

---

## **TEMA 8: RENDIMIENTO Y MONITORIZACIÓN DEL SISTEMA**

---

### **Índice**

1. Introducción .....	2
2. El administrador de tareas .....	2
3. El visor de eventos .....	14
Visor de Eventos.....	18
Registro de Eventos .....	21
4. El monitor de rendimiento.....	24
Contadores Asociados al Rendimiento del Procesador .....	28
Contadores Asociados al Rendimiento de la Memoria RAM .....	30
Contadores Asociados al Rendimiento de los Discos .....	32
5. Registros y alertas de rendimiento .....	34
Conjuntos de Recopiladores de Datos .....	34
Alertas de rendimiento.....	41
6. Monitor de recursos.....	42
7. El monitor de confiabilidad.....	44
8. Informes de almacenamiento .....	46
9. El rastreador de eventos de apagado .....	48
10. Directivas de auditoría.....	51

## 1. Introducción

Una de las funciones del administrador del sistema es velar porque el sistema funcione a un rendimiento óptimo. Algunas veces los usuarios, con motivo o sin él, se quejan de que el sistema “va muy lento”, o de que “Internet no va, le cuesta mucho”. En situaciones así, el administrador debe averiguar qué causas están haciendo que el sistema no funcione como debería, o por el contrario saber si no están justificadas las quejas. Si de verdad el sistema no funciona como debiera habría que plantearse ampliarlo, pero con una base fundamentada.

Otro caso típico de análisis del rendimiento del sistema se plantearía si decidiéramos montar en nuestro servidor un nuevo servicio, por ejemplo de virtualización, de correo electrónico o un servidor web, y no sabemos cómo afectaría al rendimiento del sistema y si sería mejor instalarlo en un nuevo servidor dedicado, con el consiguiente gasto.

En estas situaciones se hacen necesarios los análisis del rendimiento, con los cuales podemos medir de manera objetiva los parámetros del sistema relativos a la velocidad, ocupación de la CPU, memoria utilizada, velocidad y uso del disco, de la tarjeta de red, etc. En definitiva, analizar la carga del sistema y determinar si está excesivamente cargado o por el contrario está infrautilizado.

En este tema veremos las herramientas que proporciona el SO Windows para analizar todo esto, pero también qué herramientas utiliza para comunicarnos los posibles errores, avisos, etc., y poder así asegurar el buen funcionamiento del sistema.

Estudiaremos también en este tema un apartado que tiene que ver más con la seguridad que con el rendimiento. Es el dedicado a las directivas de auditoría, que nos ayudarán a monitorizar los accesos (deseados o no) a los recursos del sistema.

## 2. El administrador de tareas

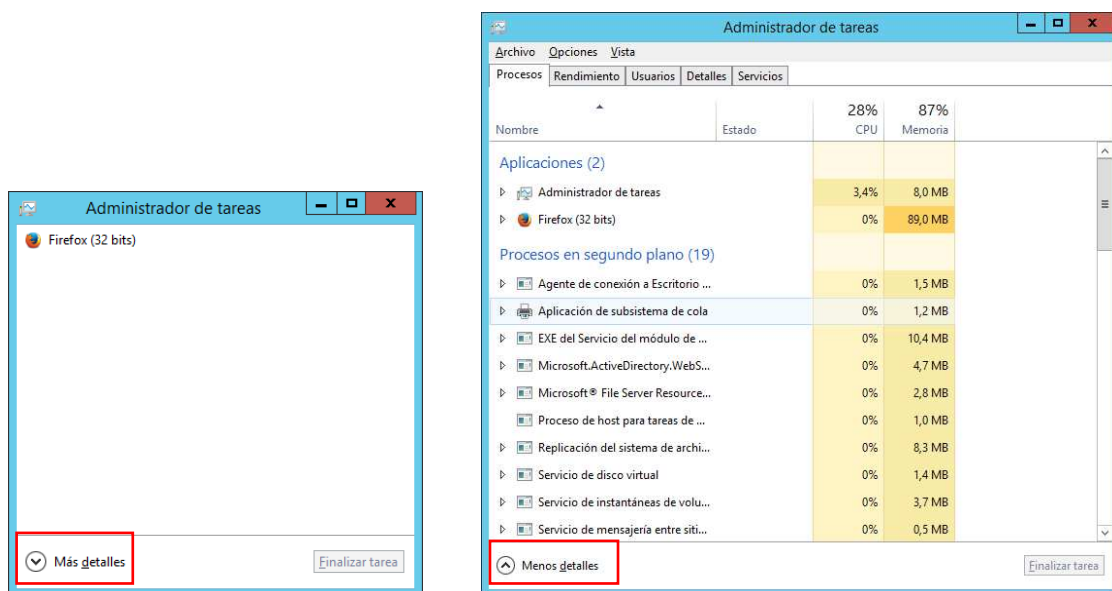
La utilidad básica para medir el rendimiento del sistema, y quizás la primera en utilizarse cuando detectamos que el sistema no funciona correctamente, es el **administrador de tareas**. El administrador de tareas (**taskmgr**) proporciona

información acerca de los programas y procesos que se están ejecutando en el equipo, pero también muestra las medidas de rendimiento utilizadas normalmente para los procesos.

Se puede utilizar para supervisar los indicadores principales del rendimiento del equipo, para ver el estado de los programas que se están ejecutando y terminar programas que han dejado de responder y también puede evaluar la actividad de los procesos en ejecución con hasta quince parámetros y ver gráficos y datos acerca de la utilización de la CPU y de la memoria. Además, si estamos conectados a una red, se puede ver el estado de la red y su funcionamiento.

Si hay varios usuarios conectados al equipo, se puede ver quiénes están conectados y en qué están trabajando, y enviarles un mensaje.

Para acceder al administrador de tareas hay que pulsar **ctrl+alt+spr** o con el botón derecho del ratón, sobre la barra de tareas → **Administrador de tareas**. Dependiendo de la opción **Mostrar más detalles** o **Mostrar menos detalles** tenemos una vista u otra de las tareas.



### Programas que se están ejecutando

La ficha Aplicaciones es accesible si tenemos la opción de **Menos detalles** seleccionada. Muestra el estado de los programas que se están ejecutando en el equipo. En esta ficha

se puede finalizar, cambiar a o iniciar un programa, así como ver las propiedades del fichero ejecutable, abrir la carpeta donde se encuentra o buscar en Internet la aplicación.

### Procesos que se están ejecutando

La ficha Procesos muestra información acerca de los procesos que se están ejecutando en el equipo, tanto aplicaciones como servicios lanzados. Se informa acerca de la utilización de la CPU y de la memoria que está consumiendo y dependiendo del sistema también del disco y la tarjeta de red. Desde aquí se pueden matar procesos (Finalizar tarea) que no responden o ver los detalles del proceso (nos lleva a la pestaña detalles que veremos a continuación). Si se trata de un servicio podemos detenerlo o abrir la consola de servicios.

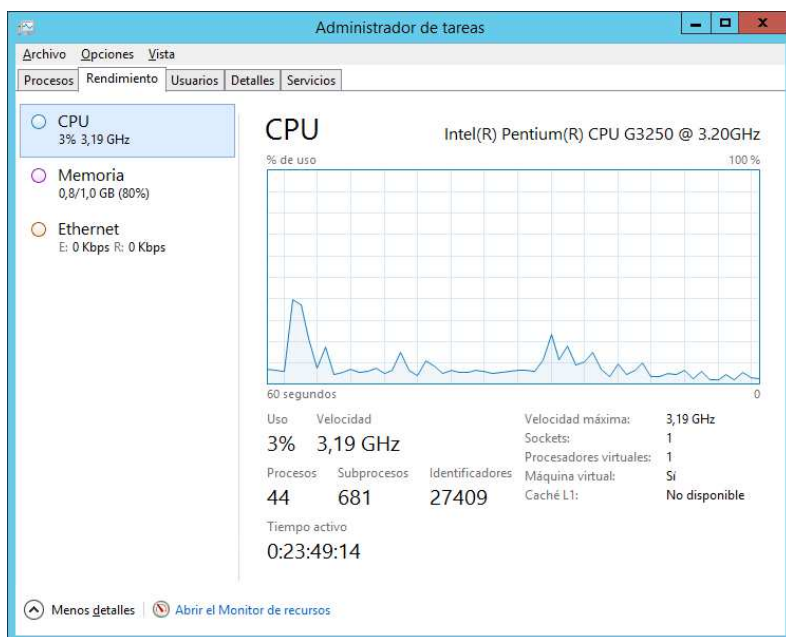
Nombre	Estado	5% CPU	85% Memoria
<b>Aplicaciones (2)</b>			
Administrador de tareas		3,3%	8,7 MB
Firefox (32 bits)		0%	86,6 MB
<b>Procesos en segundo plano (16)</b>			
Agente de conexión a Escritorio remoto		0%	1,5 MB
Agente de conexión a Escritorio remoto			
Aplicación de subsistema de cola		0%	1,2 MB
Cola de impresión			
EXE del Servicio del módulo de copia de seguridad a n...		0%	10,2 MB
Servicio del módulo de copia de seguridad a nivel de...			
Microsoft.ActiveDirectory.WebServices		0%	4,7 MB
Servicios web de Active Directory			
Proceso de host para tareas de Windows		0%	1,9 MB
Replicación del sistema de archivos distribuido		0%	8,4 MB
Replicación DFS			

### Medidas de rendimiento

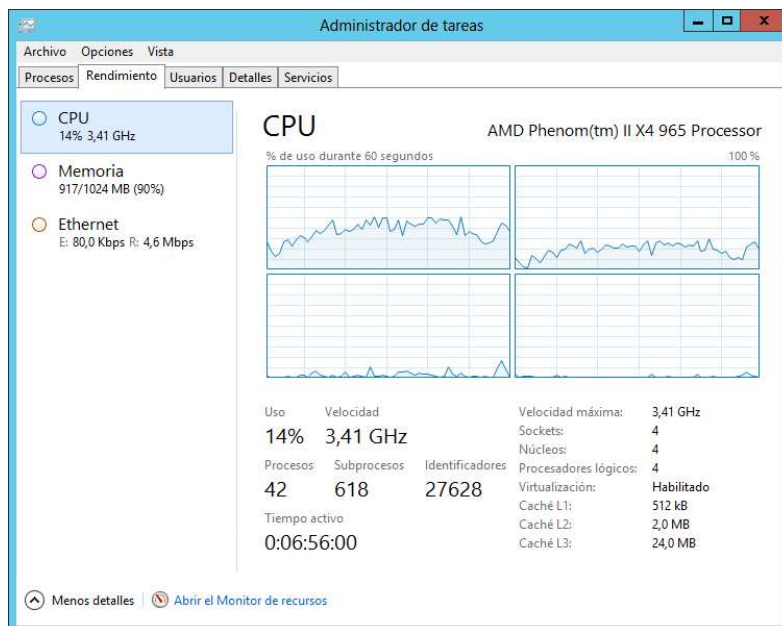
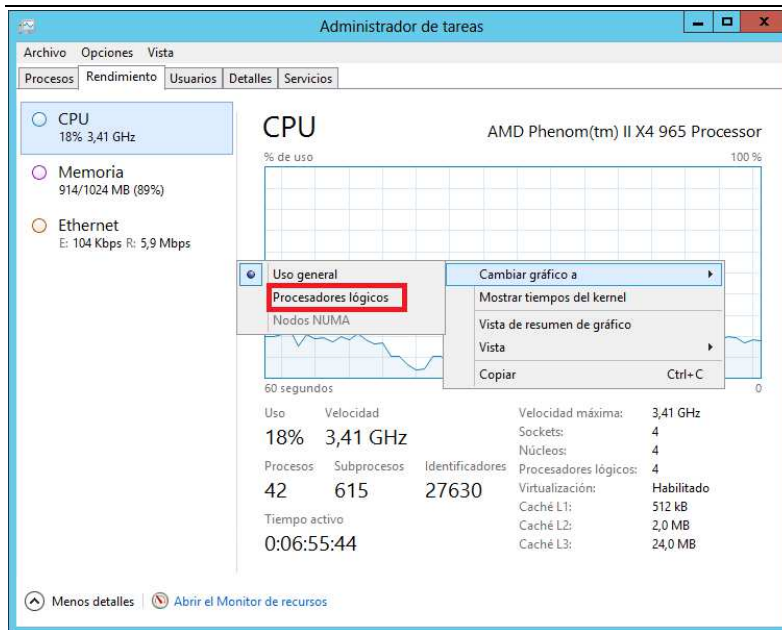
La ficha Rendimiento muestra un esquema dinámico del rendimiento del equipo que incluye:

- Gráficos de utilización de la CPU, la memoria, el disco y la tarjeta de red.

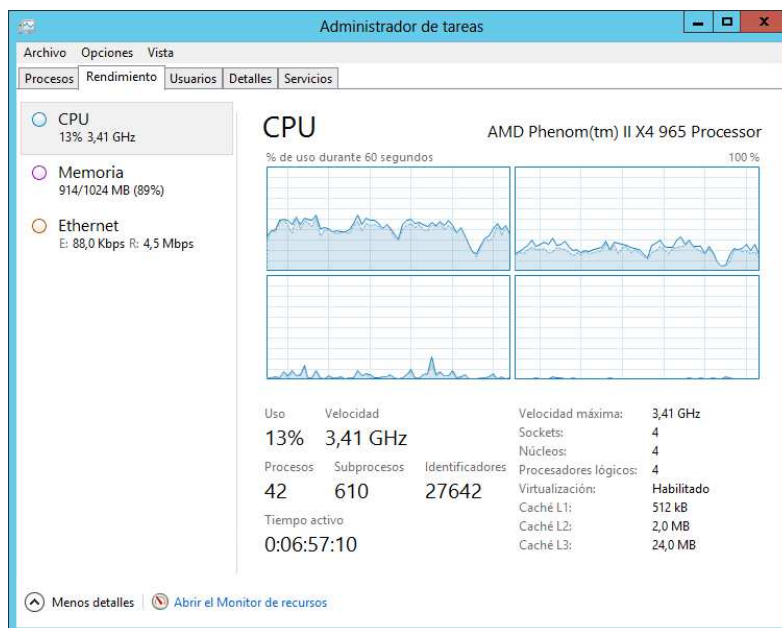
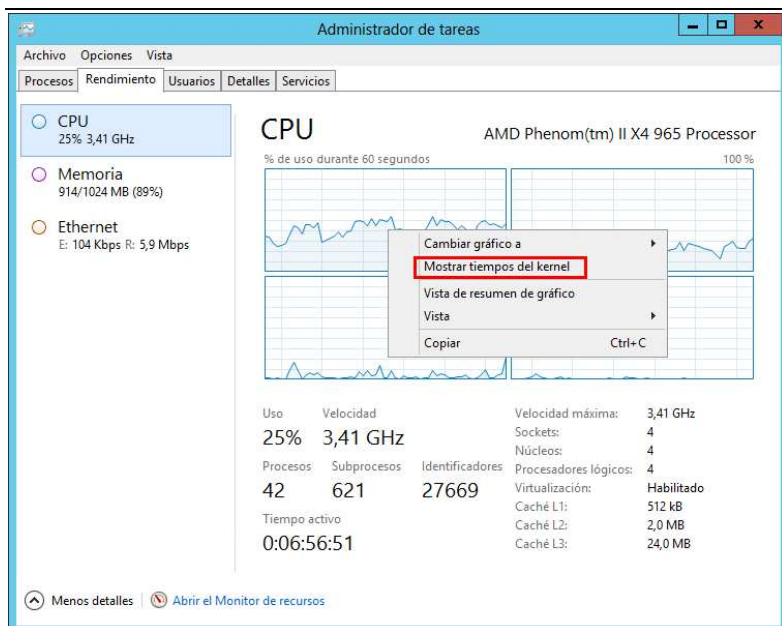
- Número total de identificadores, subprocesos y procesos que se están ejecutando en el equipo.
- Velocidades del procesador, sockets, núcleos, cantidad de memoria caché niveles L1, L2 y L3.
- Número total, en Megabytes, de memoria física, del núcleo y comprometida y velocidad de esta.
- Calidad y disponibilidad de la conexión de red, independientemente de si está conectado a una o varias redes.



Al hacer clic con el botón derecho sobre el gráfico y seleccionar la opción 'Cambiar gráfico a', 'Procesadores lógicos', veremos el porcentaje de utilización de cada núcleo del microprocesador.



Adicionalmente podemos ver qué porcentaje de utilización de los núcleos corresponde únicamente al kernel del sistema operativo. Para ello volveremos a hacer clic con el botón secundario sobre los gráficos de utilización, y seleccionaremos la opción 'Mostrar tiempos de Kernel', obteniendo una serie de gráficos, donde aparece sombreado el porcentaje de uso debido al núcleo, correspondiendo el resto del porcentaje a los procesos en marcha que no forman parte del núcleo del sistema operativo.



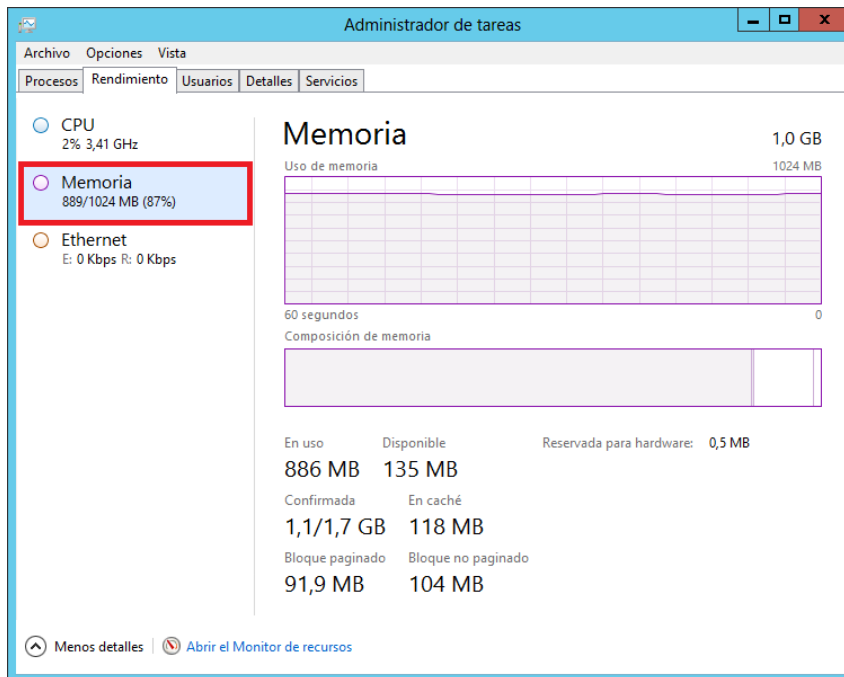
Además de la información gráfica, la cual puede ser interesante porque muestra de una forma resumida un gran volumen de datos a lo largo del tiempo (los últimos 60 segundos), también disponemos en la parte inferior del administrador de tareas de una serie de datos resumen del funcionamiento del microprocesador:

- Procesos: número de instancias de aplicaciones en ejecución.
- Subprocesos: número de hilos de ejecución en uso.
- Identificadores: número de accesos a recursos por parte de los programas.
- Tiempo activo: tiempo en marcha desde que se inició el servidor por última vez.



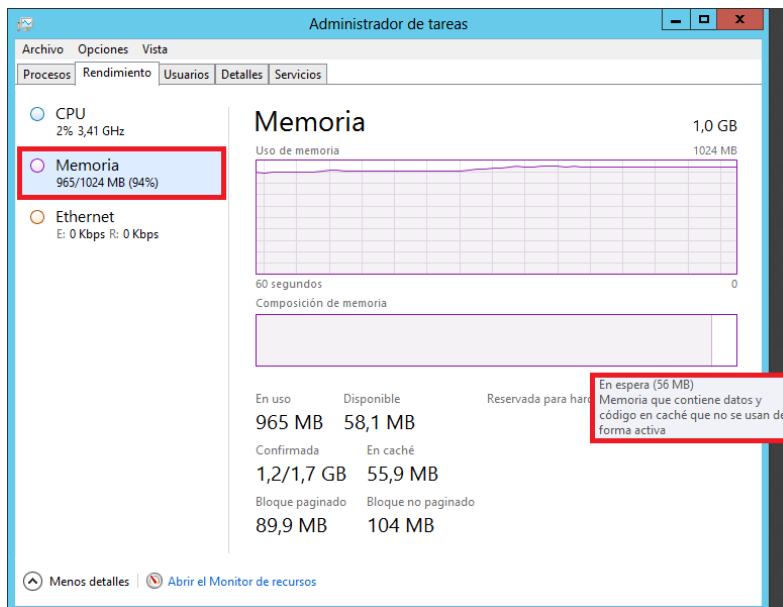
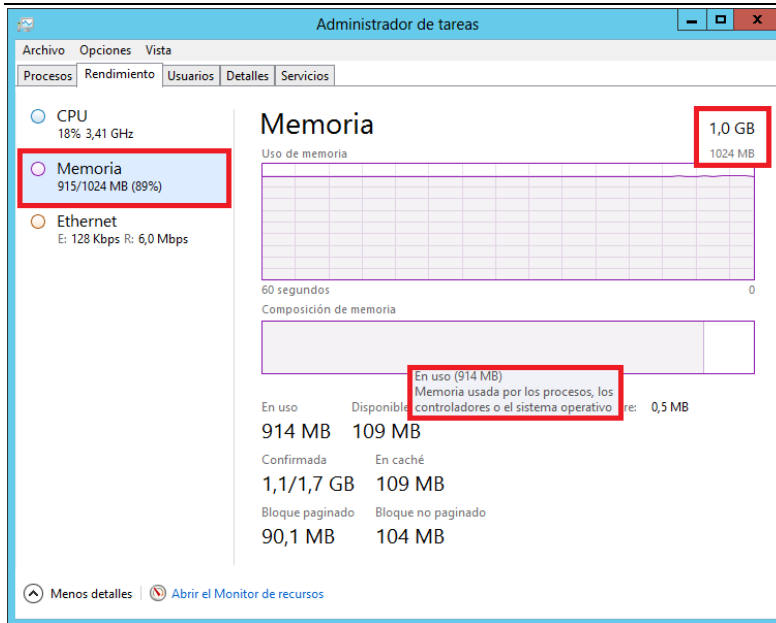
- Velocidad máxima: frecuencia de funcionamiento del microprocesador.
- Sockets: número de microprocesadores.
- Núcleos: número de núcleos del microprocesador.
- Procesadores lógicos: número de procesadores lógicos.
- Virtualización: indica si se encuentra habilitada la virtualización asistida por hardware.
- Cache L<sub>n</sub>: Cantidad de memoria en cada uno de los niveles de la caché de los que consta el microprocesador.

Si en el pestaña 'Rendimiento' del Administrador de tareas, hacemos clic sobre la opción 'Memoria' del panel izquierdo podremos obtener un resumen del rendimiento de la memoria principal del sistema.



Haciendo clic sobre la zona sombreada del histograma 'Composición de memoria', nos aparecerá un resumen de la memoria RAM utilizada, mientras que si hacemos clic en la parte de color blanco nos mostrará la porción de memoria con datos almacenados aunque no estén utilizándose actualmente, pero que en su momento se llevaron a la RAM y se mantienen ahí por si fuera necesaria su utilización, siempre que no sea necesario el espacio que ocupan.





Como se puede comprobar en las imágenes anteriores, la cantidad de RAM **total** del sistema se muestra en la esquina superior derecha. Por otra parte, en la zona inferior se listan los siguientes parámetros estadísticos de la memoria:

- En uso: RAM física utilizada por el equipo
- Disponible: RAM física que no está siendo activamente utilizada.

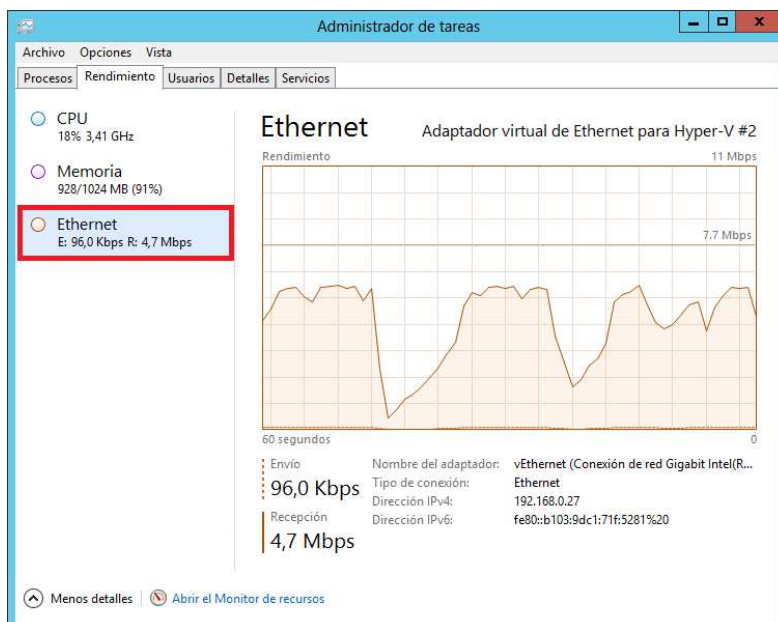
Como norma general **se recomienda que este valor no baje del 5% de la RAM total instalada**. En caso contrario habría que plantear la ampliación de la RAM física.

- Confirmada: se muestran dos valores, el primero corresponde a la memoria virtual utilizada, y el segundo corresponde a la memoria virtual total.

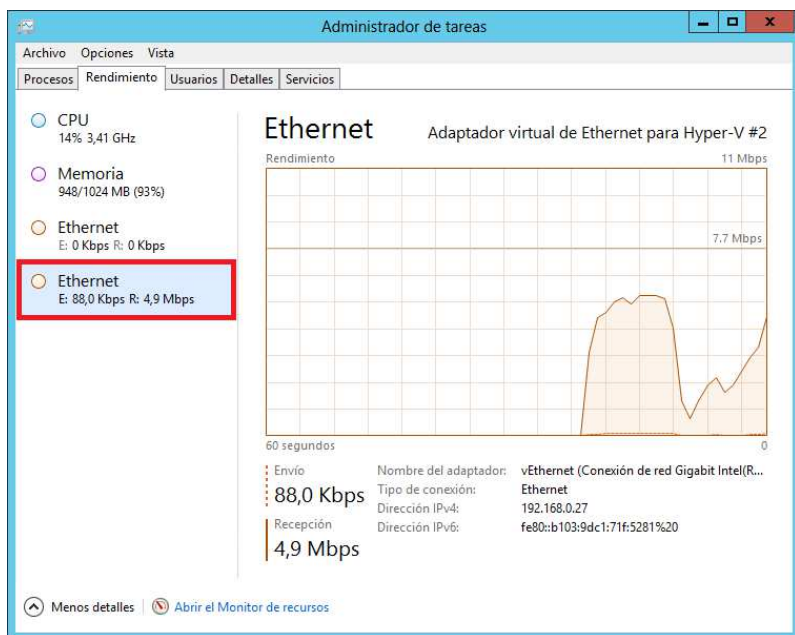
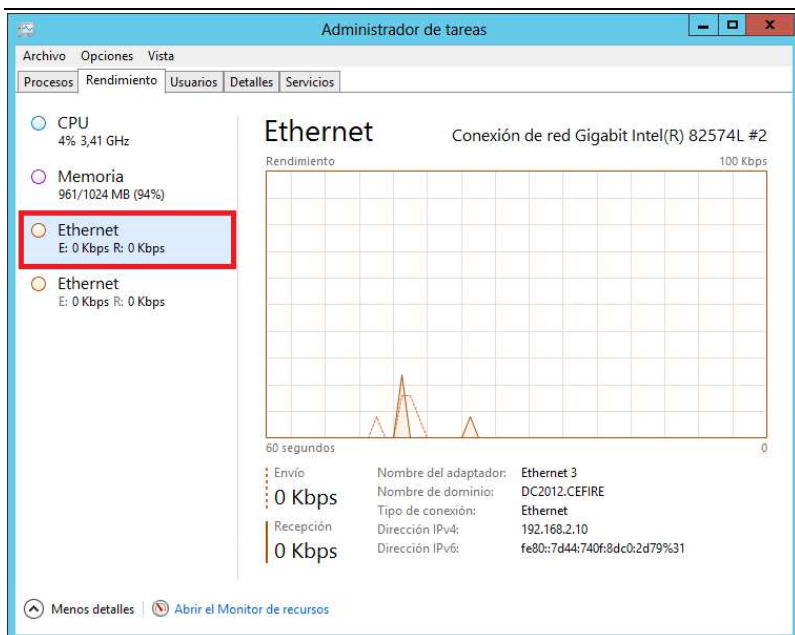
Como norma general, el valor de la **memoria virtual utilizada no debería superar el 90% de la memoria virtual total**, si no, como en el caso anterior, habría que plantear la ampliación de la memoria RAM física.

- En caché: memoria utilizada para la caché del sistema.
- Bloque paginado: memoria del núcleo no crítica.
- Bloque no paginado: memoria del núcleo crítica. Las partes críticas de la memoria deben encontrarse en la RAM, por tanto no se pueden enviar a la memoria virtual, ya que esta ofrece unas velocidades varios órdenes de magnitud inferior a la memoria principal. Por este motivo, la memoria del núcleo crítica se muestra como no paginada, pudiendo el resto paginarse.

De manera análoga a los casos anteriores, seleccionando la opción 'Ethernet' del Administrador de tareas (pestaña 'Rendimiento') obtendremos un resumen del rendimiento de la interfaz de red.



En caso de disponer de varios adaptadores, podremos seleccionar uno u otro para obtener información de su funcionamiento.



Si hacemos clic con el botón secundario sobre uno de los adaptadores de red y seleccionamos la opción 'Ver detalles de red', podremos obtener un listado exhaustivo de las estadísticas de funcionamiento de esa interfaz, como por ejemplo la velocidad del adaptador, el estado del mismo, los bytes enviados, los bytes recibidos, etc.

Detalles de la red		
Propiedad	Ethernet	Ethernet
Uso de red	0%	0,06%
Velocidad de vínculo	1 Gbps	10 Gbps
Estado	Conectado	Conectado
Rendimiento de bytes enviados	0%	0%
Rendimiento de bytes recibidos	0%	0,05%
Rendimiento de bytes	0%	0,06%
Bytes enviados	21.186	589.835
Bytes recibidos	25.589	30.835.451
Bytes	46.775	31.425.286
Bytes enviados por intervalo	82	13.548
Bytes recibidos por intervalo	128	748.276
Bytes por intervalo	210	761.824
Unidifusiones enviadas	344	20.548
Unidifusiones recibidas	227	10.661
Unidifusiones	571	31.209
Unidifusiones enviadas por int...	1	250
Unidifusiones recibidas por int...	2	498
Unidifusiones por intervalo	3	748
Otras difusiones enviadas	0	350
Otras difusiones recibidas	0	30
Otras difusiones	0	380
Otras difusiones enviadas por i...	0	0
Otras difusiones recibidas por i...	0	2
Otras difusiones por intervalo	0	2

Como norma general, si el porcentaje de utilización de la red supera el 50% de la capacidad total de una manera sistemática, habría que valorar la posibilidad de ampliar el número de interfaces de red del servidor.

## Supervisar sesiones

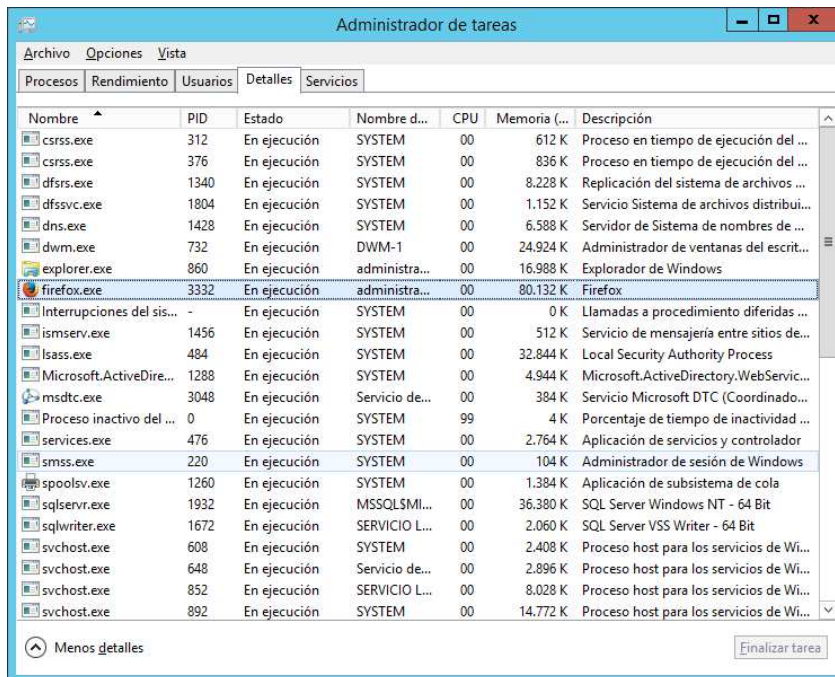
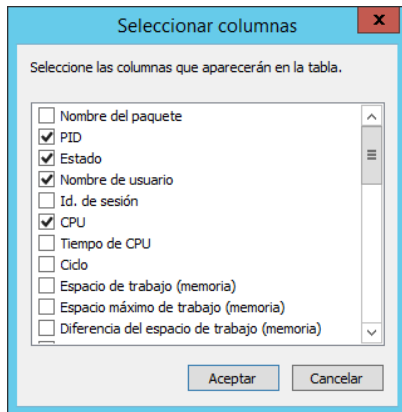
La ficha Usuarios muestra los usuarios conectados al equipo y el estado y los nombres de sesión, así como los procesos que están ejecutando.

Administrador de tareas			
Archivo Opciones Vista			
Procesos Rendimiento Usuarios Detalles Servicios			
Usuario	Estado	CPU	Memoria
administrador (8)		3%	82%
Administrador de tareas		2,6%	131,6 MB
Administrador de ventanas...		2,6%	10,0 MB
Aplicación de inicio de sesi...		0%	24,0 MB
Explorador de Windows		0%	0,5 MB
Firefox (32 bits)		0%	16,5 MB
Proceso de host para tarea...		0%	77,7 MB
Proceso en tiempo de ejec...		0%	1,4 MB
VirtualBox Guest Additions...		0%	0,8 MB
		0%	0,7 MB

Si se trata de un Windows cliente la ficha Usuarios sólo se muestra si el equipo en el que trabaja tiene habilitada la opción Cambio rápido de usuario y es un equipo independiente o es miembro de un grupo de trabajo. No está disponible en equipos que son miembros de un dominio de red.

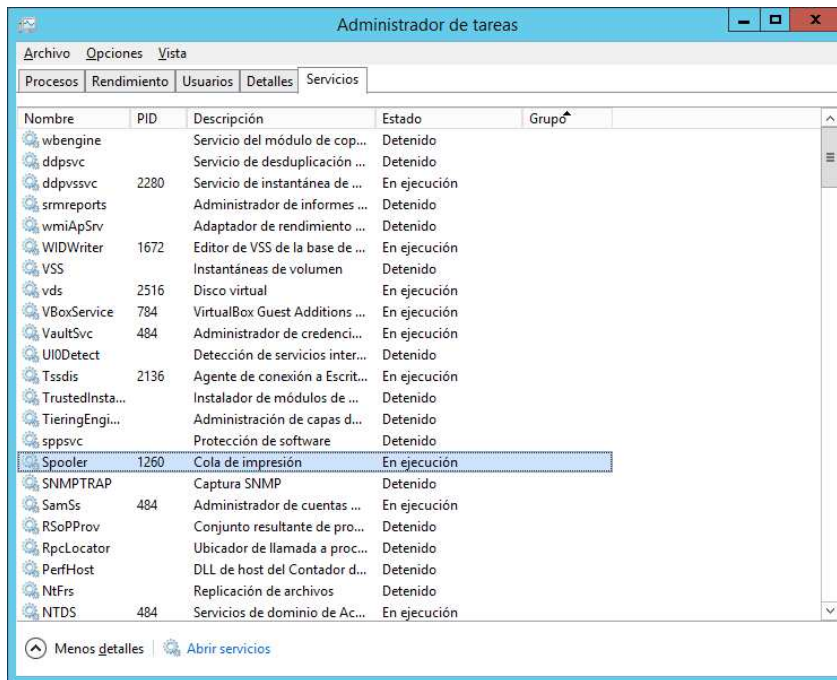
### Detalles de procesos

En la pestaña de Detalles podemos visualizar atributos de los procesos, permitiendo el añadir las columnas a visualizar. Entre otras podemos ver atributos internos como el número de proceso (PID), prioridad, estado, descripción, o datos referentes a su actividad como uso de CPU, memoria, fallos de página, bloques leídos o escritos en disco, ...



## Servicios

Desde la pestaña de servicios nos aparece una vista de los servicios iniciados y detenidos. Desde esta vista podemos Iniciar, Detener o Reiniciar un servicio o incluso acceder a la consola principal de **Servicios**. Además, tenemos una opción interesante que es la de visualizar el detalle del proceso asociado a ese servicio, llevándonos a la pestaña de **Detalles**.



## 3. El visor de eventos

Una de las maneras que tiene el SO de comunicarse con el usuario, o con el administrador del sistema, es mediante el registro de sucesos (eventos) que pueden ser visualizados mediante el visor de eventos.

Los registros de eventos contienen información acerca de los problemas de hardware y de software, y sobre los eventos de seguridad del equipo. Normalmente se registran eventos en tres tipos de registro como mínimo: aplicación, sistema y seguridad. Ahora bien, es posible que en un equipo haya disponibles otros tipos de eventos y registros de eventos, en función de los servicios que tenga instalados como pueden ser el registro de eventos del servicio de directorio y el del servicio de replicación de archivos o si está instalado, por ejemplo el servidor DNS, se registran eventos relacionados con el DNS en otro registro más.

Windows Server incluye la capacidad de recopilar copias de eventos procedentes de varios equipos remotos y guardarlas en uno solo, además de los eventos propios del equipo donde está instalado.

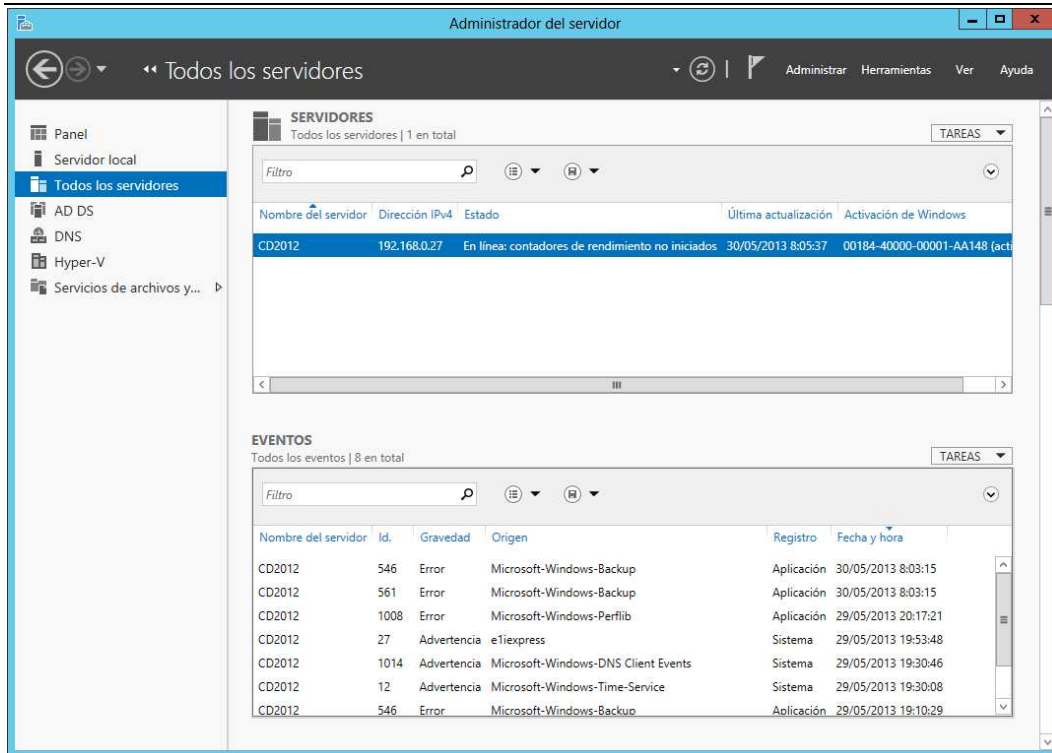
En Windows, las 3 principales categorías donde se agrupan los sucesos en el visor son Aplicación, Seguridad y Sistema. Cuando el SO genera un evento, dependiendo de qué categoría lo considere lo incluirá en una de estas 3.

Del mismo modo, independientemente de la categoría, hay 6 tipos de sucesos principales:

- **Crítico:** Problema importante que puede imposibilitar el normal funcionamiento.
- **Error:** Problema importante, como pérdida de datos o de funcionalidad. Por ejemplo, si no se puede cargar un servicio durante el inicio, se registrará un error.
- **Advertencia:** Suceso que no es importante necesariamente, pero que indica la posibilidad de problemas en el futuro. Por ejemplo, cuando queda poco espacio de disco, se puede registrar una advertencia.
- **Información:** Un suceso que describe el funcionamiento correcto de una aplicación, controlador o sistema. Por ejemplo, cuando un controlador de red carga correctamente, se registrará un suceso de Información.
- **Acceso correcto auditado:** Un suceso de seguridad auditado que es correcto. Por ejemplo, un intento satisfactorio de un usuario de iniciar una sesión en el sistema se registrará como suceso de Acceso correcto auditado.
- **Acceso erróneo auditado:** Cualquier suceso de seguridad auditado que sea erróneo. Por ejemplo, si un usuario intenta tener acceso a una unidad de red y se produce un error, el intento se registrará como suceso de Acceso erróneo auditado.

Para visualizar estos eventos podemos hacerlo desde varias consolas. Si en el Administrador del Servidor seleccionamos **Todos los servidores** y a continuación el servidor del que queremos obtener la información, nos aparecerá en la parte inferior un listado de los eventos surgidos en ese equipo.

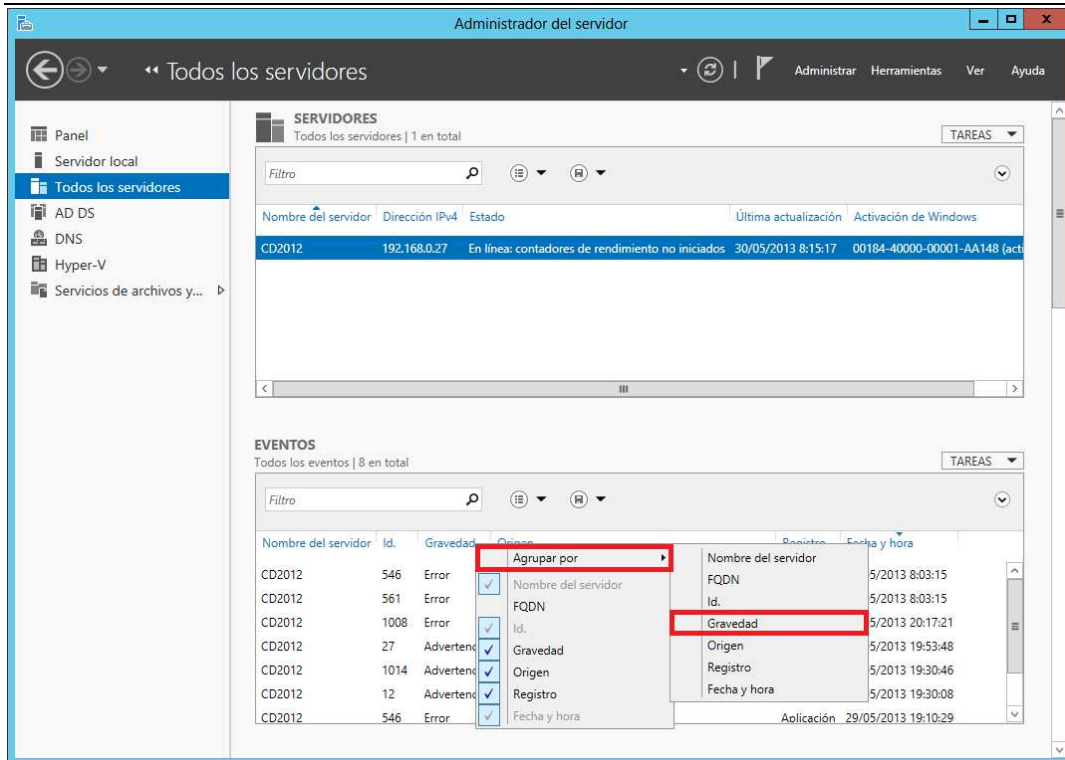




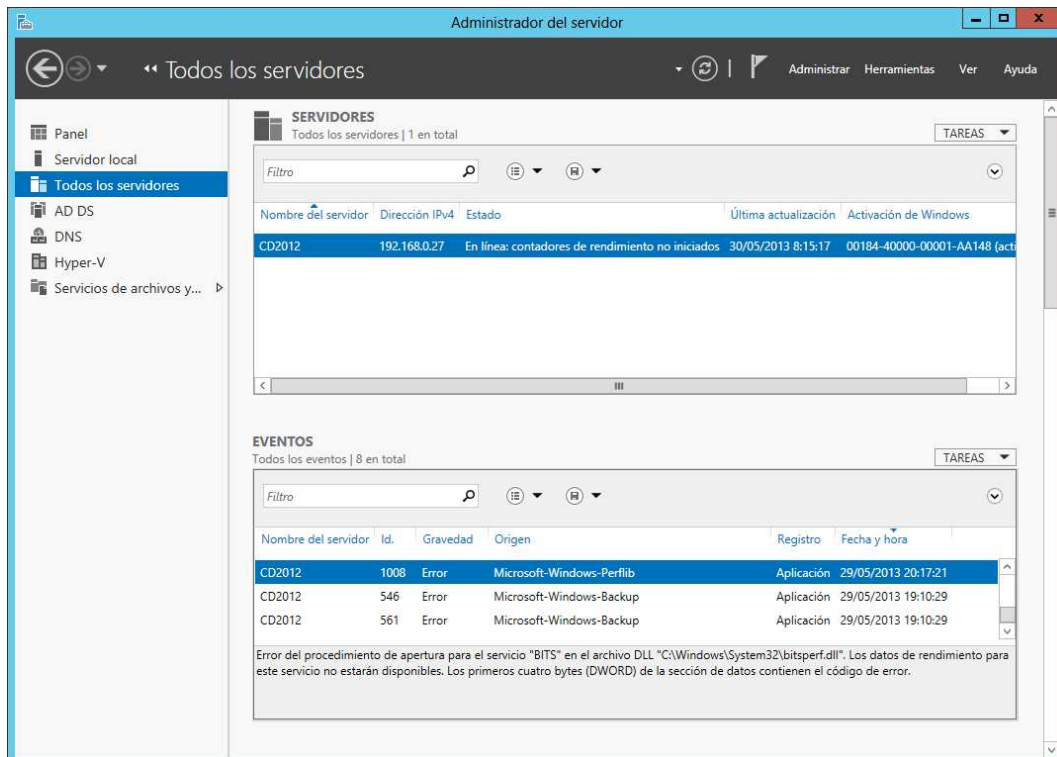
Como puede comprobarse, los eventos poseen una serie de datos que nos permite contextualizarlos y rastrearlos:

- Nombre del servidor: equipo en el que se ha producido el evento.
- Id.: Código asociado al evento.
- Gravedad: nivel del evento.
- Origen: servicio o aplicación que ha producido el evento.
- Registro: tipo de registro en el que se almacenó el evento.
- Fecha y hora: instante en el que se almacenó el evento.

Para facilitar la visualización de los eventos, estos se pueden agrupar por alguno de los campos anteriores. Para ello basta con hacer clic con el botón secundario sobre la fila en la que aparecen los identificadores de los campos, y seleccionar en **Agrupar por** el campo por el que queremos que se agrupe la información.



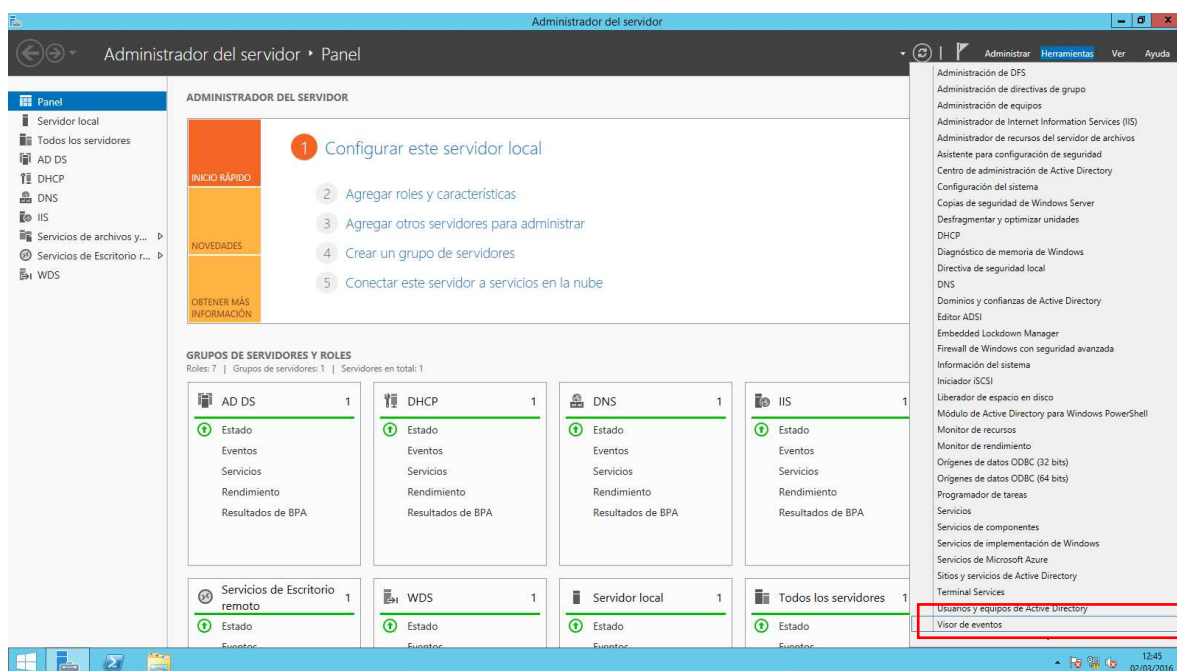
Si por ejemplo, agrupamos por 'Gravedad', obtendremos un listado como el que se muestra:



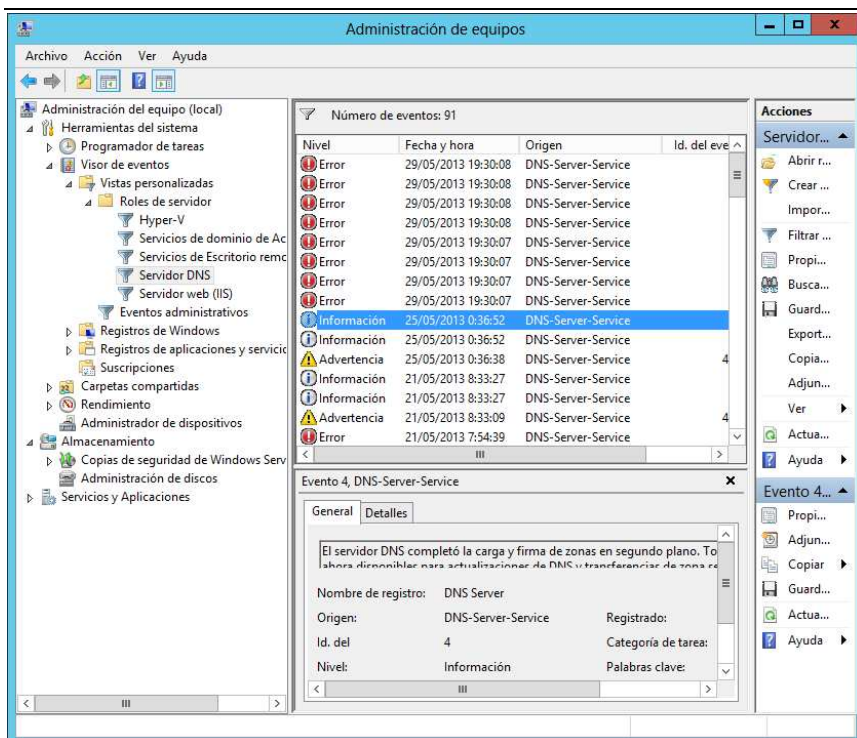
## Visor de Eventos

De una manera alternativa, disponemos del **Visor de Eventos**, el cual nos permite un trabajo más cómodo, obteniendo más información de los eventos, e incluso permitiéndonos acceder a los registros de equipos remotos. Para acceder al Visor de eventos tenemos dos vías.

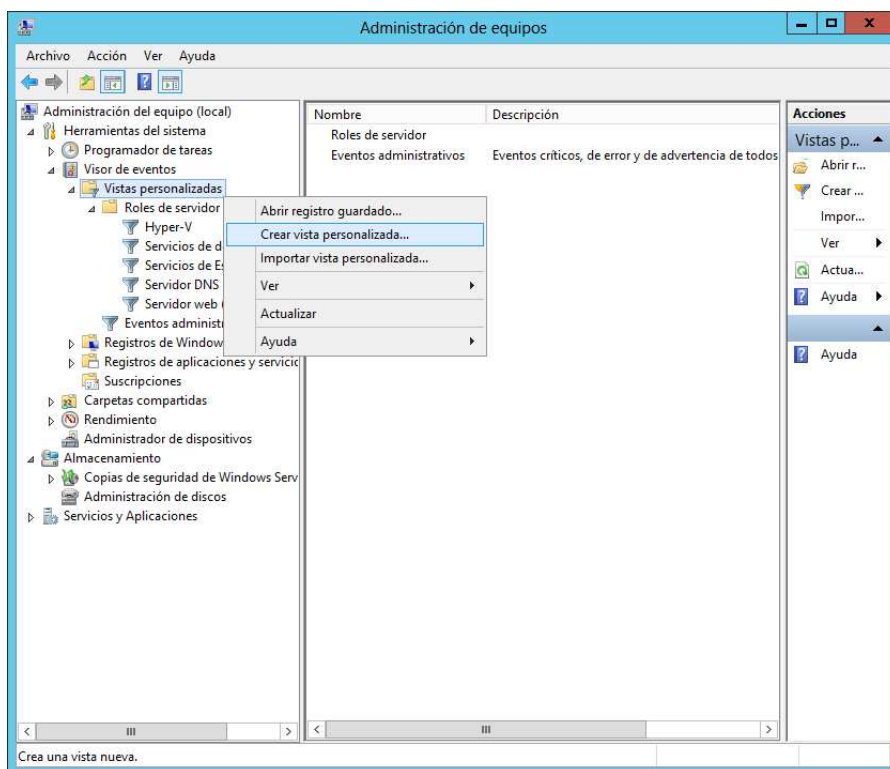
La más sencilla es utilizar la consola que aparece en el menú de Herramientas del sistema del Administrador del Servidor.



La segunda manera de acceder es abriendo el administrador del servidor, y en Herramientas seleccionamos la opción **Administración de Equipos**. Se abrirá una consola donde bajo '**Herramientas del sistema**', podemos acceder al '**Visor de eventos**'.



Existen diferentes filtros bajo 'Vistas personalizadas', que nos permiten visualizar los eventos producidos por determinados servicios. No obstante, nosotros también podemos definir vistas personalizadas de eventos. Para ello hacemos clic con el botón secundario sobre 'Vistas personalizadas' y seleccionamos la opción 'Crear vista personalizada...'.  
Crea una vista nueva.

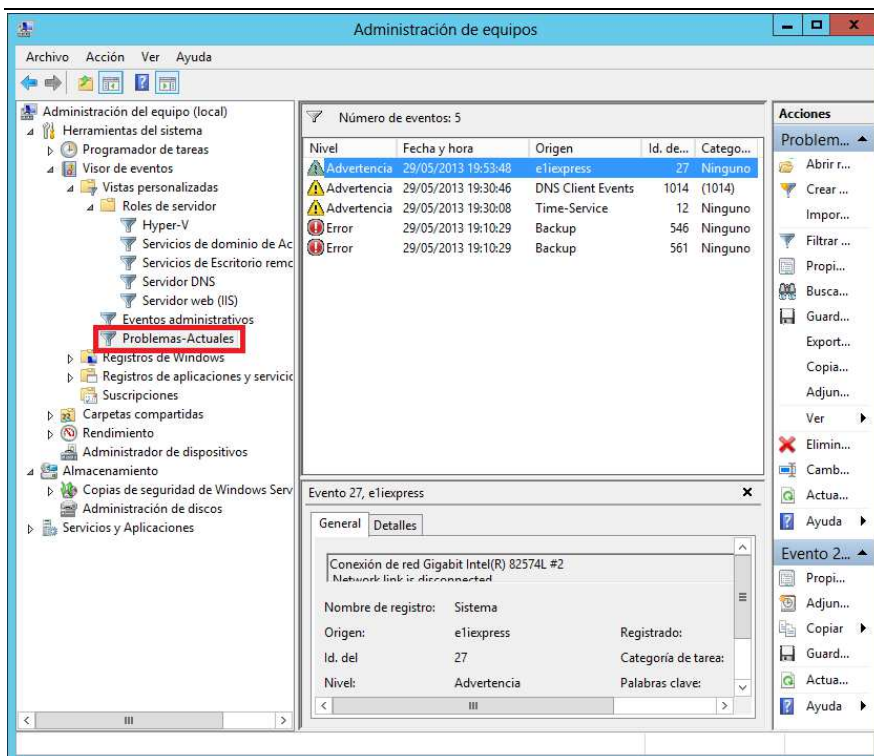


Se abrirá un cuadro de texto en el que podremos configurar el tipo de información a visualizar. En el ejemplo se registran únicamente los eventos acaecidos durante la última hora, cuya gravedad corresponda a 'Crítico', 'Advertencia' o 'Error', y que sean de Aplicación, Seguridad, Instalación, Sistema, etc.

Al pulsar 'Aceptar', nos preguntará por el nombre que queremos proporcionar al filtro de la vista personalizada, en este caso lo hemos llamado 'Problemas-Actuales', y el lugar en el que queremos que aparezca: dentro de Vistas personalizadas, a la misma altura jerárquica que 'Roles del Servidor'.

Una vez creado el filtro, podremos visualizar los eventos correspondientes haciendo clic sobre él. En este caso se muestran 5 registros, de los cuales tres son advertencias y dos son errores.

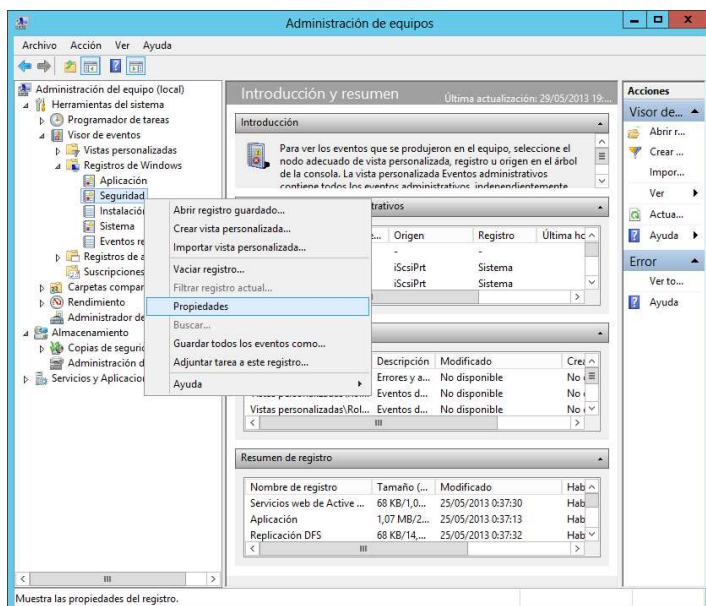




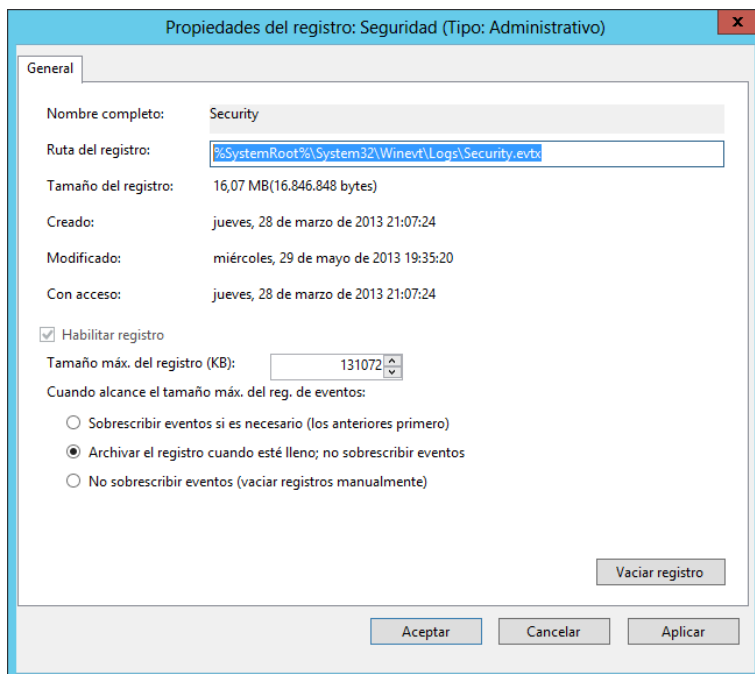
## Registro de Eventos

Yendo un paso más allá de la visualización de los eventos, también podemos generar registros, que nos permitan almacenar los eventos que cumplan una serie de condiciones en un fichero para su posterior análisis.

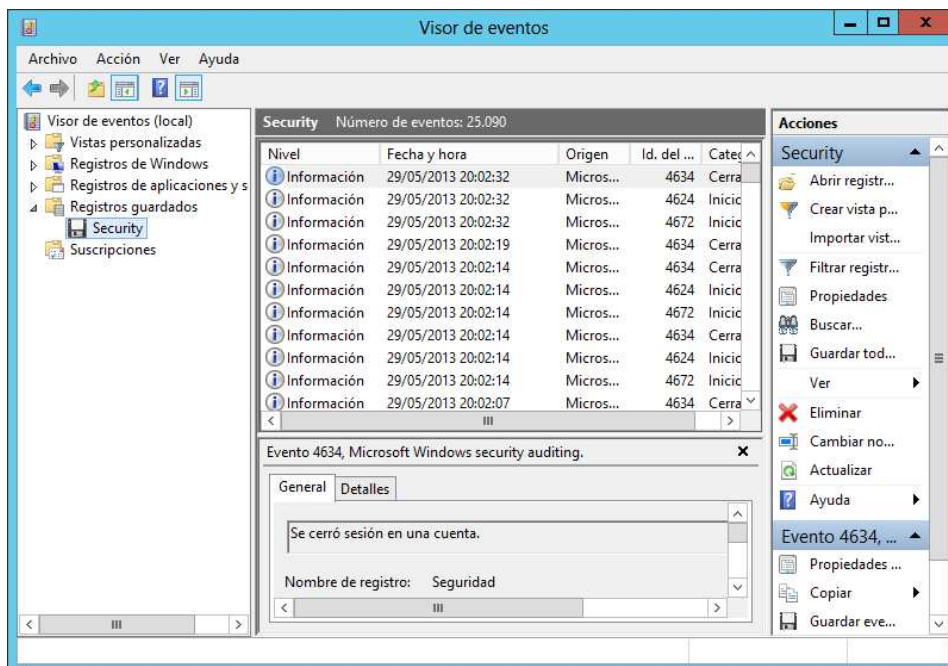
Supongamos que queremos generar un fichero con todos los registros de los eventos de 'Seguridad'. Haremos clic con el botón derecho sobre 'Seguridad', bajo 'Registros de Windows' y accederemos a 'Propiedades'.



En el cuadro que se abrirá aparecerán aspectos como la ruta donde queremos que se almacene la información, el tamaño máximo del registro (cuidado con este valor, ya que es fácil que se llene rápidamente, o que genere archivos de tamaños muy elevados), así como las tareas a realizar si el fichero ha llegado a su tamaño máximo.

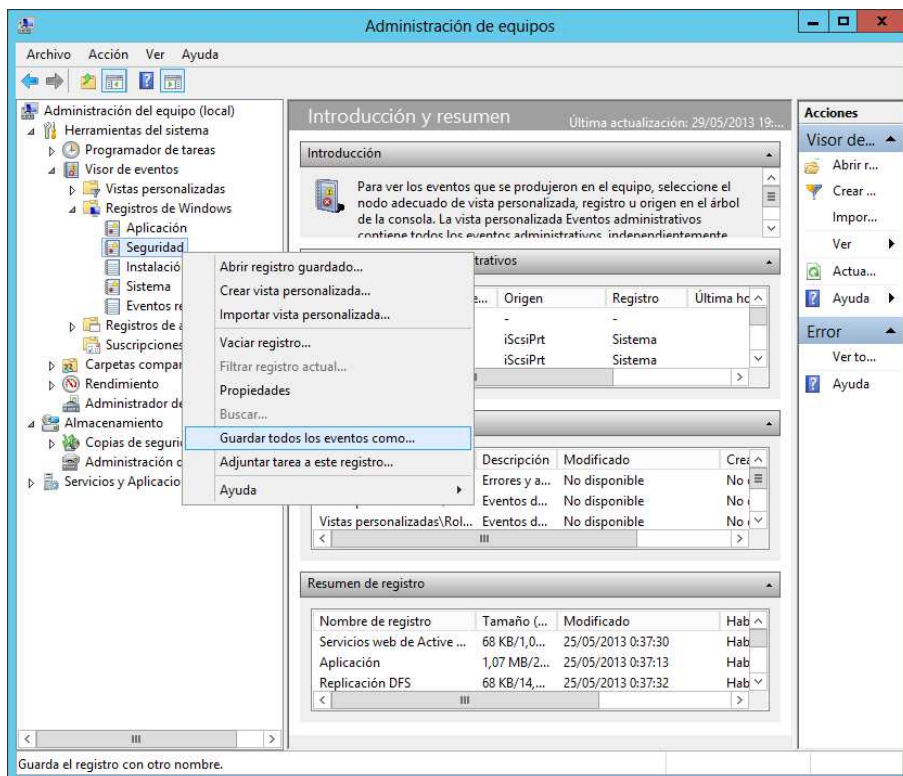


Si accedemos a 'Registros guardados' veremos que aparece el registro 'Security', y en el visor obtendremos los eventos que se han ido almacenando.

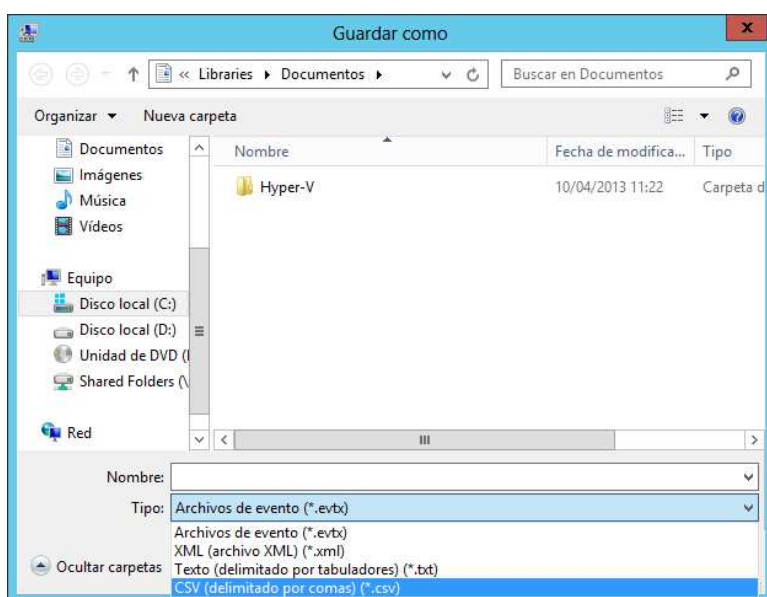




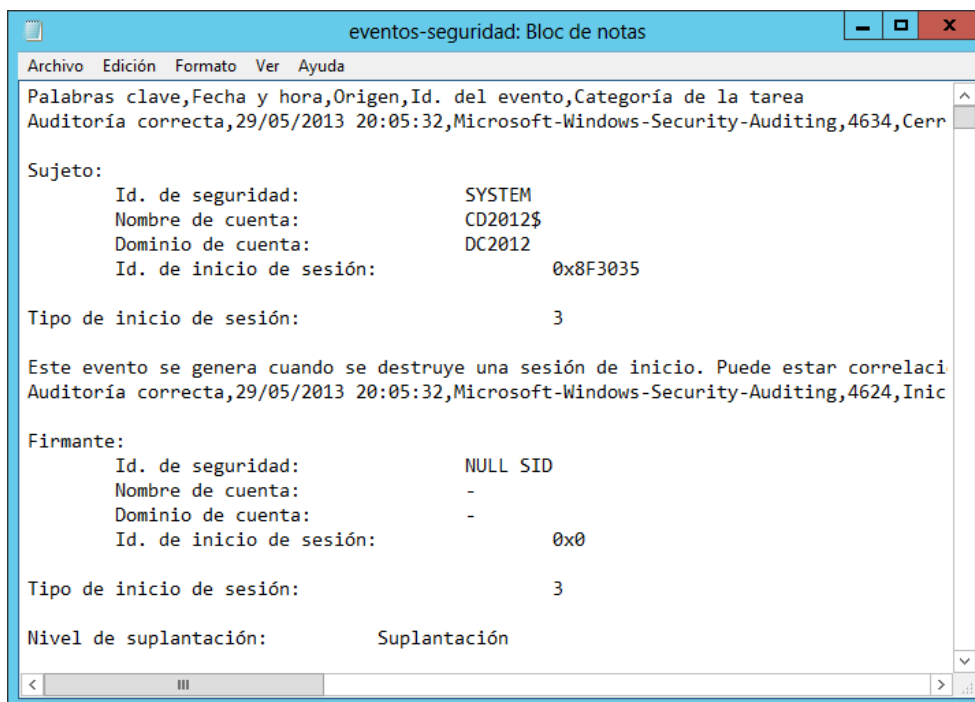
El registro generado podremos exportarlo a un tipo de fichero que nos permita su interpretación (ya que el fichero security.etx generado está codificado y comprimido). Para ello seleccionamos el tipo de registro que estamos generando, hacemos clic en el botón secundario y escogemos la opción 'Guardar todos los eventos como...'.



Se abrirá un cuadro de diálogo en el que nos permitirá indicar el lugar en el que almacenaremos el fichero con la información del registro, así como el formato.



Si por ejemplo lo guardamos con los formatos csv, o txt, podremos comprobar el tipo de información que se ha almacenado y que nos podría facilitar un posterior análisis de la misma.



## 4. El monitor de rendimiento

Además de poder visualizar los distintos eventos del sistema para controlar errores, fallos de aplicaciones o violaciones de seguridad, una de las tareas del administrador es, como hemos visto, la de controlar y supervisar el rendimiento del sistema para asegurarnos que no se producen caídas o que el sistema es capaz de soportar la carga diaria de trabajo.

Los distintos SO aportan distintas herramientas, en los sistemas Windows contamos con el **monitor de rendimiento**.

El Monitor de rendimiento de Windows es un complemento de Microsoft Management Console (MMC) que proporciona herramientas para analizar el rendimiento del sistema. Desde una sola consola se puede supervisar el rendimiento de las aplicaciones y del hardware en tiempo real, personalizar qué datos se desea recopilar en los registros, definir umbrales para alertas y acciones automáticas, generar informes y ver datos de rendimientos pasados en una gran variedad de formas.

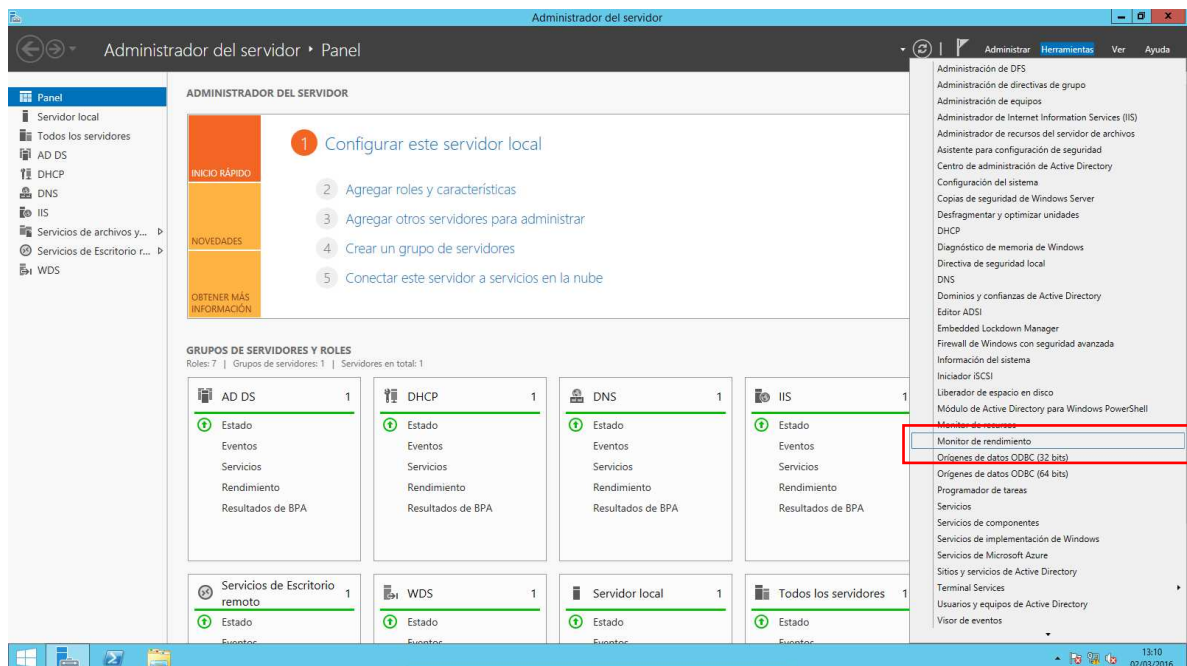
Se puede usar el Monitor de rendimiento de Windows para examinar el modo en el que los programas que ejecuta afectan al rendimiento del equipo, tanto en tiempo real como mediante la recopilación de datos de registro para su análisis posterior.

El Monitor de rendimiento de Windows usa contadores de rendimiento, datos de seguimiento de eventos e información de configuración, que se pueden combinar en conjuntos de recopiladores de datos.

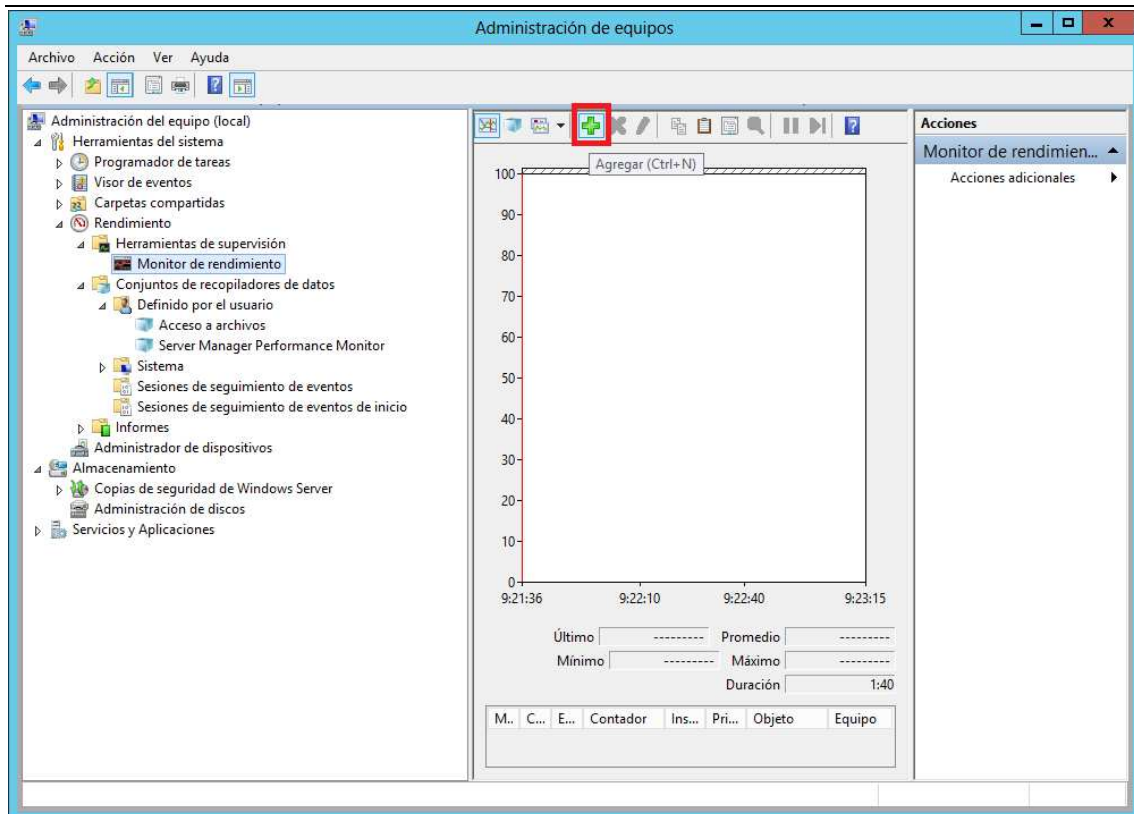
Los contadores de rendimiento son mediciones del estado o de la actividad del sistema. Se pueden incluir en el sistema operativo o formar parte de aplicaciones individuales. El Monitor de rendimiento de Windows solicita el valor actual de los contadores de rendimiento en intervalos de tiempo especificados.

Para poner en marcha el monitor de rendimiento también podemos acceder por dos vías.

La primera desde las **Herramientas** del Server Manager:

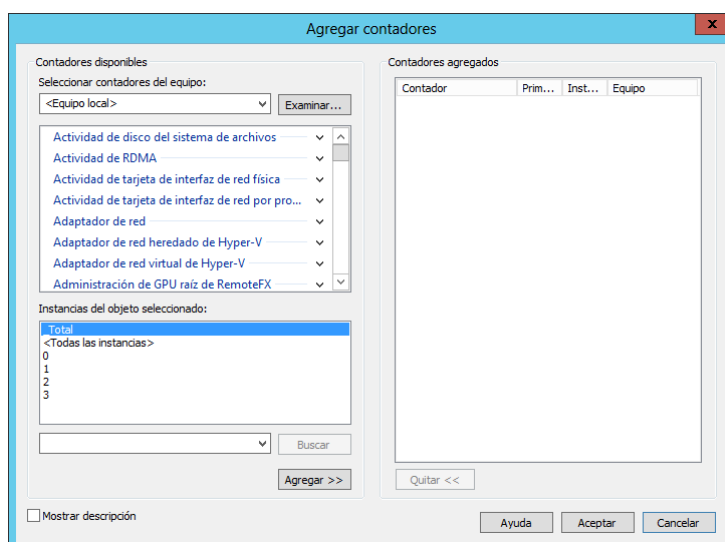


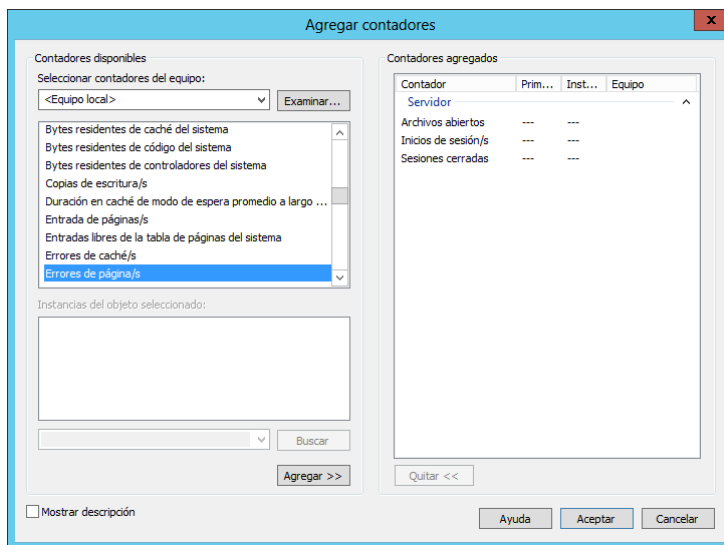
La segunda desde la consola de **Administración de equipos**, y accederemos a 'Monitor de rendimiento' que se encuentra en 'Rendimiento'→'Herramientas de supervisión'. Para agregar parámetros de monitorización, haremos clic en la cruz verde señalada en la siguiente figura.



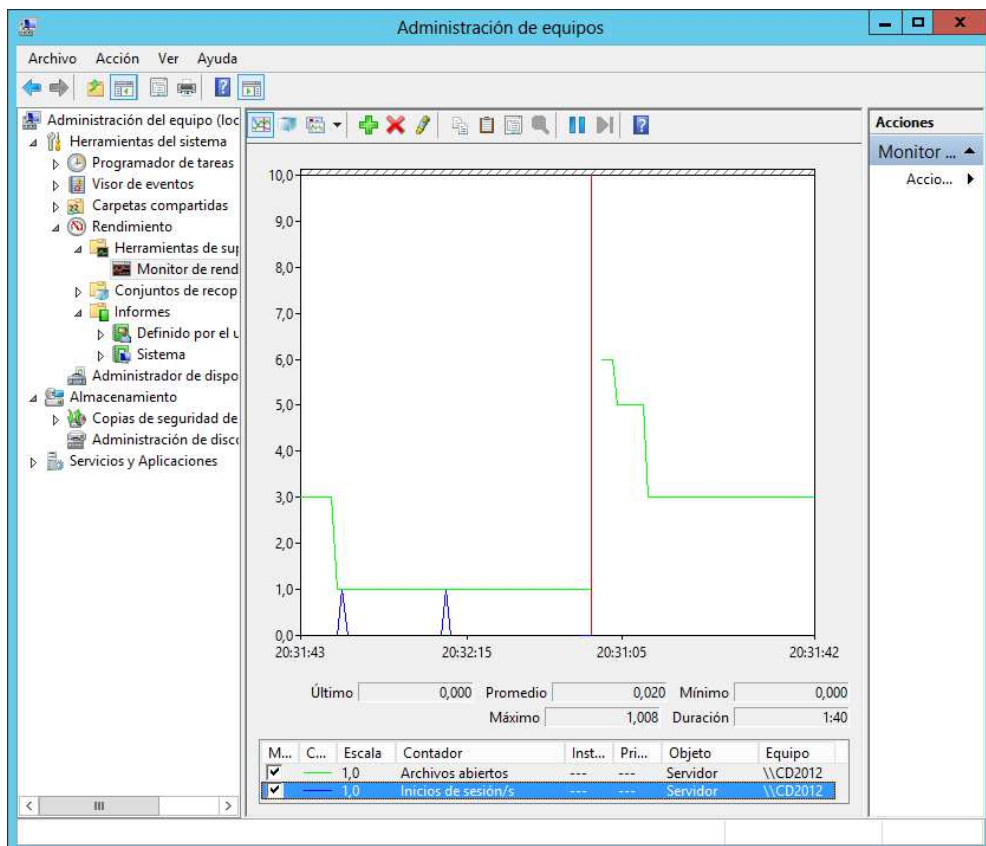
Se abrirá un asistente que nos permitirá añadir **miles** de indicadores de funcionamiento del sistema, los cuales se denominan **contadores**. Cada uno de los objetos utilizados por el Monitor de Rendimiento contiene diversos contadores que proporcionan información acerca del uso, rendimiento, recursos consumidos, etc., para cada objeto.

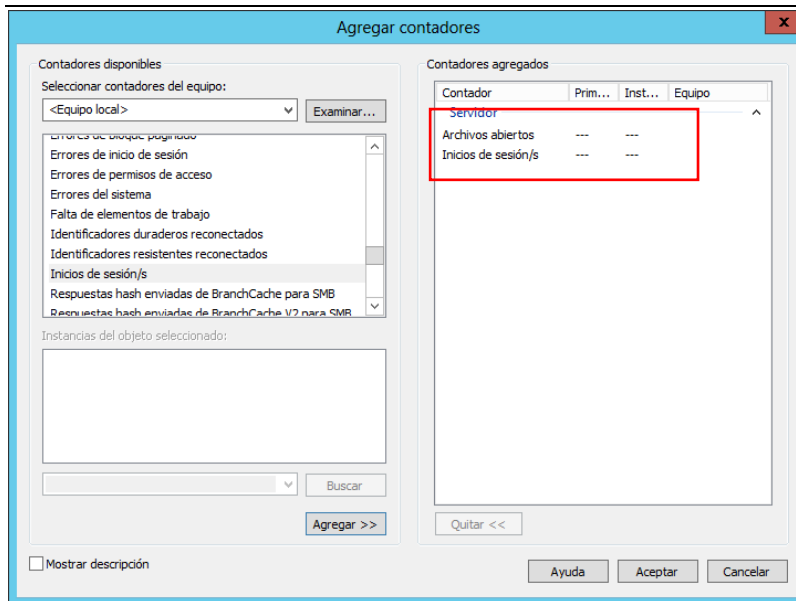
Si revisamos someramente los apartados en los que se agrupan veremos que tenemos categorías como 'Adaptador de red', IP, Procesador, Memoria, etc... A su vez, cada apartado tiene varios contadores.





Si pulsamos en 'Aceptar', automáticamente se mostrará de manera gráfica el valor de los contadores de rendimiento que hemos seleccionado. En este ejemplo se han seleccionado los contadores que suministran la información de los eventos de apertura de archivos y de inicios de sesión.





De igual modo, también podemos monitorizar el rendimiento de un equipo remoto (**Importante:** debe estar habilitada la 'Administración Remota' y configuradas las excepciones de entrada para 'Administración de servicios remotos' en el equipo cliente).

### Contadores Asociados al Rendimiento del Procesador

Aunque los servidores suelen ser equipos muy potentes dotados de varios procesadores, y grandes cantidades de memoria RAM, no es extraño que ambos aspectos constituyan los principales factores limitantes del sistema. Cuando surgen problemas de rendimiento en el equipo, suele ser una buena práctica comenzar revisando el rendimiento del microprocesador.

Los principales conjuntos de contadores que utilizaríamos para monitorizar el uso del procesador serían los siguientes:

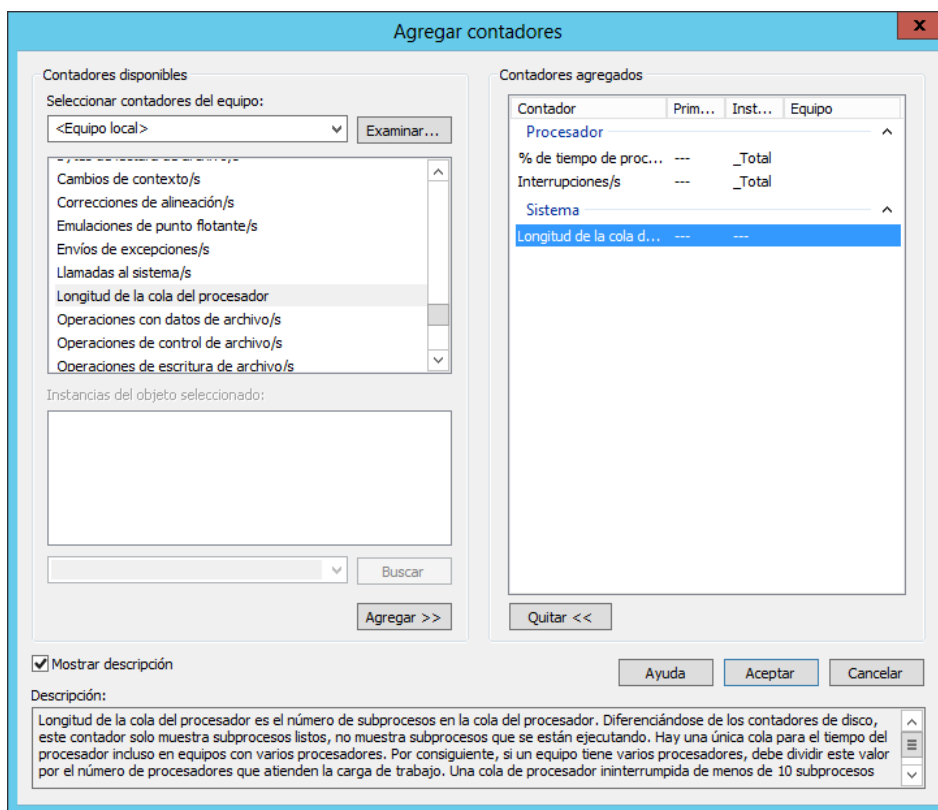
- % de tiempo del procesador: cada procesador tiene un subproceso inactivo que consume ciclos de ejecución cuando no hay ningún otro subproceso preparado para ejecutarse. El porcentaje de tiempo de procesador equivale al porcentaje de tiempo en el que el procesador no está ejecutando el subproceso inactivo, por lo que de alguna manera es un buen indicador de la carga del sistema. **Como valor de referencia, si este contador suele hallarse por encima del 50%, deberíamos plantear la ampliación del sistema.**
- Interrupciones por segundo: este contador es un indicador de la actividad de los dispositivos que generan interrupciones (como el ratón, el reloj del sistema,



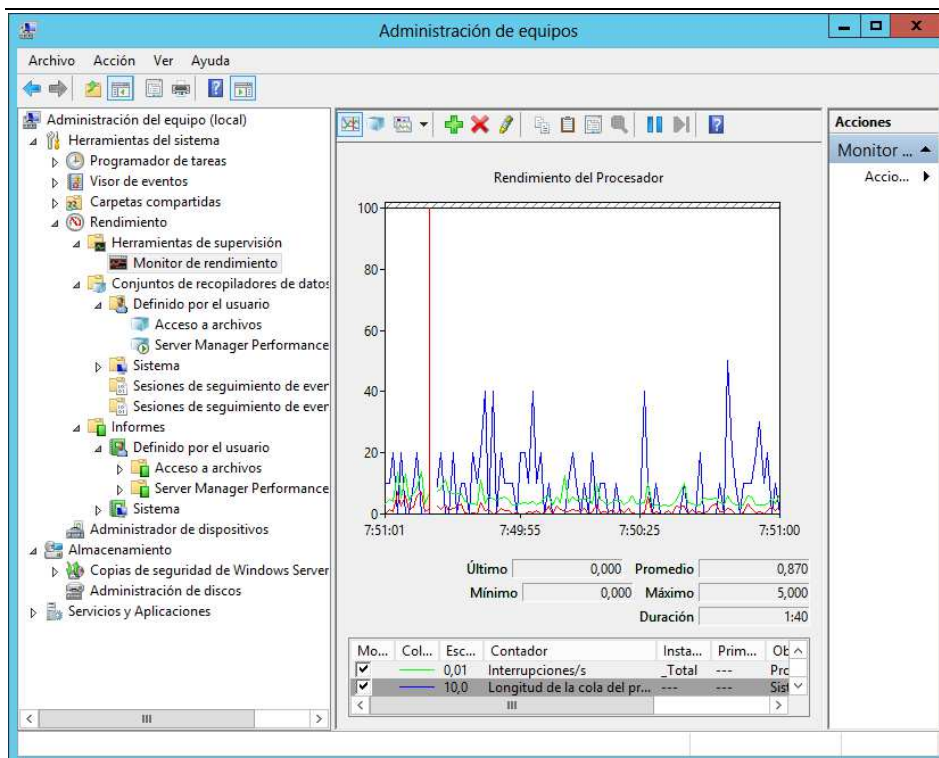
etc.). Como las interrupciones detienen la ejecución de los procesos, un número muy elevado de estas puede empeorar el rendimiento del sistema.

- Longitud de la cola del procesador: este contador no se halla bajo el objeto Procesador, sino bajo el objeto Sistema. Indica el número de procesos esperando para entrar al procesador (o procesadores). **Se suele considerar el valor orientativo de 10 como un nivel por debajo del cual el funcionamiento del sistema es adecuado.** Si en el servidor hay varios procesadores, el valor de la cola se dividirá entre el número de procesadores, ya que esta es única independientemente de las características del hardware del equipo.

En las siguientes figuras se pueden ver los contadores mencionados anteriormente, así como los objetos de los que cuelgan (panel derecho) y la información recopilada de los contadores principales del rendimiento del procesador.







## Contadores Asociados al Rendimiento de la Memoria RAM

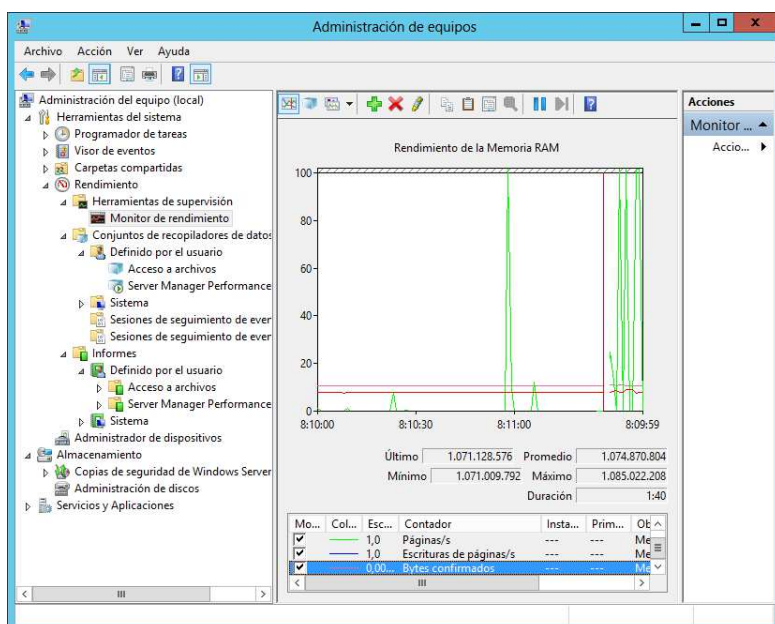
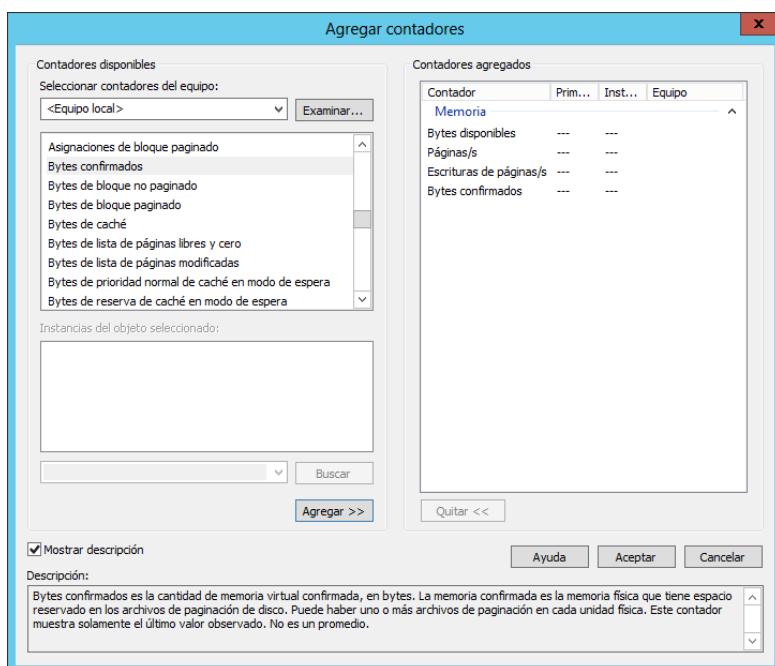
Probablemente el elemento hardware más íntimamente ligado al rendimiento de un sistema sea la memoria RAM, de hecho, cuando esta se colapsa se origina una caída significativa del rendimiento del equipo. Además, también sabemos que a medida que el sistema vaya necesitando más RAM, y esta no pueda ser proporcionada a los procesos, se utilizará la memoria virtual, la cual provoca una degradación importante del rendimiento.

Por tanto, los principales conjuntos de contadores que utilizaríamos para monitorizar el uso de la memoria RAM serían:

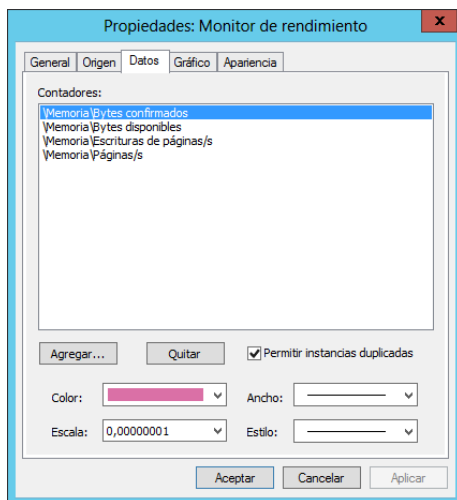
- **Bytes disponibles:** corresponde a la memoria física disponible para su asignación a un proceso. Valores por debajo de 128 MB van a ocasionar problemas de paginación al tener que trabajar con la memoria virtual.
- **Páginas por segundo:** este contador indica la cantidad de veces que el servidor debe acceder al archivo de paginación para resolver un error severo de página. Si se supera habitualmente el valor de 20 páginas por segundo, es recomendable la ampliación de la memoria física.

- Errores de páginas/segundo: indica los errores de página ocurridos durante un segundo. Un error de página consiste en que el bloque de memoria que necesita un proceso, no se encuentra en la memoria RAM y tiene que ser traído de la memoria virtual.
- Bytes confirmados: corresponde al valor de la memoria virtual utilizada. Cuanto mayor sea este valor, peor rendimiento se obtendrá.

En las siguientes figuras se pueden ver los contadores mencionados anteriormente, así como los objetos de los que cuelgan (panel derecho) y la información recopilada de los contadores principales del rendimiento del procesador.



Es importante darse cuenta de que estamos representando en el mismo gráfico valores con órdenes de magnitud muy diferentes. Por ejemplo un valor típico de 'Páginas por segundo' se hallará alrededor de 10, mientras que un valor típico de 'Bytes disponibles' se hallará en torno a 1.000.000.000, por lo que habrá que modificar la escala de los contadores para poder representarlos de una manera inteligible.

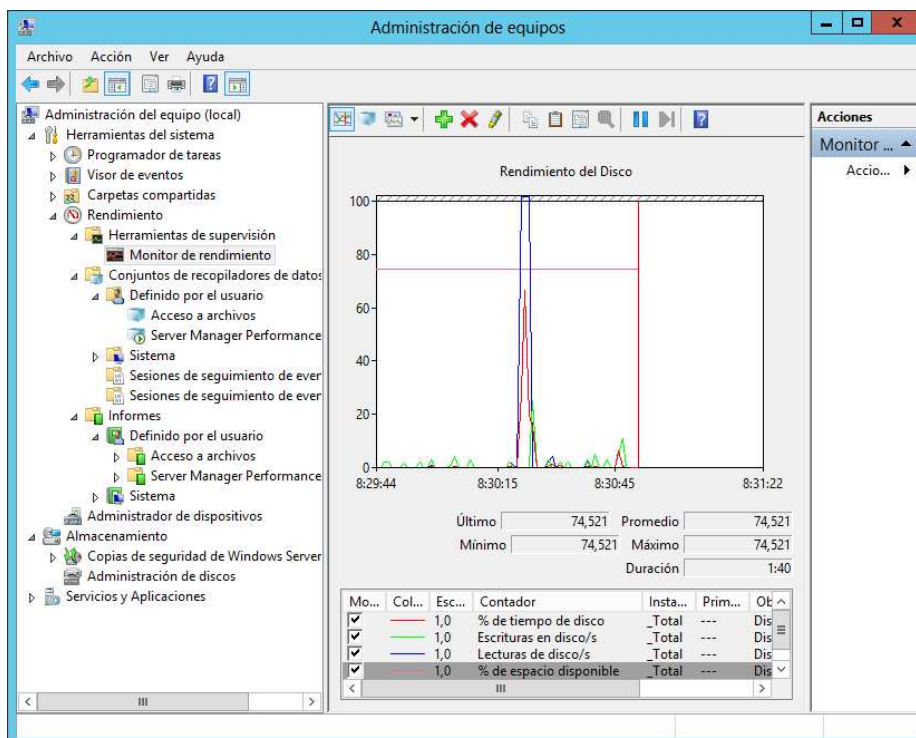
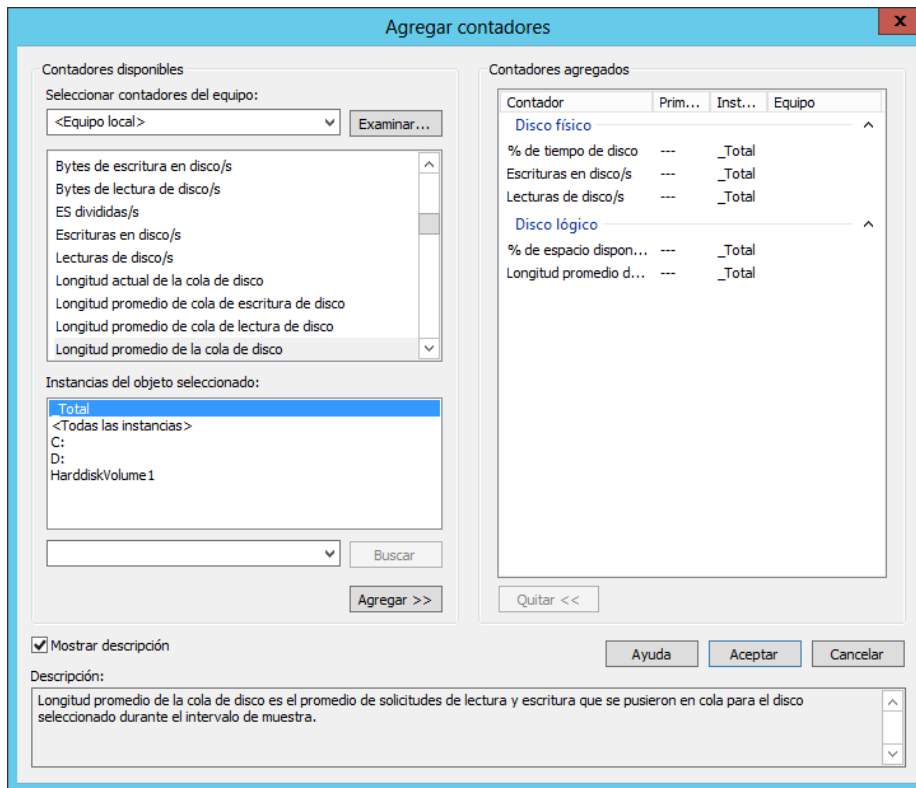


## ***Contadores Asociados al Rendimiento de los Discos***

Los principales conjuntos de contadores que utilizaríamos para monitorizar los discos serían:

- % de tiempo de disco: se halla en 'Disco Físico'. Indica el porcentaje de tiempo en el que el disco se encuentra prestando servicios de lectura o escritura. Un valor adecuado típico para este contador debería estar por debajo del 80%. Obviamente, un disco desfragmentado mejorará este valor, así como discos de mayores prestaciones.
- Escritura (y lectura) en disco: se halla en 'Disco Físico'. Indica la velocidad a la que se realizan estas operaciones.
- % de espacio disponible: se halla en 'Disco Lógico'. Indica el porcentaje de espacio total utilizable. Debería hallarse por encima del 25%.
- Longitud promedio de la cola de disco: se halla en 'Disco Lógico'. Indica la cantidad de solicitudes pendientes de atender por el disco.

En las siguientes figuras se pueden ver los contadores mencionados anteriormente, así como los objetos de los que cuelgan (panel derecho y la información recopilada de los contadores principales del rendimiento del disco.



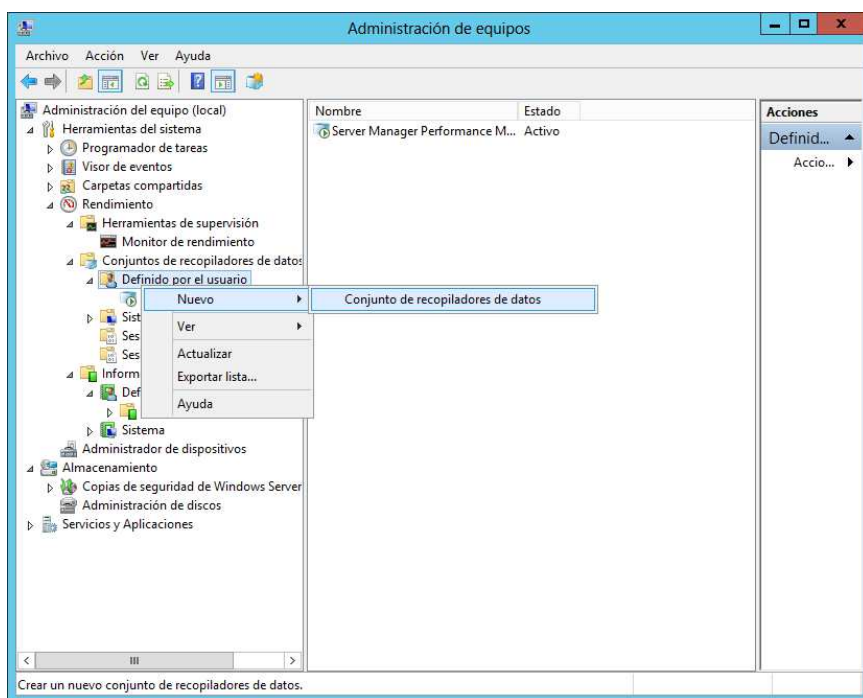
## 5. Registros y alertas de rendimiento

### Conjuntos de Recopiladores de Datos

Un recopilador de datos es un contenedor que permite agrupar contadores de rendimiento, datos de seguimiento de eventos y valores de las claves del Registro.

Como hemos visto hasta ahora, podemos utilizar el Monitor de Rendimiento para mostrar los valores instantáneos de una serie de contadores, pero también podemos almacenar registros a través de los conjuntos recopiladores de datos y analizarlos posteriormente.

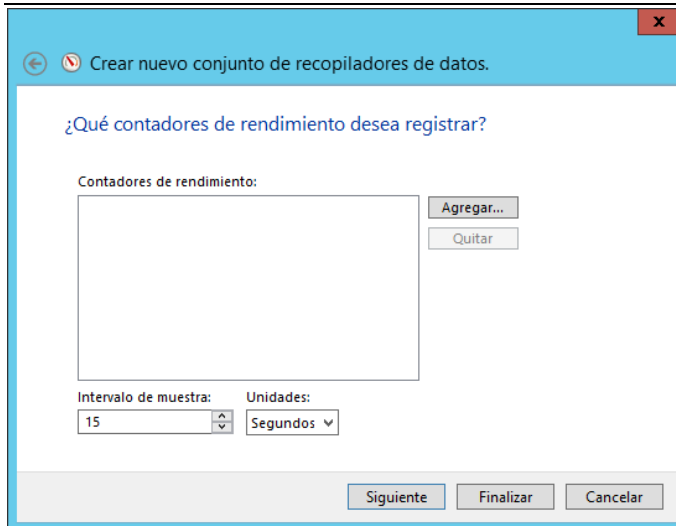
Para crear un conjunto de recopiladores de datos, accederemos a la opción 'Conjuntos de Recopiladores de Datos' → 'Definido por el usuario', haremos clic con el botón secundario y seleccionaremos 'Nuevo' → 'Conjunto de Recopiladores de Datos'.



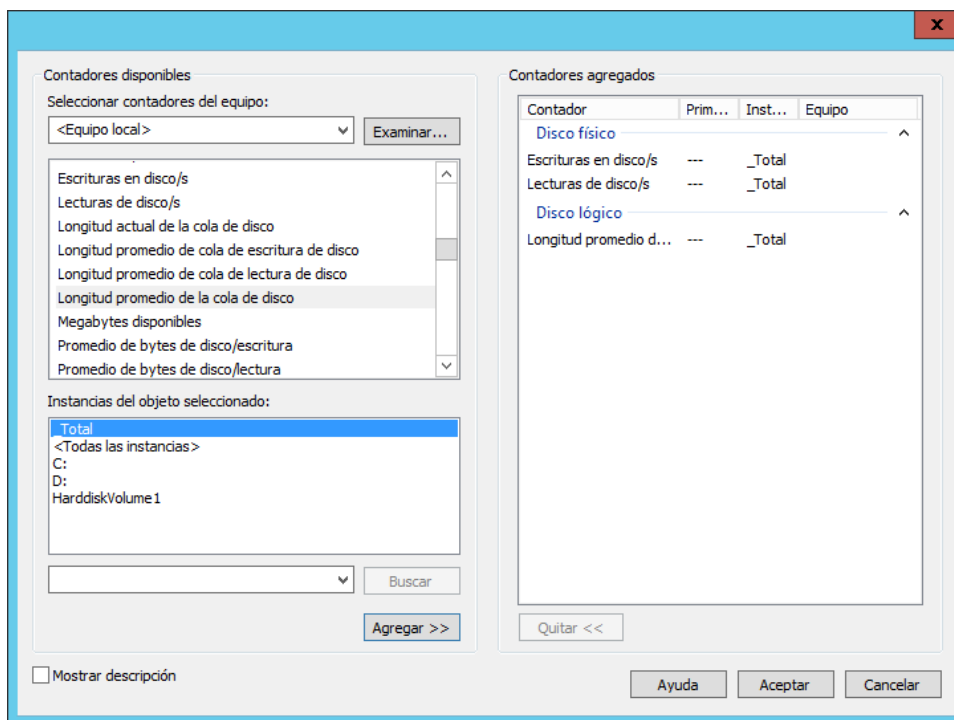
En el asistente que se abrirá, le indicaremos el nombre del conjunto, como en este caso vamos a hacer una monitorización de algunos parámetros del disco, lo llamaremos 'Acceso a Disco'.

En la siguiente pantalla se nos muestra el tipo de información que podríamos recoger. En 'Contador de Rendimiento' podemos escoger contadores de rendimiento y definir los intervalos de muestreo. En 'Datos de seguimiento de eventos' podremos seleccionar los proveedores de seguimiento de eventos y editar sus propiedades. En 'Información de configuración del sistema' podemos definir las claves del registro que se quieren supervisar. Finalmente, la opción 'Alerta del contador de rendimiento' permite definir contadores de rendimiento y asociarles unas condiciones para emitir avisos. Como sólo queremos registrar información relativa al rendimiento, en este caso seleccionaremos únicamente 'Contador de rendimiento'.

Se abrirá una nueva ventana que nos permitirá agregar contadores, de manera similar a como lo hacíamos en el monitor de rendimiento.

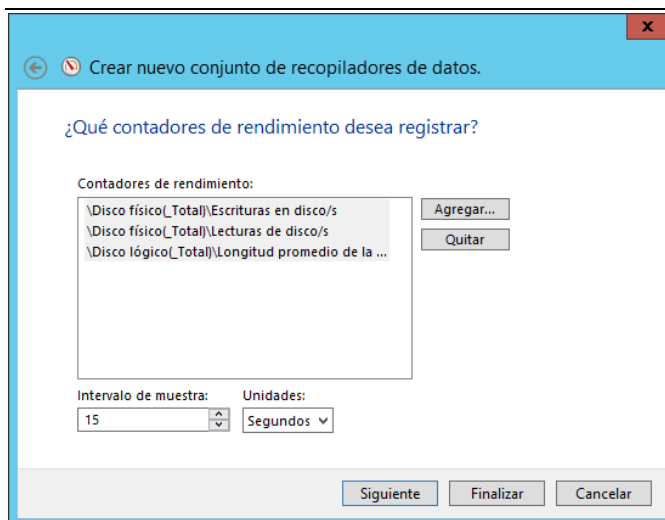


Por ejemplo seleccionaremos las escrituras y lecturas en disco, y la longitud promedio de la cola de disco.

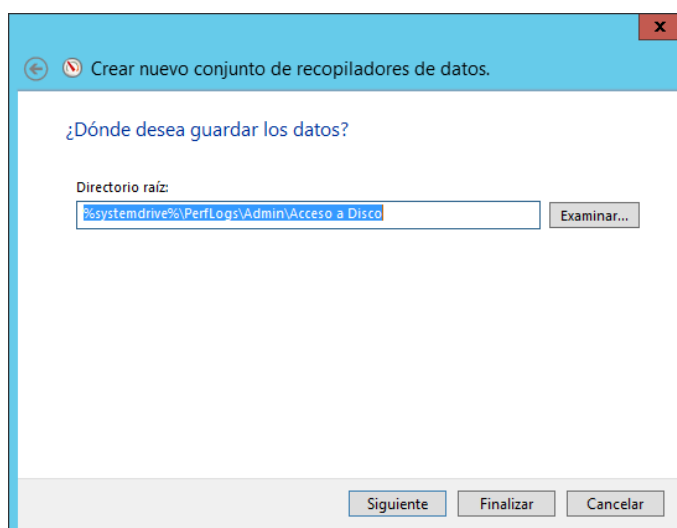


Además, también podemos modificar el intervalo de tiempo entre muestras.

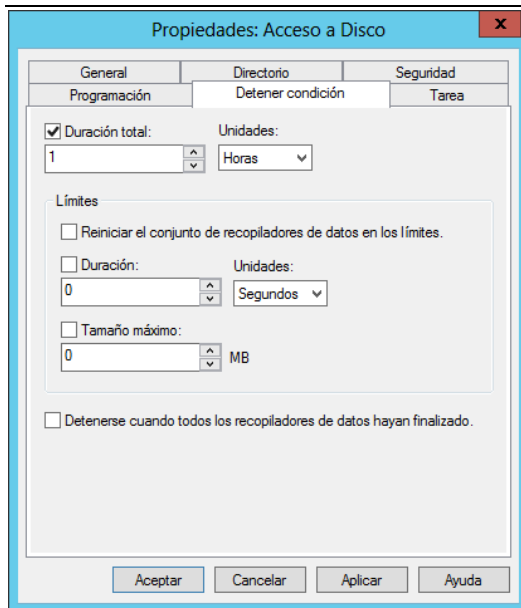




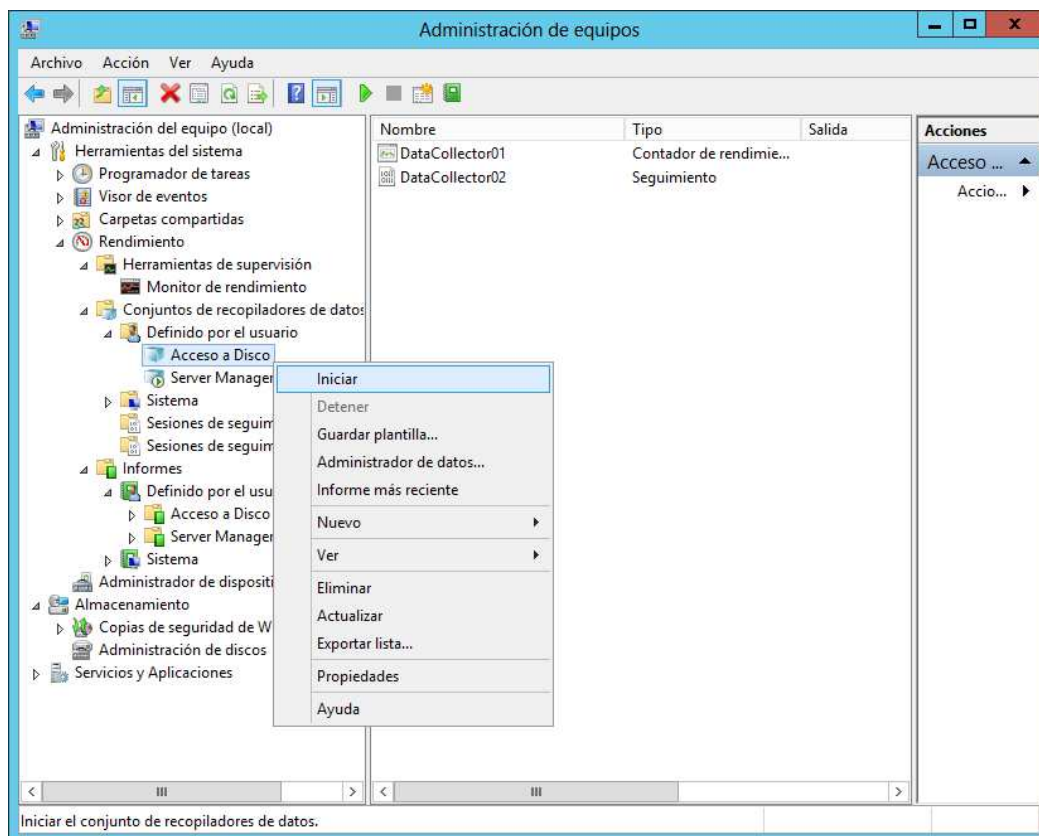
Finalmente podremos indicar dónde queremos que se almacenen los registros que se vayan generando.



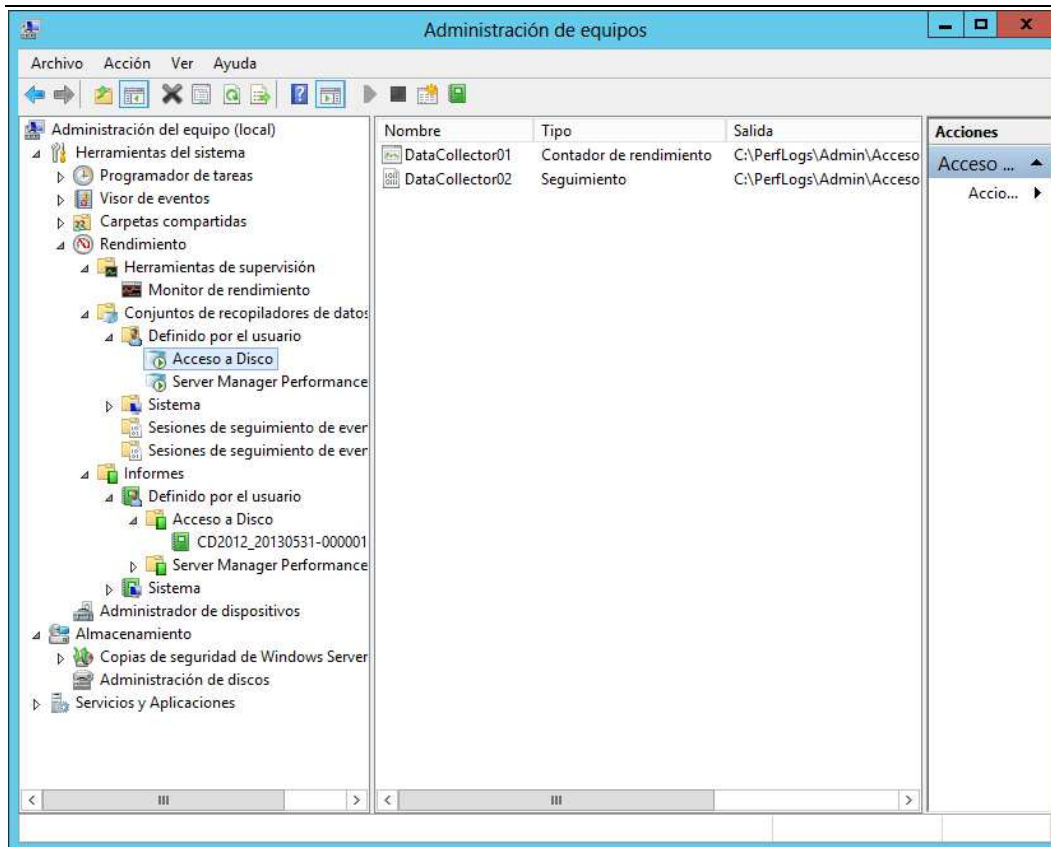
Una vez que esté creado el conjunto de recopiladores, podemos acceder a sus propiedades haciendo clic con el botón secundario del ratón, y establecer algunos parámetros de configuración, como por ejemplo la duración total del registro.



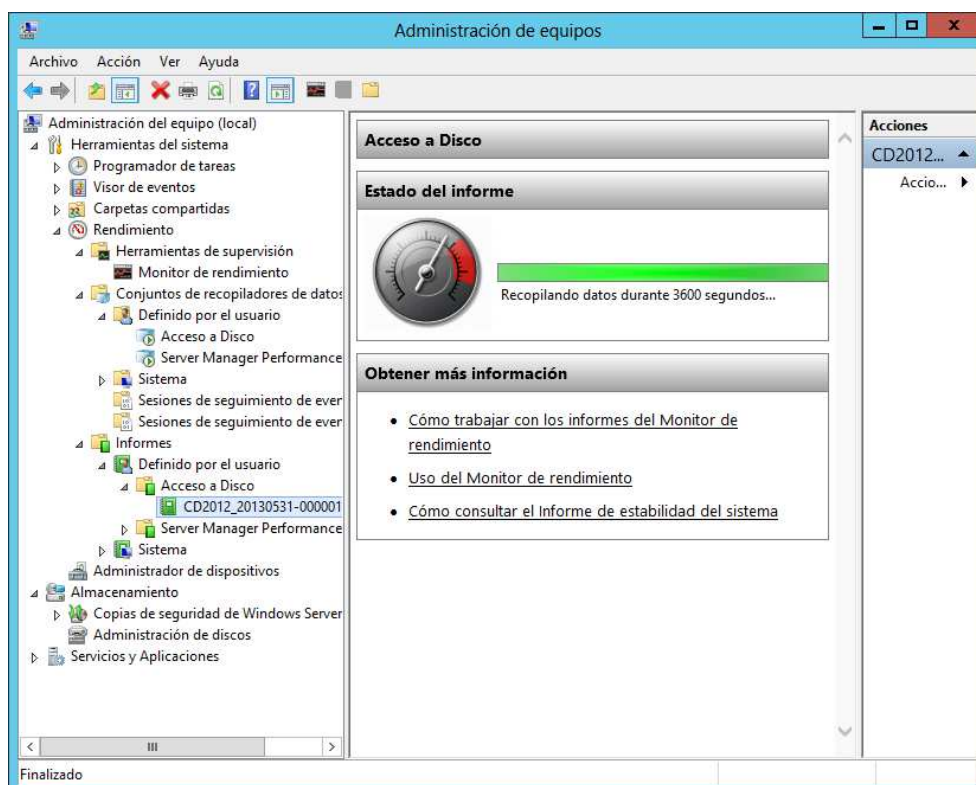
Ahora sólo queda arrancar manualmente el registro de los recopiladores de datos creados.



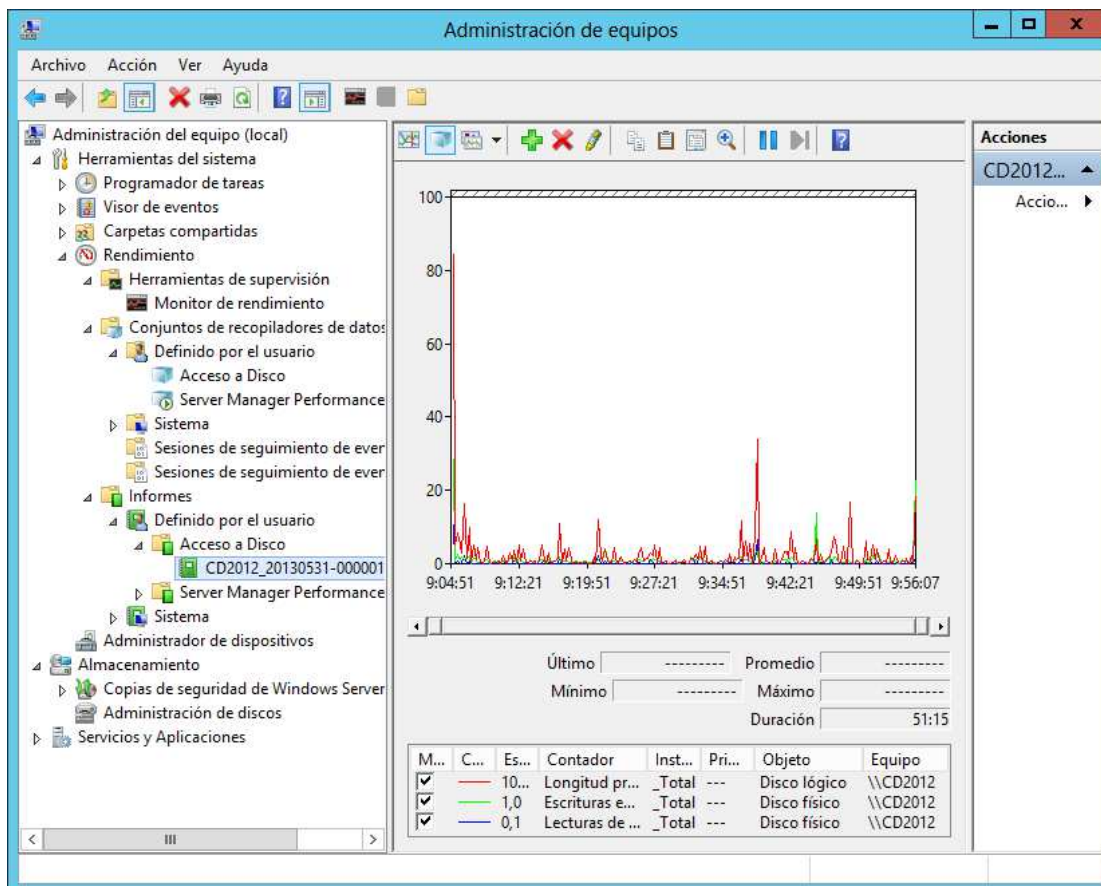
Como podemos ver, el recopilador se encuentra en marcha, y se está generando un registro en la ruta C:\PerfLogs\Admin\Acceso a Disco.



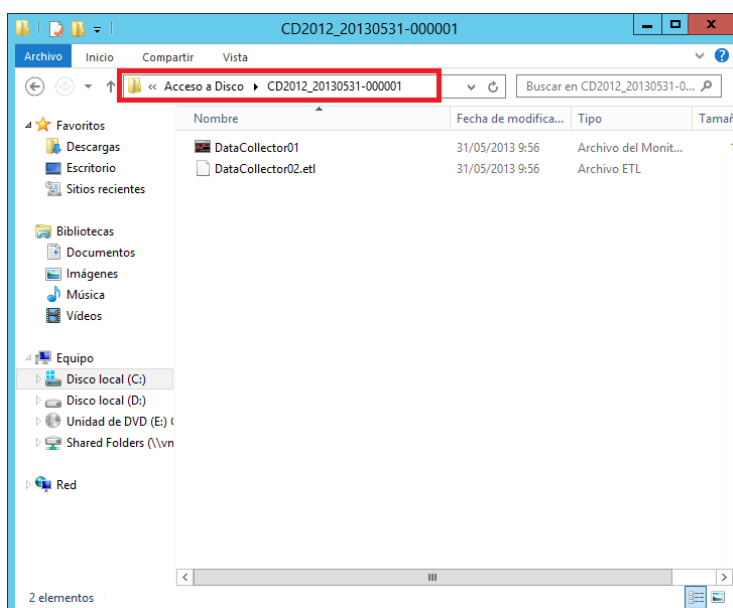
Si vamos al apartado 'Informes', veremos que se ha creado automáticamente una entrada denominada 'Acceso a Disco', que contiene el informe del registro configurado para la máquina. De hecho, como el registro aún está en marcha nos informa de que se están recopilando datos.

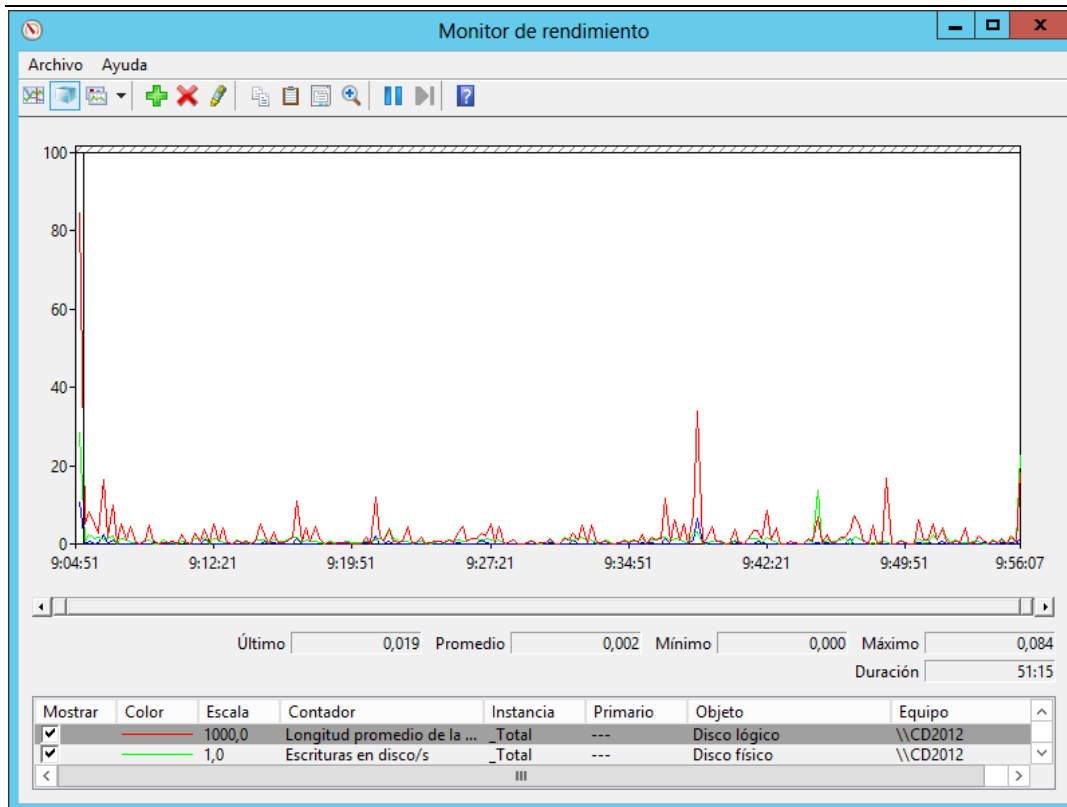


Una vez que haya finalizado el registro (bien porque se haya alcanzado la condición de detención, o bien porque hayamos parado el registro manualmente), podremos comprobar que haciendo doble clic en el informe generado, podemos acceder de manera gráfica a los datos del registro, con los estadísticos correspondientes en la parte inferior.



De una manera alternativa, también podemos buscar el fichero de registro que se ha creado y abrirlo para su análisis.





## Alertas de rendimiento

Durante el proceso de creación del conjunto de recopiladores de datos se nos ha preguntado si deseábamos crear un **Registro de datos** o una **Alerta de contador de rendimiento**.

Básicamente el funcionamiento es similar, la única diferencia es que con las alertas se permite definir contadores de rendimiento y asociarles unas condiciones para emitir avisos cuando un determinado contador alcanza un nivel, por ejemplo cuando la memoria disponible es inferior al 10% de la total.

Crear nuevo conjunto de recopiladores de datos.

¿Qué tipo de datos desea incluir?

☐ Crear registros de datos

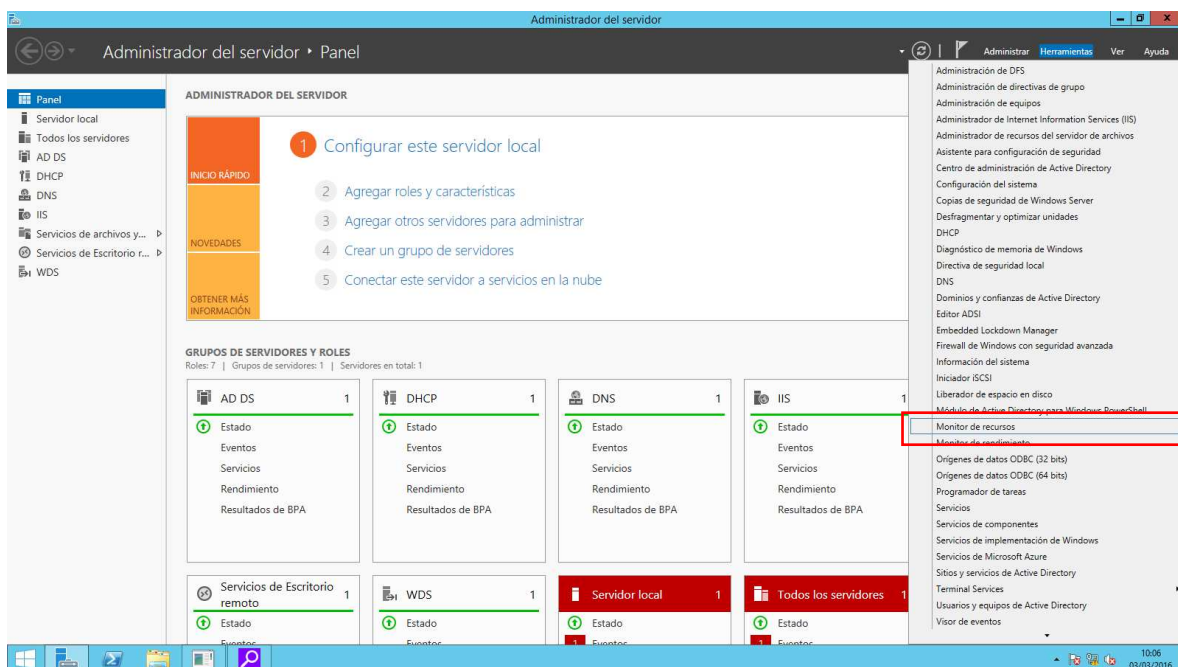
- ☐ Contador de rendimiento
- ☐ Datos de seguimiento de eventos
- ☐ Información de configuración del sistema

☒ Alerta del contador de rendimiento

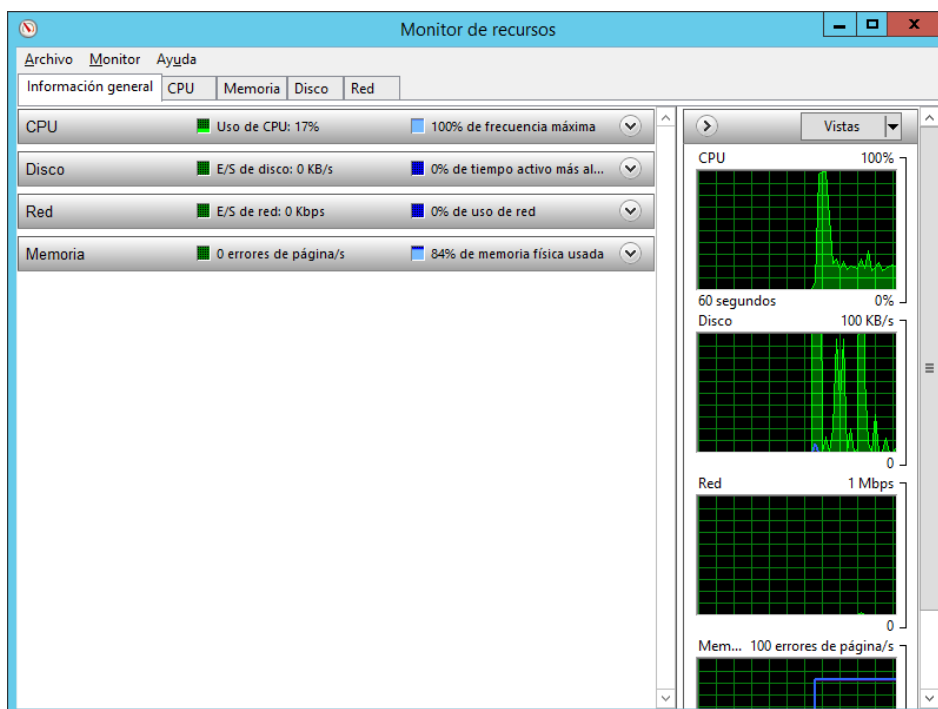
Siguiente Finalizar Cancelar

## 6. Monitor de recursos

Otra consola interesante que nos proporciona Windows para la monitorización del sistema es el **Monitor de Recursos**.

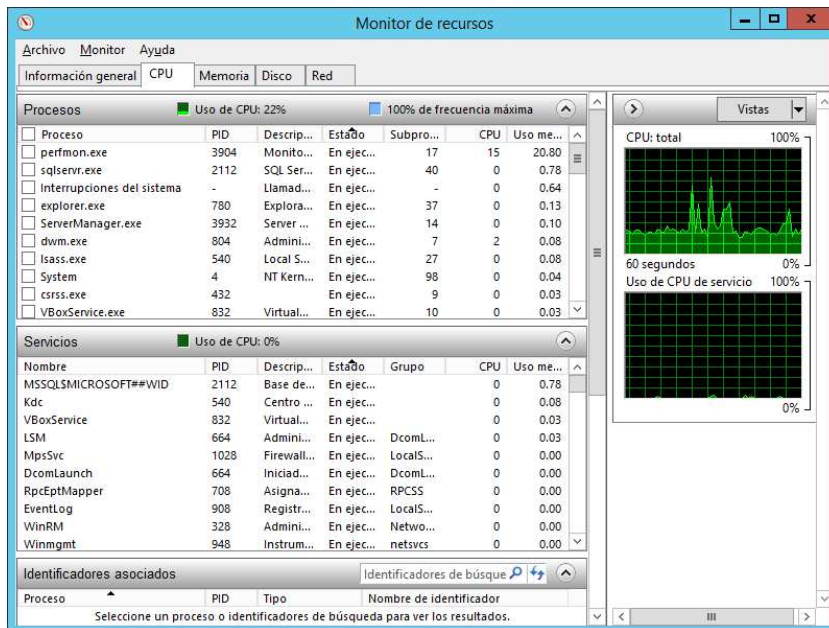


Básicamente nos proporciona información parecida al Administrador de Tareas, con detalles de la utilización de la CPU, Memoria, Disco y Tarjeta de red por parte de los distintos procesos.

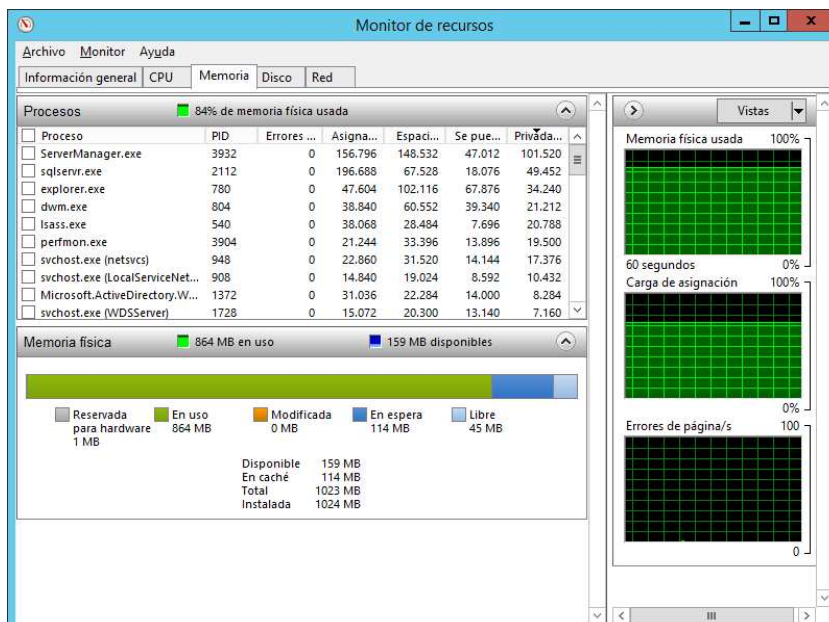




Desde la pestaña CPU podemos ver la actividad de todos los procesos, servicios, e identificadores asociados a cada uno de los procesos. Pudiendo ver el detalle de cada uno de los mismos.



En la pestaña de memoria vemos de manera detallada el uso de la misma por cada uno de los procesos lanzados en el sistema, así como de una manera gráfica el total de la memoria utilizada y disponible.



El funcionamiento es similar en las pestañas de Disco y Red.



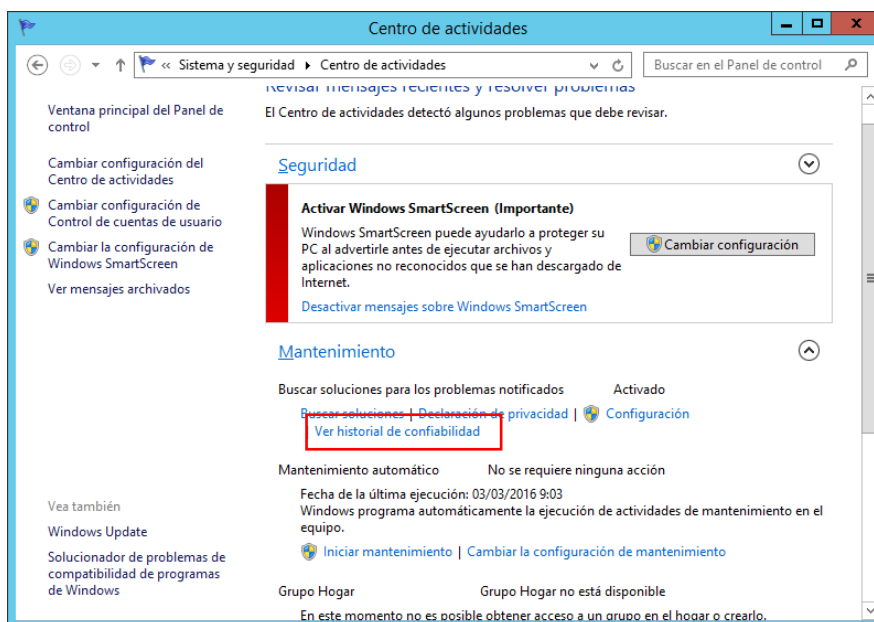
## 7. El monitor de confiabilidad

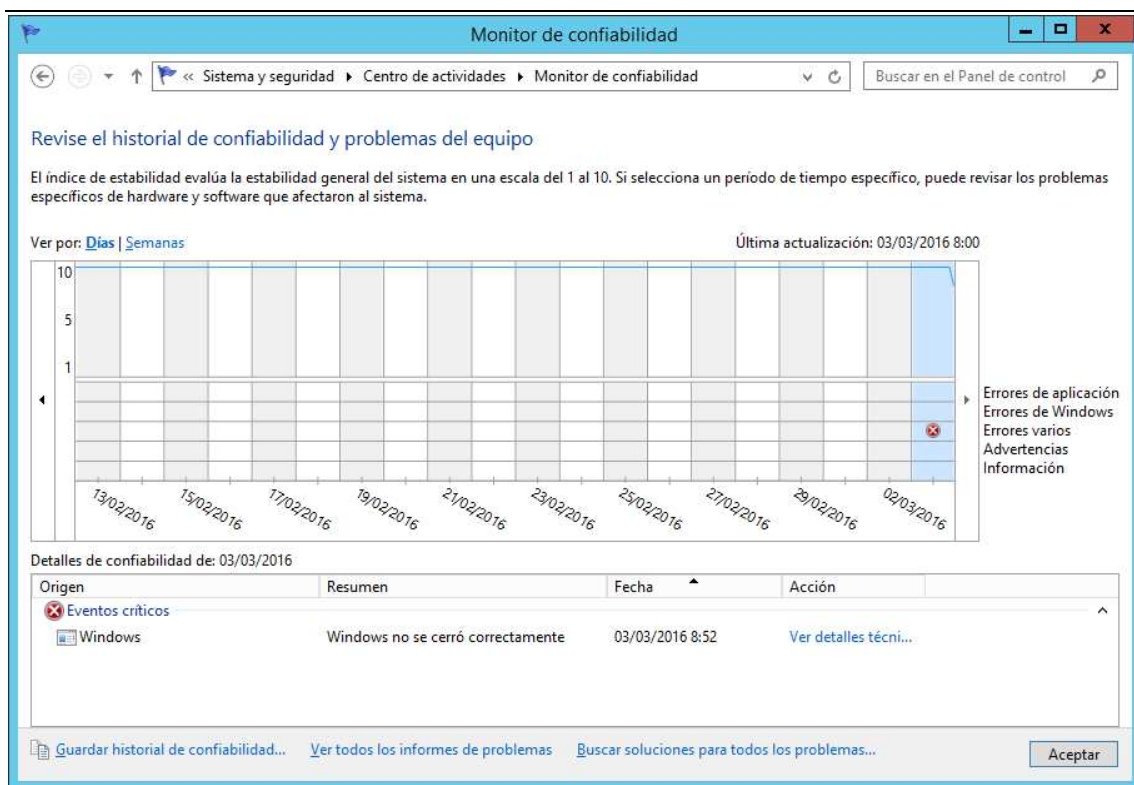
Con Windows Vista, Microsoft introdujo un nuevo complemento para medir el buen funcionamiento del sistema (la confiabilidad).

El complemento Monitor de confiabilidad proporciona una introducción a la estabilidad del sistema y detalles acerca de los eventos que tienen un impacto en la confiabilidad. Calcula el índice de estabilidad mostrado en el Gráfico de estabilidad del sistema durante la vigencia del sistema.

En función de los datos recopilados durante la vida útil del sistema, cada fecha del gráfico de estabilidad del sistema incluye un punto de gráfico que muestra la valoración del índice de estabilidad del sistema de ese día. El índice de estabilidad del sistema es un número que oscila entre 1 (mínima estabilidad) y 10 (máxima estabilidad) y consiste en una medición ponderada calculada sobre el número de errores especificados vistos a lo largo de un período sucesivo. Los eventos de confiabilidad del Informe de estabilidad del sistema describen los errores específicos.

Se accede a él desde el **Centro de Actividades** (al cual se puede acceder también desde el Panel de Control → Sistema y Seguridad).





Los errores recientes tienen un mayor peso que los errores pasados, lo que permite con el tiempo reflejar una mejora en un Índice de estabilidad del sistema ascendente una vez que se ha resuelto un problema de confiabilidad.

Los días en los que el sistema está apagado o en un estado de suspensión no se utilizan para calcular el índice de estabilidad del sistema.

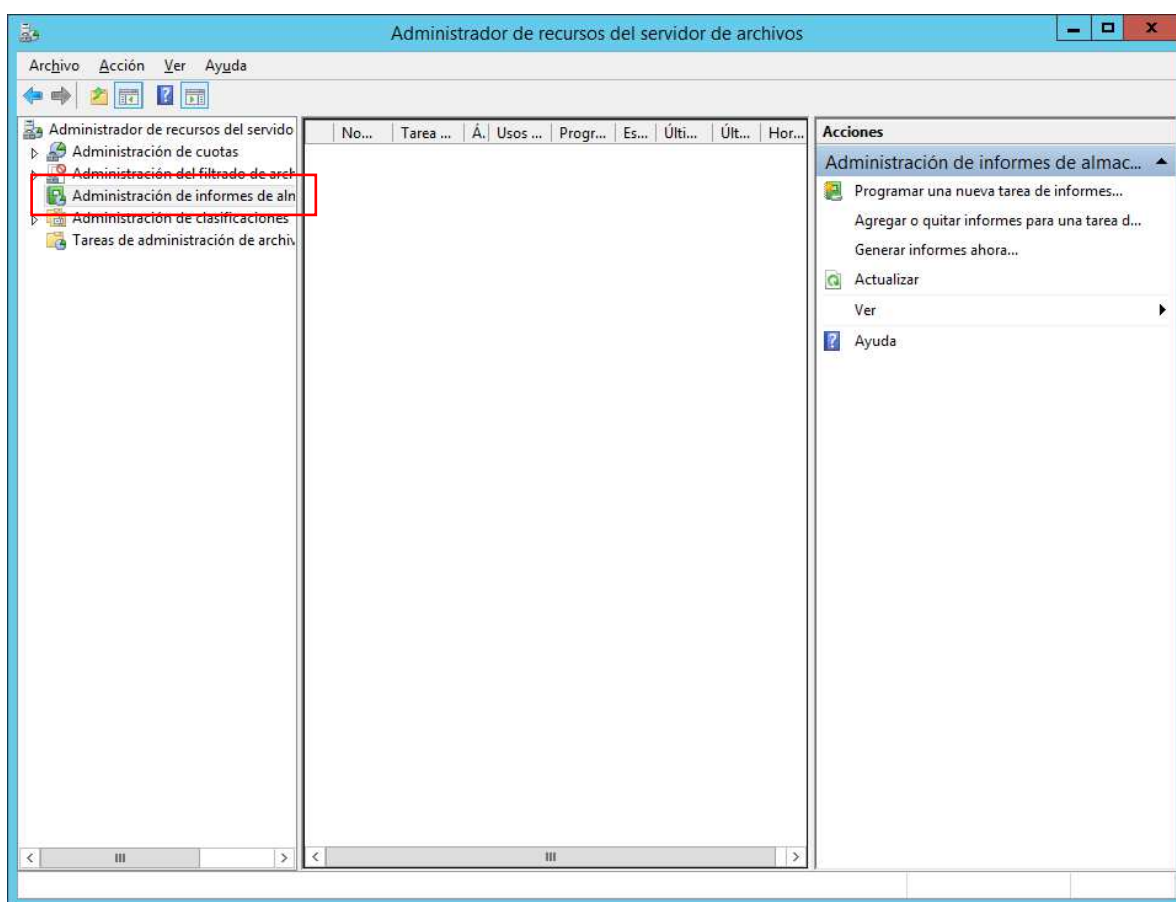
Si no hay suficientes datos para calcular un índice de estabilidad del sistema fijo, la línea del gráfico aparecerá punteada. Cuando se hayan registrado suficientes datos para generar un índice de estabilidad del sistema fijo, la línea del gráfico será sólida.

Si hay algún cambio significativo en la hora del sistema, aparecerá un icono de información en el gráfico para cada día en el que se haya ajustado la hora del sistema.

## 8. Informes de almacenamiento

Windows Server incluye la posibilidad desde varias consolas de generar informes de rendimiento, monitorización, etc. Un informe interesante que se incluye es el de **Almacenamiento**, que nos va a ayudar en la gestión eficiente de los recursos de almacenamiento.

Este informe se encuentra dentro de la consola del **Administrador de recursos del servidor de archivos** (ya vimos cómo instalar esta característica en el tema anterior).



En el nodo **Administración de informes de almacenamiento** de este complemento MMC del Administrador de recursos del servidor de archivos, se pueden realizar las siguientes tareas:

- Programar informes de almacenamiento periódicos que permitan identificar las tendencias de uso de disco.

- Realizar un seguimiento de los intentos de guardar archivos no autorizados para todos los usuarios o para un grupo de usuarios seleccionado.
- Generar informes de almacenamiento inmediatamente.

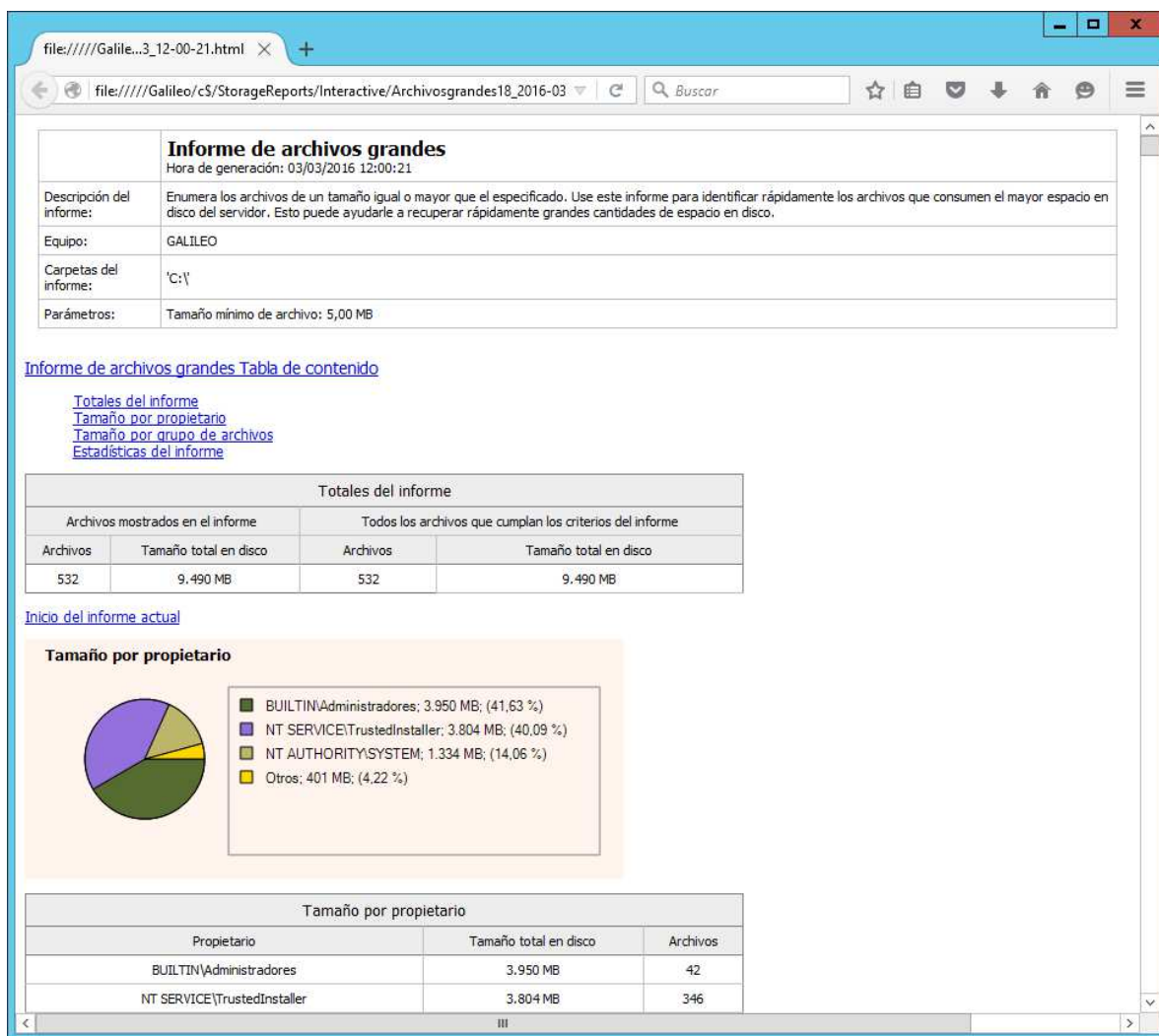
Algunos ejemplos de aplicación práctica de estos informes serían:

- Programar un informe para que se ejecute todos los domingos a medianoche y hacer que se genere una lista que incluya los archivos a los que se ha obtenido acceso más recientemente en los dos últimos días. Con esta información, se puede realizar un seguimiento de la actividad de almacenamiento del fin de semana y planear un período de inactividad del servidor que tenga un menor impacto en los usuarios que se conectan desde su casa los fines de semana.
- Ejecutar un informe en cualquier momento para identificar todos los archivos duplicados de un volumen en un servidor para que el espacio en disco pueda recuperarse rápidamente sin perder ningún dato.
- Ejecutar un informe de archivos por grupo de archivos para identificar cómo se segmentan los recursos de almacenamiento entre distintos grupos de archivos, o bien ejecutar un informe de archivos por propietario para analizar cómo usa cada usuario los recursos de almacenamiento compartido (tamaños, ficheros poco accedidos, duplicados, ...).

Entre las opciones de informes se nos pueden generar estadísticas de:

- Archivos duplicados.
- Archivos grandes.
- Archivos no usados recientemente.
- Archivos por grupos de archivo.
- Archivos por propiedad.
- Archivos por propietario.
- Archivos usados recientemente.
- Auditoría de filtrado de archivos.
- Carpetas por propiedad.
- Uso de cuotas.

El informe nos lo puede generar en varios formatos. La opción por defecto es la de DHTML el cual podemos visualizarlo mediante un navegador.



## 9. El rastreador de eventos de apagado

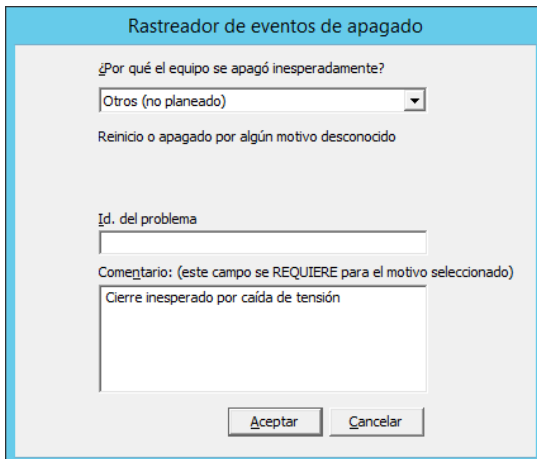
El Rastreador de eventos de apagado es una herramienta que solicita a los usuarios que registren un motivo que indique lo que les ha llevado a reiniciar o apagar el equipo. Esta información queda disponible para que pueda ser revisada en el registro de eventos. Si un equipo que ejecuta Windows 7 está conectado a un dominio que utiliza herramientas de supervisión se puede recopilar esta información como parte de los informes de red.

Cuando el Rastreador de eventos de apagado está habilitado, los usuarios no pueden apagar ni reiniciar el equipo sin proporcionar un motivo. Si el equipo se apaga o reinicia de manera inesperada, bien como resultado de una interrupción de la alimentación o un

error de hardware, al usuario se le solicita que especifique un motivo en el Rastreador de eventos de apagado cuando el equipo se vuelva a iniciar.

### **Reinicios y apagados "esperados" e "inesperados"**

Cuando está habilitado el Rastreador de eventos de apagado, al hacer clic en Inicio y, después, en Apagar, o al presionar ALT+F4 en el escritorio, o CTRL+ALT+SUPR, y hacer clic en Apagar o Reiniciar, aparece el cuadro de diálogo de apagado "esperado". A continuación, se muestra un paso en el proceso de apagado en el que se solicita que proporcione un motivo y un comentario que expliquen la acción. Los reinicios o apagados esperados proporcionan al sistema operativo tiempo para completar sus rutinas de cierre habituales. Por el contrario, el equipo no puede anticipar un reinicio o apagado "inesperado". Si el Rastreador de eventos de apagado está habilitado, se muestra el cuadro de diálogo de apagado inesperado a la primera persona miembro del grupo local Usuarios que inicie sesión en el equipo después del reinicio o apagado. Al igual que el cuadro de diálogo de apagado esperado, solicita al usuario que proporcione un motivo y un comentario.



### **Reinicios y apagados planeados y no planeados**

Un reinicio o apagado esperado puede ser planeado o no planeado. Cuando controla la temporización de un reinicio o apagado, la tarea está planeada. Por ejemplo, el departamento de sistemas puede reservar una hora específica para instalar aplicaciones nuevas en el servidor. Por el contrario, los reinicios o apagados no planeados nos obligan a realizar la tarea inmediatamente. Por ejemplo, una aplicación que no responde puede obligarnos repentinamente a reiniciar el equipo.

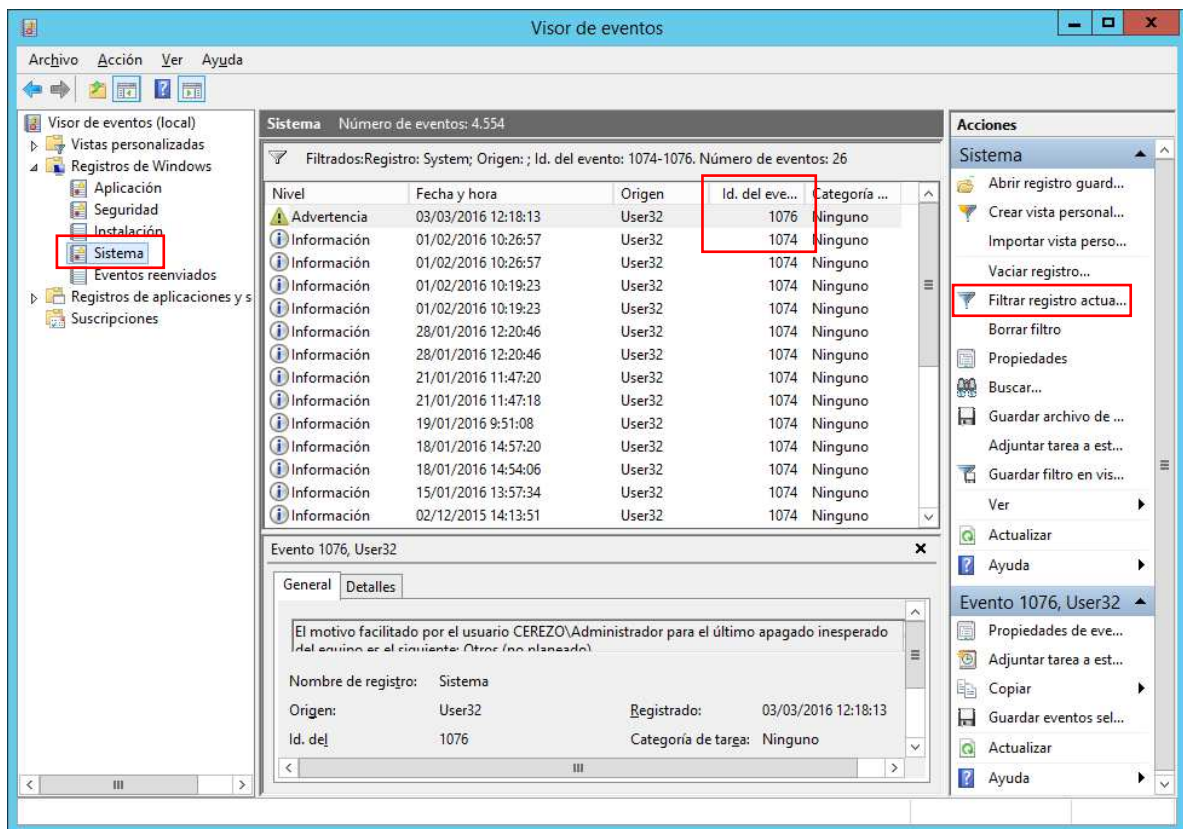
### **Reinicios y apagados locales y remotos**



Se puede usar el Rastreador de eventos de apagado y la herramienta de línea de comandos *Shutdown.exe* para reiniciar o apagar un equipo local y uno o más equipos remotos. Además, los profesionales de tecnologías de la información pueden realizar un gran número de anotaciones remotas de apagados inesperados, una alternativa a la larga tarea de registrarse en cada equipo para registrar el motivo de un apagado inesperado.

Una vez habilitado (en Windows Server lo está por defecto) el rastreador de eventos de apagado en las directivas de grupo, podemos visualizar los motivos de apagado desde el visor de eventos.

Para visualizar el motivo del apagado habría que ir al **Visor de Eventos** y comprobar los registros de Windows dentro de la carpeta **Sistema**.



Creamos un filtro para indicarle que sólo deseamos los eventos cuyo ID sea 1074 o 1076, que son los que indican los motivos de cierre del sistema (esperados e inesperados).



Y visualizamos el detalle del evento.

## 10. Directivas de auditoría

En este punto vamos a ver un aspecto que nada tiene que ver con la monitorización del rendimiento, pero que está ligado a la supervisión del buen funcionamiento del sistema, en este caso a la auditoría de los registros de seguridad generados por el sistema operativo.

A veces, debido a una mala configuración de los permisos y derechos, o a una violación de la confidencialidad por parte de un usuario autorizado, es necesario averiguar cómo se ha producido una infracción de seguridad en el sistema.

En Windows, una de las maneras de saber una vez que ha sucedido y cómo se ha producido esa infracción de seguridad es mediante el uso de las auditorías, es decir, mediante la revisión de las actividades que han supuesto la infracción.

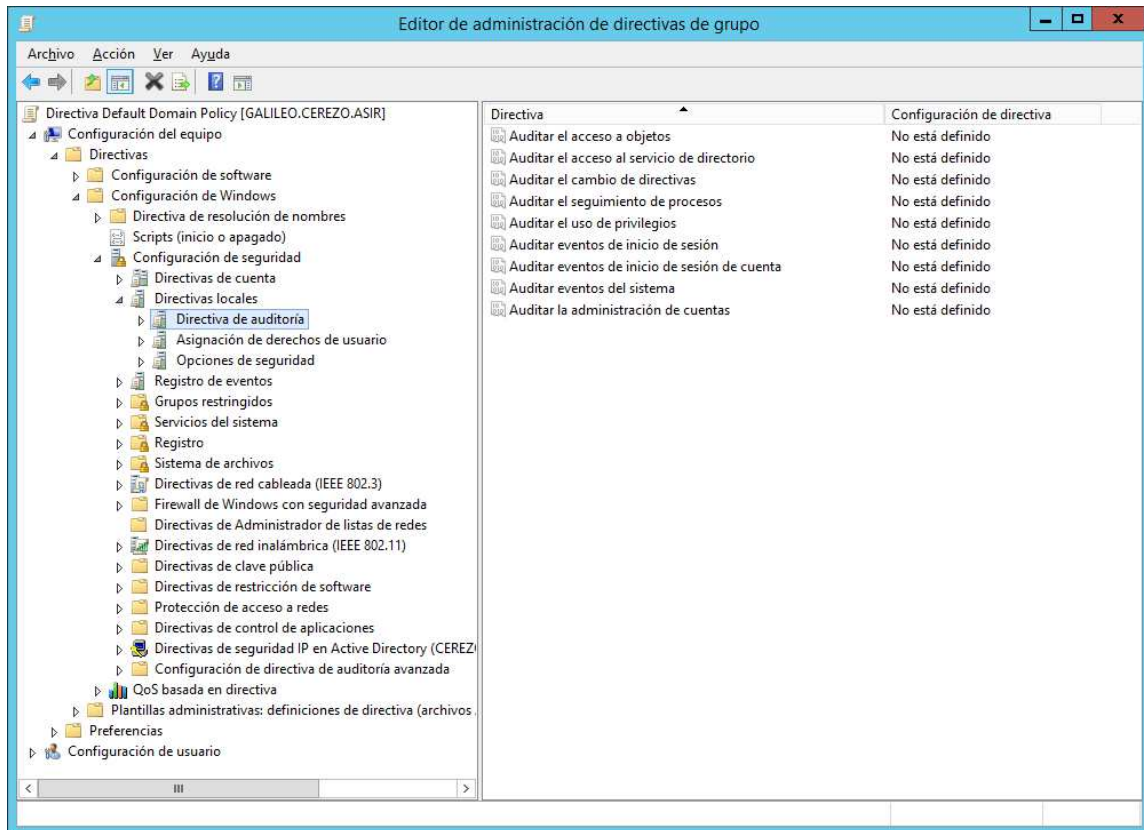
Un registro de auditoría registrará una entrada siempre que los usuarios realicen determinadas acciones que se especifiquen. Por ejemplo, la modificación de un archivo o una directiva puede desencadenar una entrada de auditoría. La entrada de auditoría muestra la acción que se ha llevado a cabo, la cuenta de usuario asociada y la fecha y hora de la acción. Se puede auditar tanto los intentos correctos como incorrectos (si no se ha podido hacer por tener permiso denegado) en las acciones.

La auditoría de seguridad es extremadamente importante para cualquier sistema empresarial, ya que los registros de auditoría puede que den la única indicación de que se ha producido una infracción de seguridad. Si se descubre la infracción de cualquier otra forma, la configuración de auditoría adecuada generará un registro de auditoría que contenga información importante sobre la infracción.

A menudo, los registros de errores son mucho más informativos que los registros de aciertos, ya que los errores suelen indicar problemas. Por ejemplo, si un usuario inicia sesión correctamente en el sistema, puede considerarse como algo normal. Sin embargo, si un usuario intenta sin éxito iniciar sesión en un sistema varias veces, esto puede indicar que alguien está intentando obtener acceso al sistema utilizando el Id. de usuario de otra persona. El registro de seguridad registra sucesos de auditoría. El contenedor de registro de sucesos de directiva de grupo se utiliza para definir atributos relacionados con la aplicación, la seguridad y los registros de sucesos del sistema como, por ejemplo, el tamaño máximo del registro, los derechos de acceso para los registros, así como la configuración y los métodos de retención.

Para activar las auditorías nos vamos al **Editor de Directivas de Grupo**. Desde ahí, en las directivas del Dominio (o en donde nos interese controlar) accedemos a la rama de

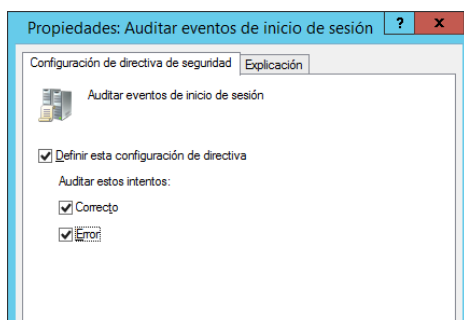
Configuración de Equipo, Configuración de Windows, Configuración de Seguridad, Directivas locales, Directivas de auditoría.



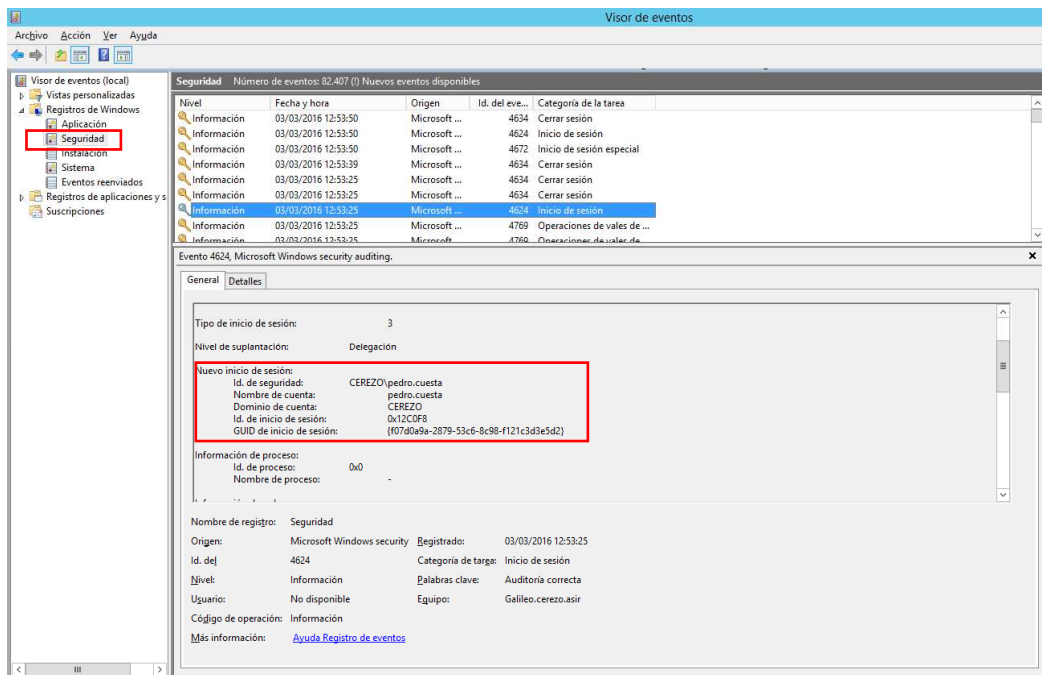
Desde esa consola se puede indicar qué acciones del sistema queremos auditar, desde los accesos a ficheros y carpetas, a los servicios de directorio, inicios de sesión, gestión de cuentas de usuarios, cambio de directivas, etc.

De este modo quedarán registrados en el sistema quiénes han intentado (con éxito o sin él) realizar la acción del sistema indicada.

En el caso del inicio de sesión basta con indicar si deseamos indicar los intentos correctos, incorrectos (fallos de usuario o contraseña) o ambos.

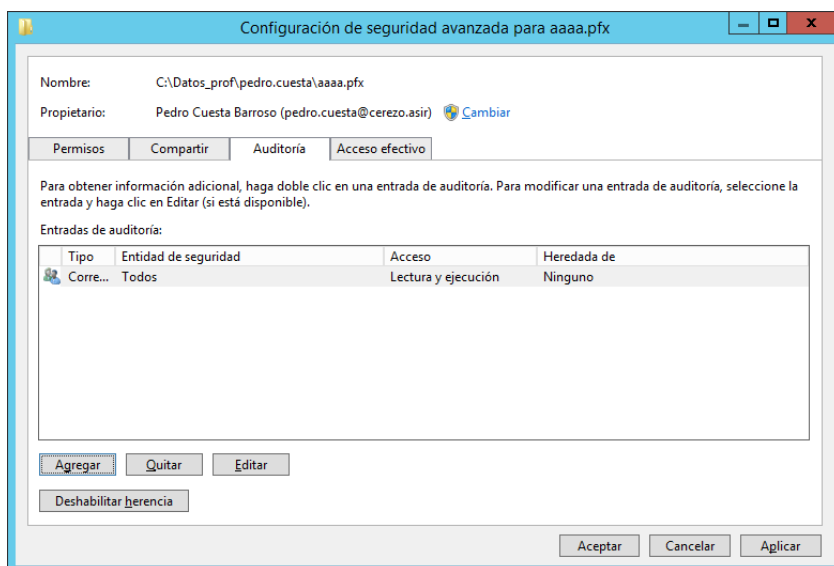


Accediendo al Visor de Eventos, en la rama de Seguridad, comprobamos el detalle del evento registrado.



En el caso de la auditoría de acceso a objetos, además de activarla desde la consola de edición de directivas, hay que activar en el objeto a auditar el evento que deseamos controlar y sobre quiénes deseamos auditar.

En el siguiente ejemplo accedemos a las propiedades de un fichero y en la pestaña **Seguridad** editamos las opciones avanzadas y accedemos a la pestaña de **Auditoría** para seleccionar sobre qué usuarios o grupos de usuarios y sobre qué acciones deseamos auditar el objeto.



---

Material elaborado a partir de:

- Página web Technet de Microsoft.
- Apuntes del curso del CEFIRE de Administración Centralizada de Redes con Windows 2012 Server del profesor José Ramón Ruiz Rodríguez bajo licencia de Creative Commons Reconocimiento-NoComercial 4.0 Internacional:



- Elaboración propia.