

Отчёт по лабораторной работе №15

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Настройка сервера сетевого журнала	6
2.2	Настройка клиента сетевого журнала	7
2.3	Просмотр журнала	8
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	10
3	Выводы	12
4	Ответы на контрольные вопросы	13

Список иллюстраций

2.1	Редактирование файла конфигурации сетевого хранения журналов /etc/rsyslog.d/netlog-server.conf	6
2.2	Перезапуск rsyslog и просмотр прослушиваемых портов	7
2.3	Настройка межсетевого экрана для работы с TCP-портом 514 . . .	7
2.4	Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт	8
2.5	Просмотр файла журнала на сервере	8
2.6	Запуск графической программы для просмотра журналов	9
2.7	Использование lnav для просмотра логов	10

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение лабораторной работы

2.1 Настройка сервера сетевого журнала

На сервере создаем файл конфигурации сетевого хранения журналов: `cd /etc/rsyslog.d` и `touch netlog-server.conf`.

В данном файле включаем прием записей журнала по TCP-порту 514 (рис. 2.1).

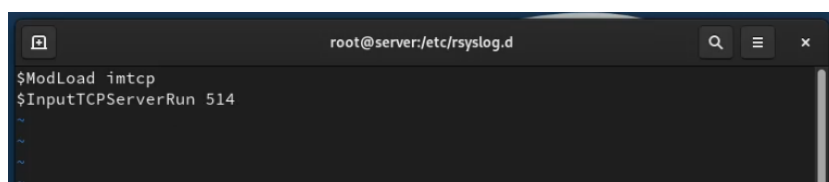


Рис. 2.1: Редактирование файла конфигурации сетевого хранения журналов `/etc/rsyslog.d/netlog-server.conf`

Перезапускаем службу `rsyslog` - `systemctl restart rsyslog` и просматриваем прослушиваемые порты, которые связаны со службой - `lsof | grep TCP` (рис. 2.2).

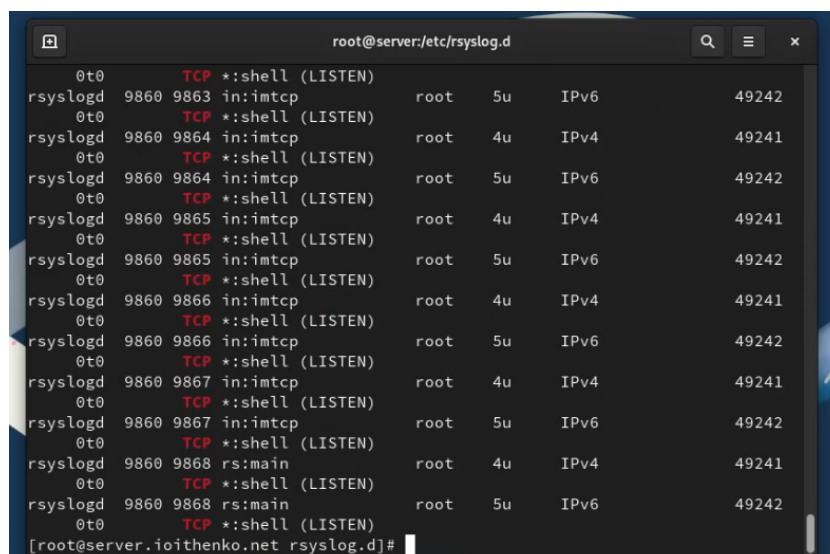


Рис. 2.2: Перезапуск rsyslog и просмотр прослушиваемых портов

На сервере настраиваем межсетевой экран для работы с TCP-портом 514 (рис. 2.3).

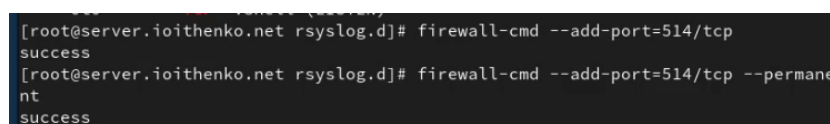


Рис. 2.3: Настройка межсетевого экрана для работы с TCP-портом 514

2.2 Настройка клиента сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов:

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

В данном файле включаем перенаправление сообщений журнала на 514 TCP-порт сервера и перезапускаем службу (рис. 2.4).

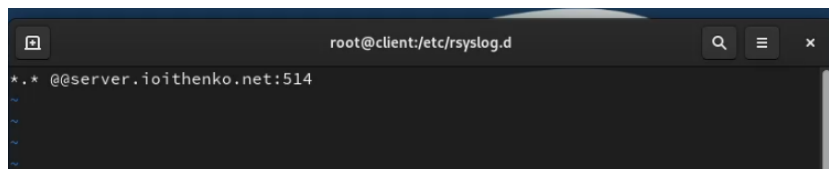


Рис. 2.4: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

2.3 Просмотр журнала

На сервере просматриваем один из файлов журнала. Обращаем внимание, что выводятся сообщения как с сервера, так и с клиента (рис. 2.5).

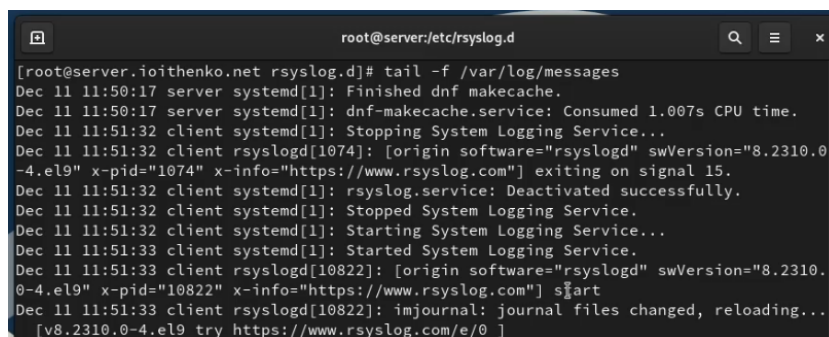


Рис. 2.5: Просмотр файла журнала на сервере

На сервере под пользователем ioithenko запускаем графическую программу для просмотра журналов (рис. 2.6).

Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ
at-spi2-registryd	ioithenko	0.00	8983	262.1 kB	319.5 kB	
at-spi-bus-launcher	ioithenko	0.00	8951	N/A	61.4 kB	
bash	ioithenko	0.00	9777	2.0 MB	6.4 MB	
bash	ioithenko	0.00	9884	2.0 MB	2.1 MB	
dbus-broker	ioithenko	0.00	8883	1.0 MB	2.0 MB	
dbus-broker	ioithenko	0.00	8957	131.1 kB	286.7 kB	
dbus-broker-launch	ioithenko	0.00	8882	131.1 kB	1.2 MB	
dbus-broker-launch	ioithenko	0.00	8956	N/A	24.6 kB	
dconf-service	ioithenko	0.00	9101	393.2 kB	1.2 MB	20
evolution-addressbook-factory	ioithenko	0.00	9106	N/A	22.8 MB	36
evolution-alarm-notify	ioithenko	0.00	9266	393.2 kB	6.8 MB	
evolution-calendar-factory	ioithenko	0.00	9085	N/A	1.9 MB	
evolution-source-registry	ioithenko	0.00	9065	N/A	4.1 MB	
gjs	ioithenko	0.00	9187	57.3 kB	1.7 MB	
gjs	ioithenko	0.00	9337	61.4 kB	2.4 MB	
gnome-keyring-daemon	ioithenko	0.00	8871	376.8 kB	N/A	
gnome-session-binary	ioithenko	0.00	8874	53.2 kB	52.4 MB	
gnome-session-binary	ioithenko	0.00	8997	426.0 kB	6.7 MB	4
gnome-session-ctl	ioithenko	0.00	8996	69.6 kB	24.6 kB	
gnome-shell	ioithenko	28.81	9016	83.8 MB	574.3 MB	
gnome-shell-calendar-server	ioithenko	0.00	9059	N/A	9.6 MB	
gnome-software	ioithenko	0.00	9284	29.7 MB	93.3 MB	
gnome-system-monitor	ioithenko	20.00	9914	15.9 MB	18.0 MB	

Рис. 2.6: Запуск графической программы для просмотра журналов

Устанавливаем просмотрщик журналов системных событий `lnav`: `dnf -y install lnav`.

Используем `lnav` для просмотра логов (рис. 2.7).

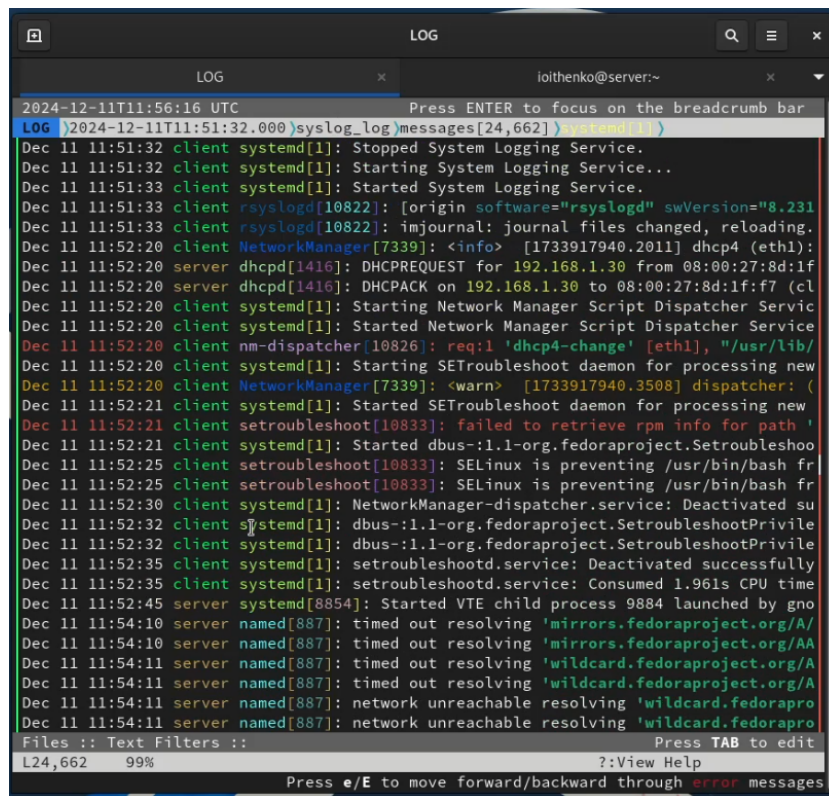


Рис. 2.7: Использование lnav для просмотра логов

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На VM server переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копируем в соответствующие каталоги конфигурационные файлы:

```
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
```

Вносим изменения в файл `/vagrant/provision/server/netlog.sh`.

На VM client переходим в каталог для внесения изменений в настройки внутреннего окружения и копируем в соответствующие каталоги конфигурационные

файлы:

```
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
```

Создаем и редактируем скрипт /vagrant/provision/client/netlog.sh.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляем записи в соответствующих разделах конфигураций для сервера и клиента:

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

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

3 Выводы

В ходе выполнения лабораторной работы я приобрела навыки по работе с журналами системных событий.

4 Ответы на контрольные вопросы

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

Для приёма сообщений от journald следует использовать модуль imjournal.

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

imklog

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

Следует использовать параметр "SystemCallFilter[include:omusrmsg.conf?]" в конфигурационном файле rsyslog.conf.

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

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле rsyslog.conf.

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

Пересылка сообщений из journald в rsyslog управляется параметром "ForwardToSyslog" в файле конфигурации journald.conf.

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

Модуль rsyslog, который можно использовать для включения сообщений из файла журнала, не созданного rsyslog, называется imfile.

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

Для пересылки сообщений в базу данных MariaDB следует использовать модуль ommysql.

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

Для позволения текущему журнальному серверу получать сообщения через TCP нужно включить две строки в rsyslog.conf:

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

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

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