

localfile

XML section name

```
<localfile>
</localfile>
```

This configuration section is used to specify the collection of log data from files, Windows events, and from output of commands.

Options

- location
- command
- alias
- frequency
- only-future-events
- query
- log_format

location

Specify the location of a log or wildcarded group of logs to be read. `strftime` format strings may be used for log file names.

For instance, a log file named `file.log-2017-01-22` could be referenced with `file.log-%Y-%m-%d` (assuming today is Jan 22nd, 2017).

Wildcards may be used on non-Windows systems. When wildcards are used, the log files must exist at the time `ossec-logcollector` is started. It will not automatically begin monitoring new log files.

Note that `strftime` format strings and wildcards cannot be used on the same entry.

Default value	n/a
Allowed values	Any log file

command

A command to be run. All output from this command will be read as one or more log messages depending on whether `command` or `full_command` is used.

Default value	n/a
Allowed values	any command line, optionally including arguments

alias

This is an alias to identify the command. This will replace the command in the log message.

Default value	n/a
Allowed values	any string

For example `<alias>usb-check</alias>` would replace:

```
ossec: output: 'reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR':
```

with:

```
ossec: output: 'usb-check':
```

frequency

The minimum time in seconds between command runs. The command will probably not run every `frequency` seconds exactly, but the time between runs will not be shorter than this setting. This is used with **command** and **full_command**.

Default value	n/a
Allowed values	any positive number of seconds

only-future-events

This is for use only with the `eventchannel` log format. By default, when Wazuh starts, it will read all log content from a given Windows Event Channel since Wazuh was last stopped. Set this option to **yes** to override this behavior if desired. Then Wazuh would only receive events that occur after the Wazuh agent is started.

Default value	n/a
Allowed values	yes or no

query

This is for use only with the `eventchannel` log format. It is possible to specify an XPATH query following the event schema in order to filter the events that Wazuh will process.


Default value	n/a
Allowed values	Any XPATH query following the event schema

For example, the following configuration will only process events with an ID of 7040:

```
<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID=7040]</query>
</localfile>
```

log_format


This is the format of the log being read.

 **Note**


For most text log files that have one entry per line, you can just use syslog.

Default value	syslog	
Allowed values	syslog	This format is for plain text files in a syslog-like format. Also can be used when the logs are single line messages.
	snort-full	This is used for Snort's full-output format.
	snort-fast	This is used for Snort's fast-output format.
	squid	This is used for squid logs.
	iis	This is used for IIS logs.
	eventlog	This is used for the classic Microsoft Windows event log format.

eventchannel	<p>This is used for Microsoft Windows event logs, using the new EventApi.</p> <p>Monitorize: standard “Windows” eventlogs and “Application and Services” logs.</p>
mysql_log	<p>This is used for <code>MySQL</code> logs. It does not support multi-line logs.</p>
postgresql_log	<p>This is used for <code>PostgreSQL</code> logs. It does not support multi-line logs.</p>
nmapg	<p>Used for monitoring files conforming to the grepable output from <code>nmap</code>.</p>
apache	<p>Apache’s default log format.</p>
command	<p>Read in arbitrary output from the command (as run by root).</p> <p>Command defined by the command tag.</p> <p>Each line of output will be treated as a separate log.</p>
full_command	<p>Read in arbitrary output from the command (as run by root)</p> <p>Command defined by the command tag.</p> <p>The entire output will be treated as a single log item.</p>
djb-multilog	<p>Read files in the format produced by the multilog service logger in daemontools.</p>
multi-line	<p>Allow applications that log multiple lines per event to be monitored.</p> <p>Require the number of lines to be consistent.</p> <p><code>multi-line:</code> is followed by the number of lines in each log entry.</p> <p>Each line will be combined with the previous lines until all lines are gathered.</p> <p>There may be multiple timestamps in a finalized event.</p> <p>The format is: <code><log_format>multi-line: NUMBER</log_format></code></p>

 Warning

The eventchannel log format cannot be used on Windows agents older than Vista since they do not produce that kind of log.

 Warning

Agents will ignore `command` and `full_command` log sources unless they have `logcollector.remote_commands=1` set in their **`/var/ossec/etc/internal_options.conf`** or **`/var/ossec/etc/local_internal_options.conf`** file. This is a security precaution since it may not be permissible in all environments to allow the Wazuh manager to run arbitrary commands on agents in their root security context.

Example:

Multi-line log message in original log file:

```
Aug 9 14:22:47 hostname log line one
Aug 9 14:22:47 hostname log line two
Aug 9 14:22:47 hostname log line four
Aug 9 14:22:47 hostname log line three
Aug 9 14:22:47 hostname log line five
```

Log message as analyzed by ossec-analysisd:

```
Aug 9 14:22:47 hostname log line one Aug 9 14:22:47 hostname log line two Aug 9 14:22:47 hostname log line
three Aug 9 14:22:47 hostname log line four Aug 9 14:22:47 hostname log line five
```

Example of configuration

Linux configuration:

```
<!-- For monitor log files -->
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!-- For monitor commands output -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>
```

Windows configuration:

```
<!-- For monitor Windows eventchannel -->
<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <only-future-events>yes</only-future-events>
  <query>Event/System[EventID != 5145 and EventID != 5156]</query>
</localfile>
```