

SISTEMAS INFORMÁTICOS

**Servicios, procesos
y monitorización**

ÍNDICE

/ 1. Introducción y contextualización práctica	3
/ 2. Servicios	4
2.1. Gestión de los servicios	5
/ 3. Procesos	6
3.1. Procesos en Windows	7
/ 4. Monitorización del sistema	8
4.1. Monitor de rendimiento	9
4.2. Monitor de recursos	10
4.3. Monitor de confiabilidad	12
/ 5. Interpretación de logs y sucesos en el sistema	13
5.1. Explotación del visor de eventos	14
/ 6. Caso práctico 1: “Detener servicios al inicio de Windows”	16
/ 7. Caso práctico 2: “Rendimiento de los componentes del servidor”	17
/ 8. Resumen y resolución del caso práctico de la unidad	18

SÓLO VOS

- Conocer e identificar los tipos de procesos y servicios de un sistema operativo.***
- Utilizar herramientas de monitorización del sistema.***
- Visualizar los sucesos del sistema.***
- Entender un log del sistema.***

/ 1. Introducción y contextualización práctica

Durante este tema, conoceremos qué es un proceso y un servicio, y cómo se gestinan en Windows Server. Gracias a los procesos y servicios, funcionan tanto el sistema operativo como sus aplicaciones. Ambos son elementos cruciales en los sistemas informáticos, ya que una de las causas de la sobrecarga de un sistema es la saturación o mal funcionamiento de los procesos o servicios.

Por ello, aprenderemos a utilizar herramientas de monitorización que nos ayuden a identificar procesos y eventos problemáticos, así como a interpretar logs que nos describan los sucesos del sistema.

A continuación, vamos a plantear un caso práctico a través del cual podremos aproximarnos de forma práctica a la teoría de este tema.



Fig. 1. Herramienta Servicios en Windows.

/ 2. Servicios

Un **servicio** es una aplicación o conjunto de aplicaciones que ejecuta un sistema operativo para ofrecer una determinada funcionalidad al resto de objetos del sistema o del dominio.

Los servicios de Windows son pequeños programas que se ejecutan en segundo plano sin que el usuario intervenga. Al iniciar Windows, muchos de ellos se inician automáticamente.

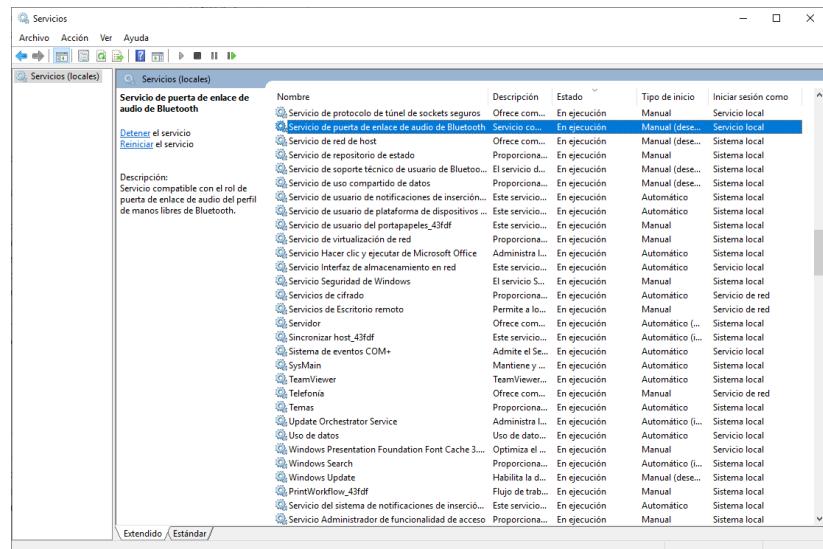


Fig. 2. Herramienta Servicios en Windows.

En los sistemas Windows, se utiliza la aplicación Servicios para visualizar y realizar modificaciones sobre ellos. Se encuentra en las Herramientas administrativas.



Fig. 3. Servicios.

Cuando se realizan modificaciones en los servicios, hay que tener en cuenta que puede acarrear efectos no deseados. Por ejemplo, si se deshabilita el servicio *Cola de impresión*, no será posible imprimir documentos.

Otros servicios críticos que se recomienda no deshabilitar:

- **Cliente DHCP.** Es el responsable de asignar automáticamente una dirección IP al equipo.
- **Conexiones de red.** Administra la red.
- **Plug and Play.** Detecta los cambios de hardware o nuevas conexiones de dispositivos para que funcionen automáticamente.
- **Programador de tareas.** Permite al usuario configurar y programar tareas automáticas.
- **Servicio de perfil de usuario.** Se encarga de cargar los perfiles de usuario al inicio de sesión.
- **Windows Update.** Gestiona la descarga e instalación de las actualizaciones de Windows.

2.1. Gestión de los servicios

Al iniciar la aplicación *Servicios*, se muestra el listado de servicios disponibles en el sistema y algunas de sus características:

- **Nombre.** Cada servicio tiene un nombre único que lo identifica.
- **Descripción.** Se describe la función principal del servicio.
- **Estado.** Un servicio puede encontrarse en ejecución o detenido.
- **Tipo de inicio.** Un servicio puede iniciarse de cuatro formas diferentes:
 - **Automático (inicio retrasado).** Se inicia junto al sistema operativo, pero una vez que ha sido cargado el sistema operativo y todos los servicios.
 - **Automático.** Se inicia simultáneamente con el sistema operativo.
 - **Manual.** Solo se inicia si el usuario lo hace manualmente o como consecuencia de la ejecución de otro programa o servicio.
 - **Deshabilitado.** El servicio no se puede iniciar ni de forma manual ni automática.

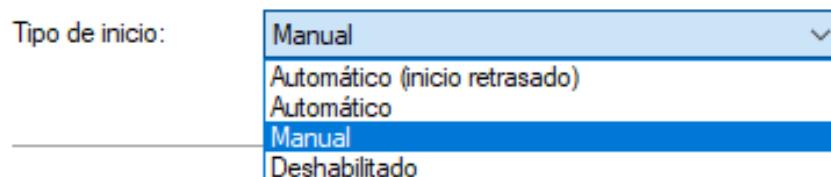


Fig. 4. Tipos de inicio para los servicios.

- **Iniciar sesión como.** Puede tratarse de un servicio local, como el administrador de credenciales, o de un servicio de red, como es el administrador de conexiones de acceso remoto.

a) Gestión de servicios por comando

Desde la línea de comandos *cmd* es posible gestionar los servicios de Windows.

A través del comando *sc query*, nos muestra el listado completo de servicios e información, así como su estado o tipo. Para iniciar un servicio, se utiliza *Net start nombredelservicio* y, para detenerlo, *net stop nombredelservicio*.

```
C:\WINDOWS\system32>net stop wuauserv
El servicio de Windows Update está deteniéndose.
El servicio de Windows Update no ha podido detenerse.

C:\WINDOWS\system32>net start wuauserv
El servicio solicitado ya ha sido iniciado.

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

Fig. 5. Detención e inicio del servicio Windows Update.

/ 3. Procesos

Un **proceso** es un programa que está en ejecución, como instancia de una aplicación. Una aplicación determinada puede necesitar varios procesos ejecutándose simultáneamente.

Por ejemplo, algunos navegadores, como Internet Explorer, ejecutan varios procesos a la vez, y cada pestaña es, en realidad, una instancia o proceso separado del mismo *software*, ya que puede necesitar procesos adicionales para reproducir contenido multimedia, flash o Java.

Otras aplicaciones, como Microsoft Word, se ejecutan desde un solo proceso, incluso no importa cuántas ventanas se hayan abierto, solo se está ejecutando una única instancia de winword.exe.

a) Tipos de procesos

Se distinguen, fundamentalmente, dos tipos de procesos:

- **Procesos en primer plano.** También conocidos como interactivos. Se inician y controlan a través de una sesión de terminal. Solo se inician a través de un usuario.
- **Procesos en segundo plano.** Son procesos que se inician automáticamente como parte del sistema o necesidad de alguno de los servicios para funcionar.

b) Estados de un proceso

Aunque podemos encontrar diferentes estados de un proceso dependiendo del sistema operativo, como mínimo encontraremos los siguientes:

- **Ejecución.** El proceso se encuentra activo.
- **Espera.** No se encuentra en activo, pero sí preparado y a la espera de que ocurra algún evento que requiera su inicio.
- **Detenido.** El proceso no se encuentra en ejecución. Puede no haberse ejecutado o haberse detenido al finalizar o cerrar una aplicación.
- **Suspendido.** El proceso no se está ejecutando, pero se ha detenido y aún tiene una entrada en la tabla de procesos.

ESTADOS DE PROCESO



Fig. 6. Estados de un proceso.

3.1. Procesos en Windows

En los sistemas Windows, a través de la tradicional herramienta *Administrador de tareas*, podemos visualizar un listado de procesos lanzados e información sobre las aplicaciones que se están ejecutando en ese momento.

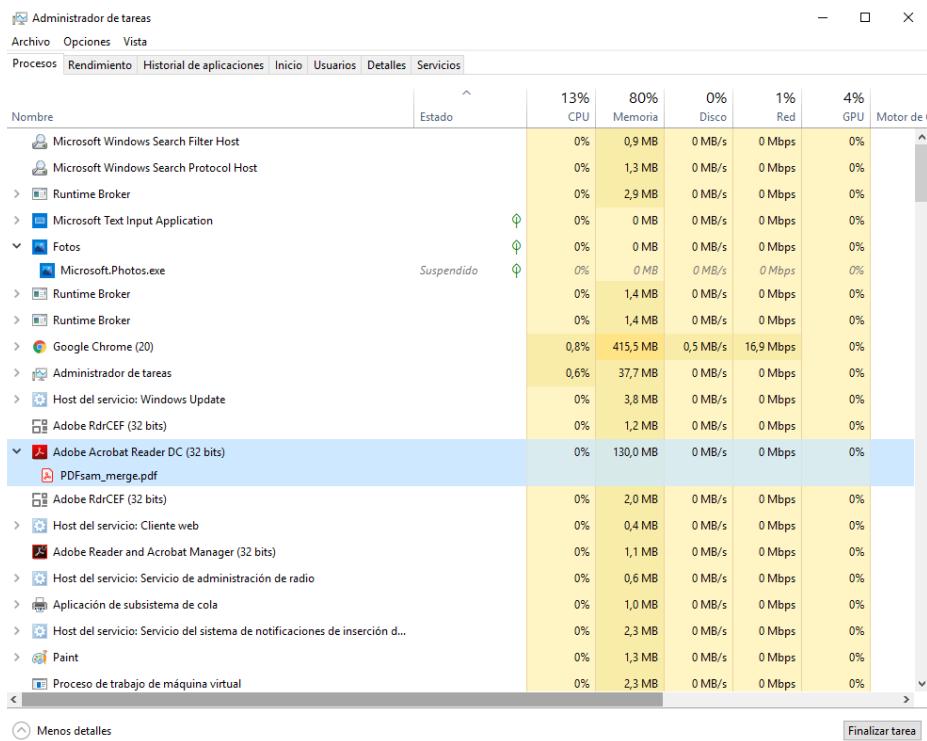


Fig. 7. Administrador de tareas en un sistema Windows.

Por cada proceso, se visualiza gran cantidad de información, como el nombre del proceso y el consumo de recursos de hardware que está realizando en tiempo real.

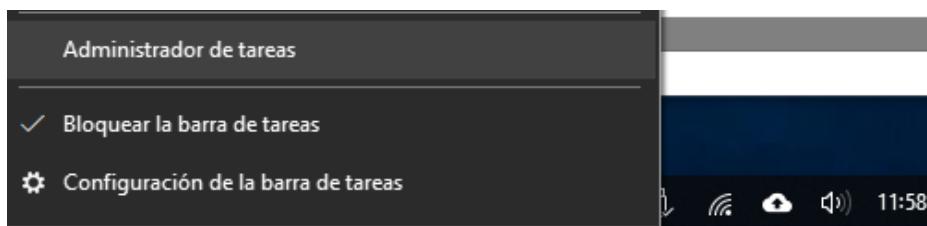


Fig. 8. Abrir el administrador de tareas desde la barra de inicio.

El *Administrador de tareas* puede abrirse presionando simultáneamente Ctrl+Alt+Supr o bien haciendo clic en la barra de inicio de Windows con el botón derecho y seleccionando *Administrador de tareas*.

En la primera pestaña, *Procesos*, se muestran todos los procesos del sistema que están en ejecución. Haciendo clic con el botón derecho sobre cualquiera de ellos, se puede:

- Abrir la ubicación del archivo.
- Finalizar tarea. Detiene el proceso, y aquellos que tenga asociados.

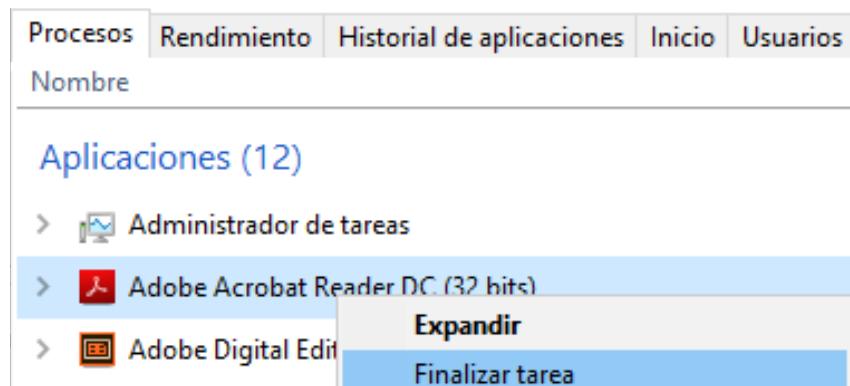


Fig. 9. Finalizar proceso.

- Modificar su prioridad respecto al resto de procesos.
- Ver las propiedades. Se muestra información acerca del proceso, permisos, ubicación, la aplicación a la que pertenece, etc.

/ 4. Monitorización del sistema

A través del proceso de monitorización, se recoge información sobre la actividad del sistema. Cuando se monitoriza un servidor, se obtiene información relativa a una serie de parámetros relacionados con su actividad, como el consumo de recursos: memoria, red, CPU o el uso de disco.

A través de la monitorización del rendimiento de un servidor, se consigue:

- Conocer la disponibilidad del servidor y sus posibles pérdidas o fallos del sistema.
- Controlar y conocer la capacidad de respuesta del servidor.
- Conocer la capacidad, carga de trabajo y velocidad del servidor.
- Prevenir futuros problemas que puedan afectar al rendimiento.

a) Herramientas de monitorización

Hay varias técnicas y herramientas de monitorización, dependiendo del análisis que efectúen, entre las que se encuentran:

- Herramientas de monitorización en **tiempo real**. Muestra la actividad del sistema, permitiendo visualizarla en todo momento y, como su nombre indica, en tiempo real. Por ejemplo, se utiliza en entornos de pruebas para verificar el funcionamiento de un servidor con nuevas aplicaciones.
- Herramientas de monitorización **continuada**. Sistema de monitorización que analiza los sistemas de forma continua y periódica, para que ante cualquier contingencia sea posible adelantarse a un problema, o reducir el tiempo de reacción si llega a producirse el problema.
- Herramientas de análisis del **rendimiento**. Recoge datos detallados sobre los recursos del sistema, servicios en ejecución o aplicaciones en tiempo real o de forma continua.

Windows Server proporciona varias herramientas que ayudan a los administradores del sistema a monitorizarlo. Pero también hay herramientas externas muy completas que monitorizan toda la infraestructura informática, incluyendo, además todo lo relacionado con los servidores, los dispositivos de red y sus servicios.

The screenshot shows the Centreon web interface. At the top, there are navigation tabs: Home, Monitoring (which is selected), Reporting, Configuration, and Administration. Below the tabs, there are sub-navigation links: Status Details, Performances, Downtimes, and Event Logs. The main content area is titled "Monitoring > Status Details > Services". It features several filter dropdowns: Service Status (All), Host (MV-HECTOR), Status (OK), Poller (All), Servicegroup (None), and Output (None). A "More actions..." button is available. The main table lists four services: Cpu, Memory, Ping, and Swap, all in OK status. Each row includes columns for Host, Service, Status, Duration, Last Check, Tries, and Status Information. The "Status Information" column for Cpu shows: OK: CPU(s) average usage is: 0.00%. For Memory: OK: RAM Total: 12.00 GB Used: 2.98 GB (24.80%) Free: 9.02 GB (75.20%). For Ping: OK - 192.168.1.56; rta 0.087ms, lost 0%. For Swap: OK: Swap Total: 13.81 GB Used: 2.94 GB (21.30%) Free: 10.87 GB (78.70%).

Fig. 10. Herramienta Centreon generando alertas sobre un servidor.

4.1. Monitor de rendimiento

El *Monitor de rendimiento* se incluye en los sistemas Windows para ver datos de rendimiento en tiempo real o desde un archivo de registro. Se encuentra en las *Herramientas administrativas*.



Fig. 11. Monitor de rendimiento.

Su funcionamiento se basa en la utilización de contadores de los cuales dependen los roles, funciones y características instaladas en el servidor. Por defecto, se incluyen algunos contadores para realizar un diagnóstico automático, pero, haciendo clic en el símbolo +, es posible agregar otros contadores a la ventana de visualización del rendimiento.

The screenshot shows the "Agregar contadores" (Add counters) dialog box. At the top, it says "Contadores disponibles" (Available counters) and "Seleccionar contadores del equipo:" (Select counters from the computer:). A dropdown menu shows "<Equipo local>" (Local Computer) and an "Examinar..." (Browse...) button. Below this is a list of performance counter categories: "Actividad de RDMA", "Actividad de tarjeta de interfaz de red física", "Actividad de tarjeta de interfaz de red por pro...", "Adaptador de red", "Ancho de banda actual", "Bytes enviados/s", "Bytes recibidos/s", and "Conexiones descargadas".

Fig. 12. Agregar contadores al Monitor de rendimiento.

Los resultados de los contadores activados se muestran gráficamente.

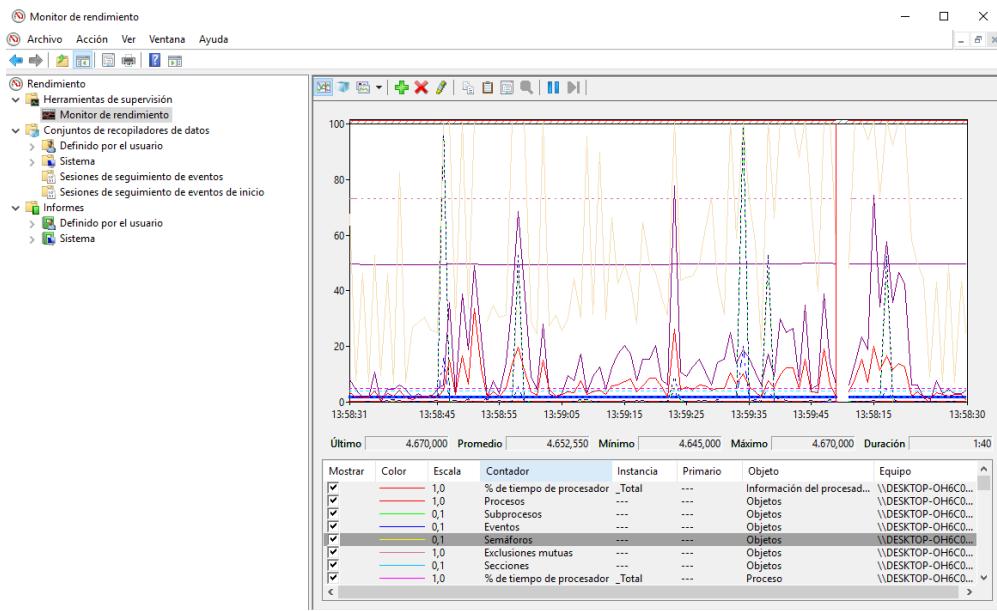


Fig. 13. Monitor de rendimiento en Windows Server.

Para ver el informe sobre los parámetros configurados hay que hacer clic en *Informe*:

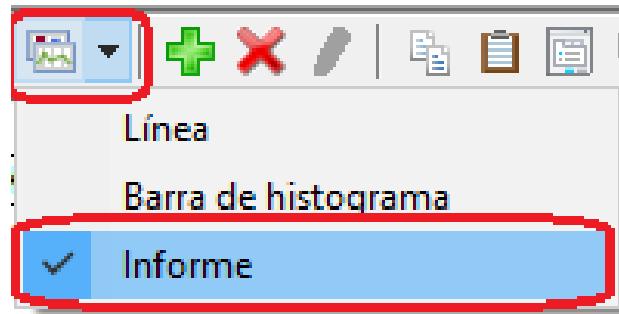


Fig. 14. Ver informe sobre los parámetros configurados.

Cuando se utiliza esta herramienta, hay que tener en cuenta que el sistema está ejecutando una aplicación más, por lo que, en algún momento, puede llegar a sobrecargarse o a ofrecer un informe que no es del todo fiable.

4.2. Monitor de recursos

El *Monitor de recursos* permite visualizar información, en tiempo real, acerca de los recursos de *hardware* y del sistema, utilizados por el sistema operativo, además de servicios y aplicaciones en ejecución. También se encuentra entre las *Herramientas administrativas*.

Al abrir el *Monitor de recursos*, se muestran varios gráficos en los que se informa sobre la CPU, el disco, la red y la memoria RAM.

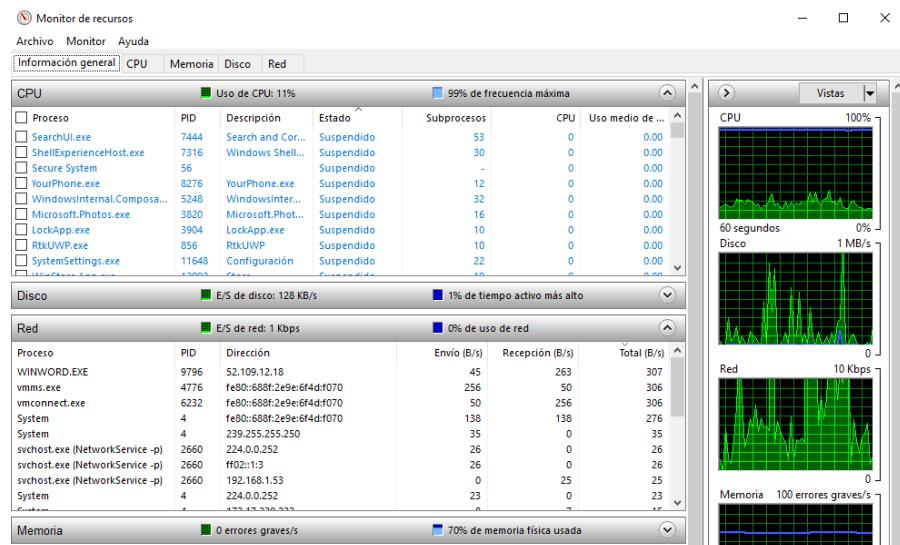


Fig. 15. Monitor de recursos.

Hay pestañas para cada uno de los componentes principales de hardware:

- **CPU:** Se muestran todos los procesos activos, junto con el número de subprocessos que dependen de cada uno de ellos.

Proceso	PID	Dirección	Envío (B/s)	Recepción (B/s)	Total (B/s)
WINWORD.EXE	9796	52.109.12.18	45	263	307
vmmem.exe	4776	f80:680f:2e9e:6f4d:f070	256	50	306
vmconnect.exe	6232	f80:680f:2e9e:6f4d:f070	50	256	306
System	4	f80:680f:2e9e:6f4d:f070	138	138	276
System	4	239.255.255.250	35	0	35
svchost.exe (NetworkService -p)	2660	224.0.0.252	26	0	26
svchost.exe (NetworkService -p)	2660	f02:1:13	26	0	26
svchost.exe (NetworkService -p)	2660	192.168.1.53	0	25	25
System	4	224.0.0.252	23	0	23

Fig. 16. Estado de los procesos.

- **Memoria:** Muestra información acerca de la memoria RAM disponible, en uso y la cantidad que está utilizando cada uno de los procesos.

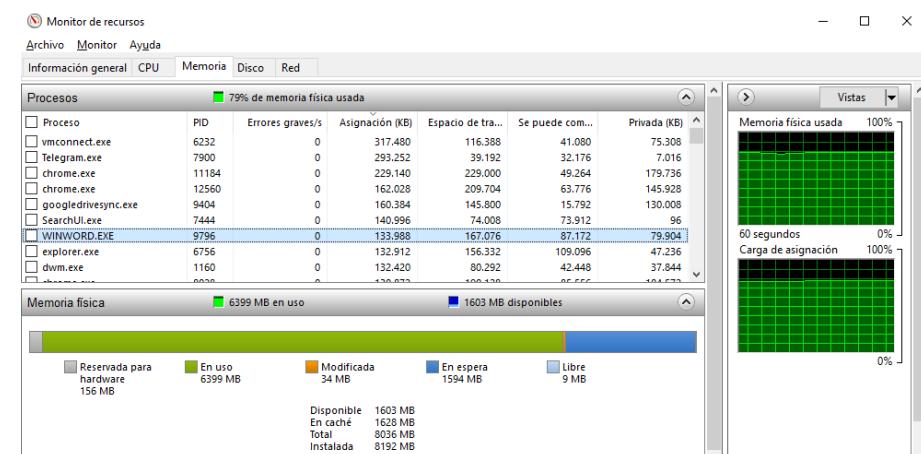


Fig. 17. Memoria.

- **Disco.** Muestra estadísticas de lectura y escritura. En la parte inferior, muestra la capacidad.

- **Red.** Hace un seguimiento real sobre toda la actividad de la red. Se incluye el uso de red, número de conexiones TCP o los puertos o direcciones de destino, a través de las cuales se realizan las comunicaciones de cada proceso.

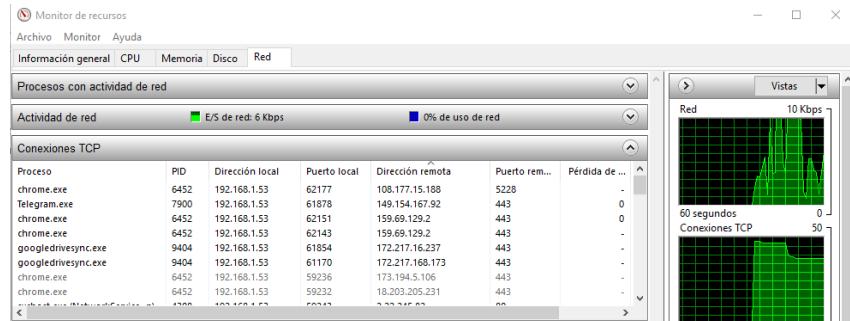


Fig. 18. Red.

4.3. Monitor de confiabilidad

En el *Monitor de confiabilidad* se registran todos aquellos problemas de *hardware* y *software* producidos en el sistema. Se accede desde *Panel de control > Seguridad y mantenimiento > Ver historial de confiabilidad*.

El *Monitor de confiabilidad* ayuda, principalmente, a determinar si la estabilidad del sistema ha cambiado desde la instalación de un *software* o componente o de un terminado evento.



Fig. 19. Monitor de confiabilidad.

Ofrece una vista gráfica sobre la estabilidad del sistema a lo largo del tiempo en la que se indica:

- Un índice de estabilidad. El valor puede ir de 1 al 10, siendo el 10 un sistema estable.
- Los días que el sistema ha estado funcionando.
- Los días en los que se ha producido algún evento informativo. Por ejemplo, instalar un *software*. Son mostrados con iconos azules y la letra i.
- Los días en los que se ha producido algún evento, pero con alguna advertencia. Por ejemplo, un error puntual de instalación de una actualización de Windows Update. Son mostrados con un ícono amarillo y una exclamación !.
- Los días en los que se ha producido un evento con error. Por ejemplo, el cierre inesperado de una aplicación. Se muestra un ícono rojo con una x.

Detalles de confiabilidad de: 08/05/2020

Origen	Resumen	Fecha
Eventos críticos		
<input type="checkbox"/> EXCEL.EXE	Dejó de funcionar	08/05/2020 12:53
Advertencias (4)		
<input type="checkbox"/> 9PLK42WDORC0-Microsoft.Ph...	Error de Windows Update	08/05/2020 11:38
<input type="checkbox"/> 9PLK42WDORC0-Microsoft.Ph...	Error de Windows Update	08/05/2020 11:38
<input type="checkbox"/> 9PLK42WDORC0-Microsoft.Ph...	Error de Windows Update	08/05/2020 11:38
<input type="checkbox"/> LibreOffice 6.4.3.2	Instalación de aplicación incorrecta	08/05/2020 10:47
Eventos informativos (3)		
<input type="checkbox"/> 9WZDNCRFBMP-MICROSOFT...	Operación correcta de Windows Update	08/05/2020 16:01
<input type="checkbox"/> 9NBLGGH4LS1F-Microsoft.Stor...	Operación correcta de Windows Update	08/05/2020 16:01
<input type="checkbox"/> QDI K42WDORC0-Microsoft Pho...	Operación correcta de Windows Update	08/05/2020 11:53

Fig. 20. Eventos con diferentes estados en el Monitor de confiabilidad.

Para ampliar información sobre el evento, tan solo hay que hacer doble clic sobre el evento deseado.

También permite almacenar un historial presionando en la parte inferior *Guardar historial de confiabilidad*.

/ 5. Interpretación de logs y sucesos en el sistema

Un evento o suceso es un acontecimiento del sistema o de cualquier *software* que provoque hecho relevante para el equipo. Dichos sucesos son almacenados en *logs*, archivos que contienen los registros ocurridos en un determinado espacio de tiempo.

La herramienta que examina y administra los eventos del sistema en Windows Server es el *Visor de eventos*, hasta hace unos años conocida como *Visor de sucesos*. Se encuentra entre las *Herramientas administrativas*, aunque también se puede acceder a través del comando *eventvwr.msc*

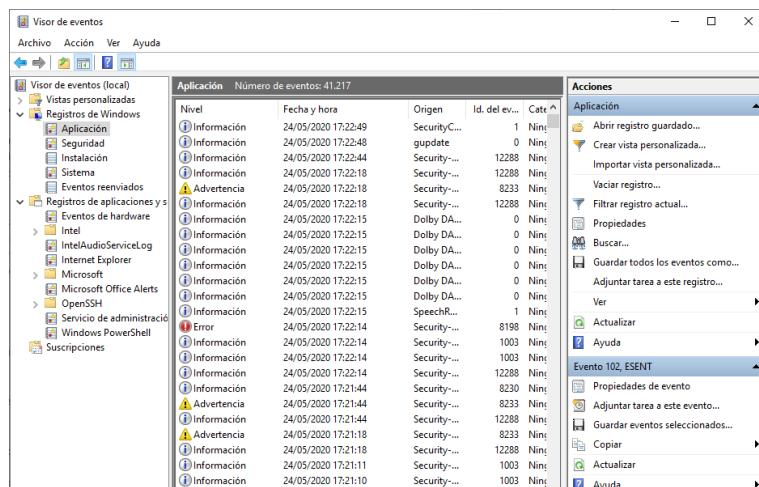


Fig. 21. Visor de eventos.

Los eventos del sistema se encuentran almacenados en el apartado *Registros de Windows*, y están organizados en:

- **Aplicaciones.** Recoge todos los sucesos relacionados con las aplicaciones del sistema.
- **Seguridad.** Son eventos de auditorías. Incluye inicios de sesión o acceso a carpetas o archivos en caso de estar activado su registro.
- **Instalación.** Muestra eventos relacionados con la instalación o actualización de software.

- **Sistema.** Engloba aquellos eventos relacionados directamente con el sistema operativo.
- **Eventos reenviados.** Incluye los eventos registrados de equipos remotos.

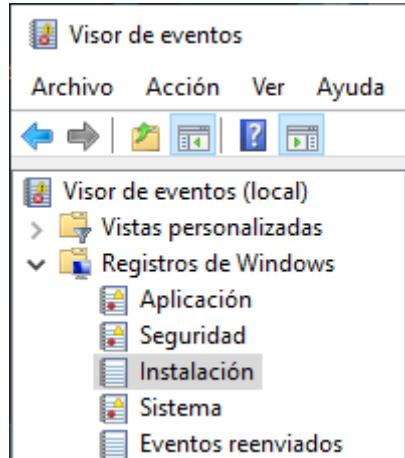


Fig. 22. Registros de Windows en el Visor de eventos.

5.1. Explotación del visor de eventos

Como hemos visto en el apartado anterior, la mayoría de sucesos o *logs* del sistema operativo están almacenados en *Registros de Windows* del *Visor de eventos*. Cada uno de los eventos está identificado con un ID.

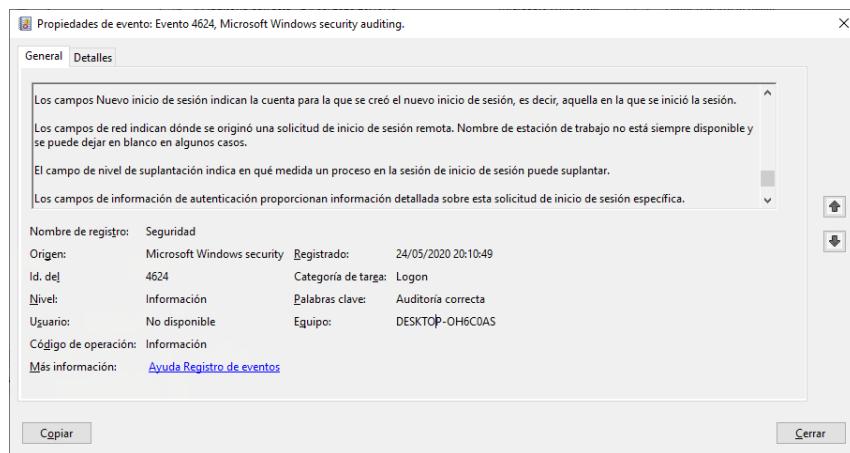


Fig. 23: Evento con ID 4624 de inicio de sesión.

El *Visor de eventos* almacena miles de *logs* de sucesos, lo que hace prácticamente inviable revisar cada uno de ellos. Pero sí es posible encontrar eventos concretos; para ello, hay que hacer clic en el panel derecho, en *Filtrar registro actual*.

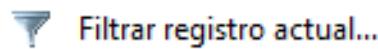


Fig. 24. Filtro para localizar eventos concretos.

Este permite filtrar eventos por horas o días, por el nivel del evento (crítico, advertencia, detallado, error o información), por ID, por palabras clave, por usuario o por equipo.

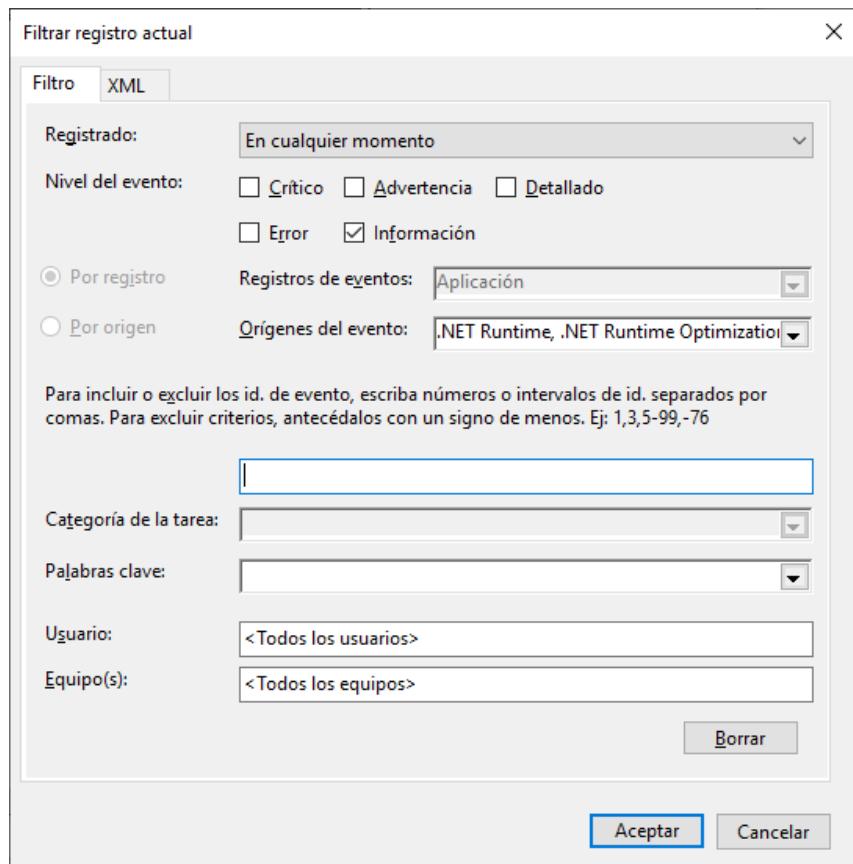


Fig. 25. Filtrar eventos.

Algunos ID de eventos del sistema son los siguientes:

ID	Descripción
44	Descarga de actualización de Windows Update
4608	Windows se está iniciando
4609	Windows se está apagando
4624	Se inició sesión correctamente con una cuenta
4625	No se pudo iniciar sesión con una cuenta
4726	Se eliminó una cuenta de usuario
4778	Inicio de sesión por Escritorio remoto
4779	Finalización de sesión de Escritorio remoto
4800	Se bloqueó una estación de trabajo
4950	Se cambió una configuración del Firewall de Windows
7034	Servicio caído de forma inesperada

Tabla. 1. Ejemplos de ID de eventos del sistema.

/ 6. Caso práctico 1: “Detener servicios al inicio de Windows”

Planteamiento: Alberto es administrador de sistemas de su empresa.

Observa que, cuando se conecta a uno de los servidores, se muestra siempre un mensaje de actualización del software Adobe Acrobat.

El problema reside en que no puede actualizar la versión de Adobe Acrobat, ya que otro software necesita la versión que tiene actualmente para funcionar correctamente.

Nudo: ¿Cómo puede Alberto eliminar el mensaje de actualización cada vez que inicia el servidor?

Desenlace: Alberto debe ir a *Servicios* y, entre el listado de servicios, buscar los correspondientes a Adobe Acrobat, en concreto Adobe Acrobat Update Services.

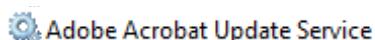


Fig. 26. Servicio de actualización de Adobe Acrobat.

Posteriormente, debe hacer doble clic sobre él y en el Tipo de inicio cambiar de Automático a **Manual o Deshabilitado**.

Lo podemos ver en la siguiente imagen:

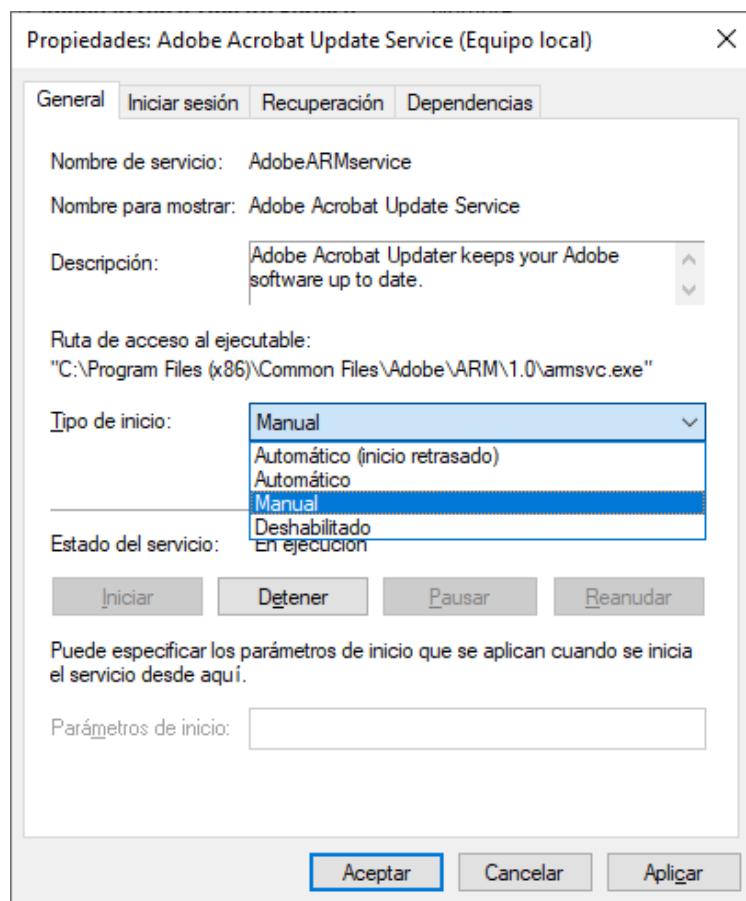


Fig. 27. Cambiar el tipo de inicio de un servicio a manual.

/ 7. Caso práctico 2: “Rendimiento de los componentes del servidor”

Planteamiento: María es la encarga de dar el soporte informático en su empresa.

Dispone de un servidor en el que presta múltiples servicios como DHCP, archivos, impresoras, aplicaciones, etc. Y ha detectado que su servidor se ralentiza constantemente.

Nudo: ¿Cómo puede saber María qué recursos del sistema se saturan o qué aplicaciones o servicios lo provocan? ¿Cómo podría solucionar el problema?

Desenlace: María debe ejecutar el Monitor de recursos. En la pestaña *Información general*, puede visualizar el rendimiento de los principales componentes del servidor.

Al prestar múltiples servicios, seguramente la memoria RAM o CPU se encuentren al límite de su uso.

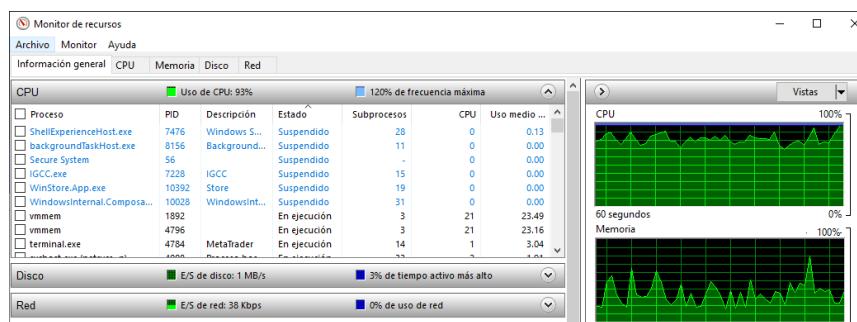


Fig. 28. Monitor de recursos.

En la pestaña CPU, puede observar el consumo que está haciendo cada proceso y servicio y ordenarlos por mayor uso:



Fig. 29. Estado de la CPU en el monitor de recursos.

En la pestaña Memoria, también puede visualizar la cantidad de memoria asignada a cada proceso.

Después de visualizar el consumo que realizan los servicios y procesos del servidor, deberá valorar si son necesarios, y si no lo fueran, detener o desinstalar la aplicación que invoca los servicios o procesos que saturan el servidor.

Si todos los servicios y procesos son necesarios, debería ampliar los recursos de hardware del servidor que ha observado que se llegan al 100%, así como los que estén próximos, para evitar futuros problemas similares.

/ 8. Resumen y resolución del caso práctico de la unidad

Durante este tema, hemos visto que un **servicio** es una aplicación o conjunto de aplicaciones que ejecuta un sistema operativo para ofrecer una determinada funcionalidad al resto de objetos del sistema o dominio. Mientras que un **proceso** es un programa que está en ejecución como instancia de una aplicación, una aplicación determinada puede necesitar varios procesos ejecutándose simultáneamente.

A través del **proceso de monitorización**, se recoge información sobre la actividad del sistema. Algunas herramientas de monitorización del sistema son el Monitor de rendimiento, el **Monitor de recursos** o el **Monitor de confiabilidad**.

Además, hemos aprendido que un evento o suceso es un acontecimiento del sistema o de un *software*. Dichos sucesos son almacenados en **logs**, archivos que contienen los registros ocurridos en un determinado espacio de tiempo.

Resolución del caso práctico de la unidad

Para averiguar quién puede haber instalado el software en el equipo de la empresa de José, este sabe que todos los sucesos del sistema están registrados en el Visor de eventos. Deberá abrirlo desde las *Herramientas administrativas*.

Una vez abierto, hay que filtrar por el ID correspondiente a la instalación de software: 11707. Para ello, debe hacer clic en *Filtrar registro actual*.

Una vez filtrado, abrirá los últimos *logs*, los cuales mostrarán el *software* instalado, el día y hora y el usuario que realizó la instalación, como se muestra en la siguiente imagen:

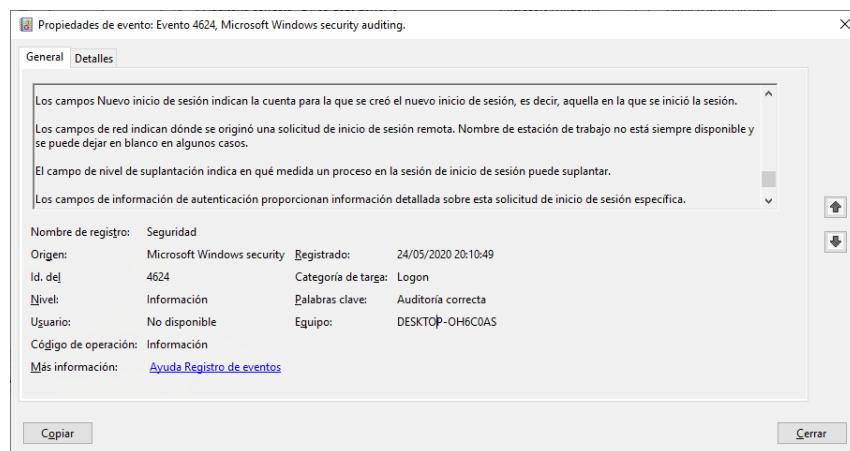


Fig. 30. Log 11707 de instalación del software PDFSam.