**TALLER POWERSHELL N° 4**

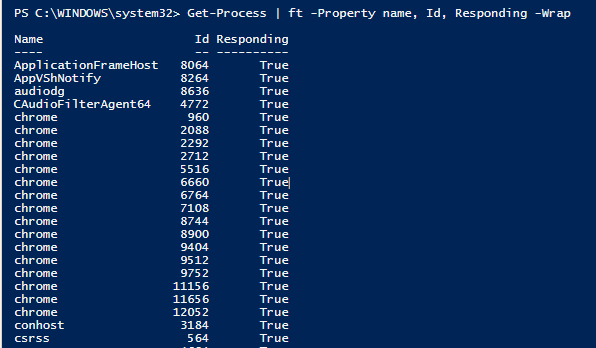
**HECHO POR:**

**Jeferson Lerma Giron - A00301456**

1. Mostrar una tabla de procesos que incluya únicamente los nombres de los procesos, sus IDs, y si están respondiendo a Windows (la propiedad Responding muestra eso). Haga que la tabla tome el mínimo de espacio horizontal, pero no permita que la información se trunque.

R// Se utiliza el comando:

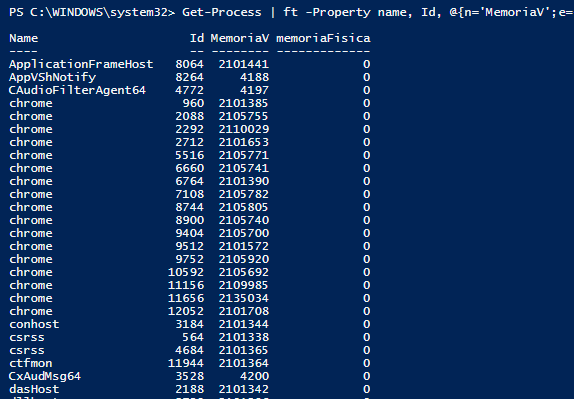
Get-Process | ft -Property name, Id, Responding -Wrap



2. Muestre una tabla de procesos que incluya los nombres de los procesos y sus IDs. También incluya columnas para uso de memoria virtual y física; exprese dichos valores en megabytes (MB).

R// Se puede usar el comando:

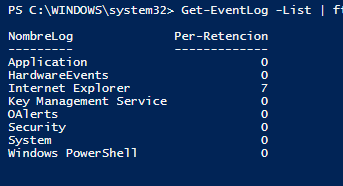
Get-Process | ft -Property name, Id, @{n='MemoriaV';e={$\_.VM / 1MB -as [int]}}, @{n='memoriaFisica';e={$\_.MP / 1MB -as [int]}} -Wrap



3. Emplee Get-EventLog para mostrar una lista de los logs de eventos disponibles (revise la ayuda para encontrar el parámetro que le permitirá obtener dicha información). Formatee la salida como una tabla que incluya el nombre de despliegue del log y el período de retención. Los encabezados de columna deben ser NombreLog y Per-Retención.

R// Se puede usar el comando:

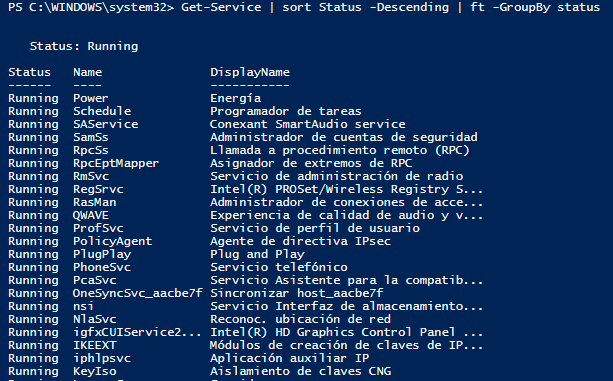
Get-EventLog -List | ft -Property @{n='NombreLog';e={$\_.Log}},@{n='Per-Retencion';e={$\_.MinimumRetentionDays}}



4. Muestre una lista de servicios, de tal manera que aparezcan agrupados los servicios que están iniciados y los que están detenidos. Los que están iniciados deben aparecer primero.

R// Se puede usar el comando:

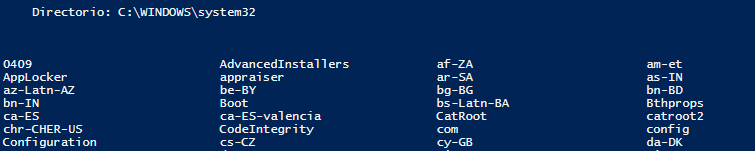
Get-Service | sort Status -Descending | ft -GroupBy status



5.Mostrar una lista a cuatro columnas de todos los directorios que están en el raíz de la unidad C:

R// Se puede utilizar el comando:

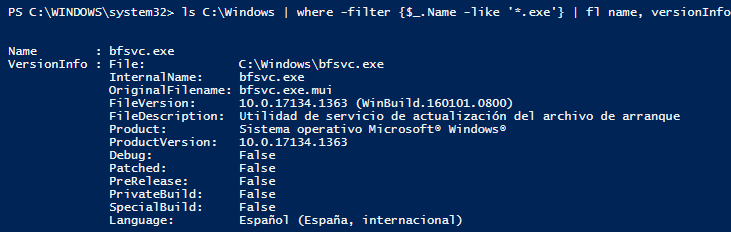
dir C: | fw -Column 4



6. Cree una lista formateada de todos los archivos .exe del directorio C:\Windows. Debe mostrarse el nombre, la información de versión, y el tamaño del archivo. La propiedad de tamaño se llama length en Powershell, pero para mayor claridad, la columna se debe llamar Tamaño en su listado.

R// Se puede usar el comando:

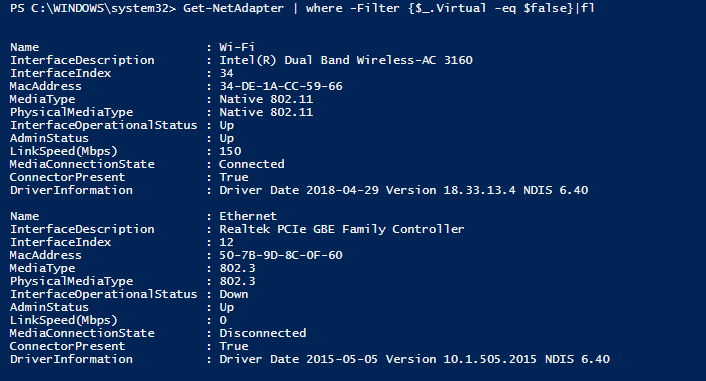
ls C:\Windows | where -filter {$\_.Name -like '\*.exe'} | fl name, versionInfo,@{n='Tamaño';e={$\_.Length}}



7.Importe el módulo NetAdapter (empleando el comando Import-Module NetAdapter). Empleando el cmdlet Get-NetAdapter, muestre una lista de adaptadores no virtuales (adaptadores cuya propiedad Virtual sea falsa. El valor lógico falso es representado por Powershell como $False).

R//Se puede usar el comando:

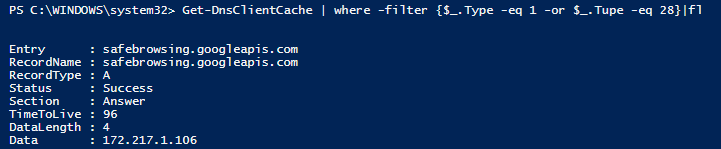
Get-NetAdapter | where -Filter {$\_.Virtual -eq $false}|fl



8.Importe el módulo DnsClient. Empleando el cmdlet Get-DnsClientCache, muestre una lista de los registros A y AAAA que estén en el caché. Sugerencia: Si el caché está vacío, visite algunos sitios web para poblarlo.

R// Se puede usar el comando:

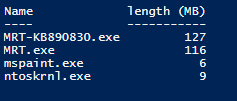
Get-DnsClientCache | where -filter {$\_.Type -eq 1 -or $\_.Tupe -eq 28}|fl



9. Genere una lista de todos los archivos .exe del directorio C:\Windows\System32 que tengan más de 5 MB.

R// Se puede usar el comando:

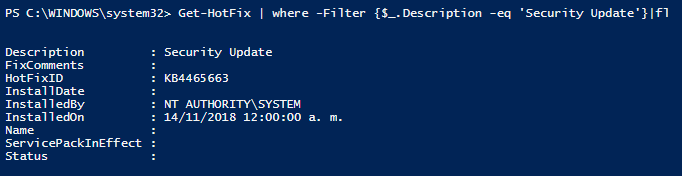
ls C:\Windows\System32 | where -filter {$\_.Name -like '\*.exe' -and $\_.Length -gt 5\*1MB} | ft Name,@{n='length (MB)';e={$\_.length / 1MB -as [int]}}



10. Muestre una lista de parches que sean actualizaciones de seguridad.

R// Se puede usar el comando:

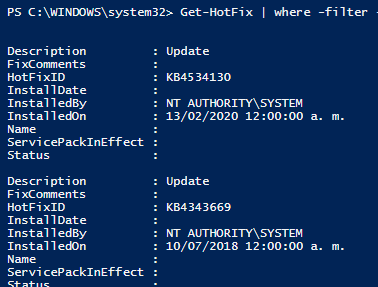
Get-HotFix | where -Filter {$\_.Description -eq 'Security Update'}|fl



11. Muestre una lista de parches que hayan sido instalados por el usuario Administrador, que sean actualizaciones. Si no tiene ninguno, busque parches instalados por el usuario System. Note que algunos parches no tienen valor en el campo Installed By.

R// Se puede usar el comando:

Get-HotFix | where -filter {$\_.Description -eq 'Update' -and $\_.InstalledBy -eq 'NT AUTHORITY\SYSTEM'}|FL



12. Genere una lista de todos los procesos que estén corriendo con el nombre Conhost o Svchost.

R// Se puede usar el comando:

Get-Process | where -filter {$\_.Name -eq 'Conhost' -or $\_.Name -eq 'Svchost'}|fl

