek
- Jelenlegi verzió 4.0 - Windows Server 2012-ben
- Jelenlegi verzió 5.0 - Windows 10-ben

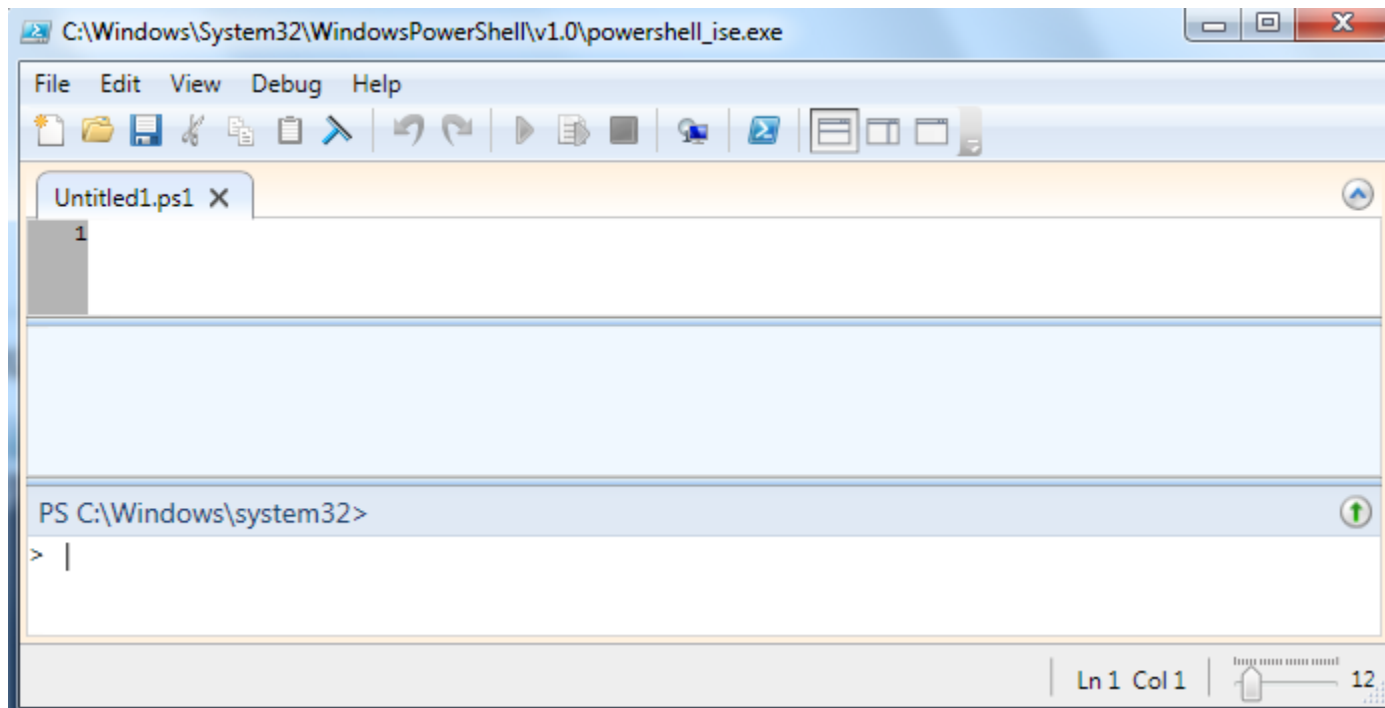
Fejlesztői felületek

- ***Konzol – Parancssoros felület. Előnyei:***
 - TAB : „Intellisense” → Automatikus parancs kiegészítés
 - Shift-TAB : Reverse
 - Esc : Törli az aktuális sort
 - F7 : History



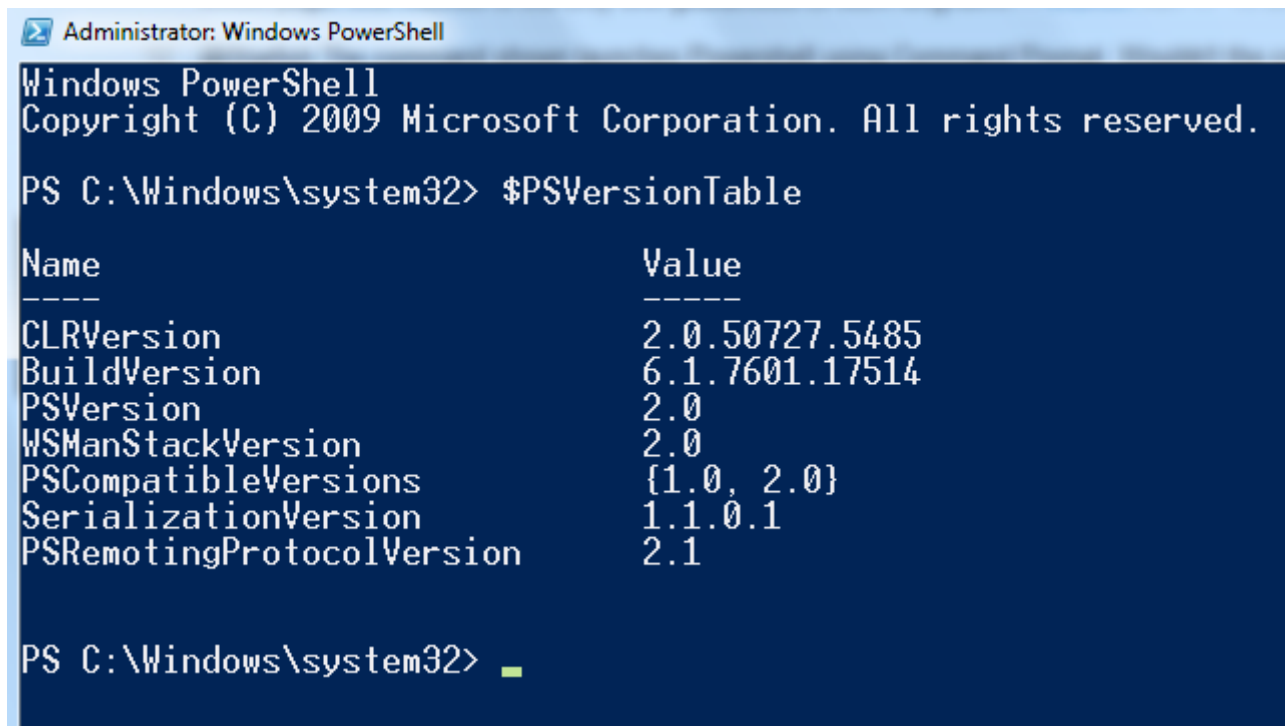
Fejlesztői felületek

- ***ISE – Integrated Scripting Environment***
 - Konzollal egybekötött scriptelési eszköz.



PowerShell verzió

- PowerShell Verzió lekérés: **\$PSVersionTable**



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $PSVersionTable

Name                           Value
----                           -
CLRVersion                     2.0.50727.5485
BuildVersion                   6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion           1.1.0.1
PSRemotingProtocolVersion      2.1

PS C:\Windows\system32> _
```

Parancs fajták

- DOS parancsok (Dir, stb.)
- Unix parancsok (ls, stb.)
- PowerShell saját parancsai (Get-Item, Get-Process, Get-Date) → „**Cmdlet**”-ek
- Minden DOS, és Unix parancs visszavezethető egy PowerShell „**Alias**”-ra.

PowerShell CMDLET

- A PowerShell „parancs-adatbázis” mely lge-Főnév formátumú.
- Visszatérési értéke mindig objektum melynek adattagjai (Property), és függvényei (Metódusai) vannak.
- Tagok lekérése: <Powershell CMDLET> | Get-Member
- **Get-Service | Get-Member**

```
PS C:\Windows\system32> Get-Service | Get-Member
```

```
TypeName: System.ServiceProcess.ServiceController
```

Name	MemberType	Definition
Name	AliasProperty	Name = ServiceName
RequiredServices	AliasProperty	RequiredServices = ServicesDepe
Disposed	Event	System.EventHandler Disposed(Sy
Close	Method	System.Void Close()
Continue	Method	System.Void Continue()
CreateObjRef	Method	System.Runtime.Remoting.ObjRef
Dispose	Method	System.Void Dispose()
Equals	Method	bool Equals(System.Object obj)

Parancs szintaxis

- 1. Ige (Add, Get, Set, New, Remove, stb.)
- 2. Főnév (Item, Service, Process, stb.)
- 3. Argumentum (Property, Confirm, stb.)
- Pl. **Get-Service**, Get-ChildItem, New-Item, stb.

```
PS C:\Windows\system32> Get-Service
```

Status	Name	DisplayName
-----	----	-----
Running	AdobeARMservice	Adobe Acrobat Update Service
Stopped	AdobeFlashPlaye...	Adobe Flash Player Update Service
Running	AeLookupSvc	Alkalmazásminősítő
Stopped	ALG	Alkalmazási réteg átjárószolgáltatása
Stopped	AppIDSvc	Alkalmazásidentitás
Running	Appinfo	Alkalmazásadatok
Stopped	AppMgmt	Alkalmazásvezérlés
Stopped	aspnet_state	ASP.NET-állapotszolgáltatás
Running	AudioEndpointBu...	Windows-hangvégpontépítő
Running	Audiosrv	Windows audio
Running	AVP16.0.0	Kaspersky Anti-Virus Service 16.0.0
Stopped	AxInstSV	ActiveX Telepítő (AxInstSV)
Stopped	BDESVC	BitLocker meghajtótitkosítási szolg...

Alias-ok

- Parancsok rövidített nevei a könnyebb kezelhetőség érdekében.
- Alias-ok listája : **Get-Alias**

```
PS C:\Windows\system32> Get-Alias
```

CommandType	Name	Definition
Alias	%	ForEach-Object
Alias	?	Where-Object
Alias	ac	Add-Content
Alias	asnp	Add-PSSnapIn
Alias	cat	Get-Content
Alias	cd	Set-Location
Alias	chdir	Set-Location
Alias	clc	Clear-Content
Alias	clear	Clear-Host
Alias	clhy	Clear-History
Alias	cli	Clear-Item
Alias	clp	Clear-ItemProperty

Alias definiálás

- Példa:

- Új Alias definiálás : **New-Alias „folyamatok” Get-Process**
- Futtatás : **folyamatok**
- Lekérdezés : **Get-Alias folyamatok**

```
PS C:\Windows\system32> New-Alias "folyamatok" Get-Process
PS C:\Windows\system32> folyamatok
```

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
206	8	7780	4168	79	0,30	5032	AcroRd32
228	17	81720	30496	231	16,72	5060	AcroRd32
2357	9	3292	5580	78	14,07	5300	AdobeARM
63	3	836	1056	33	0,02	5488	armsvc
126	5	15072	14000	66		6612	audiodg

```
PS C:\Windows\system32> Get-Alias folyamatok
```

CommandType	Name	Definition
Alias	folyamatok	Get-Process

Listázások 1.

- fl <property lista> # Formázott lista
- ft <property lista> # Formázott tábla
- **Get-Service | fl name, status**

```
PS C:\Windows\system32> Get-Service | fl name,status
```

```
Name : AdobeARMservice  
Status : Running
```

```
Name : AdobeFlashPlayerUpdateSvc  
Status : Stopped
```

```
Name : AeLookupSvc  
Status : Stopped
```

```
Name : ALG  
Status : Stopped
```

Listázások 2.

- `Get-Service | ft name, status -AutoSize`

```
PS C:\Windows\system32> Get-Service | ft name,status -AutoSize
```

Name	Status
----	-----
AdobeARMservice	Running
AdobeFlashPlayerUpdateSvc	Stopped
AeLookupSvc	Stopped
ALG	Stopped
AppIDSvc	Stopped
Appinfo	Running
AppMgmt	Stopped
aspnet_state	Stopped
AudioEndpointBuilder	Running

Fontosabb parancsok

Kategória	Parancs
Idő, dátum	Get-Date [-Format] "yyyy.MM.dd"
Fájl kezelés	Get-Item, Get-ChildItem, Remove-Item, Copy-Item, Rename-Item, Get-Content, etc.
Event viewer	Get-EventLog -LogName [LOGNAME]
Folyamatok	Get-Process, Get-Service
Egyéb	Get-Help, Get-Alias

Operátorok

Operátor	Jelentése	Operátor	Jelentése
-eq	Egyenlő	-and	Logikai és
-ne	Nem egyenlő	-or	Logikai vagy
-lt	Kisebb mint	-like	Szűrő operátor
-le	Kisebb v. egyenlő	-notlike	Negatív szűrés
-gt	Nagyobb mint	-band	Bitenkénti és
-ge	Nagyobb v. egyenlő	-bor	Bitenkénti vagy

Objektum kezelés

- Rendezés : **Sort-Object**

```
PS C:\Windows\system32> Get-Service | Sort-Object name
```

Status	Name	DisplayName
Running	AdobeARMservice	Adobe Acrobat Update Service
Stopped	AdobeFlashPlaye...	Adobe Flash Player Update Service
Running	AeLookupSvc	Alkalmazásminősítő
Stopped	ALG	Alkalmazási réteg átjárószolgáltatása
Stopped	AppIDSvc	Alkalmazásidentitás
Running	Appinfo	Alkalmazásadatok
Stopped	AppMgmt	Alkalmazásvezérlés
Stopped	aspnet_state	ASP.NET-állapotszolgáltatás
Running	AudioEndpointBu	Windows-hangvégepontépítő

```
PS C:\Windows\system32> Get-Service | Sort-Object name -Descending
```

Status	Name	DisplayName
Stopped	WwanSvc	WWAN automatikus konfigurálás
Running	wudfsvc	Windows illesztőprogram-alaprendsze...
Running	wuauclt	Windows Update
Stopped	WSearch	Windows Search
Running	wscntxt	Biztonsági központ
Running	WPDBusEnum	Hordozható eszközök számbavételi sz...
Stopped	WPCntxt	Parental Controls

Objektum kezelés

- Szűrés : **Where-Object**

```
PS C:\Windows\system32> Get-Service | Where-Object { $_.name -eq "w32time" }

Status      Name          DisplayName
-----
Running     W32Time       Windows idő

PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Get-Service | Where-Object { $_.name -like "wi*" }

Status      Name          DisplayName
-----
Running     WinDefend     Windows Defender
Running     WinHttpAutoProx... WinHTTP automatikus webproxy-kereső...
Running     Winmgmt       Windows Management Instrumentation
Stopped     WinRM         Rendszerfelügyeleti webszolgáltatások
```


Objektum kezelés

- Csoportosítás : **Group-Object**

```
PS C:\Windows\system32> Get-Service | Group-Object status
```

Count	Name	Group
69	Running	{System.ServiceProcess.ServiceController, System
91	Stopped	{System.ServiceProcess.ServiceController, System

```
PS C:\Windows\system32> _
```

Objektum kezelés

- Bejárás : **Foreach-Object**

```
PS C:\Windows\system32> Get-Process | ForEach-Object { $_.id*2 }  
10064  
10120  
10600  
10976  
3592  
7656  
9728  
1088  
1232  
5840  
4280
```

Objektum kezelés

- Mérés: **Measure-Object**

```
PS C:\Windows\system32> Get-Service | Measure-Object
```

```
Count      : 160  
Average    :  
Sum        :  
Maximum    :  
Minimum    :  
Property   :
```

```
PS C:\Windows\system32> Get-Process | Measure-Object -Property id -Maximum -Minimum -Average -Sum
```

```
Count      : 61  
Average    : 2602,29508196721  
Sum        : 158740  
Maximum    : 6100  
Minimum    : 0  
Property   : Id
```

Objektum kezelés

- Számlálás: **count**
- Szintaxis példák:

```
PS C:\Windows\system32> (Get-Service).count  
160  
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> $x = Get-Service  
PS C:\Windows\system32> $x.count  
160  
PS C:\Windows\system32>
```

Változók

- Nevük \$ jellel kezdődik
- Objektumot tárol (Property-k, Metódusok összessége)
- Betűvel vagy számjeggyel kezdődik és betűvel vagy számjeggyel folytatódhat:
- **\$x = 5**
- **\$4 = "alma"**

```
PS C:\Windows\system32> $x = 5
PS C:\Windows\system32> $x | Get-Member
```

TypeName: System.Int32

Name	MemberType	Definition
CompareTo	Method	int CompareTo(System.Object value), int CompareTo(int value)
Equals	Method	bool Equals(System.Object obj), bool Equals(int obj)
GetHashCode	Method	int GetHashCode()
GetType	Method	type GetType()
GetTypeCode	Method	System.TypeCode GetTypeCode()
ToString	Method	string ToString(), string ToString(string format), string ToString(System.IFormattable)

```
PS C:\Windows\system32>
```

Tömbök

- Létrehozás
 - `$tomb = @()` *# üres tömb*
 - `$tomb = 7,2,3` *# explicit 3 elemű tömb*
 - `$tomb = 1..100` *# tömb 1-től 100-ig*
 - `$tomb = Get-Process` *# process-eket tartalmazó tömb*
- Bővítés
 - `$tomb += 324` *# 324-es számmal mint új elemmel bővítünk*
- Hivatkozás
 - `$tomb[5]` *# 0. elemtől indul az indexelés, ez a 6. elem*
- Hash-tábla
 - `$tomb = @{"alma" = 3; "dio" = 4}`
 - `$tomb["alma"]`

Szöveg

- " és '

\$szoveg = "Madrid"

"\$szoveg-ban élek."

behelyettesítés/param.átadás

'\$szoveg-ban élek.'

nincs behelyettesítés/nincs param.átadás

```
PS C:\Windows\system32> $szoveg = "Madrid"
PS C:\Windows\system32> "$szoveg-ban élek."
Madrid-ban élek.
PS C:\Windows\system32> '$szoveg-ban élek.'
$szoveg-ban élek.
PS C:\Windows\system32>
```

Fontosabb szöveg metódusok

Parancs	Jelentés
Length	Szöveg hossza
ToUpper	Nagybetűs konverzió
Replace	Szövegrész csere
Contains	Tartalom vizsgálat
Split	Darabolás

```
PS C:\Windows\system32> $szoveg.length
6
PS C:\Windows\system32> $szoveg.ToUpper()
MADRID
PS C:\Windows\system32> $szoveg.Replace("ri","@@@")
Mad@@@
PS C:\Windows\system32> $szoveg -contains "tea"
False
PS C:\Windows\system32> $szoveg.Split("d")
Ma
ri
PS C:\Windows\system32>
```


WMI Objektumok

- Windows Management Instrumentation (WMI) egy olyan parancs halmaz / lekérő nyelv, mely alacsony szintű utasításokkal éri el, a számítógép fizikai perifériáit (processor, memória, hálózati kártya, stb.)
- Meghívása: **Get-WMIObject -Class <OSZTALY> | fl ***
- Fontosabb osztályok: Win32_processor, Win32_networkadapter, Win32_diskdrive, Win32_computersystem, Win32_operatingsystem, win32_physicalmemory

```
PS C:\Windows\system32> Get-WMIObject -Class win32_processor | fl name
```

```
name : Intel(R) Core(TM)2 Duo CPU      E7200  @ 2.53GHz
```

```
PS C:\Windows\system32> (Get-WMIObject -Class win32_processor).name  
Intel(R) Core(TM)2 Duo CPU      E7200  @ 2.53GHz
```

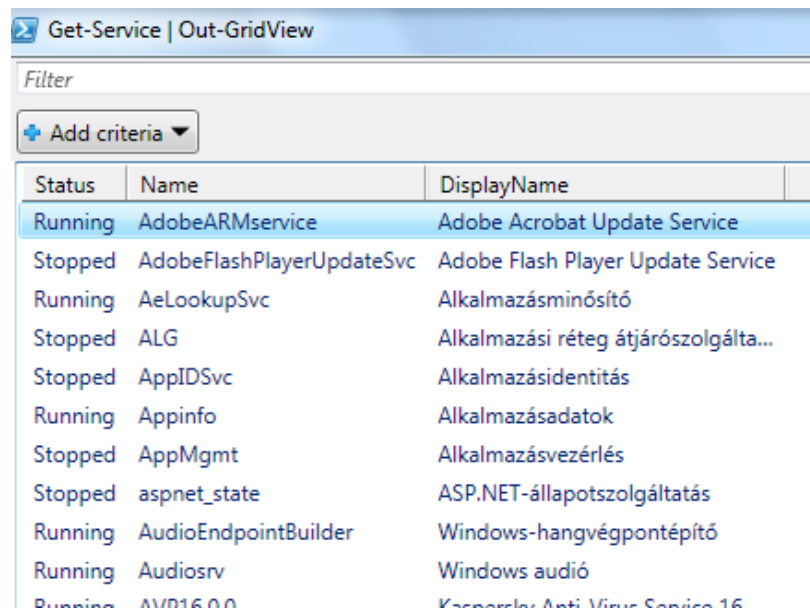
```
PS C:\Windows\system32> Get-WMIObject -Class win32_processor | fl numberofcores
```

```
numberofcores : 2
```

*Kimenet irányítás : Out-****

- Parancs kimenetet lehet irányítani:
 - Fájlba : Out-File <FILENEV>
 - Táblanézetbe : Out-GridView
 - „DEV0”-ba : Out-Null

Példa : **Get-Service | Out-GridView**



Status	Name	DisplayName
Running	AdobeARMservice	Adobe Acrobat Update Service
Stopped	AdobeFlashPlayerUpdateSvc	Adobe Flash Player Update Service
Running	AeLookupSvc	Alkalmazásminősítő
Stopped	ALG	Alkalmazási réteg átjárószolga...
Stopped	AppIDSvc	Alkalmazásidentitás
Running	Appinfo	Alkalmazásadatok
Stopped	AppMgmt	Alkalmazásvezérlés
Stopped	aspnet_state	ASP.NET-állapotszolgáltatás
Running	AudioEndpointBuilder	Windows-hangvégpontépítő
Running	Audiosrv	Windows audio
Running	AVP16.0.0	Kaspersky Anti Virus Service 16

Fájlkezelés (txt file)

- Definiálás : `$f = "C:\temp\elso.txt"`
- Beolvasás : `$tartalom = Get-Content $f`
- Tartalom megjelenítés : `$tartalom`
- Sorok száma : `$tartalom.Count`
- Fájl adatok : `Get-Item $f`

```
PS C:\Windows\system32> $f = "C:\temp\elso.txt"
PS C:\Windows\system32> $tartalom = Get-Content $f
PS C:\Windows\system32> $tartalom
egy
kettő
41
Anna
szék
PS C:\Windows\system32> $tartalom.Count
5
PS C:\Windows\system32> Get-Item $f

Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a---             2015.11.17.         0:37         26 elso.txt
```

Kérdések

???

Ellenőrző feladatok I.

(Alap szintaktika)

- 1. Kérjük le, hogy milyen nap van ma? (a hét milyen napja)
- 2. A leállt „W”-vel kezdődő service-ek neveit rendezzük csökkenő ABC sorrendbe.
- 3. A „C:\temp\” mappában keressük meg a legrégebben módosított file-t, és kérjük le az elérési útvonalát, valamint a méretét (ne keressen almappákban)
- 4. ...keressen almappákban ☺ (-**Recurse**)
- 5. Mekkora a „C:\temp\” mappában lévő fájlok összmérete?
- 6. Kérjük le a gépünkben található memória modulok számát, méretüket, gyártóit, sorozatszámát, és sebességüket. (**win32_physicalmemory**)
- 7. Az application log első 7 bejegyzését kérjük le, írassuk ki a tartalmát („**Message**”)
- 8. Hozzunk létre tömböt mely első eleme 500 utolsó pedig 314. Hány eleme van a tömbnek? Mennyi az elemek átlaga és összege?
- 9. Hozzunk létre egy változót mely értéke a saját nevünk. Egyetlen paranccsal alakítsuk nagybetűssé a szöveget, majd – egy tetszőlegesen kiválasztott betűt – cseréljünk le „|” (pipe) karakterre.

Ellenőrző feladatok II.

(Active Directory specifikus)

- 1. Az Active Directory-ből lekért usereket csoportosítsuk „Enabled” státusz szerint, ezáltal számoljuk meg melyikből mennyi van?
- 2. Ki volt az a user aki legutoljára lépett be, és mondjuk meg ez hány másodperce történt.
- 3. Akadályozzuk meg, hogy bármelyik „A” betűvel kezdődő user be tudjon lépni a domain-ba (pl.: tiltsuk le ezeket az accountokat) (**Disable-ADAccount**)
- 4. Hány darab csoport létezik a domain-ben? (**Get-ADGroup**)