

Утилита logtop. Работа с журналами логов Nginx.

Category: GNU/Linux, logtop, утилиты
2025-07-25

Введение.

Для того, чтобы держать ситуацию под контролем, всегда нужно знать что происходит на вашей территории, в вашей операционной системе. Для этого существует много интересных способов анализа файлов журналирования.

Например, утилита **Logtop** – это удобный анализатор журналов, который может показывать статистику в реальном времени из любого заданного текстового файла.

Ссылка на **GitHub** утилиты Logtop: <https://github.com/JulienPalard/logtop>.

Установка Logtop.

К сожалению установить эту утилиту из стандартных репозиториев для **Rocky Linux** не удастся, но её можно скомпилировать.

В **Debian** эта утилита имеется в стандартных репозиториях.

```
$ sudo apt install logtop
```

Установка зависимостей.

Прежде чем собирать **logtop** для **Rocky Linux**, убедитесь, что у вас установлены необходимые зависимости:

```
$ sudo dnf install -y gcc make git ncurses-devel uthash-devel
```

Клонирование репозитория.

Установим зависимости и исходные коды с **GitHub**:

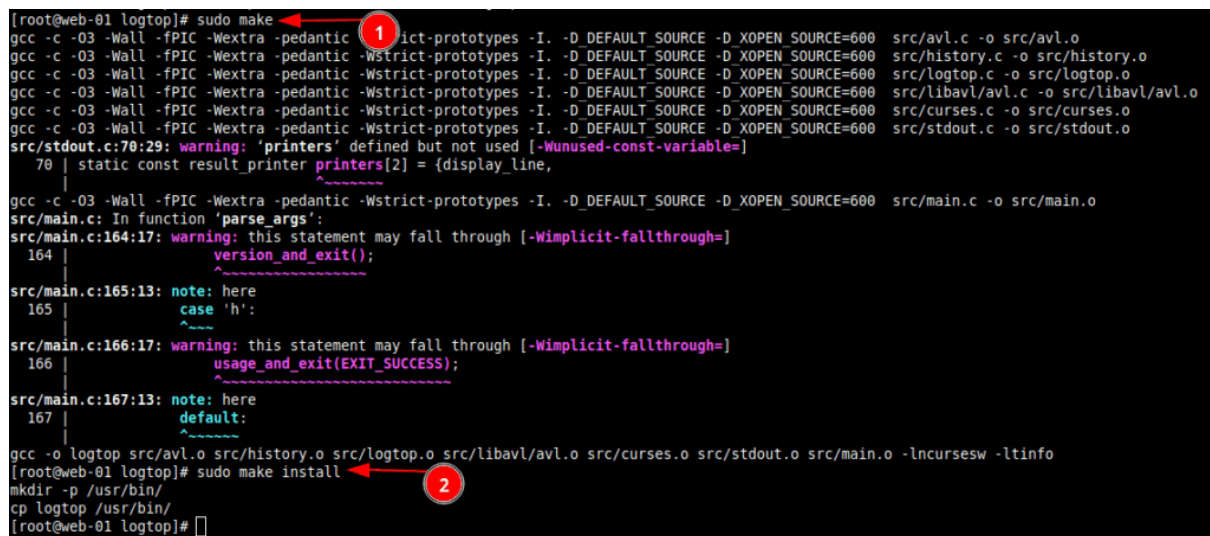
```
$ cd ~  
$ git clone https://github.com/JulienPalard/logtop.git  
$ cd logtop
```

Сборка и установка.

Скопируйте файл `uthash.h` в системный каталог для заголовочных файлов:

```
$ sudo cp /usr/include/uthash.h ~/logtop
$ sudo make
$ sudo make install
```

Ответ:



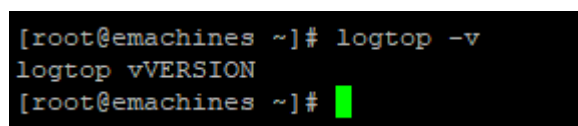
```
[root@web-01 logtop]# sudo make
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/avl.c -o src/avl.o
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/history.c -o src/history.o
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/logtop.c -o src/logtop.o
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/libavl/avl.c -o src/libavl/avl.o
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/curses.c -o src/curses.o
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/stdout.c -o src/stdout.o
src/stdout.c:70:29: warning: 'printers' defined but not used [-Wunused-const-variable=]
70 | static const result_printer printers[2] = {display_line,
    |                               ^~~~~~
gcc -c -O3 -Wall -fPIC -Wextra -pedantic -Wstrict-prototypes -I. -D DEFAULT_SOURCE -D XOPEN_SOURCE=600 src/main.c -o src/main.o
src/main.c: In function 'parse_args':
src/main.c:164:17: warning: this statement may fall through [-Wimplicit-fallthrough=]
164 |         version_and_exit();
    |         ^~~~~~
src/main.c:165:13: note: here
165 |         case 'h':
    |         ^~~~
src/main.c:166:17: warning: this statement may fall through [-Wimplicit-fallthrough=]
166 |         usage_and_exit(EXIT_SUCCESS);
    |         ^~~~~~
src/main.c:167:13: note: here
167 |         default:
    |         ^~~~~~
gcc -o logtop src/avl.o src/history.o src/logtop.o src/libavl/avl.o src/curses.o src/stdout.o src/main.o -lnursesw -ltinfo
[root@web-01 logtop]# sudo make install
mkdir -p /usr/bin/
cp logtop /usr/bin/
[root@web-01 logtop]#
```

Проверка установки.

После установки вы можете проверить, что **logtop** работает корректно:

```
$ sudo logtop -v
```

Ответ:



```
[root@emachines ~]# logtop -v
logtop vVERSION
[root@emachines ~]#
```

Использование.

```
$ sudo logtop --help
```

Ответ:

```
[root@web-01 logtop]# sudo logtop --help
Usage: tail -f something | logtop [OPTIONS]
  -s, --size=NUM          Number of log line to keep in memory
                           Defaults to : 10000
  -q, --quiet              Quiet, only display a top 10 at exit.
  -l, --line-by-line=NUM  Print result line by line
                           in a machine friendly format,
                           NUM: quantity of result by line.
  -i, --interval=NUM      Interval between graphical updates,
                           in seconds. Defaults to 1.

Line by line format is : [%d %f %s\t]*\n
  %d : Number of occurrences
  %f : Frequency of apparition
  %s : String (Control chars replaced by dots).
```

Синтаксис:

```
$ sudo tail -f лог_файл.log | logtop [ОПЦИИ]
```

Опции:

- **-s, --size=NUM** — Указывает, сколько строк лога хранить в памяти для анализа. По умолчанию используется 10 000 строк.
- **-q, --quiet** — Включает “тихий режим”, при котором **logtop** выводит только топ-10 результатов при завершении работы.
- **-l, --line-by-line=NUM** — Переключает вывод в формат, удобный для обработки программами. NUM задаёт количество результатов на одну строку.
- **-i, --interval=NUM** — Задаёт интервал (в секундах) между обновлениями графического вывода. По умолчанию — 1 секунда.

Формат построчного вывода:

```
[%d %f %s\t]*\n
```

- **%d** — Количество вхождений или случаев.
- **%f** — Частота появления или повторения.
- **%s** — Строка (управляющие символы заменены точками).

Примеры использования.

Пример 1.

Например, чтобы следить за изменениями в файле `/var/log/messages`, выполните:

```
$ sudo logtop /var/log/messages
```

Пример 2.

Здесь **logtop** будет анализировать последние 5000 строк журнала и обновлять вывод каждые 2 секунды.

```
$ sudo tail -f /var/log/syslog | logtop -s 5000 -i 2
```

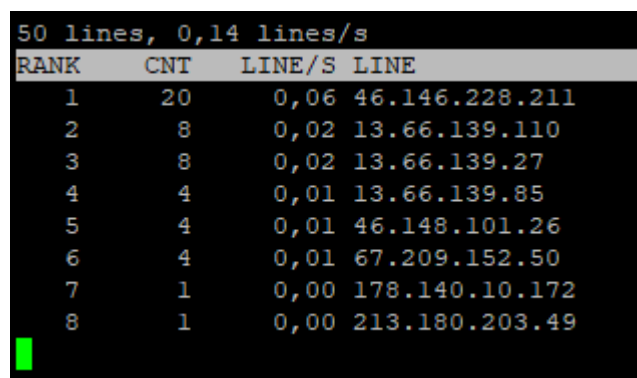
Пример 3.

Позволяет получить общую картину: распределение уникальных **IP-адреса**, с которых идут запросы, количество запросов с одного **IP-адреса** и так далее.

Посмотрим активность на текущем сайте, откуда его сейчас просматривают:

```
$ sudo tail -f /var/log/nginx/access.log | awk {'print $1; fflush  
()};' | logtop
```

Ответ:



50 lines, 0,14 lines/s			
RANK	CNT	LINE/S	LINE
1	20	0,06	46.146.228.211
2	8	0,02	13.66.139.110
3	8	0,02	13.66.139.27
4	4	0,01	13.66.139.85
5	4	0,01	46.148.101.26
6	4	0,01	67.209.152.50
7	1	0,00	178.140.10.172
8	1	0,00	213.180.203.49

Где в данном случае колонки означают:

1. **RANK** — порядковый номер.
2. **CNT** — количество запросов с данного **IP-адреса**.
3. **LINE/S** — количество запросов в секунду с данного **IP-адреса**.
4. **LINE** — сам **IP-адрес**.
5. Вверху показывается **суммарная статистика** по всем запросам.

Таким образом можно посмотреть и другие логи по аналогии. Просто замените путь на ваш log-файл и утилита его исследует.

Оригиналы источников информации.

1. [github.com](https://github.com/JulienPalard/logtop) «JulienPalard/logtop».
2. idroot.us «How To Install Logtop on CentOS 7».
3. habr.com «Пара полезных команд, которые могут пригодиться при DDoS и не только».

4. cyberciti.biz «Linux / Unix logtop: Realtime Log Line Rate Analyser».