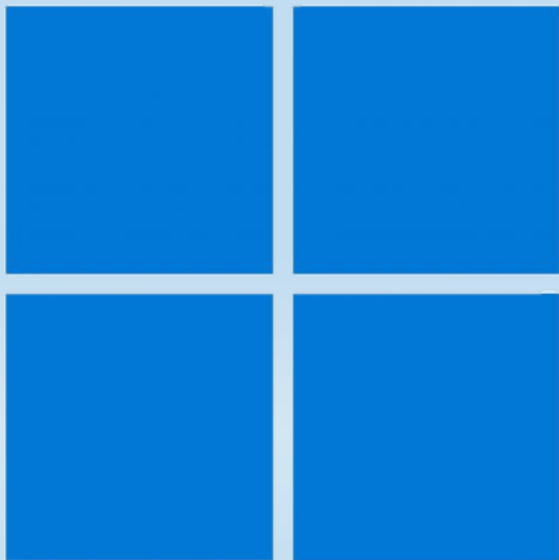
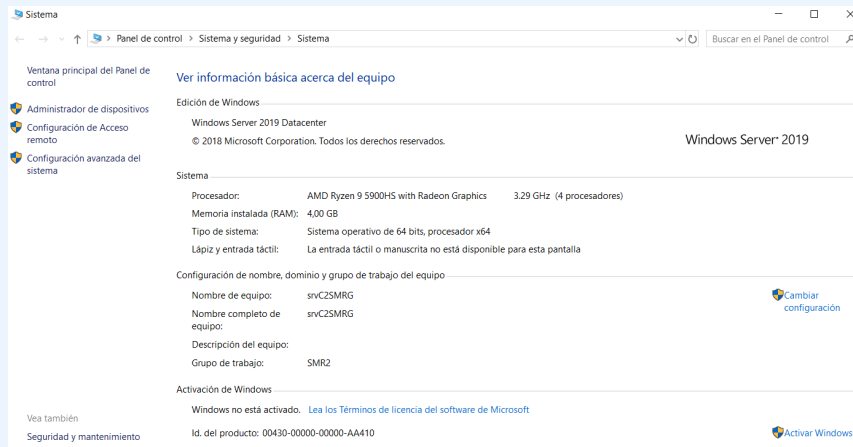


MONITORIZACIÓN DE EVENTOS Y RENDIMIENTO DEL SISTEMA

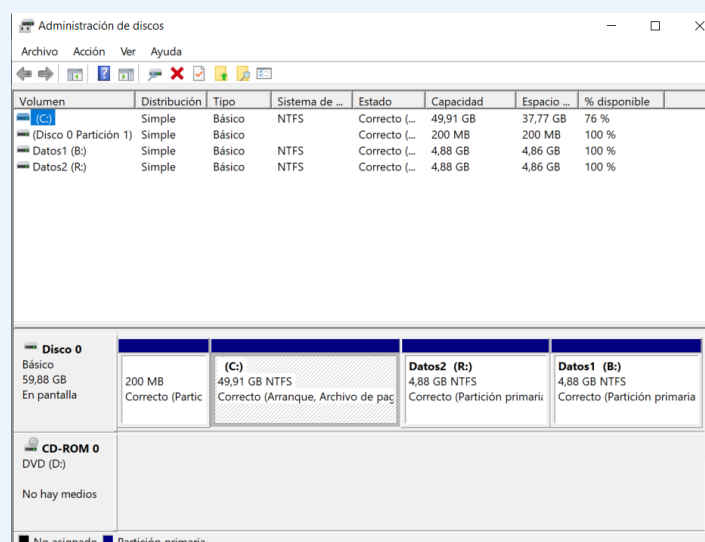


SISTEMAS OPERATIVOS EN RED
JUAN CARLOS NAVIDAD GARCÍA

1. SISTEMA: CPU, memoria y SO instalado: panel de control/sistema y seguridad/sistema y seguridad/sistema



2. ADMINISTRADOR DE DISCOS:DD: administrador del servidor/almacenamiento/administrador de discos.



3. INFORMACIÓN DEL SISTEMA: Es una herramienta administrativa de Windows.

a. Memoria física disponible

Memoria física instalad...	4,00 GB
Memoria física total	4,00 GB
Memoria física disponib...	2,46 GB

b. Memoria virtual

Memoria virtual total	5,37 GB
Memoria virtual disponi...	3,86 GB

c. Numero de cilindros

Nº total de cilindros	7.832
-----------------------	-------

d. Numero de sectores

Nº total de sectores	125.821.080
----------------------	-------------

e. DHCP: ¿habilitado?

DHCP habilitado	Sí
-----------------	----

4. HERRAMIENTAS DE MONITORIZACIÓN: Pertenecen al conjunto de herramientas administrativas

a. Enuméralas

i. Administrador de tareas;

Monitoriza la CPU, RAM, discos, red, procesos y servicios.

Se puede acceder tecleando administrador de tareas en la búsqueda del menú de inicio.

ii. Visor de eventos;

Almacena información del sistema y otros eventos generales de aplicaciones en el registro de eventos de Windows.

Se puede acceder tecleando visor de eventos en la búsqueda del menú de inicio.

iii. Monitor de recursos;

Recopila datos sobre el rendimiento del sistema mediante contadores que miden la actividad o el estado actual del sistema.

Se puede ejecutar escribiendo monitor de recursos en la búsqueda del menú de inicio.

iv. Monitor de rendimiento;

Ayuda a monitorizar un sistema tanto en tiempo real como recopilando datos que pueden ser analizados posteriormente.

Tecleando perfmon.msc en la herramienta "Ejecutar" (Windows + R) se ejecuta.

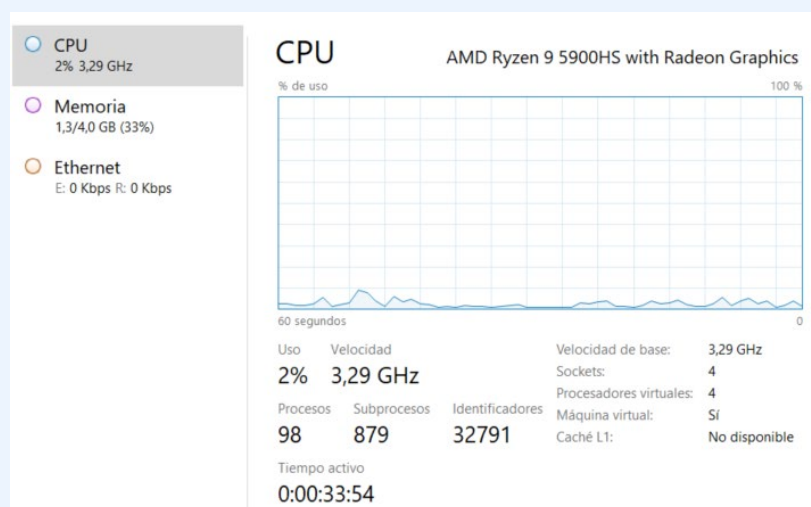
v. Programación de tareas.

Como el mismo nombre dice, se dedica programar tareas para que se ejecuten en un periodo de tiempo configurado.

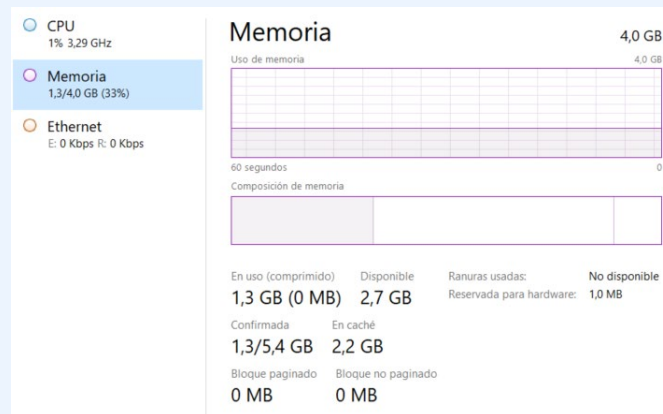
Tecleando el comando taskchd.msc en la herramienta "Ejecutar" (Windows + R) se ejecuta.

1. Monitoriza los recursos hardware de tu máquina virtual analizando con detalle el disco, procesador, memoria y red

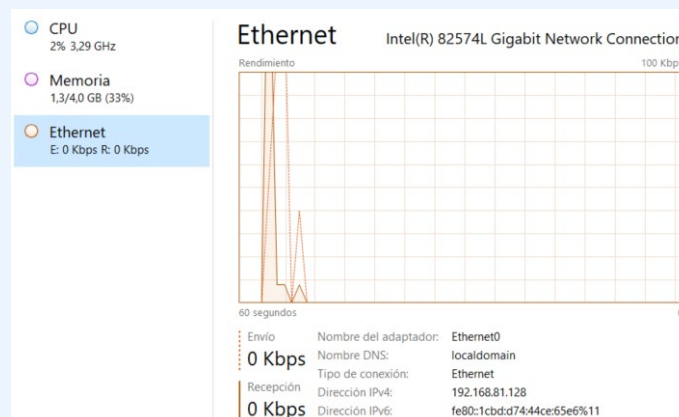
- CPU:



- **Memoria:**



- **Red:**



2. Lanza el navegador Chrome, busca el proceso asociado en el administrador de tareas y finalízalo

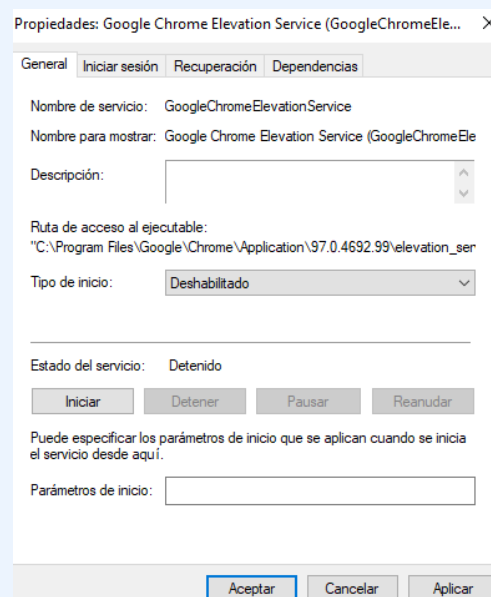
Aplicaciones (2)		
>	Administrador de tareas	1,9% 18,1 MB
>	Google Chrome (8)	1,5% 114,3 MB

Finalizar tarea

3. Detén el servicio Windows Update y después vuelve a iniciarlo

wuau servicing		Windows Update	Detenido	netsvcs
wuau servicing	3908	Windows Update	En ejecución	netsvcs

4. Cambia el servicio asociado al Chrome de Windows para que no se inicie automáticamente.



5. Vuelve a poner el servicio de Firewall de forma automática

Firewall de Windows Defen...	Firewall de Windows ...	En ejecu...	Automático	Servicio local
------------------------------	-------------------------	-------------	------------	----------------

1. Información que muestra cada evento

Visor de eventos (local)

Introducción y resumen

Introducción

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
<input checked="" type="checkbox"/> Información	-	-	-	28	289	818
	0	gupdate	Aplicación	0	3	6
	1	Diagnosis-Scri...	Microsoft...	0	0	1
	1	FilterManager	Sistema	0	1	3
	1	Kernel-General	Sistema	1	3	3
	3	Virtual Disk Ser...	Sistema	0	1	1
	3	vmci	Sistema	0	1	3
	4	Virtual Disk Ser...	Sistema	1	1	1
	6	FilterManager	Sistema	0	9	27
	12	Kernel-General	Sistema	0	1	4
	14	Wininit	Sistema	0	1	3
	15	Kernel-General	Sistema	0	0	1
	16	Kernel-General	Sistema	0	1	16
	18	Kernel-Boot	Sistema	0	1	4
	19	WindowsUpdat...	Sistema	0	1	3

2. Niveles de criticidad de eventos

Visor de eventos (local)

Introducción y resumen

Introducción

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
<input checked="" type="checkbox"/> Crítico	-	-	-	0	1	2
	41	Kernel-Power	Sistema	0	1	2

3. Muestra el registro de Windows e indica:

- a. Las categorías con su función
 - i. **Aplicación:** guarda los eventos relacionados con aplicaciones que no son del SO.
 - ii. **Seguridad:** registra los eventos relacionados con la seguridad del equipo.
 - iii. **Instalación:** almacena los eventos relacionados con la instalación de roles o características de Windows Server.
 - iv. **Sistema:** registra información y eventos relacionados con el propio SO.
 - v. **Eventos reenviados:** almacena eventos que son enviados desde otros servidores o equipos, normalmente a través de la red.

b. Extensión de los archivos que guardan la información del registro de Windows

La extensión de los archivos del registro de Windows es **.evtx**

c. Ubicación

- i. C:\Windows\System32\Winevt\Logs\
- ii. C:\Windows\System32\Config

d. Nombre del fichero de cada una categoría

- Application.evtx
- Security.evtx
- Setup.evtx
- System.evtx
- ForwardedEvents.evtx

e. Que son las vistas personalizadas del visor de eventos

Permite filtrar por eventos específicos y así conseguir que sea más fácil localizar lo que se está buscando.

4. Indica el día que se instaló la última actualización de Windows defender mirando el registro de eventos

Número de eventos: 11

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	26/01/2022 12:22:27	WindowsU...	41	Agente de ...
Información	20/01/2022 12:53:18	WindowsU...	41	Agente de ...
Información	20/01/2022 11:14:21	WindowsU...	41	Agente de ...
Información	19/01/2022 8:40:12	WindowsU...	41	Agente de ...
Información	14/01/2022 10:57:47	WindowsU...	41	Agente de ...
Información	14/01/2022 10:51:32	WindowsU...	41	Agente de ...
Información	14/01/2022 10:50:44	WindowsU...	41	Agente de ...
Información	14/01/2022 10:50:44	WindowsU...	41	Agente de ...
Información	14/01/2022 10:50:39	WindowsU...	41	Agente de ...
Información	13/01/2022 13:06:21	WindowsU...	41	Agente de ...
Información	13/01/2022 13:03:42	WindowsU...	41	Agente de ...

Evento 41, WindowsUpdateClient

General Detalles

Se descargó una actualización.

5. Busca todos los errores críticos que ha generado el sistema operativo en la última semana. Guarda la vista personalizada con el nombre Criticos-so-1semana

Criticos-so-1semana Número de eventos: 2

Número de eventos: 2

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Crítico	26/01/2022 11:21:37	Kernel-Power	41 (63)	
Crítico	20/01/2022 12:43:05	Kernel-Power	41 (63)	

6. Encuentra todos los registros (de cualquier nivel) que hayas generado PowerShell en el último mes. Guarda la vista con el nombre PowerShell-1mes

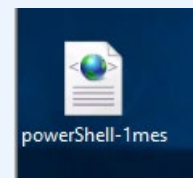
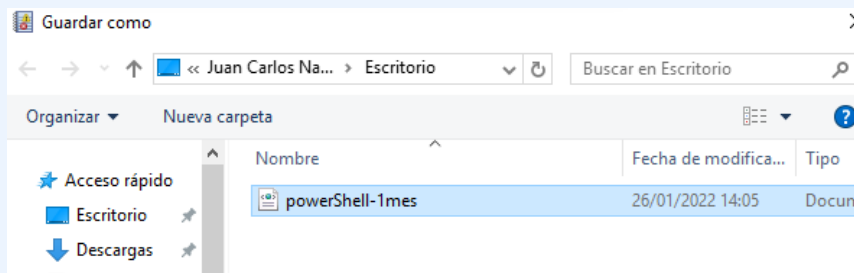
PowerShell-1mes Número de eventos: 56

Número de eventos: 56

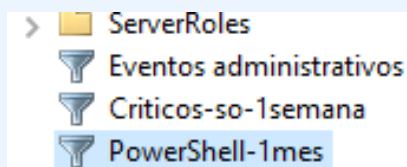
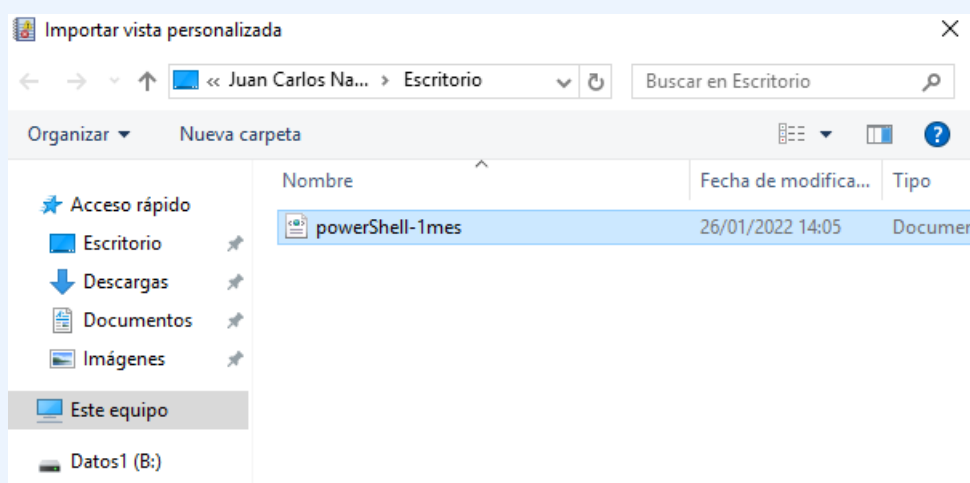
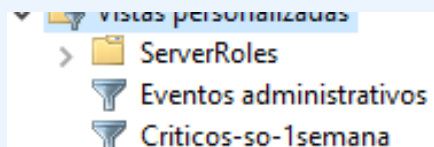
Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	20/01/2022 12:45:13	PowerShell ...	400	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 12:45:13	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	400	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:39:54	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:21:01	PowerShell ...	403	Ciclo de vid...
Información	20/01/2022 11:20:56	PowerShell ...	400	Ciclo de vid...
Información	20/01/2022 11:20:56	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:20:56	PowerShell ...	600	Ciclo de vid...
Información	20/01/2022 11:20:56	PowerShell ...	600	Ciclo de vid...

Evento 400, PowerShell (PowerShell)

7. Exporta la vista personalizada powerShell-1mes



8. Bórrala y después, impórtala a través del archivo con el formato XML generado en el apartado anterior



1. Usos del monitor de rendimiento

Ayuda a monitorizar un sistema tanto en tiempo real como recopilando datos que pueden ser analizados posteriormente.

2. Tres formas de invocar el monitor de rendimiento

Escribir en el campo de búsqueda de inicio de Windows, **Monitor de Rendimiento**.

En la ventana de Ejecutar escribir **perfmon.msc**

También lo podemos abrir desde el **panel de control** en el apartado de **Sistema y Seguridad → Herramientas Administrativas**.

3. Que muestra por defecto el monitor de rendimiento

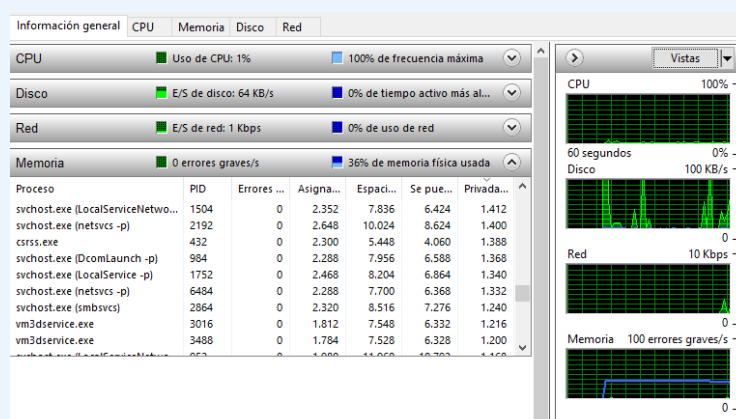
Por primera vez te mostrará una visión general y un resumen del sistema.

4. Para que sirven los contadores del monitor de rendimiento

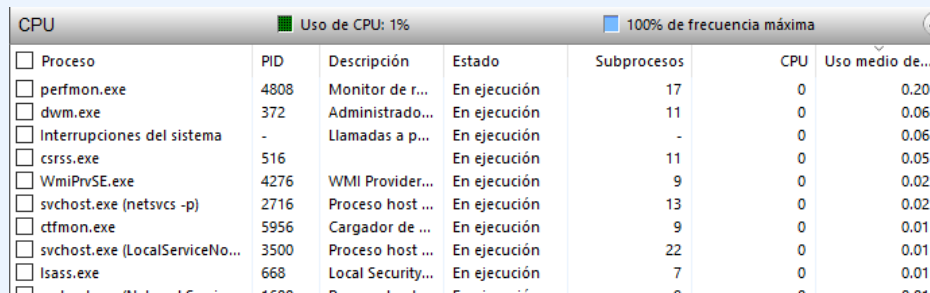
Este contador mide el tiempo que una entrada de un usuario cualquiera.

1. Monitoriza utilizando el monitor de recursos el rendimiento de un equipo del aula para saber:

a. Rendimiento de la memoria

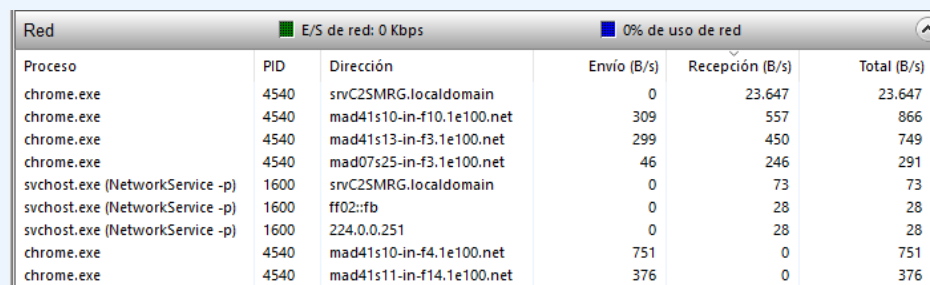


b. Procesos que más CPU están consumiendo



Proceso	PID	Descripción	Estado	Subprocesos	CPU	Uso medio de...
perfmon.exe	4808	Monitor de r...	En ejecución	17	0	0.20
dwm.exe	372	Administrado...	En ejecución	11	0	0.06
Interrupciones del sistema	-	Llamadas a p...	En ejecución	-	0	0.06
csrss.exe	516		En ejecución	11	0	0.05
WmiPrvSE.exe	4276	WMI Provider...	En ejecución	9	0	0.02
svchost.exe (netsvc...	2716	Proceso host ...	En ejecución	13	0	0.02
ctfmon.exe	5956	Cargador de ...	En ejecución	9	0	0.01
svchost.exe (LocalServiceNo...	3500	Proceso host ...	En ejecución	22	0	0.01
lsass.exe	668	Local Security...	En ejecución	7	0	0.01

c. Que procesos están recibiendo más datos de red



Proceso	PID	Dirección	Envío (B/s)	Recepción (B/s)	Total (B/s)
chrome.exe	4540	srvC2SMRG.localdomain	0	23.647	23.647
chrome.exe	4540	mad41s10-in-f10.1e100.net	309	557	866
chrome.exe	4540	mad41s13-in-f3.1e100.net	299	450	749
chrome.exe	4540	mad07s25-in-f3.1e100.net	46	246	291
svchost.exe (NetworkService -p)	1600	srvC2SMRG.localdomain	0	73	73
svchost.exe (NetworkService -p)	1600	ff02::fb	0	28	28
svchost.exe (NetworkService -p)	1600	224.0.0.251	0	28	28
chrome.exe	4540	mad41s10-in-f4.1e100.net	751	0	751
chrome.exe	4540	mad41s11-in-f14.1e100.net	376	0	376

2. Formas de invocar al programador de tareas

Se puede abrir desde el mismo administrador de tareas.

Escribiendo Programador de tareas en la barra de búsqueda del menú de inicio.

Tecleando el comando taskchd.msc en la herramienta "Ejecutar" (Windows + R) se ejecuta.

3. Donde ver la lista de tareas programadas del sistema

En la pantalla principal del programador de tareas aparecen todas las tareas programadas del sistema.

4. Programa una tarea para lanzar el desfragmentador del disco duro todos los domingos a las seis de la tarde

Inicio: 26/01/2022 18:00:00 ☐ Sincronizar zonas horarias

Repetir cada: 1 semanas en:

☒ Domingo ☐ Lunes ☐ Martes ☐ Miércoles

☐ Jueves ☐ Viernes ☐ Sábado

Programa o script:

C:\Windows\system32\dfmgrui.exe [Examinar...](#)

5. Crea una tarea programada que invoque al programa que hace limpieza en el disco duro de los archivos que no son necesarios todos los días 1 de cada mes a las 23:00 horas

Crear una tarea básica

Desencadenar

Mensualmente

Acción

Finalizar

Inicio: 01/02/2022 23:00:00 ☐ Sincronizar zonas horarias

Meses: Enero, Febrero, Marzo, Abril...

☒ Días: 1

☐ El:

Crear una tarea básica

Desencadenar

Mensualmente

Iniciar un programa

Finalizar

Programa o script:

C:\Windows\system32\cleanmgr.exe [Examinar...](#)

Agregar argumentos (opcional):

Iniciar en (opcional):