



Сумасшедший Линуксоид

2,3К подписчиков

Вы подписаны

Файлы utmp, wtmp, btmp. Что это такое и с чем его едят.

576 прочтений · 12 февраля



Технолог...

363,6К...

Следить за темой

Дзен

Найти тему

🏠

🔍

📌

📺

💬

📁

📖

🔖

🎮

🐾

Каждый раз, когда вы заходите и выходите в систему и даже, когда просто пытаетесь войти – все эти действия записываются. Существуют специальные команды, с помощью которых можно узнать все такие действия в системе.

В этой статье рассмотрим то, как просмотреть файлы, в которые ведется запись.

/var/run/utmp.

utmp отвечает за отслеживание пользователей, вошедших в вашу систему, и когда вы запускаете команду who в своем терминале, он получает информацию для входа в систему из /var/run/utmp, а затем отображает ее на вашем экране.

И он сохраняет информацию о вашем текущем входе в систему, времени загрузки системы, какой терминал или псевдотерминал используется для входа в систему, выхода из системы и т.д.

avito.ru

реклама

Альфа Банк

Кэшбэк 30% с Авито Доставкой

30%

Реклама. Срок акции – с 01.08.2024 по 31.08.2024. Условия: 30% кэшбэк на покупки товаров и услуг в Авито Доставку. Максимальная сумма кэшбэка – 1000 руб. Число покупок не ограничено. Акция действует в рамках программы «Авито Доставка». Подробности на avito.ru. © 2024 Авито. Все права защищены.

19

1

https://dzen.ru/a/ZcmtBdQGrygQd1F7

1/4



```
Terminal
vagrant@debian-host1:~$ who
user      pts/0      2024-02-09 14:47 (10.0.2.2)
vagrant   pts/1      2024-02-09 18:54 (10.0.2.2)
```

/var/log/wtmp

Бинарный файл `/var/log/wtmp` отвечает за запись всех вошедших в систему и вышедших из системы пользователей, и даже можно сказать, что он сохраняет все действия `/var/run/utmp` в `/var/log/wtmp`.

Но как долго данные журнала будут храниться в `/var/log/wtmp`? Все зависит от конфигурации в `/etc/logrotate.conf`. По умолчанию, обычно, все журналы обновляются через четыре недели.

Команда `last` использует файл `/var/log/wtmp` для отображения всех данных предыдущего входа и выхода из системы.

```
Terminal
vagrant@debian-host1:~$ last
vagrant pts/1      10.0.2.2      Fri Feb 9 18:54  still logged in
user    pts/0      10.0.2.2      Fri Feb 9 14:47  still logged in
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
vagrant pts/0      10.0.2.2      Fri Feb 9 14:46 - 14:46 (00:00)
reboot  system boot  6.1.0-15-amd64 Fri Feb 9 14:46  still running

wtmp begins Fri Feb 9 14:46:02 2024
```

/var/log/btmp.

Файл `/var/log/btmp` аналогичен приведенному выше файлу, но в нем хранятся только неудачные попытки входа в систему. И вы не можете получить доступ к команде `lastb` без привилегий `sudo`.

```
Terminal
root@debian-host1:~# lastb
user    ssh:notty  192.168.56.1  Fri Feb 9 20:05 - 20:05 (00:00)
user    ssh:notty  192.168.56.1  Fri Feb 9 20:05 - 20:05 (00:00)
user    ssh:notty  192.168.56.1  Fri Feb 9 20:05 - 20:05 (00:00)
user    ssh:notty  192.168.56.1  Fri Feb 9 20:05 - 20:05 (00:00)
support ssh:notty  192.168.56.1  Fri Feb 9 20:05 - 20:05 (00:00)
support ssh:notty  192.168.56.1  Fri Feb 9 20:04 - 20:04 (00:00)
support ssh:notty  192.168.56.1  Fri Feb 9 20:04 - 20:04 (00:00)

btmp begins Fri Feb 9 20:04:52 2024
```

Как читать utmp, wtmp и btmp в необработанном формате.

Все эти файлы в `/var/run/utmp`, `/var/log/wtmp` и `/var/log/btmp` являются двоичными файлами. Вы не можете прочитать этот файл с помощью любого текстового редактора, или например с помощью `more`, `less`, `cat` и т. д.

И если запустить команду `file`, чтобы узнать тип данных, то мы получим информацию, что это файл данных.

```
Terminal
root@debian-host1:~# file /var/run/utmp /var/log/wtmp /var/log/btmp
/var/run/utmp: data
/var/log/wtmp: data
/var/log/btmp: data
```



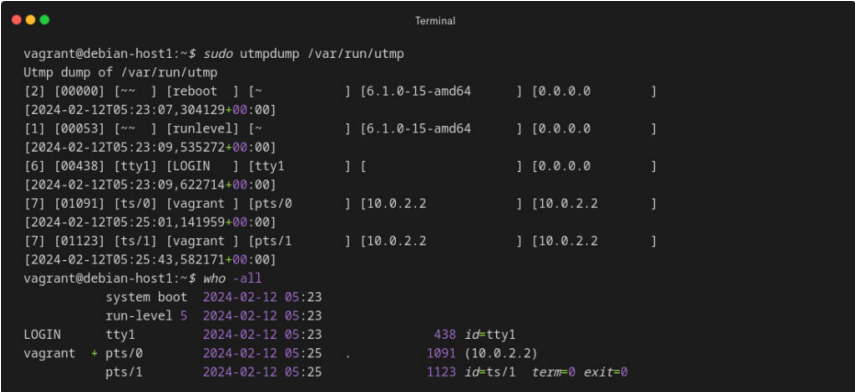
Чтобы узнать, что хранит этот файл, вы можете использовать команду `utmpdump`, которая прочитает этот файл в необработанном формате. В большинстве систем Linux эта утилита уже установлена.

Вы можете запустить любую из следующих команд, чтобы прочитать файл в необработанном формате.

```
utmpdump /var/run/utmp utmpdump /var/log/wtmp utmpdump /var/log/btmp
```

А чтобы лучше понять необработанный формат, я предлагаю вам запустить соответствующую команду вместе с приведенной выше командой, например `who`, `last` или `lastb`.

```
$ sudo utmpdump /var/run/utmp $ who -all
```



Заключение.

Вот и всё по `utmp`, `wtmp`, `btmp` и как это читать. Я думаю, теперь вы узнали, какой двоичный файл отвечает за конкретные цели ведения журнала.

Реклама • 16+

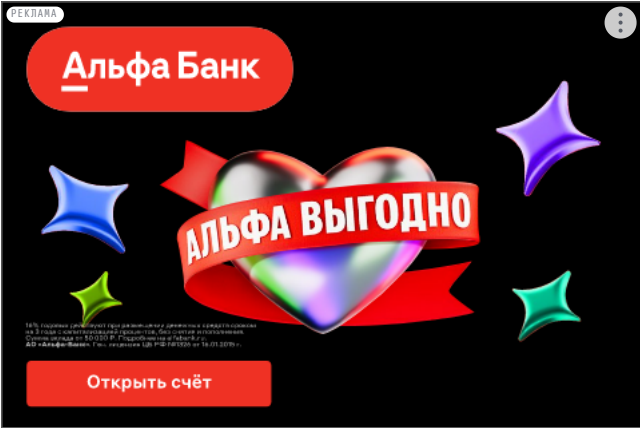
Курсы ЕГЭ по алгебре в Фоксфорде 11 класс

Поможем сдать ЕГЭ на нужный балл. Все предметы. Преподаватели МГУ, МФТИ, НИУ ВШЭ!

[Курсы ЕГЭ-2025](#)
[Репетиторы ЕГЭ](#)

foxford.ru

[Перейти на сайт](#)



Комментарии 1

Написать комментарий

Alex R. 3 м

Чет у меня нет таких файлов, может потому что пользователь один?

Ответить

Рекомендуем почитать



Plectrom

2,3К прочтений · 2 года назад

Linux и SSD

Если вас мучает вопрос - какую файловую систему работающую на Linux выбрать для твердотельного накопителя? То знаете, ч...

1 минута

Habr.com

2,4К прочтений · 3 недели назад

Главная причина, почему всё-таки Linux

Недавно на Хабре была опубликована статья Главная причина, почему не Linux, которая наделала много шума В...

6 минут

Реклама · 16+

Готовься к ЕГЭ/ОГЭ всего от 5550₽ за 4 предмета

Сотка: все, что нужно для подготовки, на одной платформе. Мы умеем учить интересно!

от 5 550 ₽

sotkaonline.ru

Перейти на сайт

Взгляните на эти темы

Технологии

Интернет вещей (IoT)

Технологии в социа

Портативные зарядные устройства (Power Bank)

Технологии в свя

https://dzen.ru/a/ZcmtBdQGrygQd1F7

4/4