Лабораторная работа № 7. Управление журналами событий в системе

Дисциплина: основы администрирования операционных систем

Жукова Арина Александровна

Содержание

# 1 Цель работы

Получить навыки 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 Теоретическое введение

## 3.1 Основные файлы журналов

В системах на базе Unix/Linux важное место при администрировании занимает отслеживание системных событий (и в частности возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журналирование системных событий заключается в фиксировании с помощью сокета syslog в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы. Обычно лог-файлы располагаются в каталоге /var/log: – /var/log/messages — общий файл журнала, в который записывается большинство сообщений системы (наиболее часто используемый файл журнала); – /var/log/dmesg — журнал сообщений ядра системы; – /var/log/secure — журнал сообщений, связанных с аутентификацией в системе; – /var/log/boot.log — журнал сообщений, связанных с запуском системы; – /var/log/audit/audit.log — журнал сообщений аудита (например, в него записываются сообщения SELinux); – /var/log/maillog — журналы сообщений, связанных с почтовой службой; – /var/log/samba — журналы сообщений службы samba (samba по умолчанию не управляется через rsyslogd); – /var/log/sssd — журналы сообщений службы sssd; – /var/log/cups — журналы службы печати cups; – /var/log/httpd/ — каталог с журналами веб-службы Apache (Apache записывает сообщения в эти файлы напрямую, а не через rsyslog).

## 3.2 Категории rsyslogd

Сообщения в rsyslogd относятся к той или иной категории. Категории сообщений и их приоритетность обеспечивают иерархичность системы хранения журналов сообщений системы и скорость реагирования на возникновение критичных для её работы событий. Выделяют следующие категории: – auth/authpriv — сообщения, связанные с аутентификацией; – cron — сообщения, генерируемые службой crond; – daemon — сообщения от неспецифицированных демонов; – kern — сообщения ядра; – lpr — сообщения, созданные через устаревшую систему печати lpd; – mail — сообщения, связанные с электронной почтой; – mark — специальный объект, который можно использовать для записи маркера; – news — сообщения, созданные системой новостей NNTP; – security — то же, что и auth/authpriv (не нужно использовать); – syslog — сообщения, созданные системой syslog; – user — сообщения, сгенерированные в пространстве пользователя; – uucp — сообщения, созданные устаревшей системой UUCP; – local0-7 — сообщения, генерируемые службами, которые настроены любым из локальных объектов.

## 3.3 Приоритеты rsyslogd

По важности (уровню опасности) сообщения разделяются по приоритетам: – debug — отладочные сообщения (уровень опасности 7); – info — информационные сообщения о нормальной работе (уровень опасности 6); – notice— используется для информационных сообщений об элементах, которые могут стать проблемой позже (уровень опасности 5); – warning/warn — что-то происходит, но пока нет реальной ошибки (уровень опасности 4); – err/error — некритическая ошибка (уровень опасности 3); – crit — критическая ошибка (уровень опасности 2); – alert — используется, когда доступность службы под угрозой (уровень опасности 1); – emerg/panic— сообщение генерируется, когда служба не доступна (уровень опасности 0).

# 4 Выполнение лабораторной работы

## 4.1 Мониторинг журнала системных событий в реальном времени

1. Запустила три вкладки терминала и в каждом из них получила полномочия администратора (рис. 1).

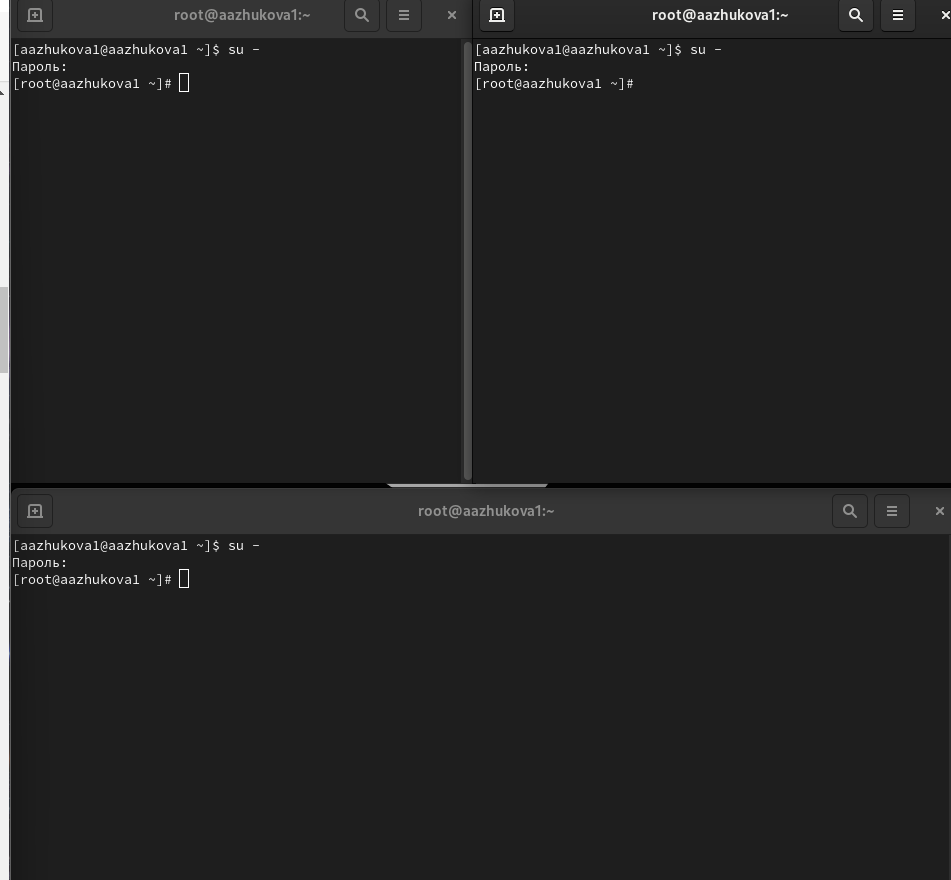


Рис. 1: Запуск трех вкладок

1. На второй вкладке терминала запустила мониторинг системных событий в реальном времени (рис. 2).

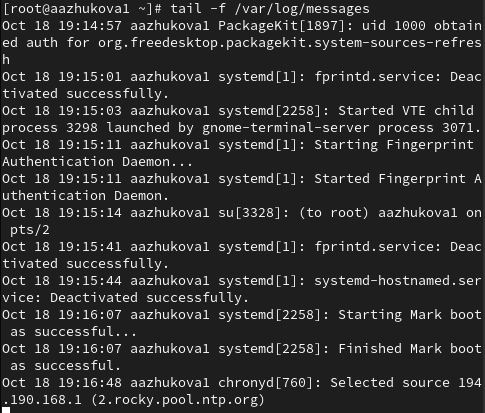


Рис. 2: Мониторинг системных событий

1. В третьей вкладке терминала вернулась к учётной записи своего пользователя (достаточно нажать Ctrl + d) и попыталась получить полномочия администратора, но ввела неправильный пароль. Обратила внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username». Отображаемые на экране сообщения также фиксировались в файле /var/log/messages (рис. 3).

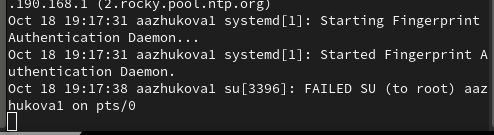


Рис. 3: Отображение сообщения

1. В третьей вкладке терминала из оболочки пользователя ввела logger hello. Во второй вкладке терминала с мониторингом увидела сообщение, которое также было зафиксировано в файле /var/log/messages (рис. 4).

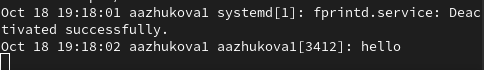


Рис. 4: Вывод сообщения

1. Во второй вкладке терминала с мониторингом остановила трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем запустила мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов) при помощи tail -n 20 /var/log/secure. Увидела сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды su (рис. 5).

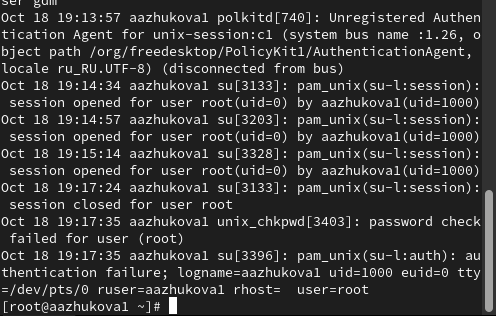


Рис. 5: Вывод сообщений об ошибках

## 4.2 Изменение правил rsyslog.conf

1. В первой вкладке терминала установила Apache (рис. 6).

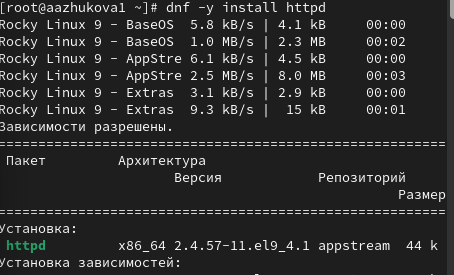


Рис. 6: Установка Apache

1. После окончания процесса установки запустила веб-службу (рис. 7).

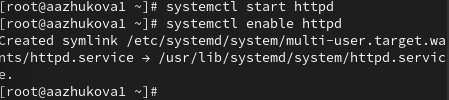


Рис. 7: Запуск веб-службы

1. Во второй вкладке терминала посмотрела журнал сообщений об ошибках веб-службы. Чтобы закрыть трассировку файла журнала, использовала Ctrl + c (рис. 8).

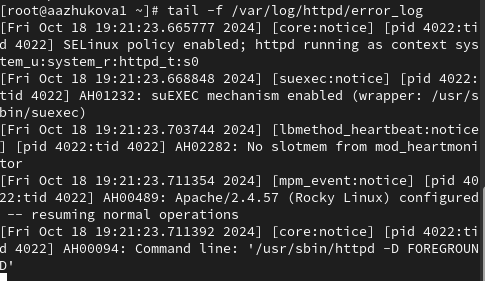


Рис. 8: Журнал сообщений об ошибках

1. В третьей вкладке терминала получила полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавила следующую строку: ErrorLog syslog:local1 (рис. 9).

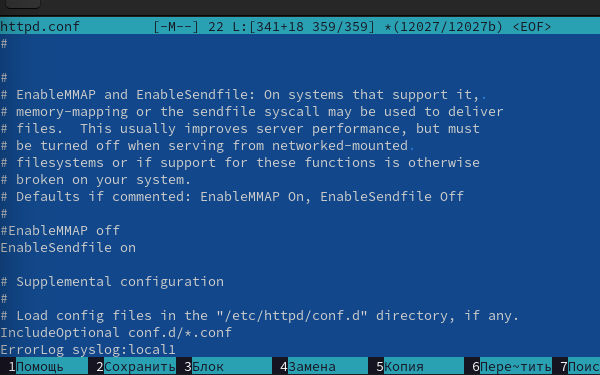


Рис. 9: Добавление строки

1. В каталоге /etc/rsyslog.d создала файл мониторинга событий веб-службы (рис. 10).

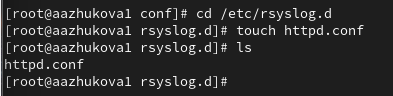


Рис. 10: Создание файла

1. Открыв его на редактирование, прописала в нём local1.\* -/var/log/httpd-error.log(рис. 11).



Рис. 11: Редактирование файла

Эта строка позволила отправлять все сообщения, получаемые для объекта local1 (который теперь использовался службой httpd), в файл /var/log/httpd-error.log.

1. Перешла в первую вкладку терминала и перезагрузила конфигурацию rsyslogd и веб-службу (рис. 12).

Перезагрузка конфигурации rsyslogd и веб-службу

Рис. 12: Перезагрузка конфигурации rsyslogd и веб-службу

Все сообщения об ошибках веб-службы теперь были 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.

1. В третьей вкладке терминала создала отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале ввела echo "\*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf (рис. 13 - 15).

Редактирование файла

Рис. 13: Редактирование файла

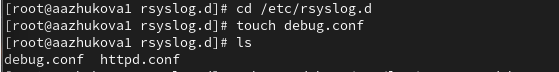


Рис. 14: Создание файла

Внесение изменений

Рис. 15: Внесение изменений

1. В первой вкладке терминала снова перезапустила rsyslogd. Во второй вкладке терминала запустила мониторинг отладочной информации. В третьей вкладке терминала ввела: logger -p daemon.debug "Daemon Debug Message" (рис. 16).

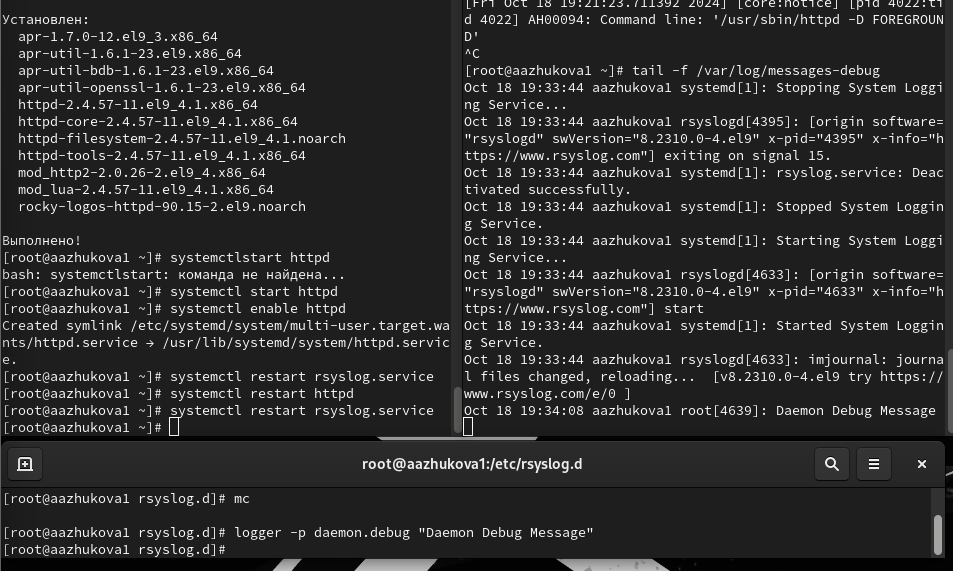


Рис. 16: Терминалы

В терминале с мониторингом посмотрела сообщение отладки. Чтобы закрыть трассировку файла журнала, использовала Ctrl + c.

## 4.3 Использование journalctl

1. Во второй вкладке терминала посмотрела содержимое журнала с событиями с момента последнего запуска системы. Для пролистывания журнала использовала или Enter (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра использовала q (рис. 17).

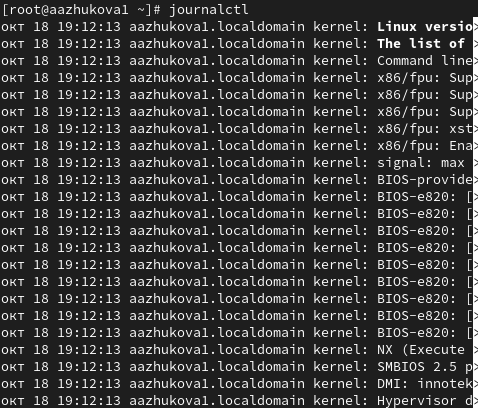


Рис. 17: Журнал событий

1. Просмотр содержимого журнала без использования пейджера (рис. 18).

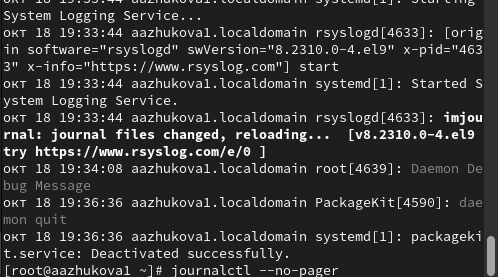


Рис. 18: Просмотр журнала без пейджера

1. Режим просмотра журнала в реальном времени journalctl -f (рис. 19).

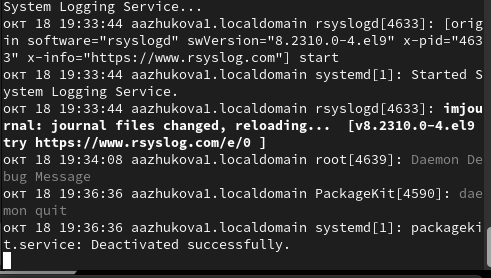


Рис. 19: Просмотр журнала в реальном времени

Использовала Ctrl + c для прерывания просмотра.

1. Просмотрела события для UID0 (рис. 20).

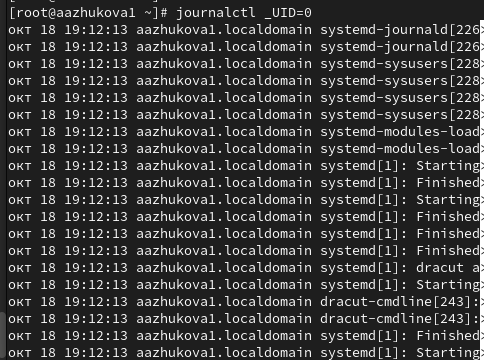


Рис. 20: Просмотр событий

1. Для отображения последних 20 строк журнала ввела journalctl -n 20 (рис. 21).

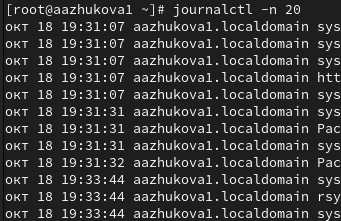


Рис. 21: Отображение последних 20 строк

1. Для просмотра только сообщений об ошибках ввела journalctl -p err (рис. 22).

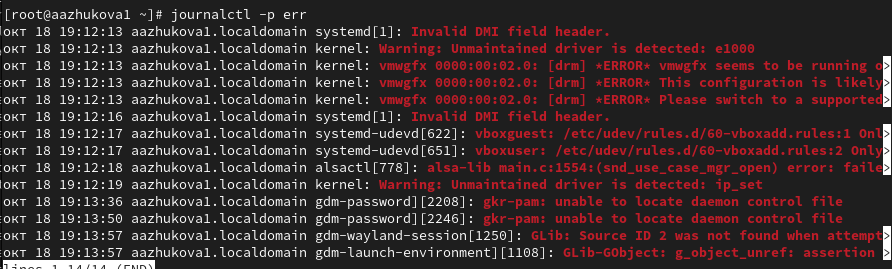


Рис. 22: Сообщения об ошибках

1. Для просмотра всех сообщений со вчерашнего дня ввела journalctl --since yesterday (рис. 23).

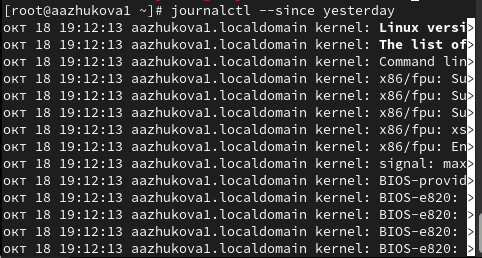


Рис. 23: Сообщения со вчерашнего дня

1. Для просмотра всех сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, использовала journalctl --since yesterday -p err (рис. 24).

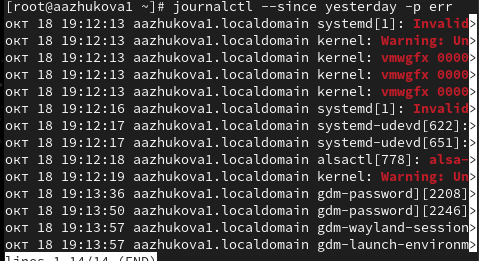


Рис. 24: Сообщения с ошибкой

1. Если нужна детальная информация, использовала journalctl -o verbose (рис. 25).

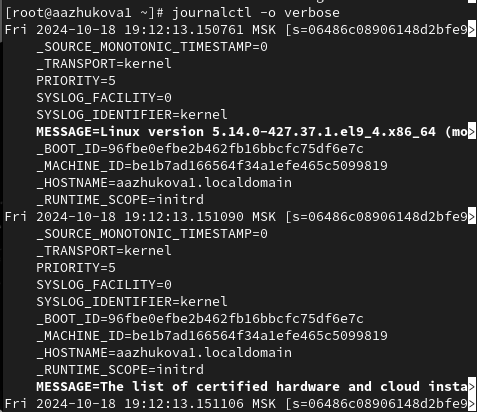


Рис. 25: Вывод детальной информации

1. Для просмотра дополнительной информации о модуле sshd ввела journalctl\_SYSTEMD\_UNIT=sshd.service (рис. 26).

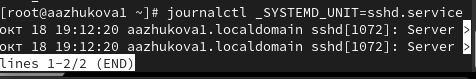


Рис. 26: Дополнительная информация о модуле

## 4.4 Постоянный журнал journald

1. Запустила терминал и получила полномочия администратора. Создала каталог для хранения записей журнала. Скорректировала права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Для принятия изменений необходимо либо перезагрузить систему (перезапустить службу systemd-journald недостаточно), либо использовать команду killall -USR1 systemd-journald (рис. 27).

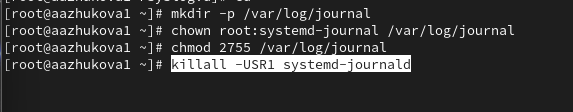


Рис. 27: Перезагрузка системы

1. Журнал systemd теперь постоянный. Для вывод сообщения журнала с момента последней перезагрузки использовала journalctl -b (рис. 28).

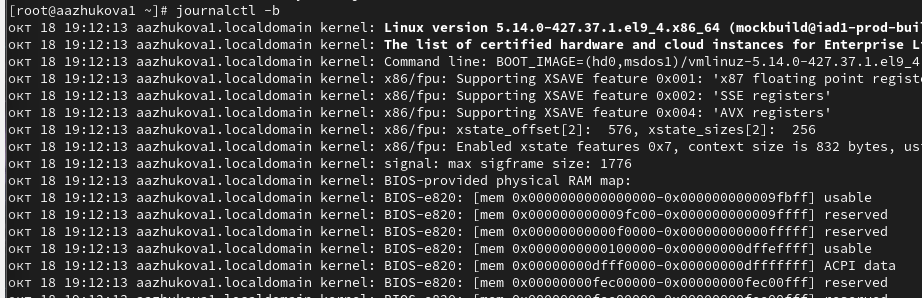


Рис. 28: Вывод сообщений

# 5 Ответы на контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

* rsyslog.conf

1. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

* auth.log

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

* По умолчанию файлы журналов будут ротироваться каждые неделю.

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

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

* journalctl -f

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

* journalctl –since ‘2023-10-26 09:00:00’ –until ‘2023-10-26 15:00:00’ \_PID=1 (замените дату на актуальную)

1. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

* journalctl -b

1. Какая процедура позволяет сделать журнал journald постоянным?
   1. Запустите терминал с правами администратора.
   2. Создайте каталог для хранения записей журнала: mkdir -p /var/log/journal
   3. Установите права доступа для каталога: chown root:systemd-journal /var/log/journal и chmod 2755 /var/log/journal
   4. Перезагрузите систему или используйте killall -USR1 systemd-journald.

# 6 Выводы

Я получила навыки работы с журналами мониторинга различных событий в системе.

# Список литературы

1. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: http: //wiki.opennet.ru/Systemd.
2. Емельянов А. Управление логгированием в systemd. — 2015. — URL: https://blog. selectel.ru/upravlenie-loggirovaniem-v-systemd/.
3. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
4. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017.
5. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.