

Шаблон отчёта по лабораторной работе

Простейший вариант

Дмитрий Сергеевич Кулябов

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	12
	Список литературы	13

Список иллюстраций

3.1	терминалы	7
3.2	журнал каталога /var/log/messages	8
3.3	выход из режима администратора	8
3.4	неправильный пароль	9
3.5	сообщение о ошибке	9
3.6	logger hello	10
3.7	сообщение hello	10
3.8	завершение журнала	11
3.9	мониторинг сообщений безопасности	11
3.10	Название	11

Список таблиц

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 .
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
3. Продемонстрируйте навыки работы с `journalctl`.
4. Продемонстрируйте навыки работы с `journal`.

3 Выполнение лабораторной работы

Сначала я открыл 3 терминала под пользователя root (рис. 3.1).

`su -`

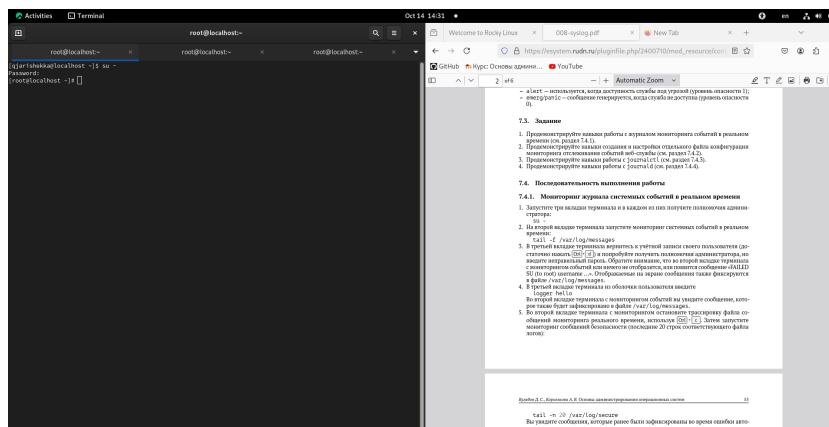


Рис. 3.1: терминалы

Потом во втором терминале я выполнил команду `tail` чтобы смотреть журнал в каталоге `/var/log/messages` (рис. 3.2).

`tail -f /var/log/messages`

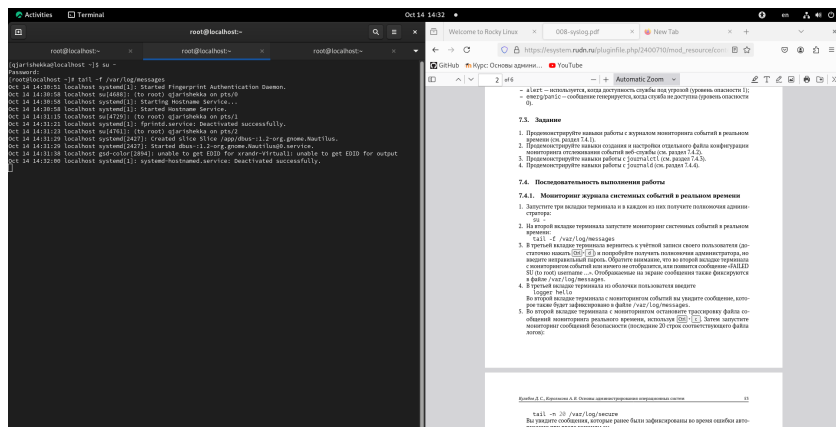


Рис. 3.2: журнал каталога /var/log/messages

Дальше в третьем терминале я вышел из режима администратора нажав клавиши Ctrl+d (рис. 3.3).

Ctrl + d

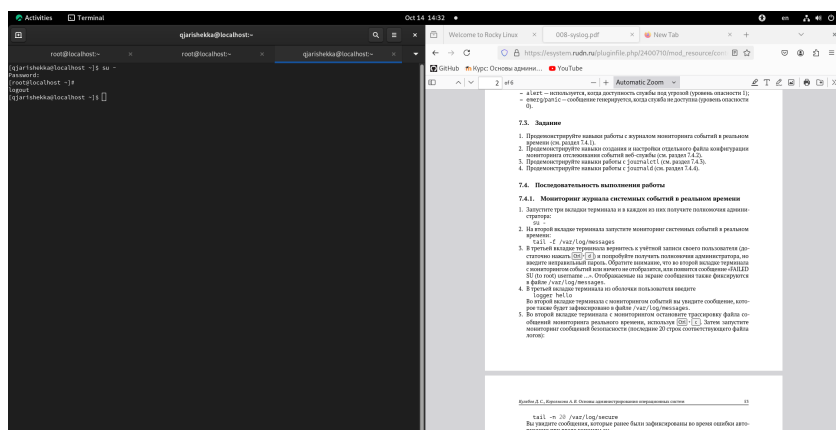


Рис. 3.3: выход из режима администратора

Затем я попытался входить в режим суперпользователя но с неправильным паролем не удаваясь (рис. 3.4).

su -
asdfsadlkfj

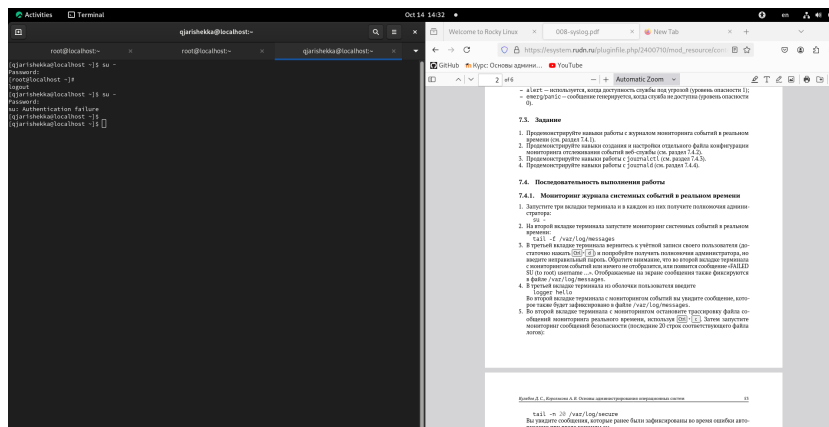


Рис. 3.4: неправильный пароль

Потом я вернулся в первую вкладку и там я смог смотреть сообщение “Failed su (to root) username...”(рис. 3.5).

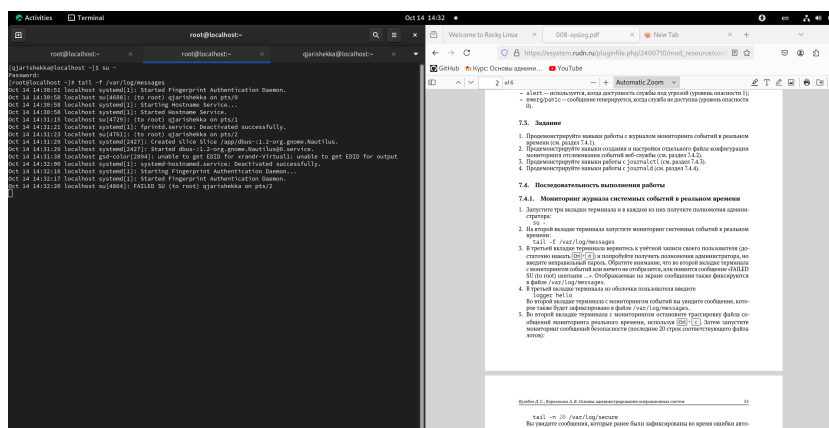


Рис. 3.5: сообщение о ошибке

Дальше я выполнил следующую команду (рис. 3.6):

logger hello

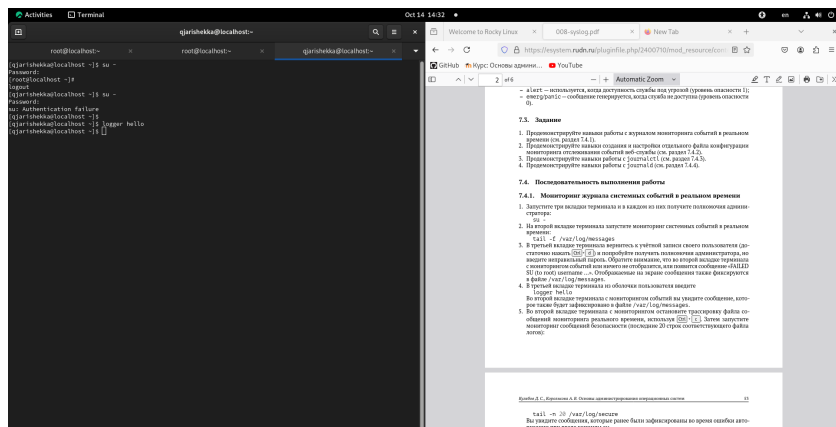


Рис. 3.6: logger hello

Тогда когда я вернулся во вторую вкладку там появились сообщение “hello” (рис. 3.7).

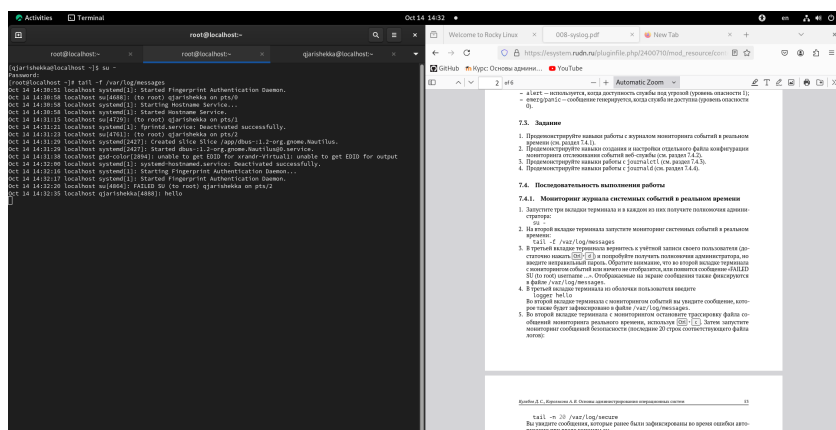


Рис. 3.7: сообщение hello

Потом я завершил просмотр журнала (рис. 3.8).

Ctrl + c

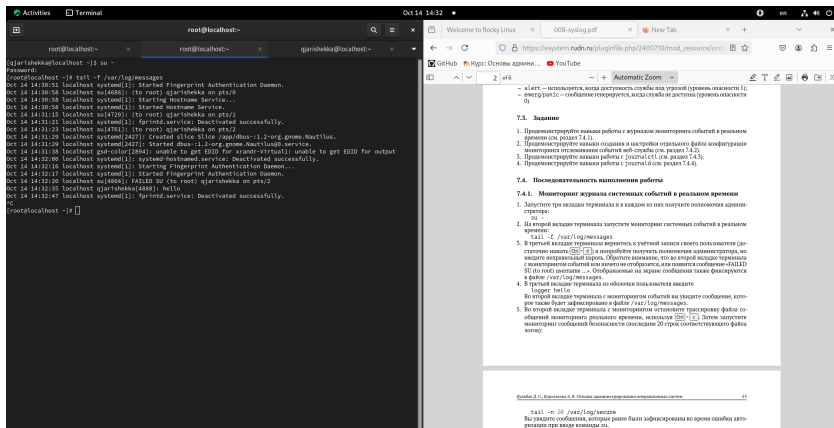


Рис. 3.8: завершение журнала

Дальше я запустил мониторинг сообщений безопасности (рис. 3.9).

`tail -n 20 /var/log/secure`

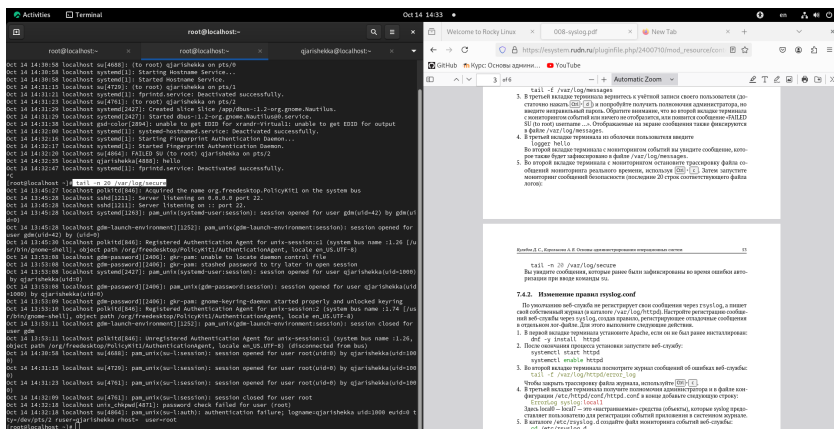


Рис. 3.9: мониторинг сообщений безопасности

(рис. 3.10).

Название

Рис. 3.10: Название

4 Выводы

После выполнения лабораторной работы я смог смотреть работу команд `tail` и `journalctl` чтобы смотреть журналы, которые сохраняют все выполненные процессы и как настройт его.

Список литературы