Лабораторная работа №7

Упарвление журналами событий в системе

Перфилов Александр Константинович | группа НПИбд 03-24

Содержание

# 1. Цель работы

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

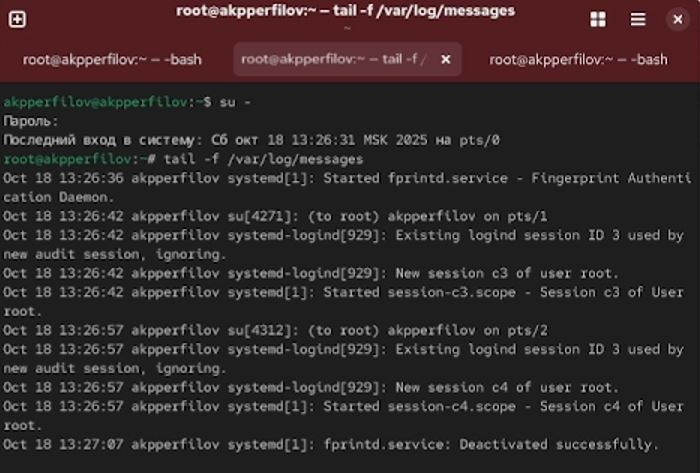
# 2. Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации 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

## 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 (рис. [**fig:001?**]).



Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.

В третьей вкладке терминала вернёмся к учётной записи своего пользователя (нажав Ctrl + d) и попробуем получить полномочия администратора, но при этом вводим неправильный пароль (рис. [**fig:002?**]).

|  |
| --- |
| Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора. |

Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора.

Обратим внимание, что во второй вкладке терминала с мониторингом событий появилось сообщение «FAILED SU (to root) mobihzova on pts/2». Отображаемые на экране сообщения также фиксируются в файле /var/log/messages (рис. [**fig:003?**]).

|  |
| --- |
| Новое сообщение в мониторинге событий во второй вкладке терминала. |

Новое сообщение в мониторинге событий во второй вкладке терминала.

В третьей вкладке терминала из оболочки пользователя введём: logger hello (рис. [**fig:004?**]).

|  |
| --- |
| Ввод в третьей вкладке терминала. |

Ввод в третьей вкладке терминала.

Далее возвращаемся во вторую вкладку терминала с мониторингом событий и видим сообщение, которое также будет зафиксировано в файле /var/log/messages («hello»). В этой же вкладке терминала с мониторингом остановим трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем 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 - (рис. [**fig:005?**]).

|  |
| --- |
| Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга сообщений безопасности (последние 20 строк). |

Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга сообщений безопасности (последние 20 строк).

## 3.2 Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache: dnf -y install httpd (рис. [**fig:006?**]).

|  |
| --- |
| Установка Apache. |

Установка Apache.

После окончания процесса установки запустим веб-службу: systemctl start httpd и systemctl enable httpd (рис. [**fig:007?**]).

|  |
| --- |
| Запуск веб-службы. |

Запуск веб-службы.

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 (рис. [**fig:008?**]).

|  |
| --- |
| Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала. |

Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала.

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавляем следующую строку: ErrorLog syslog:local (рис. [**fig:009?**], рис. [**fig:010?**]).

Здесь local0 — local7 — это «настраиваемые» средства (объекты), которые syslog предоставляет пользователю для регистрации событий приложения в системном журнале.

|  |
| --- |
| Получение в третьей вкладке терминала полномочия администратора, открытие файла httpd.conf на редактирование. |

Получение в третьей вкладке терминала полномочия администратора, открытие файла httpd.conf на редактирование.

|  |
| --- |
| Добавление строки в файл и сохранение. |

Добавление строки в файл и сохранение.

В каталоге /etc/rsyslog.d создаём файл мониторинга событий веб-службы:

cd /etc/rsyslog.d touch httpd.conf

Открыв его на редактирование, пропишем в нём local1.\* -/var/log/httpd-error.log (Рис. 2.7). Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpderror.log (рис. [**fig:011?**], рис. [**fig:012?**]).

|  |
| --- |
| Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование. |

Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование.

|  |
| --- |
| Добавление строки в файл и сохранение. |

Добавление строки в файл и сохранение.

Перейдём в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу:

systemctl restart rsyslog.service systemctl restart httpd

Все сообщения об ошибках веб-службы теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени, используя команду tail с соответствующими параметрами, или непосредственно просматривая указанный файл. (рис. [**fig:013?**]).

|  |
| --- |
| Открытие первой вкладки терминала и перезагрузка конфигурации rsyslogd и веб-службы. |

Открытие первой вкладки терминала и перезагрузка конфигурации rsyslogd и веб-службы.

В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации:

cd /etc/rsyslog.d touch debug.conf

В этом же терминале вводим: echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf (рис. [**fig:014?**]).

|  |
| --- |
| Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки. |

Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.

В первой вкладке терминала снова перезапустим rsyslogd: systemctl restart rsyslog.service (рис. [**fig:015?**]).

|  |
| --- |
| Открытие первой вкладки терминала и перезапуск rsyslogd. |

Открытие первой вкладки терминала и перезапуск rsyslogd.

Во второй вкладке терминала запустим мониторинг отладочной информации: tail -f /var/log/messages-debug (рис. [**fig:016?**]).

|  |
| --- |
| Открытие второй вкладки терминала и запуск мониторинга отладочной информации. |

Открытие второй вкладки терминала и запуск мониторинга отладочной информации.

В третьей вкладке терминала введём: logger -p daemon.debug “Daemon Debug Message” (рис. [**fig:017?**]).

|  |
| --- |
| Открытие третьей вкладки терминала и ввод команды. |

Открытие третьей вкладки терминала и ввод команды.

В терминале с мониторингом посмотрим сообщение отладки. Чтобы закрыть трассировку файла журнала, используем Ctrl + c (рис. [**fig:018?**]).

|  |
| --- |
| Просмотр сообщения отладки и закрытие трассировки файла журнала. |

Просмотр сообщения отладки и закрытие трассировки файла журнала.

## 3.3 Использование journalctl

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: journalctl. Для пролистывания журнала можно использовать или Enter (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра используется q (рис. [**fig:019?**]).

|  |
| --- |
| Открытие второй вкладки терминала и просмотр содержимого журнала с событиями с момента последнего запуска системы. |

Открытие второй вкладки терминала и просмотр содержимого журнала с событиями с момента последнего запуска системы.

Просмотрим содержимое журнала без использования пейджера: journalctl – no-pager (рис. [**fig:020?**]).

|  |
| --- |
| Просмотр содержимого журнала без использования пейджера. |

Просмотр содержимого журнала без использования пейджера.

Режим просмотра журнала в реальном времени: journalctl -f. Для прерывания просмотра: Ctrl + c (рис. [**fig:021?**]).

|  |
| --- |
| Режим просмотра журнала в реальном времени и прерывание просмотра. |

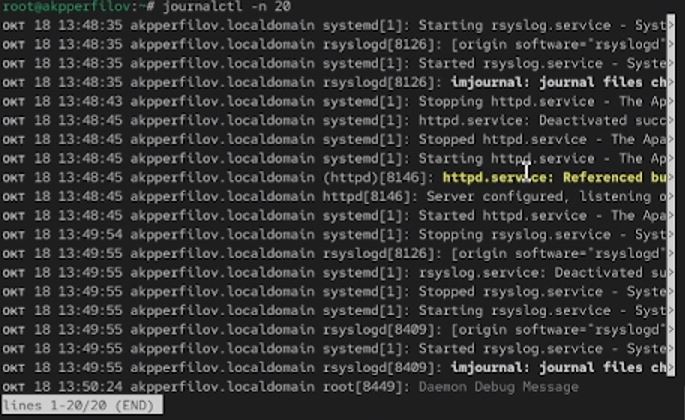
Режим просмотра журнала в реальном времени и прерывание просмотра.

Просмотрим события для UID0: journalctl \_UID=0 (рис. [**fig:022?**]).

|  |
| --- |
| Просмотр событий для UID0. |

Просмотр событий для UID0.

Для отображения последних 20 строк журнала введём: journalctl -n 20 (рис. [**fig:023?**]).



Отображение последних 20 строк журнала.

Для просмотра только сообщений об ошибках введём: journalctl -p err (рис. [**fig:024?**]).

|  |
| --- |
| Просмотр только сообщений об ошибках. |

Просмотр только сообщений об ошибках.

Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, мы можем использовать параметры –since и – until. Обе опции принимают параметр времени в формате YYYY-MM-DD hh:mm:ss Кроме того, мы можем использовать yesterday, today и tomorrow в качестве параметров. Например, для просмотра всех сообщений со вчерашнего дня введём: journalctl –since yesterday (рис. [**fig:025?**]).

|  |
| --- |
| Просмотр всех сообщений со вчерашнего дня. |

Просмотр всех сообщений со вчерашнего дня.

Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используем: journalctl –since yesterday - p err, а если нам нужна детальная информация, то используем: journalctl -o verbose (рис. [**fig:026?**]).

|  |
| --- |
| Просмотр сообщений с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Просмотр детальной информации. |

Просмотр сообщений с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Просмотр детальной информации.

Для просмотра дополнительной информации о модуле sshd введём: journalctl \_SYSTEMD\_UNIT=sshd.service (рис. [**fig:027?**]).

|  |
| --- |
| Просмотр дополнительной информации о модуле sshd. |

Просмотр дополнительной информации о модуле sshd.

## 3.4 Постоянный журнал journald

Запустим терминал и получим полномочия администратора: su -. Далее создадим каталог для хранения записей журнала: mkdir -p /var/log/journal и скорректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию:

chown root:systemd-journal /var/log/journal chmod 2755 /var/log/journal

Для принятия изменений необходимо использовать команду: killall -USR1 systemd-journald. Журнал systemd теперь постоянный. Если мы хотим видеть сообщения журнала с момента последней перезагрузки, используем: journalctl -b (рис. [**fig:028?**]).

|  |
| --- |
| Запуск терминала и получение полномочий администратора, создание каталог для хранения записей журнала, корректировка прав доступа для каталога /var/log/journal, принятия изменений, просмотр сообщения журнала с момента последней перезагрузки. |

Запуск терминала и получение полномочий администратора, создание каталог для хранения записей журнала, корректировка прав доступа для каталога /var/log/journal, принятия изменений, просмотр сообщения журнала с момента последней перезагрузки.

## 3.5 Ответы на контрольные вопросы

1. Какой файл используется для настройки rsyslogd? /etc/rsyslog.conf

1. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? /var/log/secure

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

1. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log messages.info? info.\* - /var/log/messages.info
2. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени? tail -f /var/log/messages

1. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны 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”
2. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы? journalctl - b
3. Какая процедура позволяет сделать журнал journald постоянным?

Запустите терминал и получите полномочия администратора: su – Создайте каталог для хранения записей журнала: mkdir -p /var/log/journal. Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию:

chown root:systemd-journal /var/log/journal chmod 2755 /var/log/journal

Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: killall -USR1 systemd-journald

# 4. Выводы

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