Configuration

Basic usage

Log data collection is configured in ossec.conf, mainly in the following sections: localfile, remote and global. Also, it is possible to configure it in agent.conf to centralize the distribution of these configuration settings to relevant agents.

This is a basic usage example. Provide the name of the file to be monitored and the format:

```
<localfile>
    <location>/var/log/messages</location>
    <log_format>syslog</log_format>
</localfile>
```

Monitoring logs using regular expressions for file names

Wazuh supports posix regular expressions. For example, to analyze every file that ends with a .log inside the `/var/log` directory, use the following configuration:

```
<localfile>
    <location>/var/log/*.log</location>
    <log_format>syslog</log_format>
</localfile>
```

Monitoring date-based logs

For log files that change according to the date, you can also specify a **strftime** format to replace the day, month, year, etc. For example, to monitor the log files like `C:\Windows\app\log-08-12-15.log`, where 08 is the year, 12 is the month and 15 the day (and it is rolled over every day), do:

```
<localfile>
    <location>C:\Windows\app\log-%y-%m-%d.log</location>
    <log_format>syslog</log_format>
</localfile>
```

Reading logs from Windows Event Log

To monitor a Windows event log, you need to provide the format as “eventlog” and location is the name of the event log:

```
<localfile>
    <location>Security</location>
    <log_format>eventlog</log_format>
</localfile>
```

Reading events from Windows Event Channel

You can additionally monitor specific Windows event channels. The location is the name of the event channel. This is the only way to monitor the Applications and Services logs. If the file name contains a “%4”, replace it with “/”:

```
<localfile>
    <location>Microsoft-Windows-PrintService/Operational</location>
    <log_format>eventchannel</log_format>
</localfile>
```

Filtering events from Windows Event Channel with queries

It is possible to filter the events from an event channel:

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

Using environment variables

You can use environment variables like `%WinDir%` in the location pattern. The following is an example of reading logs from an IIS server:

```
<localfile>
    <location>%WinDir%\System32\LogFiles\W3SVC3\ex%y%m%d.log</location>
    <log_format>iis</log_format>
</localfile>
```