

Gestión de Procesos

1. Mostrar información sobre los procesos.

- Mostrar los procesos activos.

```
PS C:\Windows\system32> get-process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
558	31	18392	36888	0,66	3840	6	ApplicationFrameHost
323	20	7180	25796	0,11	11020	5	ApplicationFrameHost
158	11	7308	7160	0,34	1956	0	atxComSvc
205	12	9368	14792	0,05	10572	0	audiodg
135	9	1584	8244	0,03	5180	6	browser_broker
331	15	2892	15040	0,09	5228	5	browser_broker
517	26	23908	488	0,59	11196	6	Calculator
175	9	1592	6424	0,03	1432	6	chrome
329	30	61128	90044	36,69	1588	6	chrome
237	19	18524	33100	0,25	1868	6	chrome
211	16	12844	20452	0,08	1872	6	chrome
1462	64	55228	121236	56,77	4052	6	chrome
142	11	1916	8640	0,05	5940	6	chrome
515	30	129684	143580	39,42	7112	6	chrome
405	19	13868	29056	7,14	8700	6	chrome
280	27	40024	70720	6,17	9716	6	chrome
180	16	28700	35276	1,11	9960	6	chrome
294	27	43012	68716	2,70	10024	6	chrome
257	13	5428	15708	0,27	8556	6	conhost

- Mostrar los 10 procesos que consumen más CPU.

```
PS C:\Windows\system32> get-process | sort cpu -Descending | Select-object -First 10
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
785	70	198464	153024	1.141,42	3304	0	MsMpEng
5098	0	228	13568	359,30	4	0	System
241	15	87708	88508	328,55	1768	0	svchost
1039	47	56700	84544	211,38	10880	6	dwm
302	16	6544	10372	96,33	3232	0	vmware-authd
1464	64	55264	121260	58,41	4052	6	chrome
267	13	3380	8444	52,83	1568	0	svchost
2390	90	67160	148240	50,41	10196	6	explorer
1034	73	36136	45928	50,25	5776	0	SearchIndexer
1575	21	10760	18652	44,89	904	0	svchost

- Información sobre un proceso.

```
PS C:\Windows\system32> get-process -Name notepad | fl *
```

Name	: notepad
Id	: 5960
PriorityClass	: Normal
FileVersion	: 10.0.18362.530 (WinBuild.160101.0800)
HandleCount	: 238
WorkingSet	: 13381632
PagedMemorySize	: 3084288
PrivateMemorySize	: 3084288
VirtualMemorySize	: 157417472
TotalProcessorTime	: 00:00:00.0781250
SI	: 6
Handles	: 238
VM	: 2203475640320
WS	: 13381632
PM	: 3084288
NPM	: 13304
Path	: C:\Windows\system32\notepad.exe
Company	: Microsoft Corporation
CPU	: 0,078125
ProductVersion	: 10.0.18362.530
Description	: Bloc de notas
Product	: Sistema operativo Microsoft® Windows®
__NounName	: Process
BasePriority	: 8
ExitCode	:
HasExited	: False
ExitTime	:

- Extraer propiedad de un proceso (Ubicación del archivo)

```
PS C:\Windows\system32> (get-process notepad).path  
C:\Windows\system32\notepad.exe
```

- Extraer una propiedad de un proceso (Tamaño del proceso)

```
PS C:\Windows\system32> (Get-Process notepad).ws  
13303808  
PS C:\Windows\system32> (get-Process notepad).ws/1mb  
12,6875
```

2. Detener un proceso.

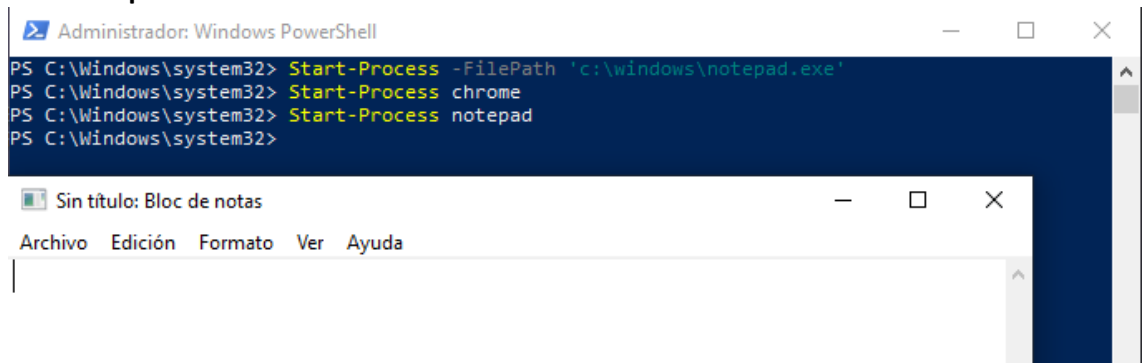
```
PS C:\Windows\system32> Get-Process -name notepad
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
231	13	2744	13060	0,08	5960	6	notepad

```
PS C:\Windows\system32> stop-process -id 5960
```

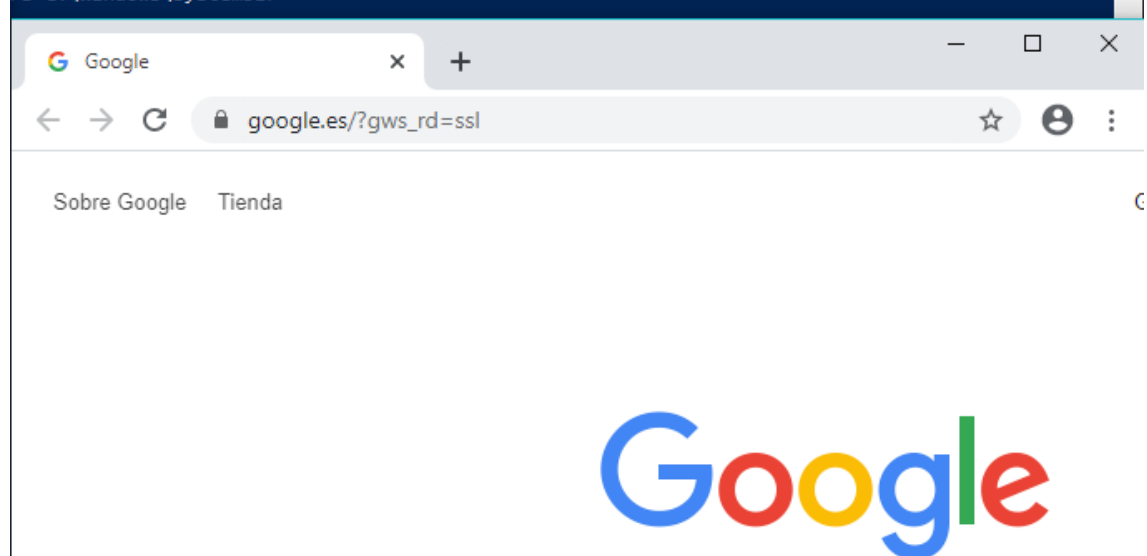
Se puede parar con Id o con el nombre (Get-Process -Name notepad)

3. Iniciar un proceso.



- Iniciar un proceso pasándole un argumento.

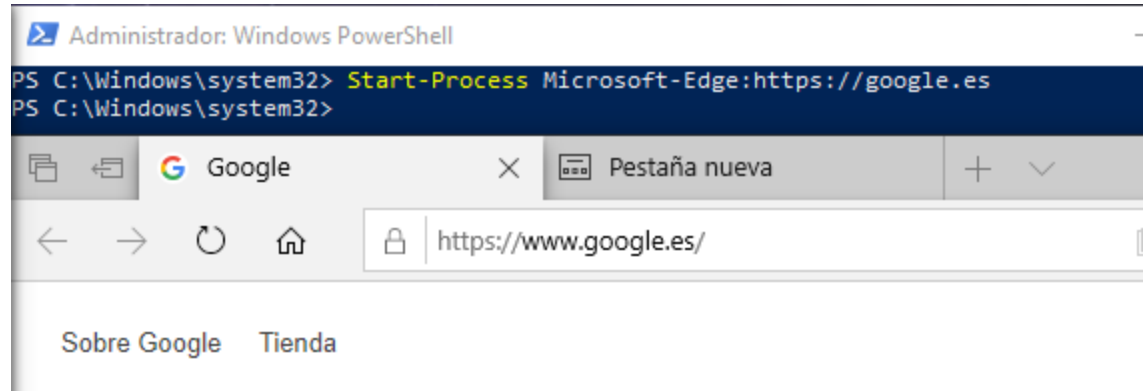
```
PS C:\Windows\system32> Start-Process chrome -ArgumentList google.es  
PS C:\Windows\system32>
```



4. Iniciar una App de Windows.

- Averiguar el protocolo asociado (no se puede mediante exe).

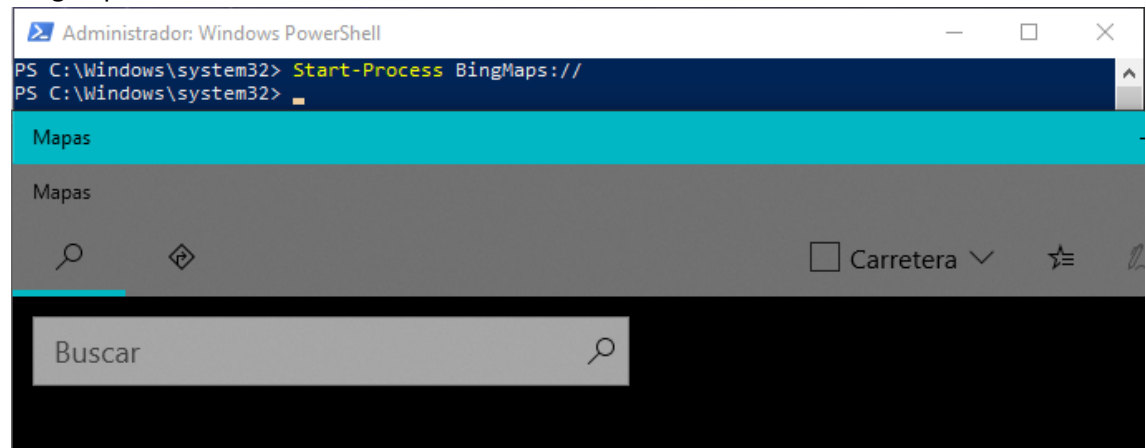
Microsoft Edge



Windows Store



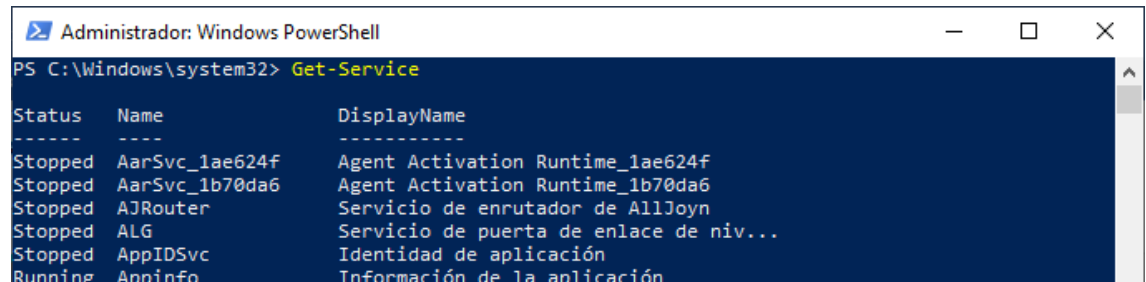
BingMaps



Gestión de Servicios

1. Información sobre los servicios

- Muestra información sobre los servicios.



- Muestra los servicios que están arrancados.

```
PS C:\Windows\system32> Get-Service |? {$_.Status -eq "Running"}

Status      Name                DisplayName
-----
Running     Appinfo             Información de la aplicación
Running     asComSvc            ASUS Com Service
Running     AudioEndpointBu...  Compilador de extremo de audio de W...
Running     Audiosrv            Audio de Windows
Running     BFE                 Motor de filtrado de base
Running     BrokerInfrastru...  Servicio de infraestructura de tare...
Running     BthAvctpSvc         Servicio AVCTP
Running     cbdhsvc_1ae624f     Servicio de usuario del portapapele...
Running     cbdhsvc_1b70da6     Servicio de usuario del portapapele...
Running     CDPSvc              Servicio de plataforma de dispositi...
Running     CDPUserSvc_1ae624f  Servicio de usuario de plataforma d...
Running     CDPUserSvc_1b70da6  Servicio de usuario de plataforma d...
Running     CoreMessagingRe...  CoreMessaging
Running     CryptSvc            Servicios de cifrado
Running     DcomLaunch          Iniciador de procesos de servidor DCOM
Running     DeviceAssociati...  Servicio de asociación de dispositivos
Running     Dhcp                Cliente DHCP
```

- Muestra información detallada de un servicio.

```
PS C:\Windows\system32> Get-Service -Name "Spoo*"

Status      Name                DisplayName
-----
Running     Spooler             Cola de impresión

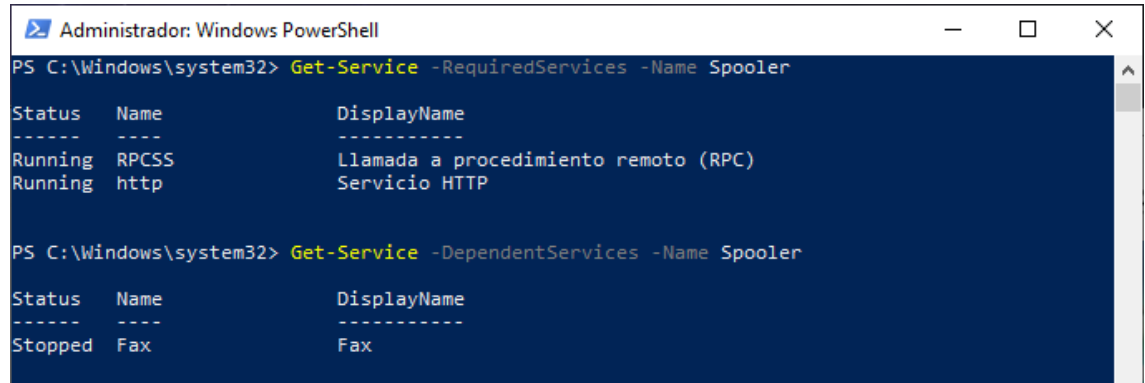
PS C:\Windows\system32> Get-Service -DisplayName "cola*"

Status      Name                DisplayName
-----
Running     Spooler             Cola de impresión

PS C:\Windows\system32> Get-Service -Name spooler |fl *

Name                : spooler
RequiredServices    : {RPCSS, http}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : True
DisplayName          : Cola de impresión
DependentServices   : {Fax}
MachineName         : .
ServiceName         : spooler
ServicesDependedOn  : {RPCSS, http}
ServiceHandle       : SafeServiceHandle
Status              : Running
ServiceType         : Win32OwnProcess, InteractiveProcess
StartType           : Automatic
Site                :
Container           :
```

- Dependencia de los servicios.



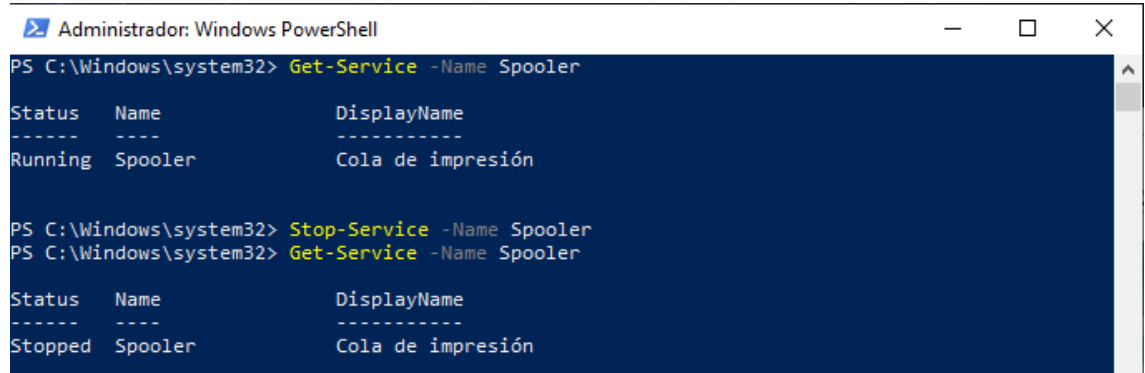
```
Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Service -RequiredServices -Name Spooler

Status  Name          DisplayName
-----
Running RPCSS      Llamada a procedimiento remoto (RPC)
Running http     Servicio HTTP

PS C:\Windows\system32> Get-Service -DependentServices -Name Spooler

Status  Name          DisplayName
-----
Stopped Fax         Fax
```

- Detener el servicio de cola de impresión.



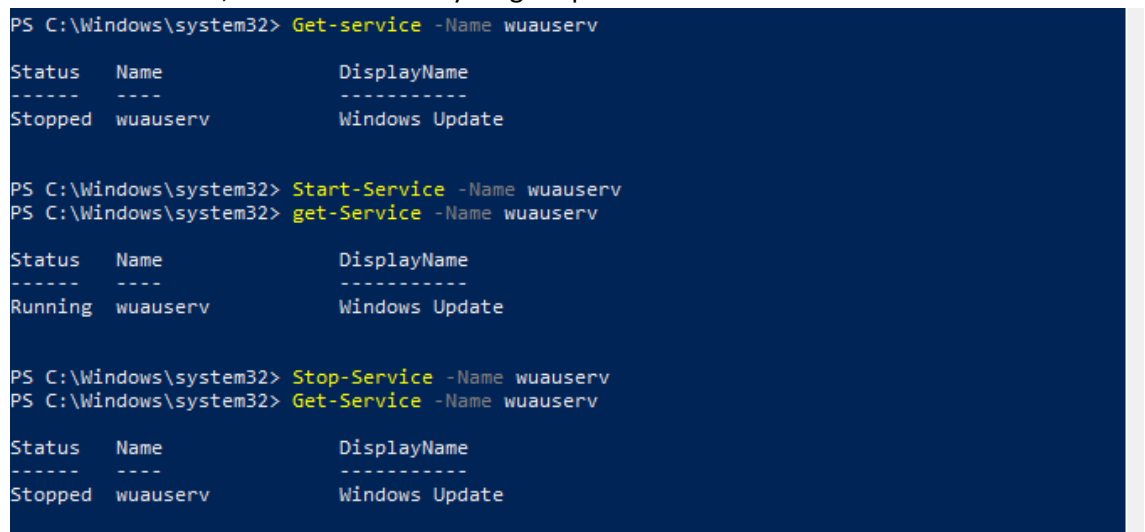
```
Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----
Running Spooler     Cola de impresión

PS C:\Windows\system32> Stop-Service -Name Spooler
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----
Stopped Spooler     Cola de impresión
```

- Detener el servicio de Windows Update.
Estaba Arrancado, entonces lo inicié y luego lo paré de nuevo.



```
PS C:\Windows\system32> Get-service -Name wuauerv

Status  Name          DisplayName
-----
Stopped wuauerv       Windows Update

PS C:\Windows\system32> Start-Service -Name wuauerv
PS C:\Windows\system32> get-Service -Name wuauerv

Status  Name          DisplayName
-----
Running wuauerv       Windows Update

PS C:\Windows\system32> Stop-Service -Name wuauerv
PS C:\Windows\system32> Get-Service -Name wuauerv

Status  Name          DisplayName
-----
Stopped wuauerv       Windows Update
```

2. Modificar un servicio.

- Modificar una propiedad: Tipo de inicio de Spooler.

```
PS C:\Windows\system32> Get-Service -name Spooler | fl *
```

Name	: Spooler
RequiredServices	: {RPCSS, http}
CanPauseAndContinue	: False
CanShutdown	: False
CanStop	: False
DisplayName	: Cola de impresión
DependentServices	: {Fax}
MachineName	: .
ServiceName	: Spooler
ServicesDependedOn	: {RPCSS, http}
ServiceHandle	: SafeServiceHandle
Status	: Stopped
ServiceType	: Win32OwnProcess, InteractiveProcess
StartType	: Automatic
Site	:
Container	:

```
PS C:\Windows\system32> Set-Service -Name Spooler -StartupType Disabled
PS C:\Windows\system32> Get-Service -name Spooler | fl *
```

Name	: Spooler
RequiredServices	: {RPCSS, http}
CanPauseAndContinue	: False
CanShutdown	: False
CanStop	: False
DisplayName	: Cola de impresión
DependentServices	: {Fax}
MachineName	: .
ServiceName	: Spooler
ServicesDependedOn	: {RPCSS, http}
ServiceHandle	: SafeServiceHandle
Status	: Stopped
ServiceType	: Win32OwnProcess, InteractiveProcess
StartType	: Disabled
Site	:
Container	: