Отчёт по лабораторной работе 15

Настройка сетевого журналирования

Цвелев С.А. НПИбд-02-22

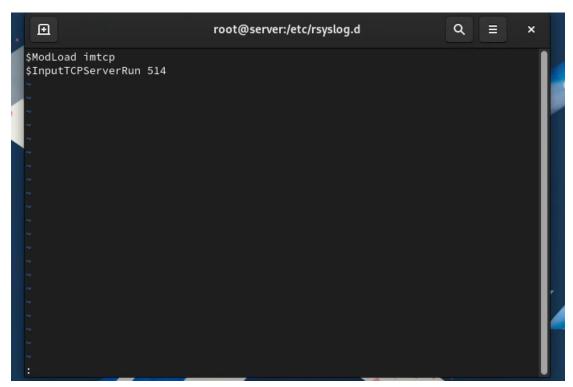
Содержание

1 Цель работы

Получить навыки по работе с журналами системных событий.

2 Ход работы

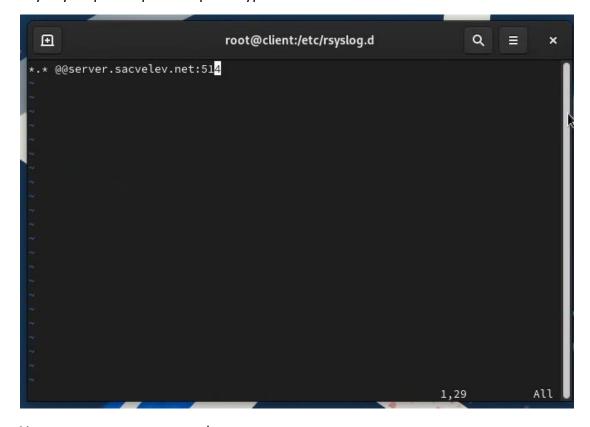
Запускаем машину server. Создаем netlog-server.conf и в нем включаем приём записей журнала по TCP-порту 514.



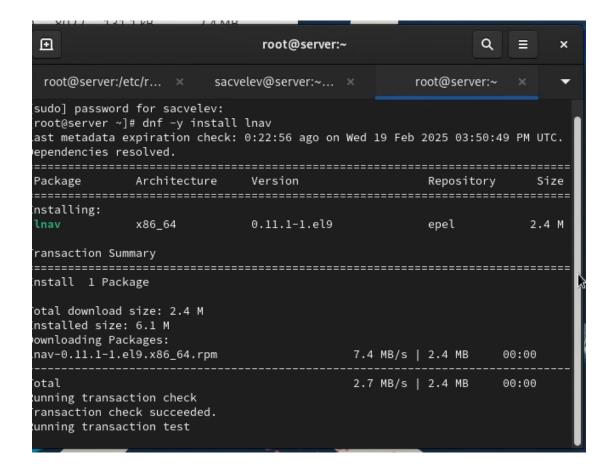
Перезапускаем службу. Просматриваем, какие порты связаны с rsyslog. Настраиваем межсетевой экран на прием сообщений по порту 514.

```
❶
                             root@server:/etc/rsyslog.d
                                                                   Q
                                                                              ×
               10427 [eventpoll:4,5]
rsyslogd 11256 11263 in:im
                                                          REG
                                          root
                                                  8w
                                                                             8,1
   314926
            25191885 /var/log/messages
rsyslogd 11256 11263 in:im
                                          root
                                                     a_inode
                                                                            0,14
               10427 inotify
rsyslogd 11256 11263 in:im
                                                          REG
                                          root
                                                11r
                                                                            0,23
  2015232
                1502 /run/log/journal/3a820b12e4ab476faf24d5a9fc5aa99c/system.j
ournal
rsyslogd 11256 11263 in:imt
                                          root
                                                12r
                                                          REG
                                                                            0,23
  2015232
                1284 /run/log/journal/3a820b12e4ab476faf24d5a9fc5aa99c/system@e
e462aeaa2e4427faa74f5c3af57919b-000000000000775-00062e8095340bb4.journal
rsyslogd 11256 11263 in:im
                                          root
                                                13r
                                                                            0,23
                 951 /run/log/journal/3a820b12e4ab476faf24d5a9fc5aa99c/system@e
   2015232
e462aeaa2e4427faa74f5c3af57919b-0000000000003ac-00062e8091d95b4b.journal
rsyslogd 11256 11263 in:im
                                                                            0,23
                                         root
                                                14r
                                                         REG
                  60 /run/log/journal/3a820b12e4ab476faf24d5a9fc5aa99c/system@e
e462aeaa2e4427faa74f5c3af57919b-000000000000001-00062e8091433243.journal
rsyslogd 11256 11264 rs:main
                                         root mem
                                                                             8,1
    34864
            25722806 /usr/lib64/rsyslog/lmnsd_ptcp.so
rsyslogd 11256 11264 rs:main
                                         root mem
                                                          REG
                                                                             8,1
    48296
            25722809 /usr/lib64/rsyslog/lmt
                                         root mem
rsyslogd 11256 11264 rs:main
                                                          REG
                                                                             8,1
    34464 25722801 /usr/lib64/rsyslog/im
[root@server rsyslog.d]# lsof | grep to
```

На клиенте создаем файл конфигурации сетевого хранения журналов. Включаем перенаправление сообщений на порт 514 сервера. Перезапускаем службу и просматриваем файл журнала.



Устанавливаем на сервере lnav и просматриваем с него логи.



3 Вывод

Мы приобрели навыки по работе с журналами системных событий.