

Лабораторная работа №15

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

1 1. Цель работы

2 2. Выполнение лабораторной работы

3 3. Выводы

Раздел 1

1. Цель работы

1.1 Цель работы

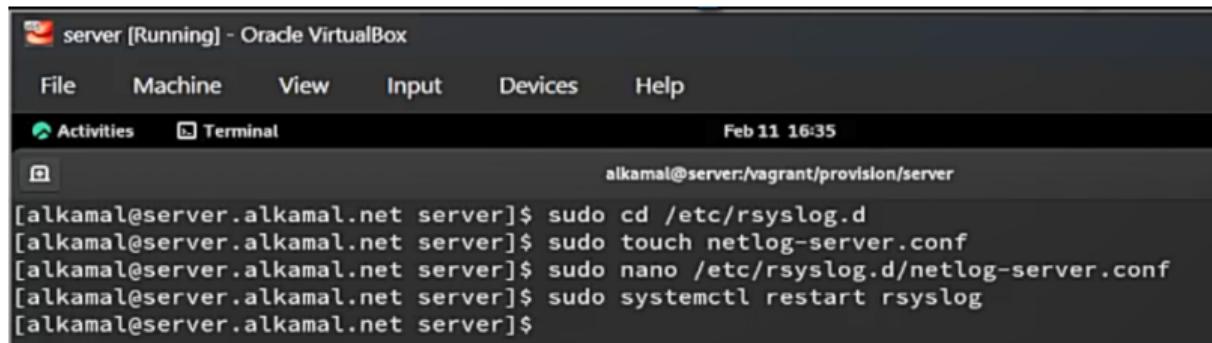
- Получение навыков по работе с журналами системных событий

Раздел 2

2. Выполнение лабораторной работы

2.1 Настройка сервера сетевого журнала

- Переход в каталог /etc/rsyslog.d
- Создание файла netlog-server.conf
- Подготовка конфигурации для сетевого хранения журналов



```
[alkamal@server.alkamal.net server]$ sudo cd /etc/rsyslog.d
[alkamal@server.alkamal.net server]$ sudo touch netlog-server.conf
[alkamal@server.alkamal.net server]$ sudo nano /etc/rsyslog.d/netlog-server.conf
[alkamal@server.alkamal.net server]$ sudo systemctl restart rsyslog
[alkamal@server.alkamal.net server]$
```

Рисунок 1: Создание файла конфигурации rsyslog netlog-server.conf

- Включён приём журналов по TCP-порту 514
- Загружен модуль `imtcp`
- Активирован сервер ввода `$InputTCPServerRun 514`

The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has a dark theme with white text. The terminal interface includes a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a toolbar with "Activities" and "Terminal" buttons. The status bar at the bottom right shows the date and time: "Feb 11 16:35". The main terminal area displays the following command being run:

```
alkamal@server:/vagrant/provision/server -- sudo nano /etc/rsyslog.d/netlog-server.conf
GNU nano 5.6.1
/etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рисунок 2: Настройка приёма журналов по TCP 514 в rsyslog

- Перезапущена служба rsyslog
- Выполнена проверка портов командой lsof | grep TCP
- Подтверждено состояние LISTEN для rsyslog

```
COMMANDS: status tasks kill stop start stopnow startnow restart
rsyslogd 8610                           root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610                           root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8613 in:imjour          root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8613 in:imjour          root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8614 in:imtcp           root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8614 in:imtcp           root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8619 w0/imtcp          root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8619 w0/imtcp          root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8620 w1/imtcp          root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8620 w1/imtcp          root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8621 rs:main           root  4u   IPv4          58273    0t0      TCP *:sh
ell (LISTEN)
rsyslogd 8610 8621 rs:main           root  5u   IPv6          58274    0t0      TCP *:sh
ell (LISTEN)
[alkamal@server.alkamal.net server]$
```

Рисунок 3: Проверка прослушиваемых TCP-портов службой rsyslog

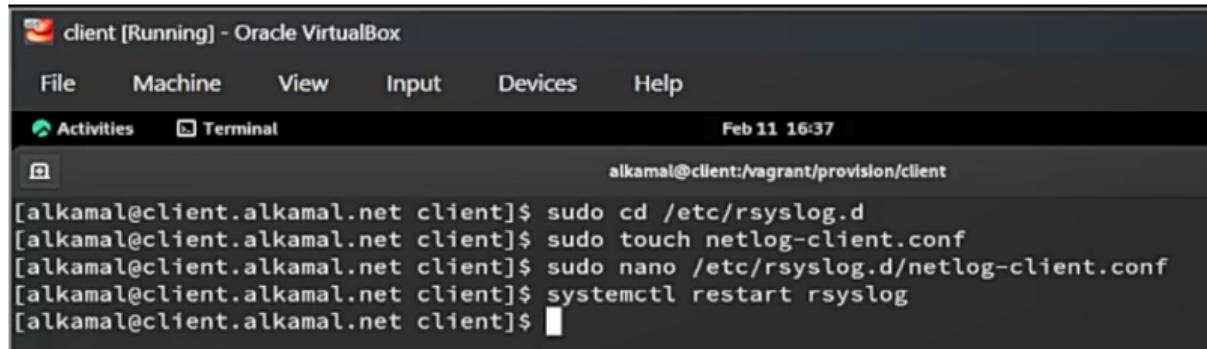
- Открыт TCP-порт 514 в firewalld
- Добавлено временное и постоянное правило
- Разрешён приём сетевых сообщений журнала

```
[alkamal@server.alkamal.net server]$ firewall-cmd --add-port=514/tcp
success
[alkamal@server.alkamal.net server]$ sudo firewall-cmd --add-port=514/tcp --permanent
success
[alkamal@server.alkamal.net server]$ █
```

Рисунок 4: Настройка firewalld для открытия TCP-порта 514

2.2 Настройка клиента сетевого журнала

- Переход в каталог /etc/rsyslog.d
- Создание файла netlog-client.conf
- Подготовка конфигурации отправки журналов



The screenshot shows a terminal window titled "client [Running] - Oracle VirtualBox". The window has a dark theme with white text. At the top, there is a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a toolbar with "Activities" and "Terminal" buttons. The status bar at the bottom shows the date and time: "Feb 11 16:37". The main area of the terminal shows the following command history:

```
[alkamal@client.alkamal.net client]$ sudo cd /etc/rsyslog.d  
[alkamal@client.alkamal.net client]$ sudo touch netlog-client.conf  
[alkamal@client.alkamal.net client]$ sudo nano /etc/rsyslog.d/netlog-client.conf  
[alkamal@client.alkamal.net client]$ systemctl restart rsyslog  
[alkamal@client.alkamal.net client]$ █
```

Рисунок 5: Создание файла конфигурации netlog-client.conf на клиенте

- Настроено перенаправление *.* @@server.alkamal.net:514
- Использован протокол TCP (@@)
- Организована передача всех сообщений на сервер
- Перезапущена служба rsyslog
- Применена новая конфигурация клиента

The screenshot shows a terminal window with the following content:

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:37
alkamal@client:/vagrant/provision/client — sudo nano /etc/rsyslog.d/netlog-client.conf
GNU nano 5.6.1 /etc/rsyslog.d/netlog-client.conf
*.* @@server.alkamal.net:514
```

Рисунок 6: Настройка перенаправления журналов на сервер по TCP 514

2.3 Просмотр журнала

- Выполнен просмотр /var/log/messages с помощью tail -f
- Отображаются записи server и client
- Подтверждён приём удалённых журналов

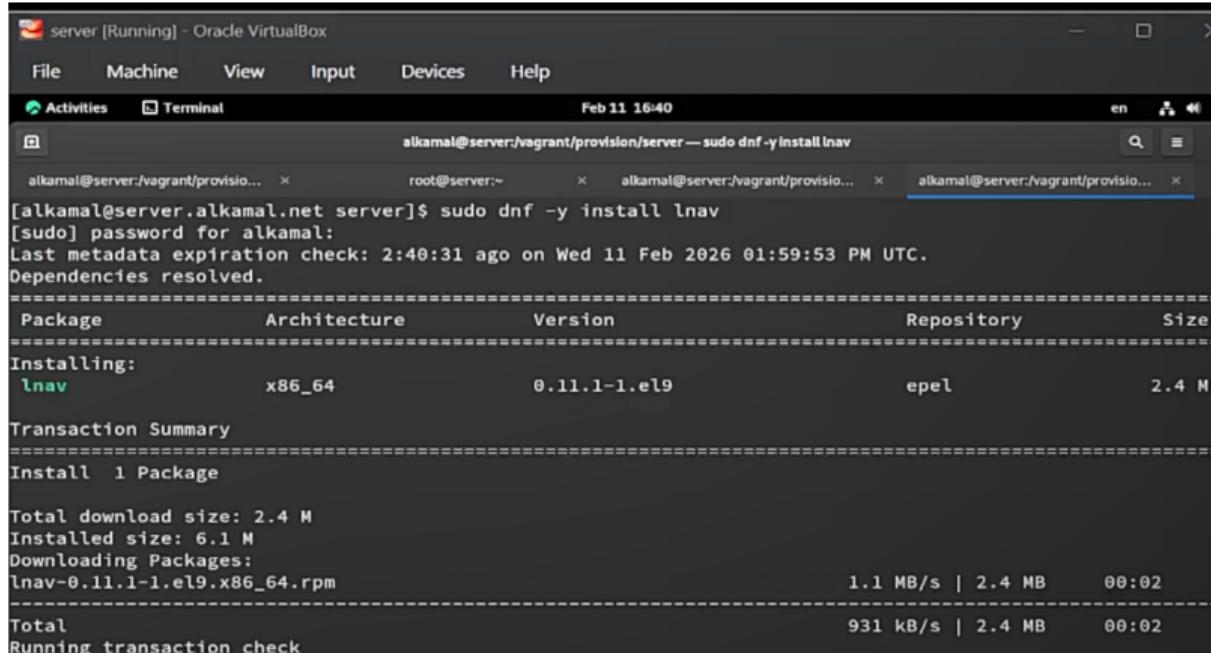
```
[sudo] password for alkamal:  
[root@server.alkamal.net ~]# tail -f /var/log/messages  
Feb 11 16:37:25 client rsyslogd[1020]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="1020" x-info="https://www.rsyslog.com"] exiting on signal 15.  
Feb 11 16:37:25 client systemd[1]: rsyslog.service: Deactivated successfully.  
Feb 11 16:37:25 client systemd[1]: Stopped System Logging Service.  
Feb 11 16:37:25 client systemd[1]: Starting System Logging Service...  
Feb 11 16:37:25 client systemd[1]: Started System Logging Service.  
Feb 11 16:37:25 client rsyslogd[5815]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="5815" x-info="https://www.rsyslog.com"] start  
Feb 11 16:37:25 client rsyslogd[5815]: imjournal: journal files changed, reloading... [v8.2506.0-2.el9 try https://www.rsyslog.com/e/0 ]  
Feb 11 16:37:33 server systemd[7431]: Started VTE child process 8693 launched by gnome-terminal-server process 8192.  
Feb 11 16:38:01 server systemd[1]: Starting Hostname Service...  
Feb 11 16:38:01 server systemd[1]: Started Hostname Service.
```

Рисунок 7: Просмотр журнала /var/log/messages на сервере

- Запущена программа gnome-system-monitor
- Отображены процессы, PID, использование CPU и памяти

| Process Name | User | % CPU | ID | Memory | Disk read tot | Disk write tot | Disk read | Disk write | Priority |
|-------------------------------|---------|-------|------|----------|---------------|----------------|-----------|------------|----------|
| at-spl2-registryd | alkamal | 0.00 | 7569 | 258.0 kB | 475.1 kB | N/A | N/A | N/A | Normal |
| at-spl-bus-launcher | alkamal | 0.00 | 7537 | 4.1 kB | 815.1 kB | N/A | N/A | N/A | Normal |
| bash | alkamal | 0.00 | 8211 | 532.5 kB | 53.9 MB | 77.8 kB | N/A | N/A | Normal |
| bash | alkamal | 0.00 | 8693 | 2.0 kB | 8.2 MB | N/A | N/A | N/A | Normal |
| bash | alkamal | 0.00 | 8767 | 2.0 kB | 16.4 kB | N/A | N/A | N/A | Normal |
| dbus-broker | alkamal | 0.00 | 7460 | 1.2 kB | 2.0 MB | N/A | N/A | N/A | Normal |
| dbus-broker | alkamal | 0.00 | 7543 | 184.3 kB | 356.4 kB | N/A | N/A | N/A | Normal |
| dbus-broker-launch | alkamal | 0.00 | 7459 | 4.1 kB | 761.9 kB | N/A | N/A | N/A | Normal |
| dbus-broker-launch | alkamal | 0.00 | 7542 | 4.1 kB | 8.2 kB | N/A | N/A | N/A | Normal |
| dconf-service | alkamal | 0.00 | 7674 | 421.9 kB | 557.1 kB | 16.4 kB | N/A | 1.3 kB/s | Normal |
| evolution-addressbook-factory | alkamal | 0.00 | 7680 | 4.1 kB | 5.4 MB | 36.9 kB | N/A | N/A | Normal |
| evolution-alarm-notify | alkamal | 0.00 | 7784 | 1.2 MB | 6.6 MB | N/A | N/A | N/A | Normal |
| evolution-calendar-factory | alkamat | 0.00 | 7653 | 4.1 kB | 2.5 MB | N/A | N/A | N/A | Normal |
| evolution-source-registry | alkamat | 0.00 | 7640 | 4.1 kB | 3.0 MB | N/A | N/A | N/A | Normal |
| gjs | alkamat | 0.00 | 7762 | 4.1 kB | 4.3 MB | N/A | N/A | N/A | Normal |
| gjs | alkamat | 0.00 | 7896 | 4.1 kB | 3.8 MB | N/A | N/A | N/A | Normal |
| gnome-keyring-daemon | alkamat | 0.00 | 7448 | 438.3 kB | N/A | N/A | N/A | N/A | Normal |
| gnome-session-binary | alkamat | 0.00 | 7451 | 4.1 kB | 13.3 MB | 4.1 kB | N/A | N/A | Normal |
| gnome-session-binary | alkamat | 0.00 | 7585 | 929.8 kB | 7.9 MB | 4.1 kB | N/A | N/A | Normal |
| gnome-session-ctl | alkamat | 0.00 | 7583 | 4.1 kB | 24.6 kB | N/A | N/A | N/A | Normal |
| gnome-shell | alkamat | 18.92 | 7603 | 122.9 MB | 397.8 MB | 20.5 kB | 37.3 kB/s | N/A | Normal |
| gnome-shell-calendar-server | alkamat | 0.00 | 7627 | 4.1 kB | 6.4 MB | N/A | N/A | N/A | Normal |
| gnome-software | alkamat | 0.00 | 7790 | 15.7 MB | 75.6 MB | N/A | N/A | N/A | Normal |
| gnome-system-monitor | alkamat | 2.70 | 8798 | 13.9 MB | 24.5 MB | N/A | N/A | N/A | Normal |
| gnome-terminal-server | alkamat | 1.54 | 8192 | 9.0 MB | 28.5 MB | 12.3 kB | 4.0 kB/s | N/A | Normal |
| goa-daemon | alkamat | 0.00 | 7649 | 8.2 kB | 671.7 kB | N/A | N/A | N/A | Normal |
| goa-identity-service | alkamat | 0.00 | 7662 | 319.5 kB | 1.3 MB | N/A | N/A | N/A | Normal |
| gsd-a11y-settings | alkamat | 0.00 | 7774 | 4.1 kB | 524.3 kB | N/A | N/A | N/A | Normal |
| gsd-color | alkamat | 0.00 | 7775 | 3.6 MB | 7.3 MB | N/A | N/A | N/A | Normal |
| gsd-datetime | alkamat | 0.00 | 7781 | 4.1 kB | 1.4 MB | N/A | N/A | N/A | Normal |
| gsd-disk-utility-notify | alkamat | 0.00 | 7794 | 4.1 kB | 634.9 kB | N/A | N/A | N/A | Normal |
| gsd-housekeeping | alkamat | 0.00 | 7785 | 458.8 kB | 1.3 MB | N/A | N/A | N/A | Normal |
| gsd-keyboard | alkamat | 0.00 | 7789 | 1.3 MB | 3.9 MB | N/A | N/A | N/A | Normal |
| gsd-media-keys | alkamat | 0.00 | 7791 | 1.7 MB | 3.6 MB | N/A | N/A | N/A | Normal |
| gsd-power | alkamat | 0.00 | 7792 | 1.7 MB | 5.6 MB | N/A | N/A | N/A | Normal |
| gsd-printer | alkamat | 0.00 | 7912 | 557.1 kB | 806.9 kB | N/A | N/A | N/A | Normal |
| gsd-print-notifications | alkamat | 0.00 | 7793 | 4.1 kB | 1.2 MB | N/A | N/A | N/A | Normal |
| gsd-rkill | alkamat | 0.00 | 7795 | 4.1 kB | 237.6 kB | N/A | N/A | N/A | Normal |
| gsd-screensaver-proxy | alkamat | 0.00 | 7798 | 4.1 kB | 487.4 kB | N/A | N/A | N/A | Normal |

- Установлен пакет `lnav` через `dnf`
- Подтверждена успешная установка версии `0.11.1-1.el9`



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has tabs for "Activities" and "Terminal". The terminal session is running under user "alkamal" and root. The command entered is `sudo dnf -y install lnav`. The output shows the package being installed from the "epel" repository. The transaction summary indicates 1 package will be installed, totaling 2.4 MB download size and 6.1 MB installed size. The download progress bar shows 1.1 MB/s speed, 2.4 MB total, and 00:02 remaining. A note at the bottom says "Running transaction check".

```
alkamal@server:/vagrant/provision/server — sudo dnf -y install lnav
[sudo] password for alkamal:
Last metadata expiration check: 2:40:31 ago on Wed 11 Feb 2026 01:59:53 PM UTC.
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          1.1 MB/s | 2.4 MB    00:02
=====
Total                                         931 kB/s | 2.4 MB    00:02
Running transaction check
```

Рисунок 9: Установка `lnav` на сервере

- Выполнен просмотр журналов с помощью lnav
- Отображаются записи сервера и клиента
- Видны сообщения systemd, rsyslog, cupsd

```

server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:41
LOG Press ENTER to focus on the breadcrumb bar
alikamal@server:vagrant/provision... x root@server:~ x alikamal@server:vagrant/provision... x LOG x
LOG 2026-02-11T16:41:47 UTC
2026-02-11T16:31:29.000 syslog.log)messages[63,331]gsd-color[7775]
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:35:48 server systemd[1]: Stopping System Logging Service...
Feb 11 16:35:48 server rsyslogd[1124]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="1"
Feb 11 16:35:48 server systemd[1]: rsyslog.service: Deactivated successfully.
Feb 11 16:35:48 server systemd[1]: Stopped System Logging Service.
Feb 11 16:35:48 server systemd[1]: Starting System Logging Service...
Feb 11 16:35:48 server systemd[1]: Started System Logging Service.
Feb 11 16:35:48 server rsyslogd[8610]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="8
Feb 11 16:35:48 server rsyslogd[8610]: imjournal: journal files changed, reloading... [v8.2506.0-2.el
Feb 11 16:37:24 client systemd[1]: Stopping System Logging Service...
Feb 11 16:37:25 client rsyslogd[1020]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="1
Feb 11 16:37:25 client systemd[1]: rsyslog.service: Deactivated successfully.
Feb 11 16:37:25 client systemd[1]: Stopped System Logging Service.
Feb 11 16:37:25 client systemd[1]: Starting System Logging Service...
Feb 11 16:37:25 client systemd[1]: Started System Logging Service.
Feb 11 16:37:25 client rsyslogd[5815]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="5
Feb 11 16:37:25 client rsyslogd[5815]: imjournal: journal files changed, reloading... [v8.2506.0-2.el
Feb 11 16:37:33 server systemd[7431]: Started VTE child process 8693 launched by gnome-terminal-server
Feb 11 16:38:01 server systemd[1]: Starting Hostname Service...
Feb 11 16:38:01 server systemd[1]: Started Hostname Service.
Feb 11 16:38:31 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Feb 11 16:38:36 server systemd[7431]: Started VTE child process 8767 launched by gnome-terminal-server
Feb 11 16:39:09 server systemd[7431]: Started VTE child process 8817 launched by gnome-terminal-server
Feb 11 16:40:08 server systemd[7431]: Started VTE child process 8876 launched by gnome-terminal-server
Feb 11 16:40:09 server cupsd[1018]: REQUEST localhost - - "POST / HTTP/1.1" 200 186 Renew-Subscription
Feb 11 16:40:28 server systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Feb 11 16:40:28 server systemd[1]: Starting man-db-cache-update.service...
Feb 11 16:40:29 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Feb 11 16:40:29 server systemd[1]: Finished man-db-cache-update.service.
Feb 11 16:40:29 server systemd[1]: run-rd70f918ac1894228b31fd8bf7dc6b14d.service: Deactivated successfully

```

- Установлен пакет lnav на клиенте
- Подтверждена подготовка к установке

The screenshot shows a terminal window titled "client [Running] - Oracle VirtualBox". The window has tabs for "Activities" and "Terminal". The terminal content is as follows:

```
alkamal@client:vagrant/provision/client — sudo dnf -y install lnav
[alkamal@client.alkamal.net client]$ sudo cd /etc/rsyslog.d
[alkamal@client.alkamal.net client]$ sudo touch netlog-client.conf
[alkamal@client.alkamal.net client]$ sudo nano /etc/rsyslog.d/netlog-client.conf
[alkamal@client.alkamal.net client]$ systemctl restart rsyslog
[alkamal@client.alkamal.net client]$ sudo dnf -y install lnav
[sudo] password for alkamal:
Last metadata expiration check: 2:05:30 ago on Wed 11 Feb 2026 02:36:44 PM UTC.
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:
[====] --- B/s | 0 B     --::-- ETA
```

Рисунок 11: Установка lnav на клиенте

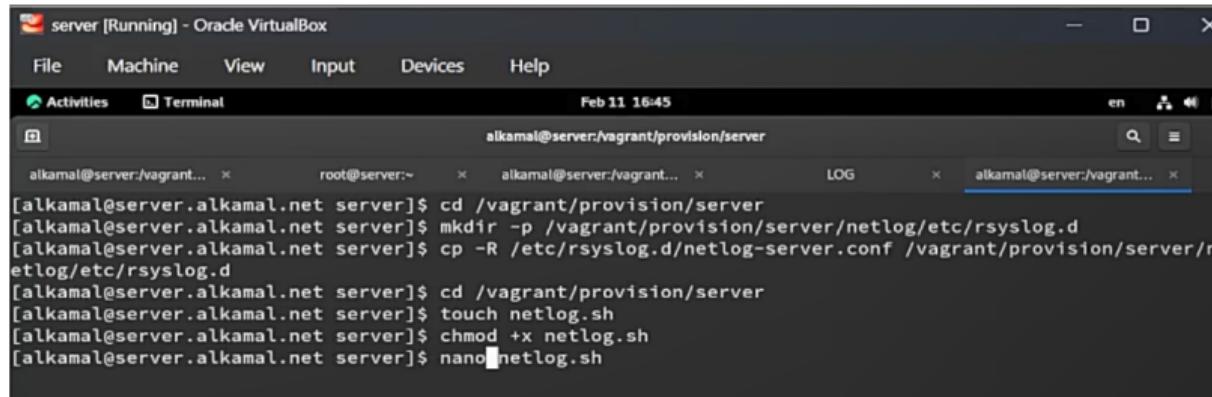
- Выполнен просмотр журналов клиента через lnav
- Отображаются записи systemd, rsyslog, packagekit
- Подтверждена корректная работа логирования

```

client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:44 en 46
LOG Press ENTER to focus on the breadcrumb bar
2016-02-11T16:44:05 UTC 2016-02-11T16:04:47.000 }syslog_log)messages[25,534]
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:47 client gsd-color[5151]: unable to get EDID for xrandr-Virtual1: unable to get EDID for
Feb 11 16:04:50 client systemd[4701]: Started Application launched by gnome-shell.
Feb 11 16:04:50 client systemd[4701]: Created slice Slice /app/org.gnome.Terminal.
Feb 11 16:04:50 client systemd[4701]: Starting GNOME Terminal Server...
Feb 11 16:04:50 client systemd[4701]: Started GNOME Terminal Server.
Feb 11 16:04:50 client systemd[4701]: Started VTE child process 5618 launched by gnome-terminal-server
Feb 11 16:04:56 client gnome-shell[4873]: Can't update stage views actor MetaWindowGroup is on because
Feb 11 16:04:56 client gnome-shell[4873]: Can't update stage views actor MetaWindowActorX11 is on beca
Feb 11 16:04:56 client gnome-shell[4873]: Can't update stage views actor MetaSurfaceActorX11 is on bec
Feb 11 16:05:21 client systemd[4701]: Starting Mark boot as successful...
Feb 11 16:05:21 client systemd[4701]: Finished Mark boot as successful.
Feb 11 16:08:21 client systemd[4701]: Created slice User Background Tasks Slice.
Feb 11 16:08:21 client systemd[4701]: Starting Cleanup of User's Temporary Files and Directories...
Feb 11 16:08:21 client systemd[4701]: Finished Cleanup of User's Temporary Files and Directories.
Feb 11 16:08:49 client systemd[1]: packagekit.service: Deactivated successfully.
Feb 11 16:08:49 client systemd[1]: packagekit.service: Consumed 4.054s CPU time.
Feb 11 16:18:21 client systemd[1]: Starting Cleanup of Temporary Directories...
Feb 11 16:18:21 client systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Feb 11 16:18:21 client systemd[1]: Finished Cleanup of Temporary Directories.
Feb 11 16:18:21 client systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactiv
Feb 11 16:22:21 client systemd[1]: Starting dnf makecache...
Feb 11 16:22:22 client dnf[5728]: Metadata cache refreshed recently.
Feb 11 16:22:22 client systemd[1]: dnf-makecache.service: Deactivated successfully.
Feb 11 16:22:22 client systemd[1]: Finished dnf makecache.
Feb 11 16:37:24 client systemd[1]: Stopping System Logging Service...
Feb 11 16:37:25 client rsyslogd[1020]: [origin software="rsyslog" swVersion="8.2506.0-2.el9" x-pid="1"]
Feb 11 16:37:25 client systemd[1]: rsyslog.service: Deactivated successfully.
Feb 11 16:37:25 client systemd[1]: Stopped System Logging Service.
Feb 11 16:37:25 client systemd[1]: Starting System Logging Service...
Feb 11 16:37:25 client systemd[1]: Started System Logging Service.
Feb 11 16:37:25 client rsyslogd[5815]: [origin software="rsyslog" swVersion="8.2506.0-2.el9" x-pid="5"
Feb 11 16:37:25 client rsyslogd[5815]: imjournal: journal files changed, reloading... [v8.2506.0-2.el9]
```

2.4 Внесение изменений в настройки внутреннего

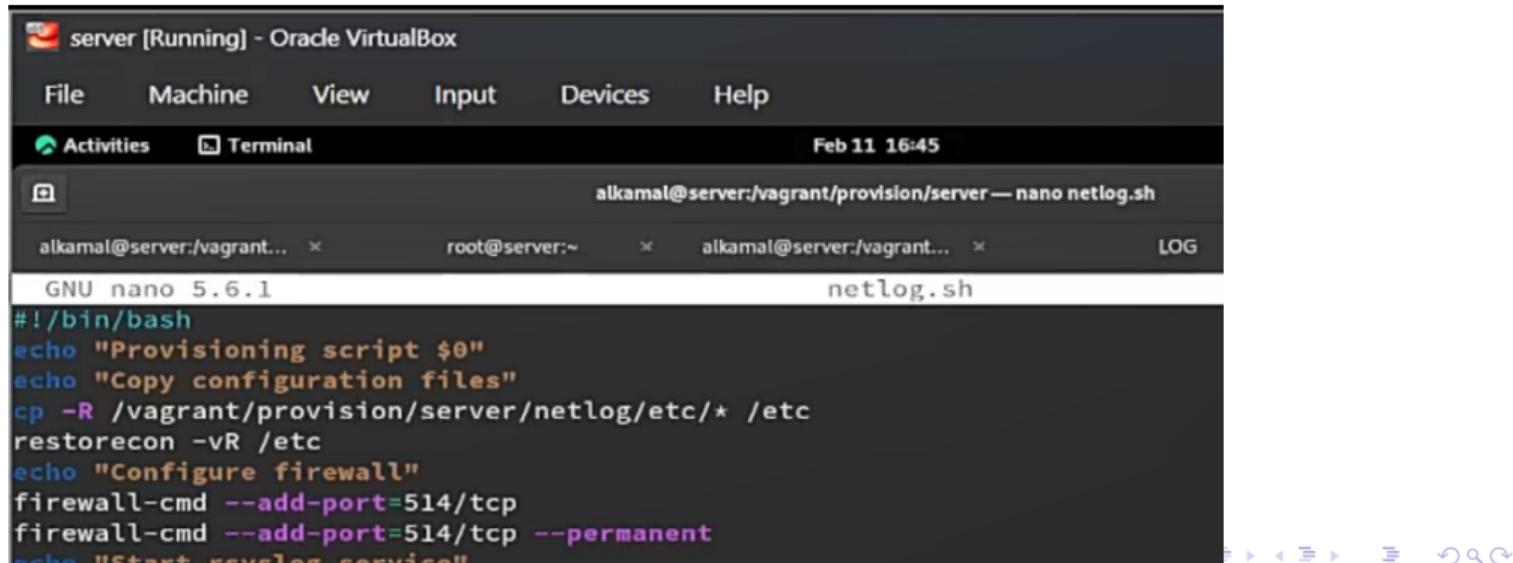
- Переход в /vagrant/provision/server
- Создание каталога netlog/etc/rsyslog.d
- Копирование netlog-server.conf
- Подготовка структуры provisioning



```
[alkamal@server:vagrant... ~]$ cd /vagrant/provision/server
[alkamal@server:vagrant... ~]$ mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[alkamal@server:vagrant... ~]$ cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[alkamal@server:vagrant... ~]$ cd /vagrant/provision/server
[alkamal@server:vagrant... ~]$ touch netlog.sh
[alkamal@server:vagrant... ~]$ chmod +x netlog.sh
[alkamal@server:vagrant... ~]$ nano netlog.sh
```

Рисунок 13: Создание каталога netlog и копирование конфигурации rsyslog

- Создан исполняемый скрипт netlog.sh
- Назначены права выполнения
- Добавлена автоматическая настройка
- Копирование файлов в /etc
- Восстановление контекстов SELinux
- Открытие порта 514
- Перезапуск rsyslog

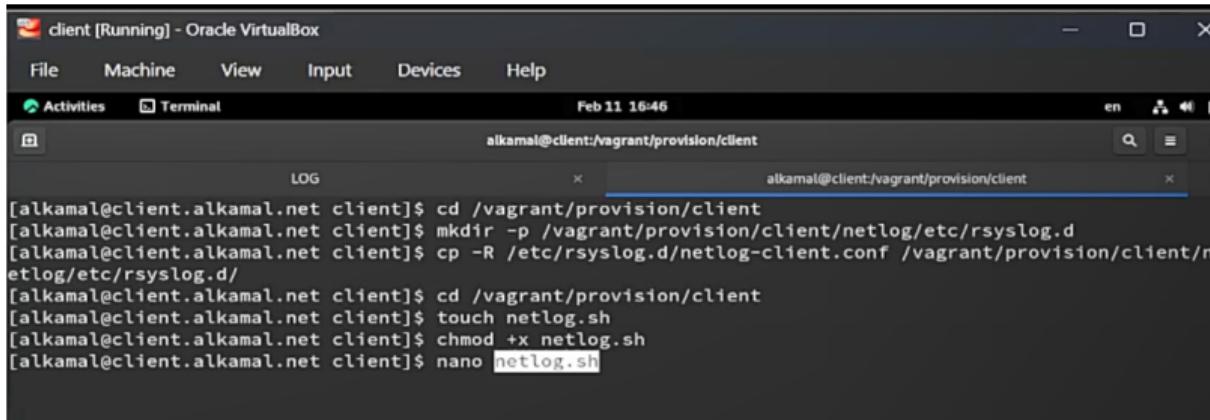


```

server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:45
alkamal@server:vagrant/provision/server — nano netlog.sh
alkamal@server:vagrant... × root@server:~ × alkamal@server:vagrant... × LOG
GNU nano 5.6.1 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"

```

- Переход в /vagrant/provision/client
- Создание каталога netlog/etc/rsyslog.d
- Копирование netlog-client.conf



```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal
Feb 11 16:46
alkamal@client:/vagrant/provision/client
LOG alkamal@client:/vagrant/provision/client
[alkamal@client.alkamal.net client]$ cd /vagrant/provision/client
[alkamal@client.alkamal.net client]$ mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[alkamal@client.alkamal.net client]$ cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/n
etlog/etc/rsyslog.d/
[alkamal@client.alkamal.net client]$ cd /vagrant/provision/client
[alkamal@client.alkamal.net client]$ touch netlog.sh
[alkamal@client.alkamal.net client]$ chmod +x netlog.sh
[alkamal@client.alkamal.net client]$ nano netlog.sh
```

Рисунок 15: Создание каталога netlog и копирование конфигурации клиента

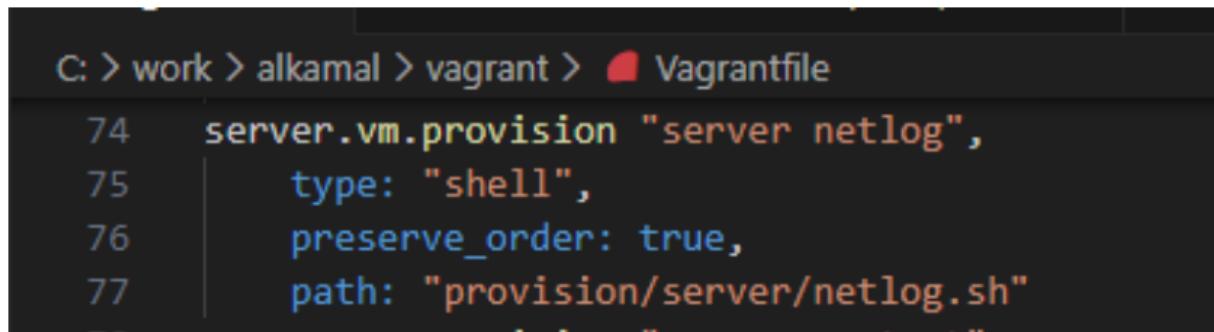
- Создан исполняемый файл `netlog.sh`
- Добавлен сценарий автоматической настройки клиента
- Установка `lnav`
- Копирование файлов в `/etc`
- Восстановление контекстов SELinux
- Перезапуск `rsyslog`

The screenshot shows a terminal window with the following details:

- Title Bar:** client [Running] - Oracle VirtualBox
- Menu Bar:** File, Machine, View, Input, Devices, Help
- Toolbar:** Activities, Terminal, Date: Feb 11 16:46
- Terminal Content:**
 - User: alkamal@client:vagrant/provision/client — sudo nano netlog.sh
 - File Name: netlog.sh
 - Content (copied from the image):

```
#!/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
```

- В Vagrantfile добавлен блок provisioning для сервера
- Указан скрипт provision/server/netlog.sh
- Сохранена последовательность выполнения



C: > work > alkamal > vagrant > Vagrantfile

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

Рисунок 17: Добавление provisioning для сервера в Vagrantfile

- Добавлен аналогичный блок для клиента
- Указан скрипт provision/client/netlog.sh
- Обеспечена автоматическая настройка при запуске ВМ

```
C: > work > alkamal > vagrant > Vagrantfile
135   client.vm.provision "client_netlog",
136     type: "shell",
137     preserve_order: true,
138     path: "provision/client/netlog.sh"
```

Рисунок 18: Добавление provisioning для клиента в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Настроено централизованное журналирование на базе `rsyslog`
- Организован приём журналов по TCP 514 на сервере
- Реализовано перенаправление сообщений с клиента
- Подтверждена корректность работы через `/var/log/messages` и `1nav`
- Реализована автоматизация через provisioning-скрипты
- Обеспечена воспроизводимость конфигурации
- Создана функционирующая система централизованного сбора журналов