МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №13
«Работа с системой учета и регистрациии событий операционной системы GNU/Linux»

Практическая работа
по дисциплине «Системное программное обеспечение»
студента 3 курса группы ИВТ-б-о-222(2)
Чудопалова Богдана Андреевича

09.03.01 «Информатика и вычислительная техника»

Симферополь, 2025

Ход работы

1. Проверить наличие в используемом дистрибутиве Linux rsyslog демона. При его отсутствии установить — в моем дистрибутиве rsyslog установлен.

```
sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-04-24 21:09:14 MSK; 8min ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 785 (rsyslogd)
      Tasks: 4 (limit: 18369)
     Memory: 3.6M (peak: 3.9M)
        CPU: 213ms
     CGroup: /system.slice/rsyslog.service
             └─785 /usr/sbin/rsyslogd -n -iNONE
```

2. Осуществить настройку сохранения сообщений от источника local7 в отдельный файл — первым шагом создал уонфигурационный файл в /etc/rsyslog.d со следующим содержимым.

```
sudo vim local7.conf
local7.*    /var/log/local7.log
~
~
```

Перезапустил rsyslog для применения настроек

```
→  rsyslog.d sudo systemctl restart rsyslog
→  rsyslog.d sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-04-24 21:26:52 MSK; 4s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
    Process: 10204 ExecStartPre=/usr/lib/rsyslog/reload-apparmor-profile (code=exited, status=0/SUCCESS)
   Main PID: 10206 (rsyslogd)
```

3. Проверить, что выполненные настройки корректны выполнением тестовой посылки сообщения утилитой logger — сделал это с помощью команды - logger -p local7.info -t test_local7 "Тестовое сообщение";

```
→  rsyslog.d logger -p local7.info -t test_local7 "Тестовое сообщение"
→  rsyslog.d sudo cat /var/log/local7.log
2025-04-24T21:28:36.669818+03:00 bogdan-laptop test_local7: Тестовое сообщение
→  rsyslog.d
```

4. Настроить хранение данных для источника local7 в базе данных PostgreSQL — первым шагом создал БД syslog

После создал таблицу и пользователя

```
postgres=# \c syslog
You are now connected to database "syslog" as user "postgres".
syslog=# CREATE TABLE SystemEvents (
    Message TEXT,
    Facility SMALLINT,
    FromHost TEXT,
    Priority SMALLINT,
    DeviceReportedTime TIMESTAMP,
    ReceivedAt TIMESTAMP,
    InfoUnitID INT,
    SysLogTag TEXT
);
CREATE TABLE
syslog=#
```

Выдал пользователю привелегии

```
syslog=# CREATE USER writer WITH PASSWORD '1234';
CREATE ROLE
syslog=# GRANT ALL PRIVILEGES ON TABLE systemevents TO writer;
GRANT
syslog=#
```

Отредактировал файл /etc/rsyslog.conf, добавив туда модуль ompgsql

```
# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
module(load="ompgsql")
###########################
#### GLOBAL DIRECTIVES ####
###########################
```

Отредактировал файл /etc/rsyslog.d/loclal7.conf

```
                                                    sudo vim /etc/rsyslog.d/local7.conf
local7.*    :ompgsql:localhost,syslog,writer,1234
```

Провел 2 теста

```
   message    | facility |   fromhost    | priority | devicereportedtime  |     receivedat      | infounitid | syslogta
g
--------------+----------+---------------+----------+---------------------+---------------------+------------+---------
--
  First test  |       23 | bogdan-laptop |        6 | 2025-05-21 11:19:18 | 2025-05-21 11:19:18 |          1 | bogdan:
  Second test |       23 | bogdan-laptop |        6 | 2025-05-21 11:19:22 | 2025-05-21 11:19:22 |          1 | bogdan:
(2 rows)
```

Результат

6. Обеспечить отправку сообщений с одного узла на другой, на котором хранение осуществляется в базе данных PostgreSQL — первыш шагом внес ищменения в /etc/rsyslog.conf следующие изменения

```
provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

На стороне отправителя внес в /etc/rsyslog.conf такие изменения

```
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.* @@192.168.0.205
```

Тестовая отправка

```
782  sudo vim /etc/rsyslog.conf
783  sudo systemctl restart rsyslog
784  sudo systemctl status rsyslog
785  clear
786  logger -p local7.info "psql first"
```

Результат

```
   message    | facility |     fromhost      | priority | devicereportedtime  |     receivedat      | infounitid | sysl
ogtag
--------------+----------+-------------------+----------+---------------------+---------------------+------------+-----
------
  First test  |       23 | bogdan-laptop     |        6 | 2025-05-21 11:19:18 | 2025-05-21 11:19:18 |          1 | bogd
an:
  Second test |       23 | bogdan-laptop     |        6 | 2025-05-21 11:19:22 | 2025-05-21 11:19:22 |          1 | bogd
an:
  psql first  |       23 | bogdan-virtualbox |        6 | 2025-05-21 11:30:03 | 2025-05-21 11:30:03 |          1 | bogd
an:
(3 rows)

(END)
```