

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №15

дисциплина: Администрирование сетевых подсистем

Студент: Жаворонков Кирилл Александрович

Студ. билет № 1132231844

Группа: НПИбд-01-23

МОСКВА

2025 г.

Цель работы:

Целью данной работы является получение навыков по работе с журналами системных событий.

Выполнение работы:

На сервере создадим файл конфигурации сетевого хранения журналов (Рис. 1.1):

```
cd /etc/rsyslog.d
```

```
touch netlog-server.conf
```



The screenshot shows a terminal window with a red header bar containing the text "root@server:/etc/rsyslog.d – sudo -i". The main area of the terminal shows the following command history:

```
[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.

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514 (Рис. 1.2):



The screenshot shows a terminal window with a red header bar containing the text "root@server:/etc/rsyslog.d – sudo -i". The main area of the terminal shows the following command history:

```
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.

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются (Рис. 1.3):

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.

На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514 (Рис. 1.4):

```
firewall-cmd --add-port=514/tcp
```

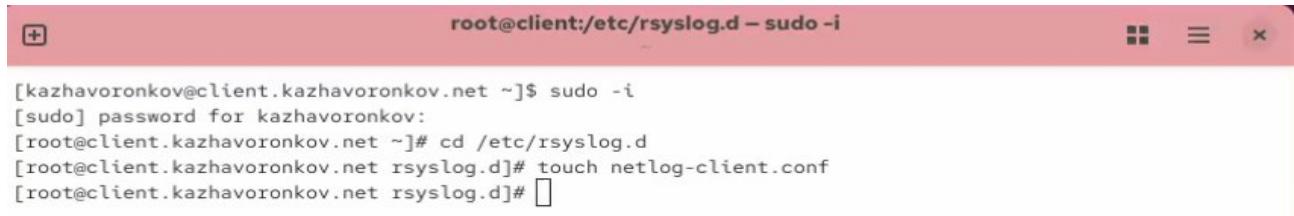
```
firewall-cmd --add-port=514/tcp --permanent
```

```
[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.

На клиенте создадим файл конфигурации сетевого хранения журналов (Рис. 2.1):

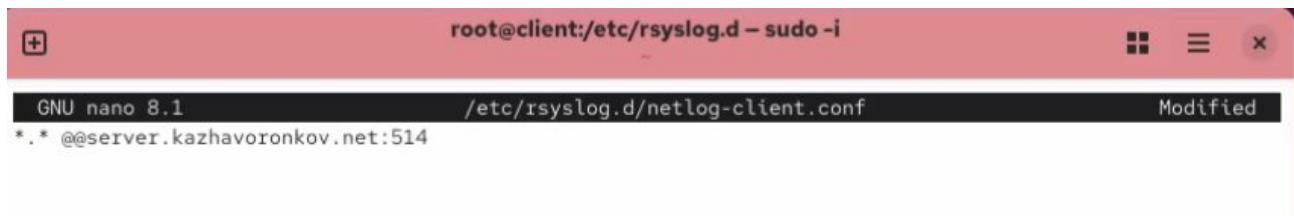
```
cd /etc/rsyslog.d  
touch netlog-client.conf
```



```
[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.

Далее в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 2.2):

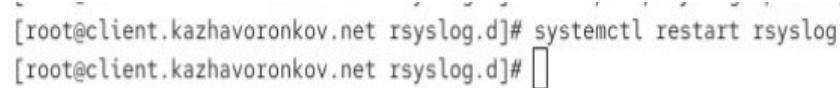


```
GNU nano 8.1          /etc/rsyslog.d/netlog-client.conf      Modified  
*.* @@server.kazhavoronkov.net:514
```

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

Перезапустим службу rsyslog (Рис. 2.3):

```
systemctl restart rsyslog
```



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

Рис. 2.3. Перезапуск службы rsyslog.

На сервере просмотрим один из файлов журнала (Рис. 3.1):



```
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.

На сервере под пользователем kazhavoronkov запустим графическую про-
грамму для просмотра журналов (Рис. 3.2):

gnome-system-monitor

kazhavoronkov@server:~ – gnome-system-monitor

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registrayd	kazhavoronkov	0.00	5701	131.1 kB	471.0 kB	
at-spi-bus-launcher	kazhavoronkov	0.00	5693	262.1 kB	307.2 kB	
bash	kazhavoronkov	0.00	7343	2.0 MB	6.6 MB	
bash	kazhavoronkov	0.00	11738	2.0 MB	1.7 MB	
catatonit	kazhavoronkov	0.00	7302	N/A	679.9 kB	
dbus-broker	kazhavoronkov	0.00	5563	1.4 MB	1.6 MB	
dbus-broker	kazhavoronkov	0.00	5700	262.1 kB	188.4 kB	
dbus-broker-launch	kazhavoronkov	0.00	5561	262.1 kB	184.3 kB	
dbus-broker-launch	kazhavoronkov	0.00	5699	N/A	N/A	
dconf-service	kazhavoronkov	0.00	7241	262.1 kB	479.2 kB	12.1 kB
evolution-addressbook-factory	kazhavoronkov	0.00	5971	N/A	3.0 MB	53.1 kB
evolution-alarm-notify	kazhavoronkov	0.00	5892	393.2 kB	1.6 MB	
evolution-calendar-factory	kazhavoronkov	0.00	5802	917.5 kB	4.1 MB	
evolution-source-registry	kazhavoronkov	0.00	5729	131.1 kB	3.0 MB	
firefox	kazhavoronkov	0.00	6651	182.4 MB	486.2 MB	171.2 kB
gdm-wayland-session	kazhavoronkov	0.00	5558	N/A	4.1 kB	
gjs	kazhavoronkov	0.00	5747	122.9 kB	98.3 kB	
nis	kazhavoronkov	0.00	5987	3.2 MB	6.5 MB	

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

На сервере установим просмотрщик журналов системных сообщений multitail (Рис. 3.3):

Установить lnav на Rocky Linux версии 10 не удается

```
dnf -y install multitail
```

```
[root@server.kazhavoronkov.net ~]# dnf -y install multitail
Last metadata expiration check: 0:04:01 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 scriptlets: multitail-7.1.3-2.el10_0.x86_64                         1/1
```

Рис. 3.3. Установка на сервере просмотрщика журналов системных сообщений lnav.

Просмотрим логи с помощью multitail (Рис. 3.4):

multitail

```
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 libXi11.so.6 from rpm libXi11-1.8.10-1.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 0x00007f40f28d4128 star t_thread (libc.so.6 + 0x95128)#012#5 0x00007f40f2944afc __clone3 (libc.so.6 + 0x105afc)#012#012Stack trace of thread 15452:#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 0x00007f40f286958e __libc_start_main (libc.so.6 + 0x2a58e)@012#5 0x00007f40f2869649 __libc_start_main@GLIBC_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 10:42:55 client systemd[1]: systemd-coredump@141-15456-0.service: Deactivated successfully.
[0] /var/log/messages *Press F1/<CTRL>+<h> for help*
```

Рис. 3.4. Просмотр логов с помощью Multitail.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh (Рис. 4.1):

```
[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]#
```

Рис. 4.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (Рис. 4.2):



```
GNU nano 8.1
#!/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
```

Рис. 4.2. Открытие файла на редактирование и добавление в него скрипта.

На виртуальной машине client перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём

каталог nentlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh (Рис. 4.3):

```
[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]#
```

Рис. 4.3. Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (Рис. 4.4):



```
GNU nano 8.1                                     netlog.sh                                         Modified
#!/bin/bash
echo "Provisioning script $@"
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
```

Рис. 4.4. Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавим в соответствующих разделах конфигураций для сервера (Рис. 4.5) и клиента (Рис. 4.6):

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

Рис. 4.5. Добавление конфигураций в конфигурационном файле Vagrantfile для сервера.

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

Рис. 4.6. Добавление конфигураций в конфигурационном файле Vagrantfile для клиента.

Вывод:

В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.

Ответы на контрольные вопросы:

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald? - Для приёма сообщений от journald в rsyslog используется модуль **imjournal**.
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog? - Устаревший модуль для приема сообщений журнала в rsyslog - **imuxsock** (или **imuxsock_legacy**).
3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать? - Для предотвращения использования устаревшего ме-

тода можно использовать параметр SystemMaxUseForward=no в файле /etc/systemd/journald.conf.

4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала? - **Настройки, позволяющие настроить работу журнала, содержатся в файле /etc/systemd/journald.conf.**
5. Каким параметром управляется пересылка сообщений из journald в rsyslog? - **Для управления пересылкой сообщений из journald в rsyslog используется параметр ForwardToSyslog=yes в файле /etc/systemd/journald.conf.**
6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog? - **Для включения сообщений из файла журнала, не созданного rsyslog, используется модуль imfile.**
7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB? - **Для пересылки сообщений в базу данных MariaDB используется модуль ommysql или ommysqlps.**
8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP? - **Добавьте следующие строки в rsyslog.conf:**

\$ModLoad imtcp

\$InputTCPServerRun 514

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514? –

Используйте команды для открытия порта:

sudo firewall-cmd --permanent --add-port=514/tcp

```
sudo firewall-cmd --reload
```

Или:

```
sudo iptables -A INPUT -p tcp --dport 514 -j ACCEPT
```

```
sudo service iptables save
```

```
sudo service iptables restart
```