

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)

Fejlesztői felületek

- **Konzol – Parancssoros felület. Előnyei:**

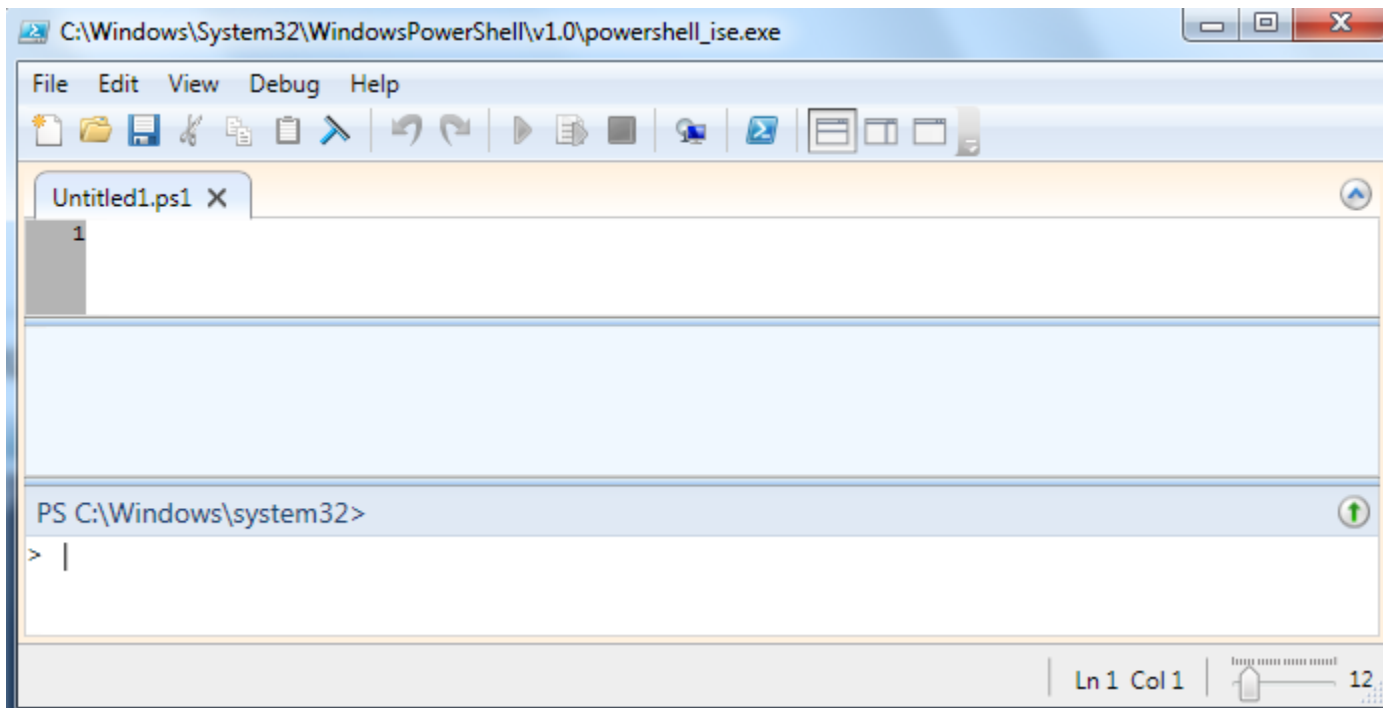
- TAB : „Intellisense” → Automatikus parancs kiegészítés
- Shift-TAB : Reverse
- Esc : Törli az aktuális sort
- F7 : History



The image shows a screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell". The window has a dark blue background and a white border. The text inside the window reads: "Windows PowerShell", "Copyright (C) 2009 Microsoft Corporation. All rights reserved.", and "PS C:\Windows\system32>". The window includes standard Windows window controls (minimize, maximize, close) in the top right corner and a scrollbar on the right side.

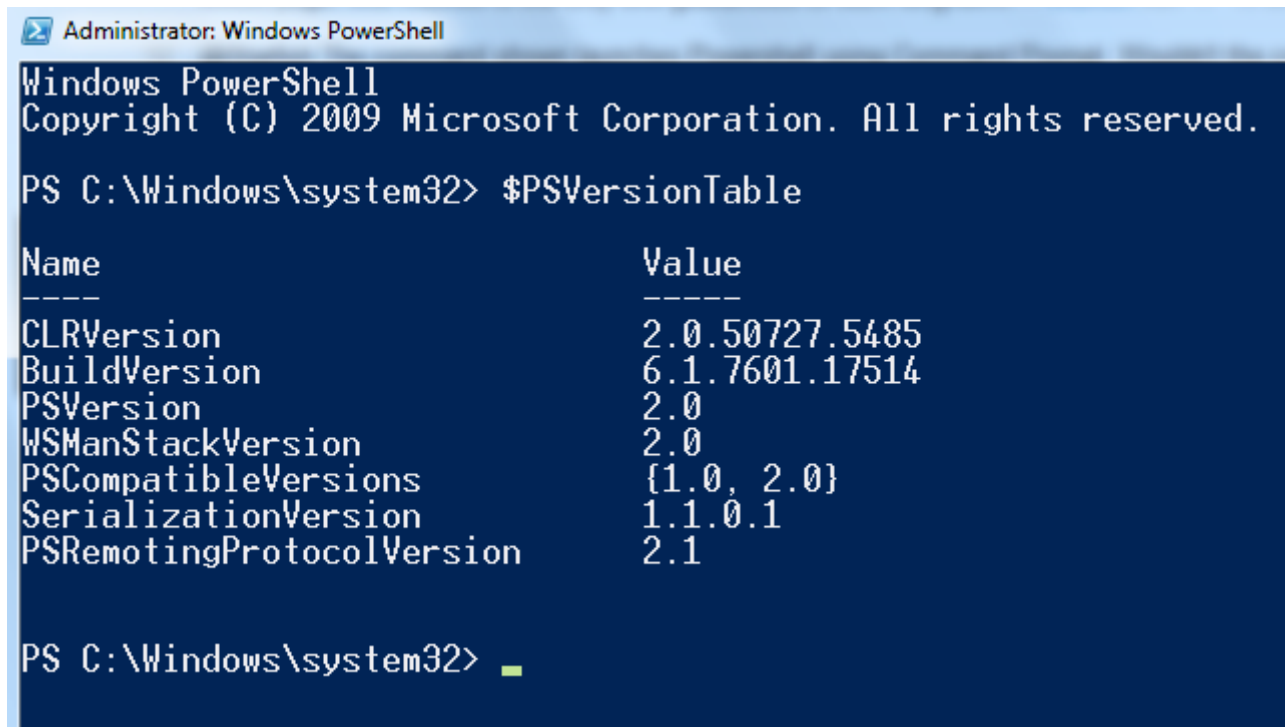
Fejlesztői felületek

- **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 Ige-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 = ServicesDeper
Disposed  Event           System.EventHandler Disposed(Sys
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     AxlInstSV         ActiveX Telepítő (AxlInstSV)
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	16000	66		6612	audiodev

```
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	wuauerv	Windows Update
Stopped	WSearch	Windows Search
Running	wscsvc	Biztonsági központ
Running	WPDBusEnum	Hordozható eszközök számbavételi sz...
Stopped	WPCSvc	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:
- **\$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.IFor

```
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

`'$szoveg-ban élek.'`

nincs behelyettesítés

```
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
```

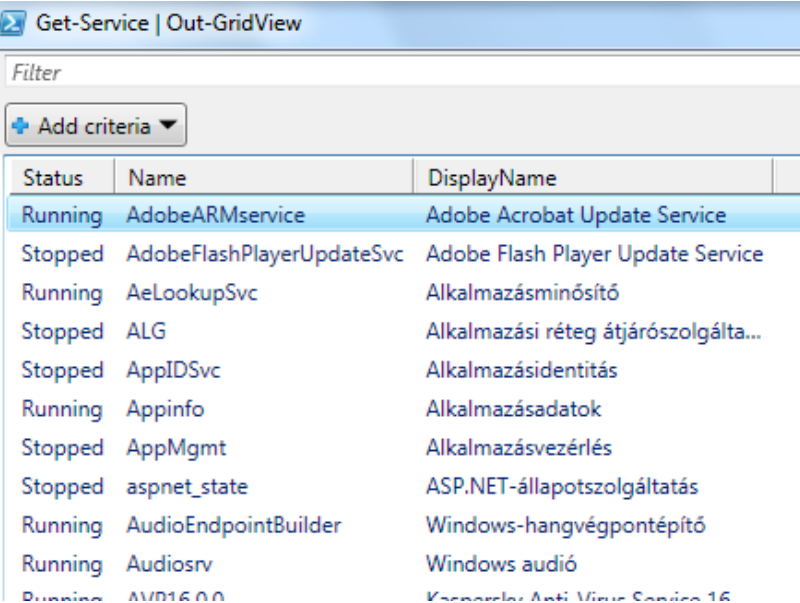
```
PS C:\Windows\system32> Get-WMIObject -Class win32_processor | fl numberofcores
```

```
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 átjárószolgálta...
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
```