Termlog - логгирование событий, происходящих на виртуальных терминалах

Опубликовано muff в Пнд, 2012-02-20 03:38

Довольно полезно знать, чем занимаются пользователи в ssh-сеансах. Инструментом в этом случае будет выступать утилита **termlog**, которая наблюдает за тем, что пользователь набирает в ssh-сессии и пишет в лог-файлы.

Установку, как всегда, выполним из системы портов:

```
# cd /usr/ports/security/termlog && make install clean && rehash
```

Установка занимает считанные секунды... По завершению установки рекомендую ознакомиться с man-страницей.

Для запуска **termlog**, необходимо добавить соответствующую запись в **rc.conf**:

```
# echo '# SSH-log deamon' >> /etc/rc.conf
# echo 'termlog_enable="YES"' >> /etc/rc.conf
```

Собственно, запуск утилиты:

```
# sh /usr/local/etc/rc.d/termlog start


Starting termlog.
2012-02-20 00:19:30.634639 session muff_ttyp3_1329697170.log created
2012-02-20 00:19:30.635226 session parazitx_ttyp6_1329697170.log created
2012-02-20 00:19:30.635492 session rs_ttyp7_1329697170.log created
2012-02-20 00:19:30.635825 session rs_ttyp8_1329697170.log created
```

Сразу же создались логи для текущих подключенных пользователей: **muff**, **parazitx** и **rs**. Проверим, кто действительно подключен на данный момент к серверу:

```
# who


muff             ttyp3     4 ??? 02:19 (10.227.206.114)parazitx         ttyp6    18
??? 19:13 (10.3.158.10)rs               ttyp7    19 ??? 19:15 (10.3.159.155)rs
         ttyp8    19 ??? 19:28 (10.3.159.155)
```

Все совпадает - и количество подключенных пользователей, и номера виртуальных терминалов, открытых пользователями.

По умолчанию **termlog** пишет логи в каталог **/var/log/termlog**.

Из замеченных недостатков - если пользователь запустил **mc** - то в логи пишется полнейший бред.

Источник (получено *2026-11-07 13:00*):

http://muff.kiev.ua/content/termlog-loggirovanie-sobytii-proiskhodyashchikh-na-virtualnykh-terminalakh