

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

1. Acceder al Monitor de Rendimiento

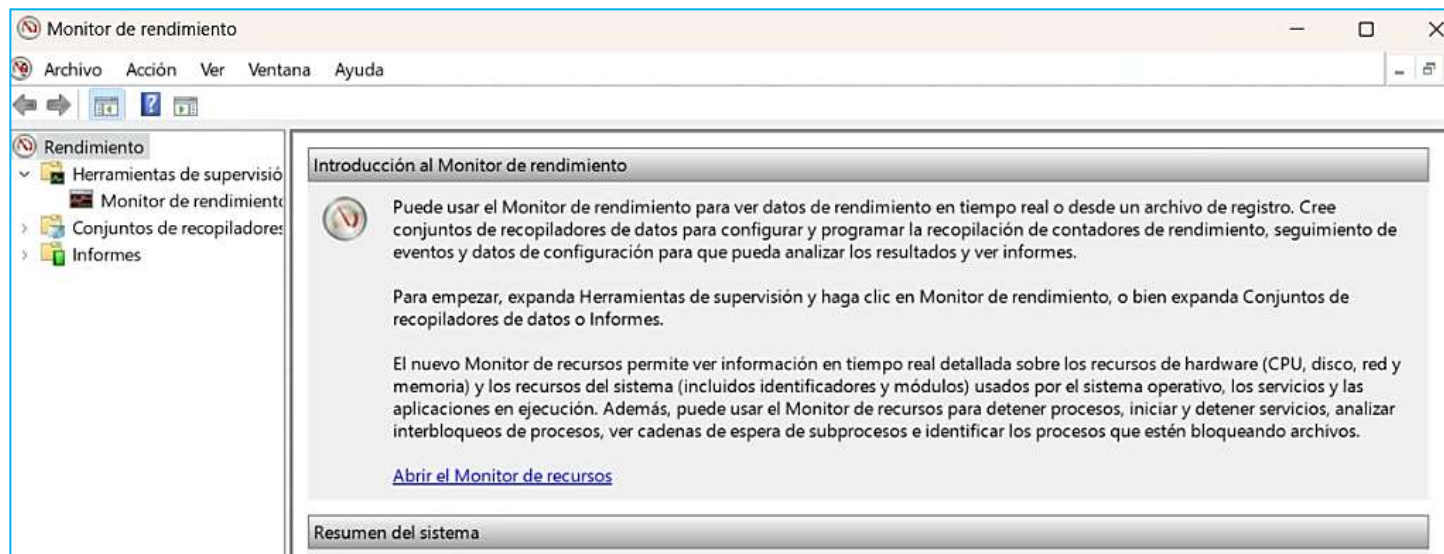
Para comenzar con la creación de un conjunto de recopiladores de datos, lo primero es acceder al **Monitor de rendimiento** en Windows. Puedes hacerlo de dos maneras:

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.

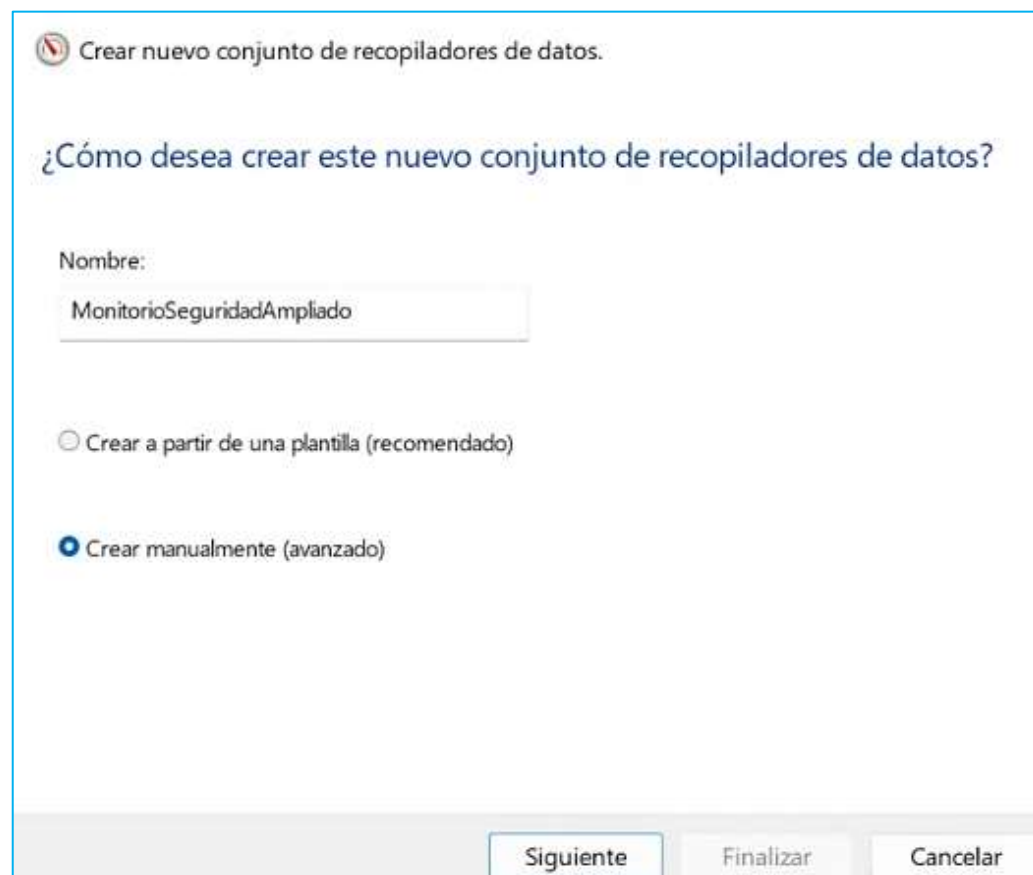
Opción 2: A través de la consola **Ejecutar**.

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



2. Asignar Nombre y Tipo de Creación

1. En el cuadro que aparece, asigna un nombre al conjunto de recopiladores. En este caso, llamaremos al conjunto **MonitoreoSeguridadAmpliado**.
2. Selecciona la opción **Crear manualmente (avanzado)** para tener un mayor control sobre las configuraciones del conjunto. Haz clic en **Siguiente**.



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

3. Seleccionar los Datos de Rendimiento

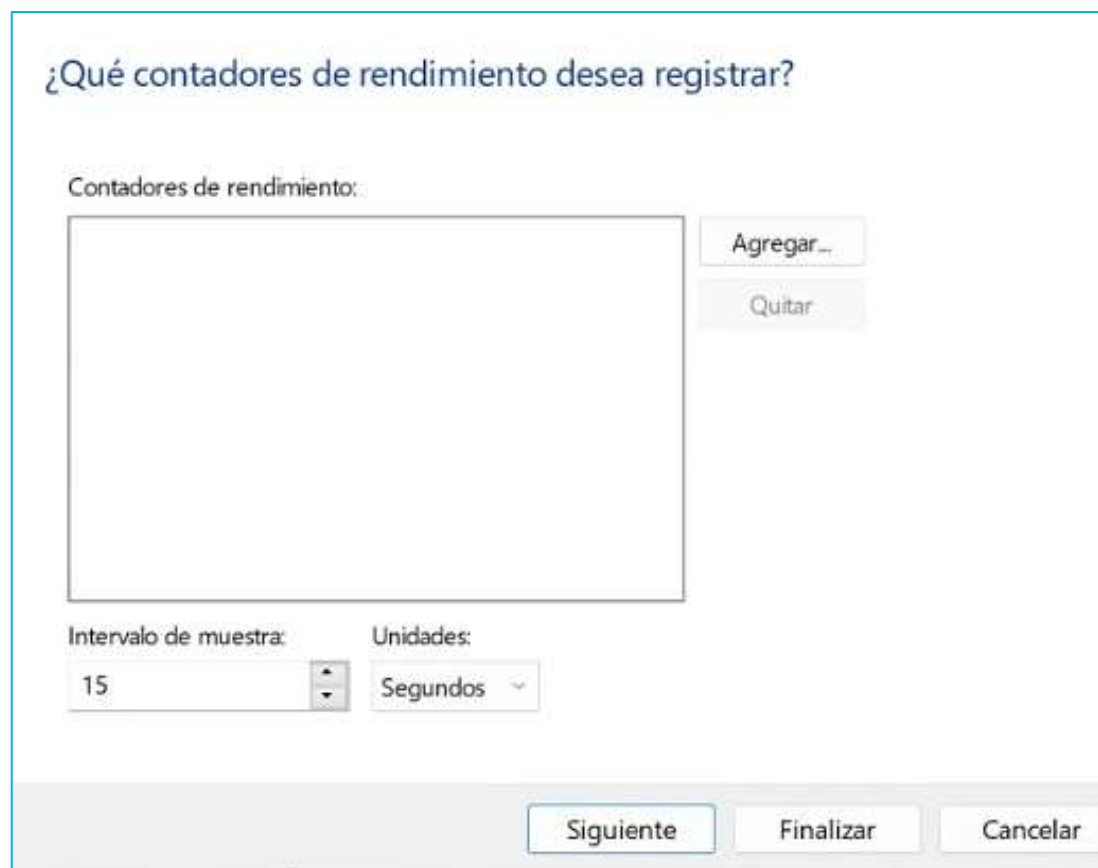
En este paso, vamos a definir qué tipo de datos queremos recopilar.

1. Selecciona **Crear registros de datos** y marca la casilla **Contador de rendimiento**.
2. 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.

1. Haz clic en el botón **Agregar** para abrir la ventana donde puedes seleccionar los contadores.



¿Qué contadores de rendimiento desea registrar?

Contadores de rendimiento:

Agregar...

Quitar

Intervalo de muestra: 15

Unidades: Segundos

Siguiente Finalizar Cancelar

2. 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.

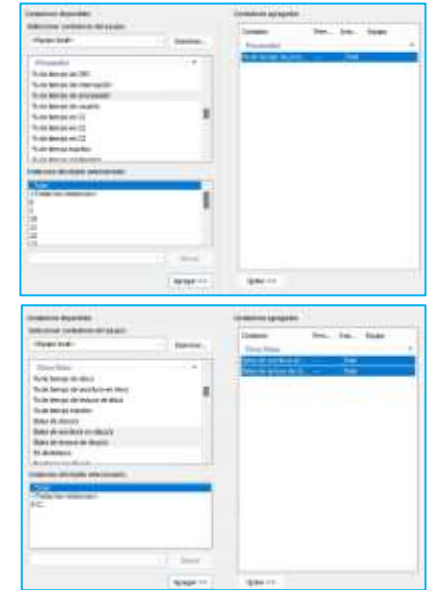
Disco físico -> Bytes de lectura/segundos: Mide el rendimiento del disco en términos de la cantidad de datos leídos por segundo.

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.

3. Haz clic en **Agregar** para cada contador seleccionado y luego en **Aceptar**.



- Ajusta el intervalo de muestreo (15 segundos es un intervalo comúnmente utilizado).
- Haz clic en **Siguiente**.

←  Crear nuevo conjunto de recopiladores de datos.

¿Qué contadores de rendimiento desea registrar?

Contadores de rendimiento:

\Procesador(_Total)\% de tiempo de procesador

\Disco físico(_Total)\Bytes de escritura en disco/s

\Disco físico(_Total)\Bytes de lectura de disco/s

\Memoria\Páginas/s

\Red de .NET CLR\Bytes enviados

\Red de .NET CLR\Bytes recibidos

\Sistema\Procesos

Agregar...

Quitar

Intervalo de muestra: Unidades:

Siguiente Finalizar Cancelar

5. Configurar Ubicación de Almacenamiento

Ahora es necesario definir dónde se guardarán los datos recopilados.

1. 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\.
2. Haz clic en **Siguiente**.

8. Completar la Creación del Conjunto

En este paso, finalizaremos la creación del conjunto de recopiladores de datos.

1. Elige si quieres que el conjunto se ejecute manualmente o a través de un programador de tareas:
 - Si lo deseas ejecutar manualmente, selecciona **Guardar y cerrar**.
 - Si prefieres automatizar su ejecución, selecciona **Iniciar este conjunto de recopiladores de datos ahora**.
2. Marca la opción **Abrir las propiedades de este conjunto de recopiladores de datos** para realizar configuraciones adicionales si es necesario.
3. Haz clic en **Finalizar**.

3. 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:

En la pestaña **Muestreo**, establece la frecuencia de recolección de datos. Para este ejercicio, selecciona un intervalo de **15 segundos**.

2. Detener condición:

En la pestaña **Deter condición**, puedes definir reglas para detener la recopilación de datos automáticamente. Por ejemplo:

- **Duración total:** Define un límite de tiempo después del cual se detendrá la recolección (por ejemplo, 10 minutos).
- **Tamaño máximo del archivo:** Limita el tamaño del archivo de registro para evitar que crezca demasiado (por ejemplo, 100 MB).

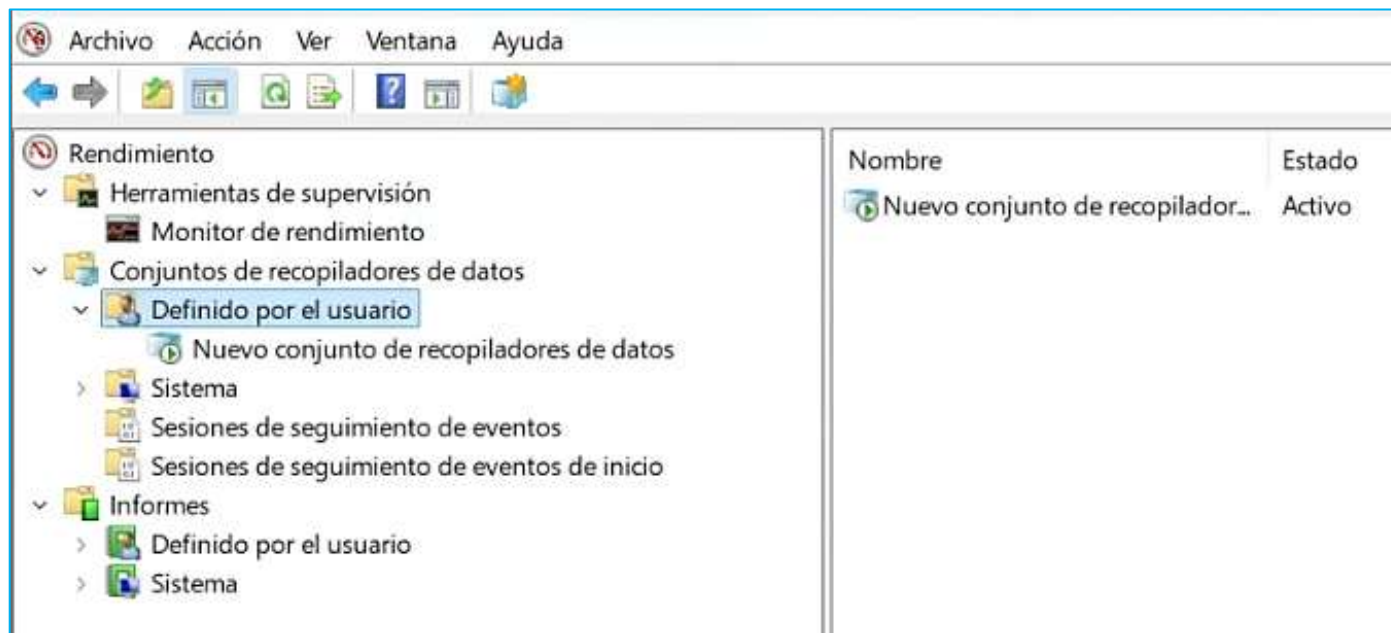
3. Haz clic en **Aceptar** para guardar las configuraciones.

The screenshot shows a dialog box titled "Propiedades: Monitoreo seguridad ampliado" with a close button (X) in the top right corner. It has three tabs: "General", "Directorio", and "Seguridad". The "Seguridad" tab is active, and within it, the "Detener condición" sub-tab is selected. The "Programación" sub-tab is also visible. The "Duración total" checkbox is checked, with a value of "10" in the adjacent field and "Minutos" in the "Unidades" dropdown. Below this, the "Límites" section contains three options: "Reiniciar el conjunto de recopiladores de datos en los límites" (unchecked), "Duración:" (unchecked) with a value of "0" and "Segundos" in the units dropdown, and "Tamaño máximo:" (checked) with a value of "100" and "MB" in the units dropdown. At the bottom, there is an unchecked checkbox for "Detenerse cuando todos los recopiladores de datos hayan finalizado." and three buttons: "Aceptar", "Cancelar", and "Aplicar".

4. Ejecutar el Conjunto de Recopiladores de Datos

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

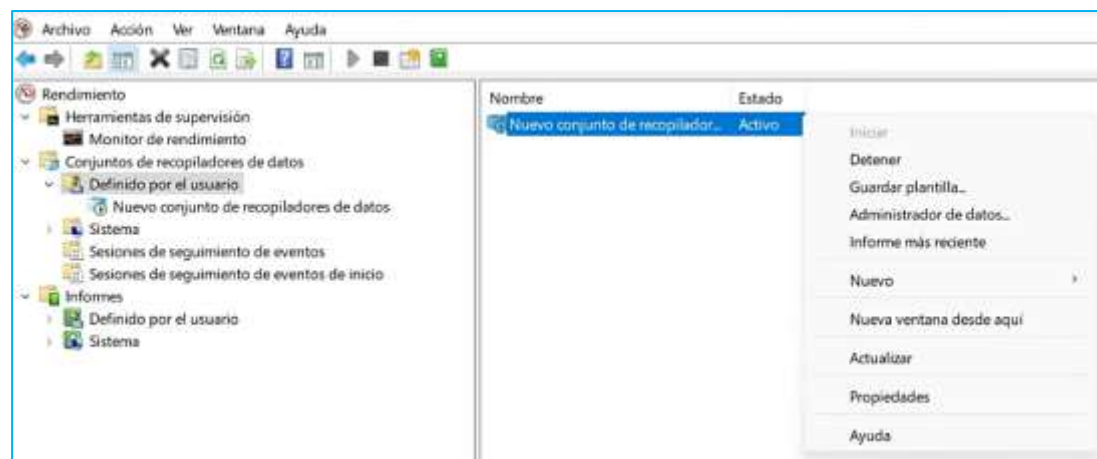
1. En el **Monitor de rendimiento**, navega a **Conjuntos de recopiladores de datos -> Definidos por el usuario**.
2. Selecciona el conjunto que acabas de crear (**MonitoreoSeguridad**).
3. Haz clic derecho sobre él y selecciona **Iniciar**.
4. Deja que el conjunto recopile datos durante un periodo de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



5. Detener el Conjunto y Analizar los Datos

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.
 - **.blg** (Binary Log File) es el formato binario para los registros de rendimiento.
 - **.csv** (Comma Separated Values) es el formato más fácil de analizar manualmente, especialmente si se abrirá en Excel.

3. Usa el **Monitor de rendimiento** para visualizar los datos o abre los archivos en **Excel** para realizar un análisis más detallado.



Equipo con poca carga de trabajo



Equipo con poca carga de trabajo media



Equipo con poca carga de trabajo alta

6. Resultados Esperados

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

1. Uso del procesador:

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:

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:

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:

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:

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

7. 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.

Se pide:

1. Realiza los pasos siguientes:
 - a. Acceder al Monitor de Rendimiento**
 - b. Creación del conjunto de recopiladores**
 - c. Configuración de las Propiedades del Conjunto de Recopiladores de Datos**
 - d. Ejecutar el Conjunto de Recopiladores de Datos**
 - e. Detener el Conjunto y Analizar los Datos**
2. Elabora un documento y súbelo a la plataforma.