**Команды Linux для управления файлами**

1. ls – отображает список файлов и каталогов в текущей директории.
2. cd – изменяет текущую директорию.
3. pwd – выводит полный путь текущей директории.
4. mkdir – создает новый каталог.
5. rm – удаляет файлы или каталоги.
6. cp – копирует файлы и каталоги. (-R – с этим флагом копирует весь каталог со всем его содержимым).
7. mv – перемещает или переименовывает файлы и каталоги.
8. touch – создает новый файл или обновляет время доступа и модификации существующего файла.
9. cat – выводит содержимое файла. Также она имеет функцию конкатенации, то есть соединения файлов (cat big.\*).
10. less – позволяет просматривать содержимое файла построчно. Также позволяет вести поиск в файле (: /kernel)
11. more - позволяет просматривать содержимое файла постранично.
12. head – выводит первые строки файла (первые 10 строчек файла, но количество строк можно менять с помощью флага (-15)).
13. tail – выводит последние строки файла (количество строк можно менять с помощью флага (-15)).
14. split - разбивает файл на другие файлы (split -b5k (флаг с размером в 5 килобайт) bigfile (название файла) big. (префикс – обязательно).
15. dd – выводит заданное количество блоков из файла, а также из стандартного ввода (dd if=/dev/zero bs=512 count=500 | od -c).
16. od – выводит дампы файлов в восьмеричном формате. С помощью этой утилиты можно увидеть содержимое файлов в восьмеричном, шестеричном и других форматах (dd if=/dev/zero bs=512 count=500 | od -c).
17. diff – сравнивает два файла (diff bigfile big.aa)
18. grep – ищет заданный текст в файлах или выводе команд, то есть осуществляет поиск по содержимому файлов, а не по их названию (-i -не учитывая регистр, искомое имя пишем в кавычках; -v – инверсный поиск; -r – рекурсивный поиск; -с – количество вхождение строки для каждого файла, сколько раз в него входили; --color – подсветить искомое).
19. egrep – ищет вхождение искомых слов в файле (egrep -w ‘bin|bash’ bigfile).
20. find – находит файлы и каталоги на основе различных критериев (find . -maxdepth 1 -name ‘\*.a\*’ - искать максимально в текущем каталоге все файлы с расширением ‘a’) или (find -name ‘\*2\*’ - найдёт все файлы и директории с цифрой 2 в текущей директории и поддиректориях).
21. wc – выводит количество вхождений строки в искомом файле (grep -i sh bigfile | wc -l - сначала найдем без учета регистра строки sh в файле bigfile, а потом посчитаем сколько таких строк с помощью wc и выведем данные с помощью флага -l).
22. chmod – изменяет права доступа к файлам и каталогам.
23. chown – изменяет владельца файлов и каталогов.
24. chgrp – изменяет группу файлов и каталогов.
25. tar – создает или распаковывает архивы.
26. zip – создает ZIP-архивы.
27. unzip – извлекает файлы из ZIP-архивов.
28. history – показывает историю команд и входов (history | grep cd > myhistory - ищет все перемещения и записывает в файл с вашей историей).

**Команды Linux для управления пользователями**

1. adduser – создает нового пользователя.
2. usermod – изменяет параметры существующего пользователя.
3. deluser – удаляет пользователя.
4. passwd – изменяет пароль пользователя.
5. su – переключается на другого пользователя или становится суперпользователем.
6. sudo – выполняет команду с привилегиями суперпользователя.
7. finger – отображает информацию о пользователе.
8. who – отображает информацию о вошедших пользователях.
9. id – отображает информацию о текущем пользователе или указанном пользователе.
10. groups – отображает группы, к которым принадлежит пользователь.
11. useradd – создает нового пользователя (альтернатива для adduser).
12. userdel – удаляет пользователя (альтернатива для deluser).
13. usermod – изменяет параметры существующего пользователя (альтернатива для usermod).
14. passwd – изменяет пароль пользователя (альтернатива для passwd).
15. last – отображает историю входа пользователей.
16. w – отображает текущих пользователей и их активность.
17. logout – выходит из текущей сессии пользователя.

**Команды Linux для управления приложениями**

1. apt-get install – устанавливает новое приложение или пакет.
2. apt-get remove – удаляет установленное приложение или пакет.
3. apt-get update – обновляет список доступных обновлений пакетов.
4. apt-get upgrade – обновляет установленные пакеты до последних версий.
5. apt-cache search – ищет пакеты по ключевому слову.
6. dpkg -i – устанавливает .deb пакет.
7. dpkg -r – удаляет .deb пакет.
8. dpkg -l – отображает список установленных пакетов.
9. snap install – устанавливает приложение из snap-пакета.
10. snap remove – удаляет установленное snap-приложение.
11. snap list – отображает список установленных snap-приложений.
12. systemctl start – запускает системную службу.
13. systemctl stop – останавливает системную службу.
14. systemctl restart – перезапускает системную службу.
15. systemctl enable – включает автозапуск системной службы при загрузке системы.
16. systemctl disable – отключает автозапуск системной службы при загрузке системы.
17. service <service> start – запускает службу.
18. service <service> stop – останавливает службу.
19. service <service> restart – перезапускает службу.
20. service <service> status – отображает статус службы.

**Команды Linux для управления системой**

1. shutdown – позволяет выключить или перезагрузить систему. Например, shutdown -h now выключает систему немедленно.
2. reboot – перезагружает систему. Просто запустите reboot в терминале.
3. halt – выключает систему. Просто запустите halt в терминале.
4. poweroff – выключает систему. Просто запустите poweroff в терминале.
5. systemctl – команда для управления системными сервисами. Например, systemctl start apache2 запускает службу Apache.
6. service – альтернативный способ управления системными службами. Например, service nginx restart перезапускает службу Nginx.
7. ifconfig – отображает и настраивает сетевые интерфейсы системы, включая IP-адреса, маски и шлюзы.
8. ip – альтернативный способ управления сетевыми интерфейсами и конфигурацией сети.
9. netstat – отображает сетевые соединения, открытые порты и другую связанную информацию.
10. ping – отправляет ICMP-пакеты на указанный IP-адрес для проверки доступности хоста в сети.
11. traceroute – отображает путь, по которому проходят пакеты до указанного IP-адреса в сети.
12. ssh – устанавливает безопасное соединение с удаленным сервером по протоколу SSH.
13. scp – копирует файлы между удаленным и локальным серверами по протоколу SSH.
14. rsync – выполняет синхронизацию и копирование файлов между удаленными и локальными серверами.
15. crontab – позволяет управлять cron-задачами, которые выполняются автоматически по заданному расписанию.
16. at – позволяет запускать команды или скрипты в определенное время в будущем.
17. shutdown – планирует выключение или перезагрузку системы по расписанию.
18. nohup – запускает команду с игнорированием сигналов завершения процесса. Это полезно для выполнения задач в фоновом режиме.
19. history – отображает историю команд, введенных пользователем в терминале.

**Команды Linux для управления процессами**

1. top – отображает список процессов и их характеристики, такие как использование CPU и памяти.
2. ps -ax  – выводит список текущих запущенных процессов с их идентификаторами (PID).
3. Kill – отправляет сигнал процессу для его завершения. Например, kill PID завершит процесс с указанным идентификатором.
4. pkill – отправляет сигнал процессам по их имени или другим атрибутам. Например, pkill firefox завершит все процессы Firefox.
5. htop – интерактивное утилита мониторинга процессов, которая позволяет видеть дополнительную информацию и управлять процессами.
6. free – отображает общую, использованную и свободную память системы, включая физическую и подкачку.
7. vmstat – предоставляет информацию о использовании памяти, процессоре, вводе-выводе, планировании и других системных ресурсах.
8. killall – завершает все процессы с указанным именем. Например, killall firefox завершит все процессы Firefox.
9. renice – изменяет приоритет процесса в реальном времени. Например, renice -n -5 -p PID увеличит приоритет процесса с указанным идентификатором.
10. nice – запускает процесс с более низким приоритетом. Например, nice -n 10 command запустит команду с очень низким приоритетом.
11. pgrep – выводит идентификаторы процессов, соответствующие указанной строке. Например, pgrep firefox выведет идентификаторы процессов Firefox.
12. strace – отслеживает системные вызовы и сигналы, связываемые с процессом. Можно использовать для отладки или анализа процессов.
13. lsof – выводит открытые файлы и сетевые соединения для всех процессов на системе.
14. sar – собирает информацию о использовании ресурсов системы, таких как процессор, память, сеть и диски, и сохраняет ее для последующего анализа.
15. uptime – выводит информацию о времени работы системы, средней загрузке и количестве активных пользователей.
16. time – запускает команду и отображает время, затраченное на ее выполнение, включая CPU-время и время ввода-вывода.

**Команды Linux для управления памятью**

1. smem – отображает детальную информацию об использовании памяти процессами, группами процессов и системой в целом.
2. sync – записывает все буферы операционной системы на диск, чтобы обеспечить сохранность данных перед завершением работы.
3. swapoff – отключает файл подкачки, что позволяет освободить диск, но может увеличить использование оперативной памяти.
4. swapon – включает файл подкачки, добавляя дополнительную виртуальную память для использования системой.
5. sysctl – позволяет просматривать и изменять настройки ядра, включая параметры, связанные с памятью.
6. ulimit – устанавливает ограничения на использование ресурсов, включая память, для отдельного пользователя или процесса.
7. pmap – выводит карту памяти процесса, позволяя увидеть как процесс использует физическую и виртуальную память.
8. slabtop – отображает информацию о кэшах ядра, которые используют физическую память системы.
9. ulimit – устанавливает ограничения на использование ресурсов, включая память, для отдельного пользователя или процесса.
10. numactl – управляет доступом процессов к памяти и процессорам, особенно в многоядерных системах.
11. sysrq – позволяет отправлять системным вызовом определенные команды ядру Linux, в том числе сброс памяти (Memory Management).
12. mdb – интерактивный отладчик для системы Solaris, который может использоваться для анализа памяти.
13. Показывает размер подкачки памяти: sudo swapon –show
14. Ctrl (right) + F2 - Переключение на вторую консоль в терминале.
15. :nano /home/vilkov/.bashrc - команда для входа в файл настройки командной оболочки bash. (В открывшемся файле настроек нужно найти следующую команду: «force\_color \_prompt=yes» и разкомментировать эту фразу).
16. :man man - справочник о командном справочнике (выход из справочника нажатием на кнопку Q.
17. :man hier - выводит справочник по файловой системе linux.
18. :cd --help - выводит справку по команде (работает на всех командах).
19. :cd - -переходишь в директорию из которой ранее пришёл.
20. :ls -R -выводит все директории и файлы в них.
21. :ls -l -выводит директории и файлы в длинном формате.
22. :ls -a -выводит все директории, файлы и скрытые папки.
23. :ls -al -выводит длинный формат всех файлов.
24. :ls -am -вывод файлов через запитую.
25. :ls -ax -вывод файлов в алфавитном порядке.
26. :ls -s -вывод информацию о количестве занятых файлами блоков.
27. :which -поиск установленных пакетов (например: which mc -покажет в какой директории он сохранен).
28. :whereis -показывает куда ещё сохранились исполняемые файлы загруженного пакета. Таким образом мы можем локализовать загруженные пакеты (например: whereis mc -покажет в каких директориях хранятся исполнительные файлы программы mc).
29. who am i - покажет в какой консоли я работаю.
30. echo ‘Hello!’ /dev/tty1 – перенаправления вывода в 1 консоль (Пример: cat /etc/hosts > /dev/tty2).
31. df -h - показывает наши диски, их размер и наличие свободного пространства.
32. lsblk - показывает наиболее полную информацию о дисках и дискового пространства.
33. fdisk - показывает всю информацию о дисках (sudo fdisk -l | less).
34. df -T - увидеть все диски подмантированные к системе (к корневому диску).
35. sudo mkfs.ext4 /dev/sdb1 - произведет форматирование диска по созданной таблицы разделов.
36. :sudo e2fsck -l bad.txt /dev/sdb1 - команда говорит о том, чтобы не использовать битые сектора памяти флэш-накопителя, указанные в файле “bad.txt”, созданный во время проверки накопителя, для записи информации.
37. :date -d “-10minutes” +%s - выводит время в формате секунд в минус 10 минут от настоящего.

ФАЙЛОВЫЕ СИСТЕМЫ:

* 1. sudo apt install sleuthkit - установка пакета для анализа данных.
  2. sudo fsstat /dev/sda1 | less - получить информацию о группах блоков на жестком диске (может быть :/dev/sda2…..).
  3. df -h - покажет все наши диски.
  4. ls -li <имя файла> - выводит номер (первый в строке) индексного дискиптера (инода).
  5. stat <имя файла> - выведет полную информацию о файле с его метаданными.

Восстановление удалённых файлов:

* + 1. :sudo init 3 - команда записывается в домашнем каталоге.
    2. :sudo /sbin/debugfs -R “dump <8> /home/Vilkov/sdb1.journal” /dev/sdb1 – делаем сохранение журнала флэшки.
    3. :sudo umount /dev/sdb1 – отмантируем флэшку.
    4. :sudo ext4magic /dev/sdb1 -f / - показывает наш сохраненный журнал (слепок журнала).
    5. :date -d “-10minutes” +%s - создаем точку времени в 10 минут назад в формате секунд (123456789).
    6. :sudo ext4magic /dev/sdb1 -H -a 123456789 | less – показывает индексные дискрипторы удаленных файлов.
    7. :sudo ext4magic /dev/sdb1 -a 123456789 -f / -l - покажет насколько пострадали наши файлы в принципе.
    8. :sudo ext4magic /dev/sdb1 -a 123456789 -f / -j sdb1.journal -r - пытаемся востановить удаленные файлы при помощи копии журнала, который мы создали (востановленные файлы помещаются в папку RECOVERDIR).