Отчет по лабораторной работе 7

Управление журналами событий в системе

Власов Артем Сергеевич

Содержание

# 1. Цель работы

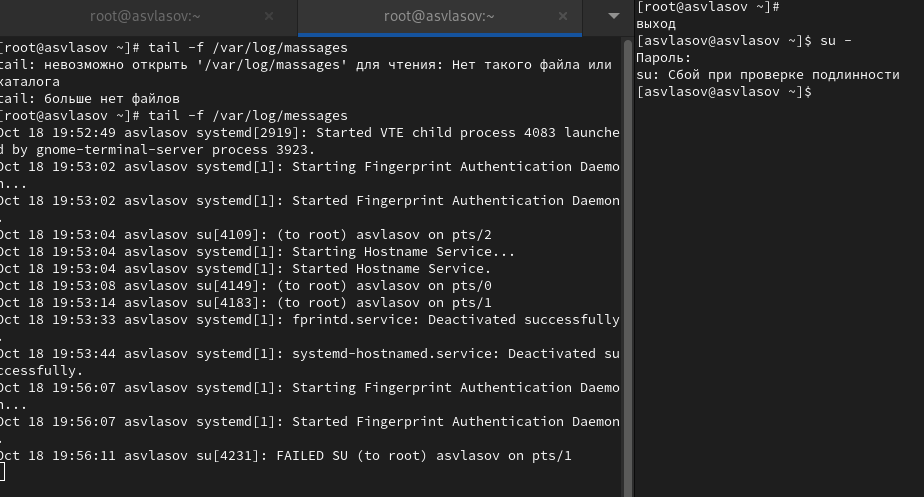
Получить навыки работы с журналами мониторинга различных событий в системе.

# 2. Задание

Продемонстрировать навыки умения работать с журналом мониторинга событий, созданием файла конфигурации мониторинга, journald и journalctl.

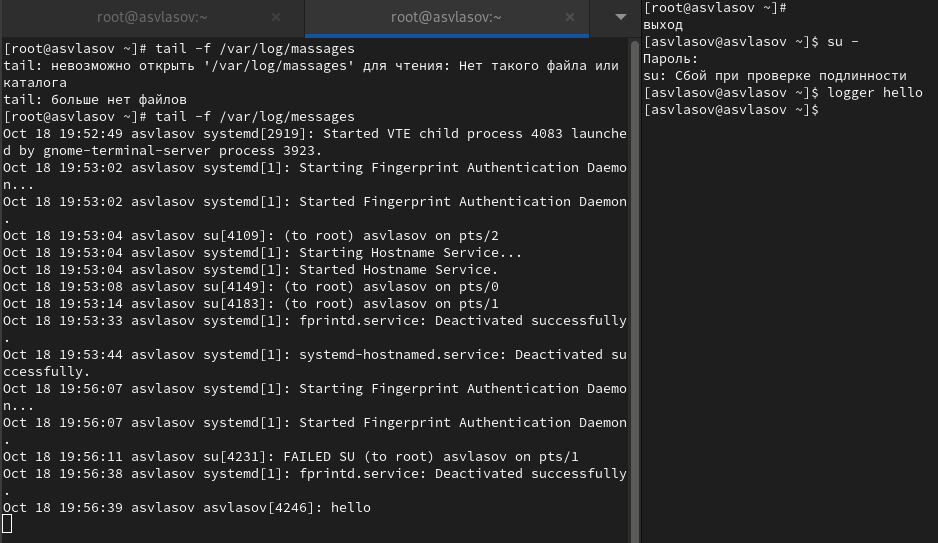
# 3. Выполнение лабораторной работы 7.

Запускаем 3 терминала, открываем во втором журнал мониторинга, на третьем пробуем получить права администратора с неверным паролем.



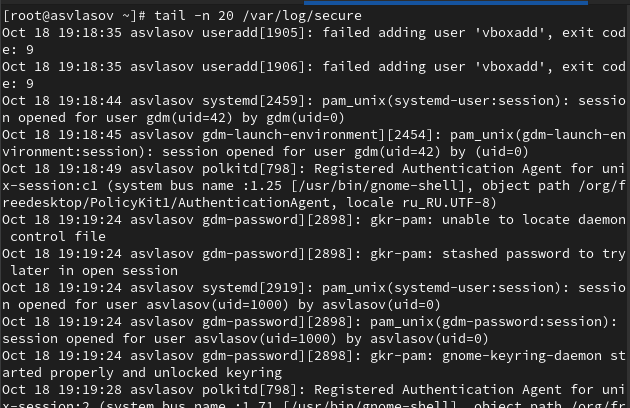
Неверный пароль администратора

Выводим в журнал сообщение hello.



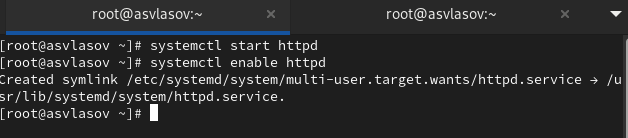
Сообщение

Открываем 20 последних строчек журнала.



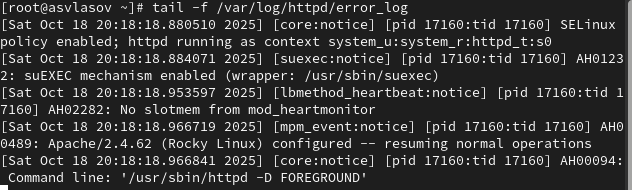
20 строчек

Устанавливаем и запускаем httpd.



httpd

Смотрим логи ошибок httpd.



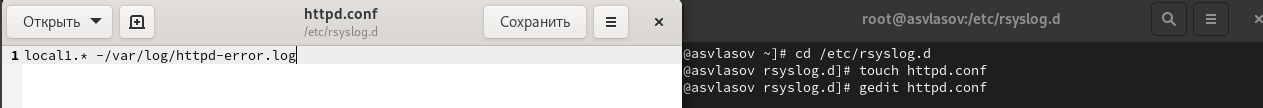
Логи ошибок

Заходим в файл конфигурации и дописываем строчку.



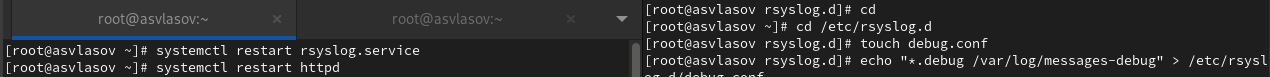
Изменение файла конфигурации

Создаем новый файл конфигурации и заполняем его.



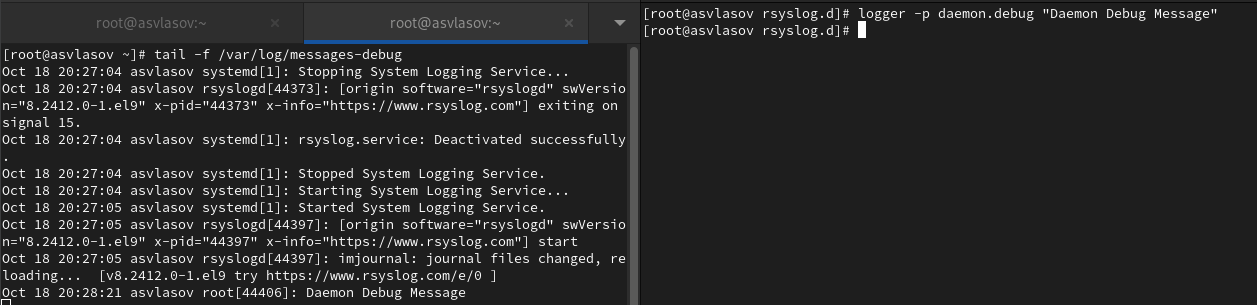
Новый файл конфигурации

Перезапускаем серивисы и дописываем строчку в файл конфигурации debug.conf.



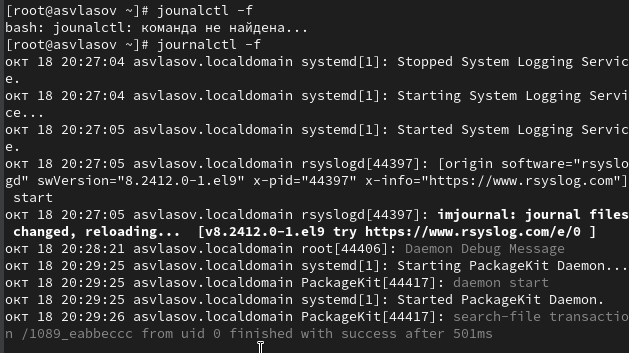
debug

Затем отправляем сообщение в дрпугой дурнал мониторинга.



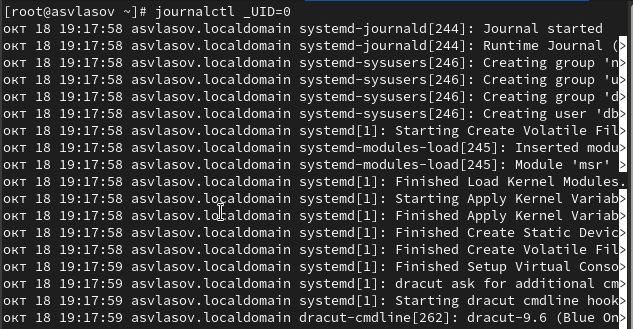
Сообщение в журнале

Начинаем работу с journalctl. Смотрим журнал в реальном времени.



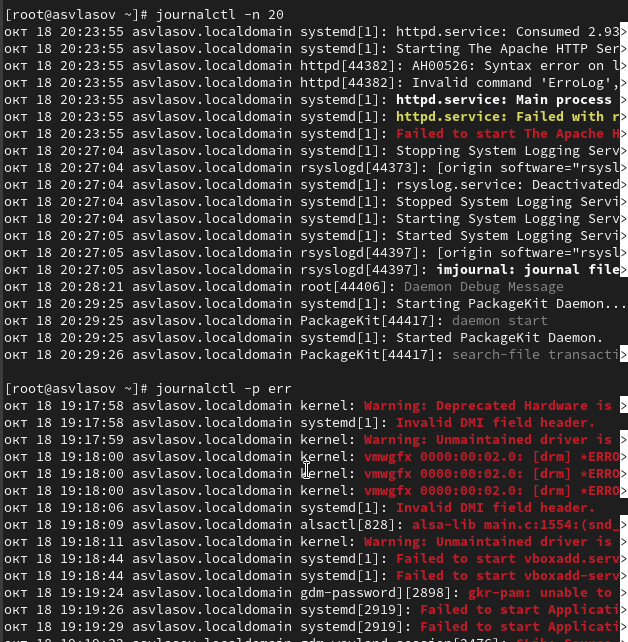
Журнал в реальном времени

Затем смотрим строки связанные с UID 0.



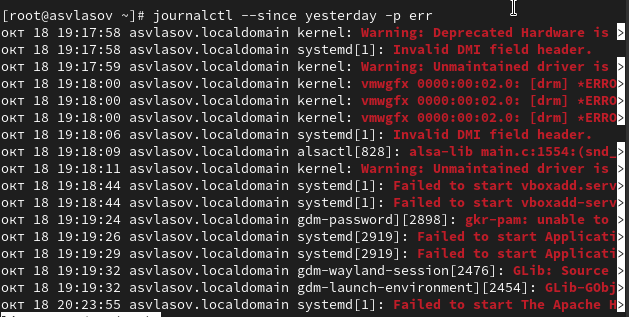
Журнал

Смотрим последние 20 строк журнала и строки с ошибками.



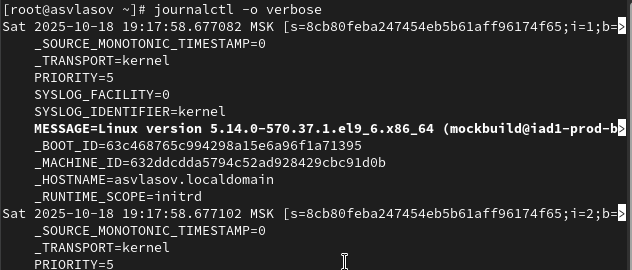
20 строк и ошибки

Смотрим все ошибки со вчерашенго дня.



Ошибки с определенной даты

Просмотр детальной информации



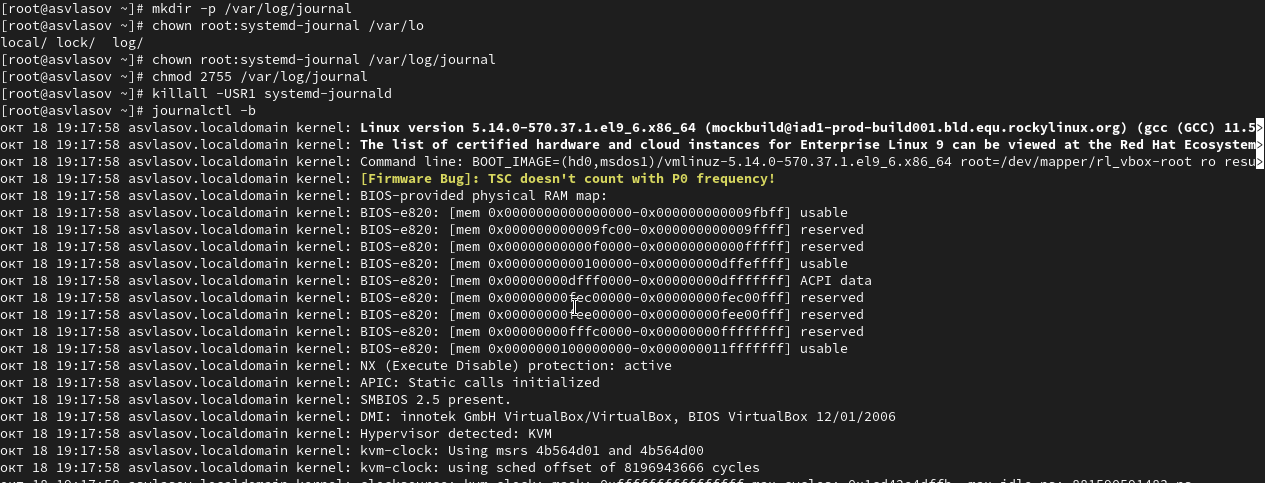
Детальная информация

Просмотр дополнительной информации о модуле sshd.

sshd

sshd

Создаем каталог для хранения записей журнала, задаем ему права, принимаем изменения командой. Теперь журнал постоянный.



Создание постоянного журнала

# 4. Выводы

Мы научились работать с журналами мониторинга событий в системе.

# Список литературы