Actividad 02. Creación de un conjunto de recopiladores de datos en Windows

1. Realiza los pasos siguientes:

1. Realiza los pasos siguientes:

A. Acceder al Monitor de Rendimiento:

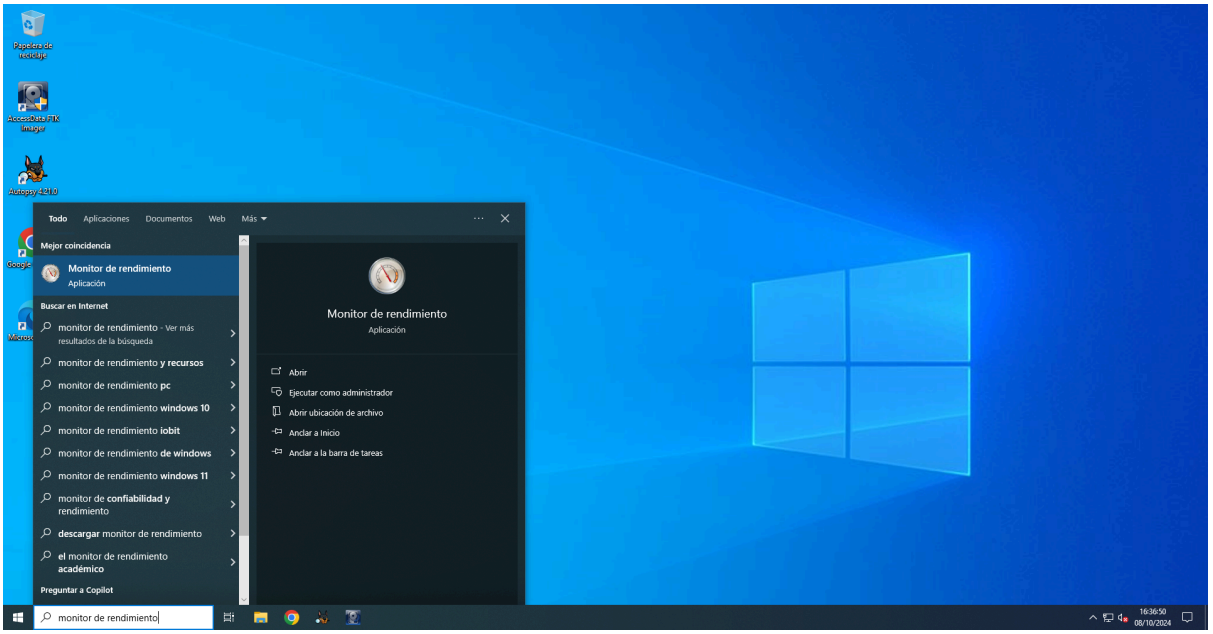
Para comenzar con la creación de un conjunto de recopiladores de datos, lo primero es acceder al Monitor de rendimiento en Windows. Puedes hacerlo de dos maneras

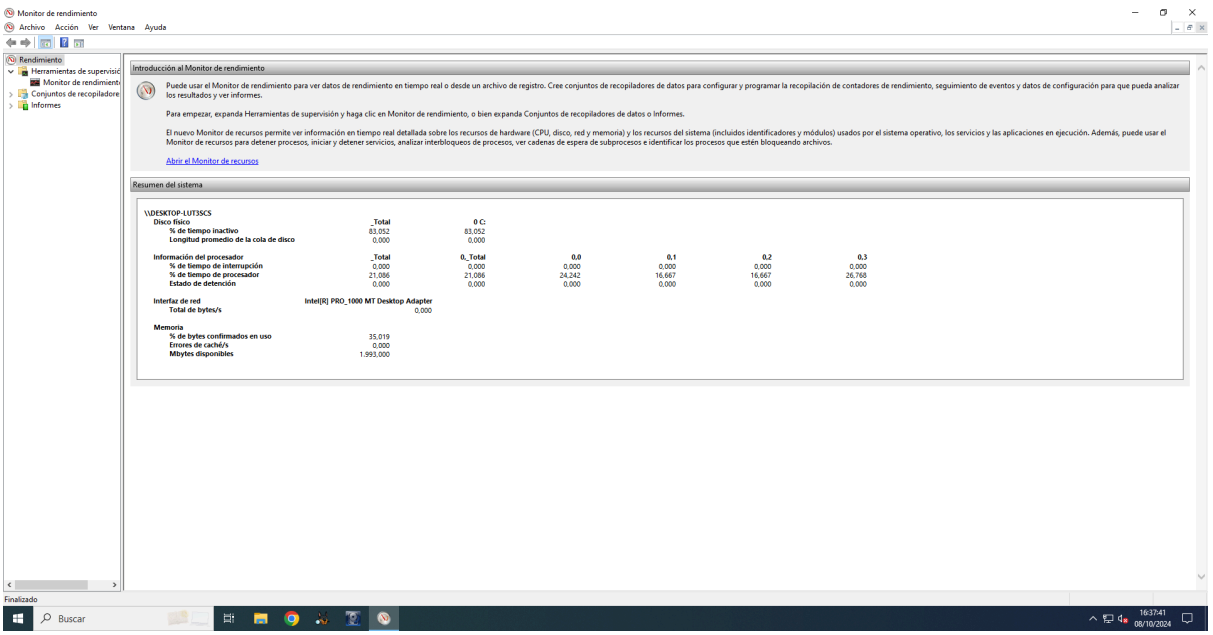
Opción 1: A través del menú Inicio.

1. Haz clic en el botón **Inicio**.
2. Escribe ***perfmon*** en el cuadro de búsqueda y presiona **Enter**.
3. El **Monitor de rendimiento** se abrirá.

Opción 2: A través de la consola **Ejecutar**.

4. Presiona las teclas Win + R para abrir la consola de **Ejecutar**.
5. Escribe ***perfmon*** y haz clic en Aceptar o presiona **Enter**.





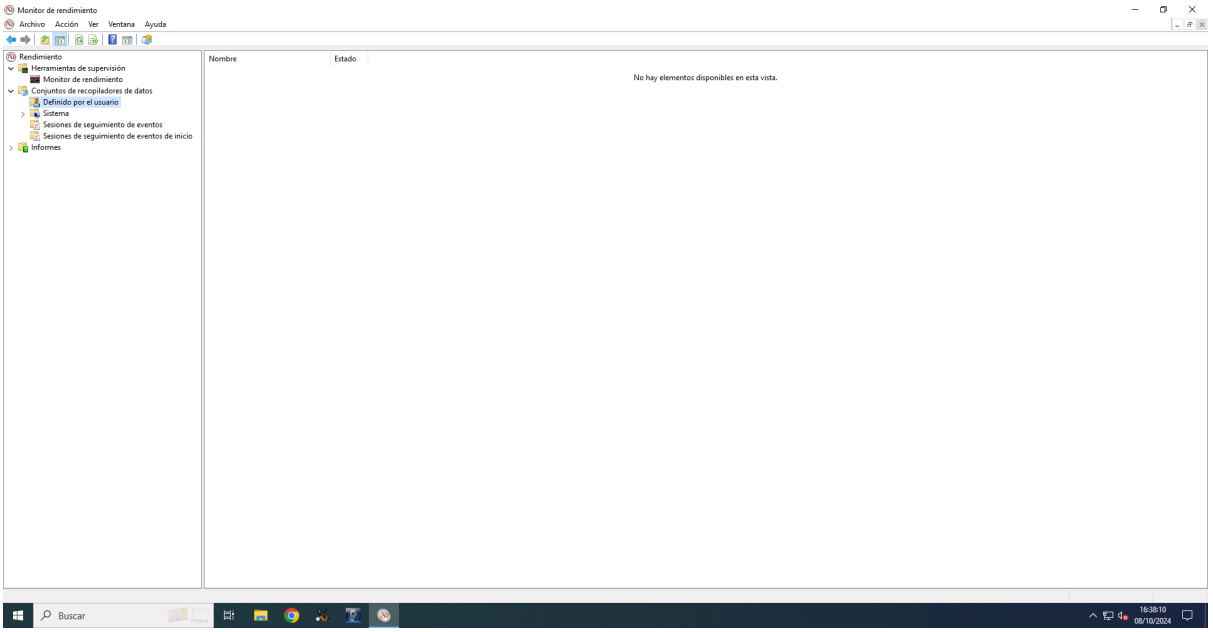
B. ***Creación del conjunto de recopiladores:***

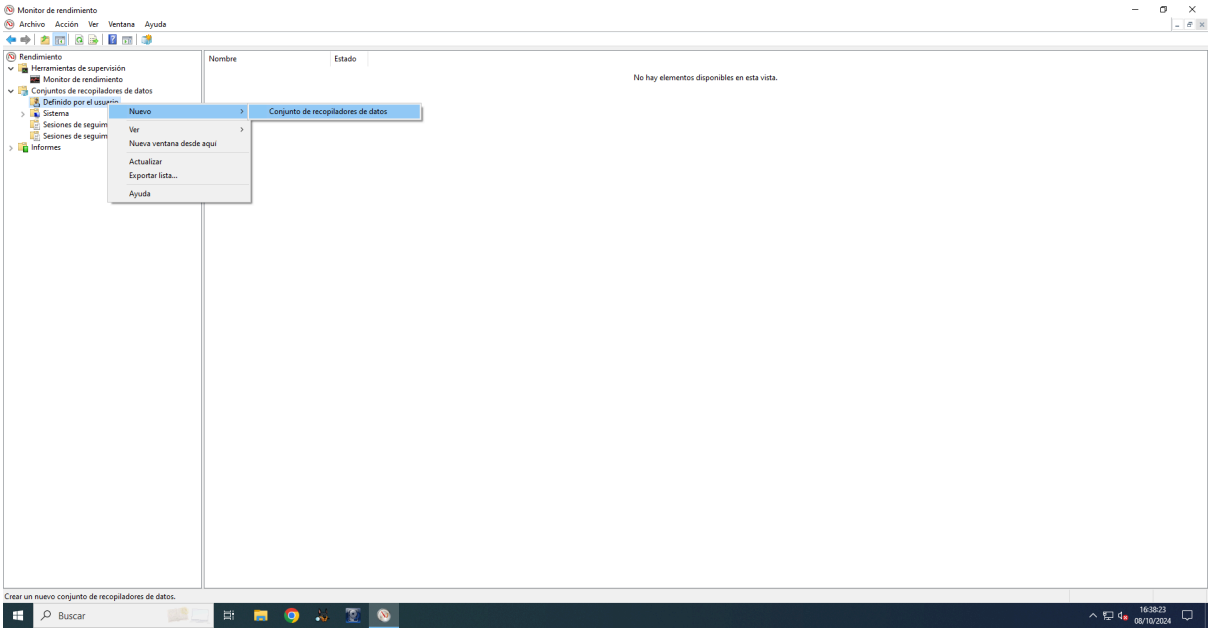
1. **Crear un Nuevo Conjunto de Recopiladores de Datos**. Una vez que el Monitor de rendimiento esté abierto, vamos a crear un nuevo conjunto de recopiladores de datos.
    a. En el panel izquierdo del **Monitor de rendimiento**, navega a la sección **Conjuntos de recopiladores de datos** y selecciona **Definidos por el usuario**.
    b. Haz clic derecho sobre **Definidos por el usuario** y selecciona **Nuevo -> Conjunto de recopiladores de datos**.

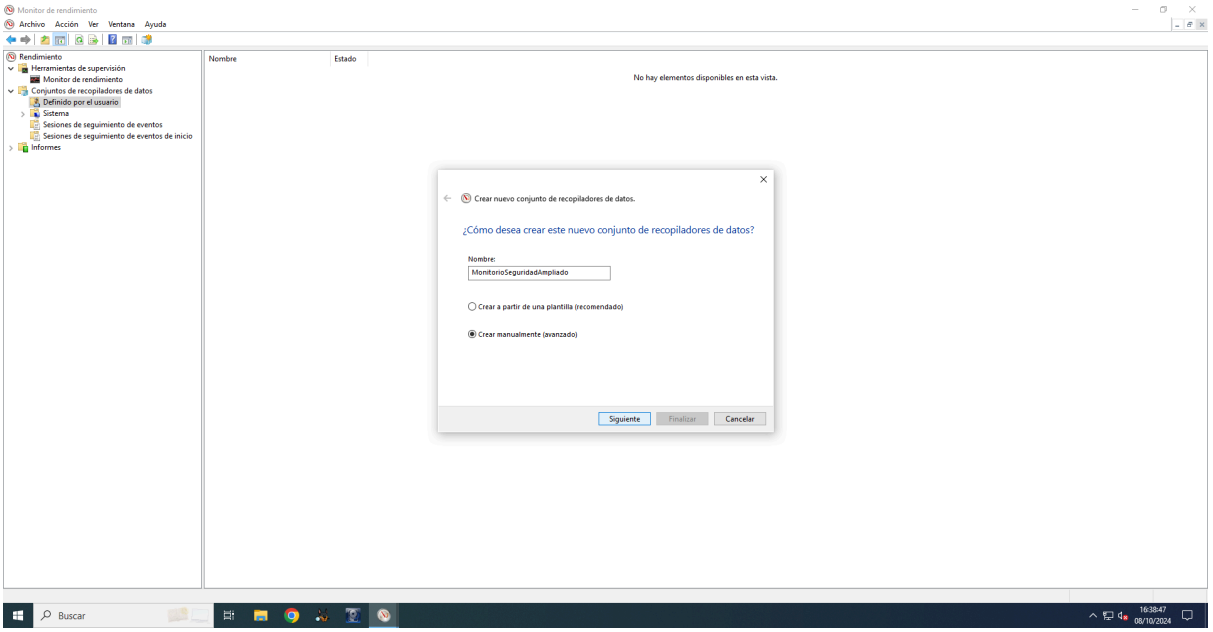
2. **Asignar Nombre y Tipo de Creación**.
    a. En el cuadro que aparece, asigna un nombre al conjunto de recopiladores. En este caso, llamaremos al conjunto **MonitoreoSeguridadAmpliado**.
    b. Selecciona la opción **Crear manualmente (avanzado)** para tener un mayor control sobre las configuraciones del conjunto. Haz clic en **Siguiente**.
3. **Seleccionar los Datos de Rendimiento**. En este paso, vamos a definir qué tipo de datos queremos recopilar.
    a. Selecciona **Crear registros de datos** y marca la casilla **Contador de rendimiento**.
    b. Haz clic en **Siguiente** para continuar.

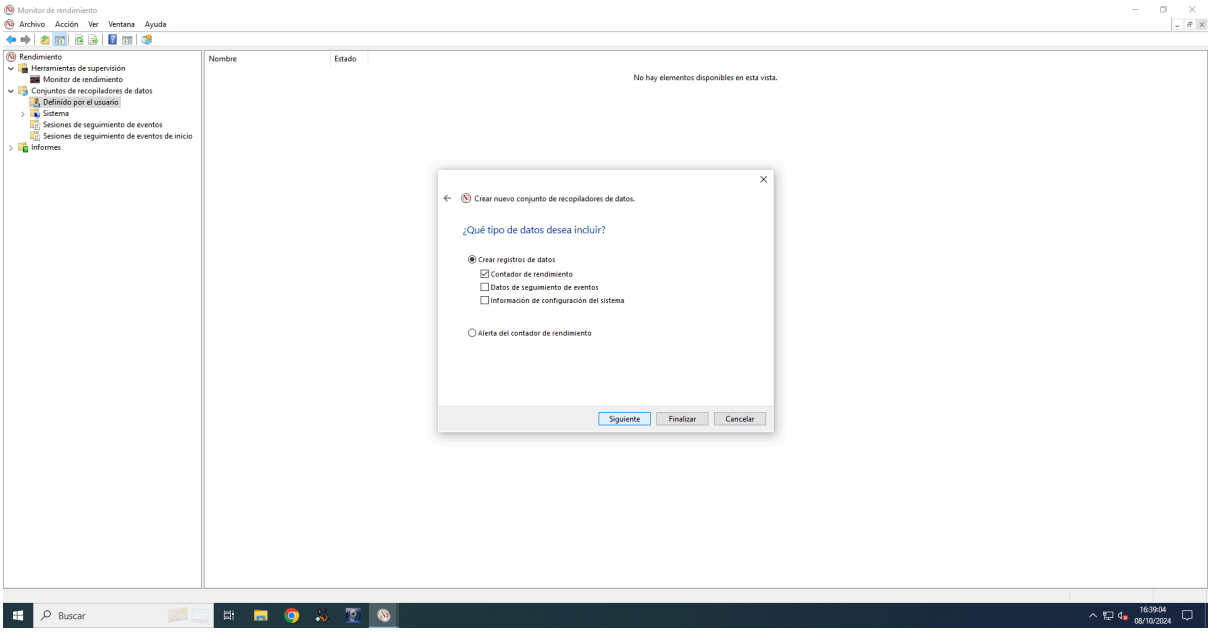
4. **Configuración de Contadores de Rendimiento**. En este punto, vamos a seleccionar los contadores de rendimiento que monitorearán aspectos clave del sistema como el uso de CPU, memoria, disco y red.
    a. Haz clic en el botón **Agregar** para abrir la ventana donde puedes seleccionar los contadores.
    b. Selecciona los siguientes contadores relevantes para la actividad: ***Procesador -> % de tiempo de procesador***: Mide el porcentaje de tiempo que el procesador está ocupado ejecutando un proceso. ***Disco físico -> Bytes de lectura/segundos***: Mide el rendimiento del disco en términos de la cantidad de datos leídos por segundo. ***Disco físico -> Bytes de escritura/segundos***: Mide el rendimiento del disco en términos de la cantidad de datos escritos por segundo. ***Memoria -> Páginas/segundos***: Mide cuántas páginas de memoria se están leyendo o escribiendo en el archivo de paginación. ***Sistema -> Procesos***: Mide el número total de procesos activos en el sistema.
    c. Haz clic en **Agregar** para cada contador seleccionado y luego en **Aceptar**.
    d. Ajusta el intervalo de muestreo (15 segundos es un intervalo comúnmente utilizado).
    e. Haz clic en **Siguiente**.
5. **Configurar Ubicación de Almacenamiento**. Ahora es necesario definir dónde se guardarán los datos recopilados.
    a. Especifica la ubicación en la que se almacenarán los archivos de registro. Puede ser una carpeta local en tu equipo o un recurso compartido en la red. Por ejemplo: **C:\MonitoreoSeguridadAmpliado**.
    b. Haz clic en **Siguiente**.
6. **Completar la Creación del Conjunto**. En este paso, finalizaremos la creación del conjunto de recopiladores de datos.
    a. Elige si quieres que el conjunto se ejecute manualmente o a través de un programador de tareas:
        i. Si lo deseas ejecutar manualmente, selecciona **Guardar y cerrar**.
        ii. Si prefieres automatizar su ejecución, selecciona **Iniciar este conjunto de recopiladores de datos ahora**.

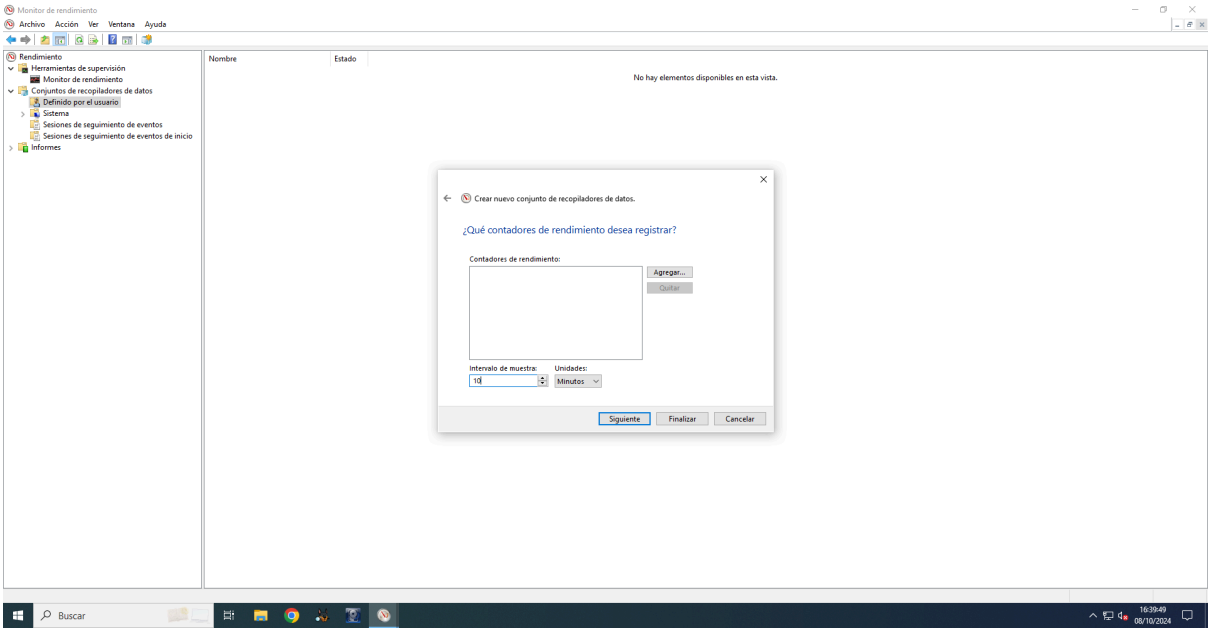
b. Marca la opción **Abrir las propiedades de este conjunto de recopiladores de datos** para realizar configuraciones adicionales si es necesario.
c. Haz clic en **Finalizar**.

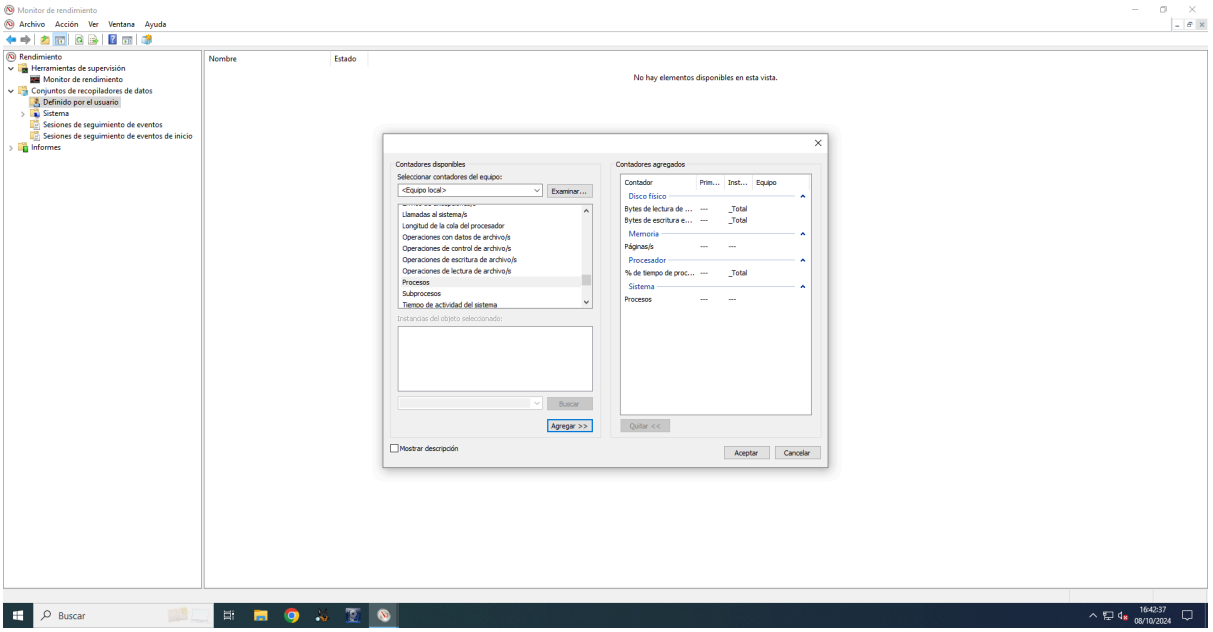


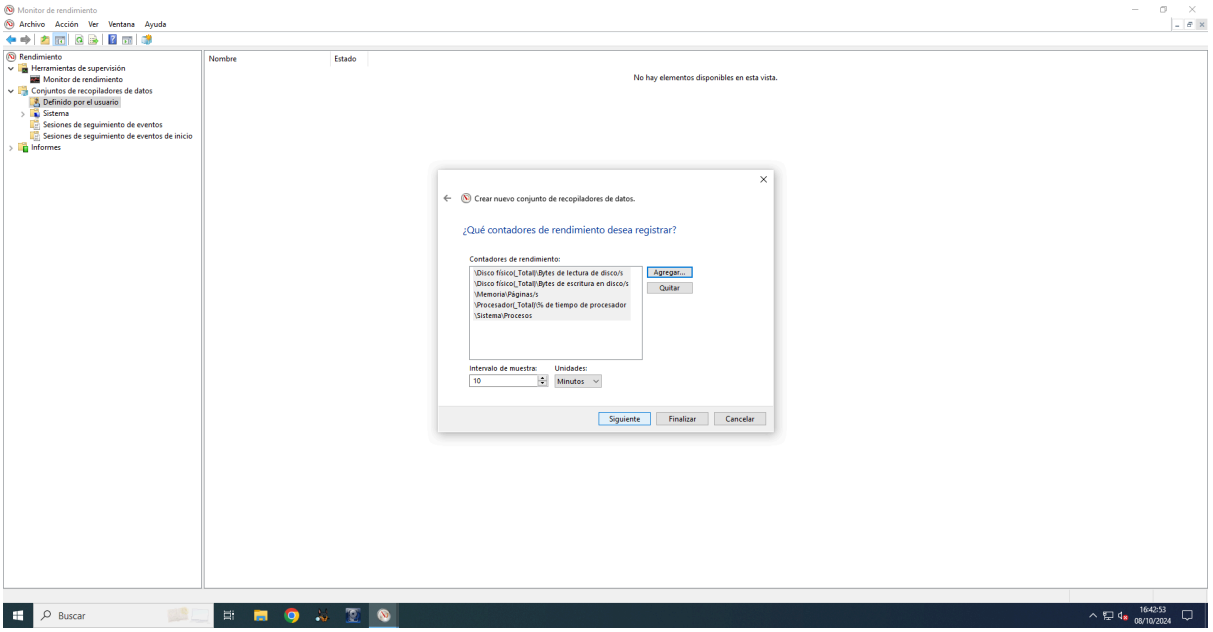


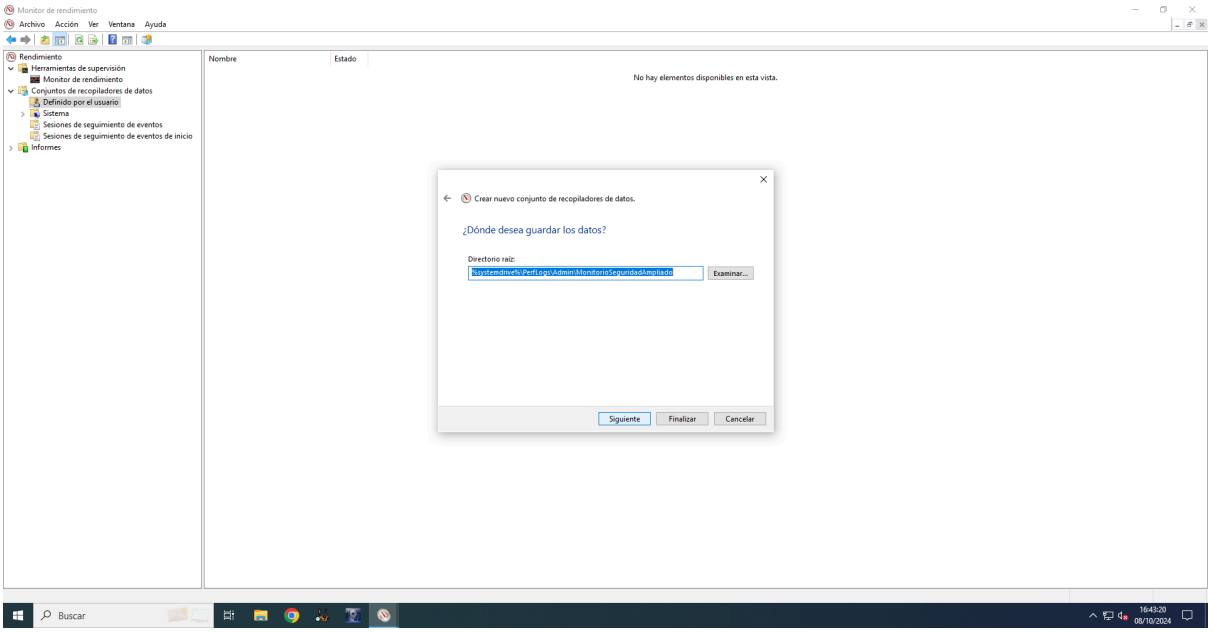

Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
Crear nuevo conjunto de recopiladores de datos.
¿Cómo desea crear este nuevo conjunto de recopiladores de datos?
Nombre:
MonitorioSeguridadAmpliado
Crear a partir de una plantilla (recomendado)
Crear manualmente (avanzado)
Siguiente
Finalizar
Cancelar
Buscar
16:38:47
08/10/2024

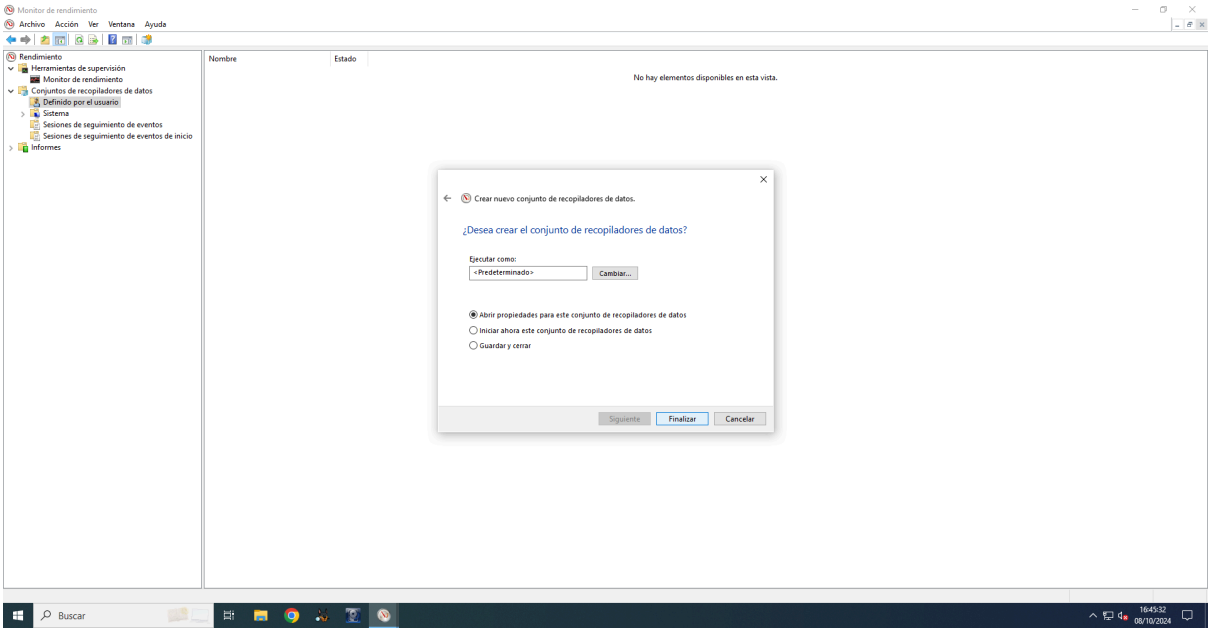

Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
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
Buscar
16:39:04
08/10/2024


Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
Crear nuevo conjunto de recopiladores de datos.
¿Qué contadores de rendimiento desea registrar?
Contadores de rendimiento:
Agregar...
Quitar
Intervalo de muestra:
Unidades:
1d
Minutos
Siguiente
Finalizar
Cancelar
Buscar
16:39:49
08/10/2024


Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
Contadores disponibles
Seleccionar contadores del equipo:
<Equipo local>
Examinar...
Llamadas al sistema/s
Longitud de la cola del procesador
Operaciones con datos de archivo/s
Operaciones de control de archivo/s
Operaciones de escritura de archivo/s
Operaciones de lectura de archivo/s
Procesos
Subprocesos
Tiempo de actividad del sistema
Instancias del objeto seleccionado:
Buscar
Agregar >>
Mostrar descripción
Contadores agregados
Contador
Prim...
Inst...
Equipo
Disco físico
Bytes de lectura de ...
Bytes de escritura e...
_Total
Memoria
Páginas/s
Procesador
% de tiempo de proc...
Sistema
Procesos
Quitar <<
Aceptar
Cancelar
Buscar
16:42:37
08/10/2024


Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
Crear nuevo conjunto de recopiladores de datos.
¿Qué contadores de rendimiento desea registrar?
Contadores de rendimiento:
\Disco físico(_Total)\Bytes de lectura de disco/s
\Disco físico(_Total)\Bytes de escritura en disco/s
\Memoria\Páginas/s
\Procesador(_Total)\% de tiempo de procesador
\Sistema\Procesos
Agregar...
Quitar
Intervalo de muestra:
10
Unidades:
Minutos
Siguiente
Finalizar
Cancelar
Buscar
16:42:53
08/10/2024

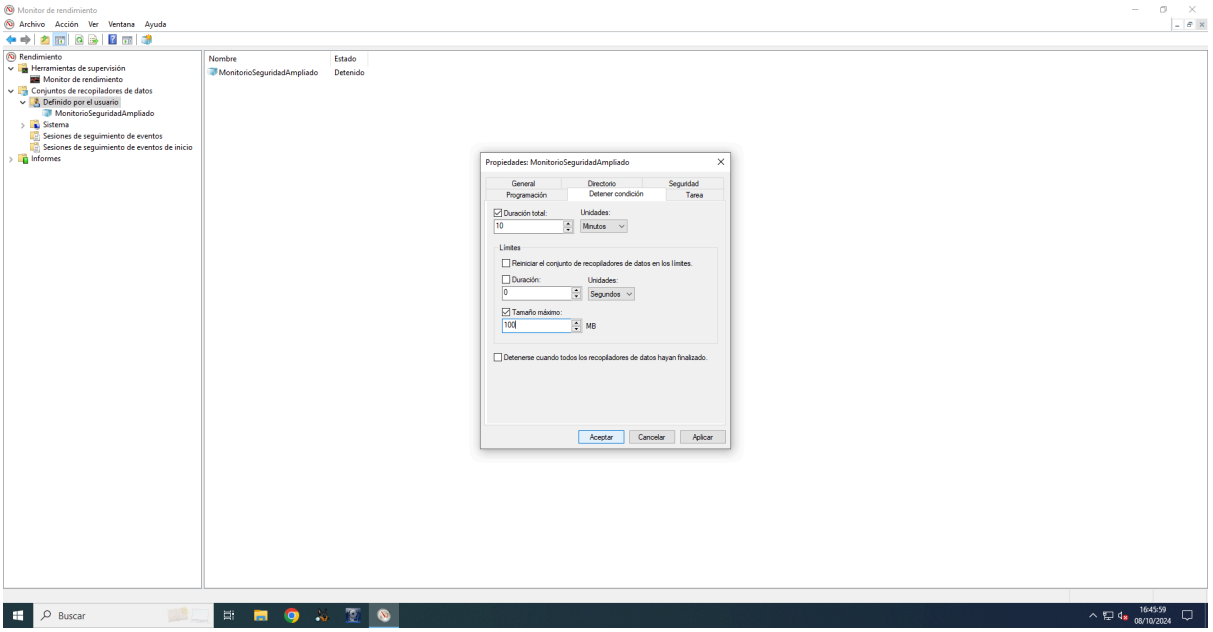

Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Nombre
Estado
No hay elementos disponibles en esta vista.
Crear nuevo conjunto de recopiladores de datos.
¿Dónde desea guardar los datos?
Directorio raíz:
%systemdrive%\PerfLogs\Admin\MonitorioSeguridadAmpliado
Examinar...
Siguiente
Finalizar
Cancelar
Buscar
16:43:20
08/10/2024



C. ***Configuración de las Propiedades del Conjunto de Recopiladores de Datos:***

Una vez creado el conjunto de recopiladores, se abrirán las propiedades para configurarlo de manera más detallada.

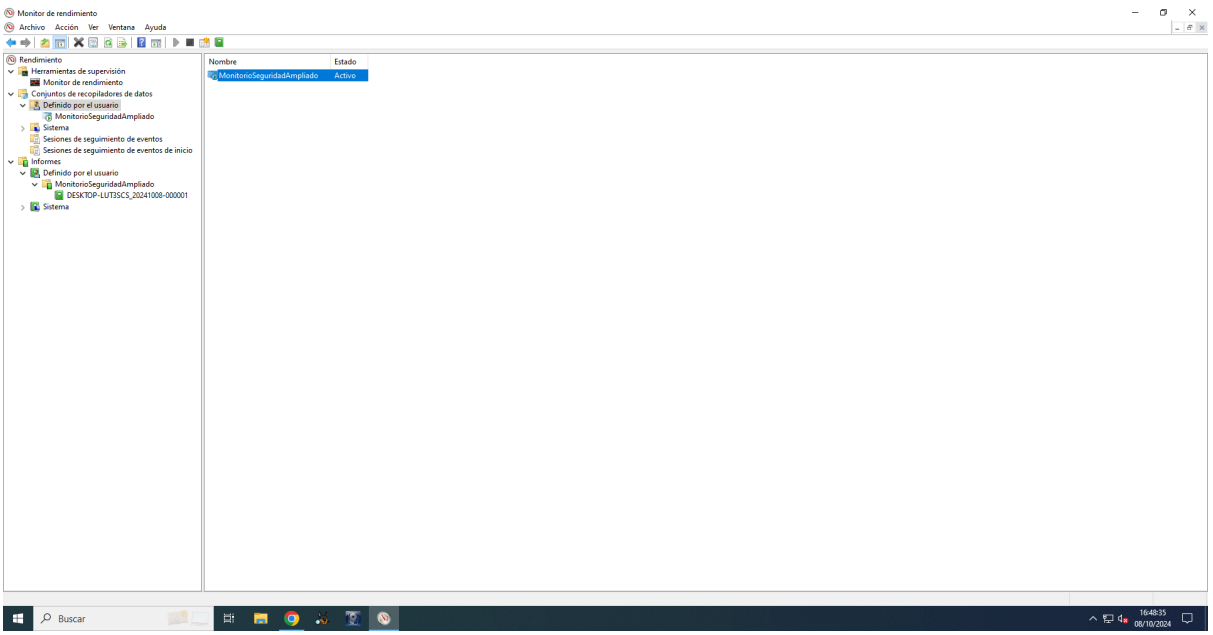
1. **Intervalos de muestreo**:
    a. En la pestaña **Muestreo**, establece la frecuencia de recolección de datos. Para este ejercicio, selecciona un intervalo de **15 minutos**.
2. **Detener condición**:
    a. En la pestaña **Deter condición**, puedes definir reglas para detener la recopilación de datos automáticamente. Por ejemplo:
        i. **Duración total**: Define un límite de tiempo después del cual se detendrá la recolección (por ejemplo, 10 minutos).
        ii. **Tamaño máximo del archivo**: Limita el tamaño del archivo de registro para evitar que crezca demasiado (por ejemplo, 100 MB).
3. Haz clic en **Aceptar** para guardar las configuraciones.



D. <u>Ejecutar el Conjunto de Recopiladores de Datos:</u>

Una vez que el conjunto ha sido configurado, está listo para ser ejecutado.

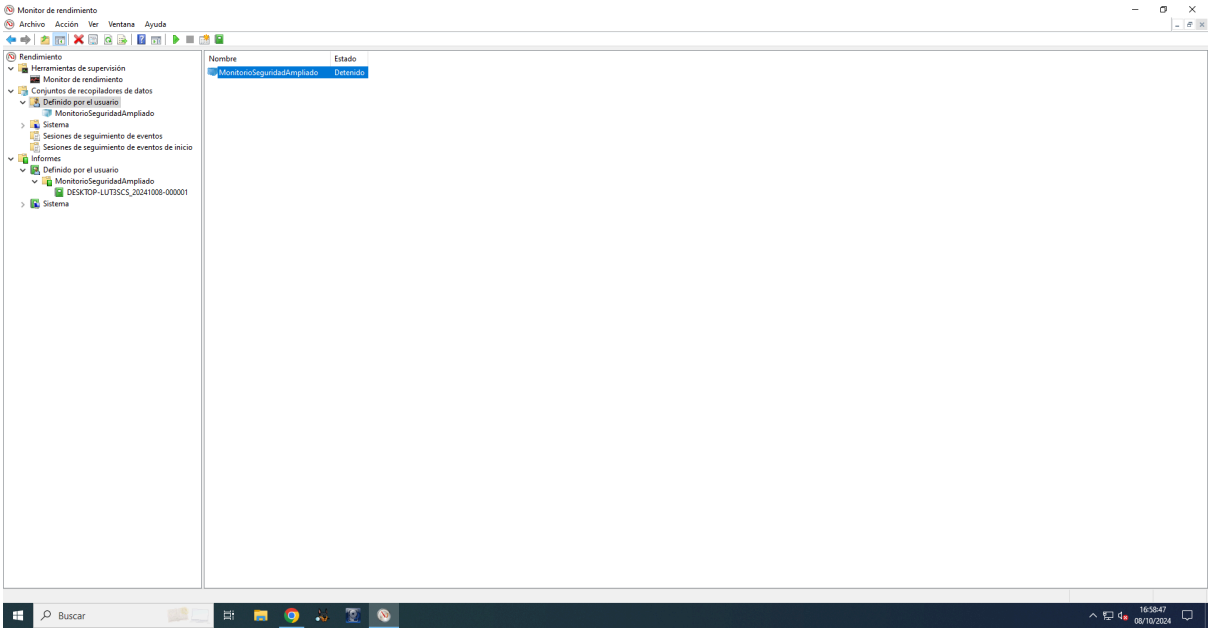
1. En el **Monitor de rendimiento**, navega a **Conjuntos de recopiladores de datos -> Definidos por el usuario**.
2. Selecciona el conjunto que acabas de crear (**MonitoreoSeguridad**).
3. Haz clic derecho sobre él y selecciona **Iniciar**.
4. Deja que el conjunto recopile los datos durante un periodo de tiempo adecuado, como **5-10 minutos**, para tener una muestra significativa de datos.

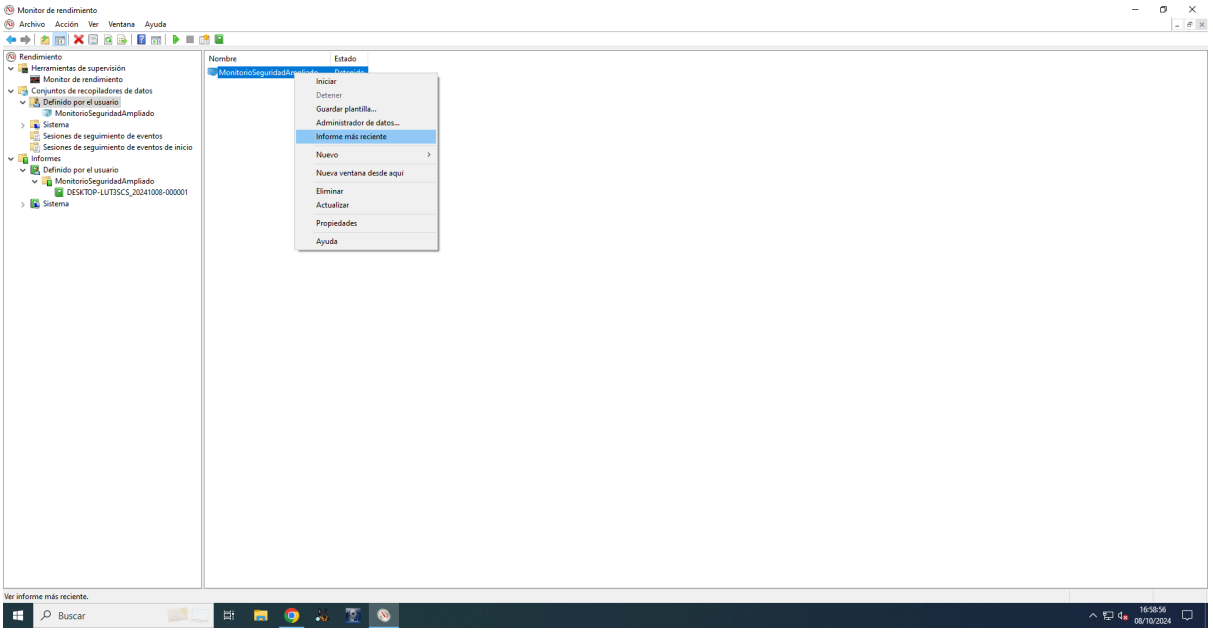


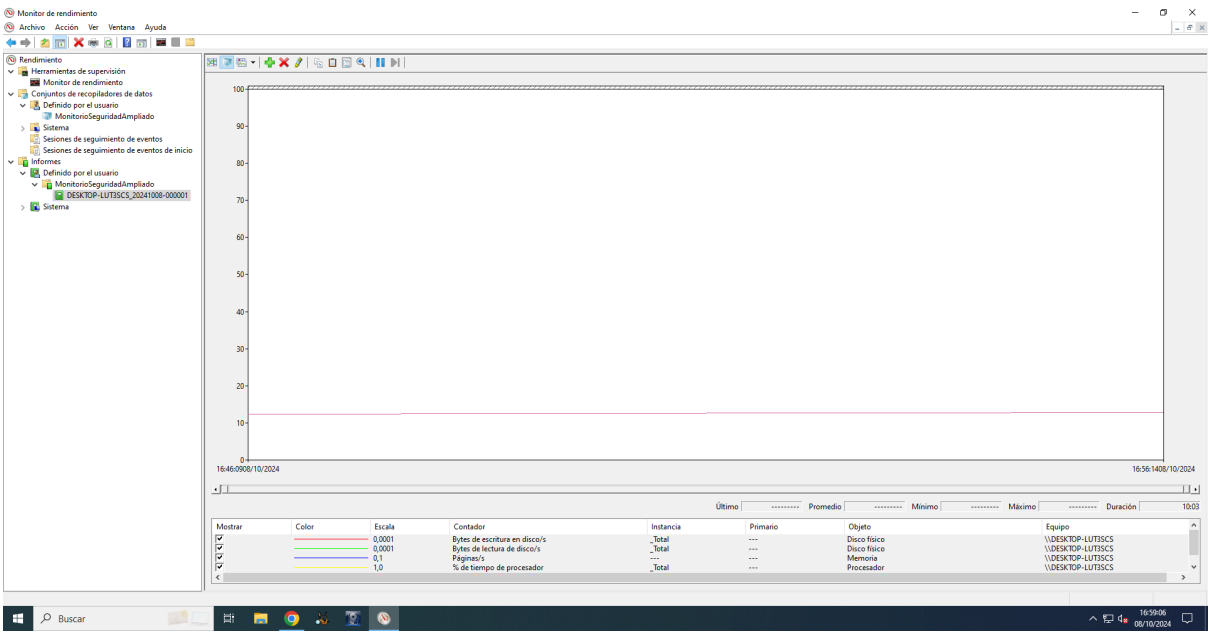
E. <u>Detener el Conjunto y Analizar los Datos:</u>

Después de haber recolectado datos, es importante detener el conjunto y revisar los resultados.

1. Para detener el conjunto, vuelve al **Monitor de rendimiento**, haz clic derecho sobre el conjunto de recopiladores y selecciona **Detener**.
2. Navega a la ubicación en la que configuraste que se guardaran los datos. Busca los archivos de registro que tendrán una extensión como .blg o .csv.
    a. **.blg** (Binary Log File) es el formato binario para los registros de rendimiento.
    b. **.csv** (Comma Separated Values) es el formato más fácil de analizar manualmente, especialmente si se abre en Excel.
3. Usa el **Monitor de rendimiento** para visualizar los datos o abre los archivos en Excel para realizar un análisis más detallado.


Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
MonitorioSeguridadAmpliado
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Definido por el usuario
MonitorioSeguridadAmpliado
DESKTOP-LUT3SCS_20241008-000001
Sistema
Nombre
Estado
MonitorioSeguridadAmpliado
Detenido
Buscar
16:58:47
08/10/2024


Monitor de rendimiento
Archivo Acción Ver Ventana Ayuda
Rendimiento
Herramientas de supervisión
Monitor de rendimiento
Conjuntos de recopiladores de datos
Definido por el usuario
MonitorioSeguridadAmpliado
Sistema
Sesiones de seguimiento de eventos
Sesiones de seguimiento de eventos de inicio
Informes
Definido por el usuario
MonitorioSeguridadAmpliado
DESKTOP-LUT3SCS_20241008-000001
Sistema
Nombre
Estado
Iniciar
Detener
Guardar plantilla...
Administrador de datos...
Informe más reciente
Nuevo
Nueva ventana desde aquí
Eliminar
Actualizar
Propiedades
Ayuda
Ver informe más reciente.
Buscar
16:58:56
08/10/2024



<u>RESULTADOS ESPERADOS:</u>

Los resultados dependerán de las condiciones del sistema durante el período de monitoreo. Aquí se describen los resultados típicos:

1. ***Uso del procesador***:
    a. El uso del procesador debería ser relativamente bajo si el sistema no está sometido a carga. Un uso elevado y constante puede indicar sobrecarga.
2. ***Actividad del disco***:
    a. Un alto número de bytes leídos/escritos por segundo puede indicar una alta carga de trabajo de E/S. Cualquier actividad anómala, como picos de escritura, puede ser signo de operaciones inesperadas o maliciosas.
3. ***Uso de la memoria***:
    a. La cantidad de páginas por segundo indicará si el sistema está moviendo demasiada memoria entre el disco y la RAM, lo que puede indicar un problema de falta de memoria.
4. ***Tráfico de red***:
    a. Un tráfico elevado de red puede ser normal si se están ejecutando aplicaciones que lo requieran. Sin embargo, un tráfico anómalo puede indicar problemas de seguridad, como la presencia de malware.
5. ***Número de procesos***:

a. Un aumento inusual en el número de procesos puede ser un indicativo de aplicaciones mal gestionadas o procesos maliciosos en ejecución.

CONCLUSIÓN DEL EJERCICIO:

Debes concluir el ejercicio preparando un informe breve sobre los datos recolectados. El informe debe incluir:

1. ***Análisis de los datos***: Comentarios sobre el uso del procesador, disco, memoria y red.
2. ***Capturas de pantalla***: Incluyendo gráficos del Monitor de rendimiento mostrando la actividad de los contadores de rendimiento.
3. ***Identificación de patrones***: Cualquier patrón o anomalía en el rendimiento debe ser destacado.