РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

Отчет лабораторной работы 15

Дисциплина: Администрирование сетевых подсистем

Студент: Астахова Марина

Группа: НПИбд-02-23

Тема: Настройка сетевого журналирования.

15.1. Цель работы.

Получение навыков по работе с журналами системных событий.

15.2. Выполнение работы.

15.2.1. Настройка сервера сетевого журнала

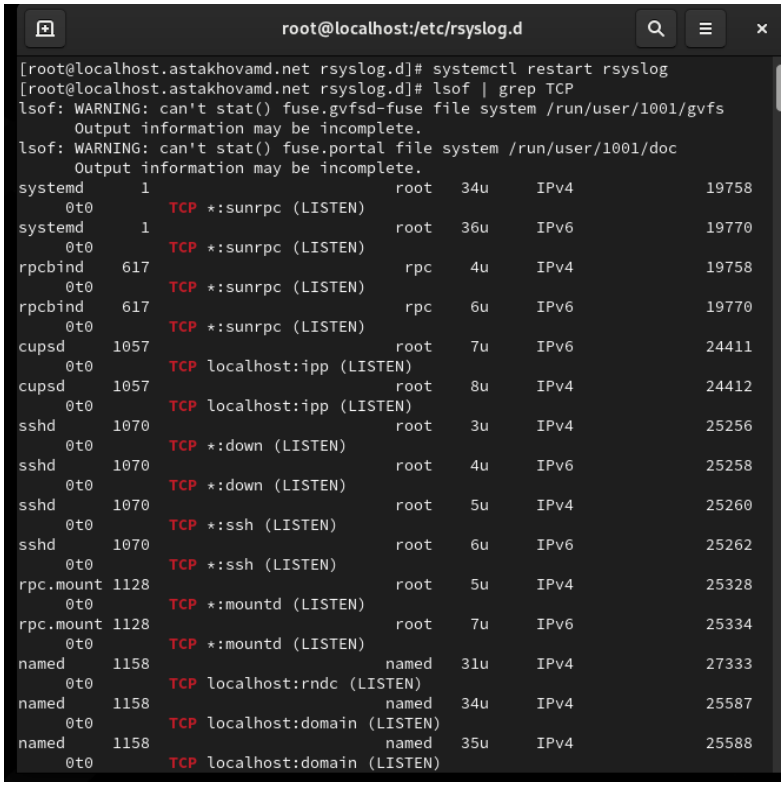
1.На сервере создаем файл конфигурации сетевого хранения журналов:

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

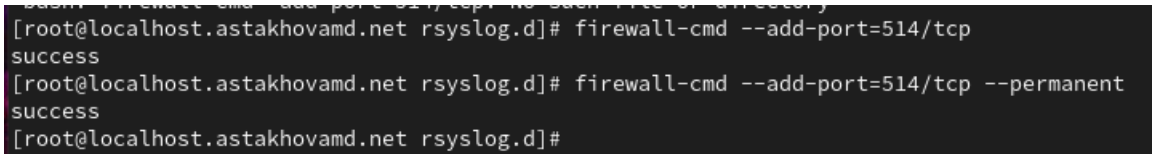
2. В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514:

```
[root@localhost.astakhovamd.net rsyslog.d]# sudo tee /etc/rsyslog.d/netlog-serve
r.conf << 'EOF'
$ModLoad imtcp

$InputTCPServerRun 514
EOF
$ModLoad imtcp

$InputTCPServerRun 514
[root@localhost.astakhovamd.net rsyslog.d]#
```

3. Перезапустим службу rsyslog и посмотрим порты, связанные с rsyslog, прослушиваются:

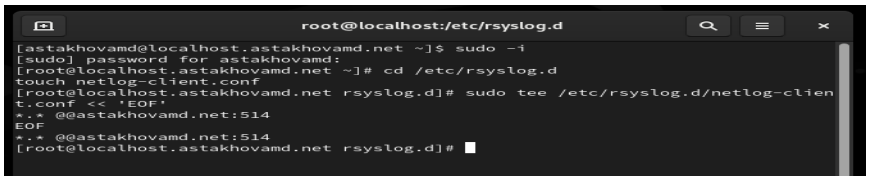


4. На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514:

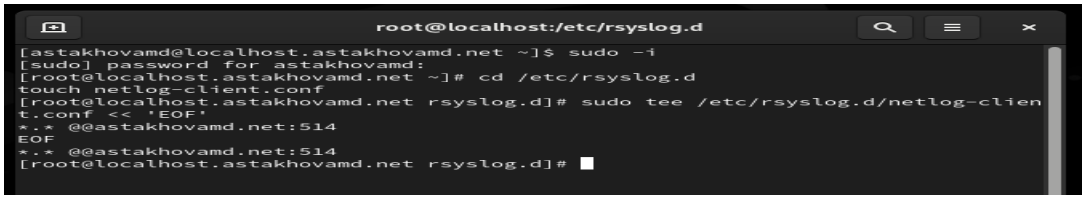


15.2.2. Настройка клиента сетевого журнала

1. На клиенте создаем файл конфигурации сетевого хранения журналов:



2. На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщений журналана 514 TCP-порт сервера

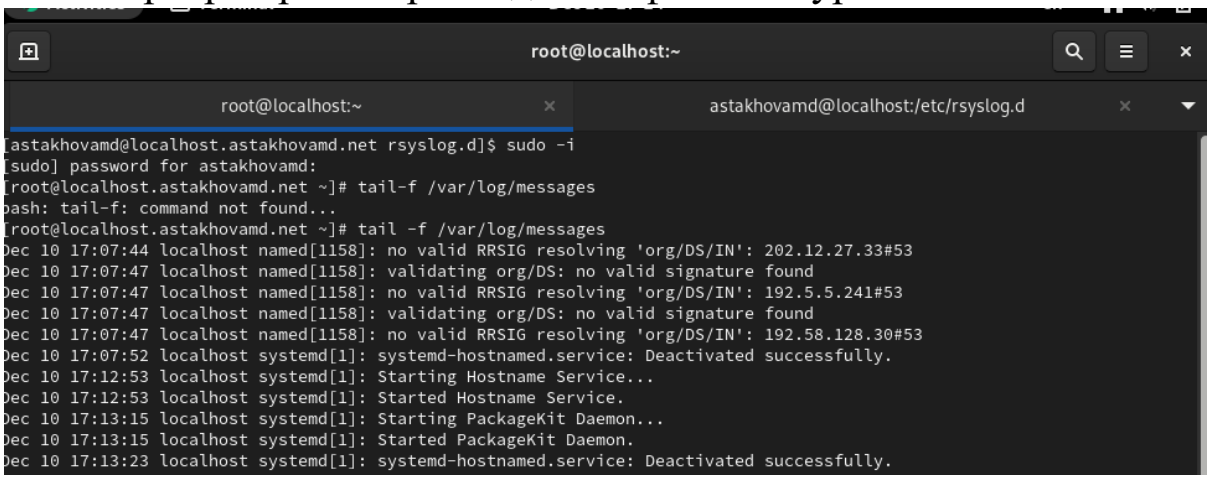


3. Перезапустим службу rsyslog

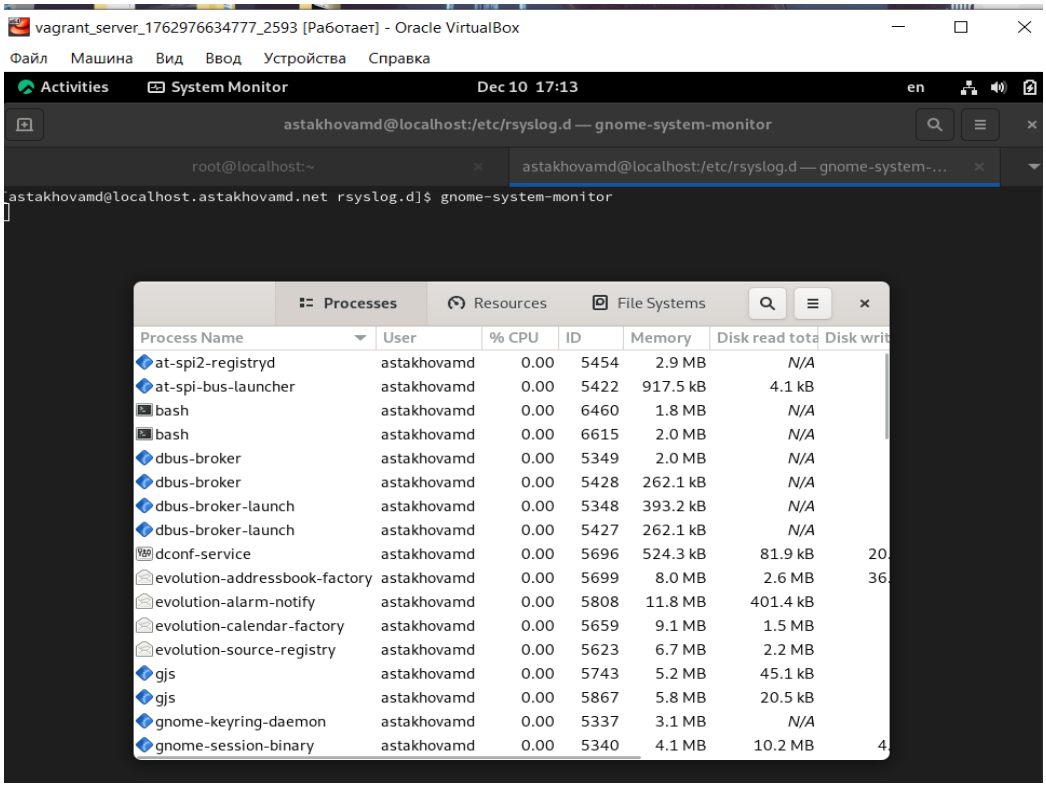
```
[root@localhost.astakhovamd.net rsyslog.d]# systemctl restart rsyslog
[root@localhost.astakhovamd.net rsyslog.d]#
```

15.2.3. Просмотр журнала

1. На сервере просмотрим один из файлов журнала



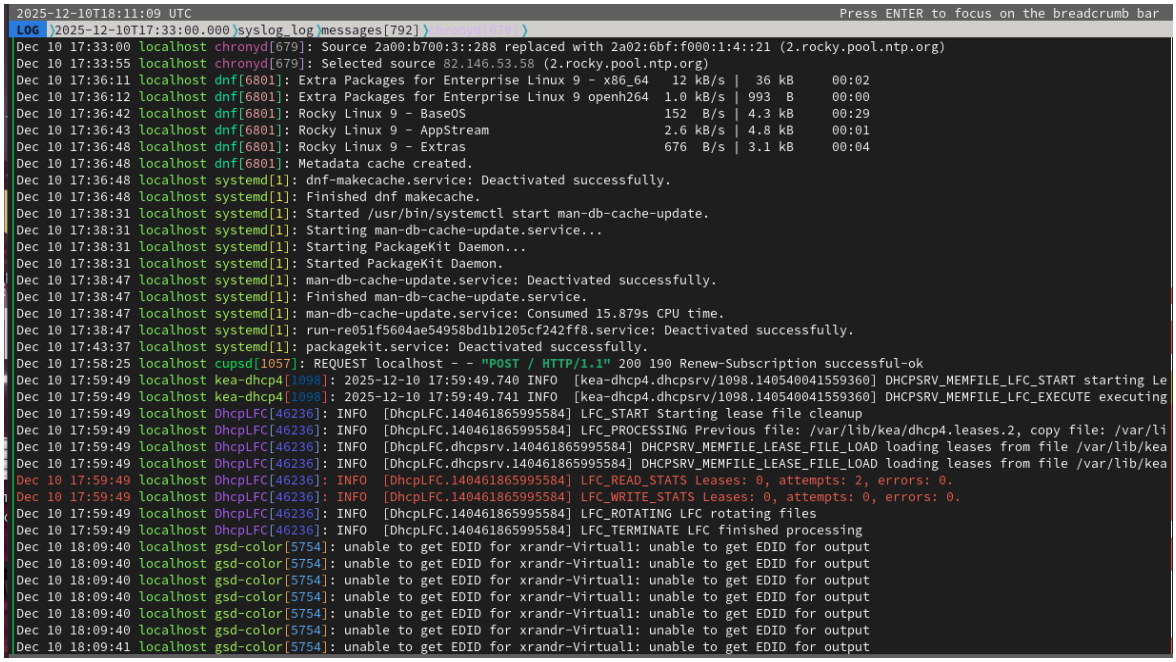
2. На сервере под пользователем запустим графическую программу для просмотра журналов:



3.На сервере установим просмотрщик журналов системных сообщений lnav или его аналог:

```
[root@localhost.astakhovamd.net ~]# dnf -y install lnav
Extra Packages for Enterprise Linux 9 - x86_64                                  2.4 kB/s |  36 kB     00:14
Extra Packages for Enterprise Linux 9 - x86_64                                   32 kB/s |  20 MB     10:41
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64             854  B/s | 993  B     00:01
Rocky Linux 9 - BaseOS                                                           216  B/s | 4.3 kB     00:20
Rocky Linux 9 - BaseOS                                                           206 kB/s | 5.1 MB     00:25
Rocky Linux 9 - AppStream                                                        576  B/s | 4.8 kB     00:08
Rocky Linux 9 - AppStream                                                         37 kB/s |  10 MB     04:44
Rocky Linux 9 - Extras                                                           397  B/s | 3.1 kB     00:07
Rocky Linux 9 - Extras                                                           1.8 kB/s |  16 kB     00:08
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                                                     20 kB/s | 2.4 MB     02:02
----------------------------------------------------------------------------------------------------------------
Total                                                                            17 kB/s | 2.4 MB     02:21
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                        1/1
  Installing       : lnav-0.11.1-1.el9.x86_64                                                               1/1
  Running scriptlet: lnav-0.11.1-1.el9.x86_64                                                               1/1
  Verifying        : lnav-0.11.1-1.el9.x86_64                                                               1/1

Installed:
  lnav-0.11.1-1.el9.x86_64

Complete!
[root@localhost.astakhovamd.net ~]#
```

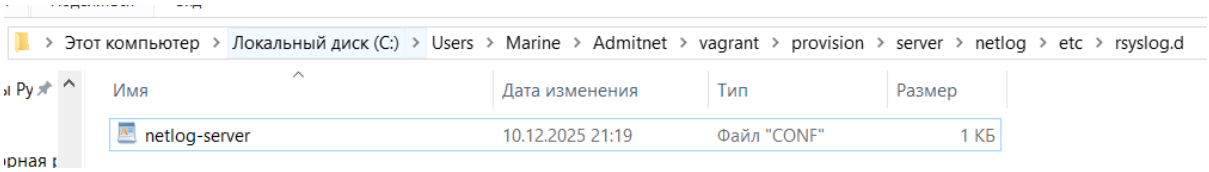
4. Просмотрим логи с помощью lnav или его аналога:



```
2025-12-10T18:11:09 UTC                                                                    Press ENTER to focus on the breadcrumb bar
LOG ⟩2025-12-10T17:33:00.000⟩syslog_log⟩messages[792]⟩chronyd[679]⟩
Dec 10 17:33:00 localhost chronyd[679]: Source 2a00:b700:3::288 replaced with 2a02:6bf:f000:1:4::21 (2.rocky.pool.ntp.org)
Dec 10 17:33:55 localhost chronyd[679]: Selected source 82.146.53.58 (2.rocky.pool.ntp.org)
Dec 10 17:36:11 localhost dnf[6801]: Extra Packages for Enterprise Linux 9 - x86_64   12 kB/s |  36 kB     00:02
Dec 10 17:36:12 localhost dnf[6801]: Extra Packages for Enterprise Linux 9 openh264  1.0 kB/s | 993  B     00:00
Dec 10 17:36:42 localhost dnf[6801]: Rocky Linux 9 - BaseOS                          152  B/s | 4.3 kB     00:29
Dec 10 17:36:43 localhost dnf[6801]: Rocky Linux 9 - AppStream                       2.6 kB/s | 4.8 kB     00:01
Dec 10 17:36:48 localhost dnf[6801]: Rocky Linux 9 - Extras                          676  B/s | 3.1 kB     00:04
Dec 10 17:36:48 localhost dnf[6801]: Metadata cache created.
Dec 10 17:36:48 localhost systemd[1]: dnf-makecache.service: Deactivated successfully.
Dec 10 17:36:48 localhost systemd[1]: Finished dnf makecache.
Dec 10 17:38:31 localhost systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 10 17:38:31 localhost systemd[1]: Starting man-db-cache-update.service...
Dec 10 17:38:31 localhost systemd[1]: Starting PackageKit Daemon...
Dec 10 17:38:31 localhost systemd[1]: Started PackageKit Daemon.
Dec 10 17:38:47 localhost systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 10 17:38:47 localhost systemd[1]: Finished man-db-cache-update.service.
Dec 10 17:38:47 localhost systemd[1]: man-db-cache-update.service: Consumed 15.879s CPU time.
Dec 10 17:38:47 localhost systemd[1]: run-re051f5604ae54958bd1b1205cf242ff8.service: Deactivated successfully.
Dec 10 17:43:37 localhost systemd[1]: packagekit.service: Deactivated successfully.
Dec 10 17:58:25 localhost cupsd[1057]: REQUEST localhost - - "POST / HTTP/1.1" 200 190 Renew-Subscription successful-ok
Dec 10 17:59:49 localhost kea-dhcp4[1098]: 2025-12-10 17:59:49.740 INFO  [kea-dhcp4.dhcpsrv/1098.140540041559360] DHCPSRV_MEMFILE_LFC_START starting Le
Dec 10 17:59:49 localhost kea-dhcp4[1098]: 2025-12-10 17:59:49.741 INFO  [kea-dhcp4.dhcpsrv/1098.140540041559360] DHCPSRV_MEMFILE_LFC_EXECUTE executing
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_START Starting lease file cleanup
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_PROCESSING Previous file: /var/lib/kea/dhcp4.leases.2, copy file: /var/li
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILE_LEASE_FILE_LOAD loading leases from file /var/lib/kea
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILE_LEASE_FILE_LOAD loading leases from file /var/lib/kea
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_READ_STATS Leases: 0, attempts: 2, errors: 0.
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_WRITE_STATS Leases: 0, attempts: 0, errors: 0.
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_ROTATING LFC rotating files
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_TERMINATE LFC finished processing
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:41 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
```

15.2.4. Внесение изменений в настройки внутреннего окружения виртуальных машин

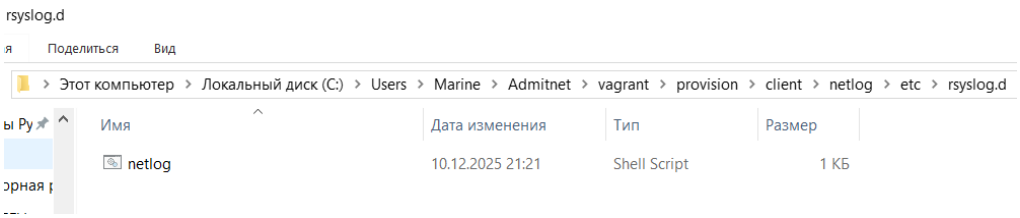
1. На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаем в нём каталог netlog, в котором поместим в соответствующие подкаталоги конфигурационные файлы и создадим файл.



Этот компьютер › Локальный диск (C:) › Users › Marine › Admitnet › vagrant › provision › server › netlog › etc › rsyslog.d

Имя	Дата изменения	Тип	Размер
netlog-server	10.12.2025 21:19	Файл "CONF"	1 КБ

2. То же самое делаем для client



rsyslog.d

Этот компьютер › Локальный диск (C:) › Users › Marine › Admitnet › vagrant › provision › client › netlog › etc › rsyslog.d

Имя	Дата изменения	Тип	Размер
netlog	10.12.2025 21:21	Shell Script	1 КБ

3. В данном файле пропишем 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
```

4. То же самое для client

```
#!/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
```

5. Внесем изменения в vagrantfile

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

end


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

nd
```

15.3. Итог работы.

В ходе выполнение лабораторной работы были получены навыки работы с системным журналом

15.4. Контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?

Модуль imjournal. Это современный модуль для приёма сообщений из systemd journal.

2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?

Модуль imuxsock. Это устаревший модуль, который читал сообщения из Unix-сокета /dev/log.

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

Параметр $OmitLocalLogging off (или установка в on для полного отключения).

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

Основной файл: /etc/systemd/journald.conf

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

Параметр ForwardToSyslog в файле /etc/systemd/journald.conf.

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

Модуль imfile. Он позволяет мониторить любые текстовые файлы.

7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?

Модуль ommysql (output module for MySQL/MariaDB).

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

$ModLoad imtcp
$InputTCPServerRun 514

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

Добавить службу syslog (порты 514/udp и 514/tcp)