

Práctica 5

Iniciar el snapshot o punto de salvado llamado “Práctica4v21_SOM” en la máquina virtual de Windows server 2016.

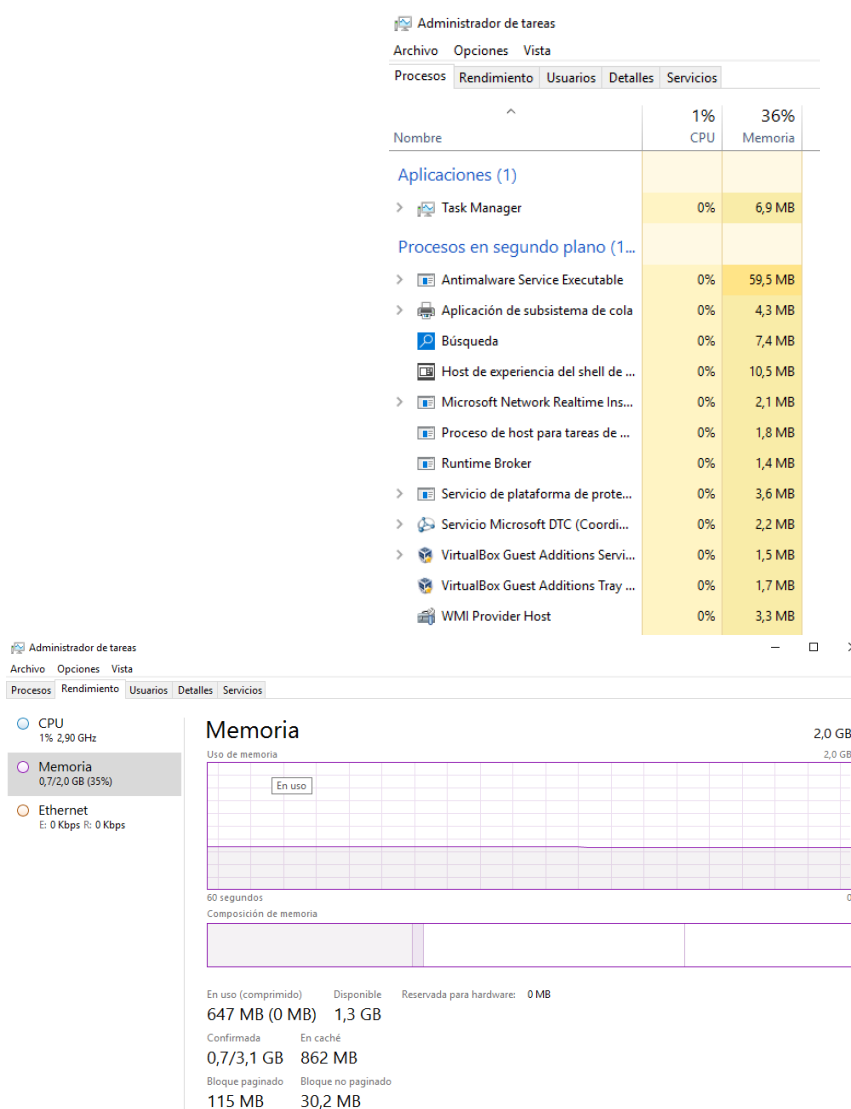
Buscar información de procesos y servicios en la máquina virtual Windows Server 2016.

1. Interfaz gráfica de Windows server 2016. Realizar una breve descripción de los dispositivos de la máquina.

La pestaña de procesos muestra los programas se están ejecutando actualmente en el equipo

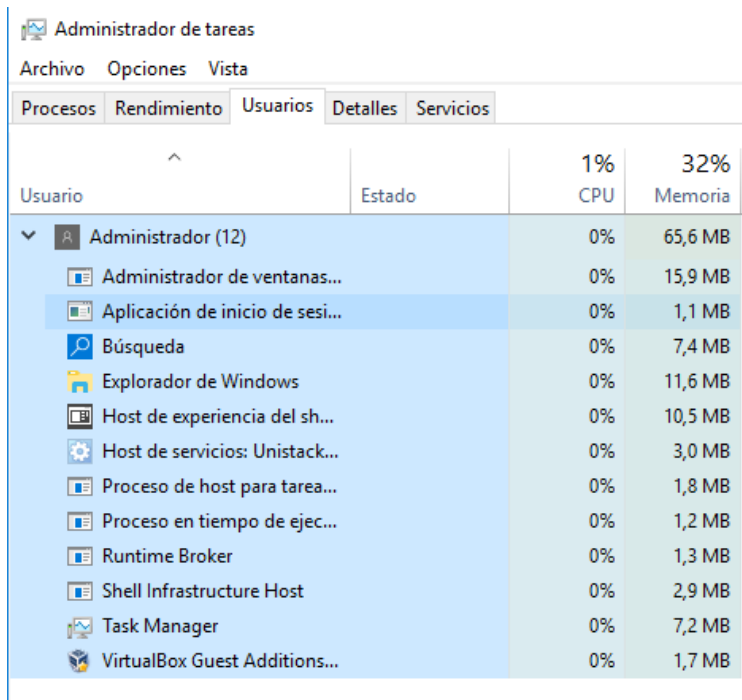
- Abrir el administrador de tareas y describir cada una de las pestañas que aparecen.

<https://www.downloadsource.es/5-maneras-de-iniciar-el-administrador-de-tareas-de-windows-10-8-y-7/n/8618/>



Carla García Parra 2ºASIR

En la pestaña de rendimiento ofrece una visión técnica del proceso en su equipo. Nos muestra los gráficos con el uso de CPU y su historial



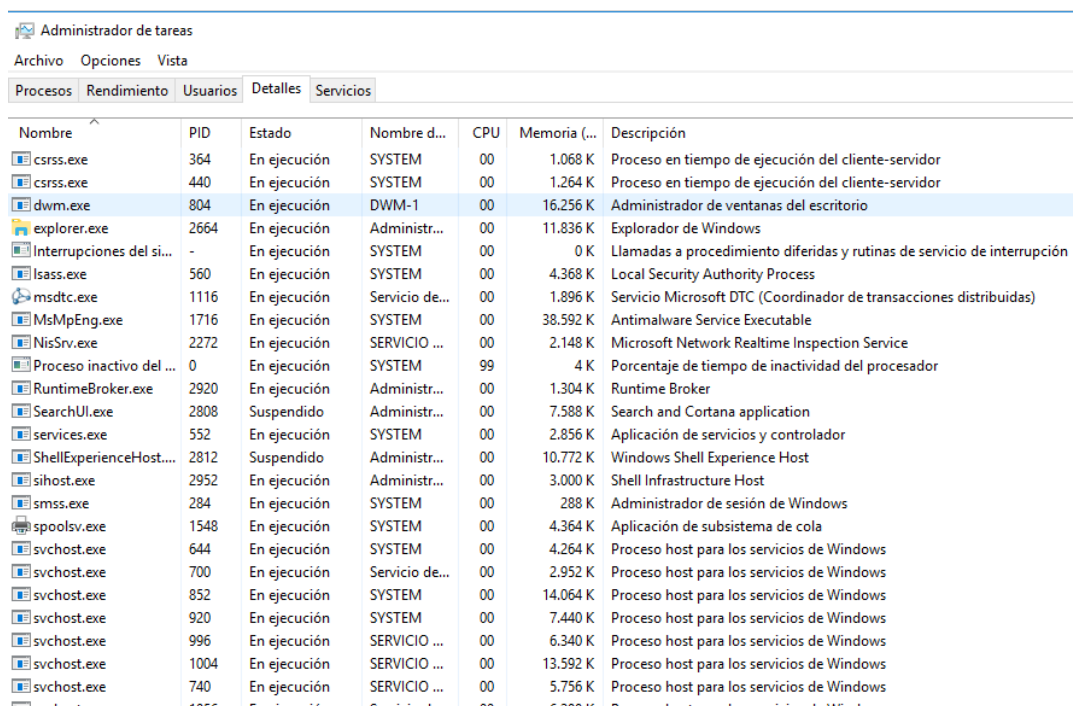
Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Usuarios Detalles Servicios

Usuario	Estado	1% CPU	32% Memoria
Administrador (12)		0%	65,6 MB
Administrador de ventanas...		0%	15,9 MB
Aplicación de inicio de sesi...		0%	1,1 MB
Búsqueda		0%	7,4 MB
Explorador de Windows		0%	11,6 MB
Host de experiencia del sh...		0%	10,5 MB
Host de servicios: Unistack...		0%	3,0 MB
Proceso de host para tarea...		0%	1,8 MB
Proceso en tiempo de ejec...		0%	1,2 MB
Runtime Broker		0%	1,3 MB
Shell Infrastructure Host		0%	2,9 MB
Task Manager		0%	7,2 MB
VirtualBox Guest Additions...		0%	1,7 MB

La pestaña de usuarios nos da informacion general del usuario activo y los procesos y servicios que está ejecutandose



Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Usuarios Detalles Servicios

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Descripción
csrss.exe	364	En ejecución	SYSTEM	00	1.068 K	Proceso en tiempo de ejecución del cliente-servidor
csrss.exe	440	En ejecución	SYSTEM	00	1.264 K	Proceso en tiempo de ejecución del cliente-servidor
dwm.exe	804	En ejecución	DWM-1	00	16.256 K	Administrador de ventanas del escritorio
explorer.exe	2664	En ejecución	Administ...	00	11.836 K	Explorador de Windows
Interrupciones del si...	-	En ejecución	SYSTEM	00	0 K	Llamadas a procedimiento diferidas y rutinas de servicio de interrupción
lsass.exe	560	En ejecución	SYSTEM	00	4.368 K	Local Security Authority Process
msdtc.exe	1116	En ejecución	Servicio de...	00	1.896 K	Servicio Microsoft DTC (Coordinador de transacciones distribuidas)
MsMpEng.exe	1716	En ejecución	SYSTEM	00	38.592 K	Antimalware Service Executable
NisSrv.exe	2272	En ejecución	SERVICIO ...	00	2.148 K	Microsoft Network Realtime Inspection Service
Proceso inactivo del ...	0	En ejecución	SYSTEM	99	4 K	Porcentaje de tiempo de inactividad del procesador
RuntimeBroker.exe	2920	En ejecución	Administ...	00	1.304 K	Runtime Broker
SearchUI.exe	2808	Suspendido	Administ...	00	7.588 K	Search and Cortana application
services.exe	552	En ejecución	SYSTEM	00	2.856 K	Aplicación de servicios y controlador
ShellExperienceHost...	2812	Suspendido	Administ...	00	10.772 K	Windows Shell Experience Host
sihost.exe	2952	En ejecución	Administ...	00	3.000 K	Shell Infrastructure Host
smss.exe	284	En ejecución	SYSTEM	00	288 K	Administrador de sesión de Windows
spoolsv.exe	1548	En ejecución	SYSTEM	00	4.364 K	Aplicación de subsistema de cola
svchost.exe	644	En ejecución	SYSTEM	00	4.264 K	Proceso host para los servicios de Windows
svchost.exe	700	En ejecución	Servicio de...	00	2.952 K	Proceso host para los servicios de Windows
svchost.exe	852	En ejecución	SYSTEM	00	14.064 K	Proceso host para los servicios de Windows
svchost.exe	920	En ejecución	SYSTEM	00	7.440 K	Proceso host para los servicios de Windows
svchost.exe	996	En ejecución	SERVICIO ...	00	6.340 K	Proceso host para los servicios de Windows
svchost.exe	1004	En ejecución	SERVICIO ...	00	13.592 K	Proceso host para los servicios de Windows
svchost.exe	740	En ejecución	SERVICIO ...	00	5.756 K	Proceso host para los servicios de Windows
svchost.exe	1056	En ejecución	Servicio de...	00	6.380 K	Proceso host para los servicios de Windows

Esta pestaña de detalles tiene un carácter más técnico. Se puede ver la lista de muchas aplicaciones que se están ejecutando actualmente en el equipo. Se puede ver el uso de la CPU y de la memoria

Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Usuarios Detalles Servicios

Nombre	PID	Descripción	Estado	Grupo
WSearch		Windows Search	Detenido	
wmiApSrv		Adaptador de rendimiento de WMI	Detenido	
WinDefend	1716	Servicio de Windows Defender	En ejecución	
WdNisSvc	2272	Servicio de inspección de red de Windows Defender	En ejecución	
VSS		Instantáneas de volumen	Detenido	
vds		Disco virtual	Detenido	
VBoxService	356	VirtualBox Guest Additions Service	En ejecución	
VaultSvc	560	Administrador de credenciales	En ejecución	
UI0Detect		Detección de servicios interactivos	Detenido	
UevAgentService		Servicio de virtualización de la experiencia de usuario	Detenido	
TrustedInstaller	612	Instalador de módulos de Windows	En ejecución	
TieringEngineService		Administración de capas de almacenamiento	Detenido	
sppsvc		Protección de software	Detenido	
Spooler	1548	Cola de impresión	En ejecución	
SNMPTRAP		Captura SNMP	Detenido	
SensorDataService		Servicio de datos del sensor	Detenido	
SamSs	560	Administrador de cuentas de seguridad	En ejecución	
RSoPProv		Conjunto resultante de proveedor de directivas	Detenido	
RpcLocator		Ubicador de llamada a procedimiento remoto (RPC)	Detenido	
PerfHost		DLL de host del Contador de rendimiento	Detenido	
NetTcpPortSharing		Servicio de uso compartido de puertos Net.Tcp	Detenido	
Netlogon		Net Logon	Detenido	
msiserver		Windows Installer	Detenido	
MSDTC	1116	Coordinador de transacciones distribuidas	En ejecución	
MexillaMaintenance		Mexilla Maintenance Service	Detenido	

En esta pestaña de Servicios lo que podemos ver son los servicios que se están ejecutando actualmente en el ordenador, podemos ver el estado del servicio

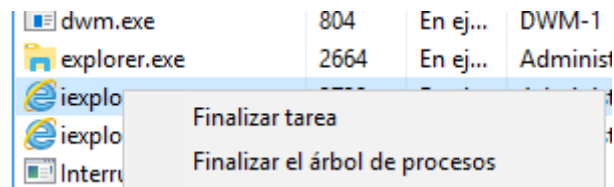
- Detener un proceso

Procesos en segundo plano (1...

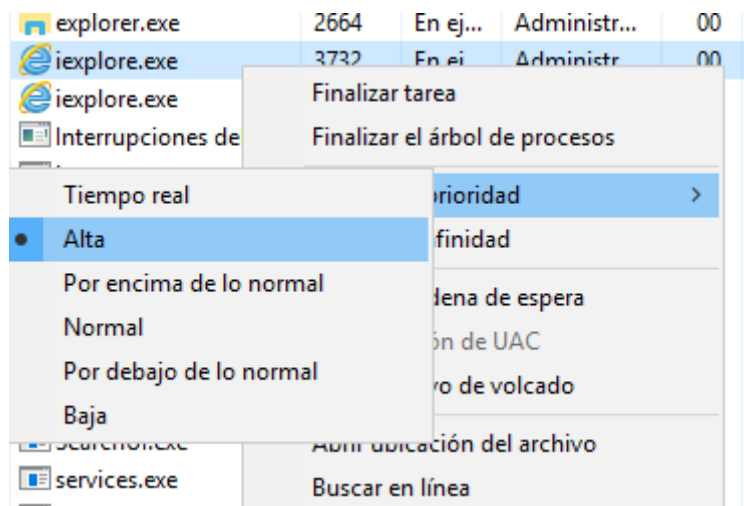
Antimalware Service Executable	0%	79,6 MB
Servicio de Windows Defender		
Búsqueda	0%	7,4 MB
Host	0%	10,4 MB
Microsoft Malware Protection C...	0%	2,0 MB

Detener
Abrir servicios
Buscar en línea

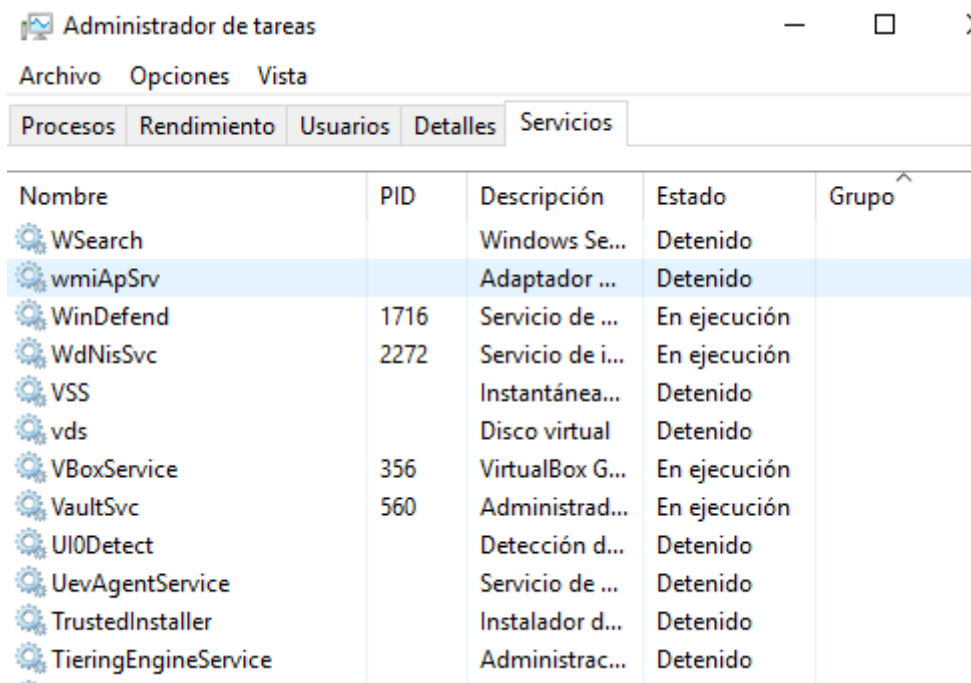
- Borrar un proceso



- Cambiar la prioridad de un proceso.



- Abrir la pantalla de servicios



- Iniciar, detener y crear un servicio.

Nombre	PID	Descripción	Estado
WSearch		Windows Se...	Detenido
wmiApSrv		...	Detenido
WinDefend		...	En ejecución
WdNisSvc		...	En ejecución
VSS		...	Detenido
vds		...	Detenido
VBoxService		...	En ejecución

WSearch		Windows Se...	Detenido
wmiApSrv		Adaptador ...	Detenido
WinDefend	1716	Servicio de ...	En ejecución
WdNisSvc		de i...	En ejecución
VSS		nea...	Detenido
vds		tual	Detenido
VBoxService		ox G...	En ejecución
VaultSvc		trad...	En ejecución

Administrador de tareas

nivo

Opciones

Vista

cesos

Rendimiento

Usuarios

Detalle

Nombre	PID
xlInstSV	
rameServer	
ystemEventsBroker	644
ower	644
lugPlay	644
SM	644
eviceInstall	
lcomLaunch	644
rokerInfrastructure	644
lefragsvc	
micrdv	
micrheartbeat	

Menos detalles
Abrir servicios

de Internet Expl

Servicios

Archivo

Acción

Ver

Ayuda

Servicios (locales)

Servicios (locales)

Agente de detección en segundo plano de DevQuery
[Iniciar](#) el servicio
 Descripción:
 Permite a las aplicaciones detectar dispositivos con una tarea en segundo plano

Nombre	Descripción	Estado	Tipo
Administración remota de ...	El servicio A...	En ejecu...	Autc
Administrador de conexio...	Crea una co...		Man
Administrador de conexio...	Administra ...		Man
Administrador de conexio...	Toma decisi...	En ejecu...	Autc
Administrador de configura...	Habilita la d...		Man
Administrador de credencia...	Proporciona...	En ejecu...	Man
Administrador de cuentas d...	El inicio de e...	En ejecu...	Autc
Administrador de mapas de...	Servicio de ...		Autc
Administrador de sesión local	Servicio cen...	En ejecu...	Autc
Administrador de usuarios	El administr...	En ejecu...	Autc
Adquisición de imágenes d...	Proporciona...		Man
Agente de conexión de red	Conexiones ...	En ejecu...	Man
Agente de detección en seg...	Permite a la...		Man
Agente de directiva IPsec	El protocolo...		Man
Agente de eventos de tiempo	Coordina la ...	En ejecu...	Man
Agente de eventos del siste...	Coordina la ...	En ejecu...	Autc
Aislamiento de claves CNG	El servicio Ai...	En ejecu...	Man
Almacenamiento de datos ...	Controla el ...		Man
Aplicación auxiliar de NetBl...	Proporciona...	En ejecu...	Man
Aplicación auxiliar IP	Proporciona...	En ejecu...	Autc

2. Consola (CMD administrador) de Windows server 2016.

- Utilizar todos los comandos que se describen en el documento "ProcesosyserviciosEnWindows.pdf"

Comando Start → inicia una ventana aparte para ejecutar un programa o un comando especificado

```
C:\Users\Administrador.WIN-V0LV1BK80EB>start firefox
```

Comando tasklist → muestra una lista de aplicaciones y las tareas o procesos asociados que se ejecutan en un sistema local o remoto

- Listar todos los procesos

```
C:\Users\Administrador.WIN-V0LV1BK80EB>tasklist
```

Nombre de imagen	PID	Nombre de sesión	Núm. de ses	Uso de memor
System Idle Process	0	Services	0	4 KB
System	4	Services	0	132 KB
smss.exe	284	Services	0	1.196 KB
csrss.exe	364	Services	0	4.196 KB
wininit.exe	432	Services	0	5.092 KB
csrss.exe	440	Console	1	9.532 KB
winlogon.exe	484	Console	1	9.276 KB
services.exe	552	Services	0	6.840 KB
lsass.exe	560	Services	0	14.352 KB
svchost.exe	644	Services	0	18.692 KB
svchost.exe	700	Services	0	8.800 KB
dwm.exe	804	Console	1	49.028 KB
svchost.exe	852	Services	0	44.808 KB
svchost.exe	920	Services	0	21.776 KB
svchost.exe	996	Services	0	17.216 KB
svchost.exe	1004	Services	0	20.432 KB
VBoxService.exe	356	Services	0	7.616 KB
svchost.exe	740	Services	0	20.904 KB
svchost.exe	1056	Services	0	20.948 KB
svchost.exe	1192	Services	0	6.836 KB
svchost.exe	1600	Services	0	22.992 KB
svchost.exe	1620	Services	0	8.092 KB
svchost.exe	1636	Services	0	16.460 KB
MsMpEng.exe	1716	Services	0	114.684 KB

- Modificar la prioridad de un proceso.

```
C:\Users\Administrador.WIN-V0LV1BK80EB>wmic process where name="notepad.exe" call setpriority 32768
```

- Detener /Borrar procesos

```
C:\Users\Administrador.WIN-V0LV1BK80EB>taskkill /IM notepad.exe  
CORRECTO: señal de terminación enviada al proceso "notepad.exe" con PID 4052.
```

- Listar todos los servicios de la máquina.

```
C:\Users\Administrador.WIN-V0LV1BK80EB>net start  
Se han iniciado estos servicios de Windows:  
  
Administración remota de Windows (WS-Management)  
Administrador de conexiones de Windows  
Administrador de credenciales  
Administrador de cuentas de seguridad  
Administrador de sesión local  
Administrador de usuarios  
Agente de conexión de red  
Agente de eventos de tiempo  
Agente de eventos del sistema  
Aislamiento de claves CNG  
Aplicación auxiliar de NetBIOS sobre TCP/IP  
Aplicación auxiliar IP  
Asignador de extremos de RPC  
CDPUserSvc_289f4  
Cliente de directiva de grupo  
Cliente de seguimiento de vínculos distribuidos  
Cliente DHCP  
Cliente DNS  
Coordinador de transacciones distribuidas  
CoreMessaging  
Detección de hardware shell  
Energía  
Estación de trabajo  
Firewall de Windows  
Hora de Windows  
Iniciador de procesos de servidor DCOM  
Instrumental de administración de Windows  
Llamada a procedimiento remoto (RPC)
```


Carla García Parra 2ºASIR

- Iniciar, detener y crear un servicio.

```
C:\Users\Administrador.WIN-V0LV1BK80EB>net start Temas
El servicio solicitado ya ha sido iniciado.

Puede obtener más ayuda con el comando NET HELPMSG 2182.
```

```
C:\Users\Administrador.WIN-V0LV1BK80EB>net stop Temas
El servicio de Temas está deteniéndose.
El servicio de Temas se detuvo correctamente.
```

3. PowerShell Windows server 2016

- Utilizar todos los comandos que se describen en la presentación en el documento "ProcesosyserviciosEnWindows.pdf".
- Listar todos los procesos

```
PS C:\Users\Administrador.WIN-V0LV1BK80EB> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
190	11	5016	12568	0,05	3176	1	cmd
166	11	4652	14492	0,31	2152	1	conhost
162	11	3412	13164	0,17	3676	1	conhost
225	10	1804	4176	0,17	364	0	csrss
261	18	2368	9572	2,34	440	1	csrss
87	7	1344	5932	0,02	3648	1	dllhost
362	32	21560	40556	3,48	804	1	dwm
1422	61	23100	72820	5,20	2664	1	explorer
0	0	0	4		0	0	Idle
862	22	5892	14380	0,59	560	0	lsass
258	12	2892	10776	0,03	1068	0	MpCmdRun
188	12	2764	9404	0,09	1116	0	msdtc
475	81	198340	126948	12,73	1716	0	MsMpEng
161	33	4836	8672	0,03	2272	0	NisSrv
603	28	57880	65024	0,47	1364	1	powershell
325	19	5356	20672	0,11	2920	1	RuntimeBroker
998	63	65680	115184	1,45	2808	1	SearchUI
216	9	3016	6828	0,66	552	0	services
677	28	14328	44416	0,17	2812	1	ShellExperienceHost
390	15	3960	19420	0,22	2952	1	sihost
51	2	388	1196	0,19	284	0	smss
630	21	5692	18744	0,47	644	0	svchost
539	16	3464	8840	0,55	700	0	svchost
593	30	7920	20824	0,34	740	0	svchost
1406	44	18820	45536	2,64	852	0	svchost
542	28	12580	21700	0,84	920	0	svchost
446	34	11256	17212	0,31	996	0	svchost
490	19	12228	20816	1,00	1004	0	svchost
725	38	8492	20960	0,38	1056	0	svchost
158	11	1644	6796	0,00	1192	0	svchost
400	21	7168	22960	0,31	1600	0	svchost
200	12	2172	8092	0,03	1620	0	svchost
213	18	5056	16464	0,14	1636	0	svchost
284	17	4296	19544	0,13	2968	1	svchost
741	0	128	132	5,77	4	0	System
312	31	6416	18280	0,31	3880	1	taskhost

Carla García Parra 2ºASIR

- Modificar la prioridad de un proceso.

```
PS C:\Users\Administrador.WIN-VOLV1BK80EB> Get-WmiObject Win32_process -filter 'name = "notepad.exe"' | foreach-object {$_. SetPriority (32)}
$ : El término '$' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 78
+ ... 32_process -filter 'name = "notepad.exe"' | foreach-object {$_. SetP ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

- Detener /Borrar procesos

```
PS C:\Users\Administrador.WIN-VOLV1BK80EB> Stop-Process -Name "Notepad" -Force
PS C:\Users\Administrador.WIN-VOLV1BK80EB> _
```

- Listar todos los servicios de la máquina.

```
PS C:\Users\Administrador.WIN-VOLV1BK80EB> Get-Service

Status      Name                DisplayName
-----
Stopped     AJRouter            Servicio de enrutador de AllJoyn
Stopped     ALG                 Servicio de puerta de enlace de niv...
Stopped     AppIDSvc            Identidad de aplicación
Stopped     AppInfo             Información de la aplicación
Stopped     AppMgmt             Administración de aplicaciones
Stopped     AppReadiness        Preparación de aplicaciones
Stopped     AppVClient          Microsoft App-V Client
Stopped     AppXSvc             Servicio de implementación de AppX ...
Stopped     AudioEndpointBu...  Compilador de extremo de audio de W...
Stopped     Audiosrv            Audio de Windows
Stopped     AxInstSV            Instalador de ActiveX (AxInstSV)
Running     BFE                 Motor de filtrado de base
Stopped     BITS                Servicio de transferencia inteligen...
Running     BrokerInfrastru...  Servicio de infraestructura de tare...
Stopped     Browser             Examinador de equipos
Stopped     bthserv             Servicio de compatibilidad con Blue...
Running     CDPSvc              Servicio de plataforma de dispositi...
Running     CDPUserSvc_289f4    CDPUserSvc_289f4
Stopped     CertPropSvc         Propagación de certificados
Stopped     ClipSvc             Servicio de licencia de cliente (Cl...
Stopped     COMSysApp           Aplicación del sistema COM+
Running     CoreMessagingRe...  CoreMessaging
Running     CryptSvc            Servicios de cifrado
Stopped     CscService          Archivos sin conexión
Running     DcomLaunch          Iniciador de procesos de servidor DCOM
Stopped     DcpSvc              DataCollectionPublishingService
Stopped     defragsvc           Optimizar unidades
Stopped     DeviceAssociati...  Servicio de asociación de dispositivos
Stopped     DeviceInstall       Servicio de instalación de disposit...
Stopped     DevQueryBroker      Agente de detección en segundo plan...
Running     Dhcp                Cliente DHCP
Stopped     diagnosticshub....  Servicio Recopilador estándar del c...
Running     DiagTrack           Telemetría y experiencias del usar...
Stopped     DmEnrollmentSvc     Servicio de inscripción de administ...
Stopped     dmwappushservice    dmwappushsvc
Running     Dnscache            Cliente DNS
Stopped     dot3svc             Configuración automática de redes c...
Running     DPS                 Servicio de directivas de diagnóstico
Stopped     DsmSvc              Administrador de configuración de d...
Stopped     DsSvc               Servicio de uso compartido de datos
Stopped     Eaphost             Protocolo de autenticación extensible
Stopped     EFS                 Sistema de cifrado de archivos (EFS)
Stopped     embeddedmode        Modo inyectado
```

Carla García Parra 2ºASIR

- Iniciar, detener, crear un servicio.

```
PS C:\Users\Administrador.WIN-VOLV1BK80EB> Start-Service -Name "Temas"  
PS C:\Users\Administrador.WIN-VOLV1BK80EB> Stop-Service -Name "Temas"
```