

Лабораторная работа №15

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Настройка сервера сетевого журнала	7
3.2 Настройка клиента сетевого журнала	8
3.3 Просмотр журнала	9
3.4 Внесение изменений в настройки внутреннего окружения виртуальных машин	12
4 Выводы	15
Список литературы	16

Список иллюстраций

3.1	Настройка приёма записей журнала по tcp:514	7
3.2	Проверка прослушиваемых tcp портов	8
3.3	Настройка межсетевого экрана на сервере	8
3.4	netlog-client.conf на клиенте	9
3.5	Лог файлов журнала	9
3.6	Просмотр журналов пользователя user	10
3.7	Установка lnav на сервер	11
3.8	Просмотр лого с помощью lnav	12
3.9	Настройки внутреннего окружения машины server	12
3.10	Настройки внутреннего окружения машины client	13
3.11	netlog.sh на server	13
3.12	netlog.sh на client	14
3.13	Правки в Vagrantfile для server	14
3.14	Правки в Vagrantfile для client	14

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

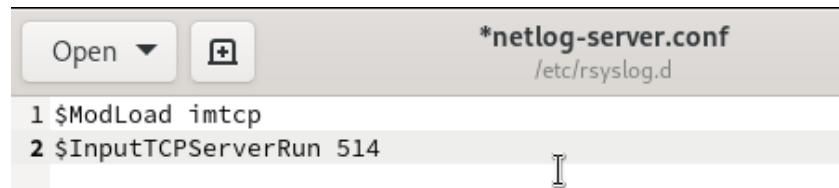
2 Задание

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотрите журналы системных событий с помощью нескольких программ. 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.

3 Выполнение лабораторной работы

3.1 Настройка сервера сетевого журнала

На сервере создаю файл конфигурации сетевого журнала. В конфигурационном файле включаю приём записей журнала по TCP-порту 514 (рис. [3.1]).



```
*netlog-server.conf  
/etc/rsyslog.d  
1 $ModLoad imtcp  
2 $InputTCPServerRun 514
```

Рис. 3.1: Настройка приёма записей журнала по tcp:514

Перезапускаю службу rsyslog и смотрю, что прослушиваются нужные нам порты (рис. [3.2]).

rsyslogd	7960	0t0	TCP	*:shell	(LISTEN)	root	4u	IPv4	49118
rsyslogd	7960	0t0	TCP	*:shell	(LISTEN)	root	5u	IPv6	49119
rsyslogd	7960	7962	in:imjour			root	4u	IPv4	49118
rsyslogd	7960	7962	in:imjour	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7963	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7963	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7964	rs:main	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7964	rs:main	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7965	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7965	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7966	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7966	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7967	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7967	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
rsyslogd	7960	7968	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv4	49118
rsyslogd	7960	7968	in:imtcp	0t0	TCP	*:shell	(LISTEN)	IPv6	49119
[root@server rsyslog.d]#									

Рис. 3.2: Проверка прослушиваемых tcp портов

Настраиваю межсетевой экран на работу с приёмом записей по tcp-порту 514 (рис. [3.3]).

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

Рис. 3.3: Настройка межсетевого экрана на сервере

3.2 Настройка клиента сетевого журнала

Создаю файл netlog-client.conf на клиенте и включаю перенаправление сообщений журнала на tcp-порт 514, т.е. на порт сервера (рис. [3.4]). После этого перезагружаю службу rsyslog.



Рис. 3.4: netlog-client.conf на клиенте

3.3 Просмотр журнала

Запускаю лог файлов журнала и просматриваю его(рис. [3.5]).

```
[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/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/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 successfully.
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. 3.5: Лог файлов журнала

Запускаю программу для просмотра журналов под пользователем user (рис. [3.6]).

	Processes	Resources	File Systems			
Process Name	User	% CPU	ID	Memory	Disk read tota	Disk wril
at-spi2-registryd	user	0.00	6808	786.4 kB	20.5 kB	
at-spi-bus-launcher	user	0.00	6776	917.5 kB	8.2 kB	
bash	user	0.00	7529	2.0 MB	282.6 kB	
bash	user	0.00	7979	1.8 MB	N/A	
bash	user	0.00	8084	2.0 MB	N/A	
dbus-broker	user	0.00	6738	1.8 MB	N/A	
dbus-broker	user	0.00	6782	262.1 kB	N/A	
dbus-broker-launch	user	0.00	6737	393.2 kB	N/A	
dbus-broker-launch	user	0.00	6781	262.1 kB	N/A	
dconf-service	user	0.00	6954	524.3 kB	81.9 kB	
evolution-addressbook-factory	user	0.00	6960	6.1 MB	3.5 MB	36
evolution-alarm-notify	user	0.00	7059	11.5 MB	1.4 MB	
evolution-calendar-factory	user	0.00	6923	9.2 MB	1.5 MB	
evolution-source-registry	user	0.00	6892	6.5 MB	2.9 MB	
file:/// Content	user	0.00	7644	16.4 MB	1.3 MB	
firefox	user	0.00	7409	229.7 MB	230.2 MB	32.1
gjs	user	0.00	7002	5.6 MB	45.1 kB	

Рис. 3.6: Просмотр журналов пользователя user

Устанавливаю Inav на сервер (рис. [3.7]).

```
[root@server rsyslog.d]# dnf -y install lnav
Last metadata expiration check: 1:56:38 ago on Thu 12 Feb 2026 04:53:07 PM MS
.
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          1.2 MB/s | 2.4 MB  00:02
-----
Total                                         421 kB/s | 2.4 MB  00:05

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@server rsyslog.d]#
```

Рис. 3.7: Установка lnav на сервер

С помощью lnav просматриваю логи (рис. [3.8]).

The screenshot shows a terminal window titled 'LOG' with a timestamp of '2026-02-12T18:48:10.000'. The log output is as follows:

```
2026-02-12T18:50:29 MSK      Press ENTER to focus on the breadcrumb bar
LOG )2026-02-12T18:48:10.000)syslog.log)messages[49,091] )systemd[6708] )
Feb 12 18:48:10 server systemd[6708]: Started VTE child process 8084 launche
Feb 12 18:48:12 server systemd[1]: Starting Cleanup of Temporary Directories
Feb 12 18:48:12 server systemd[1]: systemd-tmpfiles-clean.service: Deactivat
Feb 12 18:48:12 server systemd[1]: Finished Cleanup of Temporary Directories
Feb 12 18:48:12 server systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dcl
Feb 12 18:49:46 server named[981]: timed out resolving 'mirrors.fedoraprojec
Feb 12 18:49:46 server named[981]: timed out resolving 'mirrors.fedoraprojec
Feb 12 18:49:46 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:46 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:47 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:47 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:47 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:47 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:47 server named[981]: network unreachable resolving 'mirrors.fe
Feb 12 18:49:48 server named[981]: timed out resolving 'wildcard.fedoraproje
Feb 12 18:49:48 server named[981]: timed out resolving 'wildcard.fedoraproje
Feb 12 18:49:50 server named[981]: timed out resolving 'mirror.yandex.ru/A/I
Feb 12 18:49:50 server named[981]: timed out resolving 'mirror.yandex.ru/AAA
Feb 12 18:49:52 server systemd[1]: Started /usr/bin/systemctl start man-db-c
Feb 12 18:49:52 server systemd[1]: Starting man-db-cache-update.service...
Feb 12 18:49:52 server systemd[1]: Starting PackageKit Daemon...
Feb 12 18:49:53 server systemd[1]: Started PackageKit Daemon.
Feb 12 18:49:53 server systemd[1]: man-db-cache-update.service: Deactivated
Feb 12 18:49:53 server systemd[1]: Finished man-db-cache-update.service.
Feb 12 18:49:53 server systemd[1]: run-r1dfd5b8259fa48a3aba908ca3473bc69.ser
```

At the bottom of the terminal window, there is a status bar with the following information:

Files :: Text Filters :: Press TAB to edit
L49,091 100% ?:View Help
Press e/E to move forward/backward through error messages

Рис. 3.8: Просмотр лого с помощью lnav

3.4 Внесение изменений в настройки внутреннего окружения виртуальных машин

Вношу копии изменённых конфигов в файлы настройки внутреннего окружения машины server(рис. [3.9]) и client (рис. [3.10]).

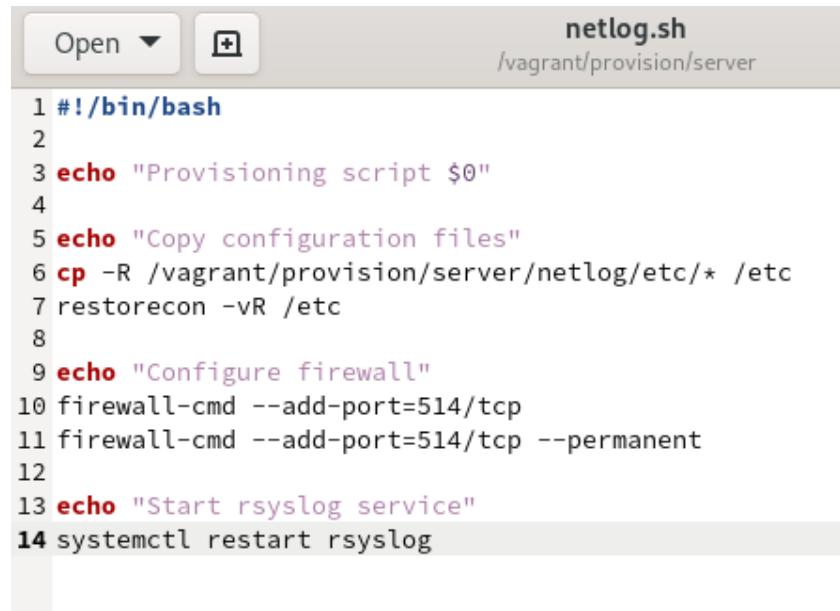
```
[root@server ~]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsy
slog.d
[root@server server]#
```

Рис. 3.9: Настройки внутреннего окружения машины server

```
[root@client rsyslog.d]# 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/
[root@client client]#
```

Рис. 3.10: Настройки внутреннего окружения машины client

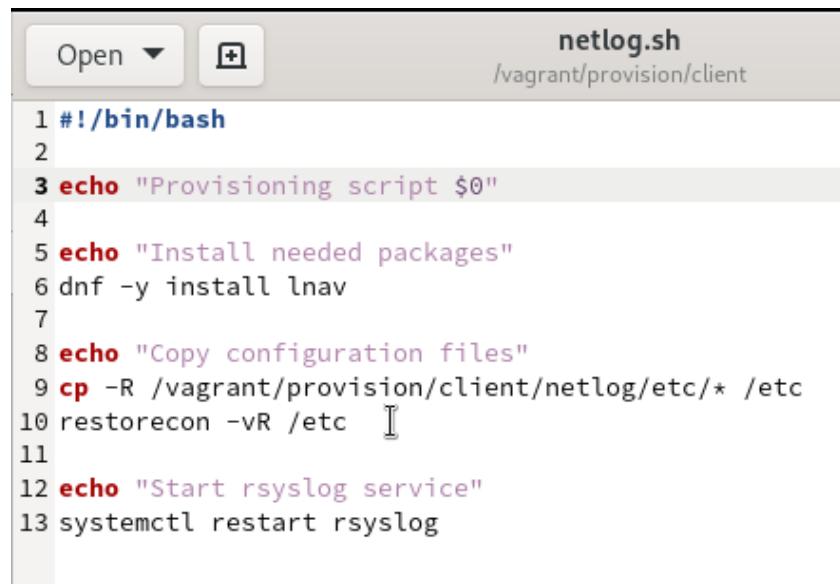
Затем создаю скрипт netlog.sh, который повторяет ключевые действия, совершенные на машине server (рис. [3.11]) и client (рис. [3.12]), при каждом запуске этих систем.



The screenshot shows a terminal window with the title "netlog.sh" and the path "/vagrant/provision/server". The window contains a bash script with the following code:

```
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. 3.11: netlog.sh на server



The screenshot shows a terminal window with the title bar "netlog.sh" and the path "/vagrant/provision/client". The script content is as follows:

```
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. 3.12: netlog.sh на client

Для отработки скрипта вношу соответствующие изменения в Vagrantfile для server (рис. [3.13]) и client (рис. [3.14]).

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

Рис. 3.13: Правки в Vagrantfile для server

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

Рис. 3.14: Правки в Vagrantfile для client

4 Выводы

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

Список литературы

Администрирование сетевых подсистем