PANDORAFMS

ENTERPRISE

getEvent plugin Open

INDEX

1. CHANGELOG

Date	Author	Cambio	Version
01/12/20	José A. Almendros	First plugin version	V1r1
18/01/21	José A. Almendros	Manual interval added	V1r1.2

2. INTRODUCTION

This agent plugin allows to easily extract the information from the Windows Events logs in a configurable time range of the last minutes and create new modules with this information, or send it directly to the log collector.

3. COMPABILITY MATRIX

Systems where it has been tested	**Windows 10** **Windows Server 2012**

4. REQUIREMENTS FOR PLUGIN EXECUTION

The requirements for the proper functioning of the plugin are as follows:

- To install the Pandora FMS agent.

- System permissions for the user that runs the Pandora FMS agent as "Local Administrator”

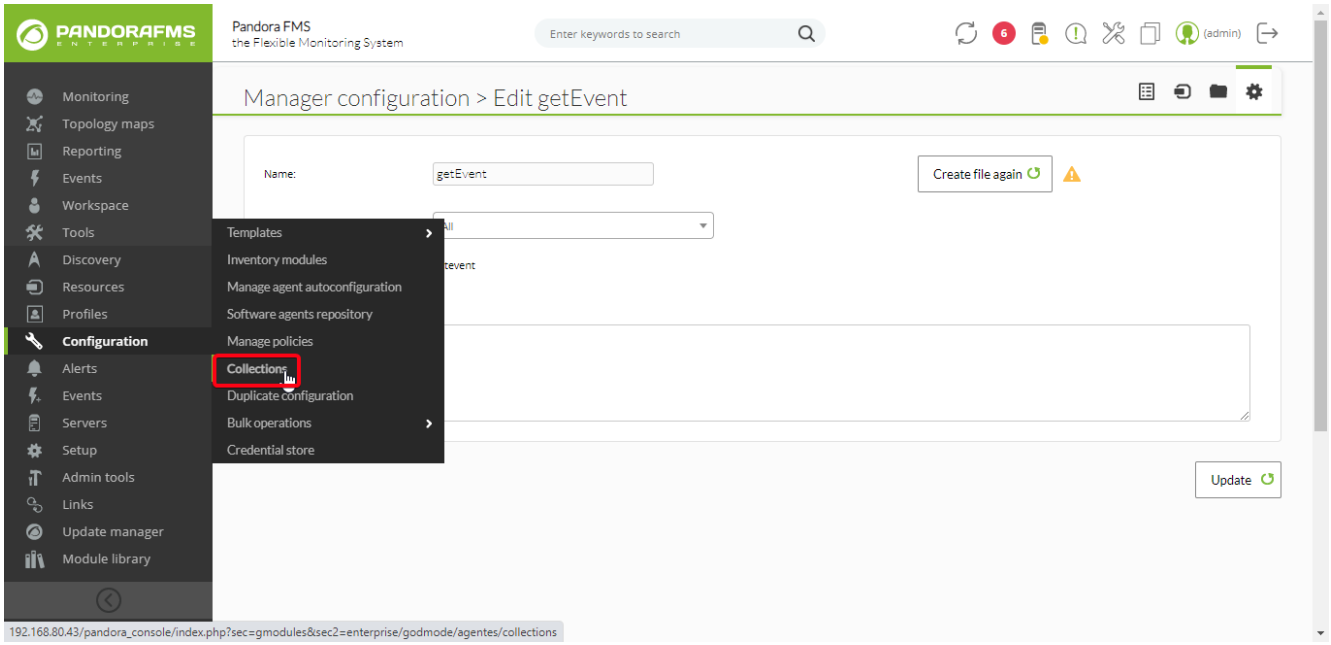
- Scripts executions policy set as RemoteSigned or lower:

```
Set-ExecutionPolicy RemoteSigned
```

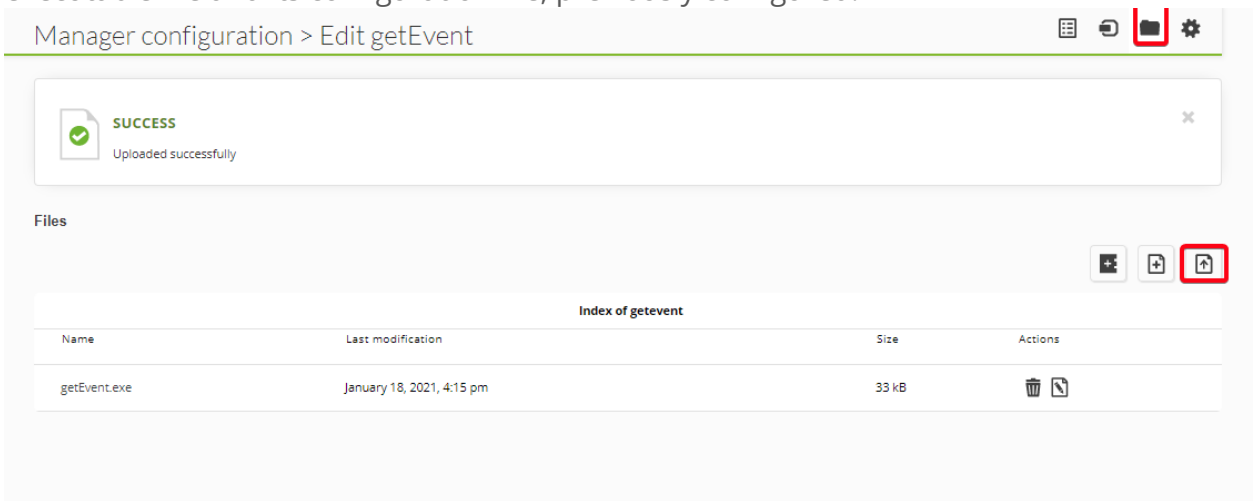
5. PLUGIN INSTALLATION

The way to execute the plugin distributed through collections from Pandora FMS console will be explained. This way it will be possible to deploy it in several servers at the same time in case of having more than one server through the policy system.

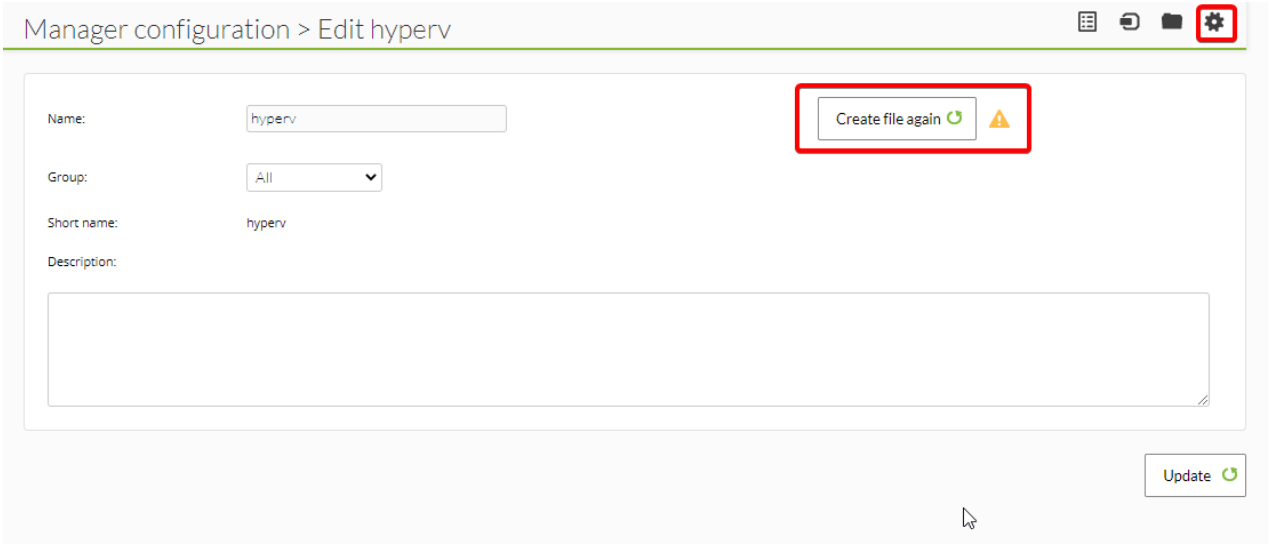
First, we will create the collection from the Configuration > Collections section with the name “getEvent” and short name “getevent”:



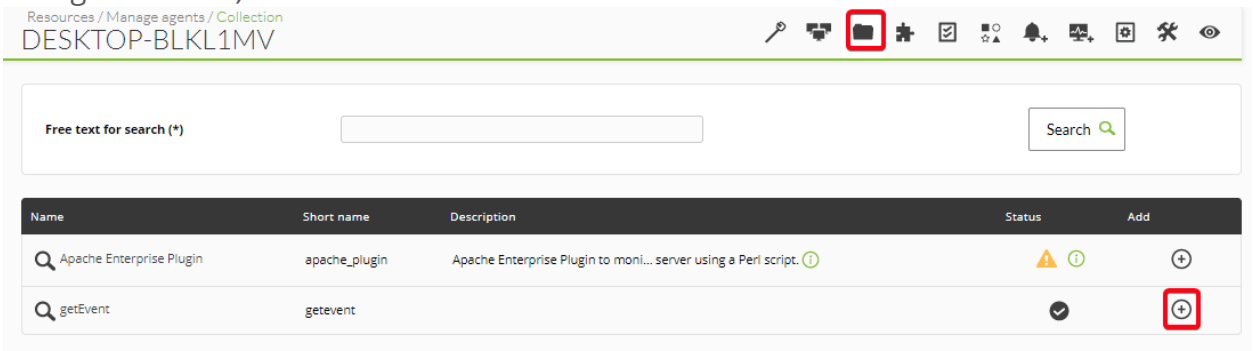
Then, we will press on the "Upload Files" button to upload to the collection the plugin's executable file and its configuration file, previously configured:



In the Data section of the collection, click on "Create File again" to regenerate the collection with the uploaded files.



Now we will add the collection to the server agent where we want to launch the plugin, clicking on the "+" button in the "getEvent" collection in the Collection section of the administration mode (or adding the line "file_collection getEvent" at the end of the agent configuration file):



Finally we will add the plugin execution line in the agent configuration file:

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

In case we haven't used collections to deploy the plugin and have copied it to the server machine by hand, we would simply add the line above with the correct path from the executable file.
Plugin parameters are explained in the next point.

6. PARÁMETROS DEL PLUGIN

As we have seen in the previous point, the correct way to launch the plugin is as follows:

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

Being:

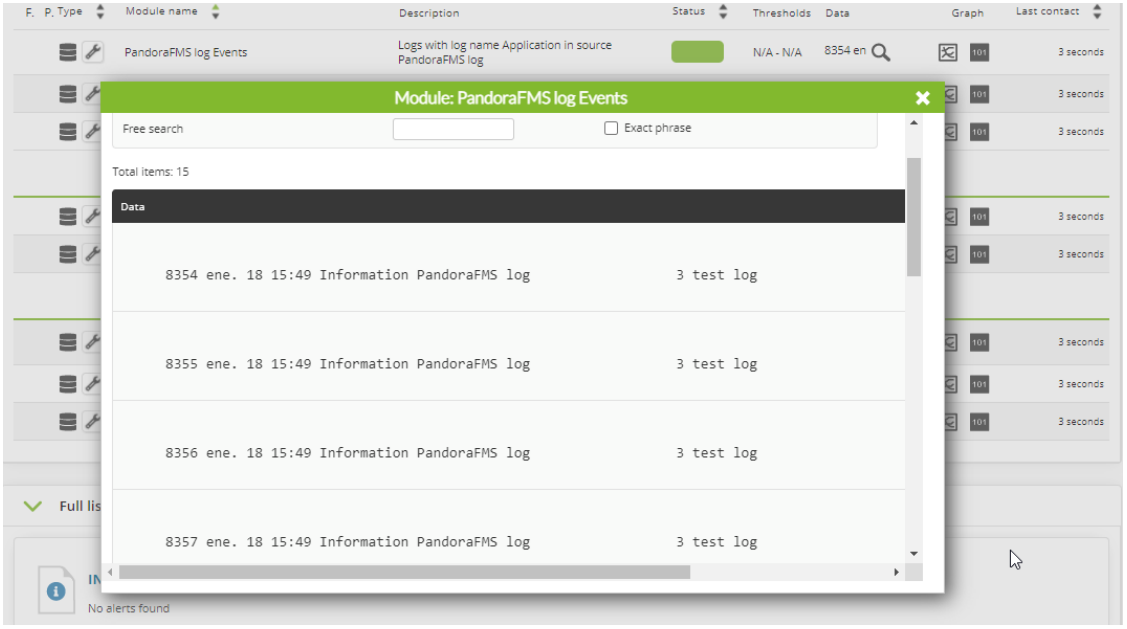
event_source: field Source of the event
log_name: field Log Name of the event
interval: time range from which event logs will be extracted in minutes. For example "5" would extract the logs of the last 5 minutes. It is recommended that it matches the agent interval from which the plugin is launched.
-nodatalist *[optional]*: inserts all the log lines in a single module data.
-**sendlog** *[optional]*: Instead of creating any module, it sends the output to the log collector.

It is possible to get the help of the plugin if it is launched with less than three parameters.

7. SCREENSHOTS OF RESULTS

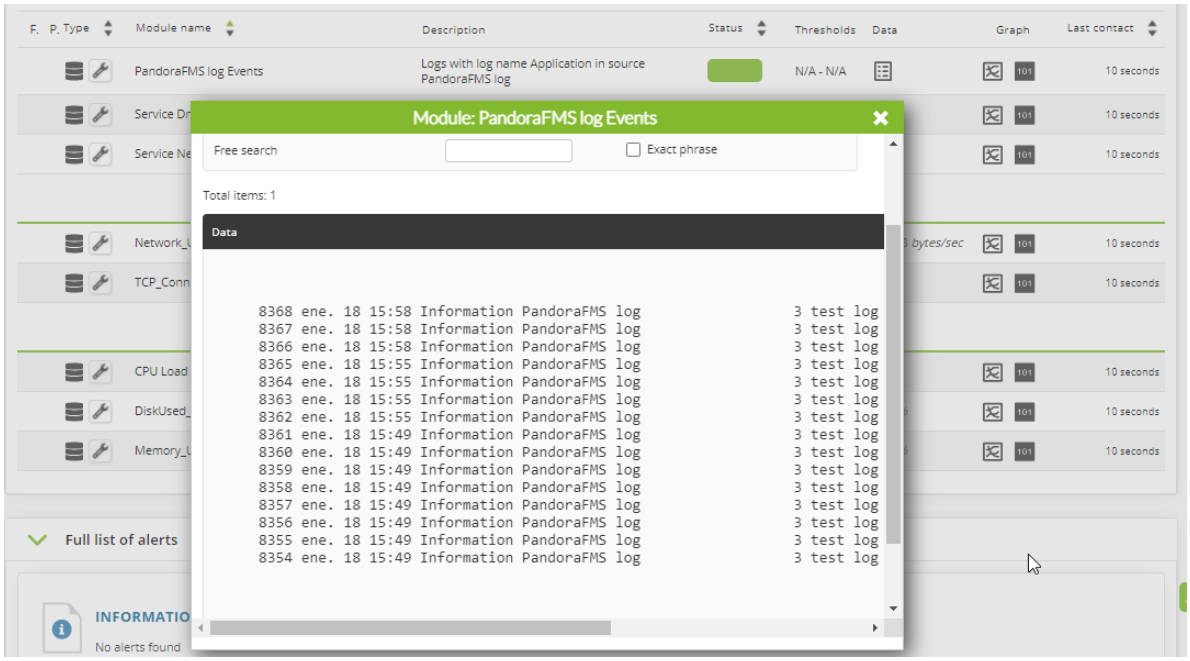
7.1 Datalist format (as default)

Launching the plugin without optional parameters, the results are obtained in datalist format, that is, adding in the module a data in the database for each of the lines obtained:



7.2 nodatalist format

Launching the plugin with *–nodatalist* parameter, all the resulting lines are inserted into a single module data.



7.3 sendlog format

Launching the plugin with *–sendlog* parameter, the output of the plugin is sent to the log collector configured in Pandora FMS system. In this case, no module is created in the agent that launches the plugin.