Unidad 7

Supervisión del rendimiento del sistema

Implantación de sistemas operativos

Índice

Introducción

Los sistemas Windows llevan muchas herramientas nativas para diferentes tareas administrativas como hemos ido viendo en unidades anteriores.

Estas herramientas, consumen una serie de recursos a los que debemos de estar atentos para en caso de necesitar más adquirirlos.

Aunque en un principio, todos pensaríamos en el Administrador de tareas, a lo largo de la unidad veremos que el sistema tiene incorporadas otras herramientas que nos ayudarán a vigilar y monitorizar el rendimiento del sistema.

Pasaremos por el visor de eventos, principal modo de avistar los registros más importantes del sistema, pasaremos por el Monitor de rendimiento y sabremos como crear un gráfico propio nuestro.

Por último, veremos que hay un comando específico para identificar registros.

Al finalizar esta unidad

- Sabremos gestionar los procesos utilizados por los distintos servicios del sistema.
- Conoceremos lo que es el visor de eventos y los distintos registros que lo componen.
- Conoceremos distintas herramientas para el seguimiento y control del sistema operativo.

7.1. El administrador de tareas

El **Administrador de tareas** es una herramienta nativa de los sistemas Windows que usamos para ver distintas características del sistema y poder gestionar varios procesos internos del sistema.

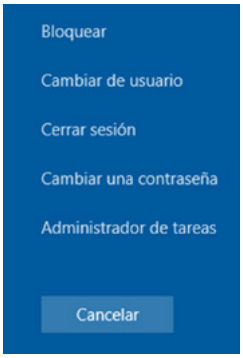

Imagen 1. Administrador de tareas 1

Para manejar el administrador de tareas, seguimos los siguientes pasos:

1. Lo primero que hacemos es pulsar la combinación de teclas Ctrl+Alt+Supr.
2. Nos aparecerá una pantalla con varias opciones, seleccionamos la última, Administrador de tareas.
3. Se nos abre una ventana como la que vemos a continuación, y en la esquina inferior izquierda seleccionamos Más detalles.

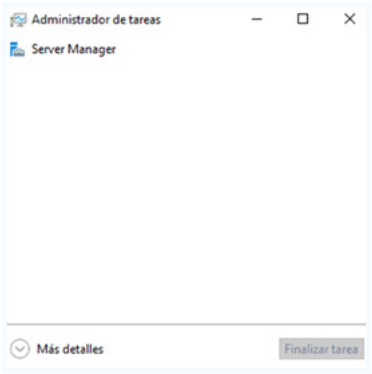

Imagen 2. Administrador de tareas 2

4. La primera pestaña es la de Procesos, que muestra la información acerca de los procesos que se encuentran en el sistema en ejecución en el momento, mostrando su carga de memoria y de CPU correspondiente. Se pueden ordenar los procesos por nombre, CPU, y memoria.

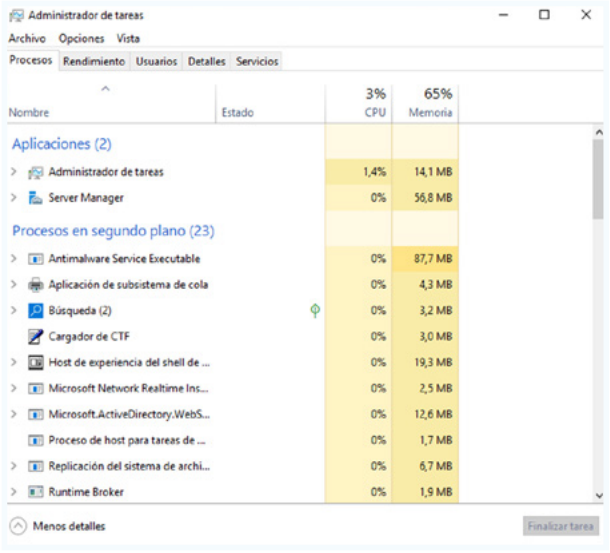

Imagen 3. Administrador de tareas 3

5. Si queremos finalizar un proceso, debemos de hacer clic derecho en este.

6. Se nos muestran una serie de opciones y debemos de seleccionar la segunda, Finalizar tarea.

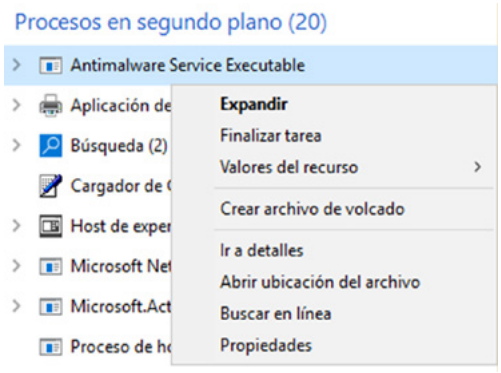

Imagen 4. Administrador de tareas 4

7. La siguiente pestaña que vamos a ver es la de Rendimiento, donde se nos muestra a modo de gráfica, los principales recursos que tenemos disponibles en el sistema y cuál es su carga actual. Se muestran a modo de gráficos.

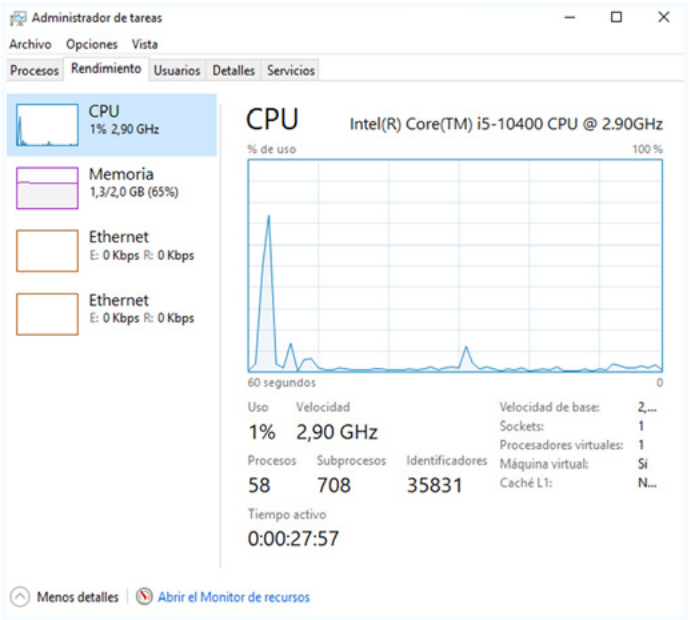

Imagen 5. Administrador de tareas 5

8. En esta misma pestaña, en la parte inferior, podríamos entrar al Monitor de recursos.

9. La pestaña Usuarios nos muestra los usuarios logueados en el sistema y cuáles son sus procesos en ejecución. Tenemos en la esquina inferior derecha la opción Desconectar en caso de querer desconectar a alguno de los usuarios, lógicamente a nosotros no podemos porque estamos en ejecución.

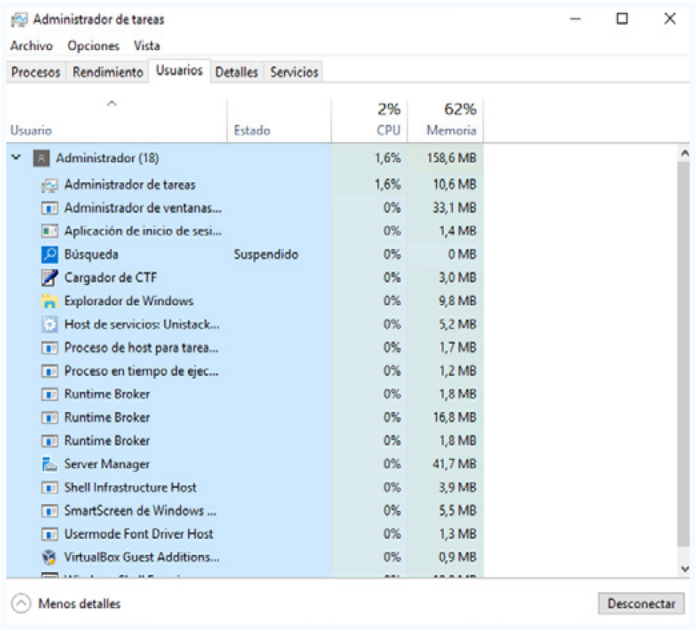

Imagen 6. Administrador de tareas 6

10. En la pestaña de Detalles tenemos los procesos, o programas en ejecución como archivos del sistema, no suele usarse, aunque nos da algunos detalles más específicos como la ruta de ejecución.

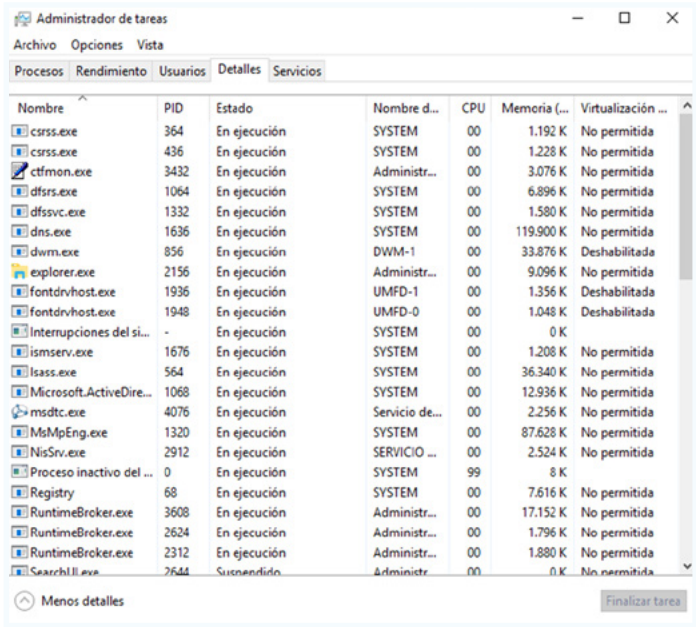

Imagen 7. Administrador de tareas 7

11. La última de las pestañas es la de Servicios, donde se encuentran reflejados todos los servicios del sistema, ya estén parados o en ejecución.

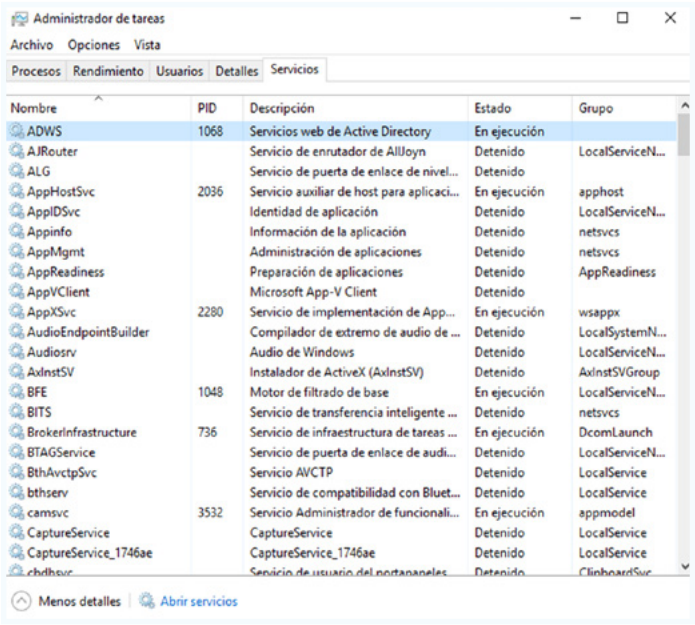

Imagen 8. Administrador de tareas 8

12. Por último, en esta pestaña podemos hacer clic derecho a algún servicio y tenemos las opciones de Iniciar, Detener o Reiniciar, para seleccionar la que queramos aplicar dependiendo de la situación.

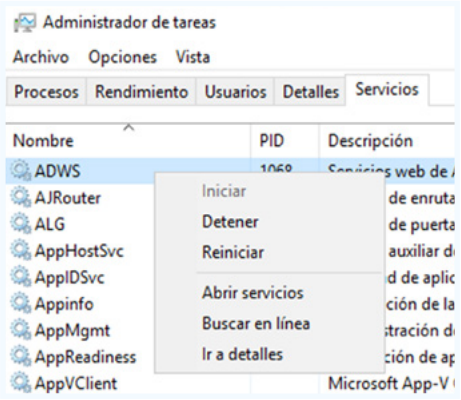

Imagen 9. Administrador de tareas 9

7.2. El visor de eventos

El **visor de eventos** de Windows, aunque veremos algunas aplicaciones suyas en temas posteriores, vamos a ver ahora en que consiste.

Los **eventos** son sucesos ocurridos en el sistema con cierta importancia o incluso una notificación que manda notificaciones al usuario del equipo.

Para abrir el visor de eventos hacemos lo siguiente:

1. Nos vamos a inicio y buscamos Visor de eventos.
2. Nos sale una herramienta como la siguiente:

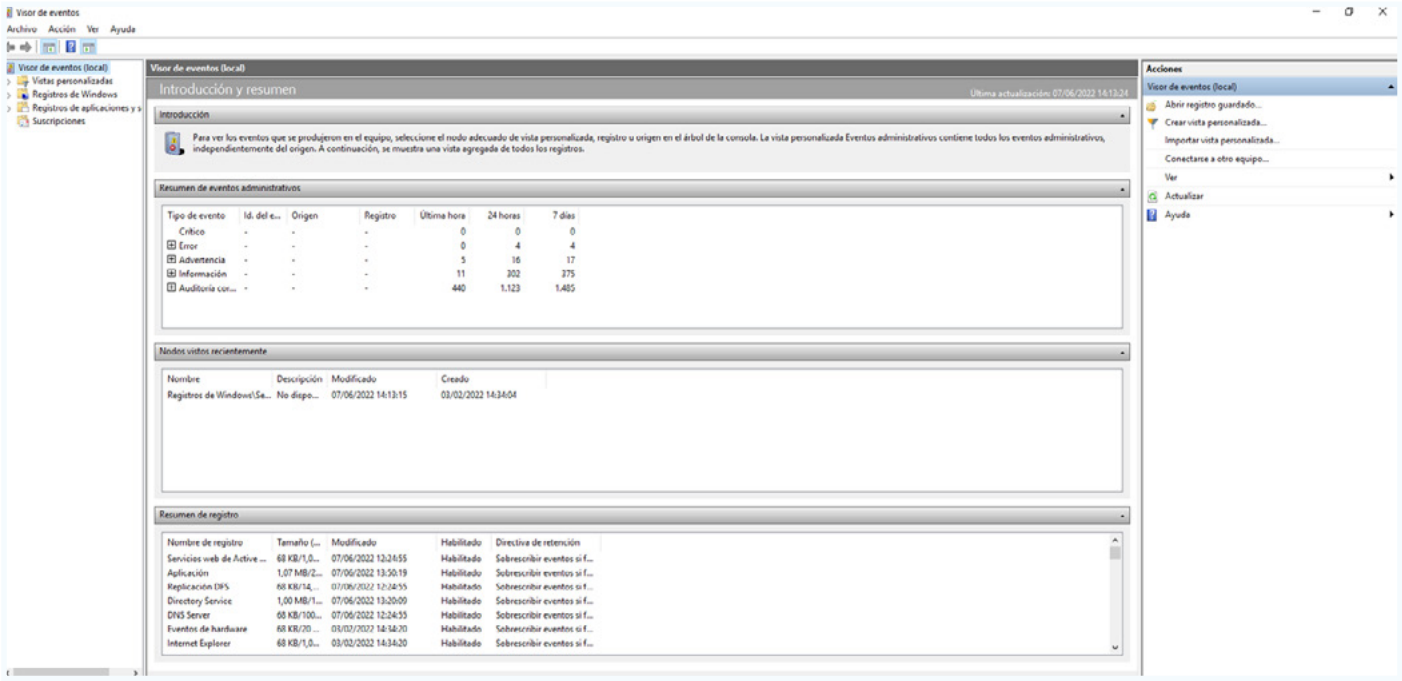

Imagen 10. Visor de eventos 1

Dentro de esa herramienta, tenemos una serie de tipos de eventos que vamos a ver ahora como funcionan:

- **Vistas personalizadas.** Son vistas de filtros que nosotros hemos creado previamente, para mostrar los filtros que hemos realizado para ver los registros que necesitamos en ese momento.

Imagen 11. Visor de eventos 2

- **Registros de Windows.** Se muestran todos los registros referentes al mismo sistema y las acciones ocurridas en el sistema.
  - Aplicación. Nos muestra los eventos que generan las aplicaciones o los programas del sistema.
  - Seguridad. Nos muestra los eventos que generan cuando hacemos mediante auditorías un seguimiento de la seguridad del sistema o si se encuentra un fallo en la seguridad de este.
  - Instalación. Nos muestra que eventos se han generado a través de la instalación del sistema o de componentes de este.
  - Sistema. Nos muestra los eventos generados por los componentes del sistema.
  - Eventos reenviados. Nos muestra aquí los eventos que han generado equipos remotos conectados al nuestro.
- **Registros de aplicaciones y servicios.** Almacenamos en dicha categoría los eventos de una aplicación o componente único, sin tener en cuenta todos lo del sistema. Dentro de estos, tenemos varios tipos:
  - Directory Service. Para los sucesos acaecidos en el AD.
  - DNS server. Para los sucesos que se producen en el servidor de DNS.
  - Eventos de hardware. Para los sucesos específicos de componentes hardware.
  - Microsoft. Para los sucesos de aplicaciones de Microsoft que estén en el sistema.
  - OpenSSH. Mostramos los eventos relacionados con SSH, y más específicamente, con OpenSSH.
  - Replicación DFS.
  - Servicio de administración de claves.
  - Servicios web de Active Directory. Para los servicios cloud del Directorio Activo.
  - Windows PowerShell. Almacenamos los eventos relacionados con esta herramienta.
- **Suscripciones.** Para recopilar eventos de varios equipos remotos que han sido administrados remotamente con alguna herramienta o aplicación.

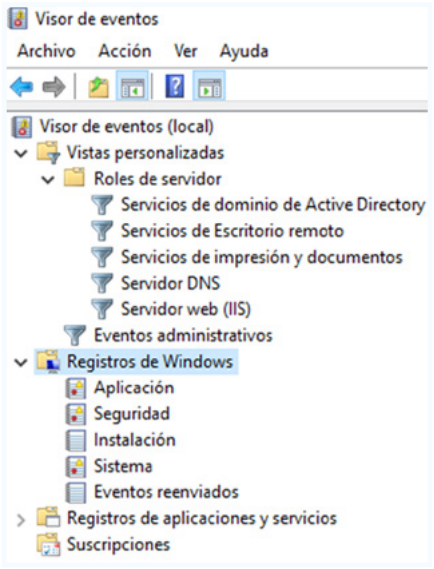

Imagen 12. Visor de eventos 3

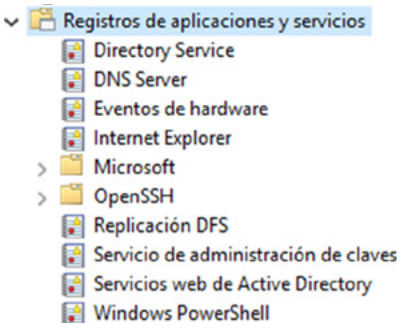

Imagen 13. Visor de eventos 4

Si lo que queremos es ver un evento, lo seleccionamos, y en la parte inferior vemos que aparece un cuadro con información como el siguiente:

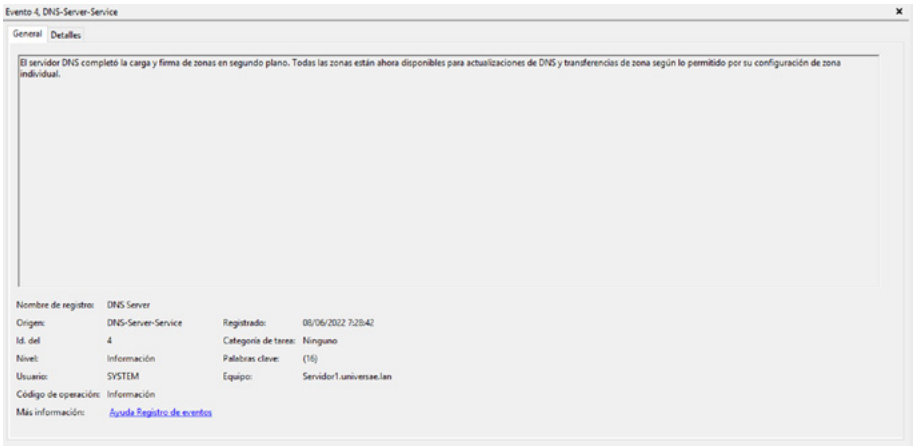

Imagen 14. Visor de eventos 5

Tenemos varios tipos de eventos en el sistema, que son los siguientes:

- **Críticos.** El error no se puede recuperar de manera automática, es decir, hay que sustituir la aplicación o componente que causó dicho evento.
- **Error.** El problema que relata el evento es bastante importante y puede hacer que el sistema se vea implicado por el fallo de algún componente o aplicación.
- **Advertencia.** Se nos indica que ha sucedido algo a lo que debemos de prestar atención por posibles problemas futuros pero que ahora mismo no causa problemas en el sistema.

Imagen 15. Advertencia

- **Información.** Nos escribe una parte del funcionamiento mediante el evento, pero todo ha ido de manera correcta.

Imagen 16. Información

- **Auditoría correcta.** Se ha realizado una auditoría y se ha notificado que no ha habido fallos en la seguridad.

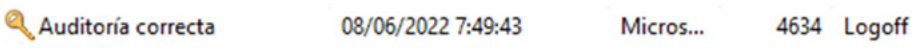

Imagen 17. Auditoría correcta

- **Error de auditoría.** Se ha realizado una auditoría y se ha notificado que ha habido algún fallo en la seguridad del sistema.

Por último, hay muchísimas acciones que realizar con los registros, como moverlos, borrarlos, cambiarlos, modificarlos, etc. Pero esto, no lo vamos a ver ya que no es necesario en casi su totalidad para el día a día de un Administrador de Sistemas.

7.3. El monitor de rendimiento

El **Monitor de Rendimiento** de Windows es una herramienta nativa gráfica del sistema que usamos para visualizar en tiempo real, los datos sobre el rendimiento del sistema basándose en los archivos de registro.

Si queremos abrir el monitor de rendimiento y trabajar con él, debemos de hacer lo siguiente:

1. 1. Seguimos los siguientes pasos:
   a. Inicio
   b. Herramientas administrativas
   c. Monitor de rendimiento

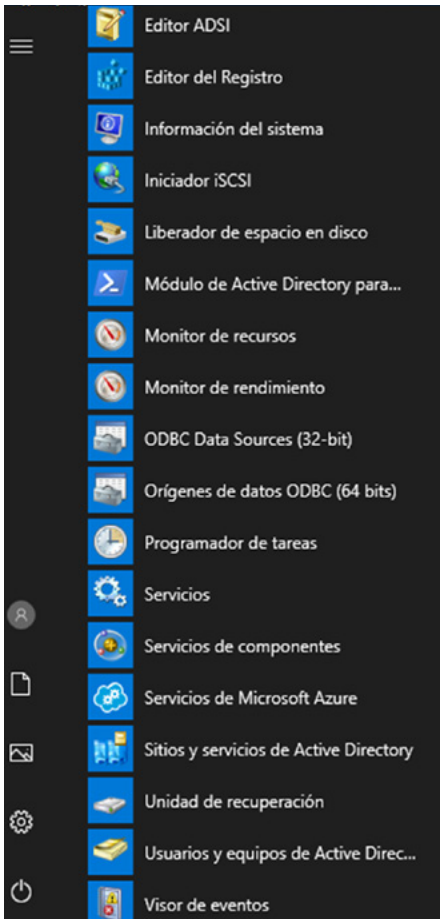

Imagen 18. Monitor de rendimiento 1

2. Se nos abre una venta como la siguiente, donde podemos ver, que en la izquierda tenemos una breve explicación sobre el funcionamiento de la herramienta y justo debajo un resumen de nuestro sistema.

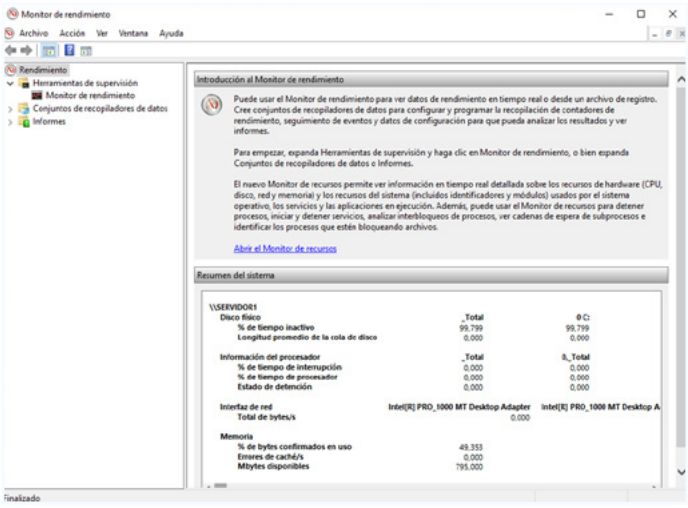

Imagen 19. Monitor de rendimiento 2

3. Si nos vamos al apartado Monitor de rendimiento, vemos que nos aparecerá el gráfico del rendimiento del sistema en cuanto a uso de procesador se refiere. Aquí podemos fijarnos en que debajo aparecen una serie de parámetros:
   a. **Último.** Último valor leído.
   b. **Promedio.** Media de todos los valores leídos.
   c. **Mínimo.** Menor valor leído.
   d. **Máximo.** Mayor valor leído.
   e. **Duración.** Tiempo que tarda el monitor en crear un gráfico completo en pantalla.

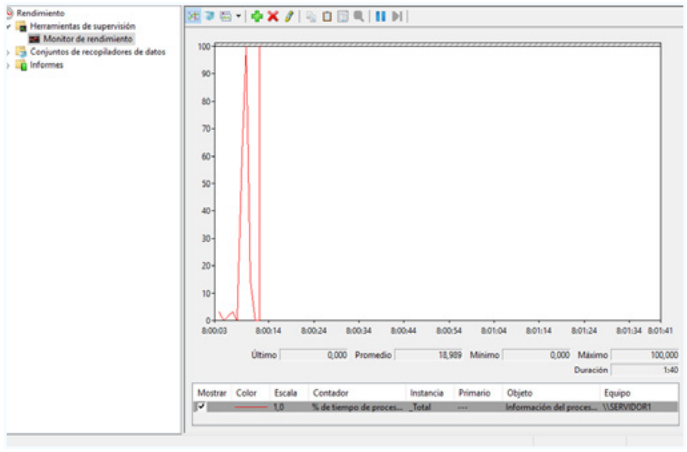

Imagen 20. Monitor de rendimiento 3

7.3.1. Como crear un gráfico nuevo en Windows Server

Dentro del Monitor de Rendimiento de Windows, nosotros podemos crear y gestionar nuestros propios gráficos para recoger la información que creemos oportuna y necesaria.

Para eso, seguimos el siguiente proceso:

1. Abrimos el Monitor de Rendimiento.
2. En la parte derecha, zona superior, tenemos una serie de iconos, clicamos en la cruz roja que nos borrará el monitor actual.

Imagen 21. Gráficos 1

3. Como podemos ver, ahora vemos que no se está registrando nada:

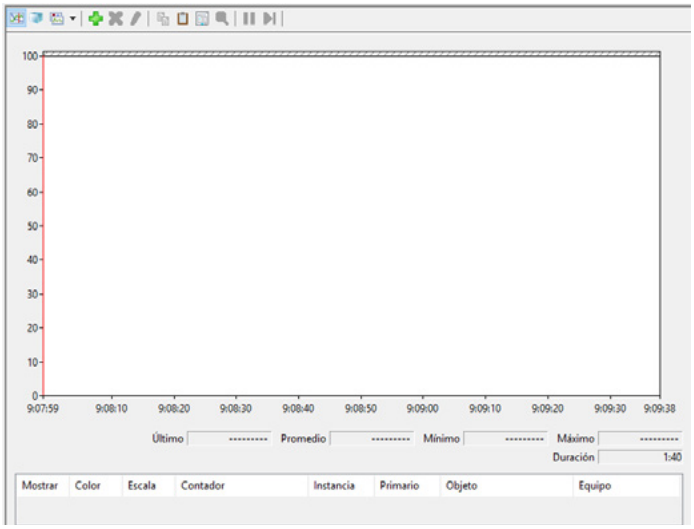

Imagen 22. Gráficos 2

4. Ahora, pulsamos sobre el signo + que tenemos en verde, que es para agregar un nuevo gráfico, y nos saldrá una venta de selección:
5. En esta ventana nos tenemos que fijar primero en la parte de la izquierda:
   a. En Seleccionar contadores del equipo, seleccionamos donde queremos que se lleve a cabo el registro y debajo seleccionamos que recursos del sistema queremos monitorizar.
   b. Cuando lo tengamos, pulsamos en Agregar >>.
   c. Debajo del todo, podemos seleccionar Mostrar descripción y debajo se nos mostrará una breve descripción del recurso a monitorizar.

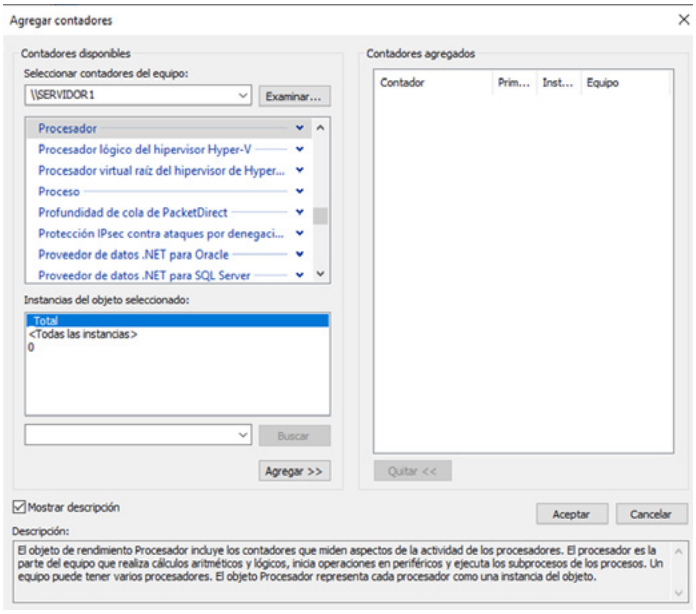

Imagen 23. Gráficos 3

6. Si hemos agregado el rendimiento que queremos monitorizar, se pasa al cuadro de la derecha, donde nos aparece y podríamos quitarlo, con la opción de más abajo.

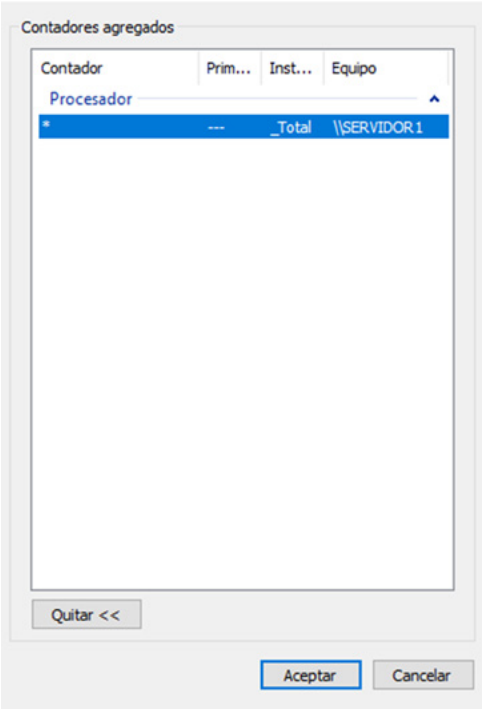

Imagen 24. Gráficos 4

7. Podemos ver ahora como se nos muestra el nuevo servicio de monitorización, con los códigos de líneas para cada aspecto abajo indicados.

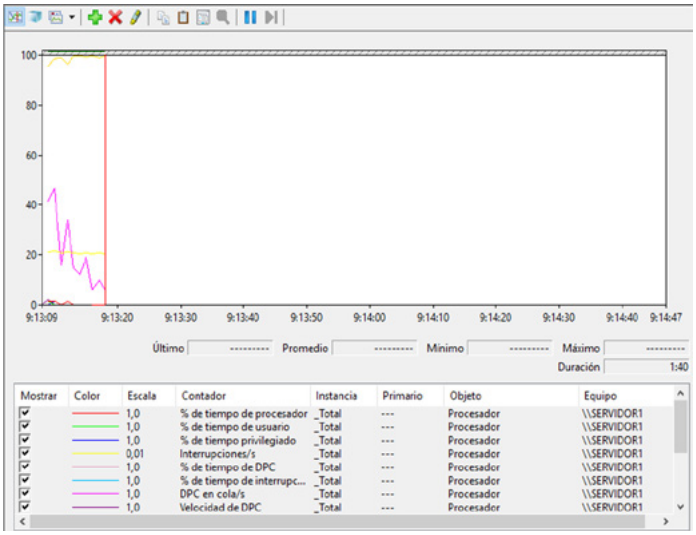

Imagen 25. Gráficos 5

8. Si hacemos clic derecho en alguno de los controladores de abajo, podemos seleccionar distintas opciones:

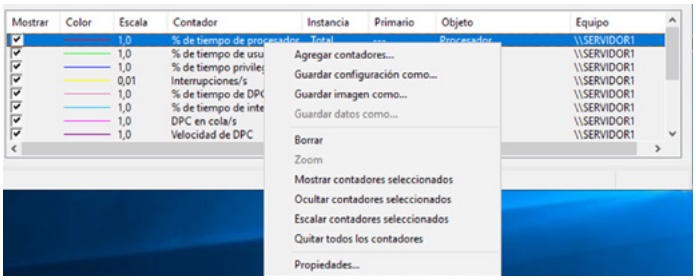

Imagen 26. Gráficos 6

a. **Propiedades.** Nos permiten realizar cambios sobre el diseño del contador en el gráfico.

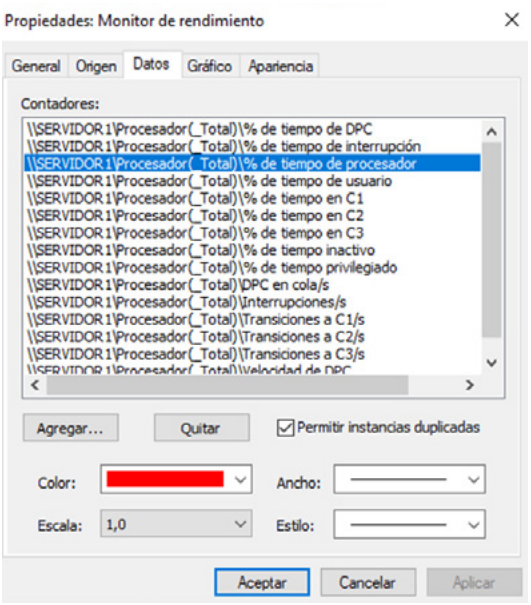

Imagen 27. Gráficos 7

b. Guardar configuración como:

Nos aparecerá una ventana para guardar la información como página web o como informe, si lo guardamos como página web se verá del siguiente modo:

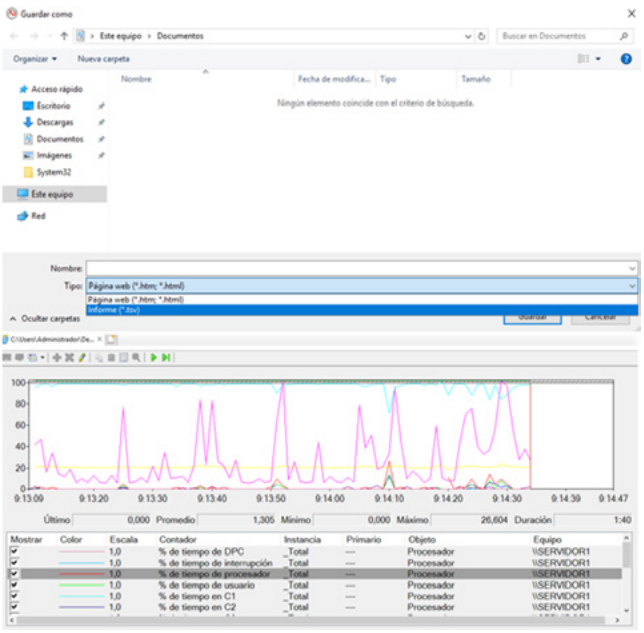

Imagen 28. Gráficos 8

c. Guardar imagen como...: si elegimos esta opción se guarda automáticamente en formato gif y nos aparecerá del siguiente modo:

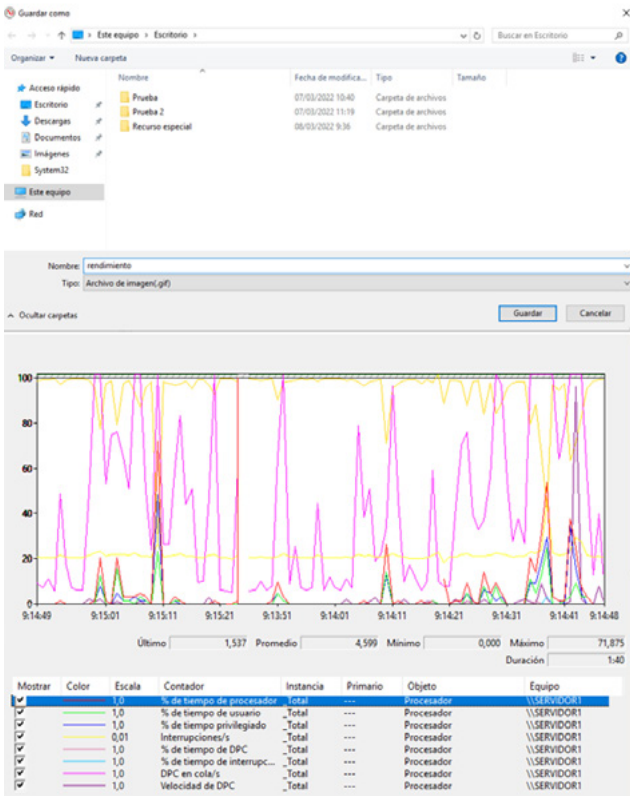

Imagen 29. Gráficos 9

d. Si seleccionamos la opción Quitar todos los contadores, nos aparecerá un mensaje de aviso, si lo aceptamos, veremos que todo desaparece y vuelve al primer estado que vimos anteriormente:

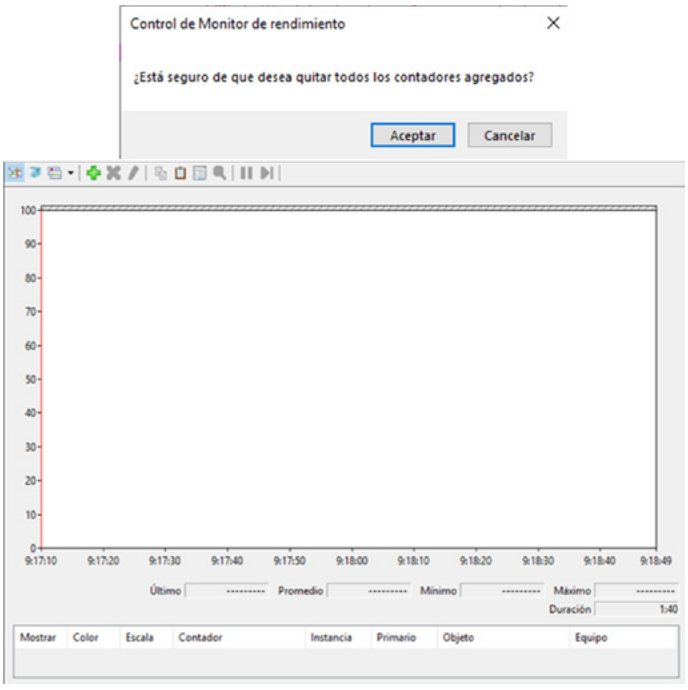

Imagen 30. Gráficos 10

7.4. El comando tracerpt

En Windows, existe el comando **tracerpt** que se usa para el procesamiento de los registros de seguimiento de sucesos o datos en tiempo real a partir del monitor de rendimiento o el Visor de eventos, que le proveerán registros del sistema. Este comando, genera principalmente dos archivos (aunque su formato y nombre se pueden modificar):

- **Dumpfile.xml.** Se trata de un archivo XML donde se refleja información sobre los datos guardados.
- **Summary.txt.** Este archivo se encuentra escrito en texto plano y separado por tabuladores con un resumen del análisis del recurso al que se le ha hecho el seguimiento.

En la siguiente imagen vemos que el comando da error ya que no se le ha introducido ningún archivo de registro.

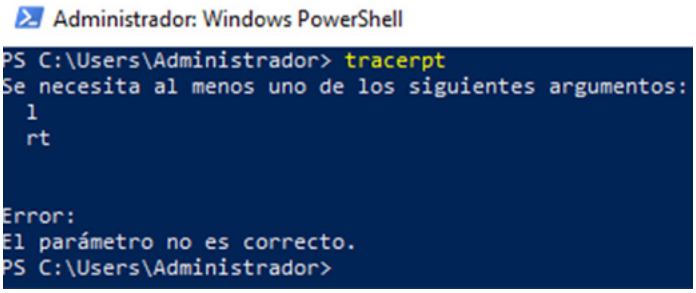

Imagen 31. Comando tracerpt

www.universae.com