Утилиты для просмотра входов в систему lastlog, btmp, utmp, wtmp

lastlog

lastlog выводит информацию (имя пользователя, порт и дату последнего входа) о входах в систему, содержащуюся в файле /var/log/lastlog. По умолчанию строки выводятся в том же порядке, в котором они указаны в /etc/passwd

btmp

Этот файл содержит логи неудачных попыток входа в систему.

Для корректного обновления этого файла у вас должен быть настроен файл конфигурации logrotate.conf примерно таким образом:

```
/var/log/btmp {
monthly
minsize 1M
create 0600 root utmp
rotate 1
}
```

Для просмотра файла используем команду:

```
# last -f /var/log/btmp
```

Вы можете изменить количество создаваемых лог файлов в параметре rotate.
Обычно мы можем наблюдать в этом файле попытки подбора имени и пароля для входа в систему.
Для очистки лога используем команду:

```
# cat /dev/null > /var/log/btmp
```

/var/run/utmp

Этот файл содержит информацию о пользователях, которые в настоящее время вошли в систему.
Команда «who» использует этот файл для отображения зарегистрированных пользователей.

wtmp

Файл wtmp записывает все логины и логауты. Его формат точно так же, как и utmp, за исключением того, что нулевое имя пользователя указывает на выход из соответствующего терминала.

Кроме того, имя терминала ~ с отключением или перезагрузкой имени пользователя указывает на выключение или перезагрузку системы, а пара имен терминалов | /} регистрирует старое / новое системное время, когда дата (1) меняет его. wtmp поддерживается логином (1), init (8) и некоторыми версиями getty (8) (например, mingetty (8) или agetty (8)).

```
# last -f /var/log/wtmp | less
# utmpdump /var/log/wtmp | less
```