

# Лабораторная работа №15

## Настройка сетевого журналирования

Жаворонков Кирилл Александрович

1132231844

НПИбд-01-23

# Настройка сервера сетевого журнала

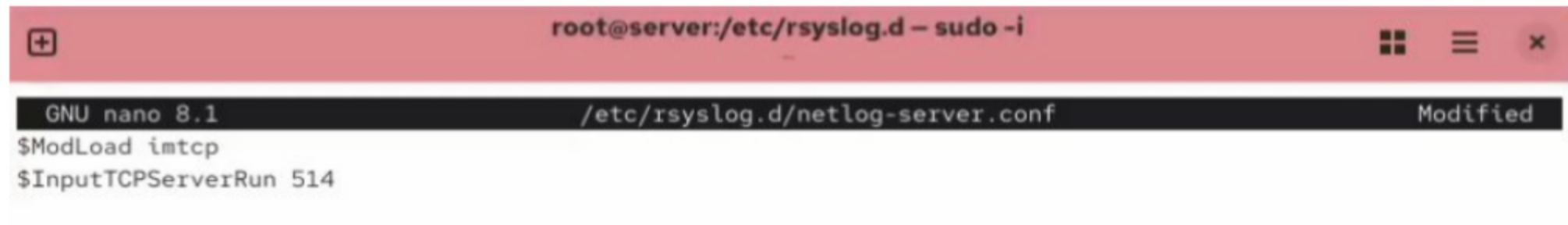


```
root@server:/etc/rsyslog.d – sudo -i

[kazhavoronkov@server.kazhavoronkov.net ~]$ sudo -i
[sudo] password for kazhavoronkov:
[root@server.kazhavoronkov.net ~]# cd /etc/rsyslog.d
[root@server.kazhavoronkov.net rsyslog.d]# touch netlog-server.conf
[root@server.kazhavoronkov.net rsyslog.d]#
```

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

# Настройка сервера сетевого журнала



The image shows a terminal window with a red title bar. The title bar text is "root@server:/etc/rsyslog.d – sudo -i". On the right side of the title bar are three icons: a window icon, a hamburger menu icon, and a close icon. The main content area of the terminal shows the GNU nano 8.1 editor editing the file /etc/rsyslog.d/netlog-server.conf. The status bar at the bottom of the editor indicates "Modified". The content of the file is as follows:

```
GNU nano 8.1 /etc/rsyslog.d/netlog-server.conf Modified
$ModLoad imtcp
$InputTCPServerRun 514
```

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

# Настройка сервера сетевого журнала

```
root@server:/etc/rsyslog.d - sudo -i

r.kazhavoronkov.net:46760->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox 6651 9957 Backgro~P kazhavoronkov 62u IPv4 77673 0t0 TCP serve
r.kazhavoronkov.net:46760->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox 6651 10386 DOM\x20Wo kazhavoronkov 62u IPv4 77673 0t0 TCP serve
r.kazhavoronkov.net:46760->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox 6651 10387 threaded- kazhavoronkov 62u IPv4 77673 0t0 TCP serve
r.kazhavoronkov.net:46760->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
rsyslogd 10539 root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10548 in:imjour root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10548 in:imjour root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10549 in:imtcp root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10549 in:imtcp root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10550 w1/imtcp root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10550 w1/imtcp root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10551 w0/imtcp root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10551 w0/imtcp root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10552 rs:main root 4u IPv4 87201 0t0 TCP *:she
ll (LISTEN)
rsyslogd 10539 10552 rs:main root 5u IPv6 87202 0t0 TCP *:she
ll (LISTEN)
[root@server.kazhavoronkov.net rsyslog.d]#
```

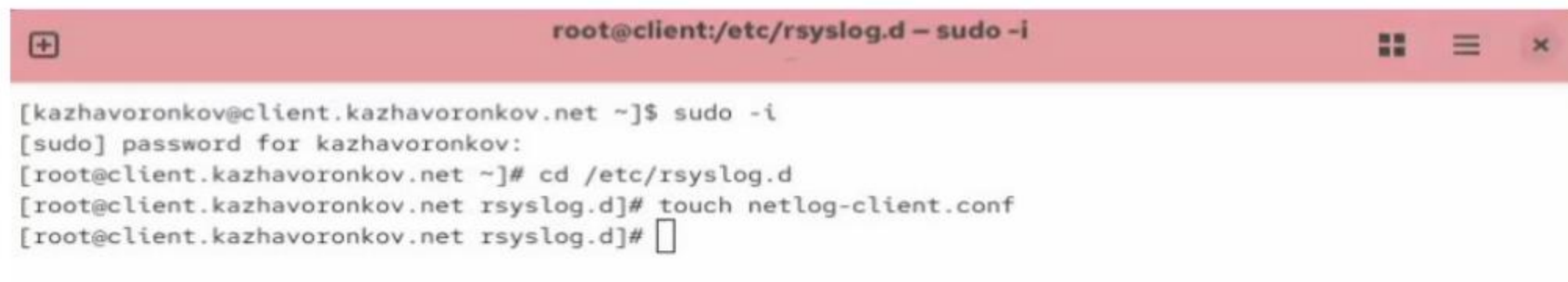
**Рис. 1.3.** Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

# 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

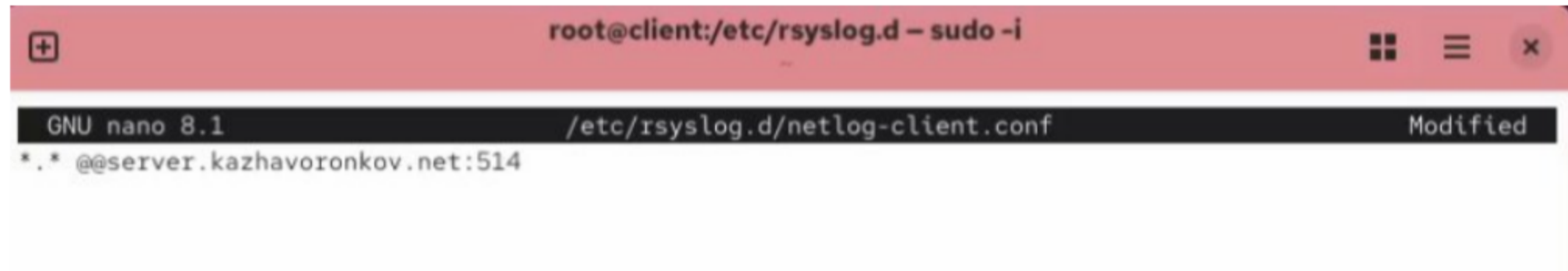


```
root@client:/etc/rsyslog.d - sudo -i

[kazhavoronkov@client.kazhavoronkov.net ~]$ sudo -i
[sudo] password for kazhavoronkov:
[root@client.kazhavoronkov.net ~]# cd /etc/rsyslog.d
[root@client.kazhavoronkov.net rsyslog.d]# touch netlog-client.conf
[root@client.kazhavoronkov.net rsyslog.d]#
```

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

# Настройка клиента сетевого журнала



The screenshot shows a terminal window with a red title bar. The title bar text is 'root@client:/etc/rsyslog.d - sudo -i'. On the right side of the title bar are three icons: a window icon, a hamburger menu icon, and a close icon. Below the title bar is a black bar with white text: 'GNU nano 8.1' on the left, '/etc/rsyslog.d/netlog-client.conf' in the center, and 'Modified' on the right. The main area of the terminal is white and contains the text '.\* @@server.kazhavoronkov.net:514'.

```
root@client:/etc/rsyslog.d - sudo -i
GNU nano 8.1 /etc/rsyslog.d/netlog-client.conf Modified
.* @@server.kazhavoronkov.net:514
```

**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

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

**Рис. 2.3.** Перезапуск службы rsyslog.



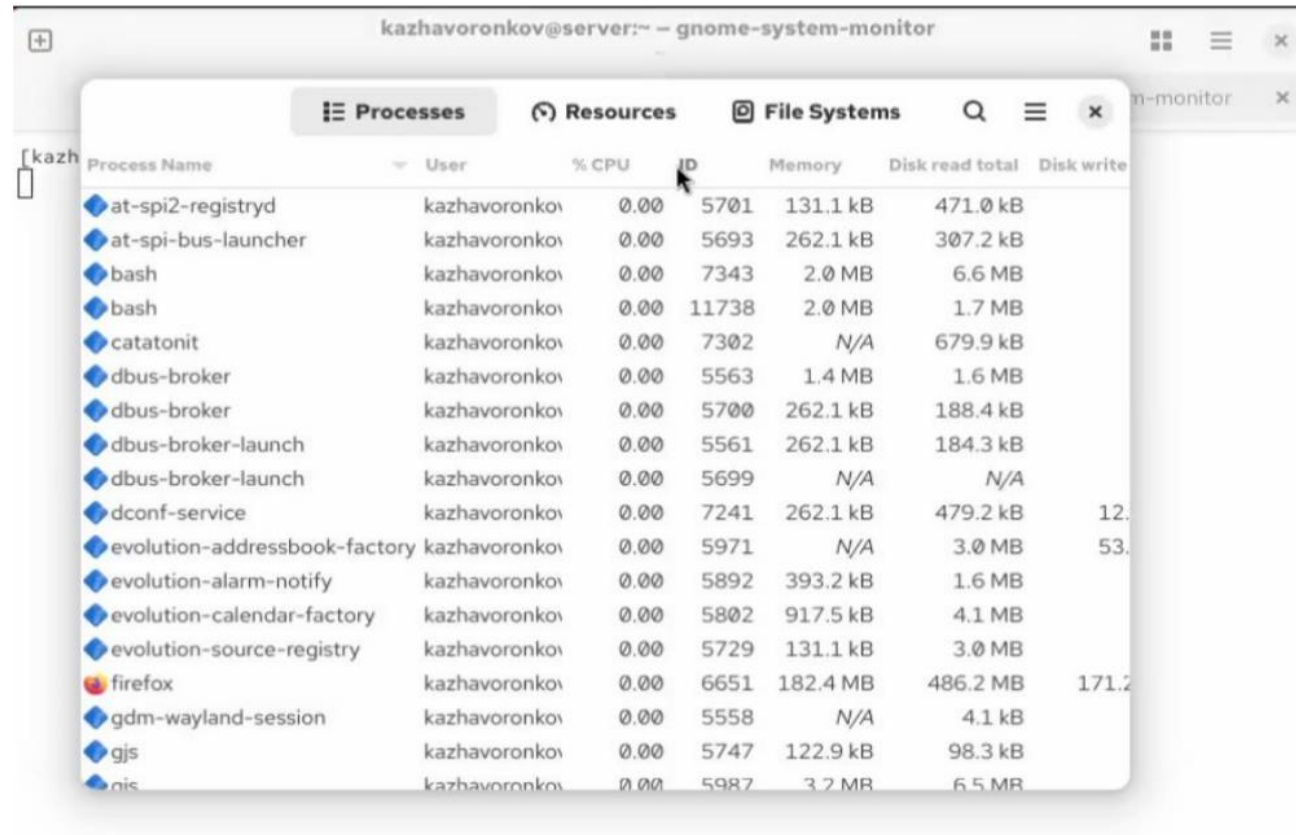
# Просмотр журнала



```
root@server:/etc/rsyslog.d - sudo -i
0x0000000000450b9c n/a (n/a + 0x0)#012#3 0x00000000004359a0 n/a (n/a + 0x0)#012#4 0x00007f575d766128 star
t_thread (libc.so.6 + 0x95128)#012#5 0x00007f575d7d6afc __clone3 (libc.so.6 + 0x105afc)#012#012Stack trace
of thread 11727:#012#0 0x00007f575d7d48fd syscall (libc.so.6 + 0x1038fd)#012#1 0x00000000004348b2 n/a (n
/a + 0x0)#012#2 0x00000000004507e6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x0000
7f575d6fb58e __libc_start_call_main (libc.so.6 + 0x2a58e)#012#5 0x00007f575d6fb649 __libc_start_main@@GLIB
C_2.34 (libc.so.6 + 0x2a649)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: A
MD x86-64
Dec 13 10:35:14 server systemd[1]: systemd-coredump@377-11731-0.service: Deactivated successfully.
Dec 13 10:35:16 client kernel: traps: VBoxClient[14273] trap int3 ip:41dc5b sp:7f40e41b4cd0 error:0 in VBox
Client[1dc5b.400000+bb000]
Dec 13 10:35:16 client systemd-coredump[14274]: Process 14270 (VBoxClient) of user 1001 terminated abnormal
ly with signal 5/TRAP, processing...
Dec 13 10:35:16 client systemd[1]: Started systemd-coredump@52-14274-0.service - Process Core Dump (PID 142
74/UID 0).
Dec 13 10:35:16 client systemd-coredump[14275]: Process 14270 (VBoxClient) of user 1001 dumped core.#012#01
2Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el1
0.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3
.4.4-10.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x86_64#012Stack trace o
f thread 14273:#012#0 0x000000000041dc5b n/a (n/a + 0x0)#012#1 0x000000000041dbd4 n/a (n/a + 0x0)#012#2
0x0000000000450b9c n/a (n/a + 0x0)#012#3 0x00000000004359a0 n/a (n/a + 0x0)#012#4 0x00007f40f28d4128 star
t_thread (libc.so.6 + 0x95128)#012#5 0x00007f40f2944afc __clone3 (libc.so.6 + 0x105afc)#012#012Stack trace
of thread 14270:#012#0 0x00007f40f29428fd syscall (libc.so.6 + 0x1038fd)#012#1 0x00000000004348b2 n/a (n
/a + 0x0)#012#2 0x00000000004507e6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x0000
7f40f286958e __libc_start_call_main (libc.so.6 + 0x2a58e)#012#5 0x00007f40f2869649 __libc_start_main@@GLIB
C_2.34 (libc.so.6 + 0x2a649)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: A
MD x86-64
Dec 13 10:35:16 client systemd[1]: systemd-coredump@52-14274-0.service: Deactivated successfully.
Dec 13 10:35:16 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 10:35:16 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at
 27.
Dec 13 10:35:16 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

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

# Просмотр журнала



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registr...	kazhavoronko...	0.00	5701	131.1 kB	471.0 kB	
at-spi-bus-lau...	kazhavoronko...	0.00	5693	262.1 kB	307.2 kB	
bash	kazhavoronko...	0.00	7343	2.0 MB	6.6 MB	
bash	kazhavoronko...	0.00	11738	2.0 MB	1.7 MB	
catatonit	kazhavoronko...	0.00	7302	N/A	679.9 kB	
dbus-broker	kazhavoronko...	0.00	5563	1.4 MB	1.6 MB	
dbus-broker	kazhavoronko...	0.00	5700	262.1 kB	188.4 kB	
dbus-broker-l...	kazhavoronko...	0.00	5561	262.1 kB	184.3 kB	
dbus-broker-l...	kazhavoronko...	0.00	5699	N/A	N/A	
dconf-service	kazhavoronko...	0.00	7241	262.1 kB	479.2 kB	12.0 kB
evolution-add...	kazhavoronko...	0.00	5971	N/A	3.0 MB	53.0 MB
evolution-alm...	kazhavoronko...	0.00	5892	393.2 kB	1.6 MB	
evolution-cal...	kazhavoronko...	0.00	5802	917.5 kB	4.1 MB	
evolution-sou...	kazhavoronko...	0.00	5729	131.1 kB	3.0 MB	
firefox	kazhavoronko...	0.00	6651	182.4 MB	486.2 MB	171.2 MB
gdm-wayland-s...	kazhavoronko...	0.00	5558	N/A	4.1 kB	
gjs	kazhavoronko...	0.00	5747	122.9 kB	98.3 kB	
gnome-sys-mo...	kazhavoronko...	0.00	5987	3.2 MB	6.5 MB	

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

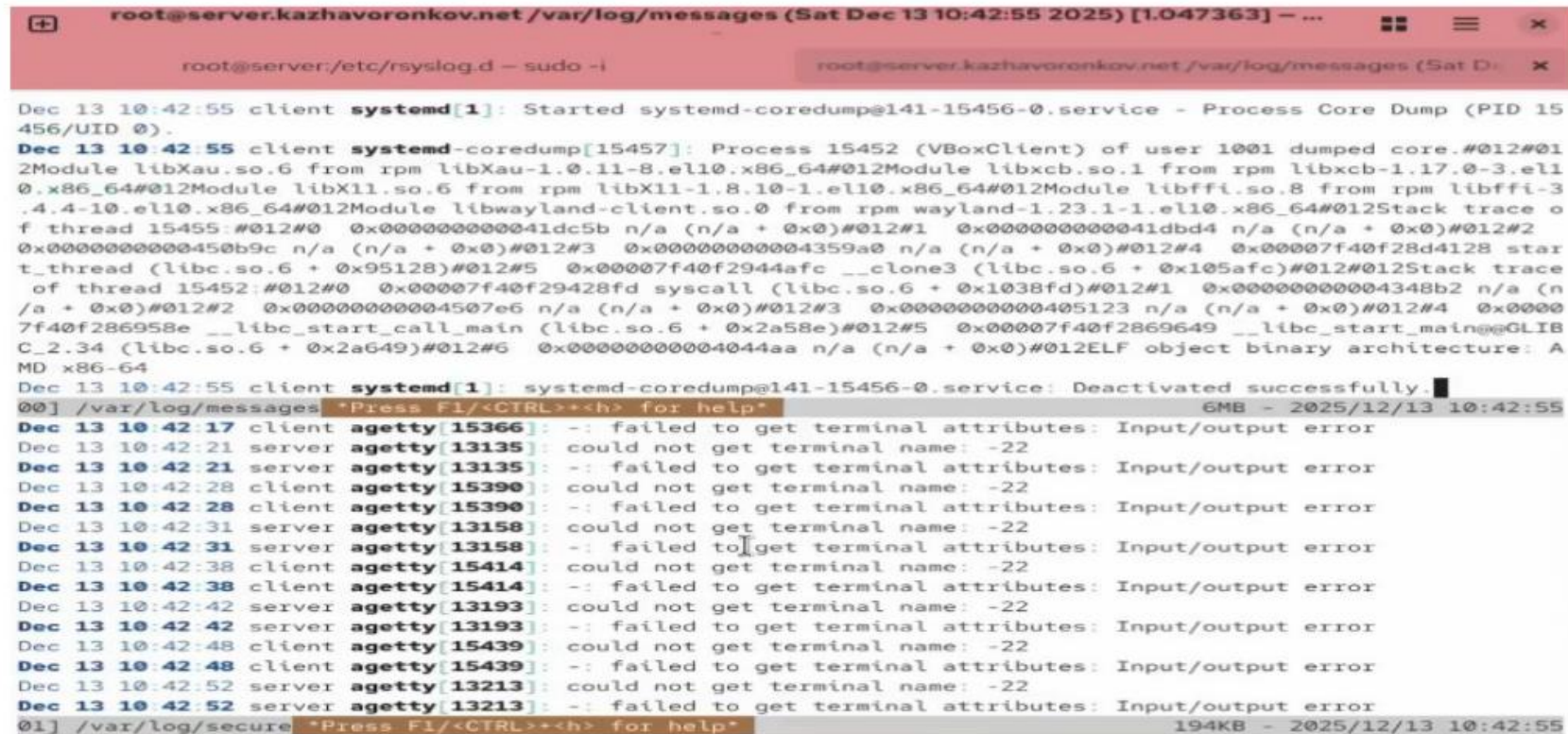
# Просмотр журнала

```
[root@server.kazhavoronkov.net ~]# dnf -y install multitail
Last metadata expiration check: 0:04:09 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

The image shows a Multitail terminal window with two panes. The top pane shows the command 'root@server:/etc/rsyslog.d - sudo -i' and the bottom pane shows the command 'root@server.kazhavoronkov.net /var/log/messages (Sat Dec 13 10:42:55 2025) [1.047363] - ...'. The main log output in the bottom pane shows a successful core dump of the systemd-coredump@141-15456-0.service process, followed by a series of 'agetty' login attempts that all fail with the message 'failed to get terminal attributes: Input/output error'. The terminal window has a red title bar and standard window controls. The log output is color-coded with blue for client/server and green for agetty processes.

```
root@server.kazhavoronkov.net /var/log/messages (Sat Dec 13 10:42:55 2025) [1.047363] - ...
root@server:/etc/rsyslog.d - sudo -i
root@server.kazhavoronkov.net /var/log/messages (Sat Dec 13 10:42:55 2025) [1.047363] - ...

Dec 13 10:42:55 client systemd[1]: Started systemd-coredump@141-15456-0.service - Process Core Dump (PID 15456/UID 0).
Dec 13 10:42:55 client systemd-coredump[15457]: Process 15452 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-10.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x86_64#012Stack trace of thread 15455:#012#0 0x000000000041dc5b n/a (n/a + 0x0)#012#1 0x000000000041dbd4 n/a (n/a + 0x0)#012#2 0x0000000000450b9c n/a (n/a + 0x0)#012#3 0x00000000004359a0 n/a (n/a + 0x0)#012#4 0x000007f40f28d4128 start_thread (libc.so.6 + 0x95128)#012#5 0x000007f40f2944afc __clone3 (libc.so.6 + 0x105afc)#012#012Stack trace of thread 15452:#012#0 0x000007f40f29428fd syscall (libc.so.6 + 0x1038fd)#012#1 0x00000000004348b2 n/a (n/a + 0x0)#012#2 0x00000000004507e6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x000007f40f286958e __libc_start_call_main (libc.so.6 + 0x2a58e)#012#5 0x000007f40f2869649 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a649)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 13 10:42:55 client systemd[1]: systemd-coredump@141-15456-0.service: Deactivated successfully.
00] /var/log/messages: *Press F1/<CTRL>+<h> for help* 6MB - 2025/12/13 10:42:55
Dec 13 10:42:17 client agetty[15366]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:21 server agetty[13135]: could not get terminal name: -22
Dec 13 10:42:21 server agetty[13135]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:28 client agetty[15390]: could not get terminal name: -22
Dec 13 10:42:28 client agetty[15390]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:31 server agetty[13158]: could not get terminal name: -22
Dec 13 10:42:31 server agetty[13158]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:38 client agetty[15414]: could not get terminal name: -22
Dec 13 10:42:38 client agetty[15414]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:42 server agetty[13193]: could not get terminal name: -22
Dec 13 10:42:42 server agetty[13193]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:48 client agetty[15439]: could not get terminal name: -22
Dec 13 10:42:48 client agetty[15439]: -: failed to get terminal attributes: Input/output error
Dec 13 10:42:52 server agetty[13213]: could not get terminal name: -22
Dec 13 10:42:52 server agetty[13213]: -: failed to get terminal attributes: Input/output error
01] /var/log/secure: *Press F1/<CTRL>+<h> for help* 194KB - 2025/12/13 10:42:55
```

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/netlog/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



The screenshot shows a terminal window with a pink title bar. The title bar contains the text 'root@server:/vagrant/provision/server - sudo -i' and window control icons. Below the title bar, there are two tabs: 'root@server:/etc/rsyslog.d - sudo -i' and 'root@server:/vagrant/provision/server - sudo -i'. The main content area shows the GNU nano 8.1 editor editing a file named 'netlog.sh'. The editor's status bar at the top indicates 'netlog.sh' and 'Modified'. The script content is as follows:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

# 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/client/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



The image shows a terminal window with a pink title bar. The title bar contains a plus icon on the left, the text 'root@client:/vagrant/provision/client - sudo -i' in the center, and window control icons (maximize, close) on the right. The terminal content shows the GNU nano 8.1 editor editing a file named 'netlog.sh'. The script contains several lines of code for provisioning, including echo statements, package installation with dnf, file copying, and service management with systemctl.

```
GNU nano 8.1 netlog.sh Modified
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install lnav
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog
```



# 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"
```