

ADMINISTRACIÓN DE WINDOWS

PROCESOS, SERVICIOS Y CARACTERÍSTICAS ADICIONALES DE WINDOWS

CONTENIDOS

1. ADMINISTRACIÓN DE PROCESOS.....	1
1.1 EN MODO GRÁFICO.....	1
1.2 COMANDOS CMD.....	2
1.3 COMANDOS POWERSHELL.....	4
2. PROCESOS EN SEGUNDO PLANO: JOB.....	4
2.1 EN CMD.....	4
2.2 EN POWERSHELL.....	5
3. ADMINISTRACIÓN DE SERVICIOS.....	6
3.1 EN MODO GRÁFICO.....	6
3.3 EN POWERSHELL.....	9
4. ADMINISTRACIÓN DE CARACTERÍSTICAS ADICIONALES DE WINDOWS.....	10

LINKS DE CONSULTA

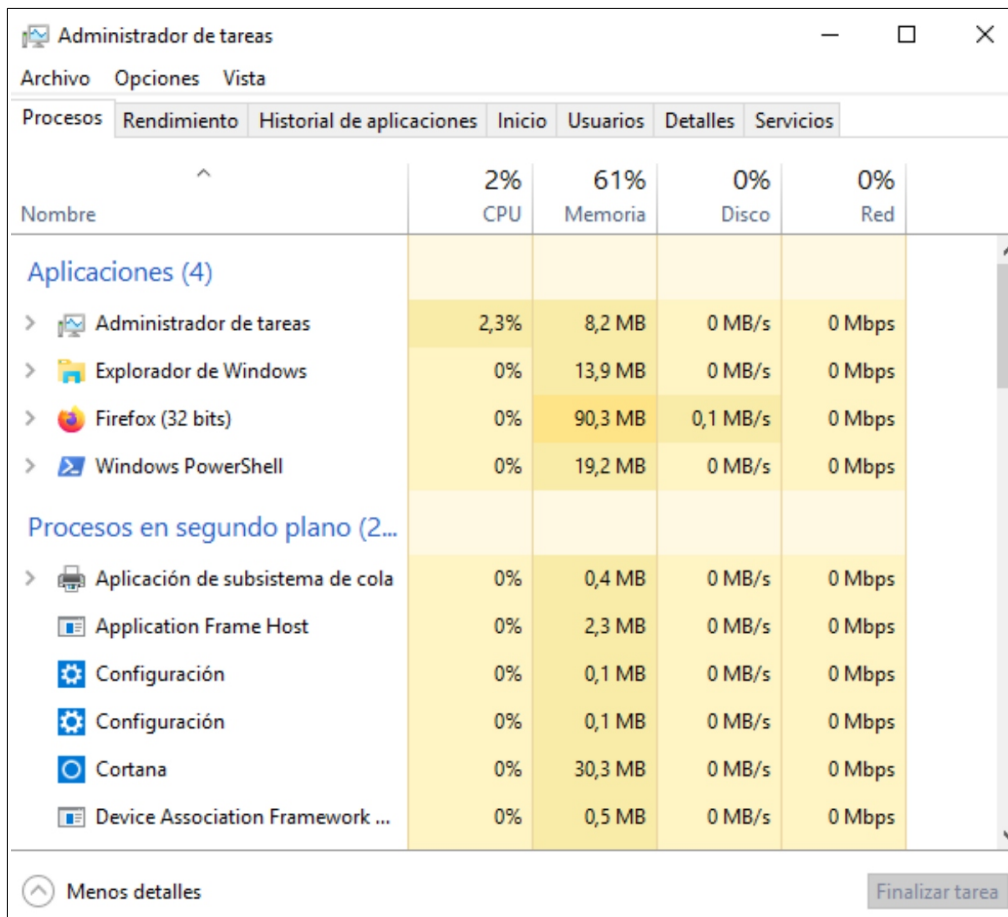
CMD: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/cmd>

POWER-SHELL: <https://learn.microsoft.com/es-es/powershell/scripting/samples/managing-processes-with-process-cmdlets?view=powershell-7.3>

1. ADMINISTRACIÓN DE PROCESOS

1.1 EN MODO GRÁFICO

- El **Administrador de tareas** es la herramienta gráfica encargada de gestionar los procesos.



- Para invocarla:
 - <Ctrl>+<Alt>+<Supr>
 - **Clic derecho** sobre la barra de tareas.
 - **Clic derecho** en botón inicio.

1.2 COMANDOS CMD

Listar procesos	tasklist
Iniciar proceso.exe	Start proceso.exe
Matar un proceso	Taskkill /pid n°

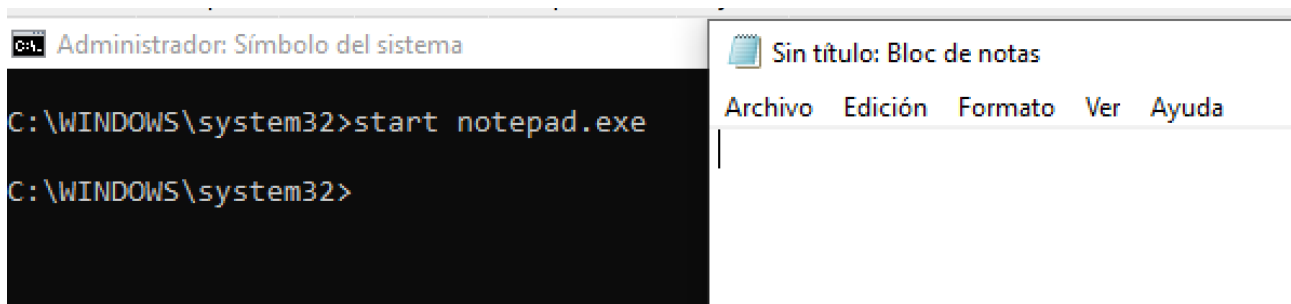
EJEMPLOS

1. Listar procesos

```
C:\WINDOWS\system32> tasklist
```

Nombre de imagen	PID	Nombre de sesión	Núm. de ses	Uso de memor
System Idle Process	0	Services	0	8 KB
System	4	Services	0	152 KB
Registry	72	Services	0	27.660 KB
smss.exe	324	Services	0	864 KB

2. Abrir proceso o aplicación notepad



3.Matar Procesos

taskkill /PID 5108

taskkill /pid 3924 /t **/t** mata padre e hijos

taskkill /f /im notepad.exe **/f** forzosamente **/im** imagen del proceso

4.Buscar proceso

C:\WINDOWS\system32>tasklist /FI "PID eq 6712"

Nombre de imagen	PID	Nombre de sesión	Núm. de ses	Uso de memor
firefox.exe	6712	Console	1	208.716 KB

1.3 COMANDOS POWERSHELL

Get-Process: Muestra información de los procesos: name, id, cpu....
Start-Process: Inicia un proceso.
Stop-Process: Detiene un proceso.

EJEMPLOS

1. Obtener información básica
Get-Process
2. Obtener información ampliada
Get-Process | Select-Object *
3. Obtener información indicando el id del proceso
Get-Process -Id 2732
4. Obtener información sobre las propiedades de nombre, pid, company
Get-Process | Select-Object Name, Id, Company
5. Obtener información sobre las propiedades y ordenar por una propiedades
Get-Process | Select-Object Name, Id, Company | Sort-Object Name
6. Obtener los 5 primeros procesos
Get-Process | Select-Object Name, Id, Company | Sort-Object Name | Select-Object -First 5
7. Listar los procesos que tienen alto consumo de cpu
Get-Process | select cpu,id,name | sort cpu -Descending
8. Mostrar la descripción
Get-Process | select Name,Product,Description
9. Mostrar información indicando el nombre del proceso
Get-Process -Name notepad
10. Módulos que se ejecutan en los procesos
Get-Process -Module
11. Mostrar los hilos de los procesos
(Get-Process).Threads
12. Mostrar la prioridad de los hijos de los procesos
(Get-Process).Threads | Select-Object Id,CurrentPriority,BasePriority | Sort-Object Id
13. Contar el número de procesos
(Get-Process).count
14. Mostrar el tiempo transcurrido en la ejecución de un proceso
Get-Process | Select-Object Id,TotalProcessorTime
1. Iniciar proceso notepad
Start-Process notepad
2. Parar proceso notepad
Get-Process -Name notepad | Stop-Process

2. PROCESOS EN SEGUNDO PLANO: JOB

2.1 EN CMD

Iniciar programa.exe en segundo plano	start /B programa.exe
Iniciar programa.exe en segundo plano y lo minimiza	start /MIN programa.exe

Parar proceso en segundo plano	Taskkill /pid n°
--------------------------------	-------------------------

EJEMPLO

start /B notepad.exe

start /MIN notepad.exe

2.2 EN POWERSHELL

Muestra procesos en segundo plano	Get-Job
Ejecuta procesos en 2º plano	Start-Job
Elimina procesos en 2º plano.	Remove-Job

```
PS C:\Windows\system32> Start-Job -ScriptBlock {notepad}
```

Id	Name	PSJobTypeName	State	HasMoreData	Location
3	Job3	BackgroundJob	Running	True	localhost

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

Id	Name	PSJobTypeName	State	HasMoreData	Location
3	Job3	BackgroundJob	Completed	True	localhost

```
PS C:\Windows\system32> remove-job -id 3
```

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

```
PS C:\Windows\system32> _
```

3. ADMINISTRACIÓN DE SERVICIOS

- Un **servicio** es un proceso o conjunto de procesos que se ejecuta para ofrecer una funcionalidad.
- **Ejemplos:** dhcp, sshd, audio...
- En Windows los servicios son aplicaciones que se ejecutan en segundo plano.
- Muchos de ellos se inician al arrancar el sistema.
- Los servicios ejecutan procesos y los procesos tienen hilos, hay relación entre procesos e hilos y entre servicios e hilos.

3.1 EN MODO GRÁFICO

En administrador de tareas



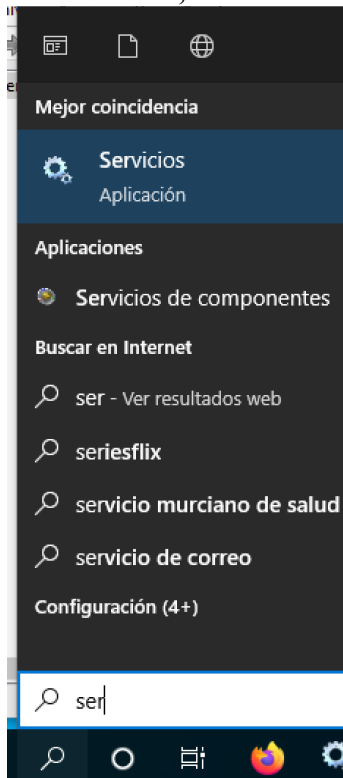
Administrador de tareas

Archivo Opciones Vista

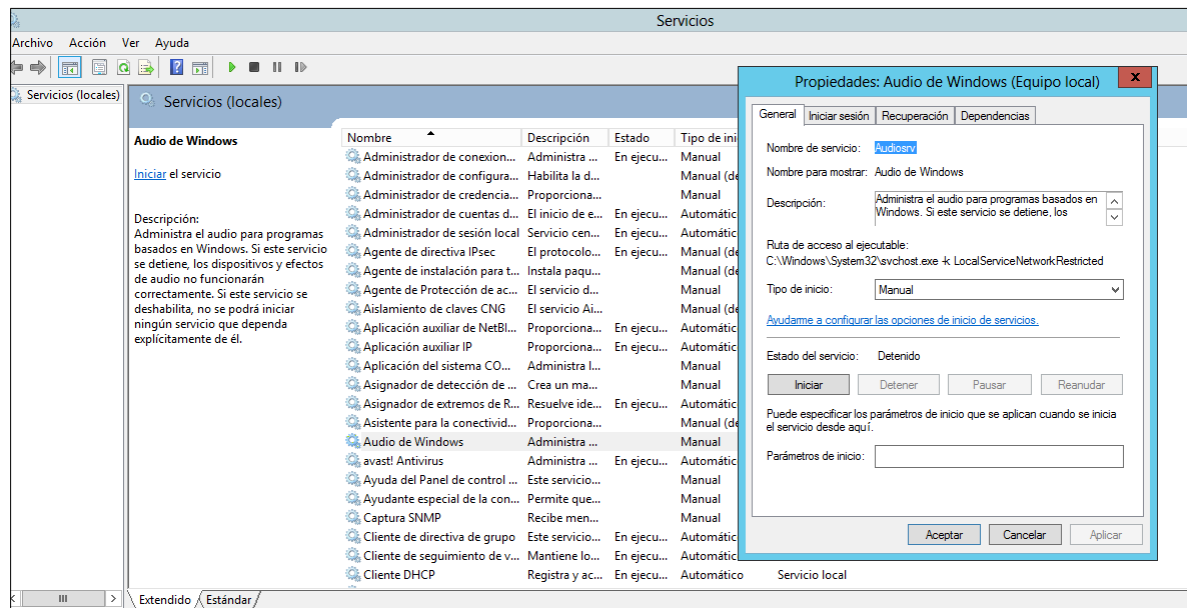
Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles **Servicios**

Nombre	PID	Descripción	Estado
Wcmsvc	1928	Administrador de conexiones de Windows	En ejecución
VaultSvc	596	Administrador de credenciales	En ejecución
SamSs	596	Administrador de cuentas de seguridad	En ejecución
TokenBroker	1020	Administrador de cuentas web	En ejecución
SEMGrSvc	1816	Administrador de pagos y NFC/SE	En ejecución
lsass	720	Administrador de sesión local	En ejecución

En buscador, teclear servicios



Para **visualizar** los detalles del servicio: **clic derecho** sobre el servicio > **Propiedades**

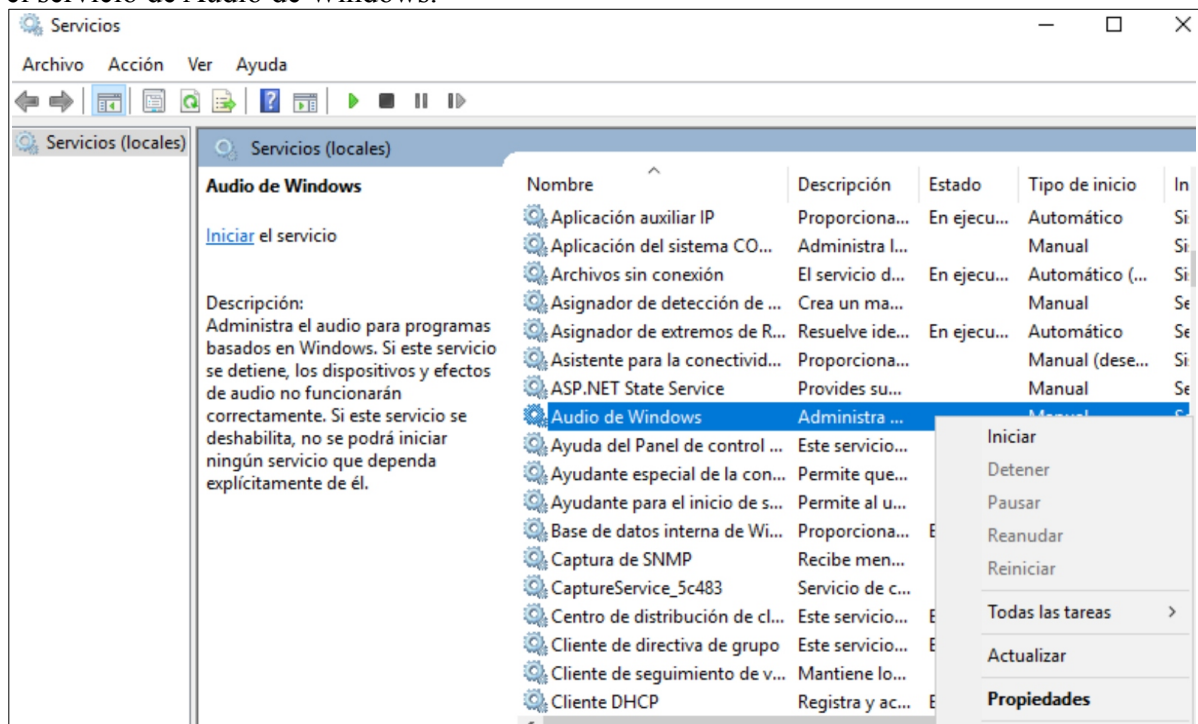


Podemos **cambiar el estado**.

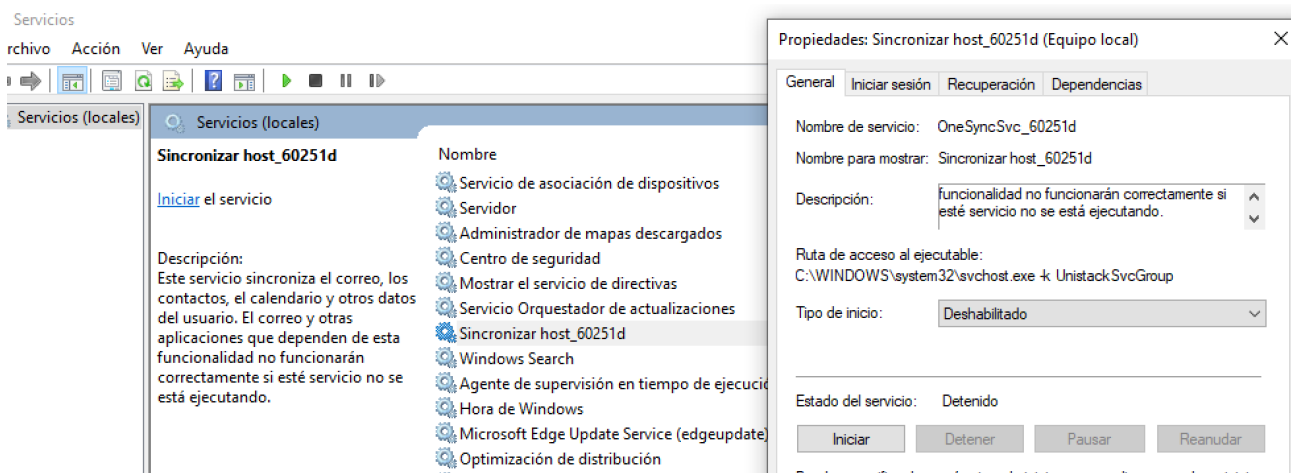
- Al modificar el estado de un servicio, puede solicitar la modificación de otro.
- En **Dependencias** se muestra un listado con todos los servicios de los que depende.

EJEMPLOS:

Iniciar el servicio de Audio de Windows.



Deshabilitar un servicio.



3.2 EN CMD

sc: consultar estado, iniciar, detener, pausar, eliminar,..

- **query:** muestra información sobre el servicio: el controlador, el tipo de servicio o el tipo de controlador especificados.
- **start:** Inicia un servicio
- **stop:** Detiene un servicio
- **pause:** Pausa un servicio
- **description:** Cambia la descripción de un servicio.

EJEMPLOS

Listar servicios	<pre>sc query</pre>
listar servicios activos	<pre>sc query type= service</pre>
listar servicios activos e inactivos	<pre>sc query state= all</pre>
Mostrar información de un servicio específico	<pre>C:\Users\usuario>sc query spooler</pre> <pre> NOMBRE_SERVICIO: spooler TIPO : 110 WIN32_OWN_PROCESS (interactive) ESTADO : 4 RUNNING (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN) CÓD_SALIDA_WIN32 : 0 (0x0) CÓD_SALIDA_SERVICIO: 0 (0x0) PUNTO_COMPROB. : 0x0 INDICACIÓN_INICIO : 0x0 </pre>
Mostrar información de servicios interactivos	<pre>sc query type=service type=interact</pre>

Parar servicio	<code>sc stop Themes</code>
Iniciar un servicio	<code>sc start Themes</code>

3.3 EN POWERSHELL

Listar todos los servicios	Get-Service
Arrancar servicio	Start-Service
Parar servicio	Stop-Service

Ejemplos

1. Listar los servicios

```
get-service
```

2. Listar los servicios que estén detenidos

```
get-service | where Status -eq Stopped
```

3. Ver el estado del servicio audiosrv

```
PS C:\WINDOWS\system32> get-service -Name Audiosrv

Status  Name      DisplayName
-----  -
Running Audiosrv  Audio de Windows
```

4. Parar el servicio audiosrv

```
PS C:\WINDOWS\system32> stop-service audiosrv
PS C:\WINDOWS\system32> get-service -Name Audiosrv

Status  Name      DisplayName
-----  -
Stopped Audiosrv  Audio de Windows
```

5. Arrancar el servicio **audiosrv**

```
PS C:\WINDOWS\system32> start-service audiosrv
PS C:\WINDOWS\system32> get-service -Name Audiosrv

Status  Name      DisplayName
-----  -
Running Audiosrv  Audio de Windows
```

6. Ver los servicios que dependen de otros

```
Get-Service | select Name, ServicesDependedOn
```


4. ADMINISTRACIÓN DE CARACTERÍSTICAS ADICIONALES DE WINDOWS

VISUALIZAR

AGREGAR

← Configuración

Características opcionales




 Agregar una característica

[Ver historial de características opcionales](#)

Características instaladas

Buscar una característica opcional instalada 

Ordenar por: Nombre ▾

	Bloc de notas	632 KB
	Cliente OpenSSH	10,1 MB
	Entorno de scripting integrado de Windows PowerShell	6,82 MB

ELIMINAR

Características opcionales

[Ver historial de características opcionales](#)

Características instaladas

Buscar una característica opcional instalada



Ordenar por: **Nombre** ▾



Bloc de notas

632 KB

Visualiza, edita y busca instantáneamente en documentos de texto sin formato y archivos de código fuente.

Desinstalar



Cliente OpenSSH

10,1 MB

Agregar una característica opcional

Buscar una característica opcional disponible



Ordenar por: **Nombre** ▾



Administración de almacenamiento de Windows

4,92 MB



Asistencia rápida de Microsoft

391 KB



Conjunto de herramientas EMS y SAC para Windows 10

82,1 KB



Consola de administración de impresión

393 KB



Controlador de herramientas de empaquetado MSIX

31,3 KB



Escucha de RIP

36,8 KB

Instalar (0)

Cancelar