Windows Server Monitoring

Transcribed on August 5, 2025 at 3:38 PM by Minutes AI

Speaker 1 (00:09)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la monitorización en Windows Server.

Vamos a hablar de qué herramientas tenemos para poder monitorizar el sistema operativo.

Hablaremos del administrador de tareas, del monitor de recursos, del monitor de rendimiento y del monitor de confiabilidad.

Windows Server nos ofrece varias herramientas para monitorizar procesos, servicios y aplicaciones.

Nos va a permitir de esta manera detectar problemas con componentes que no estén trabajando correctamente o incluso podemos detectar actividades inusuales o diferentes problemas que puedan estar asociados al funcionamiento de un determinado rol o de un determinado servicio.

Con estas herramientas podemos analizar el correcto comportamiento del sistema operativo y podemos detectar diferentes tipos de conflictos en el funcionamiento de servicios o aplicaciones.

La primera herramienta que tenemos para monitorizar el sistema operativo es el Administrador de tareas.

El administrador de tareas nos va a ofrecer una vista previa, una visión preliminar de lo que está sucediendo en el dispositivo.

Lo primero que hacemos cuando notamos que un programa, que una aplicación, que un servicio o que el propio sistema operativo no funciona correctamente es lanzar el administrador de tareas y ver qué aplicaciones están ejecutándose, los procesos relacionados con esas aplicaciones, cómo están los recursos desaturados y si tenemos un cuello de botella asociado a un determinado componente como pueda ser la CPU, la memoria RAM, proceso de escritura en disco.

Para poder ejecutar el administrador de tareas podemos hacerlo con la combinación Control al del o podemos hacerlo por ejemplo con botón derecho sobre la barra Detalles.

Se va a dividir en diferentes secciones para clasificar la información y ayudarnos a tener una vista más detallada de lo que está sucediendo.

Otra herramienta que sirve para la monitorización del sistema operativo es el Monitor de recursos.

El Monitor de recursos es una excelente herramienta para detectar cuellos de botella.

Vamos a tener una serie de gráficos asociados a la carga de trabajo de la CPU, del disco, de la parte de red o de la parte de memoria.

Esta herramienta nos va a indicar rápidamente aquellos procesos que están incidiendo con una carga masiva sobre un determinado componente.

Esto puede ayudarnos a detectar componentes que a lo mejor están funcionando mal, procesos relacionados con aplicaciones o servicios que no están funcionando correctamente o también puede ayudarnos como indicativo de que una determinada aplicación, un determinado rol o un determinado servicio que tenemos funcionando en un dispositivo requiere de una potencia superior para funcionar correctamente.

Es decir, que yo puedo instalar un determinado rol que me va a consumir todos los recursos, por ejemplo, en la parte de memoria RAM.

Entonces, para optimizar el funcionamiento de ese determinado rol, pues a lo mejor lo adecuado es incrementar o aumentar la potencia del hardware y aumentar la capacidad de RAM del dispositivo.

Luego tenemos el monitor de rendimiento.

El monitor de rendimiento que se puede ejecutar con la palabra PEFMO en el menú de inicio y va a generar una serie de informes, una serie de estadísticas sobre el funcionamiento de unos determinados componentes basándose en una serie de contadores de rendimiento.

Windows Server utiliza diferentes recopiladores de datos basados en el valor en un instante de tiempo por segundo, en un total desde el último inicio de sesión, desde el último arranque del sistema, un intervalo de tiempo o el último valor específico sobre un determinado componente o un valor mínimo o máximo determinado asociado a un componente.

El monitor de rendimiento va a trabajar con unos recopiladores de datos llamados Data Collector Set que van a almacenar información relacionada con el funcionamiento de una serie de componentes o de una serie de elementos.

Además, estos recopiladores de datos después nos van a proporcionar un informe que nosotros podemos almacenar para tener una serie de registros sobre el funcionamiento de determinados componentes.

Una de las verdaderas maravillas de esta herramienta es que nosotros podemos generar nuestros propios recopiladores de datos.

Esto lo que va a hacer es que nos va a permitir ser muy específicos a la hora de monitorizar componentes o parte del funcionamiento de componentes del propio sistema operativo o las aplicaciones.

Entonces nos va a permitir decidir exactamente qué queremos monitorizar y podemos decidir también cuándo podemos monitorizarlo y qué partes de esa aplicación, de ese servicio o de ese componente queremos monitorizar.

Todo ello nos va a servir además generando una serie de informes que nosotros después los podemos utilizar para llevar unas estadísticas o montar unas líneas bases del funcionamiento de esos elementos.

Dentro del monitor de rendimiento tenemos otro elemento que es más desconocido que es el monitor de confiabilidad.

El monitor de confiabilidad lo que va a hacer es generar una línea base con la estabilidad del sistema operativo con un valor entre 1 y 10, teniendo en cuenta que 10 sería los niveles más estables y uno sería el nivel más inestable.

A lo largo del tiempo, el sistema operativo va a ir realizando una serie de comprobaciones, una serie de pruebas que van a ir añadiendo estos índices de estabilidad al monitor de confiabilidad.

¿Cuál es la ventaja que tiene esta herramienta?

Que nosotros con esta herramienta, una de las cosas que vamos a poder detectar es aquellos elementos que han generado inestabilidad en el sistema, aunque a lo mejor a nosotros nos hayan pasado desapercibidos.

Es decir, yo puedo empezar a notar que funciona mal el dispositivo, el equipo, y cuando voy al monitor de confiabilidad veo que empieza a haber caídas en el gráfico, que empieza a haber inestabilidad en el sistema desde hace una semana y lo voy a tener asociado a una determinada hora y a un determinado día.

Cuándo empiezan esos picos, cuando empiezan esas caídas.

Entonces puedo asociar esa fecha o esa hora a la instalación de una actualización, a la instalación de un driver, a una determinada aplicación que he instalado ya que ha comenzado a funcionar en ese momento y entonces podemos detectar el origen de un problema que nosotros en un principio nos ha ido generando inestabilidad en el sistema, pero a lo mejor no lo llegamos a notar y cuando lo llegamos a notar ha pasado tiempo y no es fácil detectar cuál es el origen de ese problema.

Estamos en la máquina virtual, lo primero que vamos a hacer es lanzar el administrador de tareas.

Vamos a la parte de más detalles y el administrador de tareas lo primero que nos enseña es una visión general de las aplicaciones que se están ejecutando en el dispositivo.

Y después vamos a tener una serie de relaciones con las aplicaciones y aquellos elementos que están relacionados con cada una de las aplicaciones.

Tendríamos también la posibilidad de ir a la parte de rendimiento, donde vamos a poder ver el impacto que está teniendo el funcionamiento del dispositivo, tanto en la parte de red, como la parte de memoria, como la parte de procesador.

Y desde aquí otra de las cosas que podemos hacer es que podemos lanzar el propio monitor de recursos.

Si lanzamos el monitor de recursos vamos a tener una herramienta que es muy interesante para detectar rápidamente cuellos de botella en un determinado dispositivo.

Vamos a poder ver la carga de trabajo que tenemos y cómo está impactando en el hardware del dispositivo.

Vemos que tenemos por ejemplo aquí poca carga de trabajo en la parte de red, poca carga de trabajo en la parte de la memoria, pero sí que tenemos algo de carga de trabajo en el disco y algo de carga de trabajo en la CP.

Si nos vamos a la parte del disco, podemos ordenar la carga de trabajo de mayor a menor o viceversa y podemos seleccionar un determinado proceso y automáticamente nos lo va a marcar con una línea diferente, con lo cual tendremos un gráfico general de toda la carga de trabajo y luego tenemos una línea específica en ese gráfico de aquel proceso a aquellos procesos que nosotros hemos seleccionado.

Incluso podríamos seguir la actividad de ese proceso en la parte de red, en la parte de memoria o en la parte de CPU para ver qué impacto tiene ese determinado proceso dentro de la carga de trabajo de los diferentes componentes.

El monitor de recursos no tiene mucho más, pero es una herramienta que es interesante para detectar rápidamente cuellos de botella.

El administrador de tareas va a tener otra parte aquí en lo que sería la parte de usuarios, donde tendremos información sobre los procesos relacionados con el uso de un determinado usuario.

Tendríamos aquí la parte de servicios, donde vamos a tener información sobre los servicios que se están ejecutando en el servidor y si vamos a la parte de servicios abiertos, vamos a la parte de servicios.

Desde aquí podemos lanzar la consola de servicios que vamos a tener información mucho más detallada de todo el funcionamiento de la parte de servicios.

En la consola de servicios vamos a tener información sobre la descripción de todos los servicios, el tipo de status, es decir, si se está ejecutando, la manera que tiene de ejecución, es decir, si se inicia de forma automática, se inicia de forma manual, se inicia de forma automática pero tiene un inicio retrasado para tener menos impacto en el arranque del dispositivo y también cuál es la cuenta que se utiliza para ese determinado servicio, si se está ejecutando como localización, como network service, como local service, etc.

Finalmente, dentro de lo que sería la parte del administrador de tareas, lo siguiente que vamos a tener es la parte de detalles, que quizás es la parte más interesante.

En la parte de detalles nosotros vamos a tener todos los procesos que se están ejecutando y podemos seleccionar cualquiera de estos procesos.

Podríamos finalizar el proceso o podríamos terminar el árbol del proceso, es decir, todos los procesos relacionados relacionados con ese determinado proceso.

Podemos ver la prioridad a la que se ejecuta el proceso, podemos analizar la cadena de espera, es decir, que podemos ver si ese proceso está esperando para su funcionamiento que otros procesos terminen una determinada ejecución.

Podríamos hacer un volcado de memoria de ese proceso de tal forma que después podríamos analizarlo con otras herramientas.

Podríamos abrir la localización del proceso.

Esto puede ser interesante porque cuando nosotros abrimos la localización del proceso o de la imagen o el archivo que lanzó ese proceso, podemos detectar si ese proceso o esa imagen o ese software está en una ubicación extraña.

Entonces si algo que tiene que estar en System está en archivos de programa, pues algo está sucediendo ahí.

Si algo que está en archivos de programa está en una carpeta, en una ubicación diferente, pues algo extraño está sucediendo con ese determinado proceso.

Puede ser el indicativo de un programa no autorizado o de un malware que está tratando de pasar desapercibido haciéndose pasar por otro determinado elemento.

Y después podemos ir a la parte de propiedades.

Dentro de la parte de propiedades nosotros vamos a tener información sobre ese determinado proceso, vamos a tener la posibilidad de ver la firma digital de ese proceso y vamos a poder ver el certificado digital asociado a ese proceso, de tal forma que nosotros podemos verificar si el fabricante que ha firmado digitalmente como certificado digital esa ISO, esa ejecutable, esa DLL, tiene un certificado digital válido que nos va a asegurar que ese fabricante es realmente el que ha decidido o el que ha firmado ese software que

Una de las cosas que es más interesante dentro del administrador de tareas es que si nosotros nos vamos a la parte de seleccionar columnas, en la parte de seleccionar columnas vamos a tener mucha información que el monitor de tareas está recopilando pero que no nos muestra en la consola por defecto.

Entonces hay por ejemplo elementos como el identificador de sesión, elementos por ejemplo en lo que se refiere a la parte del uso de la memoria, fallos de página, deltas de fallos de página, una serie de elementos que nos pueden ayudar a depurar fallos cuando estamos comprobando una determinada aplicación, cómo funciona una aplicación, también los manejadores, los diferentes hilos, procesos de escritura, de lectura y después una serie de tecnologías que están relacionadas directamente con los temas de seguridad.

Por ejemplo podemos ver si el proceso respeta la virtualización del control de cuentas de usuario, o si se está ejecutando con privilegios elevados o si tiene habilitado del el contexto donde se está ejecutando, la memoria dedicada, la memoria compartida o por ejemplo si utiliza Control Flow Guard.

Entonces si un proceso tiene todas estas tecnologías o está utilizando todas estas tecnologías, pues vamos a saber si es más fácil o más difícil que ese proceso sea un proceso legítimo, si ese proceso puede haber sido atacado, si puede haber un malware que está ejecutándose dentro de ese proceso, entonces tendríamos una información bastante interesante de lo que sucede o lo que se está ejecutando dentro del sistema operativo.

Si nos vamos a la parte de Tools, en la parte de Tools nosotros vamos a tener aquí el visor de eventos, vamos a tener aquí el monitor de recursos y tenemos aquí también el monitor de rendimiento.

El monitor de rendimiento es una herramienta muy interesante, pero antes de ver el monitor de rendimiento, si damos botón derecho y vamos aquí a la parte de ver la confiabilidad del sistema, vamos a tener el monitor de confiabilidad.

El monitor de confiabilidad es esta herramienta que yo os estaba comentando que nos va a marcar un índice de estabilidad entre el 1 y el 10, indicándonos aquellos elementos que pueden producir inestabilidad en el sistema.

Esta máquina virtual es una máquina virtual nueva, por lo tanto tiene muy poco recorrido en el gráfico y además tiene un recorrido totalmente estable.

Aunque tenemos aquí un warning, si seleccionamos este elemento tendríamos información aquí sobre una serie de advertencias o una serie de información que la herramienta nos está indicando.

Esta herramienta si nosotros generáramos alguna incoherencia, alguna inestabilidad en el sistema, automáticamente nos la mostraría en el gráfico asociada a una hora y además según el tipo de error que sea en un momento determinado incluso podría darnos indicativos de posibles soluciones para el problema o el error que ha detectado.

Dentro del monitor de rendimiento nosotros vamos a tener aquí los recopiladores de datos y dentro de la parte de recopiladores de datos en la parte de sistema vamos a tener por un lado lo que sería el diagnóstico de sistema y vamos a tener otro lado lo que sería el diagnóstico de rendimiento.

Si nosotros ejecutamos el recopilador de datos, el recopilador de datos y nos vamos a la parte de informes, vemos que nos genera un informe y que además lo que está haciendo es que nos dice que está recopilando datos por un periodo de 60 segundos.

Vamos a esperar a que termine de recopilar los datos.

Una vez que termina de recopilar los datos nos va a generar un informe y si nosotros vamos a ver el informe vamos a ver que tenemos muchísima información, en este caso sobre muchísimos componentes del sistema, de la parte de la CPU, vamos a tener muchísima información sobre la parte de componentes y así con cada uno de estos elementos.

En la parte de servicios también tendríamos muchísima información sobre el rendimiento.

Tendríamos aquí información detallada sobre diferentes servicios en la parte del sistema, en la parte de red, dentro de la parte de red fijaros la cantidad de categorías diferentes que tenemos y la información que recopila de cada una de las categorías IP, TCP, UDP.

Luego tendríamos la parte de disco también con diferentes categorías, por ejemplo la parte de disco físico y luego tendríamos aquí la parte de memoria, la parte de procesos y después informes estadísticos, tendríamos aquí informes estadísticos finalmente en el informe que nos genera del sistema de rendimiento.

Pero en muchos casos nosotros no queremos toda esta información sino que queremos una información mucho más específica que se adapta a nuestras necesidades.

Entonces una de las cosas que nosotros podemos hacer es que podemos generar nuestros propios recopiladores de datos.

Entonces yo voy a crearlo de forma manual, doy a siguiente, voy a crear, podría crear una alerta, pero voy a crear un recopilador de datos que podría ser para rastrear los datos para la configuración del sistema, información de la configuración del sistema o un contador de rendimiento.

Voy a la parte de contador de rendimiento y aquí es donde tenemos la verdadera potencia que tiene esta herramienta.

Yo puedo seleccionar aquí cualquier elemento, es decir que yo puedo coger el procesador, seleccionar el procesador y decir que me recopile información total del procesador o puedo seleccionar y puedo desplegar el procesador y seleccionar aquellos elementos específicos del procesador que yo quiero.

Entonces yo despliego aquí y voy a ver que me interesa una serie de elementos específicos dentro del funcionamiento del procesador, que no tiene por qué ser todos los elementos relacionados con el procesador.

Podríamos seleccionar un recopilador de datos que sólo tomará información del procesador o que tomará información de diferentes partes del procesador o de la memoria RAM, que tomará datos de diferentes partes de la memoria RAM, pero también podemos hacer que nos muestre información sobre diferentes componentes.

Entonces yo por ejemplo podría venir aquí a la parte de memoria y dentro de la parte de memoria lo mismo, podría seleccionar que me recopilará datos de toda la memoria o puedo recopilar datos específicos de aquellos componentes de la memoria que a mí me puedan interesar, entonces podría venir aquí por ejemplo los fallos de página por segundo, las páginas por segundo, entonces puedo ir seleccionando aquellos elementos que me interesan y específicamente recopilar datos sobre esos elementos.

Tendríamos por ejemplo muchísimas categorías diferentes, por ejemplo, por ejemplo NetLogo, adaptadores de red.

Dentro de los adaptadores de red veis que tenemos diferente información que podemos capturar.

Entonces esta herramienta nos permite generar todos estos recopiladores de datos y hacer que estos recopiladores de datos sean muy generales o muy específicos, pero sobre todo que se adapten exactamente a lo que nosotros queremos.

Un elemento que es importante es el intervalo de recopilación de datos.

Nosotros por defecto nos marca 15 segundos.

Si yo voy a generar un recopilador de datos que va a estar activo una hora, puede ser interesante que tome muestras cada 15 segundos, pero si yo voy a hacer un recopilador de datos y ese recopilador de datos va a estar recopilando datos, va a estar ejecutándose durante un minuto o durante 30 segundos.

Si pongo cada 15 segundos realmente sólo va a tomar dos muestreos o solo va a tomar cuatro muestreos.

Entonces cuando vamos a utilizar recopiladores de datos que se van a ejecutar por un periodo de tiempo pequeño, tendremos que poner un intervalo muy pequeño.

Cuando nosotros vamos a utilizar recopiladores de datos que van a estar monitorizando una parte del sistema durante mucho tiempo, una hora o dos horas o diez horas, entonces podemos hacer que se tomen muestreos cada hora o cada 15 segundos o cada 30 segundos o cada día, en función del recopilador de datos que nosotros generemos.

Luego tendremos información de donde queremos que se almacene el informe y finalizaríamos.

Una vez que nosotros tenemos el recopilador de datos, este recopilador de datos, si nos vamos a la parte de propiedades, vamos a tener aquí información general, podemos poner una descripción para que otros compañeros sepan para qué sirve ese recopilador de datos.

Podemos seleccionar con qué cuenta queremos que se ejecute, vemos que por defecto se ejecuta como System, tendríamos el directorio donde se va a almacenar ese recopilador de datos y el formato en el que se van a generar los informes.

Y si nosotros queremos que los informes se vayan acumulando cada vez que lo ejecutamos, tendríamos la parte de permisos de seguridad y tendríamos la parte de programación.

Nosotros aquí podríamos seleccionar que el recopilador de datos funcionará unos determinados días a unas determinadas horas y de esta manera tendríamos un proceso automatizado para ese recopilador de datos y luego tendríamos una condición de parada.

Una condición de parada es que nosotros podemos ponerla aquí 30 segundos y lo que vamos a hacer es que se va a ejecutar durante ese periodo de 30 segundos.

Aparte aparte, luego nosotros podemos asignar una tarea a ese recopilador de datos.

Si necesitamos que se ejecute algo previamente a que ese recopilador de datos comience a funcionar, pues podríamos hacerlo e incluirlo en la parte de configuración.

Si yo inicio este recopilador de datos, me voy a la parte de informes y dentro de la parte de informes veis que me genera un informe y que en este caso me dice que está recopilando datos durante un periodo de 30 segundos.

Una vez que me generan los informes yo tengo aquí diferentes maneras de ver esos informes.

En este caso vemos que tenemos muy poquitos datos porque realmente nosotros lo que hemos hecho es indicar muy pocos recopiladores de datos.

Como conclusión vemos que Windows Server tiene una serie de herramientas que nos sirven para monitorizar el sistema y que además algunas de estas herramientas nos van a permitir generar una serie de informes que nos pueden ayudar a marcar unas líneas base que después nos servirán a su vez para detectar cuando algo está funcionando correctamente, Tiene una carga de trabajo que no es habitual o tenemos una actividad que tenemos que investigar porque no es una actividad del sistema operativo.

Una carga de trabajo de los componentes del sistema que no es común o que no es frecuente puede ser indicado de un ataque o puede ser indicativo del mal funcionamiento de un componente o la mala configuración de un determinado elemento.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.