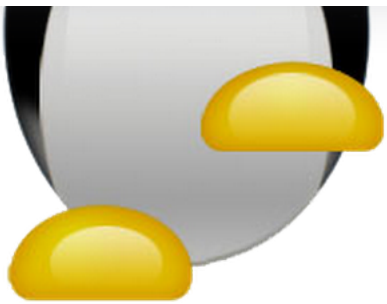
Сумасшедший Линуксоид
2,3К подписчиков

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



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.

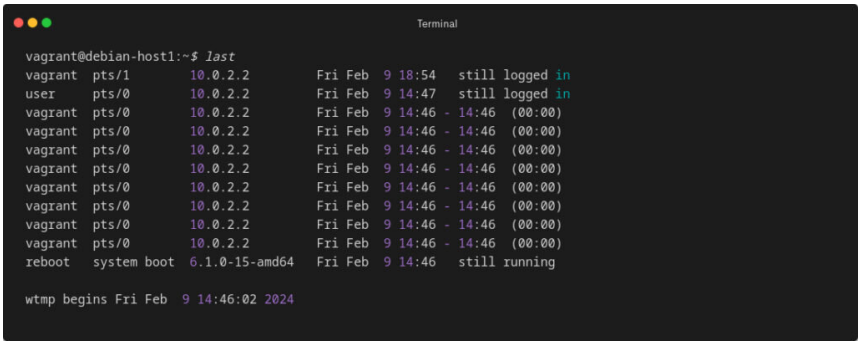
И он сохраняет информацию о вашем текущем входе в систему, времени загрузки системы, какой терминал или псевдотерминал используется для входа в систему, выхода из системы и т.д.

/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.



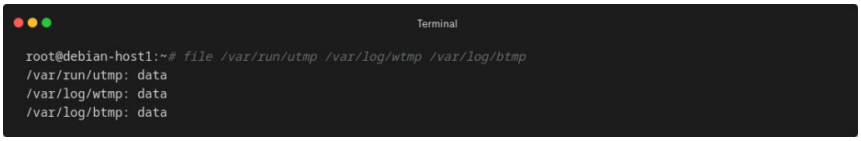
/var/log/btmp.

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.

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.



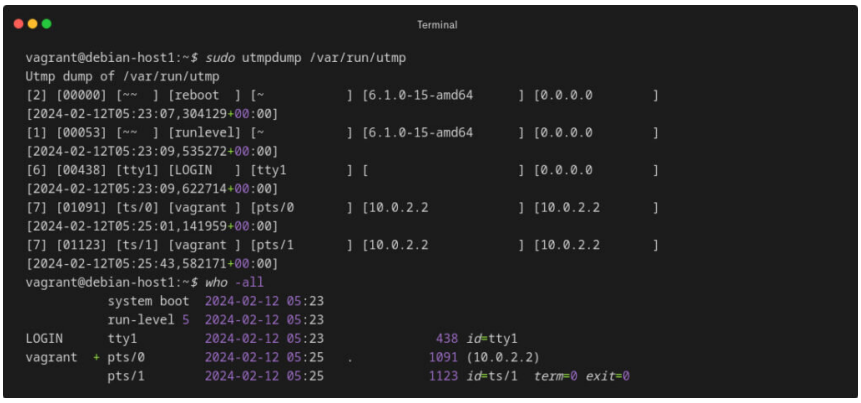
Чтобы узнать, что хранит этот файл, вы можете использовать команду utmpdump, которая прочитает этот файл в необработанном формате. В большинстве систем Linux эта утилита уже установлена.

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.

Комментарии 1

Написать комментарий

Alex R. 3 м

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

Ответить

Рекомендуем почитать

3 дня назад

Plectrom
2,3K прочтений · 2 года назад

Linux и SSD

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

1 минута

Habr.com
2,4K 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

Взгляните на эти темы


Технологии

Интернет вещей (IoT)


Технологии в социа


Портативные зарядные устройства (Power Bank)


Технологии в свя