

10 Мониторинг файлов логов

13.6 Обзор

Zabbix может использоваться для централизованного мониторинга и анализа лог-файлов как с ротацией так и лог-файлов без ротации. Оповещения могут быть использованы для предупреждения пользователей, если лог-файл содержит некоторые строки или шаблоны строк.

2009/12/13 15:13

13.2 Как это работает

Мониторинг лог файлов требует запущенного Zabbix агента на удаленном узле сети. Элемент данных используемый для мониторинга лог-файла должен иметь тип *Zabbix Агент (Активный)*, его тип значения должен быть *Журнал* и ключ должен быть установлен как *log[файл,<шаблон>,<кодировка>,<макс кол-во строк>]* или *logrt[путь к файлу журнала с форматированным именем файла,<шаблон>,<кодировка>,<макс кол-во строк>]*.

Например:

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

Последний пример будет собирать данные из файлов, таких как "filelog_abc_1" или "filelog_001".

Важные замечания:

- Сервер и агент следят за размером наблюдаемого журнала и временем последнего изменения (для logrt) в двух счетчиках.
- Агент начинает читать лог-файл с той позиции, в которой он остановился последний раз.
- Количество уже проанализированных данных (счетчик размера) и время последнего изменения (счетчик времени) хранятся в базе данных Zabbix и отправляются агенту, чтобы указать ему с какой именно позиции следует начинать читать лог-файл.
- Всякий раз, когда лог-файл становится меньше, чем известное агенту значение счетчика размера, счетчик обнуляется и агент начинает читать лог-файл с самого начала, принимая во внимание счетчик времени.
- Все файлы, соответствующие формату имени файла в соответствующей папке, анализируются каждый цикл и агент пытается получить следующую строку из лог-файла (для logrt).
- Если в папке существует несколько соответствующих файлов с тем же временем последнего изменения, то агент будет лексикографически читать наименьший из этих файлов.
- Zabbix агент обрабатывает новые записи лог-файла один раз на *Период обновления в секундах*.
- Zabbix агент отправляет не более чем **maxlines** записей из лог-файла в секунду. Это ограничение предотвращает перегрузку сети и ресурсов процессора и переопределяет

значение по умолчанию предусмотренное параметром **MaxLinesPerSecond** в [файле настроек агента](#).

- Специальное примечание для разделителей пути “\”: если формат файла представлен как “file\log”, тогда там не должно быть папки “file”, поскольку невозможно однозначно определить, экранируется ли это символ “.” или это первый символ в имени файла.

2009/12/13 15:26

From:

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

Permanent link:

https://www.zabbix.com/documentation/1.8/ru/manual/log_file_monitoring

Last update: **2014/09/25 14:52**

