Лабораторная работа №15 Настройка сетевого журналирования

Жаворонков Кирилл Александрович

1132231844

НПИбд-01-23

Настройка сервера сетевого журнала

Рис. 1.1. Создание на сервере файла конфигурации сетевого хранения журналов.

Настройка сервера сетевого журнала

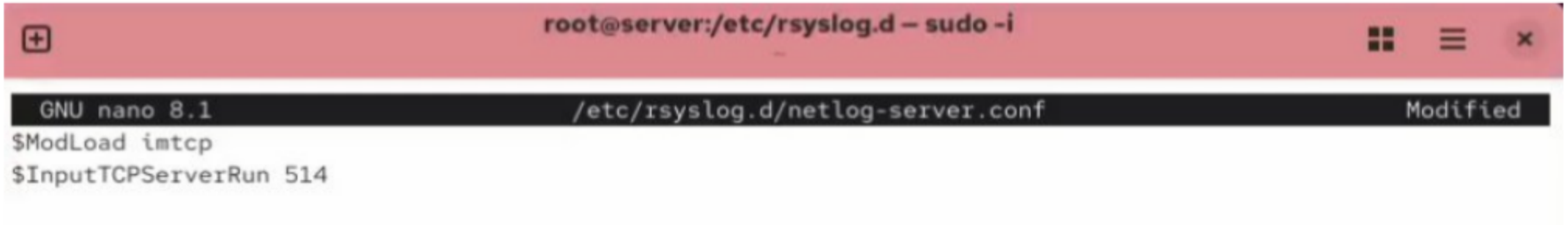

Рис. 1.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514.

Настройка сервера сетевого журнала

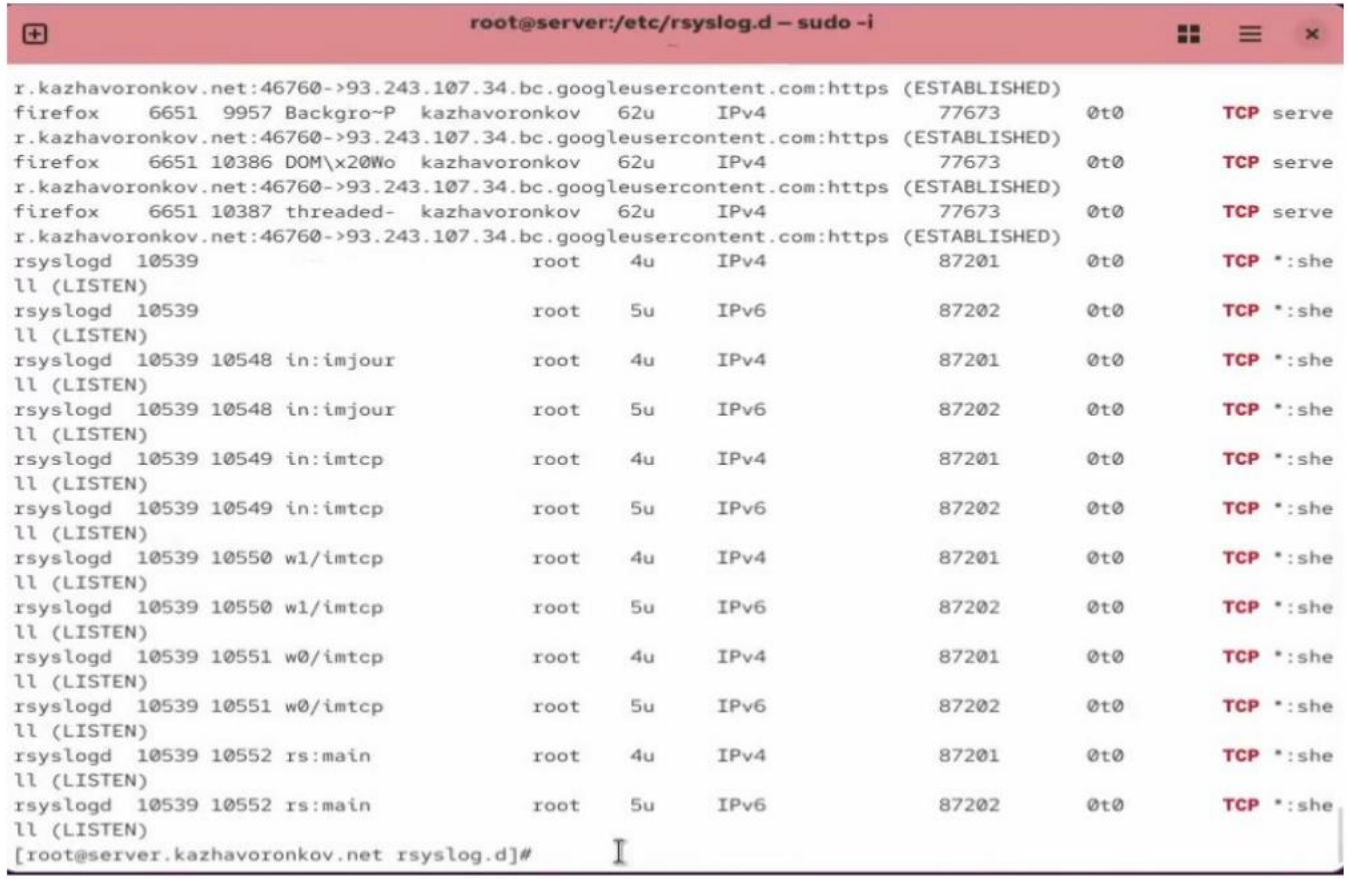

Рис. 1.3. Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

Настройка сервера сетевого журнала

```
[root@server.kazhavoronkov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.kazhavoronkov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.kazhavoronkov.net rsyslog.d]#
```

Рис. 1.4. Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

Настройка клиента сетевого журнала

Рис. 2.1. Создание на клиенте файла конфигурации сетевого хранения журналов.

Настройка клиента сетевого журнала

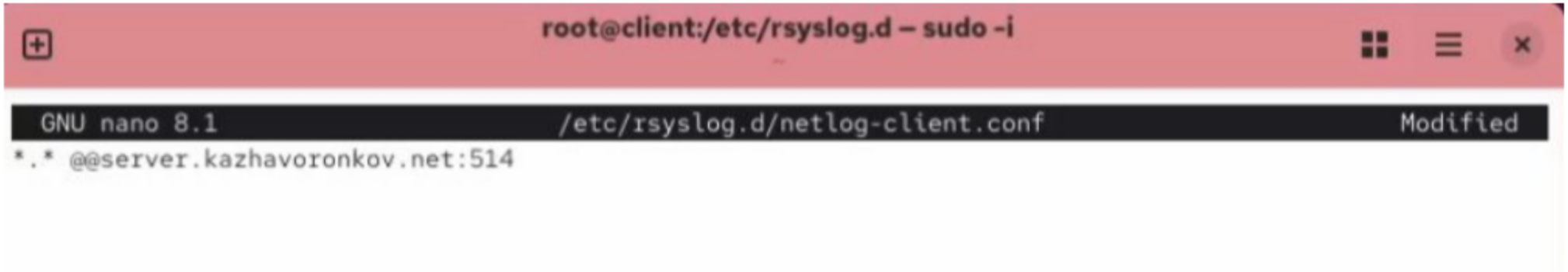

Рис. 2.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Настройка клиента сетевого журнала

```
[root@client.kazhavoronkov.net rsyslog.d]# systemctl restart rsyslog
[root@client.kazhavoronkov.net rsyslog.d]#
```

Рис. 2.3. Перезапуск службы rsyslog.

Просмотр журнала

Рис. 3.1. Просмотр на сервере одного из файлов журнала.

Просмотр журнала

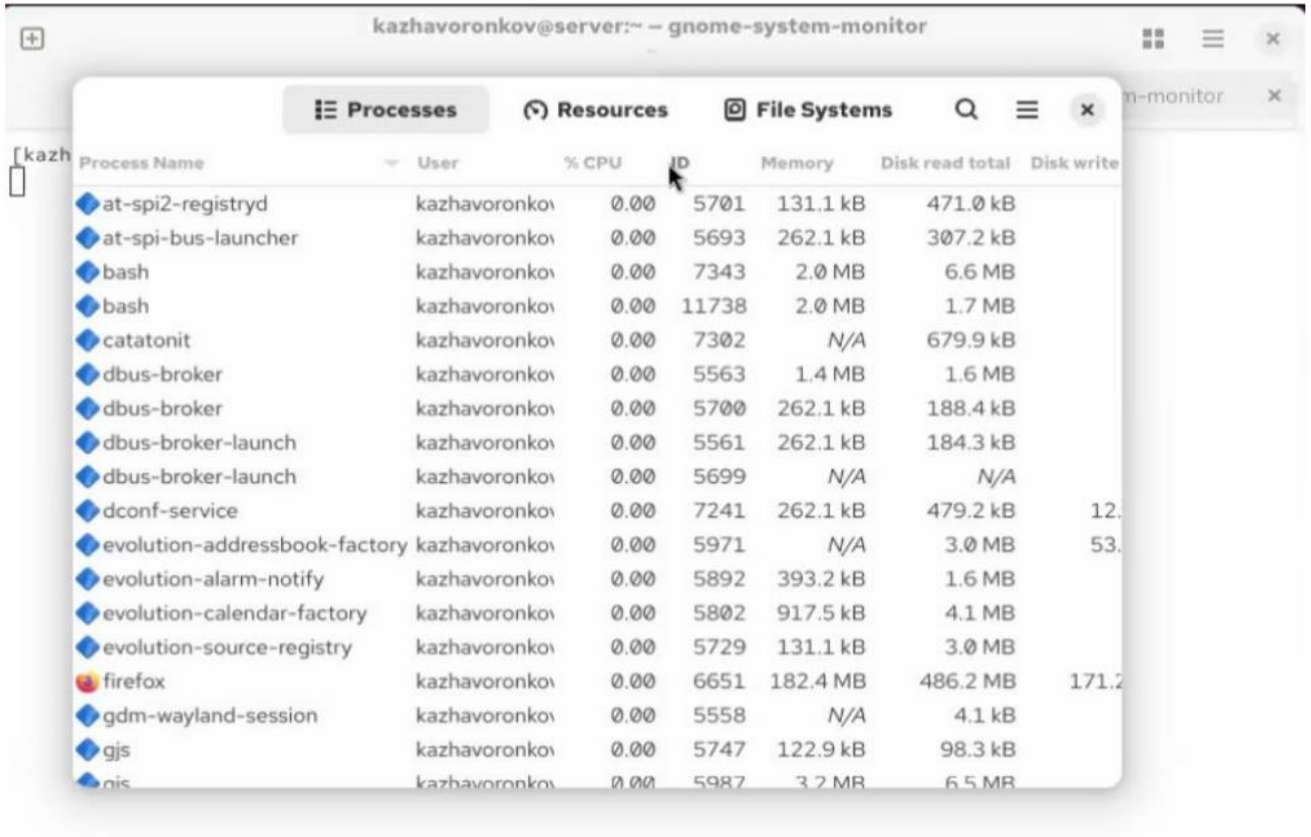

Рис. 3.2. Запуск на сервере под пользователем kazhavoronkov графической программы для просмотра журналов.

Просмотр журнала

```
[root@server.kazhavoronkov.net ~]# dnf -y install multitail
Last metadata expiration check: 0:04:0[illegible] ago on Sat 13 Dec 2025 10:37:10 AM UTC.
Dependencies resolved.
================================================================================
 Package                Architecture          Version                  Repository           Size
================================================================================
Installing:
 multitail              x86_64                7.1.3-2.el10_0           epel                148 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 148 k
Installed size: 326 k
Downloading Packages:
multitail-7.1.3-2.el10_0.x86_64.rpm                 185 kB/s | 148 kB     00:00
--------------------------------------------------------------------------------
Total                                                51 kB/s | 148 kB     00:02
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : multitail-7.1.3-2.el10_0.x86_64                        1/1
  Running scriptlet: multitail-7.1.3-2.el10_0.x86_64                        1/1
```

Просмотр журнала

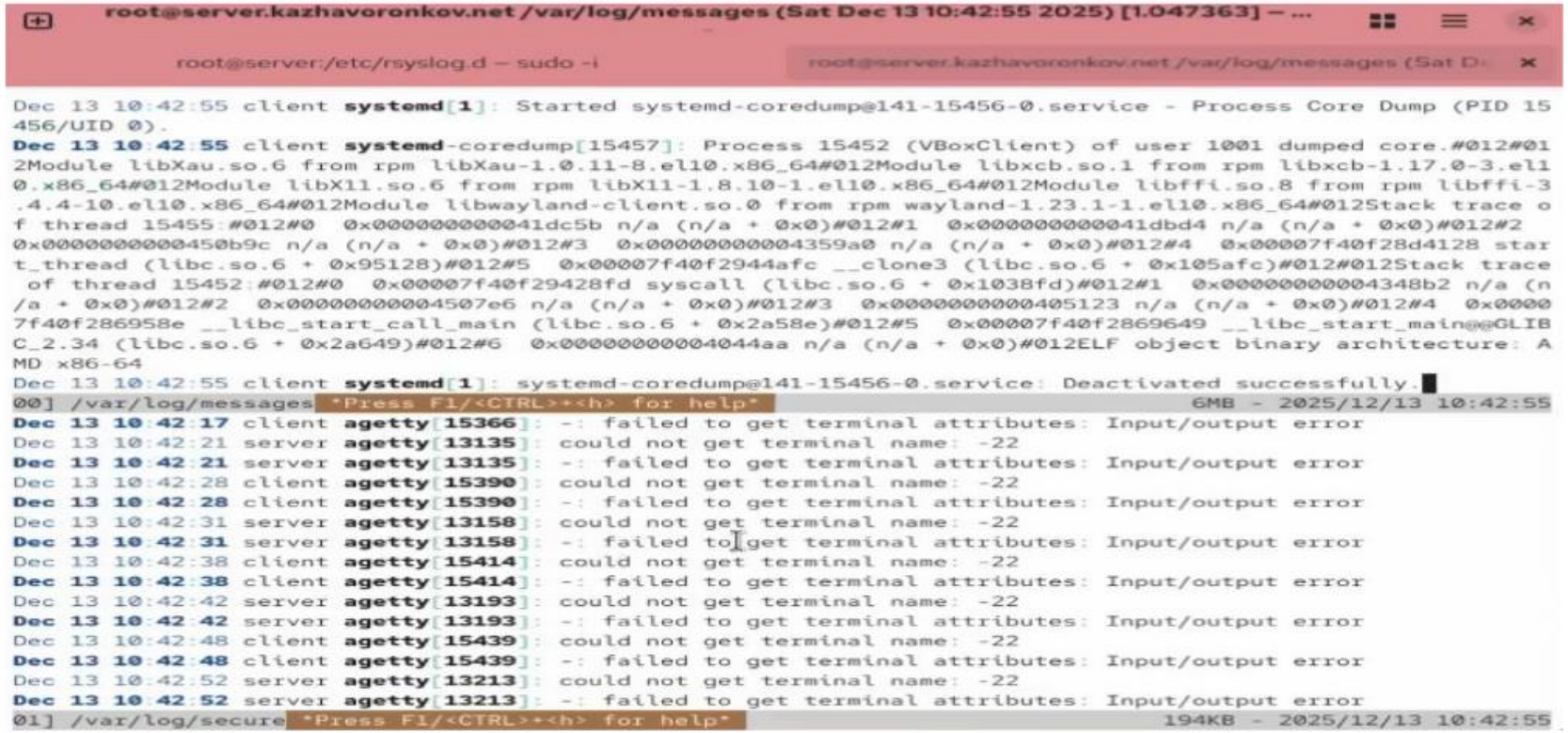

Рис. 3.4. Просмотр логов с помощью Multitail.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[root@server.kazhavoronkov.net ~]# cd /vagrant/provision/server
[root@server.kazhavoronkov.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.kazhavoronkov.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/n
etlog/etc/rsyslog.d
[root@server.kazhavoronkov.net server]# touch netlog.sh
[root@server.kazhavoronkov.net server]# chmod +x netlog.sh
[root@server.kazhavoronkov.net server]#
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[root@client.kazhavoronkov.net rsyslog.d]# cd /vagrant/provision/client
[root@client.kazhavoronkov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.kazhavoronkov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf
cp: missing destination file operand after '/etc/rsyslog.d/netlog-client.conf'
Try 'cp --help' for more information.
[root@client.kazhavoronkov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/clien
t/netlog/etc/rsyslog.d/
[root@client.kazhavoronkov.net client]# touch netlog.sh
[root@client.kazhavoronkov.net client]# chmod +x netlog.sh
[root@client.kazhavoronkov.net client]#
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
server.vm.provision "server netlog",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/netlog.sh"
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
client.vm.provision "client netlog",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/netlog.sh"
```