Отчет по лабораторной работе 7

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

В рамках этой лабораторной работы требуется выполнить операции по управлению сервисом ведения логов rsyslogd.

2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигура- ции мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с journalctl (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с journald (см. раздел 7.4.4).

3 Выполнение лабораторной работы

Сначала я открыл для чтения файл `/var/log/messages`. Затем, сделав в другом терминале действия, я увидел, как сообщения об этих действиях были добавлены в конец этого файла.

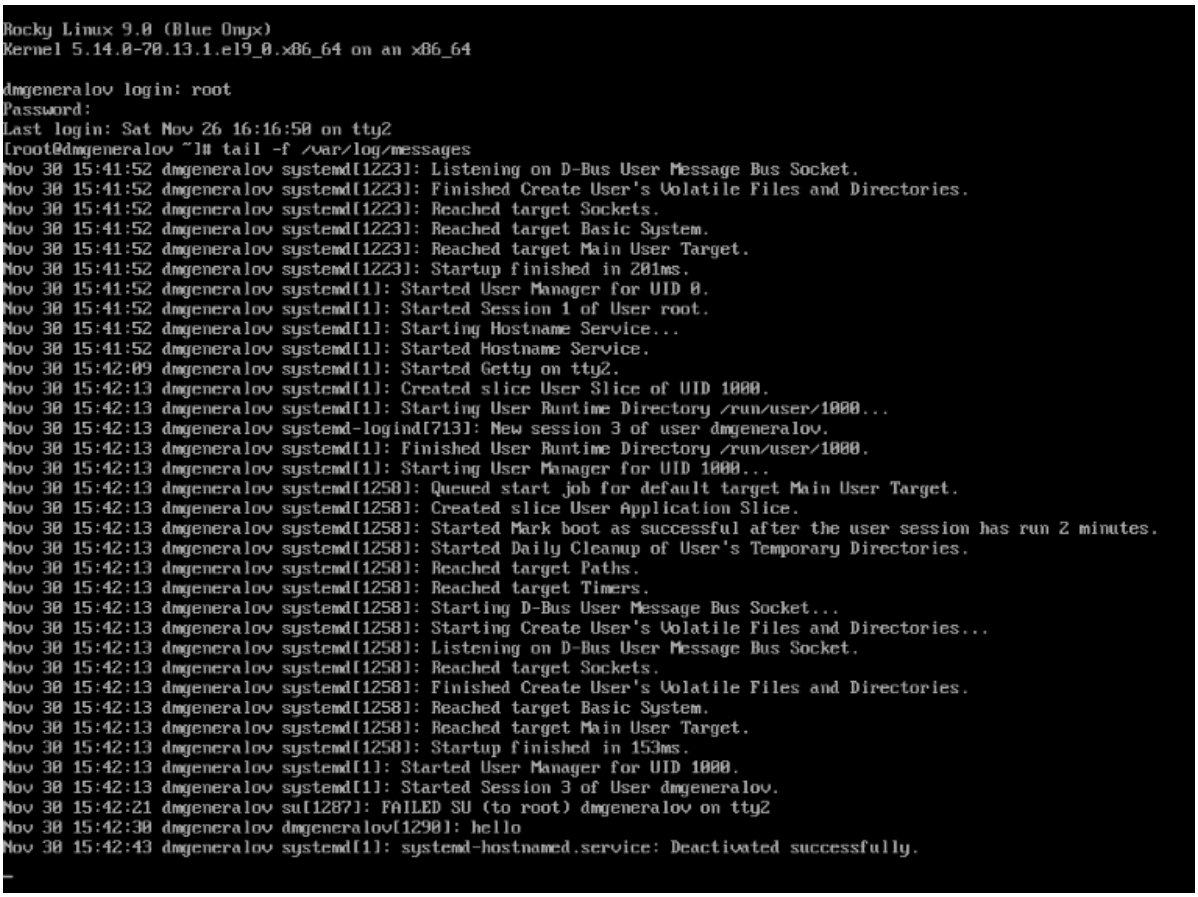

Рис. 3.1: messages

Аналогично, в файле `/var/log/secure` хранятся сообщения о событиях, связан-

ных с безопасностью: например, о попытках входа в систему или использовании команды su.

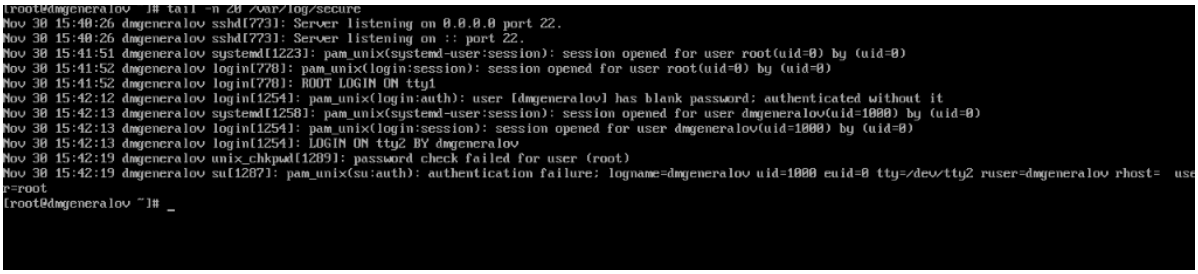

Рис. 3.2: secure

Можно настроить службы, чтобы они записывали свои события в системный лог. Например, веб-сервер `httpd` по умолчанию записывает свои события в файл `/var/log/httpd/access_log` и `/var/log/httpd/error_log`, но в настройках можно указать, чтобы он записывал их в системный лог. После этого нужно добавить в `/etc/rsyslog.d` файл, который бы описывал, что делать с записями в системный лог – в нашем случае, мы хотим сохранить их в файле `/var/log/httpd-error.log`

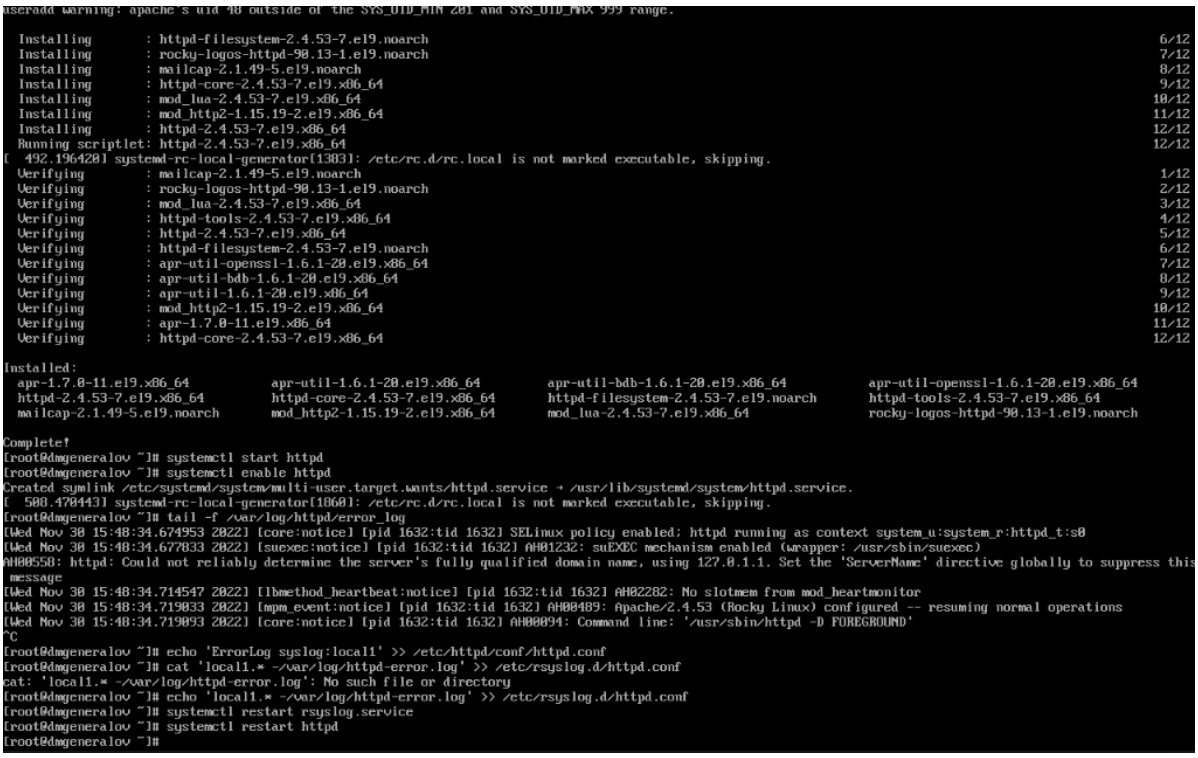

Рис. 3.3: httpd

Файлы конфигурации rsyslog описывают, какие сообщения следует записывать в какие файлы. Например, можно создать правило, которое будет сохранять все сообщения уровня debug в файл `/var/log/messages-debug`.

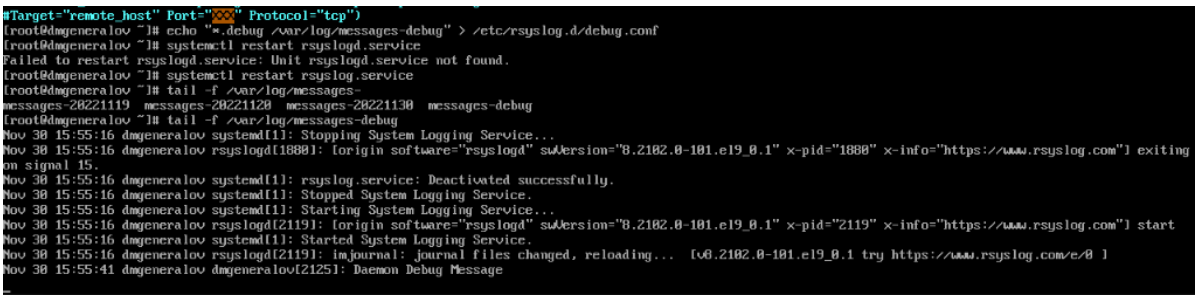

Рис. 3.4: debug

Программа journalctl позволяет просматривать журнал всех системных событий, а также фильтровать те события которые выводятся. Например, можно

следить в реальном времени за событиями, которые созданы процессом под пользователем `root` с важностью `err`.

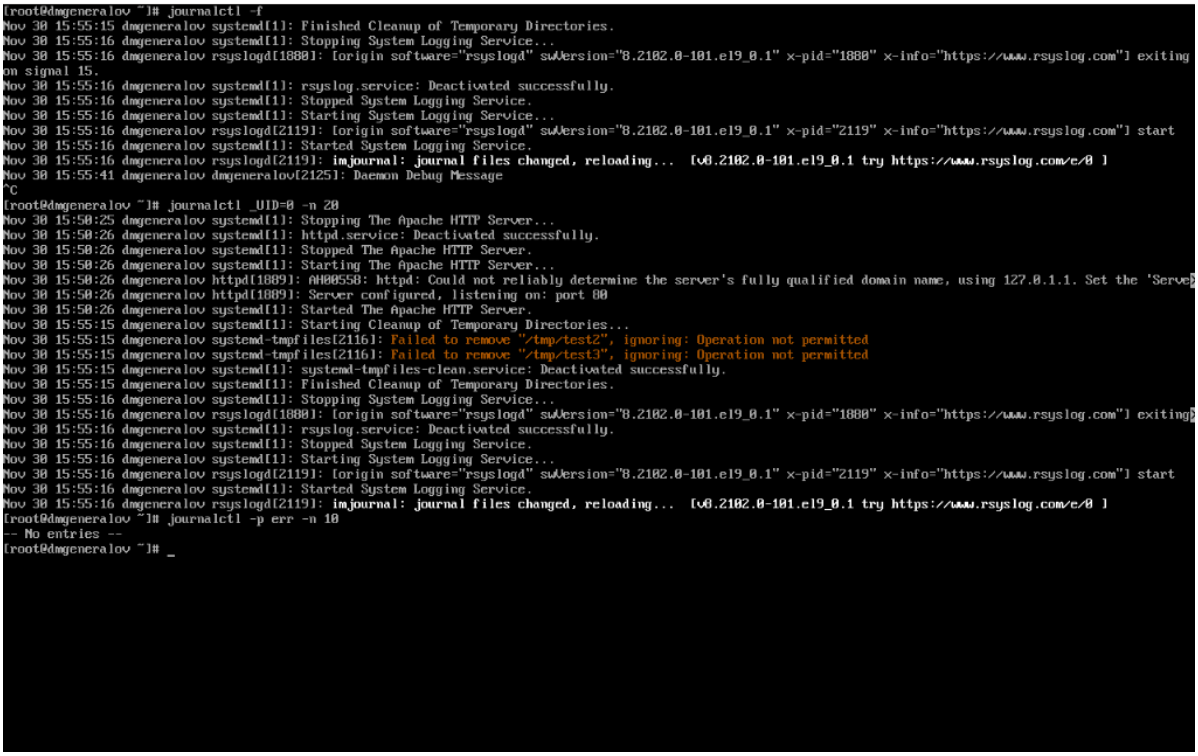

Рис. 3.5: journalctl

Можно также выделить только те сообщения, которые были добавлены со вчерашнего дня (которые, в случае этой виртуальной машины, – это сообщения начиная с загрузки системы), которые имеют важность `err`. Можно также посмотреть каждое сообщение более подробно, используя опцию `-o verbose`.

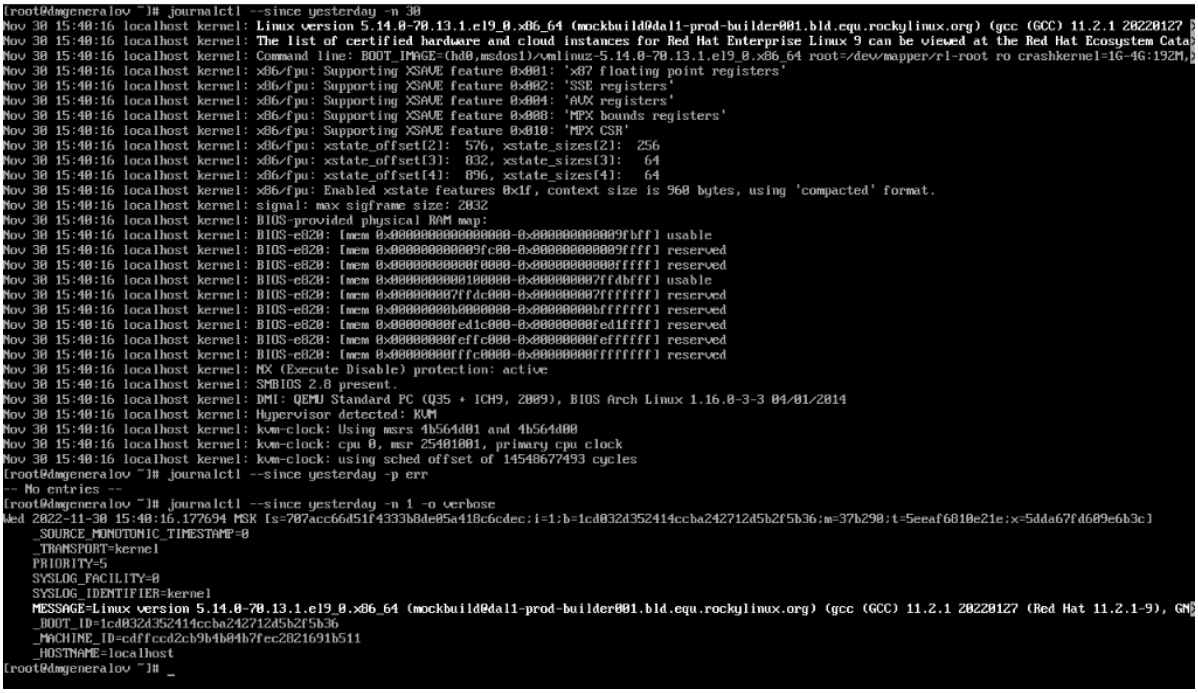

Рис. 3.6: journalctl

Наконец, можно выделить сообщения от какого-то конкретного сервиса, например, `sshd` или `httpd`.

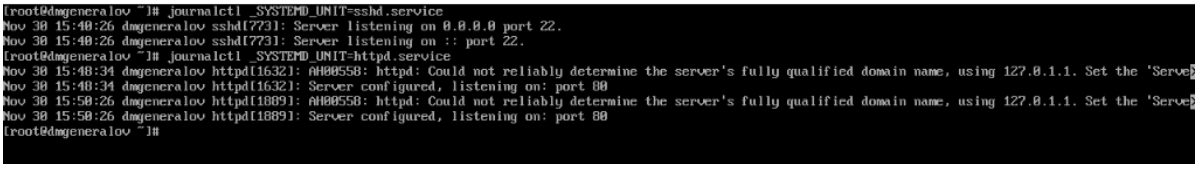

Рис. 3.7: journalctl

По умолчанию журнал journald сохраняется в памяти, но можно настроить его сохранение на диск. Для этого нужно, чтобы существовала директория `/var/log/journal`, чтобы ей владел `root:systemd-journal`, и чтобы у нее были права на чтение и запись для группы `systemd-journal`. После этого там будут храниться журналы для каждой загрузки системы.

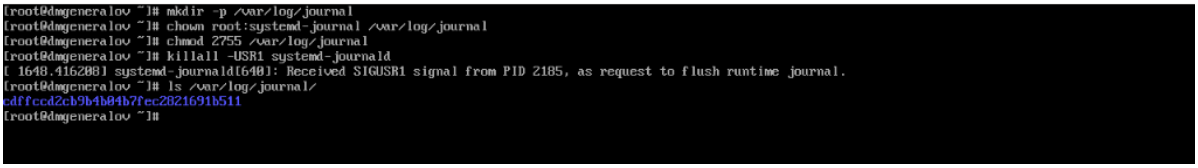

Рис. 3.8: journalctl

4 Выводы

Я получил опыт работы с rsyslogd и journald.

5 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

`/etc/rsyslog.conf`, который подключает файлы из директории `/etc/rsyslog.d/`.

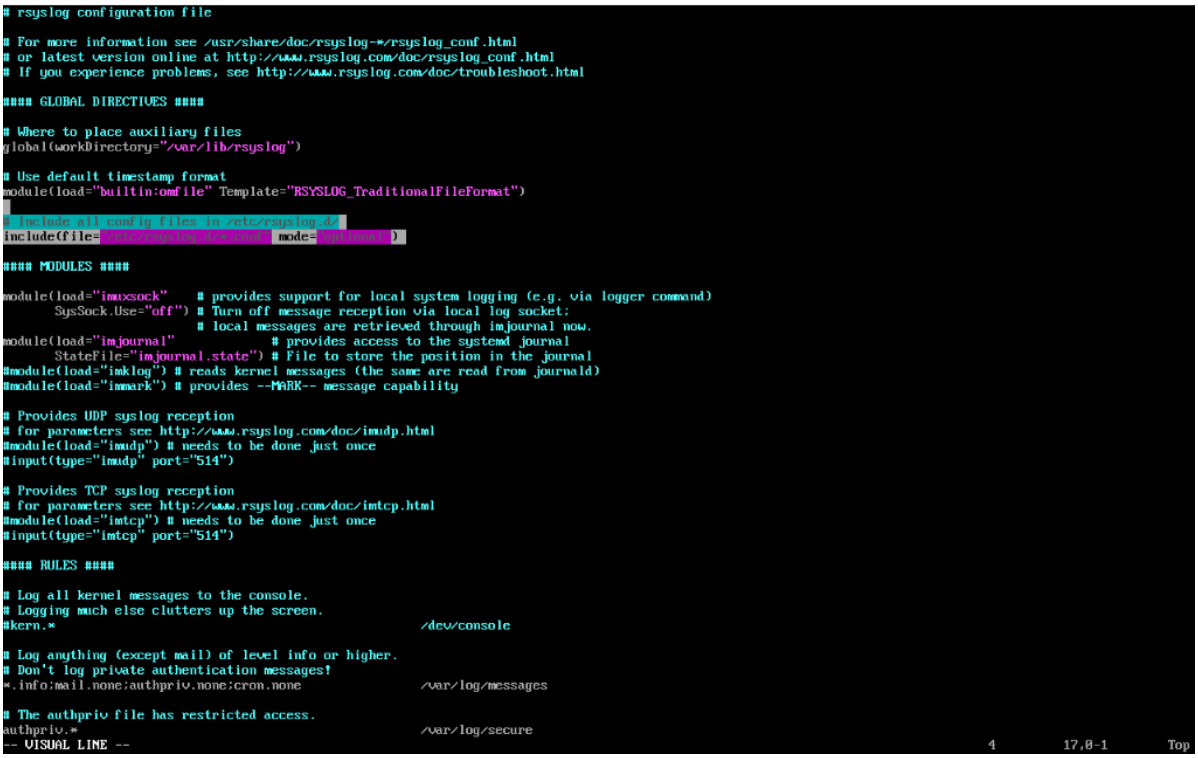

Рис. 5.1: rsyslog.conf

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутенти- фикацией?

`/var/log/secure`

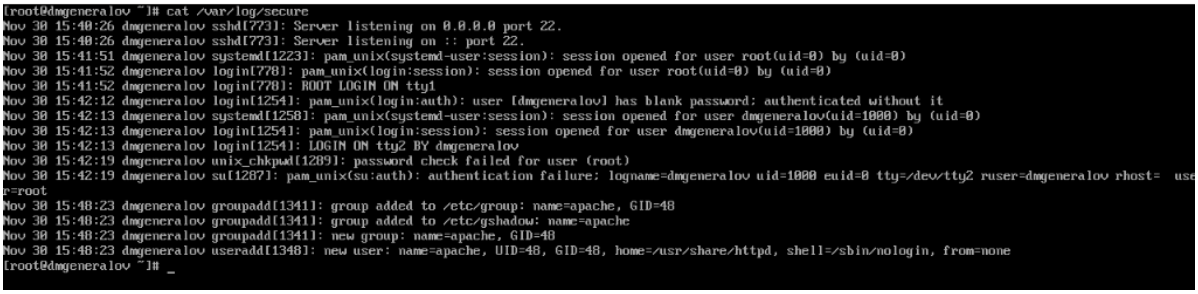

Рис. 5.2: secure

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

Одна неделя.

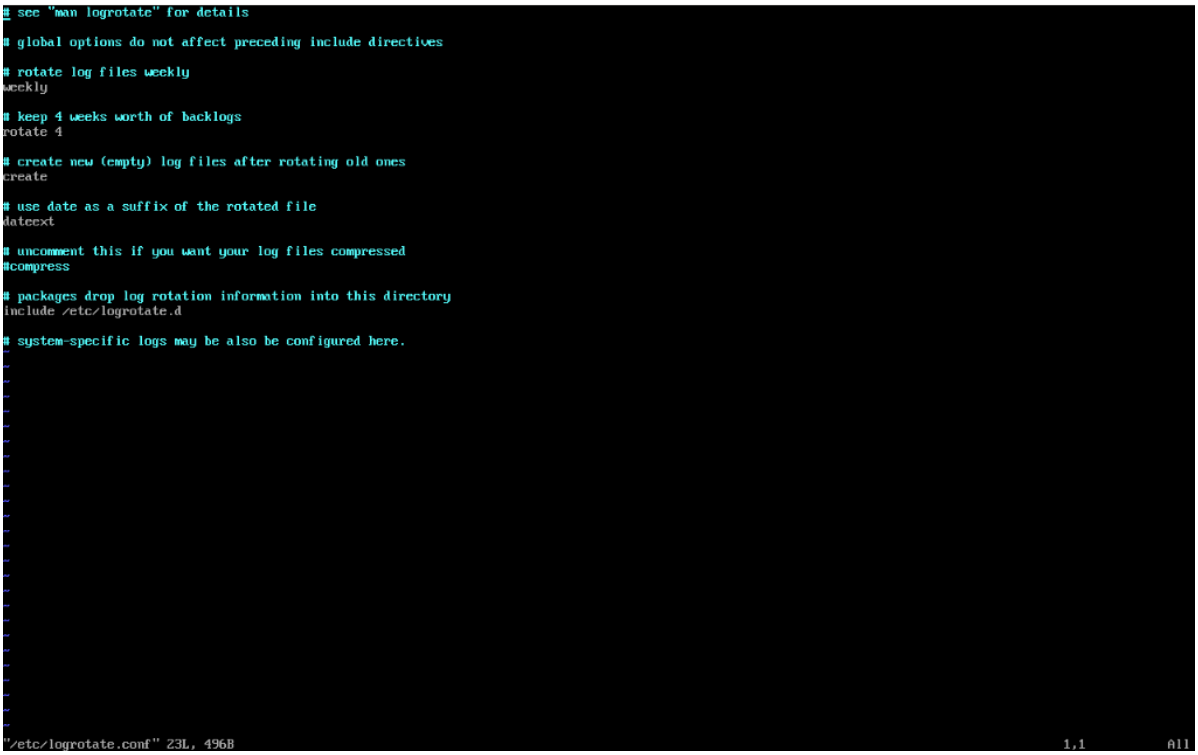

Рис. 5.3: logrotate.conf

4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

```
*.info /var/log/messages.info
```

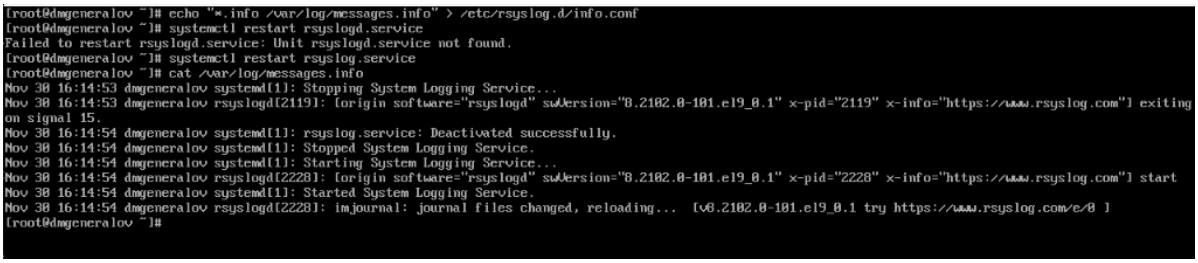

Рис. 5.4: rsyslog.conf

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

```
journalctl -f
```

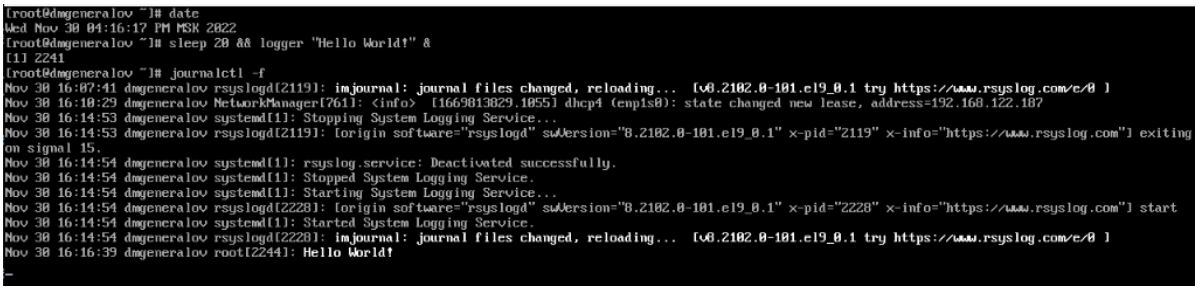

Рис. 5.5: journalctl

6. Какая команда позволяет вам видеть все сообщения журнала, которые были напи- саны для PID 1 между 9:00 и 15:00?

```
journalctl _PID=1 --since "9:00" --until "15:00"
```

7. Какая команда позволяет вам видеть сообщения journald после последней пере- загрузки системы?

```
journalctl -b
```

8. Какая процедура позволяет сделать журнал journald постоянным?

Создать директорию `/var/log/journal`, сделать ее владельцем `root:systemd-journal`, и дать права на чтение и запись для группы `systemd-journal`.

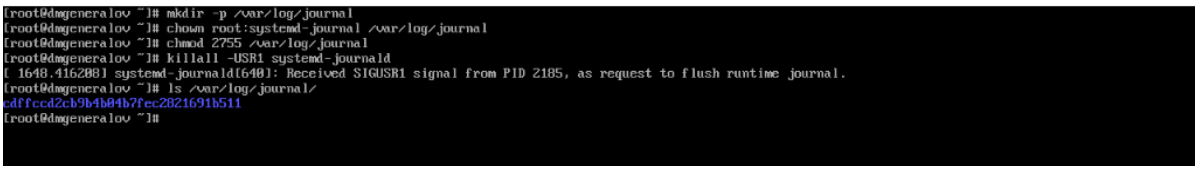

Рис. 5.6: journalctl