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**:

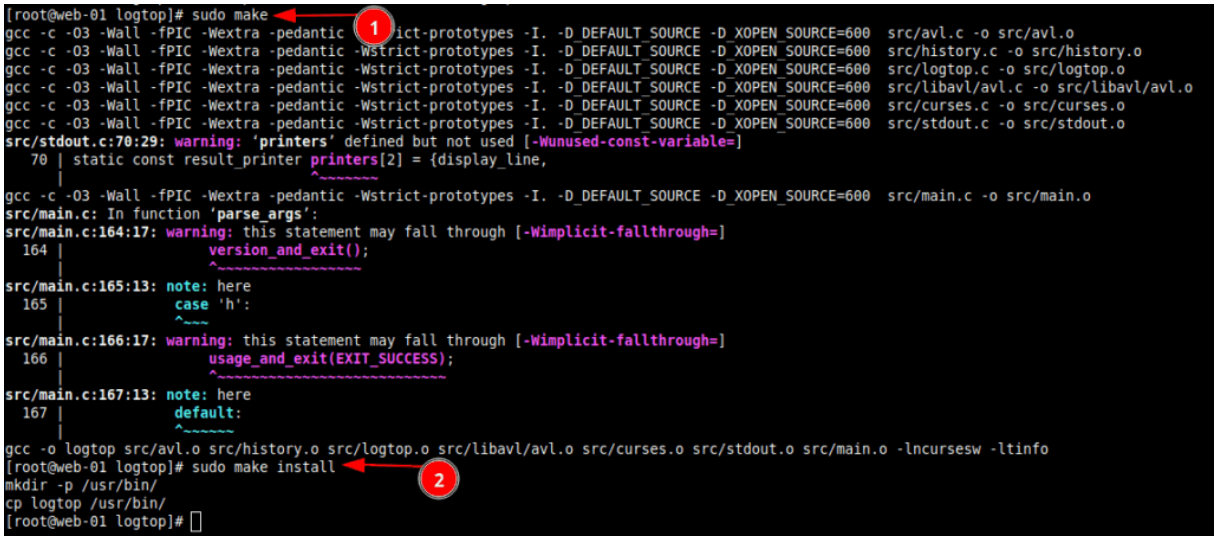
```
$ cd ~
$ git clone https://github.com/JulienPalard/logtop.git
$ cd logtop
```

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:

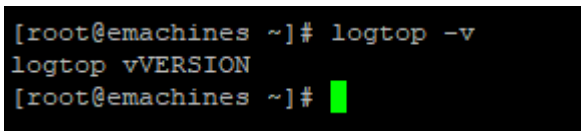


Проверка установки.

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

```
$ sudo logtop -v
```

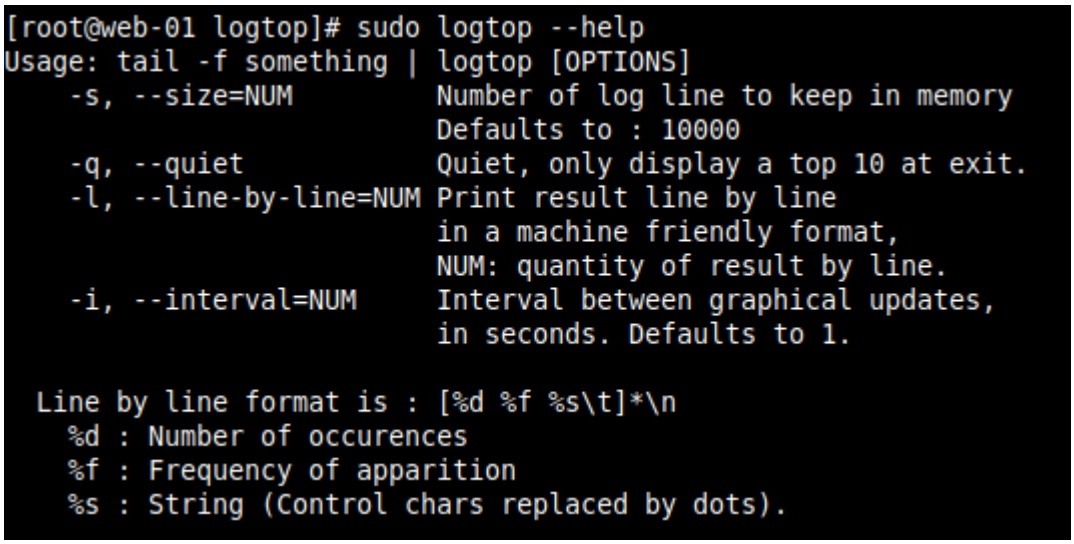
Ответ:



Использование.

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

Ответ:



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
```

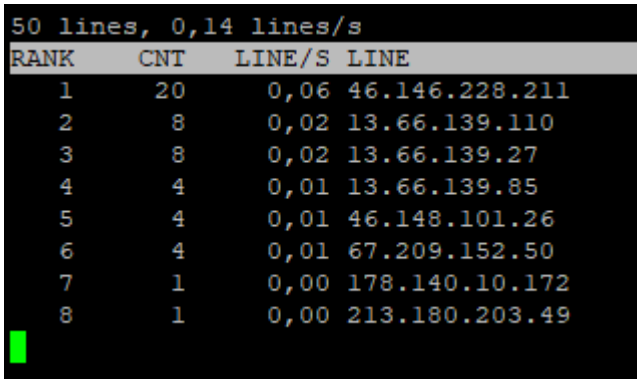
Пример 3.

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:



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.

Таком 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 «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».