Лабораторная работа №1
«Журналирование и справочные ресурсы»

1. Теоретическая часть

1.1. Справочная информация

Командная строка ОС Linux содержит в себе множество различных команд, которые очень сложно быстро запомнить. Для вывода руководства по командам, утилитам, программированию и другим областям системы существует библиотека с документацией. Доступ к ней осуществляется с помощью утилиты man.

man – справочная система Astra Linux, предназначенная для вывода и форматирования справочных страниц

Справочные страницы поделены на 8 стандартных разделов:

1 – исполняемые программы и (не всегда) команды оболочки

2 – системные вызовы (функции, предоставляемые ядром)

3 – библиотечные вызовы (функции библиотек)

4 – файлы устройств

5 – форматы файлов и соглашений

7 – разное (пакеты и соглашения)

8 – команды администрирования системы

Чтобы получить руководство по использованию какой-либо команды нужно выполнить команду:

man [ключ] название команды

В таблице представлены некоторые из возможных ключей.

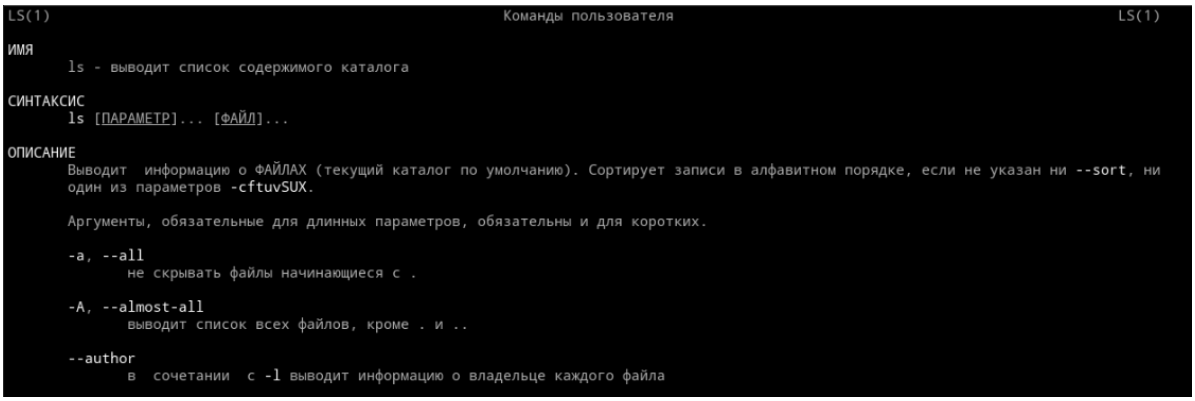
Ключ	Значение
-f	Вывести оглавление
N	Вывести страницу N
-k	Поиск утилит по описанию

Пример применения ключей:

```
adminmsc@ru01wks001:~$ man -f cat
cat (1)              - объединяет файлы и направляет их на стандартный вывод
adminmsc@ru01wks001:~$ man -f printf
printf (1)           - format and print data
printf (3)           - formatted output conversion
adminmsc@ru01wks001:~$ man -f chmod
chmod (1)            - change file mode bits
chmod (2)            - change permissions of a file
adminmsc@ru01wks001:~$ man -f chroot
chroot (2)           - change root directory
chroot (8)           - run command or interactive shell with special root directory
adminmsc@ru01wks001:~$ man -f hosts
hosts (5)            - статическая таблица для поиска имён узлов
```

Пример работы программы:

man ls



Для эффективного использования man-страниц в Linux, важно знать горячие клавиши и команды для навигации и поиска. Перечислим основные команды, которые помогут вам работать с man-страницами:

- **q**: Выйти из man-страницы.
- **h**: Показать справку по навигации.
- **Space**: Прокрутка вперед на одну страницу.
- **b**: Прокрутка назад на одну страницу.
- **Enter** или **Down Arrow**: Прокрутка вперед на одну строку.
- **Up Arrow**: Прокрутка назад на одну строку.
- **g**: Перейти в начало документа.
- **G**: Перейти в конец документа.
- **/слово**: Поиск слова в документе
    - **n**: Перейти к следующему совпадению после выполнения поиска.
    - **N**: Перейти к предыдущему совпадению после выполнения поиска.

1.2. Журналирование

Процесс настройки и поддержки программного обеспечения в ОС Linux является нетривиальной задачей. Для упрощения взаимодействия системного администратора с программным обеспечением утилитам, ядром и приложениями генерируются журнальные данные, которые в дальнейшем возможно обработать и проанализировать.

Журналирование в Linux — это процесс записи событий, сообщений и логов операционной системы и приложений для их последующего анализа, диагностики проблем и аудита безопасности.

Исторически, система UNIX управляла журналами с использованием системы syslog. Это достаточно сложная и громоздкая система, предназначенная для сбора сообщений и их последующей записи в файлы. Из-за её недостатков в дальнейшем многие утилиты разработали свои средства журналирование, что привело еще к большей путанице.

Большинство журналов хранится в директории /var/log/. Рассмотрим некоторые из них.

Название журнала	Основные программы	Содержимое
apt/history.log	apt-get	Сообщения об установке пакетов
auth.log	passwd, polkitd, sshd, su, sudo, useradd, userdel, usermod	Авторизационные сообщения
cron.log	cron	Сведения о работе демона cron
daemon.log	-||-	Сведения о работе различных демонов
dmesg	Ядро	Сообщения ядра ОС
dpkg.log	dpkg	Журнал управления пакетом
kern.log	Ядро	Все сообщения от ядра ОС

mail.log	Почтовые программы (postfix)	Все сообщения, связанные с электронной почтой
syslog	Различные программы	Основной системный журнал

Все перечисленные файлы возможно открыть и прочитать с помощью текстового редактора. Журналы lastlog и wtmp, хранящие в себе сообщения о последней регистрации пользователей в системе хранятся в бинарном виде, поэтому прочитать их возможно с помощью специальных утилит – lastlog и last.

Во многих современных системах, к которым относится в том числе Astra Linux журналирование параллельно ведется системой инициализации systemd. Все события в системе обрабатываются демоном journald, которых сохраняет их в виде бинарных файлов. Для просмотра логов применяется утилита journalctl**.**

Все логи в журнале хранятся в следующем формате:

дата хост источник сообщение

Например,

янв 09 20:55:55 server sshd[1041]: Server listening on 0.0.0.0 port 22

- **янв 09 20:55:55** - дата и время события;
- **server** - хост, на котором произошло событие;
- **sshd[1041]**- источник события, обычно это программа или сервис. В данном случае демон ssh, его pid=1041;
- **Server listening on 0.0.0.0 port 22**- само сообщение.

Перечислим основные команды и параметры journalctl. Вызов производится в привилегированном режиме.

Просмотр всего журнала

journalctl

Просмотр всего журнала с конца

journalctl -e

Вывод сообщений журнала, отфильтрованные по коду важности. journalctl выводит все сообщения с этим кодом и выше

journalctl -p <код>

Для уровней важности, приняты следующие обозначения:

0: emergency (неработоспособность системы)

1: alerts (предупреждения, требующие немедленного вмешательства)

2: critical (критическое состояние)

3: errors (ошибки)

4: warning (предупреждения)

5: notice (уведомления)

6: info (информационные сообщения)

7: debug (отладочные сообщения)

Просмотр журнала во временном промежутке

journalctl --since "2020-12-17" --until "2020-12-18 10:00:00
journalctl –since “1 minute ago”

Просмотр сообщений ядра

journalctl –k

Просмотр журналов определенного сервиса

journalctl -u NetworkManager.service

2. Практическая часть

Задание 1.

1. Проанализируйте, какой из пользователей не смогу войти в свою учетную запись при вводе пароля в окне логина.
2. Выведите все сообщение из журнала auth.log, содержащие строку sudo. В выведенном тексте искомая строка должна подсвечиваться. Для выполнения задания воспользуйтесь справочной информацией по утилите grep.

Задание 2.

1. С помощью команды journalctl найдите сообщения, поступившие в журнал службы systemd-journald с 12 до 17 часов вчерашнего дня.
2. Просматривайте сообщения, поступающие от службы Network Manager в журнал службы systemd-journald.

Задание 3.

1. Определите по значениям логов, сколько пользователей было создано и удалено в системе.
2. Определите, какая утилита чаще всего писала в файл syslog

Контрольные вопросы

1. На какой странице man возможно прочитать про системные вызовы?
2. В каком файле хранятся сообщения от ядра ОС?
3. В чем отличие в хранении логов syslog и journalctl?