Лабораторная работа №7

Управление журналами событий в системе

Ко Антон Геннадьевич

Содержание

Список иллюстраций

Список таблиц

# 1 РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

## 1.1 Факультет физико-математических и естественных наук

### 1.1.1 Кафедра прикладной информатики и теории вероятностей

# 2 ОТЧЕТ

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**  
*Дисциплина: Основы администрирования операционных систем*

### 2.0.1 Студент: Ко Антон Геннадьевич

**Студ. билет №** 1132221551  
**Группа:** НПИбд-02-23

## 2.1 МОСКВА

2024 г.

## 2.2 Цель работы

Целью данной работы является получение навыков работы с журналами мониторинга различных событий в системе.

## 2.3 Выполнение работы

### 2.3.1 Мониторинг журнала системных событий в реальном времени

Для начала запустим три вкладки терминала и в каждом из них получим полномочия администратора:

su -

На второй вкладке терминала запустим мониторинг системных событий в реальном времени:

tail -f /var/log/messages

#### 2.3.1.1 В третьей вкладке терминала:

1. Вернёмся к учётной записи своего пользователя:

Ctrl + d

1. Попробуем получить полномочия администратора, но при этом вводим неправильный пароль.

Во второй вкладке терминала с мониторингом событий появится сообщение:

FAILED SU (to root) agko on pts/2

Отображаемые на экране сообщения также фиксируются в файле:

/var/log/messages

Далее, в третьей вкладке терминала введём:

logger hello

Затем возвращаемся во вторую вкладку терминала с мониторингом событий и видим сообщение, которое также будет зафиксировано в файле:

/var/log/messages

Чтобы остановить трассировку файла сообщений мониторинга реального времени, используем:

Ctrl + c

Запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов):

tail -n 20 /var/log/secure

Мы видим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды su -.

### 2.3.2 Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache:

dnf -y install httpd

После окончания процесса установки запустим веб-службу:

systemctl start httpd  
systemctl enable httpd

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы:

tail -f /var/log/httpd/error\_log

Чтобы закрыть трассировку файла журнала, используем:

Ctrl + c

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавляем строку:

ErrorLog syslog:local1

Затем создаём файл мониторинга событий веб-службы:

cd /etc/rsyslog.d  
  
touch httpd.conf

Открываем его на редактирование и прописываем:

local1.\* - /var/log/httpd-error.log

Перезагружаем конфигурацию rsyslogd и веб-службу:

systemctl restart rsyslog.service  
systemctl restart httpd

### 2.3.3 Создание файла конфигурации для мониторинга отладочной информации

cd /etc/rsyslog.d  
  
touch debug.conf  
  
echo "\*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf

Перезапускаем rsyslogd:

systemctl restart rsyslog.service

Запускаем мониторинг отладочной информации:

tail -f /var/log/messages-debug

В третьей вкладке терминала введём:

logger -p daemon.debug "Daemon Debug Message"

Чтобы закрыть трассировку файла журнала, используем:

Ctrl + c

### 2.3.4 Использование journalctl

Смотрим содержимое журнала с событиями с момента последнего запуска системы:

journalctl

Просмотр журнала без использования пейджера:

journalctl --no-pager

Режим просмотра журнала в реальном времени:

journalctl -f

Прерывание просмотра:

Ctrl + c

Просмотр событий для UID 0:

journalctl \_UID=0

Отображение последних 20 строк журнала:

journalctl -n 20

Просмотр только сообщений об ошибках:

journalctl -p err

Просмотр сообщений с ошибками со вчерашнего дня:

journalctl --since yesterday -p err

Просмотр дополнительной информации о модуле sshd:

journalctl \_SYSTEMD\_UNIT=sshd.service

### 2.3.5 Постоянный журнал journald

su -  
mkdir -p /var/log/journal  
chown root:systemd-journal /var/log/journal  
chmod 2755 /var/log/journal  
killall -USR1 systemd-journald  
journalctl -b

## 2.4 Ответы на контрольные вопросы:

1. **Какой файл используется для настройки rsyslogd?**  
   /etc/rsyslog.conf
2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**  
   /var/log/secure
3. **Сколько времени потребуется для ротации файлов журналов по умолчанию?**  
   *Неделя*
4. **Как записать все сообщения с приоритетом info в файл /var/log/messages.info?**  
   info.\* - /var/log/messages.info
5. **Какая команда позволяет видеть сообщения журнала в режиме реального времени?**  
   tail -f /var/log/messages
6. **Какая команда позволяет видеть все сообщения журнала для PID 1 между 9:00 и 15:00?**  
   journalctl \_PID=1 --since "2022-02-01 09:00:00" --until "2022-02-01 15:00:00"
7. **Какая команда позволяет видеть сообщения journald после последней перезагрузки системы?**  
   journalctl -b

## 2.5 Вывод

В ходе выполнения лабораторной работы были получены навыки работы с журналами мониторинга различных событий в системе.