

# **Отчёт по лабораторной работе №15**

**Дисциплина: Администрирование сетевых подсистем**

Ибрахим Мохсейн Алькамаль

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
2.1 Настройка сервера сетевого журнала . . . . .	6
2.2 Настройка клиента сетевого журнала . . . . .	8
2.3 Просмотр журнала . . . . .	8
2.4 Внесение изменений в настройки внутреннего . . . . .	12
<b>3 Выводы</b>	<b>16</b>
<b>4 Ответы на контрольные вопросы</b>	<b>17</b>

# Список иллюстраций

2.1	Создание файла конфигурации rsyslog netlog-server.conf . . . . .	6
2.2	Настройка приёма журналов по TCP 514 в rsyslog . . . . .	7
2.3	Проверка прослушиваемых TCP-портов службой rsyslog . . . . .	7
2.4	Настройка firewalld для открытия TCP-порта 514 . . . . .	7
2.5	Создание файла конфигурации netlog-client.conf на клиенте . . . . .	8
2.6	Настройка перенаправления журналов на сервер по TCP 514 . . . . .	8
2.7	Просмотр журнала /var/log/messages на сервере . . . . .	9
2.8	Запуск gnome-system-monitor на сервере . . . . .	9
2.9	Установка lnav на сервере . . . . .	10
2.10	Просмотр журналов сервера в lnav . . . . .	11
2.11	Установка lnav на клиенте . . . . .	11
2.12	Просмотр журналов клиента в lnav . . . . .	12
2.13	Создание каталога netlog и копирование конфигурации rsyslog . . . . .	13
2.14	Содержимое скрипта netlog.sh для автоматической настройки . . . . .	13
2.15	Создание каталога netlog и копирование конфигурации клиента . . . . .	14
2.16	Содержимое скрипта netlog.sh на клиенте . . . . .	14
2.17	Добавление provisioning для сервера в Vagrantfile . . . . .	15
2.18	Добавление provisioning для клиента в Vagrantfile . . . . .	15

# **Список таблиц**

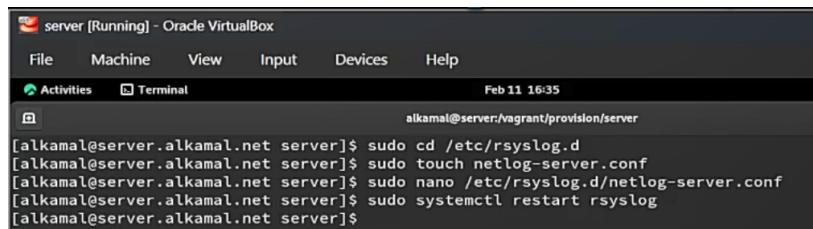
# **1 Цель работы**

Получение навыков по работе с журналами системных событий.

# 2 Выполнение лабораторной работы

## 2.1 Настройка сервера сетевого журнала

В каталоге `/etc/rsyslog.d` на сервере создан файл конфигурации `netlog-server.conf` для настройки сетевого хранения журналов (рис. 2.1). Команды `cd /etc/rsyslog.d` и `touch netlog-server.conf` обеспечивают размещение и создание нового конфигурационного файла.



```
server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:35
alkamal@server:/vagrant/provision/server
[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 2.1: Создание файла конфигурации rsyslog netlog-server.conf

В файле `/etc/rsyslog.d/netlog-server.conf` включён приём журналов по TCP-порту 514 посредством загрузки модуля `imtcp` и активации сервера ввода (`$ModLoad imtcp`, `$InputTCPServerRun 514`) (рис. 2.2). Данные директивы активируют обработку входящих TCP-соединений службой `rsyslog`.

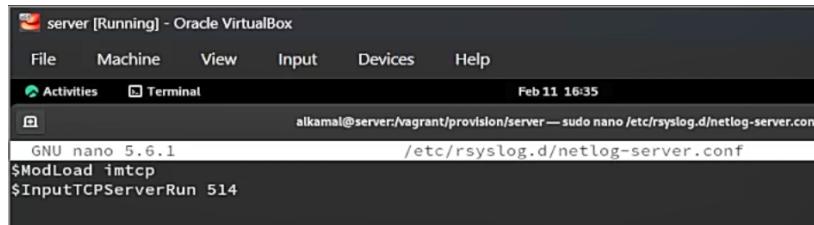


Рисунок 2.2: Настройка приёма журналов по TCP 514 в rsyslog

После перезапуска службы `rsyslog` выполнена проверка прослушиваемых TCP-портов с использованием `lsof | grep TCP` (рис. 2.3). В выводе отображается процесс `rsyslog`, находящийся в состоянии `LISTEN`, что подтверждает активацию TCP-приёма.

rsyslogd processes						
Process ID	User	State	Memory Usage	IP Address	Port	Protocol
rsyslogd 8610	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610	root	running	4u	IPv6	58274	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8613 in:imjourn	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8613 in:imjourn	root	running	5u	IPv6	58274	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8614 in:imtcp	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8614 in:imtcp	root	running	5u	IPv6	58274	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8619 w0/imtcp	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8619 w0/imtcp	root	running	5u	IPv6	58274	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8620 w1/imtcp	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8620 w1/imtcp	root	running	5u	IPv6	58274	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8621 rs:main	root	running	4u	IPv4	58273	TCP *:sh
ell (LISTEN)						
rsyslogd 8610 8621 rs:main	root	running	5u	IPv6	58274	TCP *:sh
ell (LISTEN)						

Рисунок 2.3: Проверка прослушиваемых TCP-портов службой rsyslog

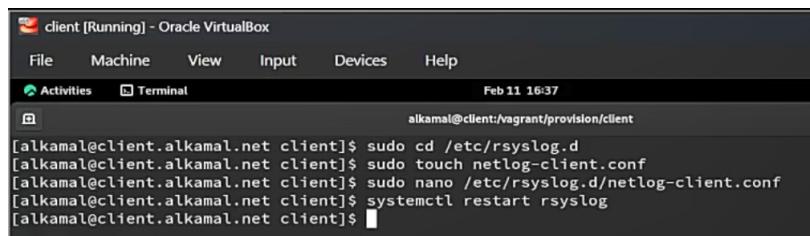
На сервере настроен межсетевой экран для разрешения входящих соединений по TCP-порту 514 с помощью команд `firewall-cmd --add-port=514/tcp` и `firewall-cmd --add-port=514/tcp --permanent` (рис. 2.4). Это обеспечивает как временное, так и постоянное открытие порта для приёма сетевых сообщений журнала.

```
[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 2.4: Настройка firewalld для открытия TCP-порта 514

## 2.2 Настройка клиента сетевого журнала

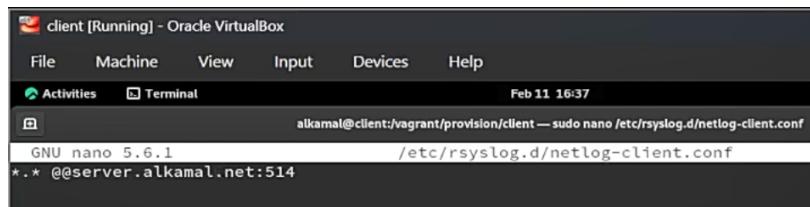
В каталоге `/etc/rsyslog.d` на клиенте создан файл конфигурации `netlog-client.conf` для настройки сетевой отправки журналов (рис. 2.5). Команды `cd /etc/rsyslog.d` и `touch netlog-client.conf` обеспечивают размещение и создание конфигурационного файла клиента.



```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:37
alkamal@client:vagrant/provision/client
[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 2.5: Создание файла конфигурации `netlog-client.conf` на клиенте

В файле `/etc/rsyslog.d/netlog-client.conf` настроено перенаправление всех сообщений журнала на TCP-порт 514 сервера с использованием строки `* . * @@server.alkamal.net :514` (рис. 2.6). Символы `@@` указывают на передачу сообщений по протоколу TCP.



```
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 2.6: Настройка перенаправления журналов на сервер по TCP 514

После внесения изменений выполнен перезапуск службы `rsyslog` командой `systemctl restart rsyslog`, что применяет новую конфигурацию клиента.

## 2.3 Просмотр журнала

На сервере выполнен просмотр файла системного журнала `/var/log/messages` с использованием команды `tail -f` (рис. 2.7). В выводе отображаются сообщения

служб `rsyslog`, `systemd`, а также указаны имена хостов `client` и `server`, что подтверждает поступление удалённых записей журнала.

```
[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="102
0" 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="581
5" 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 p
rocess 8192.
Feb 11 16:38:01 server systemd[1]: Starting Hostname Service...
Feb 11 16:38:01 server systemd[1]: Started Hostname Service.
```

Рисунок 2.7: Просмотр журнала `/var/log/messages` на сервере

Под пользователем `alkamal` на сервере запущена графическая программа мониторинга системы `gnome-system-monitor` (рис. 2.8). Интерфейс отображает активные процессы, их идентификаторы, использование CPU и памяти.

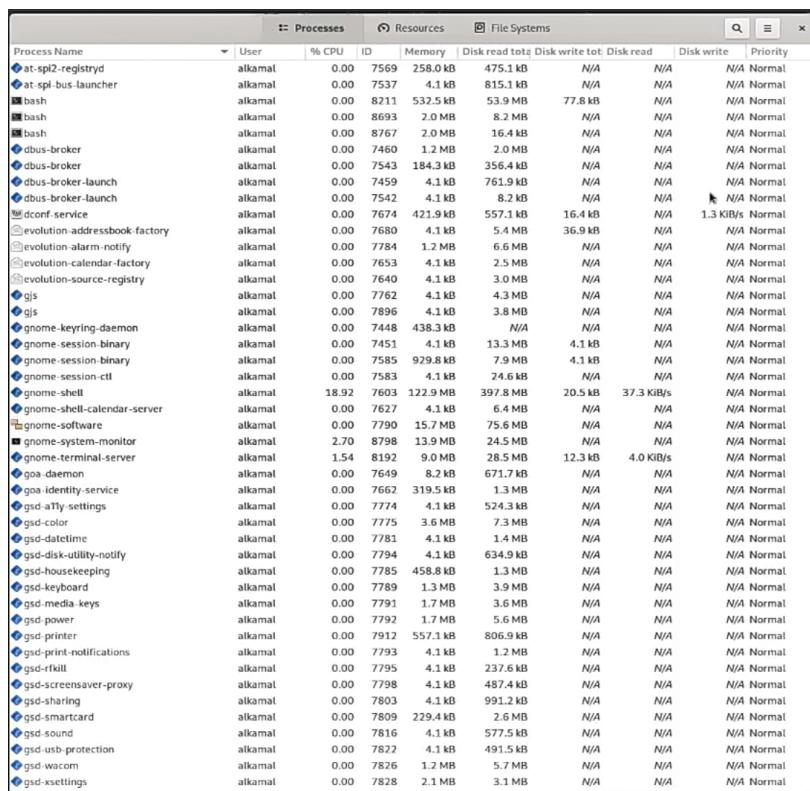
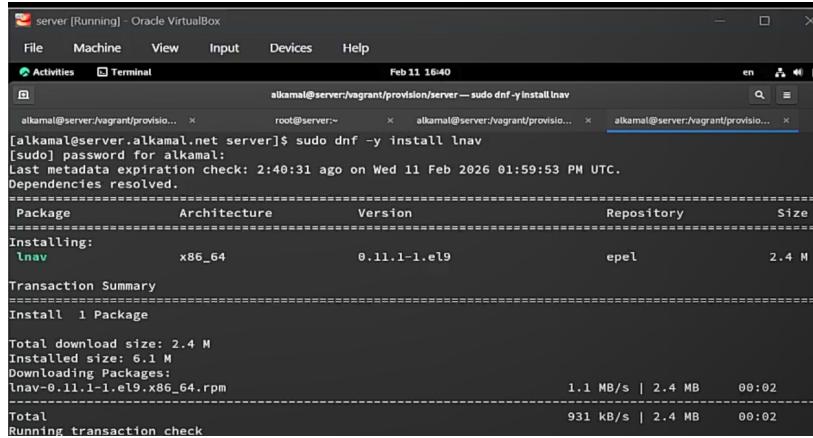


Рисунок 2.8: Запуск `gnome-system-monitor` на сервере

На сервере установлен просмотрщик системных журналов `lnav` с помощью пакетного менеджера `dnf` (рис. 2.9). В выводе подтверждена успешная установка пакета версии `0.11.1-1.el9` из репозитория `epel`.



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has tabs for "Activities" and "Terminal". The terminal tab is active, showing the command `sudo dnf -y install lnav` being run by user "alkamal". The output shows the package being installed from the "epel" repository. The transaction summary indicates the download and installation of the `lnav-0.11.1-1.el9.x86_64.rpm` package.

```
[alkamal@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.

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 2.9: Установка `lnav` на сервере

Просмотр журналов на сервере выполнен с использованием `lnav` (рис. 2.10). В интерфейсе отображаются записи как локального сервера, так и клиента, включая сообщения служб `systemd`, `rsyslog`, `cupsd` и других.

```

server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:41
alkamal@server:vagrant/provision... x root@server:~ x alkamal@server:vagrant/provision... x LOG
LOG
Press ENTER to focus on the breadcrumb bar
2026-02-11T16:41:47 UTC
Log [2026-02-11T16:31:29.000]syslog_log)messages[63,331]:xd_color[7775]
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:31:29 server gsd-color[7775]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:35:48 server systemd[1]: Stopping System Logging Service...
Feb 11 16:35:48 server syslogd[1124]: [origin software="syslogd" swVersion="8.2506.0-2.el9" x-pid="1
Feb 11 16:35:48 server systemd[1]: syslog.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 syslogd[8610]: [origin software="syslogd" swVersion="8.2506.0-2.el9" x-pid="8
Feb 11 16:35:48 server syslogd[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 syslogd[1020]: [origin software="syslogd" swVersion="8.2506.0-2.el9" x-pid="1
Feb 11 16:37:25 client systemd[1]: syslog.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 syslogd[5815]: [origin software="syslogd" swVersion="8.2506.0-2.el9" x-pid="5
Feb 11 16:37:25 client syslogd[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 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-rd70f918ac1894228b31fd8bfadcb614d.service: Deactivated successf
Feb 11 16:40:29 server systemd[1]: Starting PackageKit Daemon...
Feb 11 16:40:29 server systemd[1]: Started PackageKit Daemon.
Feb 11 16:40:36 server packagekitd[9129]: Failed to get cache filename for kernel-devel-matched
Feb 11 16:40:36 server packagekitd[9129]: Failed to get cache filename for kernel
Feb 11 16:41:09 server packagekitd[9129]: Failed to get cache filename for kernel-devel-matched
Feb 11 16:41:09 server packagekitd[9129]: Failed to get cache filename for kernel

```

Рисунок 2.10: Просмотр журналов сервера в lnav

На клиенте выполнена установка пакета lnav командой `dnf -y install lnav` (рис. 2.11). Вывод подтверждает загрузку и подготовку к установке пакета.

```

client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:42
alkamal@client:vagrant/provision/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.
=====
Transaction Summary
=====
Install 1 Package

Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
[====] --- B/s | 0 B    --:-- ETA

```

Рисунок 2.11: Установка lnav на клиенте

На клиенте выполнен просмотр системных журналов с помощью lnav

(рис. 2.12). В журнале отображаются записи служб клиента (`systemd`, `rsyslog`, `packagekit`), что подтверждает корректную работу локального логирования и передачу сообщений на сервер.

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:44
LOG Press ENTER to focus on the breadcrumb bar
Log 2026-02-11T16:04:47.000) syslog_log)messages[25,534]
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: unable to get EDID for
Feb 11 16:04:47 client gsd-color[515]: unable to get EDID for xrandr-Virtual: 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 16:04:56 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 because
Feb 11 16:04:56 client gnome-shell[4873]: Can't update stage views actor MetaSurfaceActorX11 is on because
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[1]: packagekit.service: Deactivated successfully.
Feb 11 16:08:49 client systemd[1]: packagekit.service: Consumed 4.054s CPU time.
Feb 11 16:10:21 client systemd[1]: Starting Cleanup of Temporary Directories...
Feb 11 16:10:21 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-systemdxdtmpfiles/x2dclean.service.mount: Deactivat
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 syslogd[1028]: [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 syslogd[5815]: imjournal: journal files changed, reloading... [v8.2506.0-2.el9]
Feb 11 16:43:51 client systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Feb 11 16:43:51 client systemd[1]: Starting man-db-cache-update.service...
Feb 11 16:43:51 client systemd[1]: man-db-cache-update.service: Deactivated successfully.
Feb 11 16:43:51 client systemd[1]: Finished man-db-cache-update.service.
Feb 11 16:43:51 client systemd[1]: run-rf61f49bd4f93494ab9ffcc7d0ee3dd46.service: Deactivated successf
Feb 11 16:43:52 Client systemd[1]: Starting PackageKit Daemon...
Feb 11 16:43:52 Client systemd[1]: Started PackageKit Daemon.
Feb 11 16:43:59 Client packagekitd[6053]: Failed to get cache filename for kernel-devel-matched
Feb 11 16:43:59 Client packagekitd[6053]: Failed to get cache filename for kernel
```

Рисунок 2.12: Просмотр журналов клиента в lnav

## 2.4 Внесение изменений в настройки внутреннего

На виртуальной машине server выполнен переход в каталог /vagrant/provision/server и создан каталог netlog/etc/rsyslog.d и скопирован файл конфигурации netlog-server.conf для последующего автоматического развёртывания (рис. 2.13). Команды mkdir -р и cp -R обеспечивают формирование структуры каталогов и размещение конфигурационного файла в директории provisioning.

```

server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:45
alkamal@server:vagrant... x root@server:~ x alkamal@server:vagrant... x LOG x alkamal@server:vagrant...
[alkamal@server.alkamal.net server]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[alkamal@server.alkamal.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[alkamal@server.alkamal.net server]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ touch netlog.sh
[alkamal@server.alkamal.net server]$ chmod +x netlog.sh
[alkamal@server.alkamal.net server]$ nano netlog.sh

```

Рисунок 2.13: Создание каталога netlog и копирование конфигурации rsyslog

В каталоге `/vagrant/provision/server` создан исполняемый скрипт `netlog.sh`, которому назначены права выполнения, и в него добавлен сценарий автоматической настройки (рис. 2.14). Скрипт выполняет копирование конфигурационных файлов в `/etc`, восстановление контекстов SELinux (`restorecon -vR /etc`), открытие TCP-порта 514 в `firewalld` и перезапуск службы `rsyslog`, что обеспечивает автоматизацию настройки сетевого журнала.

```

server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 16:45
alkamal@server:vagrant... x root@server:~ x alkamal@server:vagrant... x netlog.sh
GNU nano 5.6.1
#!/bin/bash
# Provisioning script $0
# Copy configuration files
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
# Configure firewall
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
# Start rsyslog service
systemctl restart rsyslog

```

Рисунок 2.14: Содержимое скрипта netlog.sh для автоматической настройки

На виртуальной машине `client` выполнен переход в каталог `/vagrant/provision/client`, создан каталог `netlog/etc/rsyslog.d` и скопирован файл конфигурации `netlog-client.conf` для последующего автоматического развёртывания (рис. 2.15). Команды `mkdir -p` и `cp -R` обеспечивают формирование структуры каталогов и размещение конфигурационного файла клиента.

```

[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/netlog/etc/rsyslog.d
[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 2.15: Создание каталога netlog и копирование конфигурации клиента

В каталоге `/vagrant/provision/client` создан исполняемый файл `netlog.sh`, которому назначены права выполнения, и в него добавлен сценарий автоматической настройки клиента (рис. 2.16). Скрипт выполняет установку пакета `lnav`, копирование конфигурационных файлов в `/etc`, восстановление контекстов SELinux и перезапуск службы `rsyslog`.

```

GNU nano 5.6.1
netlog.sh
#!/bin/bash
# Provisioning script $0
# Install needed packages
dnf -y install lnav
# Copy configuration files
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
# Start rsyslog service
systemctl restart rsyslog

```

Рисунок 2.16: Содержимое скрипта `netlog.sh` на клиенте

В конфигурационном файле `Vagrantfile` в разделе сервера добавлен блок автоматического выполнения скрипта `provision/server/netlog.sh` при загрузке виртуальной машины (рис. 2.17). Параметр `preserve_order: true` обеспечивает сохранение последовательности выполнения provisioning-скриптов.

```
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 2.17: Добавление provisioning для сервера в Vagrantfile

Аналогичный блок добавлен в разделе клиента для автоматического запуска скрипта provision/client/netlog.sh при старте виртуальной машины (рис. 2.18). Это обеспечивает применение настроек сетевого журналирования на обеих машинах при их инициализации.

```
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 2.18: Добавление provisioning для клиента в Vagrantfile

## 3 Выводы

В ходе работы выполнена настройка централизованного сетевого журналирования на базе `rsyslog` с использованием TCP-порта 514. На сервере организован приём журналов по протоколу TCP и настроено разрешение соответствующего порта в межсетевом экране. На клиенте реализовано перенаправление всех сообщений журнала на сервер.

Корректность конфигурации подтверждена просмотром файла `/var/log/messages`, где зафиксированы записи как локального сервера, так и удалённого клиента. Использование утилиты `lnav` позволило проанализировать системные сообщения в удобном интерактивном режиме.

Дополнительно реализована автоматизация развёртывания конфигурации посредством provisioning-скриптов `netlog.sh` и интеграции их в `Vagrantfile`, что обеспечивает воспроизводимость и автоматическое применение настроек при запуске виртуальных машин.

Таким образом, создана функционирующая система централизованного сбора и анализа системных журналов.

## 4 Ответы на контрольные вопросы

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

Для приёма сообщений от `journald` следует использовать модуль `imjournal`.

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

`imklog`

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

Следует использовать параметр “`SystemCallFilter[include:omusrmsg.conf?]`” в конфигурационном файле `rsyslog.conf`.

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

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле `rsyslog.conf`.

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

Пересылка сообщений из `journald` в `rsyslog` управляется параметром “`ForwardToSyslog`” в файле конфигурации `journald.conf`.

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

Модуль `rsyslog`, который можно использовать для включения сообщений из файла журнала, не созданного `rsyslog`, называется `imfile`.

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

Для пересылки сообщений в базу данных MariaDB следует использовать модуль `ommysql`.

8. Какие две строки вам нужно включить в `rsyslog.conf`, чтобы позволить текущему журнальному серверу получать сообщения через TCP?

Для позволения текущему журнальному серверу получать сообщения через TCP нужно включить две строки в `rsyslog.conf`:

```
$ModLoad imtcp  
$InputTCPServerRun 514
```

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

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