|  |
| --- |
| **Лабораторная работа №** 25 |
| **Тема**:Изучение журналов и оповещений Windowsи Unix, настройка службы аудита вWindowsи Unix |
| **Цель выполнения работы**:ознакомление с журналами и оповещениями в операционных системах Windows, Unix. Изучение видов и назначений журналов. Изучение типов событий. Изучение служб аудита. Изучение средств для просмотра событий. |
| **Оборудование** (*приборы, материалы, дидактическое обеспечение*): |
| Отсутствуют |
| **Компьютерная программа** (*если используется*):VirtualBox, дистрибутив WindowsServer 2008 R2, дистрибутив Ubuntu(версия Serverили Desktop) |

**Теория**

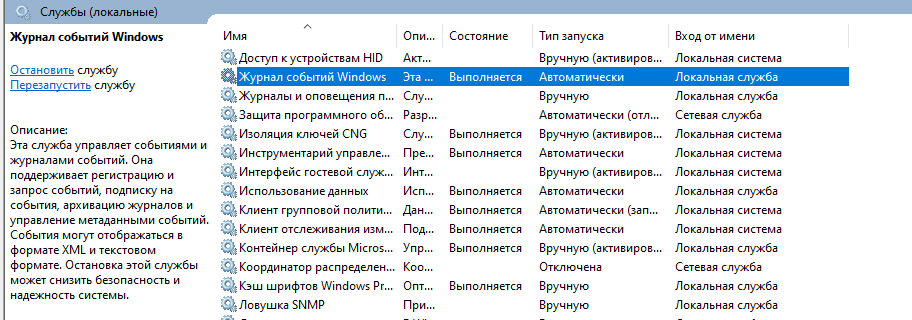
1. Книга Станек Уильям Р. Windows Server 2008 Справочник администратора; глава 4 Мониторинг процессов, служб и событий - раздел Журналы событий - страница 88; Глава 15 Общий доступ, безопасность и аудит – раздел Аудит системных ресурсов – страница 479.
2. Книга Немет Эви, Снайдер Гарт, Хейн Трент, Уэйли Бэн. Unix и Linux: руководство системного администратора; Глава 11. Система Syslog и журнальные файлы; страница 388.
3. [Руководство по syslogd](http://www.opennet.ru/man.shtml?topic=syslogd&category=8)
4. [Руководство по auditd](http://www.opennet.ru/man.shtml?topic=auditd&category=8&russian=0)
5. [Справка по Logger](http://www.opennet.ru/cgi-bin/opennet/man.cgi?topic=logger&category=1)
6. [Статья про auditd](https://xakep.ru/2011/03/30/54897/)

**Порядок выполнения**

Часть 1. Журналы и оповещения в Windows

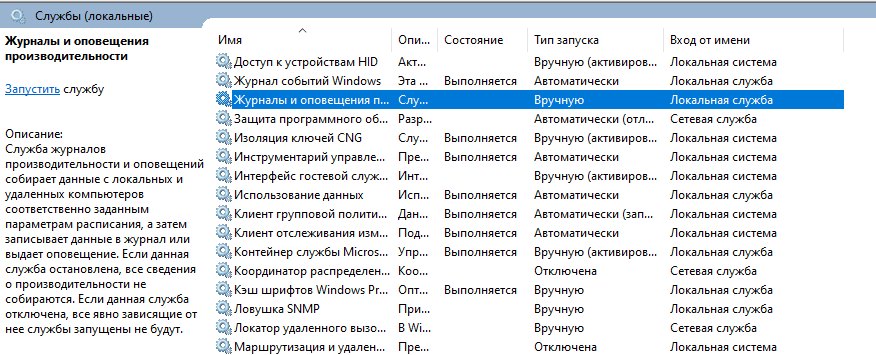
Раздел про журналы и события

1. Открыть оснастку **Службы.** Найти службу Журнал событий Windows (Windows Event Log). Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.

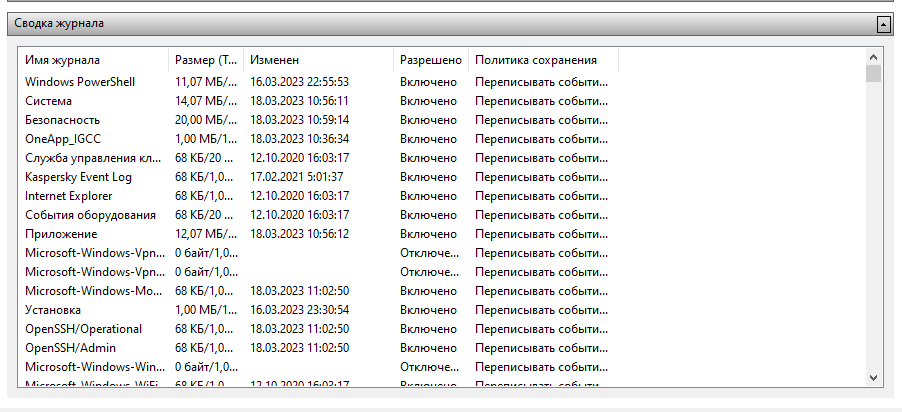
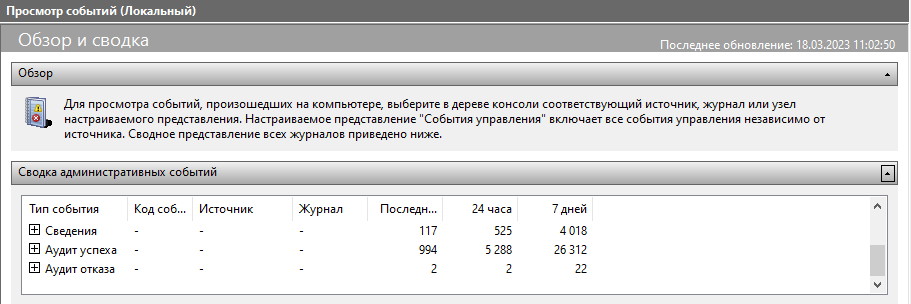


eventvwr.msc

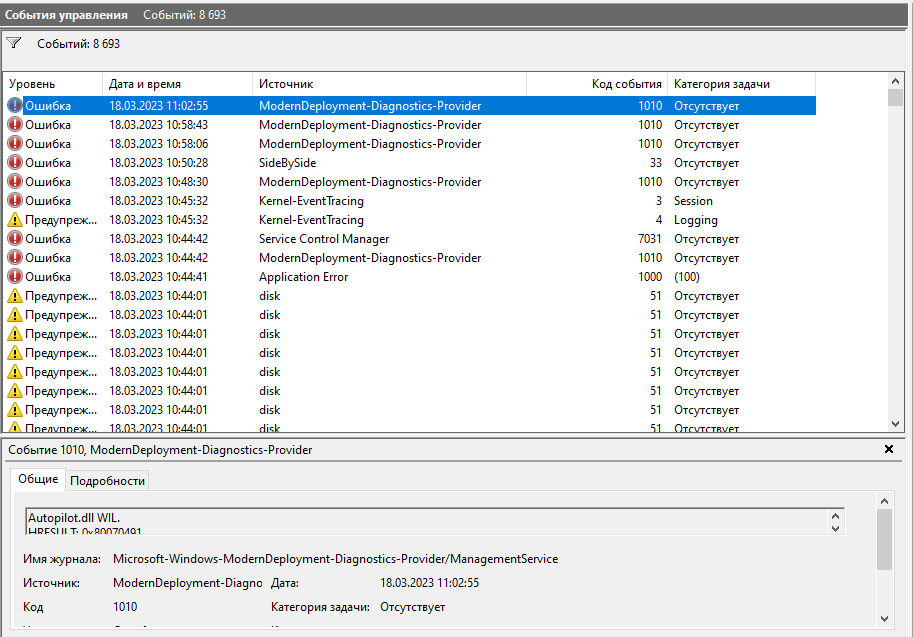
1. Найти службу Журналы и оповещения производительности. Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.



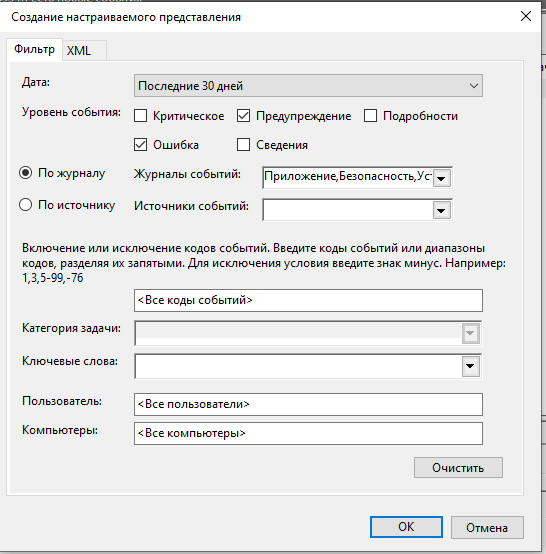
1. Открыть оснастку Просмотр событий. Изучить, что отображается в окне Сводка административных событий. Изучить, что отображается в окне Сводка журнала.



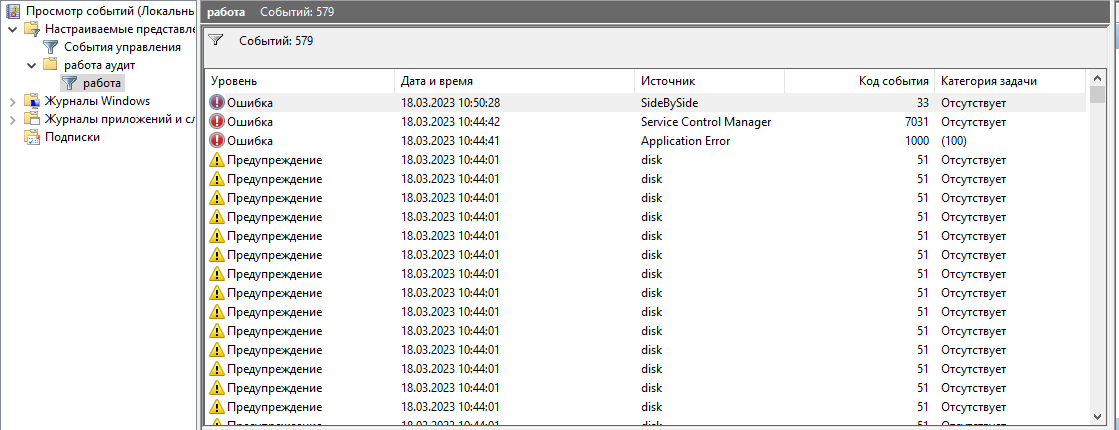
1. Просмотреть все ошибки и предупреждения – для этого развернуть узел **Настраиваемые представления** и выделить**События управления**. В отчет для первых пяти событий, записать: уровень, источник, код события.



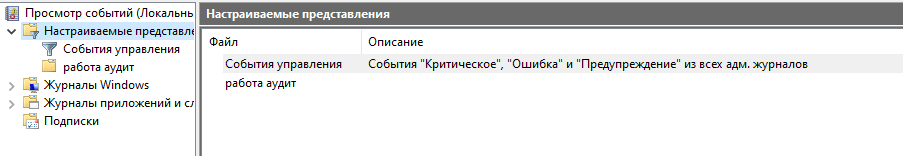
1. Создать настраиваемое представление. Отобразить все ошибки и предупреждения за последние 30 дней, для всех журналов, всех источников, всех кодов событий, всех пользователей и всех компьютеров.



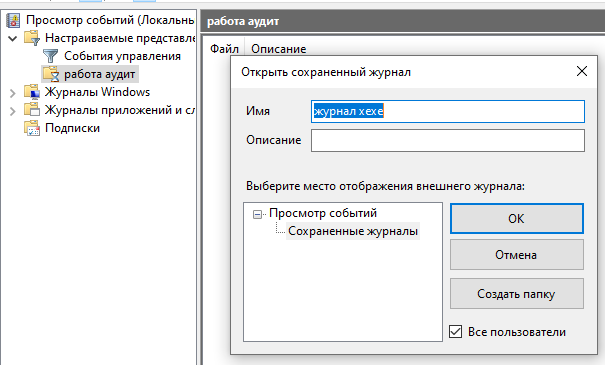
1. Сохранить все события в настраиваемом представлении в новый журнал.



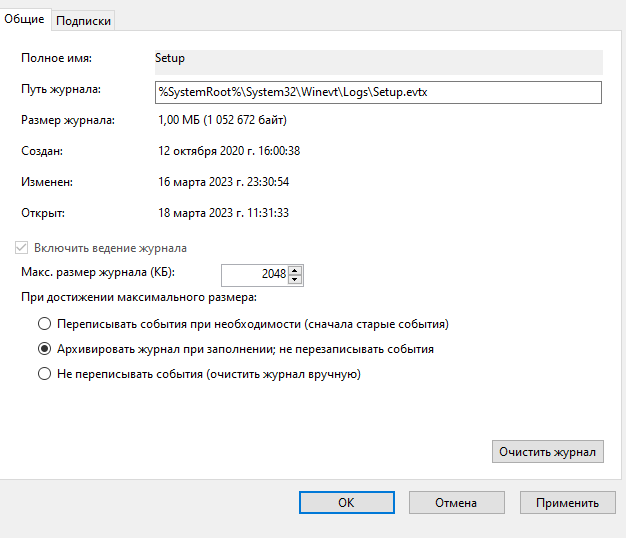
1. Удалите настраиваемое представление.



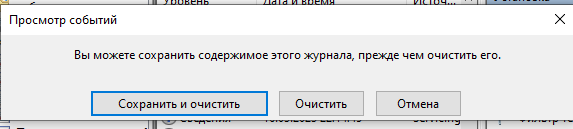
1. Открыть сохраненный журнал.



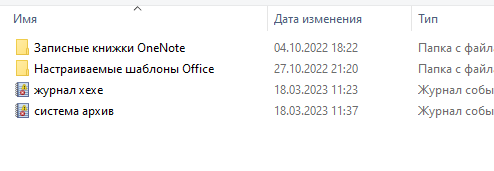
1. Настроить максимальный размер журнала **Установка** – 2048 КБ. Настроить **поведение при достижении максимального размера** – Архивировать журнал при заполнении; не перезаписывать события.



1. Очистить журнал **Установка,** не сохраняя содержимое.

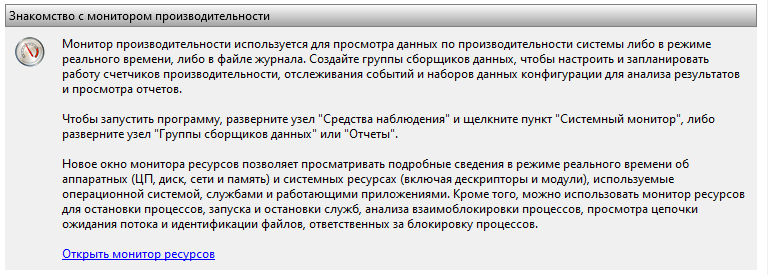


1. Заархивировать содержимое журнала **Система.**  Выбрать формат .evtx.

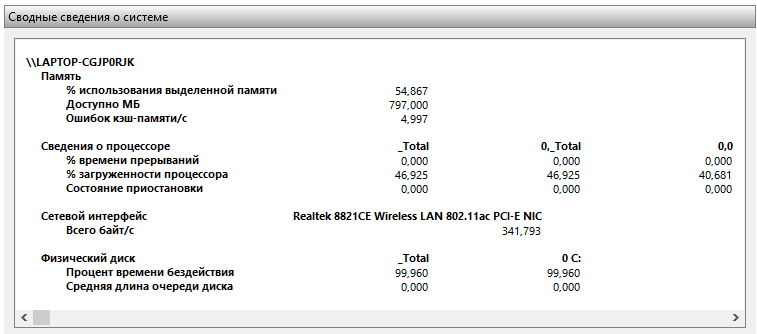


Раздел про оповещения

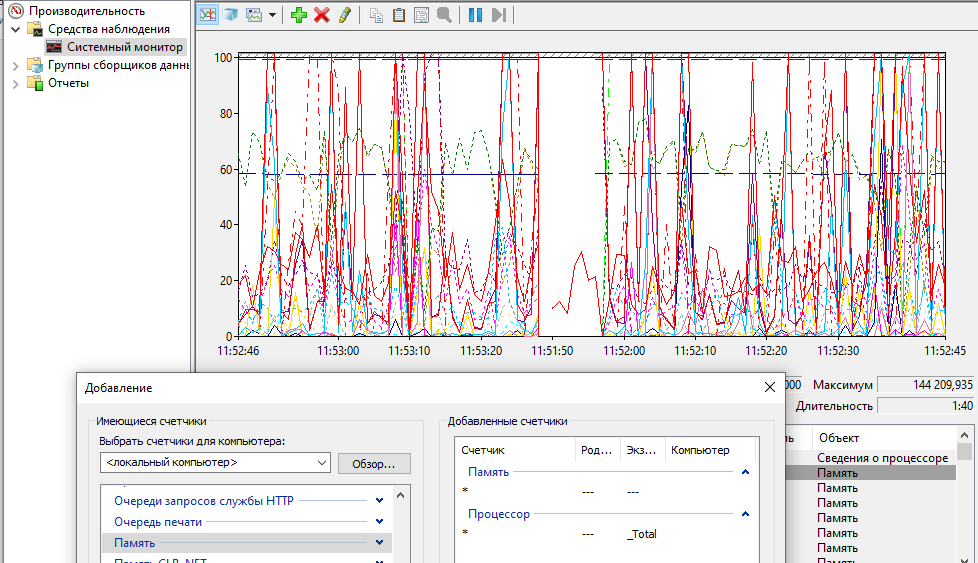
1. Открыть оснастку **Системный монитор**.
2. Прочитать содержимое окна Знакомство с монитором производительности



1. Изучить содержимое окна Сводные сведения о системе



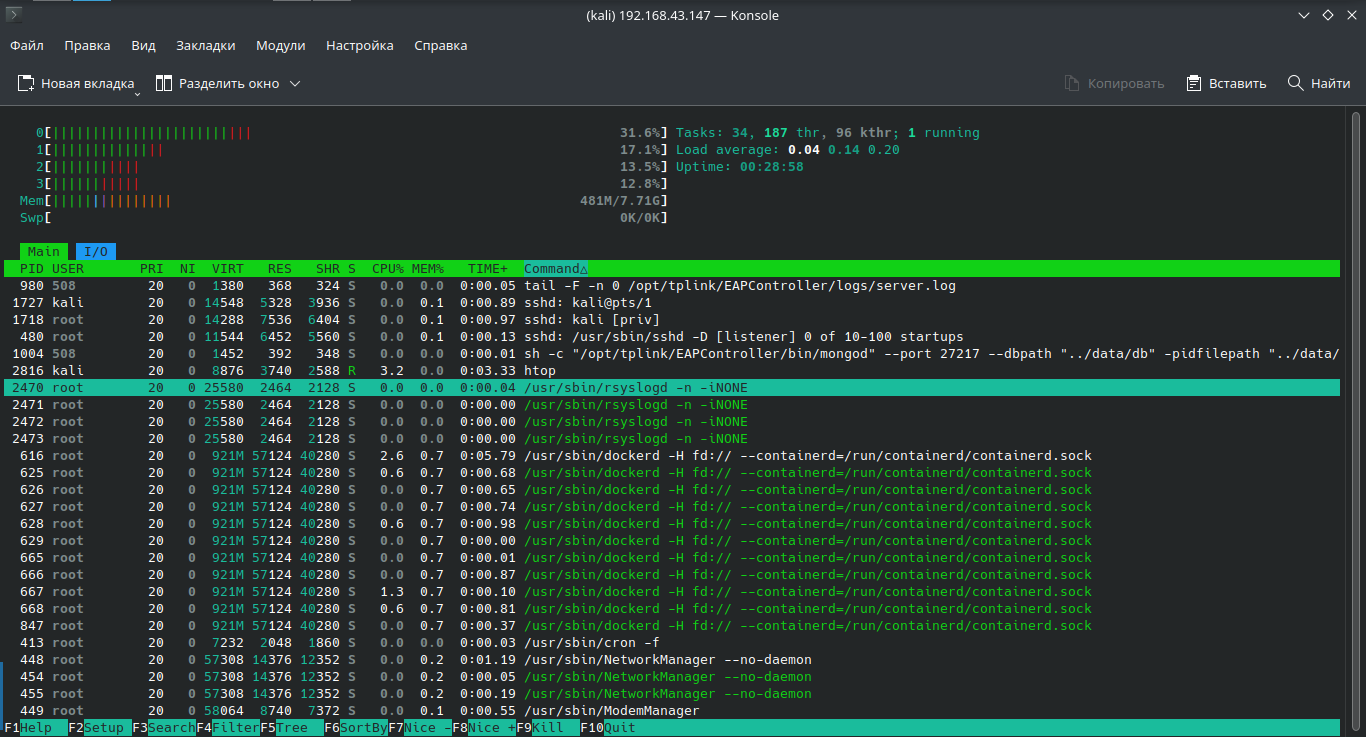
1. Открыть Системный монитор. Добавить счетчики для памяти и для процессора. Сохранить как группу сборщиков данных.



1. Создать оповещение счетчиков производительности для счетчика: Процессор/ % загруженности процессора. Оповещение при: выше, порог: 90. Развернуть получившийся узел новой группы сборщиков данных. Открыть свойства оповещения. Настроить **интервал выборки:** 30 сек. Настроить **действие оповещения**: Сделать запись в журнале событий приложений и **запустить группу сборщиков данных**: выбрать группу созданную ранее для памяти и процессора.

Часть 2. Журналы и оповещения в Unix

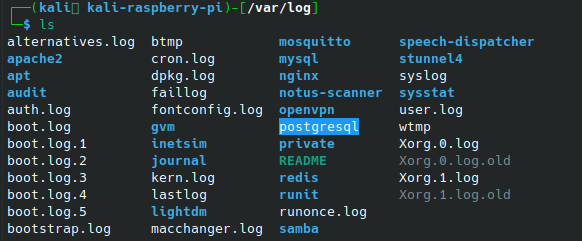
1. Запустить утилиту top и найти rsyslogd. Выписать в отчет – пользователя запустившего процесс, PID.



1. Перейти в каталог с журналам **/var/log**.



1. Вывести список всех журнальных файлов.



1. Определить назначение журналов – auth.log, boot.log, dpkg.log, kern.log, syslog.

*Auth.log - это файл журнала, который содержит информацию о входах и выходах в систему, а также о попытках аутентификации пользователей.*

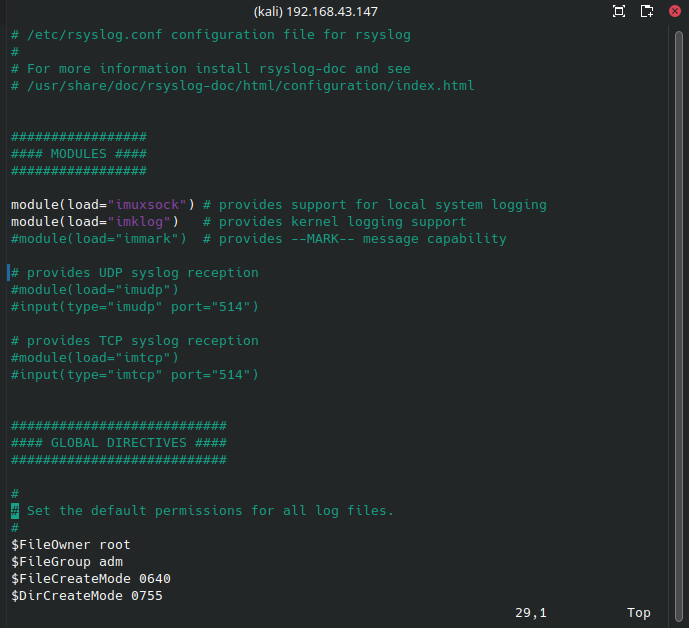
*Boot.log - это файл журнала, который содержит информацию о процессе загрузки операционной системы. Он может быть полезен для диагностики проблем при загрузке.*

*Dpkg.log - это файл журнала, который содержит информацию о всех операциях установки, удаления и обновления пакетов в системе, которые были выполнены с помощью утилиты dpkg.*

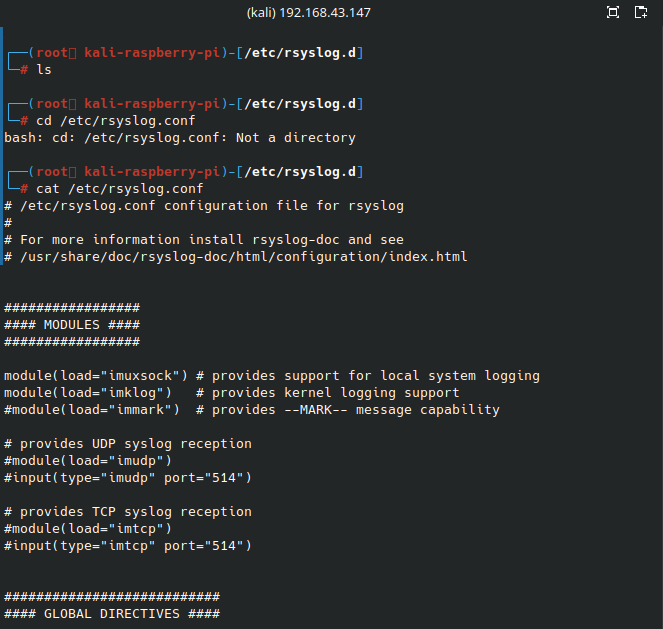
*Kern.log - это файл журнала, который содержит информацию о ядре операционной системы, включая сообщения об ошибках, предупреждения и другие события, связанные с ядром.*

*Syslog - это файл журнала, который содержит информацию о различных событиях в системе, таких как сообщения от демонов, ошибки и предупреждения. Он может быть полезен для диагностики проблем в системе и отслеживания ее работы.*

1. Изучить содержимое файла **/etc/rsyslog.conf**



1. Изучить содержимое файла **/etc/rsyslog.d/50-default.conf**. Сделать вывод как этот файл связан с файлом /**etc/rsyslog.conf**

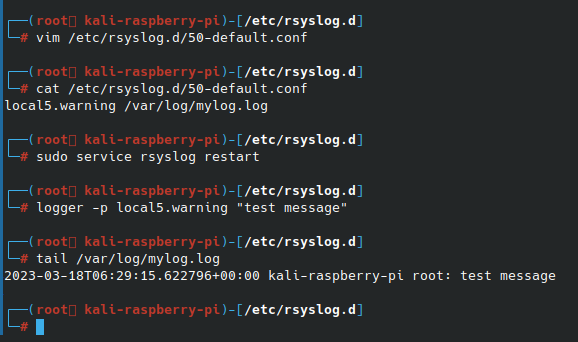


*Файл /etc/rsyslog.d/50-default.conf содержит настройки для журналов, которые должны быть записаны в системный журнал. Этот файл является одним из многих файлов конфигурации, которые могут быть использованы для настройки rsyslog.*

*Файл /etc/rsyslog.conf является главным файлом конфигурации rsyslog и определяет общие настройки для системного журнала. Этот файл может содержать ссылки на другие файлы конфигурации, включая файл /etc/rsyslog.d/50-default.conf.*

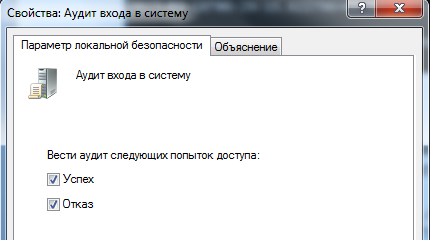
*Таким образом, файл /etc/rsyslog.d/50-default.conf связан с файлом /etc/rsyslog.conf через использование ссылок на другие файлы конфигурации.*

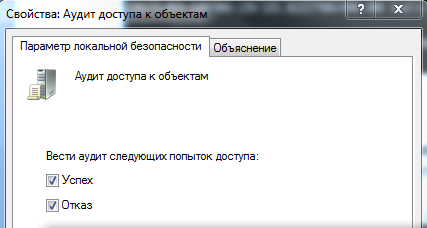
1. **(\*** Необязательное задание) Добавить в файл /etc/rsyslog.d/50-default.confправило для фиксации события **local5.warning** в журнал**mylog.log**. Перезапустить службу rsyslogd. С помощью команды loggerдобавить событие в созданный журнал – **logger –plocal5.warning “testmessage”**. Проверить наличие события в журнале.



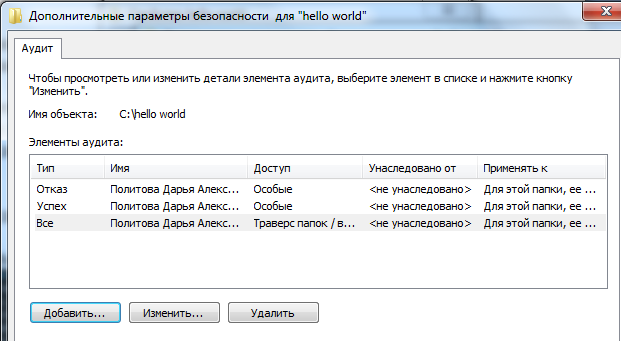
Часть 3. Аудит в Windows

1. Настроить политику аудита: Конфигурация компьютера – Конфигурация Windows - Параметры безопасности - Локальные политики - Политика аудита.
2. Включить Аудит входа в систему, Аудит доступа к объектам.

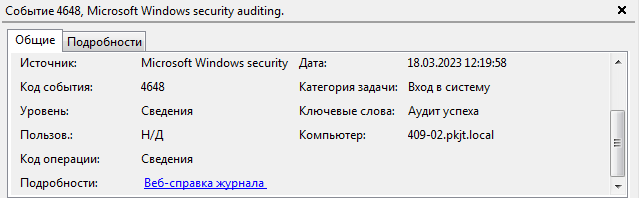




1. Создать папку C:/Files. Настроить аудит для папки. Создавать и удалять файлы и папки в C:/Files

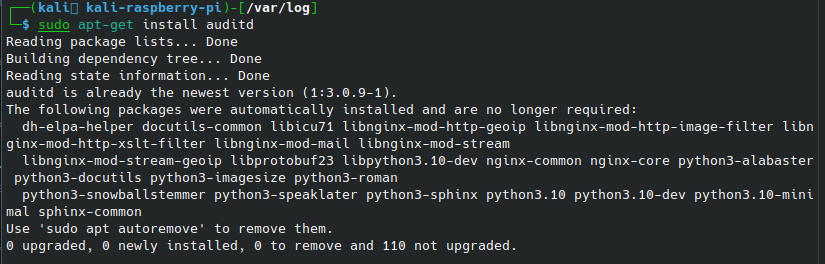


1. Найти в оснастке Просмотр событий – события входа/выхода пользователя в систему; события создания/удаления файлов и папок (например: Выполнение попытки получения доступа к объекту, где операция доступа: DELETE). Зафиксировать события в отчете.

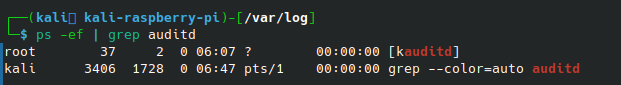


Часть 4. Аудит в Unix

1. Установить auditd.



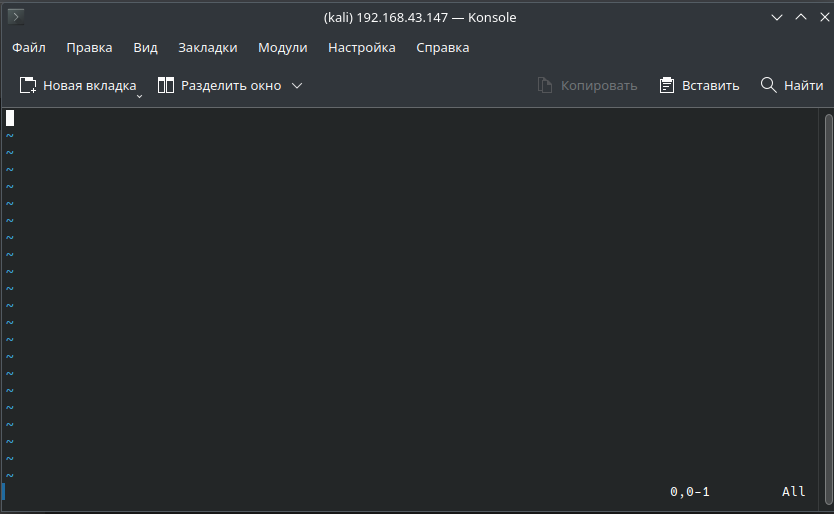
1. Найти процесс auditd.



1. Посмотреть список правил аудита **sudoauditctl –l**



1. Посмотреть файл конфигурации /etc/audit/audit.conf



1. Создать каталог /home/имя-вашего-домашнего-каталога/secret



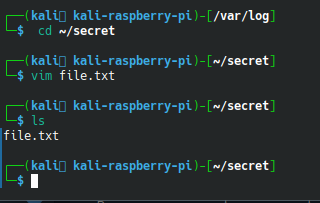
1. Создать правило для аудита доступа к каталогу /home/имя-вашего-домашнего-каталога/secret.



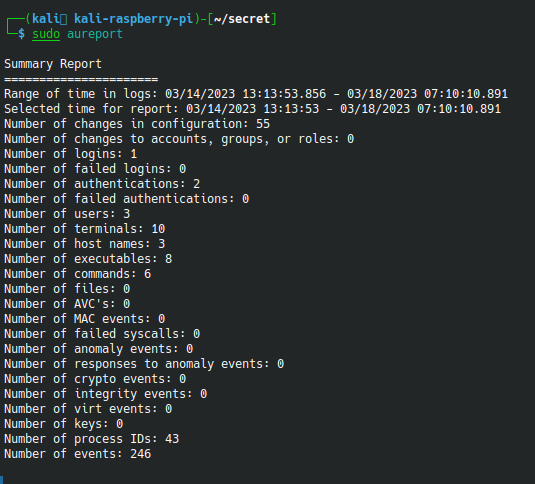
1. Перезапустить auditd.



1. Открыть каталог **secret**. Создать в нем текстовый файл.

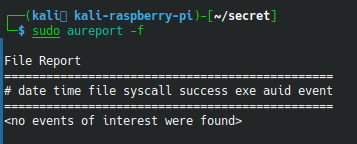


1. Выполнить aureport. Разобрать вывод.



*Вывод содержит информацию о событиях аудита, таких как успешные или неудачные попытки входа в систему, изменения файловой системы и т.д.*

1. Выполнить aureport –f. Разобрать вывод.



*Вывод содержит информацию о файлах, которые были изменены или созданы в течение определенного периода времени.*

1. Найти событие в журнале аудита.



**Контрольные вопросы**

Про Windows:

1. Какие уровни событий бывают?

*Уровни событий: информационный, предупреждение, ошибка, критическая ошибка, успешное выполнение аудита, неудачное выполнение аудита, аудит событий безопасности.*

1. В какой журнал пишутся события аудита?

*События аудита пишутся в журнал Security.*

1. В какой консоли можно смотреть журналы событий?

*Журналы событий можно смотреть в консоли Event Viewer.*

Про Unix:

1. В каком каталоге находятся журнальные файлы?

*Журнальные файлы находятся в каталоге /var/log.*

1. Что такое Syslog?

*Syslog - это стандартный протокол для записи и передачи системных сообщений.*

1. Как работает syslogd?

*Syslogd принимает сообщения от различных компонентов системы и записывает их в соответствующие журнальные файлы.*

1. Назовите уровни важности сообщений Syslog?

*Уровни важности сообщений Syslog: emergency, alert, critical, error, warning, notice, info, debug.*

1. Какие способы обработки сообщения Syslogвы знаете?

*Способы обработки сообщений Syslog: запись в файлы журналов, отправка на удаленный сервер, вывод на консоль или почту.*

1. Какие события можно протоколировать с помощью аудита?

*С помощью аудита можно протоколировать различные события, например, изменение прав доступа к файлам и папкам, запуск и завершение процессов, подключение и отключение устройств и т.д.*