

# **Отчет по лабораторной работе №15**

**Дисциплина: Администрирование сетевых подсистем**

Иванов Сергей Владимирович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Настройка сервера сетевого журнала . . . . .	6
3.2	Настройка клиента сетевого журнала . . . . .	7
3.3	Просмотр журнала . . . . .	9
3.4	Внесение изменений в настройки внутреннего окружения виртуальных машин . . . . .	11
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>14</b>
<b>5</b>	<b>Выводы</b>	<b>16</b>

## Список иллюстраций

3.1	Запуск Server . . . . .	6
3.2	Создание конф. файла . . . . .	6
3.3	Редактирование конф. файла . . . . .	7
3.4	Просмотр портов связанных с rsyslog . . . . .	7
3.5	Настройка firewall . . . . .	7
3.6	Запуск Client . . . . .	8
3.7	Создание конф.файла . . . . .	8
3.8	Редактирование конф. файла . . . . .	8
3.9	Перезапуск службы . . . . .	8
3.10	Просмотр файла журнала . . . . .	9
3.11	Запуск программы для просмотра журналов . . . . .	9
3.12	Установка lnav . . . . .	10
3.13	Просмотр логов . . . . .	10
3.14	Установка lnav . . . . .	10
3.15	Просмотр логов . . . . .	11
3.16	Создание каталогов и копирование конф.файлов . . . . .	11
3.17	Создание скрипта . . . . .	12
3.18	Создание каталогов и копирование конф.файлов . . . . .	12
3.19	Создание скрипта . . . . .	13
3.20	Редактирование Vagrantfile . . . . .	13
3.21	Редактирование Vagrantfile . . . . .	13

# **1 Цель работы**

Получение навыков по работе с журналами системных событий.

## 2 Задание

1. Настройте сервер сетевого журналирования событий
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере
3. Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.
4. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

## 3 Выполнение лабораторной работы

### 3.1 Настройка сервера сетевого журнала

Запускаю виртуальную машину Server. (рис. 1)

```
C:\work_asp\svivanov\vagrant>vagrant halt server  
  
C:\work_asp\svivanov\vagrant>vagrant up server  
Bringing machine 'server' up with 'virtualbox' provider...  
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.  
==> server: This is very often used by the router and can cause the  
==> server: network to not work properly. If the network doesn't work  
==> server: properly, try changing this IP.  
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.  
==> server: This is very often used by the router and can cause the
```

Рис. 3.1: Запуск Server

На сервере создадим файл конфигурации сетевого хранения журналов:

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

```
touch netlog-server.conf (рис. 2)
```

```
[root@server.svivanov.net ~]# cd /etc/rsyslog.d  
[root@server.svivanov.net rsyslog.d]# touch netlog-server.conf
```

Рис. 3.2: Создание конф. файла

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

```
$ModLoad imtcp
```

```
$InputTCPServerRun 514 (рис. 3)
```

```
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 3.3: Редактирование конф. файла

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются:

```
systemctl restart rsyslog
```

```
lsof | grep TCP (рис. 4)
```

```
rsyslogd 13438          root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438          root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13440 in:imjour    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13440 in:imjour    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13441 in:imtcp    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13441 in:imtcp    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13442 in:imtcp    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13442 in:imtcp    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13443 in:imtcp    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13443 in:imtcp    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13444 rs:main    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13444 rs:main    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13445 in:imtcp    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13445 in:imtcp    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13446 in:imtcp    root    4u    IPv4    45592    0t0    TCP *:shell (LISTEN)
rsyslogd 13438 13446 in:imtcp    root    5u    IPv6    45593    0t0    TCP *:shell (LISTEN)
[root@server.svivanov.net rsyslog.d]#
```

Рис. 3.4: Просмотр портов связанных с rsyslog

На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514:

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

```
firewall-cmd --add-port=514/tcp --permanent (рис. 5)
```

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

Рис. 3.5: Настройка firewall

## 3.2 Настройка клиента сетевого журнала

Запускаю виртуальную машину Client. (рис. 6)

```
C:\work_asp\svivanov\vagrant>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
      client: Adapter 1: nat
      client: Adapter 2: intnet
==> client: Forwarding ports...
```

Рис. 3.6: Запуск Client

На клиенте создадим файл конфигурации сетевого хранения журналов:

`cd /etc/rsyslog.d`

`touch netlog-client.conf` (рис. 7)

```
[root@client.svivanov.net ~]# cd /etc/rsyslog.d
[root@client.svivanov.net rsyslog.d]# touch netlog-client.conf
[root@client.svivanov.net rsyslog.d]#
```

Рис. 3.7: Создание конф.файла

На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включим перенаправление сообщений журнала на 514 TCP-порт сервера: `@[server.user.net:514?]` (рис. 8)

```
*.* @@server.svivanov.net:514
~
~
~
```

Рис. 3.8: Редактирование конф. файла

Перезапустим службу rsyslog: `systemctl restart rsyslog` (рис. 9)

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

Рис. 3.9: Перезапуск службы

### 3.3 Просмотр журнала

На сервере посмотрим один из файлов журнала: `tail -f /var/log/messages` (рис. 10)

```
[root@server.svivanov.net rsyslog.d]# tail -f /var/log/messages
Dec 3 09:41:08 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 53.
Dec 3 09:41:08 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:18 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:18 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 54.
Dec 3 09:41:18 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:28 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:29 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 55.
Dec 3 09:41:29 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:34 server named[1334]: timed out resolving 'mirrors.fedoraproject.org/A/IN': 127.0.0.1#53
Dec 3 09:41:34 server named[1334]: timed out resolving 'mirrors.fedoraproject.org/AAAA/IN': 127.0.0.1#53
Dec 3 09:41:39 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:39 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 56.
Dec 3 09:41:39 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

Рис. 3.10: Просмотр файла журнала

На сервере под пользователем `user` запустим графическую программу для просмотра журналов: `gnome-system-monitor` (рис. 11)

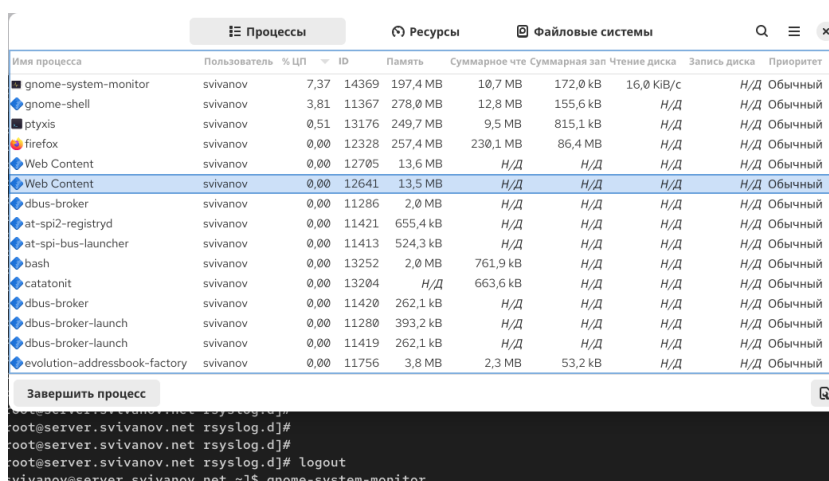


Рис. 3.11: Запуск программы для просмотра журналов

На сервере установим просмотрщик журналов системных сообщений `lnav`: `dnf -y install lnav` (рис. 12)

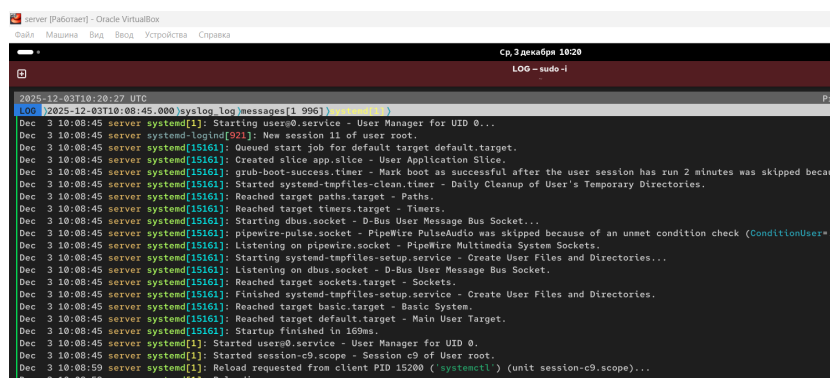
```
[svivanov@server.svivanov.net ~]$ sudo dnf -y install lnav
Last metadata expiration check: 0:00:06 ago on Cp 03 дек 2025 10:09:10.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
lnav                   x86_64            0.11.1-1.el9     epel              2.4 M

Transaction Summary
=====
Install 1 Package

Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
lnav-0.11.1-1.el9.x86_64.rpm                                5.7 MB/s | 2.4 MB  00:00
-----
Total
2.4 MB/s | 2.4 MB  00:00
Extra Packages for Enterprise Linux 9 - x86_64
1.6 MB/s | 1.6 kB  00:00
Importing GPG key 0x3228467C:
Userid : "Fedora (epel9) <epel@fedoraproject.org>"
```

Рис. 3.12: Установка lnav

## Просмотр логов с помощью lnav на сервере: (рис. 13)



```
server [Работает] - Oracle VM VirtualBox
Файлы Машина Вид Ввод Устройства Справка
LOG - sudo -i
2025-12-03T10:28:27 UTC
[LOG] 2025-12-03T10:08:45.000 syslog_log/messages[1 996]
Dec 3 10:08:45 server systemd[1]: Starting users@.service - User Manager for UID 0...
Dec 3 10:08:45 server systemd-logind[521]: New session 11 of user root.
Dec 3 10:08:45 server systemd[15161]: Created slice app.slice - User Application Slice.
Dec 3 10:08:45 server systemd[15161]: grub-boot-success.timer - Mark boot as successful after the user session has run 2 minutes was skipped because...
Dec 3 10:08:45 server systemd[15161]: Started systemd-tmpfiles-clean.timer - Daily Cleanup of User's Temporary Directories.
Dec 3 10:08:45 server systemd[15161]: Reached target paths.target - Paths.
Dec 3 10:08:45 server systemd[15161]: Reached target timers.target - Timers.
Dec 3 10:08:45 server systemd[15161]: Starting dbus.socket - D-Bus User Message Bus Socket...
Dec 3 10:08:45 server systemd[15161]: pipewire-pulse.socket - PipeWire PulseAudio was skipped because of an unmet condition check (ConditionUser=inc...
Dec 3 10:08:45 server systemd[15161]: Listening on pipewire.socket - PipeWire Multimedia System Sockets.
Dec 3 10:08:45 server systemd[15161]: Starting systemd-tmpfiles-setup.service - Create User Files and Directories...
Dec 3 10:08:45 server systemd[15161]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Dec 3 10:08:45 server systemd[15161]: Reached target sockets.target - Sockets.
Dec 3 10:08:45 server systemd[15161]: Finished systemd-tmpfiles-setup.service - Create User Files and Directories.
Dec 3 10:08:45 server systemd[15161]: Reached target basic.target - Basic System.
Dec 3 10:08:45 server systemd[15161]: Reached target default.target - Main User Target.
Dec 3 10:08:45 server systemd[15161]: Startup finished in 169ms.
Dec 3 10:08:45 server systemd[1]: Started users@.service - User Manager for UID 0.
Dec 3 10:08:45 server systemd[1]: Started session-c9.scope - Session c9 of user root.
Dec 3 10:08:59 server systemd[1]: Reload requested from client PID 15200 ('systemctl') (unit session-c9.scope)...
Dec 3 10:08:59 server systemd[1]: Reloading...
```

Рис. 3.13: Просмотр логов

На клиенте установим просмотрщик журналов системных сообщений lnav:  
dnf -y install lnav (рис. 14)

```
[root@client.svivanov.net ~]$ dnf install -y lnav
Extra Packages for Enterprise Linux 9 - x86_64                2.4 MB/s | 5.9 MB  00:02
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64 878 B/s | 1.7 kB  00:01
Зависимости разрешены.
=====
Пакет                Архитектура      Версия           Репозиторий        Размер
=====
Установка:
lnav                   x86_64            0.11.1-1.el9     epel              2.4 M

Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 2.4 M
Объем изменений: 6.1 M
Загрузка пакетов:
lnav-0.11.1-1.el9.x86_64.rpm                                5.5 MB/s | 2.4 MB  00:00
```

Рис. 3.14: Установка lnav

## Просмотр логов с помощью lnav на клиенте: (рис. 15)

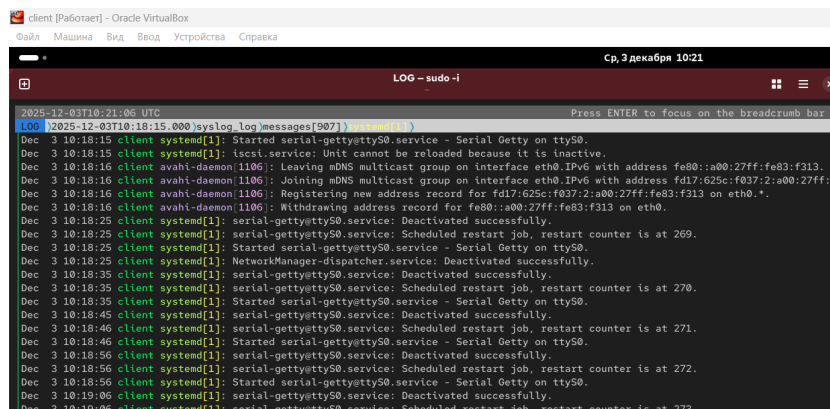


Рис. 3.15: Просмотр логов

### 3.4 Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине `server` перейдем 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: (рис. 16)

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf
-> /vagrant/provision/server/netlog/etc/rsyslog.d
```

```
[root@server.svivanov.net ~]# cd /vagrant/provision/server
[root@server.svivanov.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.svivanov.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.svivanov.net server]#
```

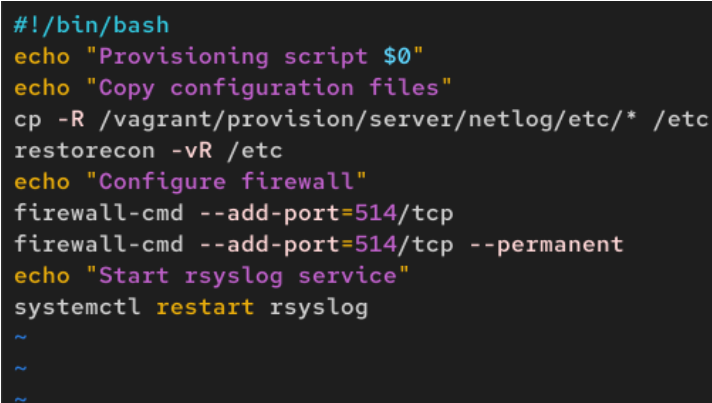
Рис. 3.16: Создание каталогов и копирование конф.файлов

В каталоге `/vagrant/provision/server` создайте исполняемый файл `netlog.sh`: (рис. 17)

```
cd /vagrant/provision/server
```

```
touch netlog.sh
chmod +x netlog.sh
```

Открыв его на редактирование, пропишем в нём следующий скрипт:




```
#!/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. 3.17: Создание скрипта

На виртуальной машине client перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы: (рис. 18)

```
cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-client.conf
-> /vagrant/provision/client/netlog/etc/rsyslog.d/
```



```
[root@client.svivanov.net rsyslog.d]# cd /vagrant/provision/client
[root@client.svivanov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.svivanov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.svivanov.net client]#
```

Рис. 3.18: Создание каталогов и копирование конф.файлов

В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh:

```
cd /vagrant/provision/client
touch netlog.sh
chmod +x netlog.sh
```

Открыв его на редактирование, пропишем в нём следующий скрипт: (рис. 19)

```
#!/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
```

Рис. 3.19: Создание скрипта

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента: (рис. 20, 21)

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

Рис. 3.20: Редактирование Vagrantfile

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

Рис. 3.21: Редактирование Vagrantfile

## 4 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 приёма сообщений журнала — imuxsock (хотя он всё ещё используется для приёма сообщений через сокет, но для интеграции с journald лучше использовать imjournal).

**3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?**

Чтобы отключить устаревший метод, в файле конфигурации rsyslog следует добавить параметр:

```
$OmitLocalLogging off
```

Или явно отключить imuxsock, если он не требуется.

**4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?**

Основной конфигурационный файл rsyslog — /etc/rsyslog.conf, а также дополнительные файлы в директории /etc/rsyslog.d/.

**5. Каким параметром управляется пересылка сообщений из journald в rsyslog?**

Пересылка сообщений из journald в rsyslog управляется параметром ForwardToSyslog= в файле /etc/systemd/journal.conf.

**6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?**

Для чтения сообщений из внешних файлов журнала 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.

**8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?**

В файл rsyslog.conf или в файл в /etc/rsyslog.d/ нужно добавить:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

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

Для настройки firewallld можно использовать команды:

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

## **5 Выводы**

В ходе выполнения лабораторной работы мы получили навыки по работе с журналами системных событий.