

# 10 Log File Monitoring

## 4 Overview

Zabbix can be used for centralized monitoring and analysis of log files with/without log rotation support. Notifications can be used to warn users when a log file contains certain strings or string patterns.

2009/08/13 14:14

## 2 How it works

Monitoring of log files requires Zabbix Agent running on a host. An item used for monitoring of a log file must have type *Zabbix Agent (Active)*, its value type must be *Log* and key set to *log[file,<pattern>,<encoding>,<max lines>]* or *logrt[path to log file with filename format,<pattern>,<encoding>,<max lines>]*.

For example:

```
log["/home/user/file.log","pattern_to_match","UTF-8",100]
or
logrt["/home/user/filelog_.*_[0-9]{1,3}","pattern_to_match","UTF-8",100]
```

The last one will collect data from files such "filelog\_abc\_1" or "filelog\_\_001".

Important notes:

- The server and agent keep a trace of the monitored log's size and last modification time (for logrt) in two counters.
- The agent starts reading the log file from the point it stopped the previous time.
- The number of bytes already analyzed (the size counter) and the last modification time (the time counter) are stored in the Zabbix database and are sent to the agent, to make sure it starts reading the log file from this point.
- Whenever the log file becomes smaller than the log size counter known by the agent, the counter is reset to zero and the agent starts reading the log file from the beginning taking the time counter into account.
- All files matching the filename format in the provided directory are analyzed every cycle the agent tries to get the next line from the log (for logrt).
- If there are several matching files with the same last modification time in the directory, then the agent will read lexicographically the smallest one.
- Zabbix Agent processes new records of a log file once per *Update interval* seconds.
- Zabbix Agent does not send more than **maxlines** of a log file per second. The limit prevents overloading of network and CPU resources and overrides the default value provided for **MaxLinesPerSecond** parameter in the [configuration file of the agent](#).
- Special note for "\" path separators: if file\_format is "file\\.log", then there should not be directory "file", since it is not possible to unambiguously define whether "." is escaped or is the first symbol of the file name.

2010/02/05 13:51

From:

<https://www.zabbix.com/documentation/1.8/> - **Zabbix Documentation 1.8**

Permanent link:

[https://www.zabbix.com/documentation/1.8/manual/log\\_file\\_monitoring](https://www.zabbix.com/documentation/1.8/manual/log_file_monitoring)

Last update: **2014/09/25 15:00**

