

Operációs rendszerek BSc

4. Gyak.

2022. 03. 02.

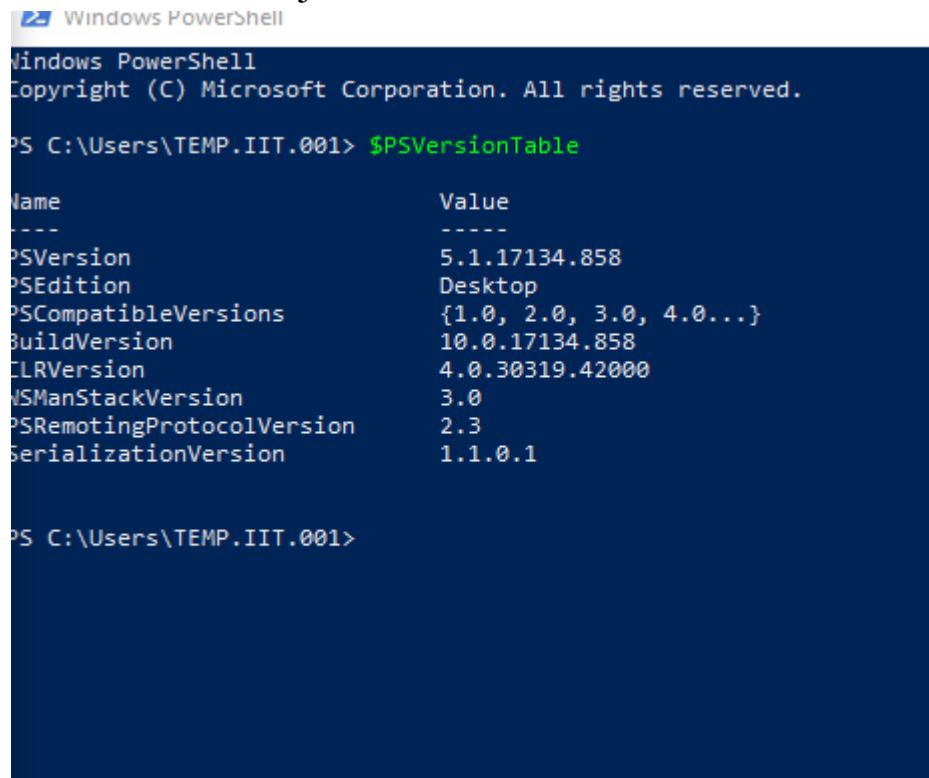
Készítette:

Biszterszky Máttyás Bsc
Programtervező informatikus
L27NCJ

Miskolc, 2022

1.

1 PowerShell verziójának lekérése



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

PS C:\Users\TEMP.IIT.001> $PSVersionTable

Name                           Value
----                           -
PSVersion                      5.1.17134.858
PSEdition                     Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.17134.858
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

PS C:\Users\TEMP.IIT.001>
```

2 Aktuális dátum és idő lekérdezése

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

PS C:\Users\TEMP.IIT.001> $PSVersionTable

Name                           Value
----                           -
PSVersion                      5.1.17134.858
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.17134.858
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

PS C:\Users\TEMP.IIT.001> Get-Service | Get-Member

TypeName: System.ServiceProcess.ServiceController

Name                MemberType Definition
-----
Name                AliasProperty Name = ServiceName
RequiredServices    AliasProperty RequiredServices = ServicesDependedOn
Disposed            Event          System.EventHandler Disposed(System.Object, System.EventArgs)
Close               Method         void Close()
Continue            Method         void Continue()
CreateObjRef        Method         System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Dispose             Method         void Dispose(), void IDisposable.Dispose()
Equals              Method         bool Equals(System.Object obj)
ExecuteCommand       Method         void ExecuteCommand(int command)
GetHashCode          Method         int GetHashCode()
GetLifetimeService  Method         System.Object GetLifetimeService()
GetType             Method         type GetType()
InitializeLifetimeService Method         System.Object InitializeLifetimeService()
Pause               Method         void Pause()
Refresh             Method         void Refresh()
Start               Method         void Start(), void Start(string[] args)
Stop                Method         void Stop()
WaitForStatus       Method         void WaitForStatus(System.ServiceProcess.ServiceControllerStatus desiredStatus), void Wait..
CanPauseAndContinue Property       bool CanPauseAndContinue {get;}
CanShutdown         Property       bool CanShutdown {get;}
CanStop             Property       bool CanStop {get;}
Container            Property       System.ComponentModel.IContainer Container {get;}
DependentServices   Property       System.ServiceProcess.ServiceController[] DependentServices {get;}
DisplayName          Property       string DisplayName {get;set;}
MachineName          Property       string MachineName {get;set;}
ServiceHandle        Property       System.Runtime.InteropServices.SafeHandle ServiceHandle {get;}
ServiceName          Property       string ServiceName {get;set;}
ServicesDependedOn   Property       System.ServiceProcess.ServiceController[] ServicesDependedOn {get;}
ServiceType          Property       System.ServiceProcess.ServiceType ServiceType {get;}
Site                 Property       System.ComponentModel.ISite Site {get;set;}
StartType            Property       System.ServiceProcess.ServiceStartMode StartType {get;}
Status               Property       System.ServiceProcess.ServiceControllerStatus Status {get;}
ToString             ScriptMethod   System.Object ToString();

PS C:\Users\TEMP.IIT.001>
```

3 Szolgáltatások lekérdezése

Windows PowerShell

```
Stopped TieringEngineSe... Storage Tiers Management
Running TimeBrokerSvc Time Broker
Running TokenBroker Web Account Manager
Running TrkKws Distributed Link Tracking Client
Stopped TrustedInstaller Windows Modules Installer
Stopped tzautoupdate Auto Time Zone Updater
Stopped UevAgentService User Experience Virtualization Service
Running UmRdpService Remote Desktop Services UserMode Po...
Stopped UnistoreSvc_ee968 User Data Storage_ee968
Stopped upnphost UPnP Device Host
Stopped UserDataSvc_ee968 User Data Access_ee968
Running UserManager User Manager
Running UsoSvc Update Orchestrator Service
Stopped VacSvc Volumetric Audio Compositor Service
Running VaultSvc Credential Manager
Stopped vds Virtual Disk
Stopped vmicguestinterface Hyper-V Guest Service Interface
Stopped vmicheartbeat Hyper-V Heartbeat Service
Stopped vmickvpexchange Hyper-V Data Exchange Service
Stopped vmicrdv Hyper-V Remote Desktop Virtualizati...
Stopped vmictimesync Hyper-V Time Synchronization Service
Stopped vmicvmsession Hyper-V PowerShell Direct Service
Stopped vmicvss Hyper-V Volume Shadow Copy Requestor
Stopped vmicshutdown Hyper-V Guest Shutdown Service
Stopped VSS Volume Shadow Copy
Stopped VSStandardColle... Visual Studio Standard Collector Se...
Stopped VSStandardColle... Visual Studio Standard Collector Se...
Running W32Time Windows Time
Stopped WaaSMedicSvc Windows Update Medic Service
Stopped WalletService WalletService
Stopped WarpJITSvc WarpJITSvc
Stopped wbengine Block Level Backup Engine Service
Running WbioSvc Windows Biometric Service
Running Wcmsvc Windows Connection Manager
Stopped wcncsvc Windows Connect Now - Config Registrar
Running WdiServiceHost Diagnostic Service Host
Running WdiSystemHost Diagnostic System Host
Running WdNisSvc Windows Defender Antivirus Network ...
Stopped WebClient WebClient
Stopped Wecsvc Windows Event Collector
Stopped WEPHOSTSvc Windows Encryption Provider Host Se...
Stopped werclpsupport Problem Reports and Solutions Contr...
Stopped WerSvc Windows Error Reporting Service
Stopped WFDSConMgrSvc Wi-Fi Direct Services Connection Ma...
Stopped WiaRpc Still Image Acquisition Events
Running WinDefend Windows Defender Antivirus Service
Running WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running Winmgmt Windows Management Instrumentation
Stopped WinRM Windows Remote Management (WS-Manag...
Stopped wisvc Windows Insider Service
Stopped WlanSvc WLAN AutoConfig
Running wldsvc Microsoft Account Sign-in Assistant
Stopped wlpasvc Local Profile Assistant Service
Stopped wmiApSrv WMI Performance Adapter
Stopped WMPNetworkSvc Windows Media Player Network Sharin...
Stopped workfolderssvc Work Folders
Stopped WpcMonSvc Parental Controls
Stopped WPDBusEnum Portable Device Enumerator Service
Running WpnService Windows Push Notifications System S...
Running WpnUserService_... Windows Push Notifications User Ser...
Running wscsvc Security Center
Running WSearch Windows Search
Running wuauerv Windows Update
Stopped WwanSvc WWAN AutoConfig
Stopped xbgm Xbox Game Monitoring
Stopped XblAuthManager Xbox Live Auth Manager
Stopped XblGameSave Xbox Live Game Save
Stopped XboxGipSvc Xbox Accessory Management Service
Stopped XboxNetApiSvc Xbox Live Networking Service
```

4 „processz” nevű alias létrehozása, futtatása

```
PS C:\> Get-ChildItem

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         2017. 04. 06.          8:05          7af4af4e1f79ad1f6260ad
d-----         2017. 04. 07.         11:10          app
d-----         2016. 05. 24.         12:21          Intel
d-----         2016. 02. 13.         14:21          Logs
d-----         2018. 04. 12.          1:38          PerfLogs
d-----         2021. 09. 10.         10:33          portapps
d-r---         2021. 09. 10.         11:20          Program Files
d-r---         2021. 09. 10.         11:38          Program Files (x86)
da----         2016. 06. 21.          9:40          Python34
d-----         2019. 11. 26.         10:09          test
d-r---         2022. 03. 02.         12:11          Users
d-----         2020. 07. 06.         12:07          Windows
d-----         2020. 09. 18.          9:40          xampp
d-----         2022. 02. 15.         16:02          YE6BLB
-a----         2022. 03. 02.         11:10          0 HaxLogs.txt
-a----         2016. 08. 02.         20:57          0 Recovery.txt

PS C:\>
```

5 Parancsok rövidített nevének (alias) lekérdezése

```
PS C:\> Get-Alias

CommandType      Name                                Version      Source
-----
Alias            % -> ForEach-Object
Alias            ? -> Where-Object
Alias            ac -> Add-Content
Alias            asnp -> Add-PSSnapin
Alias            cat -> Get-Content
Alias            cd -> Set-Location
Alias            CFS -> ConvertFrom-String          3.1.0.0      Microsoft.PowerShell.Utility
Alias            chdir -> Set-Location
Alias            clc -> Clear-Content
Alias            clear -> Clear-Host
Alias            clhy -> Clear-History
Alias            cli -> Clear-Item
Alias            clip -> Clear-ItemProperty
Alias            cls -> Clear-Host
Alias            clv -> Clear-Variable
Alias            cnsn -> Connect-PSSession
Alias            compare -> Compare-Object
Alias            copy -> Copy-Item
Alias            cp -> Copy-Item
Alias            cpi -> Copy-Item
Alias            cpp -> Copy-ItemProperty
Alias            curl -> Invoke-WebRequest
Alias            cvpa -> Convert-Path
Alias            dbp -> Disable-PSBreakpoint
Alias            del -> Remove-Item
Alias            diff -> Compare-Object
Alias            dir -> Get-ChildItem
Alias            dnsn -> Disconnect-PSSession
Alias            ebp -> Enable-PSBreakpoint
Alias            echo -> Write-Output
Alias            epal -> Export-Alias
Alias            epsv -> Export-Csv
Alias            epsn -> Export-PSSession
Alias            erase -> Remove-Item
Alias            etsn -> Enter-PSSession
Alias            exsn -> Exit-PSSession
Alias            fc -> Format-Custom
Alias            fhx -> Format-Hex                  3.1.0.0      Microsoft.PowerShell.Utility
Alias            fl -> Format-List
Alias            foreach -> ForEach-Object
Alias            ft -> Format-Table
Alias            fw -> Format-Wide
Alias            gal -> Get-Alias
Alias            gbp -> Get-PSBreakpoint
Alias            gc -> Get-Content
Alias            gcb -> Get-Clipboard                3.1.0.0      Microsoft.PowerShell.Management
Alias            gci -> Get-ChildItem
Alias            gcm -> Get-Command
Alias            gcs -> Get-PSCallStack
Alias            gdr -> Get-PSDrive
Alias            ghy -> Get-History
Alias            gi -> Get-Item
Alias            gin -> Get-ComputerInfo           3.1.0.0      Microsoft.PowerShell.Management
Alias            gjb -> Get-Job
Alias            gl -> Get-Location
Alias            gm -> Get-Member
Alias            gmo -> Get-Module
Alias            gp -> Get-ItemProperty
Alias            gps -> Get-Process
Alias            gpv -> Get-ItemPropertyValue
Alias            group -> Group-Object
Alias            gsn -> Get-PSSession
Alias            gsnp -> Get-PSSnapin
Alias            gsv -> Get-Service
Alias            gtz -> Get-TimeZone              3.1.0.0      Microsoft.PowerShell.Management
```

6 „processz” nevű alias létrehozása, futtatása

```
PS C:\> New-Alias "processz" Get-Process
PS C:\> processz
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
116	7	1404	1356		2300	0	98.0.4758.102_98.0.4758.82_chrome_updater
304	18	7572	12324	0,17	7228	1	ApplicationFrameHost
141	9	2196	5920		5820	0	armsvc
156	10	6532	11628	0,23	7136	0	audiodg
163	10	1940	8288	0,05	7500	1	browser_broker
166	9	1996	5816	0,02	1264	1	chrome
350	19	55068	98368	8,03	2952	1	chrome
243	15	6976	16556	0,11	4228	1	chrome
240	14	7280	15252	0,16	4708	1	chrome
410	49	553196	553796	82,47	6796	1	chrome
293	17	11612	30608	5,92	7012	1	chrome
297	16	45996	80676	16,98	7024	1	chrome
1505	56	69756	124908	44,75	8176	1	chrome
197	14	7036	15772	0,13	8664	1	chrome
349	18	142400	193460	8,22	9840	1	chrome
336	18	53592	98352	18,09	10004	1	chrome
282	16	30640	72080	2,47	11220	1	chrome
115	6	1168	168		4048	0	CompatTelRunner
626	25	70020	2404		5836	0	CompatTelRunner
145	9	5668	372		1500	0	conhost
248	13	4048	13892	3,19	5700	1	conhost
116	7	5328	4672		8684	0	conhost
370	15	5544	14752	10,88	4804	1	ctfmon
684	24	1944	4612		516	0	csrss
542	16	2548	4908		596	1	csrss
146	8	2064	11288	0,55	5332	1	dllhost
218	19	4316	12176	0,19	9700	1	dllhost
594	41	102820	63852		440	1	dwm
2098	73	43388	85580	34,38	2152	1	explorer
179	10	2056	5600		5948	0	fdhost
97	6	1028	4704		8592	0	fdlauncher
45	8	3296	4016		980	1	fontdrvhost
45	6	1580	2508		988	0	fontdrvhost
216	13	2592	1544		4772	0	GoogleUpdate
216	14	2420	212		5440	0	GoogleUpdate
366	20	7076	16040		8600	0	GoogleUpdate
0	0	52	8		0	0	Idle
481	36	52800	23236		7976	0	Launchpad
1762	30	7708	16964		772	0	lsass
0	0	1476	1152		1920	0	Memory Compression
863	71	25920	25708	0,72	7400	1	MicrosoftEdge
405	18	5360	9700	0,20	7860	1	MicrosoftEdgeCP
519	22	6120	14696	0,17	7868	1	MicrosoftEdgeCP
673	68	170284	108256		2996	0	mpdwsvc
161	10	1964	8444	0,03	6500	1	MSASCuIL
261	23	54088	16824		8336	0	MsDtsSrvr
1773	38	65364	36064		7628	0	msmdsrv
923	84	276580	181952		3064	0	MsMpEng
663	19	330044	41592		3728	0	mysqld
195	13	4416	8648		2584	0	NisSrv
652	42	21224	60636	2,78	9412	1	OneDrive
615	29	59056	70872	3,55	5000	1	powershell
0	30	7964	16636		96	0	Registry
442	22	6752	26140	1,67	1884	1	RuntimeBroker
446	22	7664	25900	30,55	6220	1	RuntimeBroker

7 Meghajtón lévő szolgáltatások listázása (formázott lista/tábla)


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

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

```
Name : AJRouter  
Status : Stopped
```

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

```
Name : AppIDSvc  
Status : Stopped
```

```
Name : Appinfo  
Status : Stopped
```

```
Name : AppMgmt  
Status : Stopped
```

```
Name : AppReadiness  
Status : Stopped
```

```
Name : AppVClient  
Status : Stopped
```

```
Name : AppXSvc  
Status : Stopped
```

```
Name : aspnet_state  
Status : Stopped
```

```
Name : AssignedAccessManagerSvc  
Status : Stopped
```

```
Name : AudioEndpointBuilder  
Status : Running
```

```
Name : Audiosrv  
Status : Running
```

```
Name : AxInstSV  
Status : Stopped
```

```
Name : BcastDVRUserService_ee968  
Status : Stopped
```

```
Name : BDESVC  
Status : Stopped
```

```
Name : BFE  
Status : Running
```

```
Name : BITS  
Status : Running
```

```
Name : BluetoothUserService_ee968  
Status : Stopped
```

```
Name : BrokerInfrastructure  
Status : Running
```

```
Name : Browser  
Status : Running
```

```
Name : BTAGService  
Status : Stopped
```

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

Name	Status
----	-----
AdobeARMservice	Running
AJRouter	Stopped
ALG	Stopped
AppIDSvc	Stopped
Appinfo	Stopped
AppMgmt	Stopped
AppReadiness	Stopped
AppVClient	Stopped
AppXSvc	Stopped
aspnet_state	Stopped
AssignedAccessManagerSvc	Stopped
AudioEndpointBuilder	Running
Audiosrv	Running
AxInstSV	Stopped
BcastDVRUserService_ee968	Stopped
BDESVC	Stopped
BFE	Running
BITS	Running
BluetoothUserService_ee968	Stopped
BrokerInfrastructure	Running
Browser	Running
BTAGService	Stopped
BthAvctpSvc	Stopped
bthserv	Stopped
camsvc	Stopped
CaptureService_ee968	Stopped
CDPSvc	Running
CDPUserService_ee968	Running
CertPropSvc	Running
ClipSVC	Stopped
COMSysApp	Stopped
CoreMessagingRegistrar	Running
CryptSvc	Running
CscService	Stopped
DcomLaunch	Running
defragsvc	Stopped
DeviceAssociationService	Running
DeviceInstall	Stopped
DevicePickerUserSvc_ee968	Stopped
DevicesFlowUserSvc_ee968	Stopped
DevQueryBroker	Stopped
Dhcp	Running
diagnosticshub.standardcollector.service	Stopped
diagsvc	Stopped
DiagTrack	Running
DmEnrollmentSvc	Stopped
dmwappushservice	Stopped
Dnscache	Running
DoSvc	Running
dot3svc	Stopped
DPS	Running
DsmSvc	Stopped
DsSvc	Stopped
DusmSvc	Running
Eaphost	Stopped
EFS	Stopped
embeddedmode	Stopped
EntAppSvc	Stopped
EventLog	Running
EventSystem	Running
Fax	Stopped
fdPHost	Stopped
FDResPub	Stopped
fhsvc	Stopped
FontCache	Running
FontCache3.0.0.0	Stopped
FrameServer	Stopped
GoogleChromeElevationService	Stopped

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

Name	Status
----	-----
AdobeARMservice	Running
AJRouter	Stopped
ALG	Stopped
AppIDSvc	Stopped
Appinfo	Stopped
AppMgmt	Stopped
AppReadiness	Stopped
AppVClient	Stopped
AppXSvc	Stopped
aspnet_state	Stopped
AssignedAccessManagerSvc	Stopped
AudioEndpointBuilder	Running
Audiosrv	Running
AxInstSV	Stopped
BcastDVRUserService_ee968	Stopped
BDESVC	Stopped
BFE	Running
BITS	Running
BluetoothUserService_ee968	Stopped
BrokerInfrastructure	Running
Browser	Running
BTAGService	Stopped
BthAvctpSvc	Stopped
bthserv	Stopped
camsvc	Stopped
CaptureService_ee968	Stopped
CDPSvc	Running
CDPUserSvc_ee968	Running
CertPropSvc	Running
ClipSvc	Stopped
COMSysApp	Stopped
CoreMessagingRegistrar	Running
CryptSvc	Running
CscService	Stopped
DcomLaunch	Running
defragsvc	Stopped
DeviceAssociationService	Running
DeviceInstall	Stopped
DevicePickerUserSvc_ee968	Stopped
DevicesFlowUserSvc_ee968	Stopped
DevQueryBroker	Stopped
Dhcp	Running
diagnosticshub.standardcollector.service	Stopped
diagsvc	Stopped
DiagTrack	Running
DmEnrollmentSvc	Stopped
dmwappushservice	Stopped
Dnscache	Running
DoSvc	Running
dot3svc	Stopped
DPS	Running
DsmSvc	Stopped
DsSvc	Stopped
DusmSvc	Running
Eaphost	Stopped
EFS	Stopped
embeddedmode	Stopped
EntAppSvc	Stopped
EventLog	Running
EventSystem	Running
Fax	Stopped
fdPHost	Stopped
FDResPub	Stopped
Shvc	Stopped

8 Objektumok, névszerinti sorba rendezése (növekvő, csökkenő)

```
PS C:\> Sort-Object
PS C:\> processz | Sort-Object
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
116	7	1404	1352		2300	0	98.0.4758.102_98.0.4758.82_chrome_updater
304	18	7572	12300	0,17	7228	1	ApplicationFrameHost
141	9	2124	5896		5820	0	armsvc
156	10	6364	11524	0,20	224	0	audiodg
163	10	1940	8288	0,05	7500	1	browser_broker
220	14	10760	22516	0,09	8996	1	chrome
197	14	7064	15776	0,13	8664	1	chrome
1584	58	71884	127604	52,70	8176	1	chrome
284	16	31412	73668	2,47	11220	1	chrome
318	17	131980	185160	9,80	9840	1	chrome
310	16	35252	75652	1,45	9440	1	chrome
299	16	46764	82184	17,00	7024	1	chrome
241	15	6944	16316	0,11	4228	1	chrome
350	19	55660	100308	8,70	2952	1	chrome
173	9	1996	5748	0,02	1264	1	chrome
334	22	11776	30804	6,86	7012	1	chrome
411	43	313500	324620	89,92	6796	1	chrome
243	14	7328	15288	0,17	4708	1	chrome
611	25	69832	2272		5836	0	CompatTelRunner
113	6	1132	276		4048	0	CompatTelRunner
116	7	5328	4580		8684	0	conhost
244	12	4000	13592	6,06	5700	1	conhost
145	9	5668	372		1500	0	conhost
366	15	6200	15420	14,13	4804	1	ctfmon
546	16	2548	4904		596	1	csrss
676	23	1840	4612		516	0	csrss
226	19	4300	11764	0,25	9700	1	dllhost
142	8	2008	11272	0,63	5332	1	dllhost
594	41	103360	60156		440	1	dwm
2166	74	40984	83996	37,89	2152	1	explorer
179	10	2056	5588		5948	0	fdhost
97	6	1028	4652		8592	0	fdlauncher
45	6	1580	2500		988	0	fontdrvhost
45	8	3296	3972		980	1	fontdrvhost
366	20	7940	16876		8600	0	GoogleUpdate
212	13	2268	1100		5440	0	GoogleUpdate
210	13	2520	2124		4772	0	GoogleUpdate
0	0	52	8		0	0	Idle
467	36	52192	17796		7976	0	Launchpad
1733	30	7856	16900		772	0	lsass
0	0	772	44556		1920	0	Memory Compression
863	71	25920	25708	0,72	7400	1	MicrosoftEdge
519	22	6120	14696	0,17	7868	1	MicrosoftEdgeCP
405	18	5360	9700	0,20	7860	1	MicrosoftEdgeCP
161	10	1964	8280	0,03	6500	1	MSASCuil
261	23	54088	16824		8336	0	MsDtsSrvr
1775	38	65396	33200		7628	0	msmdsrv
858	85	270564	161352		3064	0	MsMpEng
659	19	329988	19332		3728	0	mysqld
191	13	4248	8272		2584	0	NisSrv
633	42	21008	59164	2,78	9412	1	OneDrive
653	29	63156	71428	5,63	5000	1	powershell
0	30	7844	16304		96	0	Registry
494	23	7288	25152	10,63	6816	1	RuntimeBroker
150	8	1952	6708	0,06	7664	1	RuntimeBroker
444	23	6820	26156	1,69	1884	1	RuntimeBroker
456	22	7928	25440	30,66	6220	1	RuntimeBroker
146	9	1844	7592		8476	0	SearchFilterHost
2040	79	45912	45212		5152	0	SearchIndexer
369	12	2752	9508		11052	0	SearchProtocolHost
1371	102	145740	84292	132,48	3252	1	SearchUI

9 Nevek lekérdezése amelyeknek első két betűje „wi”

PS C:\> processz | Sort-Object -Descending

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
243	11	1852	5984		936	0	WUDFHost
174	11	3160	9428		2736	0	WmiPrvSE
232	11	2528	7648		668	1	winlogon
151	10	1300	5604		624	0	wininit
119	8	1784	6568		3860	0	TrustedInstaller
159	10	2216	8688		5620	0	TiWorker
330	31	6476	16560	0,75	4864	1	taskhostw
324	18	5592	15164	0,30	10816	1	taskhostw
218	11	3216	14724	0,08	3116	1	SystemSettingsBroker
3395	0	184	476		4	0	System
317	13	2980	11468		2000	0	svchost
455	38	53544	39440		1908	0	svchost
325	12	2384	7912		2096	0	svchost
123	8	1588	5556		2088	0	svchost
192	11	2100	8232		1812	0	svchost
163	9	1932	7152		1728	0	svchost
161	10	2056	7572		1864	0	svchost
177	10	1868	6944		1856	0	svchost
203	16	2152	10648		2212	0	svchost
163	9	5252	12616		2364	0	svchost
399	14	7796	15676		2328	0	svchost
209	13	2256	8440		2488	0	svchost
210	10	2768	8380		2456	0	svchost
176	10	2112	7044		2248	0	svchost
238	13	2764	6460		2240	0	svchost
244	13	4008	14136	0,98	2268	1	svchost
151	12	1756	6388		2256	0	svchost
174	10	2128	6356		1160	0	svchost
135	22	4492	6436		1156	0	svchost
186	11	2076	8588		1220	0	svchost
194	12	1772	6896		1164	0	svchost
84	5	980	3692		884	0	svchost
307	11	2892	8424		508	0	svchost
415	14	3724	9772		1116	0	svchost
1286	23	23804	29268		912	0	svchost
152	9	2720	11484		1352	0	svchost
429	13	14700	15936		1644	0	svchost
278	14	2808	10876		1612	0	svchost
223	14	77064	85072		1716	0	svchost
173	7	1328	5500		1712	0	svchost
217	10	2424	7220		1396	0	svchost
266	13	3492	14760		1360	0	svchost
409	18	6844	13816		1520	0	svchost
254	14	3876	8788		1424	0	svchost
194	11	2276	8592		4468	0	svchost
1287	106	108376	100792		4120	0	svchost
352	15	4120	14324		5236	0	svchost
828	36	23728	28384		4788	0	svchost
231	14	2320	8200		3712	0	svchost
139	15	1692	6588		3704	0	svchost
118	7	1292	5316		3884	0	svchost
217	15	4044	13420		3844	0	svchost
274	17	3964	14180		5380	0	svchost
515	31	10876	20432		8720	0	svchost
170	0	1000	6640		6512	0	svchost

10 Objektumok állapot szerinti csoportosítása

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

Status	Name	DisplayName
Running	W32Time	Windows Time

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

Status	Name	DisplayName
Stopped	WiaRpc	Still Image Acquisition Events
Running	WinDefend	Windows Defender Antivirus Service
Running	WinHttpAutoProx...	WinHTTP Web Proxy Auto-Discovery Se...
Running	Winmgmt	Windows Management Instrumentation
Stopped	WinRM	Windows Remote Management (WS-Manag...
Stopped	wisvc	Windows Insider Service

11 Objektumok megszámlálása

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

Count	Name	Group
98	Running	{AdobeARMservice, AudioEndpointBuilder, Audiosrv, BFE...}
170	Stopped	{AJRouter, ALG, AppIDSvc, Appinfo...}

```
PS C:\>
```

12 Objektumok megszámlálása (max, min, avg, sum szerint)

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

Count	: 268
Average	:
Sum	:
Maximum	:
Minimum	:
Property	:

13 Windows idő lekérdezése

```
PS C:\> (Get-Service).count
268
PS C:\> Get-Date -format "YYYY/MM:mm"
YYYY. 12:56
PS C:\> Get-Date -format "YYYY:MM:mm"
YYYY:12:56
PS C:\> Get-Date -format "yyyy/MM:mm"
2022.12:56
PS C:\> Get-Date -format "yyyy/MM:mm"
2022. 12:56
PS C:\> Get-Date -format "yyyy,MM:mm"
2022,12:56
PS C:\>
```

14 „szoveg” változó létrehozása és értékadás: Miskolc

```
2022,12:56
PS C:\> $szoveg="Miskolc"
PS C:\> $szoveg
Miskolc
PS C:\>
```

15 Műveletek végrehajtása a változó értékeivel

```
PS C:\> $szoveg.length
7
PS C:\> $szoveg.ToUpper

OverloadDefinitions
-----
string ToUpper()
string ToUpper(cultureinfo culture)

PS C:\> $szoveg.ToUpper()
MISKOLC
PS C:\> $szoveg.Contains()
>>
Cannot find an overload for "Contains" and the arguments
At line:1 char:1
+ $szoveg.Contains()
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Null],
+ FullyQualifiedErrorId : MethodCountCouldNotFindMethod

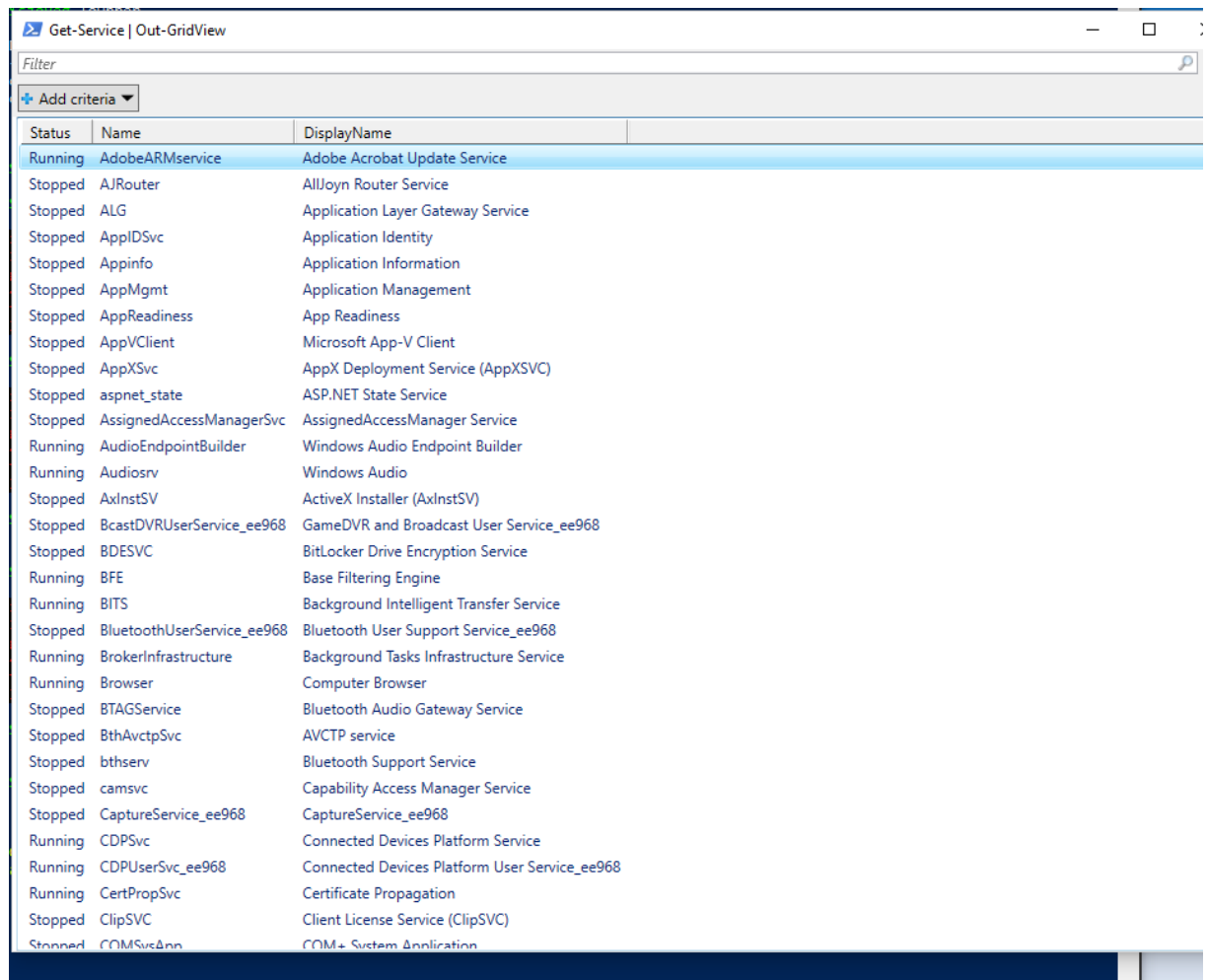
PS C:\> $szoveg.Contains()
>>
Cannot find an overload for "Contains" and the arguments
At line:1 char:1
+ $szoveg.Contains()
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Null],
+ FullyQualifiedErrorId : MethodCountCouldNotFindMethod

PS C:\> $szoveg.Contains("Mi")
>>
True
PS C:\> $szoveg.Contains("Mi", "im")
>>
Cannot find an overload for "Contains" and the arguments
At line:1 char:1
+ $szoveg.Contains("Mi", "im")
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Null],
+ FullyQualifiedErrorId : MethodCountCouldNotFindMethod

PS C:\> $szoveg.Replace("Mi", "im")
>>
imskolc
PS C:\> $szoveg.Split("s")
>>
Mi
kolc
PS C:\>
```

16

17 Get Services



Status	Name	DisplayName
Running	AdobeARMSvc	Adobe Acrobat Update Service
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Stopped	Appinfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	aspnet_state	ASP.NET State Service
Stopped	AssignedAccessManagerSvc	AssignedAccessManager Service
Running	AudioEndpointBuilder	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserService_ee968	GameDVR and Broadcast User Service_ee968
Stopped	BDESVC	BitLocker Drive Encryption Service
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Service
Stopped	BluetoothUserService_ee968	Bluetooth User Support Service_ee968
Running	BrokerInfrastructure	Background Tasks Infrastructure Service
Running	Browser	Computer Browser
Stopped	BTAGService	Bluetooth Audio Gateway Service
Stopped	BthAvctpSvc	AVCTP service
Stopped	bthserv	Bluetooth Support Service
Stopped	camsvc	Capability Access Manager Service
Stopped	CaptureService_ee968	CaptureService_ee968
Running	CDPSvc	Connected Devices Platform Service
Running	CDPUserService_ee968	Connected Devices Platform User Service_ee968
Running	CertPropSvc	Certificate Propagation
Stopped	ClipSVC	Client License Service (ClipSVC)
Stopped	COMSurfAnn	COM+ System Application

18 Szöveg szerkesztés, c# parancsok

```
PS C:\> $szoveg.Replace("Mi", "im")
>>
imskolc
PS C:\> $szoveg.Split("s")
>>
Mi
kolc
PS C:\> Get-Service | Out-GridView
PS C:\> $n= "C:\127ncj.txt"
PS C:\> $n= "C:\Users\TEMP.IIT.001\Documents\127ncj.txt"
PS C:\> $127ncj = Get-Content $n
PS C:\> $127ncj
Biszterszky Mátyás
PS C:\> $127ncj.Count
1
PS C:\> $127ncj
Biszterszky Mátyás
PS C:\> $127ncj.Count
1
```



```
PS C:\> Get-Item $n

Directory: C:\Users\TEMP.IIT.001\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----      2022. 03. 02.      13:08             18 127ncj.txt

PS C:\>
```

```
PS C:\> $szoveg.Replace("Mi", "im")
>>
imiskolc
PS C:\> $szoveg.Split("s")
>>
Mi
kolc
PS C:\> Get-Service | Out-GridView
PS C:\> $n= "C:\127ncj.txt"
PS C:\> $n= "C:\Users\TEMP.IIT.001\Documents\127ncj.txt"
PS C:\> $127ncj = Get-Content $n
PS C:\> $127ncj
Biszterszky Mátyás
PS C:\> $127ncj.Count
1
PS C:\> $127ncj
Biszterszky Mátyás
PS C:\> $127ncj.Count
1
PS C:\> Get-Item $f
Get-Item : Cannot bind argument to parameter 'Path' because it is null.
At line:1 char:10
+ Get-Item $f
+ ~~~~~
+ CategoryInfo          : InvalidData: (:) [Get-Item], ParameterBindingVali
+ FullyQualifiedErrorId : ParameterArgumentValidationErrorNullNotAllowed,M

PS C:\> Get-Item $n

Directory: C:\Users\TEMP.IIT.001\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----      2022. 03. 02.      13:08             18 127ncj.txt

PS C:\>
```

2. Feladat

- a. Jelentés készítése az aktuálisan futó processzekről, a processzek és adataik kilistázása top paranccsal

```
top - 19:48:58 up 82 days, 20:43, 1 user, load average: 0.01, 0.02, 0.05
Tasks: 3 total, 1 running, 2 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.1 sy, 0.0 ni, 99.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 8025292 total, 4935036 free, 1093668 used, 1996588 buff/cache
KiB Swap: 2097148 total, 2097148 free, 0 used. 6708136 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
19772	biszter+	20	0	87036	4448	3548	S	0.0	0.1	0:00.01	sshd
19773	biszter+	20	0	16432	5068	2992	S	0.0	0.1	0:00.10	bash
19791	biszter+	20	0	39792	3480	2932	R	0.0	0.0	0:00.00	top

- b.) A memóriáról kapott adatok kilistázása vmstat paranccsal

```
biszterszky@jerry:~$ vmstat
procs -----memory----- --swap-- -----io----- -system-- -----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 4941164 2152 1986248 0 0 0 0 0 0 0 0 0 100 0 0
biszterszky@jerry:~$
```

- c. A bejelentkezés információi

```
biszterszky@jerry:~$ vmstat
procs -----memory----- --swap-- -----io----- -system-- -----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 4941164 2152 1986248 0 0 0 0 0 0 0 0 0 100 0 0
biszterszky@jerry:~$ w
19:50:44 up 82 days, 20:45, 1 user, load average: 0.05, 0.03, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
biszterszky@jerry:~$
biszterszky@jerry:~$
```

- d. A rendszer indulása óta eltelt idő

```
biszterszky@jerry:~$ vmstat
procs -----memory----- --swap-- -----io----- -system-- -----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 4941164 2152 1986248 0 0 0 0 0 0 0 0 0 100 0 0
biszterszky@jerry:~$ w
19:50:44 up 82 days, 20:45, 1 user, load average: 0.05, 0.03, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
biszterszky@jerry:~$
biszterszky@jerry:~$ who -b
system boot 2021-12-10 23:05
biszterszky@jerry:~$
```

- e. Aktuálisan futó processzek listája

```
system boot 2021-12-10 23:05
biszterszky@jerry:~$ ps
PID TTY TIME CMD
19773 pts/0 00:00:00 bash
19854 pts/0 00:00:00 ps
biszterszky@jerry:~$
```

```
biszterszky@jerry:~$ ps -Alf
  S UID          PID  PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
  S biszter+ 19772 19762   0  80   0 - 21759 -      19:48 ?          00:00:00 sshd: biszterszky@pts/0
  S biszter+ 19773 19772   0  80   0 - 4108 -      19:48 pts/0    00:00:00 -bash
  R biszter+ 19900 19773   0  80   0 - 8327 -      19:53 pts/0    00:00:00 ps -Alf
biszterszky@jerry:~$
```

Az összes process listája

```
biszterszky@jerry:~$ ps ax
  PID TTY          STAT TIME COMMAND
 19772 ?            S      0:00 sshd: biszterszky@pts/0
 19773 pts/0        Ss      0:00 -bash
 19907 pts/0        R+      0:00 ps ax
biszterszky@jerry:~$
```

- f. Memóriák méretét kihasználtságát és a még szabad memóriát mutatja

```
biszterszky@jerry:~$ free
              total        used         free       shared    buff/cache   available
Mem:           8025292       1103040       4933832        172864        1988420        6706956
Swap:          2097148           0         2097148
biszterszky@jerry:~$
```

- g. A CPU aktivitása valamint írási olvasási sebességének adatai láthatók

```
Swap:          2097148           0         2097148
biszterszky@jerry:~$ iostat
Linux 4.1.6-grsec (jerry)          03/03/2022      _x86_64_      (6 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
            0.03    0.00    0.03    0.00    0.00   99.94

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
biszterszky@jerry:~$
```

- h. A cpu teljesítményét figyeli és erről készít átlagot statisztikát

```
biszterszky@jerry:~$ sar 4 5
sensors_init: Kernel interface error
Linux 4.1.6-grsec (jerry)          03/03/2022      _x86_64_      (6 CPU)

```

- i. Elérhető processz aktivitása

```
Average:      all       0.04       0.00       0.05       0.00       0.00       99.91
biszterszky@jerry:~$ mpstat
Linux 4.1.6-grsec (jerry)          03/03/2022      _x86_64_      (6 CPU)

07:55:55 PM CPU    %usr   %nice    %sys %iowait  %irq   %soft  %steal  %guest  %gnice   %idle
07:55:55 PM all     0.03    0.00    0.03    0.00    0.00    0.00    0.00    0.00    0.00   99.94
biszterszky@jerry:~$
```

- j. Processzek memória használata

```
biszterszky@jerry:~$ vmstat
procs -----memory----- --swap--  -----io----- -system--  -----cpu-----
 r  b   swpd   free   buff  cache   si   so    bi   bo    in   cs us sy id wa st
  0   0       0 4931464   2152 1986272    0    0     0    0    0    0  0  0 100  0  0
biszterszky@jerry:~$
```