

# **Отчет по лабораторной работе №15**

**Настройка сетевого журналирования**

Галацан Николай, НПИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Настройка сервера сетевого журнала . . . . .	5
2.2	Настройка клиента сетевого журнала . . . . .	6
2.3	Просмотр журнала . . . . .	7
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	9
<b>3</b>	<b>Выводы</b>	<b>11</b>
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>12</b>

# Список иллюстраций

2.1	Редактирование файла конфигурации сетевого хранения журналов /etc/rsyslog.d/netlog-server.conf . . . . .	5
2.2	Перезапуск rsyslog и просмотр прослушиваемых портов . . . . .	6
2.3	Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт . . . . .	7
2.4	Просмотр файла журнала на сервере . . . . .	7
2.5	Запуск графической программы для просмотра журналов . . . . .	8
2.6	Использование lnav для просмотра логов . . . . .	8
2.7	Редактирование netlog.sh на сервере . . . . .	9
2.8	Редактирование netlog.sh на клиенте . . . . .	10

# **1 Цель работы**

Получение навыков по работе с журналами системных событий.

## 2 Выполнение лабораторной работы

### 2.1 Настройка сервера сетевого журнала

На сервере создаю файл конфигурации сетевого хранения журналов:

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

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

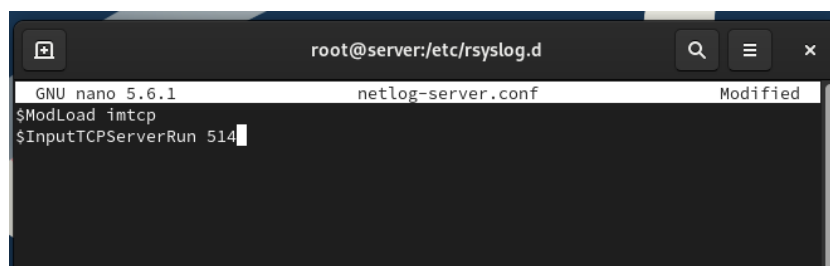
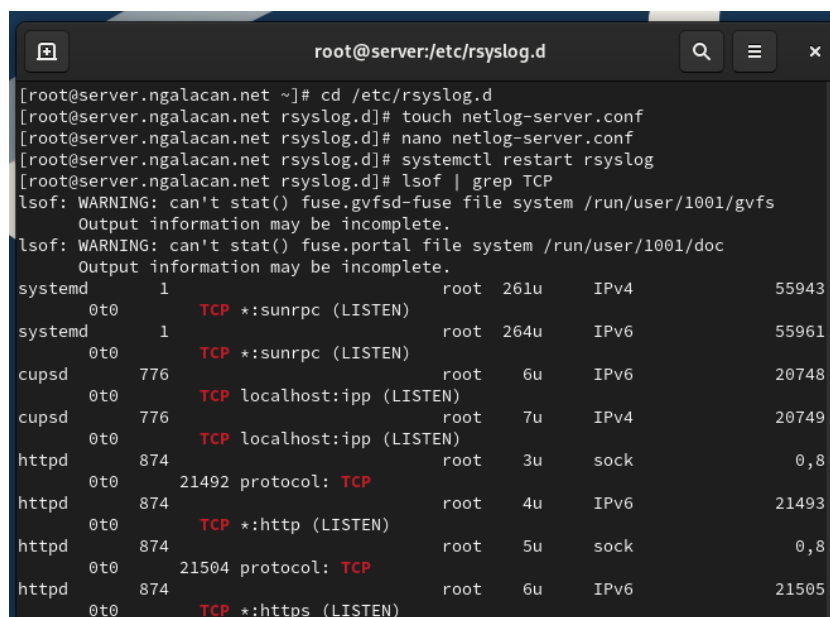


Рис. 2.1: Редактирование файла конфигурации сетевого хранения журналов /etc/rsyslog.d/netlog-server.conf

Перезапускаю службу rsyslog и просматриваю прослушиваемые порты, которые связаны со службой (рис. 2.2)



```
root@server:/etc/rsyslog.d
[root@server.ngalacan.net ~]# cd /etc/rsyslog.d
[root@server.ngalacan.net rsyslog.d]# touch netlog-server.conf
[root@server.ngalacan.net rsyslog.d]# nano netlog-server.conf
[root@server.ngalacan.net rsyslog.d]# systemctl restart rsyslog
[root@server.ngalacan.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd    1      TCP *:sunrpc (LISTEN)    root    261u    IPv4      55943
0t0
systemd    1      TCP *:sunrpc (LISTEN)    root    264u    IPv6      55961
0t0
cupsd      776    TCP localhost:ipp (LISTEN) root     6u     IPv6      20748
0t0
cupsd      776    TCP localhost:ipp (LISTEN) root     7u     IPv4      20749
0t0
httpd      874    21492 protocol: TCP      root     3u     sock      0,8
0t0
httpd      874    TCP *:http (LISTEN)      root     4u     IPv6      21493
0t0
httpd      874    21504 protocol: TCP      root     5u     sock      0,8
0t0
httpd      874    TCP *:https (LISTEN)     root     6u     IPv6      21505
0t0
```

Рис. 2.2: Перезапуск rsyslog и просмотр прослушиваемых портов

На сервере настраиваю межсетевой экран для работы с TCP-портом 514:

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

## 2.2 Настройка клиента сетевого журнала

На клиенте создаю файл конфигурации сетевого хранения журналов:

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

В данном файле включаю перенаправление сообщений журнала на 514 TCP-порт сервера и перезапускаю службу (рис. 2.3)

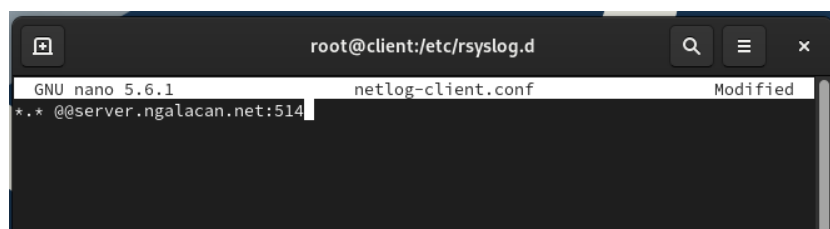


Рис. 2.3: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

## 2.3 Просмотр журнала

На сервере просматриваю один из файлов журнала. Обращаю внимание, что выводятся сообщения как с сервера, так и с клиента (рис. 2.4)

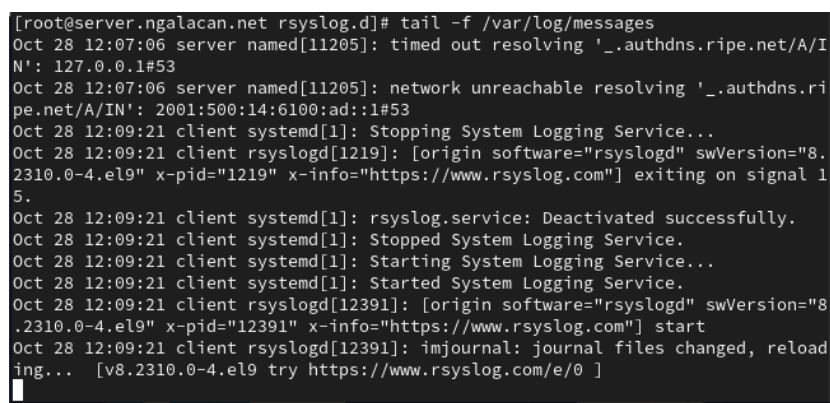


Рис. 2.4: Просмотр файла журнала на сервере

На сервере под пользователем ngalacan запускаю графическую программу для просмотра журналов (рис. 2.5).

Process Name	User	% CPU	ID	Memory	Disk read tot	Disk writ
at-spi2-registrd	ngalacan	0.00	10084	131.1 kB	10.2 MB	
at-spi-bus-launcher	ngalacan	0.00	10053	N/A	1.4 MB	
bash	ngalacan	0.00	51733	N/A	6.2 MB	
bash	ngalacan	0.00	51995	N/A	7.6 MB	4.0 MB
bash	ngalacan	0.00	53118	2.0 MB	10.9 MB	
dbus-broker	ngalacan	0.00	10022	1.0 MB	9.7 MB	
dbus-broker	ngalacan	0.00	10059	131.1 kB	1.5 MB	
dbus-broker-launch	ngalacan	0.00	10021	N/A	2.3 MB	
dbus-broker-launch	ngalacan	0.00	10058	N/A	8.2 kB	
dconf-service	ngalacan	0.00	10195	393.2 kB	1.3 MB	20.0 MB
evolution-addressbook-factory	ngalacan	0.00	10200	N/A	22.7 MB	36.0 MB
evolution-alarm-notify	ngalacan	0.00	10370	393.2 kB	12.1 MB	
evolution-calendar-factory	ngalacan	0.00	10183	N/A	2.4 MB	
evolution-source-registry	ngalacan	0.00	10159	N/A	5.1 MB	
file:/// Content	ngalacan	0.00	52385	1.2 MB	12.9 MB	
firefox	ngalacan	0.00	52252	58.3 MB	896.6 MB	62.8 MB
gjs	ngalacan	0.00	10283	53.2 kB	888.8 kB	

Рис. 2.5: Запуск графической программы для просмотра журналов

Устанавливаю просмотрщик журналов системных событий lnav:

```
dnf -y install lnav
```

Использую lnav для просмотра логов (рис. 2.6).

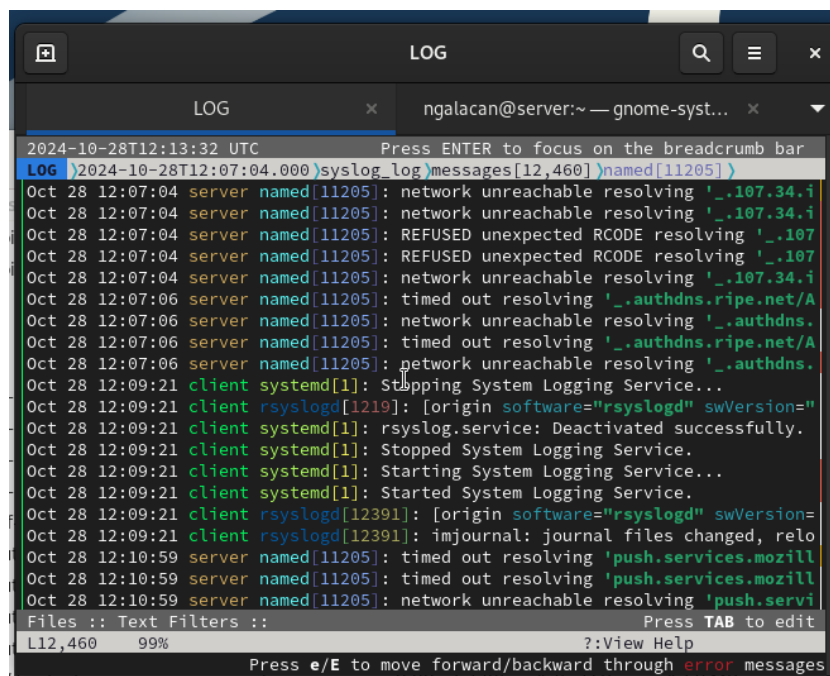


Рис. 2.6: Использование lnav для просмотра логов



## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копирую 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
```

Вношу изменения в файл `/vagrant/provision/server/netlog.sh` (рис. 2.7).

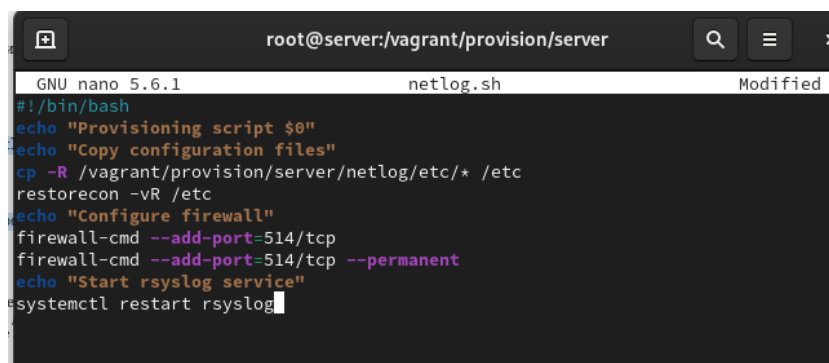
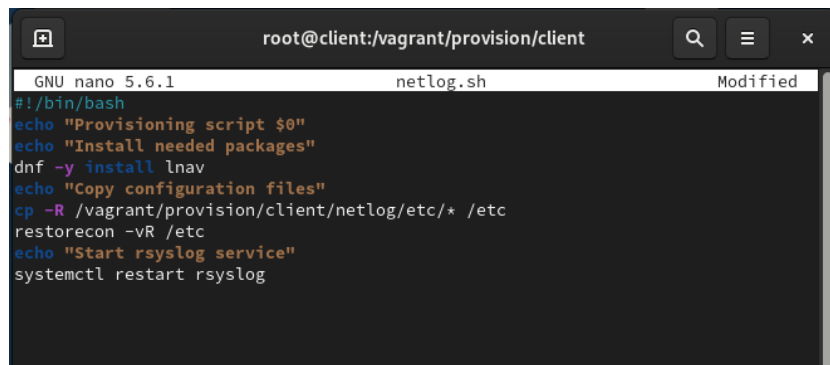


Рис. 2.7: Редактирование netlog.sh на сервере

На VM client перехожу в каталог для внесения изменений в настройки внутреннего окружения и копирую 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/
```

Создаю и редактирую скрипт /vagrant/provision/client/netlog.sh (рис. 2.8).



```
root@client:/vagrant/provision/client
GNU nano 5.6.1 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
```

Рис. 2.8: Редактирование netlog.sh на клиенте

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляю 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 результате выполнения работы были приобретены 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
```