PANDORAFMS

ENTERPRISE

getEvent plugin Open

ÍNDICE

1. HISTÓRICO DE CAMBIOS

Fecha	Autor	Cambio	Versión
01/12/20	José A. Almendros	Primera version del plugin	V1r1
18/01/21	José A. Almendros	Revisión global	V1r1.2

2. INTRODUCCIÓN

Este plugin de agente permite extraer de una forma sencilla la información de los logs de Eventos de Windows que haya en un rango configurable de los últimos minutos y crear nuevos módulos con esta información, o bien mandarla directamente al recolector de logs.

3. MATRIZ DE COMPATIBILIDAD

Sistemas donde se ha probado	**Windows 10** **Windows Server 2012**

4. REQUISITOS PARA LA EJECUCIÓN DEL PLUGIN

Los requisitos para el correcto funcionamiento del plugin son los siguientes:

- Instalación del agente de Pandora FMS.

- Permisos del sistema para el usuario que ejecuta el agente de Pandora FMS como "Administrador Local"

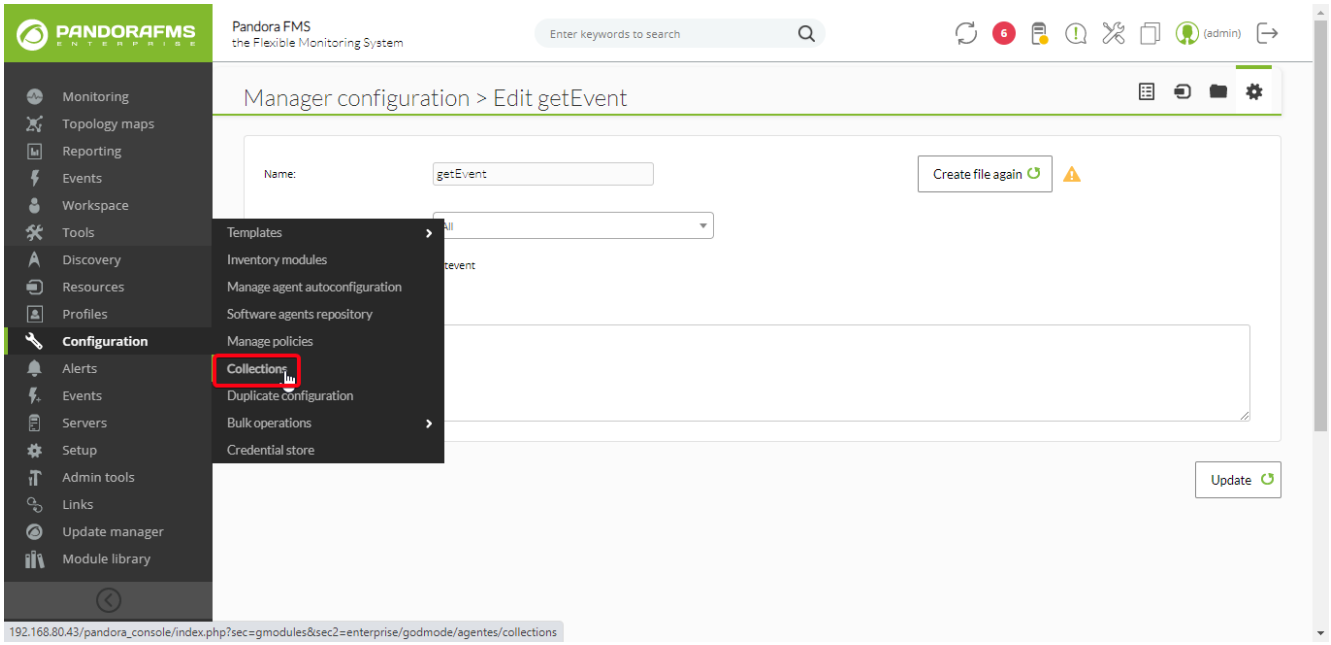
- Política de ejecución de scripts de Powershell establecida como RemoteSigned o inferior:

```
Set-ExecutionPolicy RemoteSigned
```

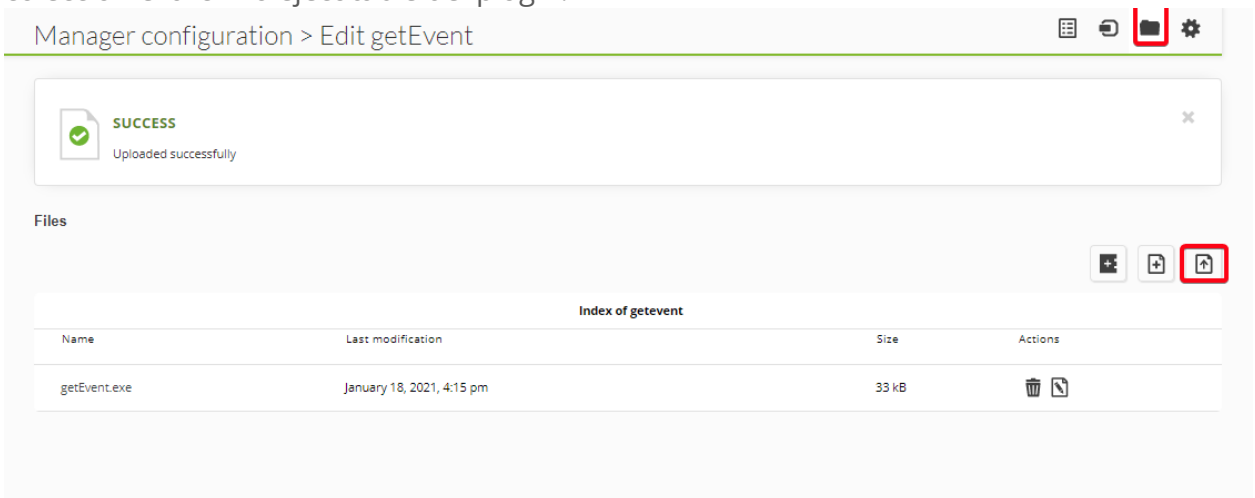
5. INSTALACIÓN DEL PLUGIN

Se explicará la forma de ejecutar el plugin distribuido mediante colecciones desde la consola de Pandora FMS. De esta forma será posible desplegarlo en varios servidores al mismo tiempo mediante el sistema de políticas.

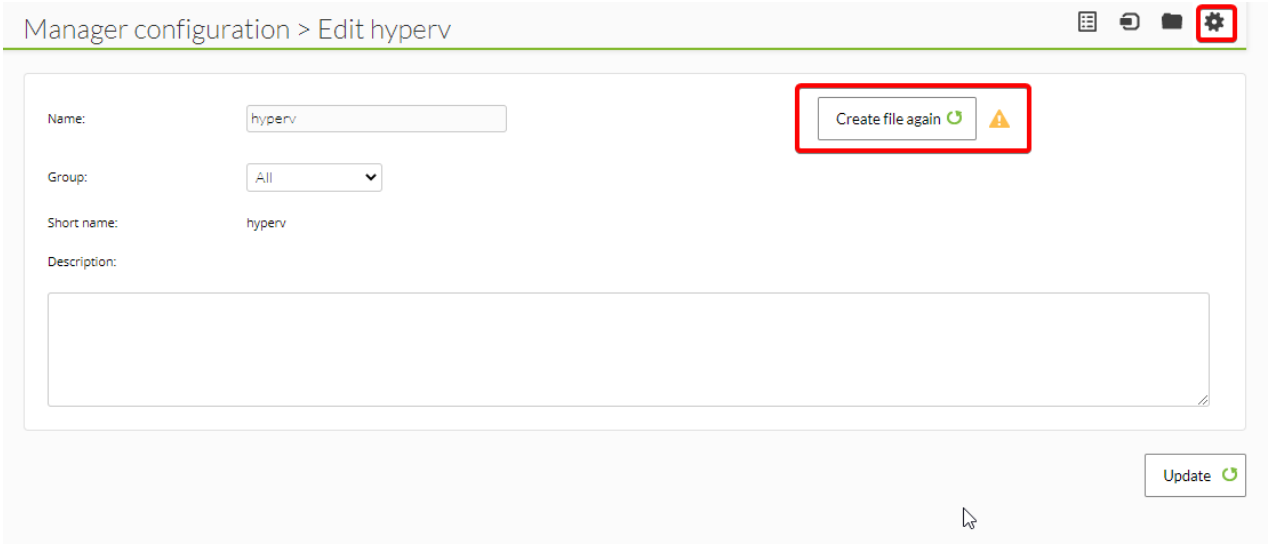
Primero, crearemos la colección desde la sección Configuration > Collections con el nombre "getEvent" y el nombre corto "getevent":



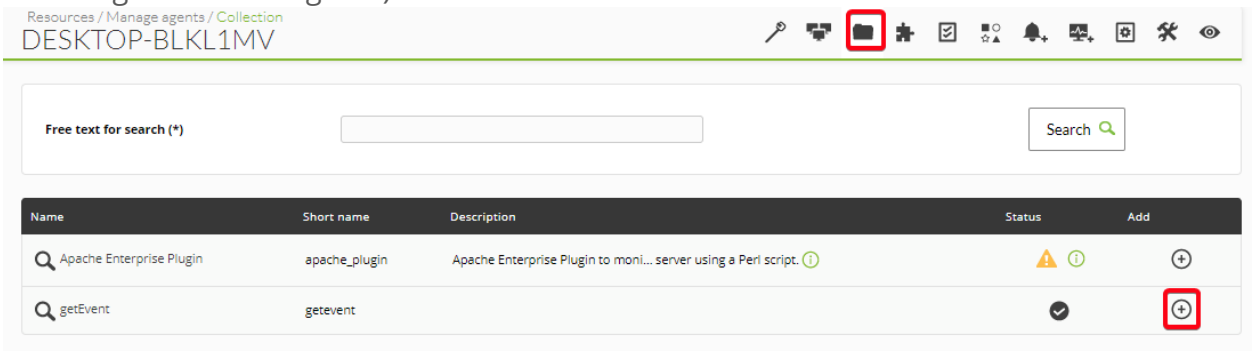
Después dentro de la pestaña Files, pulsaremos en el botón "Upload Files" para subir a la colección el archivo ejecutable del plugin:



En la sección Data de la colección, pulsaremos en "Create File again" para que se regenere la colección con los archivos subidos.



Ahora agregaremos la colección al agente equipo en el que queremos lanzar el plugin, pulsando en el botón del "+" en la colección de "getEvent" en la sección de Collection del modo administración (o bien añadiendo la línea "file_collection getEvent" al final del fichero de configuración del agente):



Por último añadiremos la línea de ejecución del plugin en el fichero de configuración del agente:

```
module_plugin
"%ProgramFiles%\pandora_agent\collections\getevent\getEvent.exe"
[event_source] [log_name] [interval] *[-nodatalist] *[-sendlog]
```

En caso de que no hayamos utilizado colecciones para desplegar el plugin y lo hayamos copiado en el equipo del servidor a mano, simplemente habría que añadir la línea anterior con las rutas correctas del fichero ejecutable. Los parámetros del plugin se explican en el siguiente punto.

6. PARÁMETROS DEL PLUGIN

Como se ha visto en el punto anterior, la forma correcta de lanzar el plugin es la siguiente:

[ruta_al_plugin]getEvent.exe" [event_source] [log_name] [interval] *[-nodatalist] *[-sendlog]

Donde:

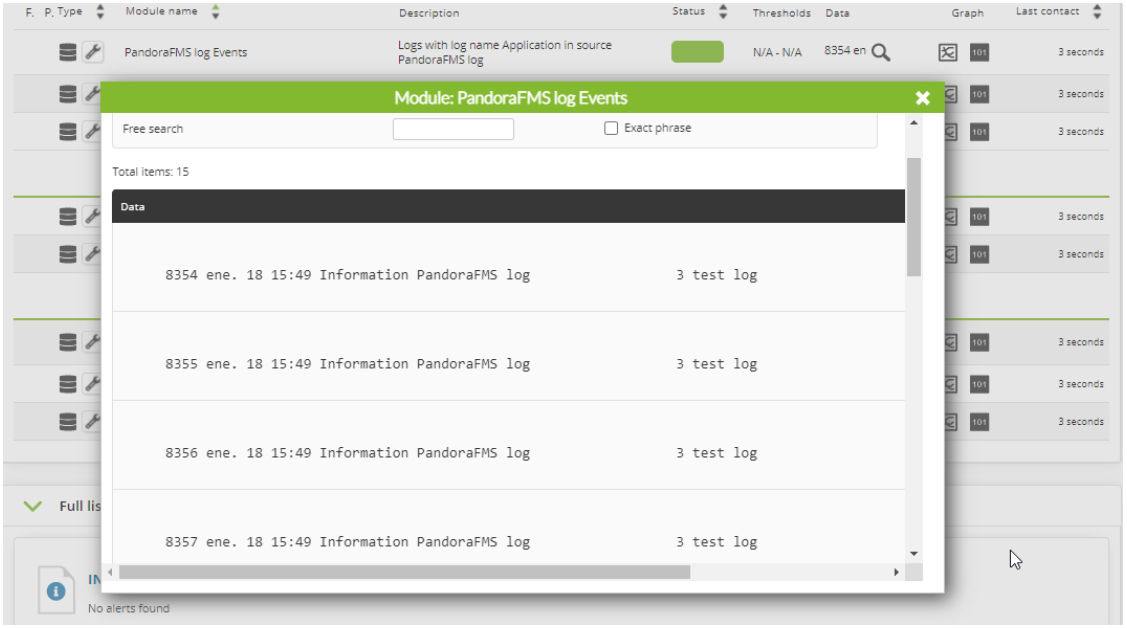
event_source: campo Origen del evento
log_name: campo Nombre del Registro del evento
interval: rango de tiempo desde el que se extraerán los logs de eventos en minutos. Por ejemplo "5" extraería los logs de los últimos 5 minutos. Se recomienda que coincida con el intervalo del agente desde el que se lanza el plugin.
-nodatalist *[opcional]*: inserta todas las líneas de logs en un solo dato del módulo.
-**sendlog** *[opcional]*: en lugar de crear un módulo, envía la salida al recolector de logs.

Es posible obtener la ayuda del plugin si se lanza con menos de tres parámetros.

7. CAPTURAS DE RESULTADOS

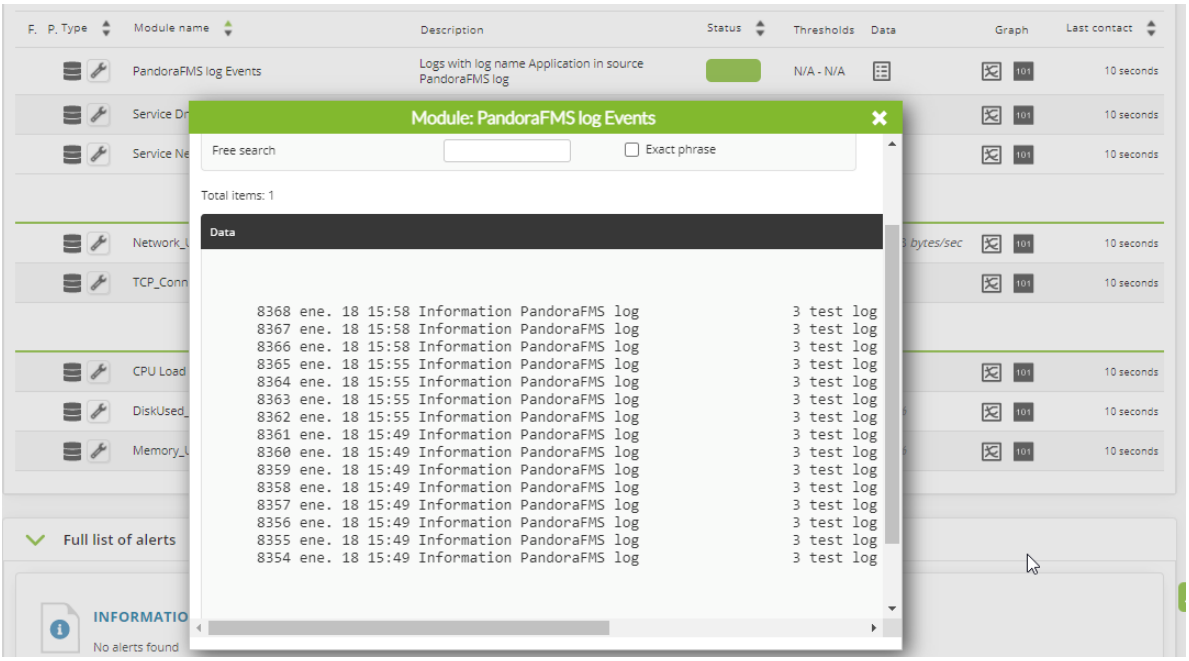
7.1 Formato datalist (por defecto)

Lanzando el plugin sin parámetros opcionales se obtienen los resultados en formato datalist, esto es, añadiendo en el módulo un dato en base de datos por cada una de las líneas obtenidas:



7.2 Formato nodatalist

Lanzando el plugin con el parámetro *–nodatalist* se insertan todas las líneas resultantes en un único dato del módulo.



7.3 Formato sendlog

Lanzando el plugin conel parámetro *–sendlog* se envía la salida del plugin al recolector de logs configurado en el sistema de Pandora FMS. En este caso no se crea ningún módulo en el agente que lanza el plugin.