

# **Лабораторная работа**

## **Номер 15**

Кобзев Д. К.  
Российский университет дружбы народов, Москва, Россия  
7 декабря 2025

## **Информация**

- ▶ Кобзев Дмитрий Константинович
- ▶ Студент
- ▶ Российский университет дружбы народов
- ▶ НПИбд-01-23

Целью данной работы является получение навыков по работе с журналами системных событий.

На сервере создаем файл конфигурации сетевого хранения журналов (Рис. 12.1).

```
[dkkobzev@server.dkkobzev.net ~]$ cd /etc/rsyslog.d
[dkkobzev@server.dkkobzev.net rsyslog.d]$ touch netlog-server.conf
touch: cannot touch 'netlog-server.conf': Permission denied
[dkkobzev@server.dkkobzev.net rsyslog.d]$ sudo -i
[sudo] password for dkkobzev:
[root@server.dkkobzev.net ~]# touch netlog-server.conf
```

**Рис. 1:** Создание файла конфигурации сетевого хранения журналов

В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включаем приём записей журнала по TCP-порту 514 (Рис. 12.2).



```
GNU nano 8.1 /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

**Рис. 2:** Файл конфигурации `/etc/rsyslog.d/netlog-server.conf`

## Настройка сервера сетевого журнала

Перезапускаем службу rsyslog и смотрим, какие порты, связанные с rsyslog, прослушиваются. На сервере настраиваем межсетевой экран для приёма сообщений по TCP-порту 514 (Рис. 12.3).

```
rsyslogd 13129          root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129          root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13131 in:imjour    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13131 in:imjour    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13132 in:imtcp    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13132 in:imtcp    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13133 in:imtcp    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13133 in:imtcp    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13134 in:imtcp    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13134 in:imtcp    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13135 in:imtcp    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13135 in:imtcp    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13136 in:imtcp    root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13136 in:imtcp    root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13137 rs:main     root    4u     IPv4          44519        0t0      TCP *:shell (LISTEN)
rsyslogd 13129 13137 rs:main     root    5u     IPv6          44520        0t0      TCP *:shell (LISTEN)
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp
success
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рис. 3: Настройка сервера сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов (Рис. 12.4).

```
[dkkobzev@client.dkkobzev.net ~]$ sudo -i  
[sudo] password for dkkobzev:  
[root@client.dkkobzev.net ~]# cd /etc/rsyslog.d  
[root@client.dkkobzev.net rsyslog.d]# touch netlog-client.conf
```

**Рис. 4:** Создание файла конфигурации сетевого хранения журналов



На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включаем перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 12.5).

A screenshot of a terminal window with a black background. The top bar of the nano editor shows 'GNU nano 8.1' on the left and 'netlog-client.conf' on the right. The main area of the terminal displays the configuration line '\*. \* @@server.dkkobzev.net:514' in a light blue monospaced font, with a white cursor at the end of the line.

```
GNU nano 8.1 netlog-client.conf
*. * @@server.dkkobzev.net:514
```

**Рис. 5:** Файл конфигурации `/etc/rsyslog.d/netlog-client.conf`

Перезапускаем службу rsyslog (Рис. 12.6).

A terminal window showing a root user at a client machine. The prompt is [root@client.dkkobzev.net rsyslog.d]#. The command systemctl restart rsyslog is entered.

```
[root@client.dkkobzev.net rsyslog.d]# systemctl restart rsyslog
```

**Рис. 6:** Перезапуск службы rsyslog

На сервере смотрим один из файлов журнала (Рис. 12.7).

```
[root@server.dkkobzev.net ~]# tail -f /var/log/messages
Dec  7 16:56:08 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec  7 16:56:08 server systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
Dec  7 16:56:57 client systemd[1]: Stopping rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[1447]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="1447" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec  7 16:56:57 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec  7 16:56:57 client systemd[1]: Stopped rsyslog.service - System Logging Service.
Dec  7 16:56:57 client systemd[1]: Starting rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[9941]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="9941" x-info="https://www.rsyslog.com"] start
Dec  7 16:56:57 client systemd[1]: Started rsyslog.service - System Logging Service.
Dec  7 16:56:57 client rsyslogd[9941]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Dec  7 16:57:41 server systemd[6406]: Started run-pl3552-113852.scope - [systemd-run] /usr/bin/bash.
Dec  7 16:58:10 client systemd[8440]: Created slice background.slice - User Background Tasks Slice.
Dec  7 16:58:10 client systemd[8440]: Starting systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directories...
Dec  7 16:58:10 client systemd[8440]: Finished systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directories.
```

Рис. 7: Один из файлов журнала

На сервере под пользователем user запускаем графическую программу для просмотра журналов (Рис. 12.8).

Processes										
Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total	Disk read	Disk write	Priority	
at-spi2-registryd	dkkobzev	0.00	9066	131.1 kB	987.1 kB	N/A	N/A	N/A	Normal	
at-spi-bus-launcher	dkkobzev	0.00	9017	N/A	716.8 kB	N/A	N/A	N/A	Normal	
bash	dkkobzev	0.00	12463	131.1 kB	25.7 MB	N/A	N/A	N/A	Normal	
bash	dkkobzev	0.00	13552	N/A	614.4 kB	N/A	N/A	N/A	Normal	
catatonit	dkkobzev	0.00	12378	N/A	725.0 kB	N/A	N/A	N/A	Normal	
dbus-broker	dkkobzev	0.17	8425	917.5 kB	4.2 MB	N/A	1.3 KiB/s	N/A	Normal	
dbus-broker	dkkobzev	0.00	9849	131.1 kB	626.7 kB	N/A	N/A	N/A	Normal	
dbus-broker-launch	dkkobzev	0.00	8485	N/A	1.3 MB	N/A	N/A	N/A	Normal	
dbus-broker-launch	dkkobzev	0.00	9048	131.1 kB	8.2 kB	N/A	N/A	N/A	Normal	
dconf-service	dkkobzev	0.35	9246	393.2 kB	1.7 MB	278.5 kB	N/A	56.0 KiB/s	Normal	
evolution-addressbook-factory	dkkobzev	0.00	9806	131.1 kB	2.4 MB	53.2 kB	N/A	N/A	Normal	
evolution-alarm-notify	dkkobzev	0.00	9376	393.2 kB	6.0 MB	N/A	N/A	N/A	Normal	
evolution-calendar-factory	dkkobzev	0.00	9693	131.1 kB	4.5 MB	N/A	N/A	N/A	Normal	
evolution-source-registry	dkkobzev	0.00	9277	131.1 kB	2.2 MB	N/A	N/A	N/A	Normal	
firefox	dkkobzev	0.52	11203	170.2 MB	2.3 GB	170.8 MB	94.7 KiB/s	52.0 KiB/s	Normal	
firefox	dkkobzev	0.00	22091	3.0 MB	57.7 MB	N/A	N/A	N/A	Normal	
gdm-wayland-session	dkkobzev	0.00	8393	N/A	12.3 kB	N/A	N/A	N/A	Normal	
gjs	dkkobzev	0.00	9315	41.0 kB	3.5 MB	N/A	N/A	N/A	Normal	
gjs	dkkobzev	0.00	9681	77.8 kB	3.4 MB	N/A	N/A	N/A	Normal	
gnome-keyring-daemon	dkkobzev	0.00	6561	192.5 kB	6.1 MB	4.1 kB	N/A	N/A	Normal	
gnome-session-binary	dkkobzev	0.00	8431	N/A	90.1 kB	N/A	N/A	N/A	Normal	
gnome-session-binary	dkkobzev	0.00	8584	262.1 kB	4.8 MB	4.1 kB	N/A	N/A	Normal	
gnome-session-ctl	dkkobzev	0.00	8579	N/A	24.6 kB	N/A	N/A	N/A	Normal	
gnome-shell	dkkobzev	0.51	8658	148.7 MB	956.7 MB	176.1 kB	4.0 MiB/s	N/A	Normal	
gnome-shell-calendar-server	dkkobzev	0.00	9228	131.1 kB	8.9 MB	N/A	N/A	N/A	Normal	
gnome-software	dkkobzev	0.00	9480	2.6 MB	122.1 MB	N/A	N/A	N/A	Normal	
gnome-system-monitor	dkkobzev	23.78	13581	92.1 MB	216.4 MB	65.5 kB	1.4 MiB/s	5.3 KiB/s	Normal	
gpa-daemon	dkkobzev	0.00	9502	131.1 kB	667.6 kB	N/A	N/A	N/A	Normal	
gpa-identity-service	dkkobzev	0.00	9703	262.1 kB	774.1 kB	N/A	N/A	N/A	Normal	
gsd-atty-settings	dkkobzev	0.00	9321	N/A	8.2 kB	N/A	N/A	N/A	Normal	
gsd-color	dkkobzev	0.00	9325	393.2 kB	2.1 MB	N/A	N/A	N/A	Normal	

Рис. 8: Графическая программа для просмотра журналов

Просмотрите логи с сервера с помощью Inav (Рис. 12.9).

```
2025-12-07T17:10:55.000 syslog.log : messages[205] : systemd[6400] :
Dec 07 17:10:59 server tracker-miner-fs-3.service: Main process exited, code=exit, status=1/FAILURE
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 1.
Dec 07 17:10:59 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server tracker-miner-fs-3.service: Could not create store: Database version is too old: got version 0, but 29 is a
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exit, status=1/FAILURE
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 2.
Dec 07 17:10:59 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server tracker-miner-fs-3.service: Could not create store: Database version is too old: got version 0, but 29 is a
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exit, status=1/FAILURE
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 3.
Dec 07 17:10:59 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server tracker-miner-fs-3.service: Could not create store: Database version is too old: got version 0, but 29 is a
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exit, status=1/FAILURE
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 4.
Dec 07 17:10:59 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server tracker-miner-fs-3.service: Could not create store: Database version is too old: got version 0, but 29 is a
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exit, status=1/FAILURE
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 5.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Start request repeated too quickly.
Dec 07 17:10:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:10:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:11:00 server systemctl[1000]: Unable to create connection for session with Tracker indexes: Could not activate reus
Dec 07 17:11:02 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service.
Dec 07 17:11:02 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 07 17:11:03 server gnome-shell[1000]: Window manager warning: last_focus_time (17053007) is greater than comparison time
Dec 07 17:11:04 server systemd[1000]: 2025-12-07 17:11:04.000+0000: no interface given, using all interfaces
Dec 07 17:11:13 server Firefox.desktop[1000]: Crash Annotation GraphicsCriticalError: [GFX]GFX-1: Managed to allocate after
Dec 07 17:11:23 server systemd[1]: packagekit.service: Deactivated successfully.
Dec 07 17:11:23 server systemd[1]: packagekit.service: Consumed 30.42% CPU time, 500.3M memory peak, 232.0M memory swap peak.
Dec 07 17:11:23 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 07 17:11:27 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service.
Dec 07 17:11:27 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 07 17:12:07 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 07 17:12:25 server systemd[6400]: Started run-p08040-120740.scope - [systemd-run] run/bin/bush.
Dec 07 17:12:41 server systemd[6400]: Started run-p08753-121001.scope - [systemd-run] run/bin/bush.
Dec 07 17:13:56 server systemd[1]: Starting packagekit.service - PackageKit Daemon.
Dec 07 17:13:57 server systemd[1]: Started packagekit.service - PackageKit Daemon.
Dec 07 17:13:59 server systemd[6400]: dbus-1.2-esp.gnome.Nautilus.service: Consumed 3.854s CPU time, 277.0M memory peak, 16
Dec 07 17:14:12 server systemd[1]: Starting plocate-updatedb.service - Update the plocate database.
Dec 07 17:14:15 server systemd[1]: plocate-updatedb.service: Deactivated successfully.
```

Рис. 9: Логи с сервера

Просмотрите логи с клиента с помощью `lnav` (Рис. 12.10).

```
2025-12-07T17:33:03 UTC Press F2 to enable mouse support
Dec 07 17:27:12 client systemd[1]: Started session-c6.scope - Session c6 of User root.
Dec 07 17:27:12 client systemd-logind[907]: Session c6 logged out. Waiting for processes to exit.
Dec 07 17:27:12 client systemd[1]: session-c6.scope: Deactivated successfully.
Dec 07 17:27:12 client systemd-logind[907]: Removed session c6.
Dec 07 17:27:15 client systemd[1]: packagekit.service: Deactivated successfully.
Dec 07 17:28:17 client pipewire[8064]: pa.node: (auto,null-35) graph xrun not-triggered (2 suppressed)
Dec 07 17:28:17 client pipewire[8064]: pa.node: (auto,null-35) xrun state:0x7f3295ad1000 pending:0/2 s:2481759130965 a:24817592311
Dec 07 17:28:35 client pipewire[8064]: pa.node: (auto,null-35) graph xrun not-triggered (0 suppressed)
Dec 07 17:28:35 client pipewire[8064]: pa.node: (auto,null-35) xrun state:0x7f3295ad1000 pending:0/2 s:2499714883926 a:24997150720
Dec 07 17:29:23 client systemd-logind[907]: Existing logind session ID 5 used by new audit session, ignoring.
Dec 07 17:29:23 client systemd-logind[907]: New session c7 of user root.
Dec 07 17:29:23 client systemd[1]: Started session-c7.scope - Session c7 of User root.
Dec 07 17:29:23 client systemd-logind[907]: Session c7 logged out. Waiting for processes to exit.
Dec 07 17:29:23 client systemd[1]: session-c7.scope: Deactivated successfully.
Dec 07 17:29:23 client systemd-logind[907]: Removed session c7.
Dec 07 17:30:00 client systemd[1]: Starting plocate-updatedb.service - Update the plocate database...
Dec 07 17:30:04 client systemd[1]: plocate-updatedb.service: Deactivated successfully.
Dec 07 17:30:04 client systemd[1]: Finished plocate-updatedb.service - Update the plocate database.
Dec 07 17:30:04 client systemd[1]: plocate-updatedb.service: Consumed 1.291s CPU time, 184.9M memory peak.
Dec 07 17:31:00 client systemd[1]: Starting dnf-makecache.service - dnf makecache...
Dec 07 17:31:02 client dnf[11176]: Extra Packages for Enterprise Linux 10 - x86_64 35 kB/s | 37 kB 00:01
Dec 07 17:31:04 client dnf[11176]: Rocky Linux 10 - BaseOS 3.2 kB/s | 4.3 kB 00:01
Dec 07 17:31:04 client dnf[11176]: Rocky Linux 10 - AppStream 12 kB/s | 4.3 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Rocky Linux 10 - CRB 12 kB/s | 4.3 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Rocky Linux 10 - Extras 9.2 kB/s | 3.1 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Metadata cache created.
Dec 07 17:31:05 client systemd[1]: dnf-makecache.service: Deactivated successfully.
Dec 07 17:31:05 client systemd[1]: Finished dnf-makecache.service - dnf makecache.
Dec 07 17:31:05 client systemd[1]: dnf-makecache.service: Consumed 999ms CPU time, 134.9M memory peak.
Dec 07 17:32:00 client systemd-logind[907]: Existing logind session ID 5 used by new audit session, ignoring.
Dec 07 17:32:09 client systemd-logind[907]: New session c8 of user root.
Dec 07 17:32:09 client systemd[1]: Started session-c8.scope - Session c8 of User root.
Dec 07 17:32:09 client systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Dec 07 17:32:09 client systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 07 17:32:15 client systemd[6448]: run-p1070-11802.scope: Consumed 1.807s CPU time, 119.3M memory peak, 1.9M memory swap peak
Dec 07 17:32:15 client systemd[1]: session-c8.scope: Deactivated successfully.
Dec 07 17:32:15 client systemd-logind[907]: Session c8 logged out. Waiting for processes to exit.
Dec 07 17:32:15 client systemd-logind[907]: Removed session c8.
Dec 07 17:32:19 client systemd[6448]: app-gnome-firefox-10117.scope: Consumed 2min 18.782s CPU time, 868.3M memory peak, 302.6M me
Dec 07 17:32:39 client systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 07 17:32:53 client systemd[1]: session-c3.scope: Deactivated successfully.
Dec 07 17:32:53 client systemd-logind[907]: Session c3 logged out. Waiting for processes to exit.
Dec 07 17:32:53 client systemd-logind[907]: Removed session c3.
```

Рис. 10: Логи с клиента

На виртуальной машине `server` переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создаем в нём каталог `netlog`, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/server` создаем файл `netlog.sh` (Рис. 12.11).

```
[root@server.dkkobzev.net ~]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf
cp: missing destination file operand after '/etc/rsyslog.d/netlog-server.conf'
Try 'cp --help' for more information.
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# touch netlog.sh
[root@server.dkkobzev.net server]# chmod +x netlog.sh
```

**Рис. 11:** Внесение изменений в настройки внутреннего окружения виртуальной машины

Прописываем скрипт в netlog.sh (Рис. 12.12).



```
GNU nano 8.1 netlog.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 12: Файл netlog.sh



На виртуальной машине client переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создаем в нём каталог netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создаем файл netlog.sh (Рис. 12.13).

```
[root@client.dkkobzev.net rsyslog.d]# cd /vagrant/provision/client
[root@client.dkkobzev.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.dkkobzev.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.dkkobzev.net client]# cd /vagrant/provision/client
[root@client.dkkobzev.net client]# touch netlog.sh
[root@client.dkkobzev.net client]# chmod +x netlog.sh
```

**Рис. 13:** Внесение изменений в настройки внутреннего окружения виртуальной машины

Прописываем скрипт в netlog.sh (Рис. 12.14).

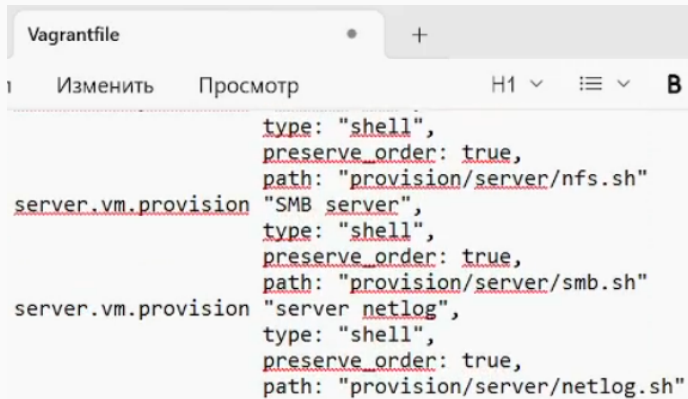


```
GNU nano 8.1 netlog.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install lnav
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 14: Файл netlog.sh

## Внесение изменений в настройки внутреннего окружения виртуальных машин

Для отработки созданного скрипта во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервера и клиент (Рис. 12.15), (Рис. 12.16).

The image shows a code editor window titled 'Vagrantfile'. It has a tab bar with a '+' icon and a toolbar with buttons for 'Изменить' (Edit), 'Просмотр' (View), a zoom level of 'H1', a menu icon, and a 'B' button. The code is written in a monospaced font and includes syntax highlighting. It defines three provision scripts for a VM named 'server'.

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

Рис. 15: Vagrantfile

## Внесение изменений в настройки внутреннего окружения виртуальных машин

```

client.vm.network :private_network,
  ip: "192.168.1.2",
  virtualbox____intnet: true

client.vm.provider :virtualbox do |virtualbox|
  virtualbox.customize ["__mod__vm__", :id, "--vrdm", "on"]
  virtualbox.customize ["__mod__vm__", :id, "--vrdmport",
end

client.vm.provision "client dummy",
  type: "shell",
  preserve_order: true,
  path: "provision/client/01-dummy.sh"

client.vm.provision "client routing",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/01-routing"

client.vm.provision "client mail",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/mail.sh"

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

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

client.vm.provision "SMB client",
  type: "shell",
  preserve_order: true,
  path: "provision/client/smb.sh"

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

```

**Рис. 16:** Vagrantfile

В результате выполнения лабораторной работы мною были получены навыки по работе с журналами системных событий.