# Log collection and monitoring

# Log collection and monitoring

We are working on the translation of the Pandora FMS documentation. Sorry for any inconvenience.

## Introduction

Log monitoring in Pandora FMS is established in two different ways:

1. Based on modules: It represents logs in Pandora FMS as asynchronous monitors, being able to associate alerts to detected entries that meet a series of conditions preconfigured by the user. The modular representation of the logs allows:
    1. Creating modules that count the occurrences of a regular expression in a log.
    2. Obtaining the lines and context of the log messages.
2. Based on combined display: It allows the user to see in a single Console all the log information from multiple sources that is desired to be captured, organizing the information sequentially, using the timestamp in which the logs were processed.

Starting with version 7.0 NG 774, Pandora FMS incorporates OpenSearch to store log information. See also "OpenSearch installation and configuration".

## How it works

- The logs analyzed by the Software Agents (eventlog or text files), are forwarded to Pandora FMS server, in RAW form within the XML agent report.
- The Pandora FMS Data Server receives the agent's XML, which contains both monitoring and log information.
- When the Data Server processes the XML data, it identifies the information in the logs, saving in the main database the references of the reporting agent and the source of the log and then automatically sending the information to OpenSearch.
- Pandora FMS stores data in OpenSearch indexes, generating a unique index daily for each Pandora FMS instance.
- Pandora FMS server has a maintenance task that deletes the indexes at the interval defined by the system administrator (by default, 30 days).

## Log collection

Starting with version 7.0 NG 774, Pandora FMS incorporates OpenSearch to store log information; first have said server before starting to collect logs. See also "OpenSearch installation and configuration".

## Console Settings

To activate the log display system you must activate Management → Setup → Setup → Enterprise. Click Activate Log Collector and click Update.

A new tab called Log Collector will appear in which it first shows the connection status (OpenSearch status) with the OpenSearch server. The following values must be configured in the OpenSearch options section:

1. OpenSearch IP: IP address of the OpenSearch server to use with Pandora FMS.
2. Use https: Must be enabled if the installed OpenSearch environment has HTTPS enabled for its connection.
3. OpenSearch Port: TCP port number.
4. Days to purge old information: Number of days before deleting the collected data.
5. Basic authentication: (optional) if basic authentication has been installed in OpenSearch (recommended) the user (User) and password (Password) must be entered.

## Agent configuration

Log collection is done through agents, both in the agent for Microsoft Windows® and in Unix® agents (Linux®, MacOS X®, Solaris®, HPUX®, AIX®, BSD®, etc.). In the case of MS Windows® agents, information can also be obtained from the operating system's event viewer, using the same filters as in the event viewer monitoring module.

#### Example on MS Windows

For version 774 or later, the lines that appear under `Logs extraction` must be uncommented:

```
# Log extraction
#module_begin
#module_name X_Server_log
#module_description Logs extraction module
#module_type log
#module_regexp C:\server\logs\xserver.log
#module_pattern .*
#module_end
```

For more information about the description of log type modules, check the following section referring to Specific directives.

```
module_type log
```

By defining this type of tag, `module_type log`, it is indicated that it must not store in the

database, but rather it must be sent to the log collector. Any module with this type of Data will be sent to the collector, as long as it is enabled: otherwise the information will be discarded.

For versions prior to 774:

Starting with version 750, this action can be performed
using the agent plugins by activating the Advanced option.

Executions of the type shown below may be carried out:

logchannel module

```
module_begin
module_name MyEvent
module_type log
module_logchannel
module_source <logChannel>
module_eventtype <event_type/level>
module_eventcode <event_id>
module_pattern <text substring to match>
module_description <description>
module_end
```

logevent module

```
module_begin
module_name Eventlog_System
module_type log
module_logevent
module_source System
module_end
```

regexp module

```
module_begin
module_name PandoraAgent_log
module_type log
module_regexp <%PROGRAMFILES%>\pandora_agent\pandora_agent.log
module_description This module will return all lines from the specified logfile
module_pattern .*
module_end
```

**Example on Unix systems**

For version 774 or later, the lines that appear under `Logs extraction` must be *uncommented*:

```
# Log extraction
#module_begin
#module_name Syslog
#module_description Logs extraction module
#module_type log
#module_regexp /var/log/logfile.log
#module_pattern .*
#module_end
```

For more information about the description of log type modules check the following section referring to Specific directives.

```
module_type log
```

By defining this type of tag, `module_type log`, it is indicated that it must not be stored in the database, but rather that it must be sent to the log collector. Any module with this type of data will be sent to the collector, as long as it is enabled: otherwise the information will be discarded.

For versions earlier than 744:

```
module_plugin grep_log_module /var/log/messages Syslog \.\*
```

Similar to the log parsing plugin (grep_log), the grep_log_module plugin sends the processed log information to the Log Collector with the name “Syslog” as the source. It uses the regular expression `\.\*` (in this case “everything”) as a pattern when choosing which lines to send and which not to send.

### Pandora FMS Syslog Server

E This component allows Pandora FMS to analyze the syslog of the machine where it is located, analyzing its content and storing the references in the corresponding OpenSearch server.

https://www.rsyslog.com/

The main advantage of Syslog Server is to complement log unification. Supported by Syslog Server's export features from Linux® and Unix® environments, Syslog Server allows querying logs regardless of their source, searching in a single common point (Pandora FMS console log viewer).

The installation of Syslog Server 8.2102 must be performed on both the client and the server:

```
dnf install rsyslog
```

Access the configuration file `/etc/rsyslog.conf` to enable TCP and UDP input.

```
  (...)

# Provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# Provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

  (...)
```

Restart the rsyslog service. Once the service is available, verify that port 514 is accessible with:

```
netstat -ltnp
```

On the client it is configured so that it can send logs to the Syslog Server, access rsyslog `/etc/rsyslog.conf` . Locate and enable the line that allows you to configure the remote host (change `remote-host` to the server's IP address):

```
action(type="omfwd Target="remote-host" Port="514" Protocol="tcp")
```

The size of the logs received by rsyslog is 8 kilobytes by default. If larger logs are received, new entries are added with the remaining content until the complete log is received. These new entries do not contain the name of the host that sent the log, so this behavior can cause both new unwanted log sources and new agents to be created in the console. To avoid this, it is recommended to increase the size of the logs received by adding the following line:

```
$MaxMessageSize 512k
```

Save the file and exit the text editor.

Sending logs generates a container agent with the client's name, so it is recommended to create the agents with “alias as name” making it match the client's hostname, thus avoiding duplicity in agents.

To activate this feature in Pandora FMS Server, enable the following content in `pandora_server.conf` file:

```
# Enable (1) or disable (0) the Pandora FMS Syslog Server
# (PANDORA FMS ENTERPRISE ONLY).
```

```
syslogserver 1

# Full path to syslog's output file (PANDORA FMS ENTERPRISE ONLY).
syslog_file /var/log/messages

# Number of threads for the Syslog Server
# (PANDORA FMS ENTERPRISE ONLY).
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
# producer on each run (PANDORA FMS ENTERPRISE ONLY).
syslog_max 65535
```

Remember that you need to modify the configuration of your device so that logs are sent to Pandora FMS server.

#### Filters at PFMS server level

On Pandora FMS server, using the token syslog_whitelist, you may admit only logs that match a regular expression or regexp, which is case-sensitive (e.g. `windows` is not the same as `Windows`) and discard everything else.

With the token syslog_blacklist you may deny logs that match the set regexp (and let everything else in).

Both tokens are disabled by default.

- syslog_whitelist: By activating this tokenl only logs that comply with the regexp will be accepted and the rest will be discarded.
  - If this token is activated and you have the default filter `.*`, everything will be accepted.
  - Important: If said token is activated WITHOUT regexp, NOTHING will be admitted.
- Filtering of allowed keywords is done first, this reduces the work for the next step.
- syslog_blacklist: Placing a regexp will discard everything that complies with it (if this token is activated but left WITHOUT regexp, NOTHING will be blocked.).
- Filtering by syslog_blacklist is done last.

## OpenSearch interface

ENG version 774 or later.

## Display and search

In a log collection tool, two features are mainly of interest: being able to search for information - filtering by date, data sources and/or keywords, etc. - and being able to see that information

(menu Operation → Monitoring → Log viewer) drawn in occurrences per time unit.

The most important -and useful- field will be the search string to be entered in the Search text box in combination with the three available search types (Search mode):

- Exact match: Literal string search, the log contains an exact match.
- All words: Search that contains all the indicated words, regardless of the order in the same log line.
- Any word: Search that contains any of the indicated words, regardless of the order.
- If you check the option to see the context of the filtered content, you will get an overview of the situation with information from other log lines related to the search.

### Advanced Display and Search

With this feature you may display log entries graphically, classifying the information based on data capture models.

These data capture models are basically regular expressions and identifiers that allow you to parse data sources and display them as a graph.

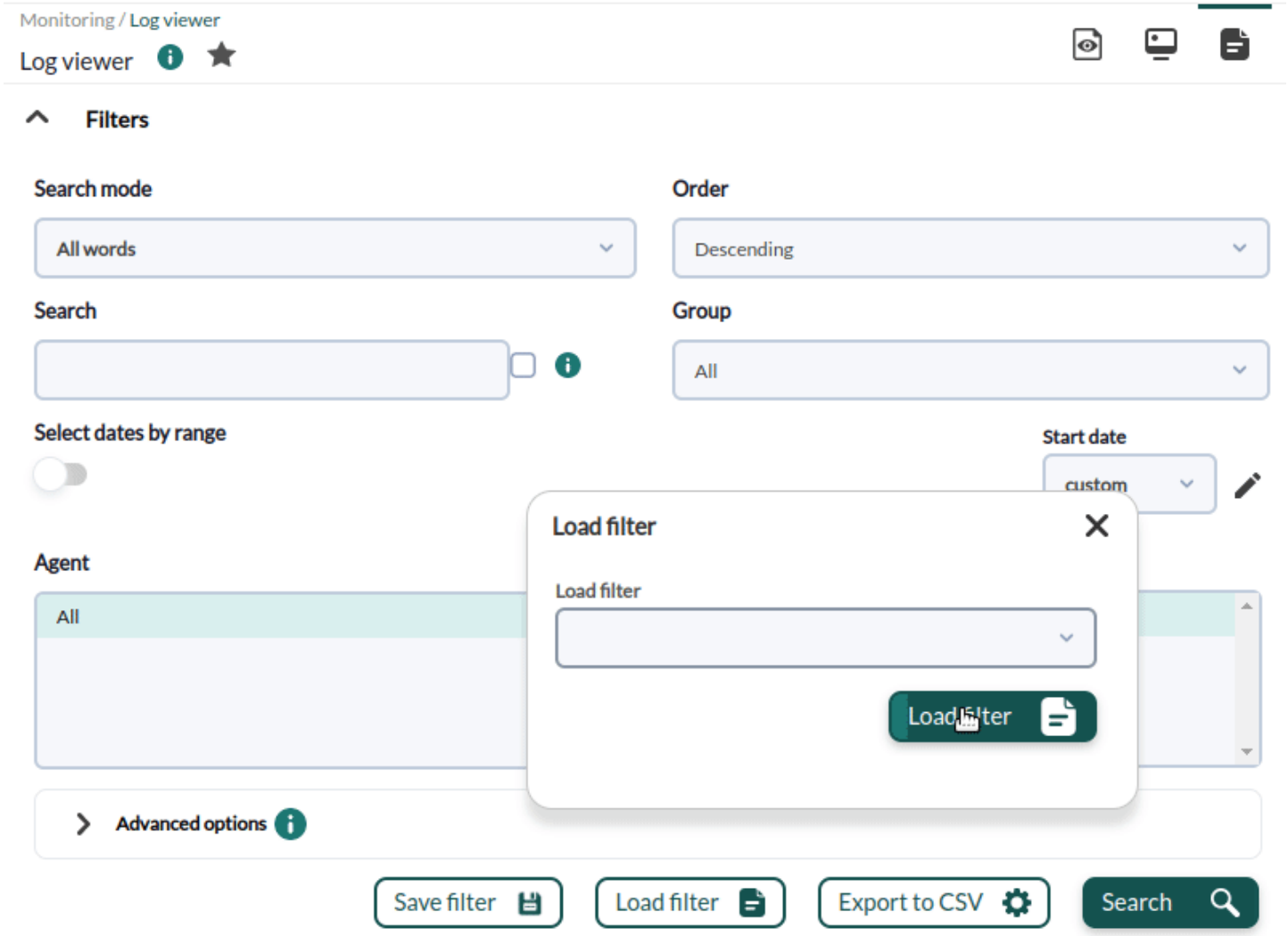
To access advanced options click on Advanced options. A form will be displayed where you may choose the type of results view:

- Show log entries (plain text).
- Show log graph.
- Using the display log graph option (Display mode) you can select the capture model (Use capture model).
- The default model, Apache log model, offers the possibility of processing or parsing Apache logs in standard format (access_log), being able to retrieve comparative graphs of response time, grouping by page visited and response code:
- You may either click edit or create to make a new capture model.

### Common filters

Version 771 or later

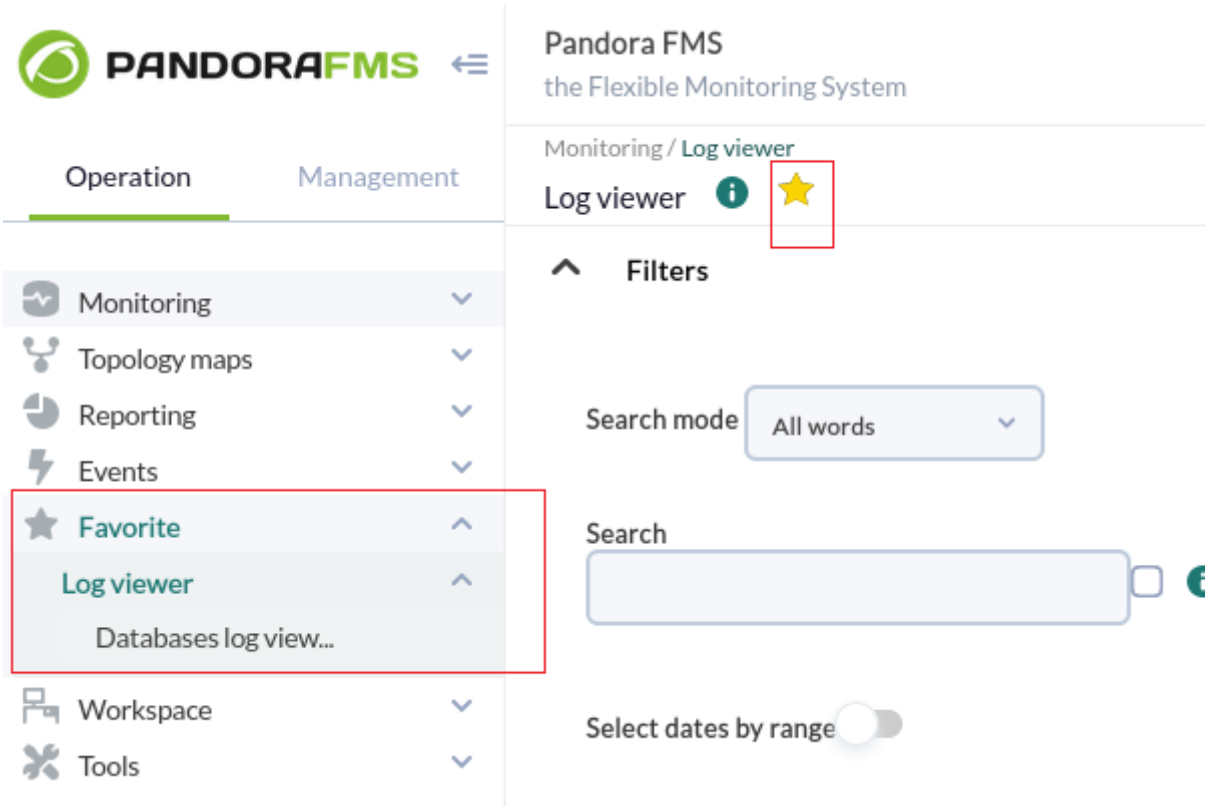
Through this option you may save frequently used filtering preferences, thus creating a list of frequent filters. When you have configured all the filter values, click Save filter, assign a name and click Save. At any other time you may load these preferences using the Load filter button, then download the list of saved filters, select one of them and click Load filter.




## Filters saved as favorite items

Version 770 or later.

Using the favorites system in PFMS you may save a shortcut for the Log viewer with filtering preferences by clicking the star icon in the section title.




## Log Source in Agent View

Starting with version 749 of Pandora FMS, a box called Log sources status has been added to the Agent View, in which the date of the last update of the logs by that agent will appear. When you click on the Review magnifying glass icon, you will be redirected to the Log Viewer view filtered by that log.

Version 774 or later: By default the data shown in both views is limited to the last 24 hours, and can be changed as needed.

Return to Pandora FMS documentation index