PowerShell para administradores (intermedio)

Manuel Domínguez

@mafradoti

https://github.com/mftienda

ÍNDICE

1.- Introducción.

Podemos definir el **proceso** como la unidad más pequeña de ejecución.

Como administradores nos interesa conocer en todo momento los procesos que se están ejecutando y los recursos que están consumiendo.

1.- Introducción.

Mostrar información sobre los procesos.
Detener e iniciar un proceso.
Iniciar una aplicación de Windows.

2.-Cmdlets

Conocer los cmdlets para trabajar con procesos:
Get-Command *process*

Get-Command -Module Microsoft.PowerShell.Management

Obtener ayuda de un comando:
Get-Help Get-Process -Examples

3.- Mostrar información sobre los procesos.

Mostrar los procesos activos.

Get-Process Alias → ps

Get-Process |Out-GridView

Columnas:

Handles: nº de referencias abiertas por el proceso.
NPM y PM (KB): memoria utilizada (no paginada y paginada) por el proceso.
WS(KB): Tamaño del proceso.
CPU(s): Tiempo de procesador utilizado por el proceso.
Id: Número que identifica al proceso.
SI: Es un número que identifica al dueño del proceso.
ProcessName: Nombre del proceso.

3.- Mostrar información sobre los procesos.

Mostrar los 10 procesos que consumen más CPU.

1.- Ordenamos los procesos por consumo de CPU descendientemente.
2.- Seleccionamos los 10 primeros.

```
Get-Process|sort cpu -Descending |Select-Object -First 10
```

3.- Mostrar información sobre los procesos.

Información sobre un proceso: notepad.
Abrimos el bloc de notas → Escribimos Notepad
Get-Process -Name notepad
Get-Process -Name Notepad|fl *

Extraemos una propiedad de un proceso: Ubicación del archivo.
(Get-Process notepad).path
Extraemos una propiedad de un proceso: Tamaño del proceso.
(Get-Process notepad).ws →Nos quedamos con la propiedad ws
(Get-Process notepad).ws/1mb → expresado en MB

4.- Detener un proceso.

Detener un proceso.
1.- Localizamos el proceso → notepad
Get-Process –Name notepad

2.- Lo paramos.
Stop-Process -Name Notepad

Stop-Process -Id 4388

5.- Iniciar un proceso.

Iniciar un proceso.
1.- Localizamos el proceso → 'c:\windows\notepad.exe'
2.- Start-Process **-FilePath** 'c:\windows\notepad.exe'
3.- Start-Process -FilePath 'C:\Program Files(x86)\Google\Chrome\Application\chrome.exe'

Start-Process notepad Start-Process chrome
También funcionará porque está en el PATH.
echo $env:path → Ver las variables de entorno PATH

5.- Iniciar un proceso.

Iniciar un proceso pasándole un argumento.
Abrimos Chrome pasándole una página web.

Start-Process chrome -ArgumentList google.es

6.- Iniciar una app de Windows.

Aunque las apps de Windows tienen un archivo exe asociado que se encuentran en c:\Windows\SystemApps, no se pueden ejecutar desde el archivo .exe. Hay que utilizar el **protocolo asociado**.
ls C:\Windows\SystemApps\ |flclear
ls C:\windows\SystemApps\|fl name

Edge: Start-Process Microsoft-Edge://
Edge: Start-Process Microsoft-Edge:https://google.es
Windows Store: Start-Process Ms-Windows-Store:// → WinStore.App
Alarmas y reloj: Start-Process Ms-clock://
Mapas: Start-Process BingMaps://

7.-Resumen de comandos.

Gestión de procesos:

Get-Process: muestra información de los procesos.
Stop-Process: detiene un proceso.
Start-Process: Inicia un proceso.

PowerShell para administradores (intermedio)

Manuel Domínguez

@mafradoti

https://github.com/mftienda