

Отчет по лабораторной работе 15

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
5	Контрольные вопросы	11

Список иллюстраций

3.1	rsyslog	7
3.2	rsyslog	8
3.3	rsyslog	8
3.4	vagrant	9

Список таблиц

1 Цель работы

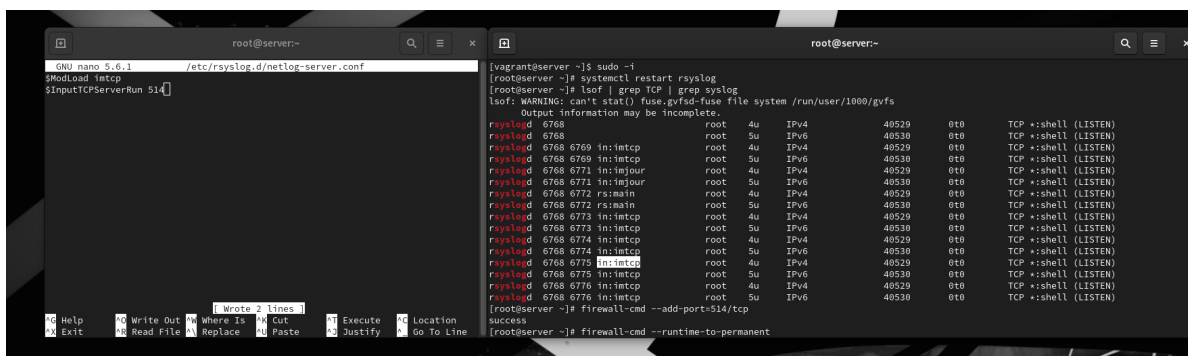
Получение навыков по работе с журналами системных событий.

2 Задание

1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере (см. раздел 15.4.2).
3. Просмотрите журналы системных событий с помощью нескольких программ (см. раздел 15.4.3). 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 (см. раздел 15.4.4).

3 Выполнение лабораторной работы

Сначала мы добавили файл в настройки rsyslog, который запускает сервер приема логов через IMTCP по порту 514. Затем мы перезагружаем rsyslog, и видим, что он открывает этот порт, поэтому мы добавляем его в firewalld.



```
root@server:~# nano /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514

[ vagrant@server ~]$ sudo -i
[root@server ~]# systemctl restart rsyslog
[root@server ~]# ss -tlnp | grep TCP | grep syslog
ss: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
rsyslogd 6768 root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6769 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6769 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6771 in:imjour root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6771 in:imjour root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6772 rs:main root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6772 rs:main root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6773 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6773 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6774 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6774 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6775 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6775 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6776 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6776 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
[root@server ~]# firewall-cmd --add-port=514/tcp
success
[root@server ~]# firewall-cmd --runtime-to-permanent
```

Рис. 3.1: rsyslog

После этого, на клиенте мы добавляем настройку, которая направляет все логи на сервер. После этого мы перезагружаем rsyslog, и сообщения об этом уже можно увидеть на сервере в /var/log/messages.

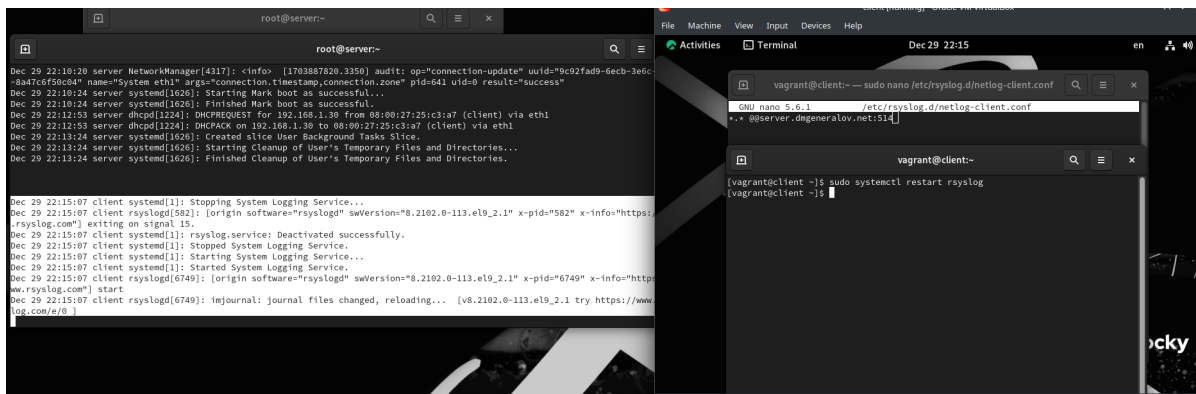


Рис. 3.2: rsyslog

Теперь сообщения системного лога на клиенте появляются как сообщения лога сервера, и их можно увидеть в Inav.

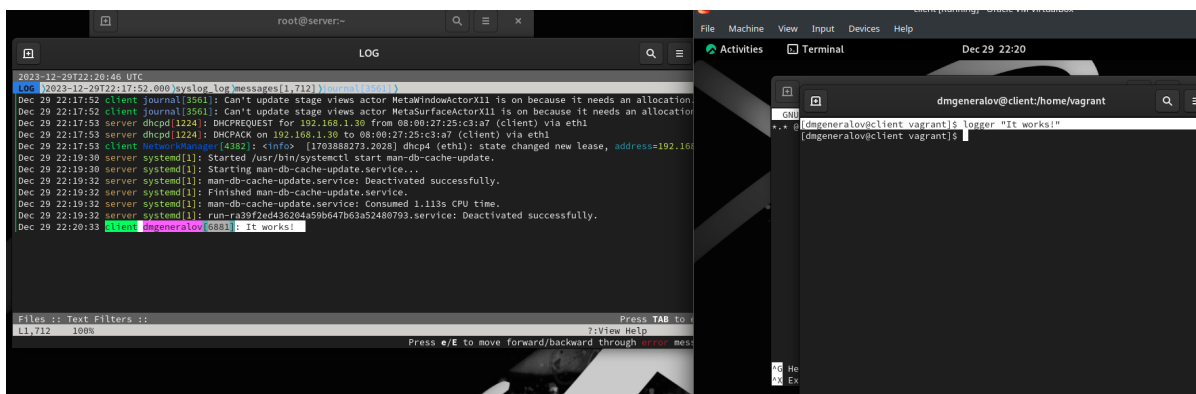


Рис. 3.3: rsyslog

Наконец мы экспортируем настройки в Vagrant.

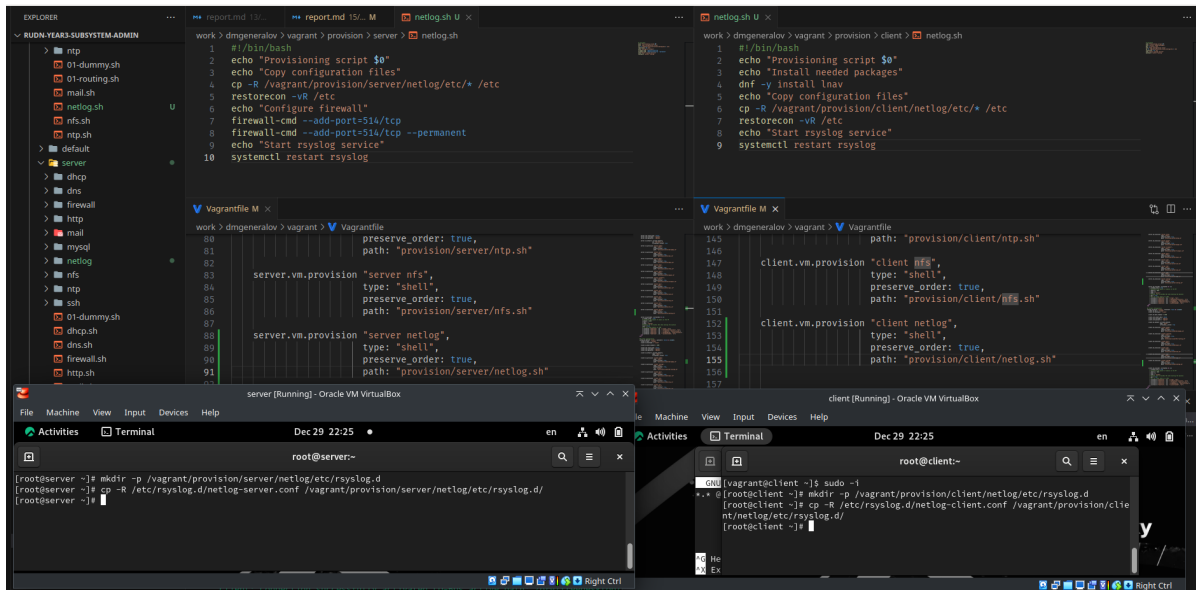


Рис. 3.4: vagrant

4 Выводы

Я получил опыт настройки службы сетевых логов rsyslog.

5 Контрольные вопросы

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

`imjournal`

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

???

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

???

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

`/etc/rsyslog.conf`

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

`module(load="imjournal")`

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

`imfile`

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

`ommysql`

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?

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