

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 учёта и регистрации событий в среде GNU/Linux»

Практическая работа
по дисциплине «Системное программное обеспечение»
студента 3 курса группы ИВТ-б-о-222(1)
Гоголева Виктора Григорьевича

09.03.01 «Направление подготовки»

Симферополь, 2025

Цель работы: Получение навыков по самостоятельному конфигурированию подсистемы регистрации и учёта событий в операционной системе Linux.

```
(root@kali)~[/home/kali]
# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-06-08 03:53:34 EDT; 3min 28s ago
 TriggeredBy: ● syslog.socket
    Docs: man:rsyslogd(8)
          man:rsyslog.conf(5)
          https://www.rsyslog.com/doc/
   Main PID: 2483 (rsyslogd)
     Tasks: 4 (limit: 2265)
    Memory: 1.5M
       CPU: 8ms
   CGroup: /system.slice/rsyslog.service
           └─2483 /usr/sbin/rsyslogd -n -iNONE

Home
Jun 08 03:53:34 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Jun 08 03:53:34 kali rsyslogd[2483]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2302.0]
Jun 08 03:53:34 kali rsyslogd[2483]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2483" x-info="https://www.rsyslog.com"] start
Jun 08 03:53:34 kali systemd[1]: Started rsyslog.service - System Logging Service.

(root@kali)~[/home/kali]
```

Рисунок – проверка наличия и статуса службы rsyslog

1. Осуществления настройки сохранения сообщений от источника в отдельный файл

Возможные категории для логов (facility):

№	Категория	Описание
0	kern	Сообщения, отправляемые ядром
1	user	Пользовательские программы
2	mail	Почта
3	daemon	Сервисы (демоны)
4	auth	Безопасность/вход в систему/аутентификация
5	syslog	Сообщения от syslog
6	lpr	Логи печати
7	news	Новостные группы (usenet)
8	uucp	Unix-to-Unix CoPy (копирование файлов между компьютерами)
9	cron	Планировщик заданий
10	authpriv	Безопасность/вход в систему/аутентификация - защищенный режим
11	ftp	Логи при передачи данных по FTP
12	ntp	Лог службы синхронизации времени (существует не везде)
13	security, log audit	Журнал аудита (существует не везде)
14	console, log alert	Сообщения, отправляемые в консоль (существует не везде)
15	solaris-cron, clock daemon	Cron в solaris (существует не везде)
16-23	local0 - local7	Зарезервированы для локального использования. Уровень серьезности определяется числом от 0 до 7.

```
(root@kali)-[/home]
# nano /etc/rsyslog.conf

(root@kali)-[/home]
# cd /var/log

(root@kali)-[/var/log]
# touch local1.log
```

Рисунок – создание файла для лога

```
GNU nano 7.2 /etc/rsyslog.conf
#input(type="imtcp" port="514")

#####
### GLOBAL DIRECTIVES ###
#####

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

#####
### RULES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*.*;auth,authpriv.none      -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*             /var/log/auth.log
cron.*                      -/var/log/cron.log
kern.*                      -/var/log/kern.log
mail.*                      -/var/log/mail.log
user.*                      -/var/log/user.log

local1.*                    /var/log/local1.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                     :omusrmsg:*
```

Рисунок – конфигурирование файла rsyslog.conf

В файл добавлена строка: local1. * -/var/log/user.log

2. Тестовая посылка сообщения утилитой logger

Возможные категории для логов (severity):

№	Уровень	Расшифровка
0	emerg	Система не работает (PANIC)
1	alert	Серьезная проблема, требующая внимания
2	crit	Критическая ошибка
3	err	Ошибка (ERROR)
4	warning	Предупреждение (WARN)
5	notice	Важное информационное сообщение
6	info	Информационное сообщение
7	debug	Отладочная информация



```
(root@kali)-[/home/kali]
# logger -p local1.crit -t TEST "Test warning"

(root@kali)-[/home/kali]
# logger -p local1.err -t TEST "Test warning"

(root@kali)-[/home/kali]
# logger -p local1.warning -t TEST "Test warning"

(root@kali)-[/home/kali]
# logger -p local1.notice -t TEST "Test warning"

(root@kali)-[/home/kali]
# logger -p local1.info -t TEST "Test warning"

(root@kali)-[/home/kali]
# logger -p local1.debug -t TEST "Test warning"
```

Рисунок – проверка работы утилиты logger

3. Настройка хранения данных для источника в базе данных

```
(root@kali)-[/home/kali]  
# apt install rsyslog-pgsql  
Reading package lists ... Done  
Building dependency tree ... Done
```

Рисунок – установка модуля для работы с pgsql

```
File Actions Edit View Help  
GNU nano 7.2 /etc/rsyslog.d/pgsql.conf *  
### Configuration file for rsyslog-pgsql  
### Changes are preserved  
  
module (load="ompgsql")  
local1.* action(type="ompgsql" server="localhost" db="syslog" uid="rsyslog" pwd="12345")
```

Рисунок – конфигурирование rsyslog для работы с pgsql

```

(root@kali)-[/home]
# apt install postgresql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  postgresql-client-common postgresql-common
Suggested packages:
  postgresql-doc
The following packages will be upgraded:
  postgresql postgresql-client-common postgresql-common
3 upgraded, 0 newly installed, 0 to remove and 558 not upgraded.
Need to get 225 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://fastmirror.pp.ua/kali kali-rolling/main amd64 postgresql-common all 248 [179 kB]
Get:2 http://fastmirror.pp.ua/kali kali-rolling/main amd64 postgresql-client-common all 248 [35.1 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 postgresql all 15+248 [10.1 kB]
Fetched 225 kB in 2s (141 kB/s)
Preconfiguring packages ...
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali
debian found in ID_LIKE, treating as Debian
(Reading database ... 392574 files and directories currently installed.)
Preparing to unpack .../postgresql-common_248_all.deb ...
Leaving 'diversion of /usr/bin/pg_config to /usr/bin/pg_config.libpq-dev by postgresql-common'
Unpacking postgresql-common (248) over (247) ...
Preparing to unpack .../postgresql-client-common_248_all.deb ...
Unpacking postgresql-client-common (248) over (247) ...
Preparing to unpack .../postgresql_15+248_all.deb ...
Unpacking postgresql (15+248) over (15+247) ...
Setting up postgresql-client-common (248) ...
Setting up postgresql-common (248) ...
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali
debian found in ID_LIKE, treating as Debian
postgresql.service is a disabled or a static unit, not starting it.
Setting up postgresql (15+248) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...

(root@kali)-[/home]
# systemctl start postgresql

(root@kali)-[/home]
# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
   Active: active (exited) since Thu 2023-06-08 09:23:03 EDT; 7s ago
     Process: 15454 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 15454 (code=exited, status=0/SUCCESS)
       CPU: 2ms

Jun 08 09:23:03 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS ...
Jun 08 09:23:03 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

```

Рисунок – установка postgress и включение службы

List of databases							
Name	Owner	Encoding	Collate	Ctype	ICU Locale	Locale Provider	Access privileges
postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	
template0	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	=c/postgres + postgres=CTc/postgres
template1	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	=c/postgres + postgres=CTc/postgres

(3 rows)

Рисунок – просмотр списка БД

```
(root@kali)-[/home]
# sudo su - postgres
postgres@kali:~$ psql
psql (15.2 (Debian 15.2-1))
Type "help" for help.

postgres=# \l
postgres=# \l
postgres=# create database syslog;
CREATE DATABASE
postgres=# create user rsyslog with encrypted password '12345';
CREATE ROLE
postgres=# grant all privileges on database syslog to rsyslog;
GRANT
postgres=# \c syslog
You are now connected to database "syslog" as user "postgres".
syslog=#
```

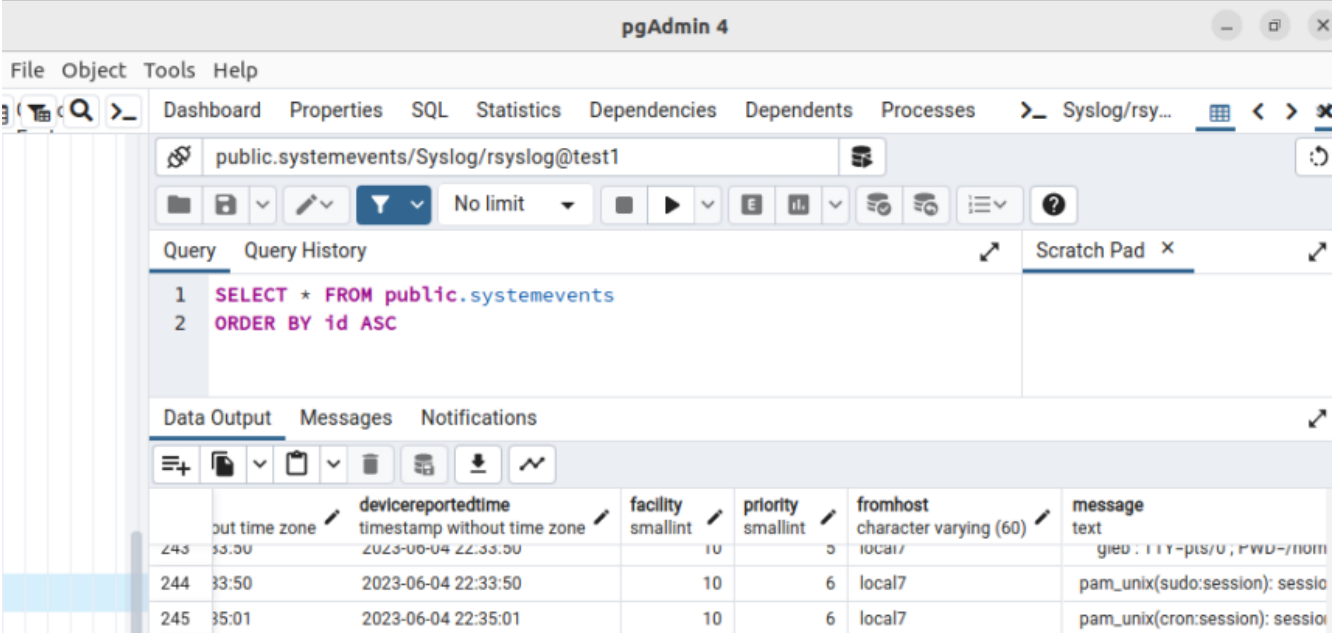
Рисунок – создание БД syslog (куда будут писаться логи) и пользователя для неё

List of databases							
Name	Owner	Encoding	Collate	Ctype	ICU Locale	Locale Provider	Access privileges
postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	
syslog	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	=Tc/postgres + postgres=CTc/postgres+ rsyslog=CTc/postgres
template0	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	=c/postgres + postgres=CTc/postgres
template1	postgres	UTF8	en_US.UTF-8	en_US.UTF-8		libc	=c/postgres + postgres=CTc/postgres

(4 rows)

Рисунок – видим что в списке БД появилась syslog

4. Проверка сохранения данных в БД syslog



The screenshot shows the pgAdmin 4 interface. The top menu bar includes File, Object, Tools, and Help. Below it is a toolbar with various icons. The main pane is divided into two sections: 'Query' and 'Query History'. The 'Query' section contains a SQL query:

```
1 SELECT * FROM public.systemevents
2 ORDER BY id ASC
```

The 'Query History' section is empty. Below the query section is the 'Data Output' tab, which displays the results of the query in a table format. The table has the following columns: id, out time zone, devicereportedtime, facility, priority, fromhost, and message. The data is as follows:

id	out time zone	devicereportedtime	facility	priority	fromhost	message
243	33:50	2023-06-04 22:33:50	10	5	local7	glibc: TTY=pts/0; PWD=/home
244	33:50	2023-06-04 22:33:50	10	6	local7	pam_unix(sudo:session): sessio
245	35:01	2023-06-04 22:35:01	10	6	local7	pam_unix(cron:session): sessio

Рисунок - видим что при запросе отображаются логи от rsyslog