Администрирование сетевых подсистем

Лабораторная работа №15

Машков И. Е.

13 февраля 2026

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Машков Илья Евгеньевич
- Студент 3-го курса, группа НФИбд-02-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- https://github.com/7S7eVe7N7

Цель работы

Получение навыков по работе с журналами системных событий.

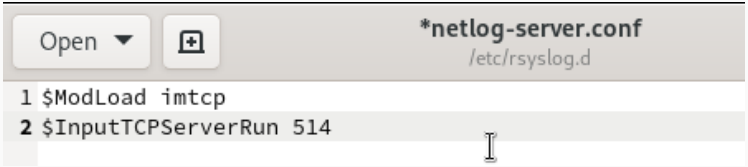

Рис. 1: Настройка приёма записей журнала по tcp:514

Выполнение лабораторной работы

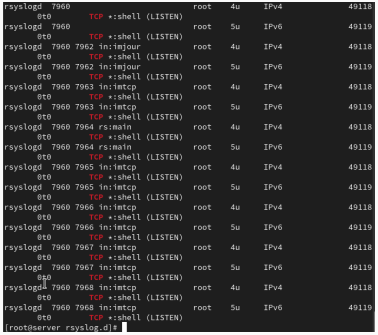

Рис. 2: Проверка прослушиваемых tcp портов

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

Рис. 3: Настройка межсетевого экрана на сервере

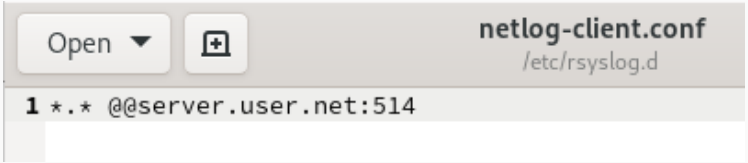

Рис. 4: netlog-client.conf на клиенте

Выполнение лабораторной работы

```
[root@server ~]# tail -f /var/log/messages
Feb 12 18:42:58 server named[981]: network unreachable resolving 'o.pki.goog/A
/IN': 2001:4860:4802:34::72#53
Feb 12 18:42:58 server named[981]: network unreachable resolving 'o.pki.goog/A
AAA/IN': 2001:4860:4802:34::72#53
Feb 12 18:42:58 server named[981]: network unreachable resolving 'o.pki.goog/A
/IN': 2001:4860:4802:38::72#53
Feb 12 18:42:58 server named[981]: network unreachable resolving 'o.pki.goog/A
AAA/IN': 2001:4860:4802:38::72#53
Feb 12 18:43:00 server named[981]: timed out resolving 'pki-goog.l.google.com/
A/IN': 192.168.1.1#53
Feb 12 18:43:00 server named[981]: timed out resolving 'pki-goog.l.google.com/
AAAA/IN': 192.168.1.1#53
Feb 12 18:45:16 server systemd[6708]: Started VTE child process 7979 launched
by gnome-terminal-server process 7501.
Feb 12 18:45:21 server systemd[1]: Starting Hostname Service...
Feb 12 18:45:21 server systemd[1]: Started Hostname Service.
Feb 12 18:45:51 server systemd[1]: systemd-hostnamed.service: Deactivated succ
essfully.
Feb 12 18:46:47 server gnome-shell[6844]: Window manager warning: Buggy client
 sent a _NET_ACTIVE_WINDOW message with a timestamp of 0 for 0x26000f8
```

Рис. 5: Лог файлов журнала

Выполнение лабораторной работы

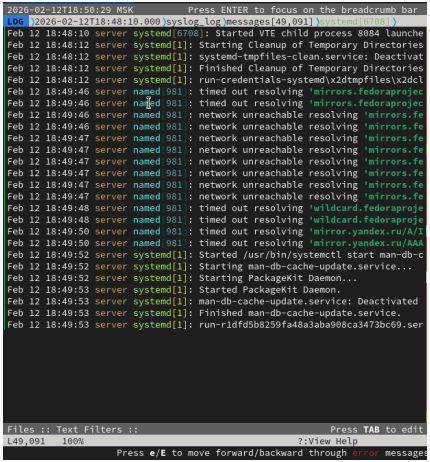

Рис. 6: Просмотр лога с помощью lnav

Выполнение лабораторной работы

Open

netlog.sh
/vagrant/provision/server

```
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/netlog/etc/* /etc
7  restorecon -vR /etc
8
9  echo "Configure firewall"
10 firewall-cmd --add-port=514/tcp
11 firewall-cmd --add-port=514/tcp --permanent
12
13 echo "Start rsyslog service"
14 systemctl restart rsyslog
```

Рис. 7: netlog.sh на server

Open

netlog.sh
/vagrant/provision/client

```
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Install needed packages"
6  dnf -y install lnav
7
8  echo "Copy configuration files"
9  cp -R /vagrant/provision/client/netlog/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start rsyslog service"
13 systemctl restart rsyslog
```

Рис. 8: netlog.sh на client

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

Рис. 9: Правки в Vagrantfile для server

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

Рис. 10: Правки в Vagrantfile для client

Выводы

В процессе выполнения данной лабораторной работы я освоил навыки по работе с журналами системных событий.