***shasum b2br.vdi***

***diff b2br.vdi …..***

***uname -a вывод данных о системе***

***ПЕРВЫЙ ЗАПУСК И ПРОВЕРКА***

***$lsblk // проверяем структуру разделов***

***$su - // логинимся под рутом (именно с - !)***

***Обновление:***

***apt-get update //проверка обновлений apt-get moo***

***$ apt-get upgrade***

***Смена пользователя:***

***su carys //смена пользователя***

***cut -d: -f1 /etc/passwd //отфильтрованный список пользователей***

***$ getent passwd carys***

***getent passwd | grep "username" //есть ли данный пользователь в системе***

***sudo adduser "username" //создать нового пользователя***

***usermod -l newuser olduser //переименовать пользователя***

***deluser "username" //удалить пользователя***

***sudo -lU "username" //какими привилегиями обладает конкретный пользователь***

***sudo cat /etc/passwd***

***СОЗДАНИЕ ГРУППЫ***

***$addgroup carys42***

***$ sudo groupadd evaluating // создаём группу groupadd "groupname"***

***$ getent group***

***$sudo usermod -aG carys42 carys // помещаем туда нашего пользователя***

***sudo adduser "username" "groupname" //добавить в группу пользователя***

***getent group carys42 //проверить наличие пользователя в группе***

***groups carys или id -nG carys // проверить все группы пользователя***

***cat /etc/group //вывести все группы из каталога групп вместе с системными***

***sudo groupdel "groupname" или delgroup "groupname" //удалить группу***

***sudo deluser "username" "groupname" //удалить пользьвателя из группы***

***sudo usermod -G group1,group2 "username"//удалить пользователя из (перечисление) групп***

***sudo usermod -G "username" //удалить пользователя из всех групп***

***sudo whoami //усли у пользователя есть доступ к sudo то выводится root***

***Установить:***

***apt install sudo //установить sudo***

***apt-get install git***

***$ git –version***

***$ sudo apt-get install wget***

***sudo apt-get install vim //установить VIM***

***sudo apt install openssh-server ssh //установить SSH сервер***

***sudo apt-get remove "name" //удаление пакета/программы***

***sudo apt-get --purge remove evolution //удаление пакета/программы с коняги файлами***

***find / -name "name" //ищем файлы по имени***

***sudo dpkg -S /usr/bin/evolution //смотрим имя пакета, которому принадлежит файл***

***systemctl status //активные программы***

***dpkg -s "имя пакета" //проверка установка***

***dpkg -l | grep sudo /проверка установки судо или sssh $ dpkg -l | grep ssh***

***apt-get screenfetch***

***НАСТРОЙКА SSH***

***sudo systemctl status sshd //отображаемся статус SSH сервера***

***$ service ssh restart***

***sudo vim /etc/ssh/sshd\_config //открываем файл конфигурации SSH***

***#~~Port 22~~ меняем значение на Port 4242 //делаем замену порта и пишем без #***

***~~#PermitRootLogin prohibit-password~~ на PermitRootLogin no***

***(По соображениям безопасности делаем невозможно подключение с использованием SSH как root)***

***$ sudo grep Port /etc/ssh/sshd\_config Check if port settings got righ $ sudo service ssh restart***

***ФАЙЕРВОЛ UFW***

***$ sudo apt install ufw или $apt-get install ufw // устанавливаем ufw***

***$ dpkg -l | grep ufw***

***$sudo ufw enable // запускаем файервол***

***$sudo ufw status // убеждаемся, что он работает***

***// даём дефолтные настройки***

***$sudo ufw default deny incoming //запрещает все входящие подключения***

***$sudo ufw default allow outgoing // разрешает исходящие***

***$ sudo ufw allow ssh***

***$sudo ufw allow 4242 // разрешаем наш порт ssh***

***sudo ufw status numbered //выведете нумерованный список текущих правил***

***sudo ufw delete "номер\_правила" //удалить правило***

***sudo ufw delete allow 8888***

***(1. Go to VirtualBox-> Choose the VM->Select Settings 2. Choose “Network”-> “Adapter 1"->”Advanced”->”Port Forwarding) 4242***

***$ sudo systemctl restart ssh***

***$ sudo service ssh status***

***sudo ufw app info 'Apache' //доп информацию о конкретном профиле и опр правилах***

***ufw allow 8080 ufw status***

***ufw deny 8080 ufw status***

***ROOT-ПРАВА ПОЛЬЗОВАТЕЛЮ***

***su - name***

***$usermod -aG root carys***

***$ sudo visudo //Open sudoers file***

***$vim /etc/sudoers // правим конфиг sudo***

***carys ALL=(ALL:ALL) ALL //добавляем строку с именем пользователя, даёт все права sudo***

***$cp /etc/sudoers /etc/sudoers.backup // бэкапим конфиг sudo***

***$shutdown now //выключить комп***

***$reboot // перезагружаемся***

***ДОСТУП ЧЕРЕЗ ТЕРМИНАЛ***

***$ssh carys@localhost -p 4242 // Проброс портов в virtualbox $ ssh carys@127.0.0.1 -p 4242***

***$ logout или $ exit***

***НАСТРОЙКА ВХОДА ПОД SUDO***

***$su - // логинимся под рутом***

***$groups root $groups carys // проверяем группы пользователей***

***$vim /etc/hostname /проверяем и/или меняем имя машины ( файл с названием компьютера)***

***$vim/etc/hosts // проверяем имя хоста***

***hostnamectl //Проверить наименование хоста***

***hostnamectl set-hostname "новое имя хоста" //Установить новое имя хоста***

***sudo reboot //перезагрузка компьютера***

***ЛОГИРОВАНИЕ SUDO***

***$mkdir /var/log/sudo // создаём каталог логирования:***

***$touch /var/log/sudo/sudo.log***

***$vim /etc/sudoers // ещё раз правим конфиг судо sudo visudo***

***Defaults secure\_path=":/usr/bin:/sbin:/bin:/snap/bin”//по сообр без-ти пути, ктр м исп sudo, дб ограничены***

***Defaults passwd\_tries=3 //количество попыток ввода пароля перед тем, как sudo прекратит работу***

***Defaults badpass\_message=“please try again"//выводит сообщение в случае ошибочного ввода sudo пароля***

***Defaults logfile="/var/log/sudo/sudo.log"// (создать саму папку и файл!!!) записывать в лог все попытки подключения к sudo***

***~~Defaults iolog\_dir="/var/log/sudo"~~***

***Defaults log\_input,log\_output //позволяют sudo запускать команду в pseudo-tty и регистрировать все вводимые пользователем и все выходные данные, отправленные на экран***

***Defaults requiretty //разрешить вызов sudo с реального терминала, но не с помощью таких методов, как скрипты***

***// совершаем действие под пользователем через sudo***

***$vim /var/log/sudo/sudo.log // проверяем, заолгировалось ли оно:***

***ПОЛИТИКА ПАРОЛЕЙ***

***$sudo vim /etc/login.defs // правим файл политики паролей***

***PASS\_MAX\_DAYS 30 //Срок действия пароля***

***PASS\_MIN\_DAYS 2 //Минимальное количество дней между сменами пароля***

***PASS\_WARN\_AGE 7 //Количество дней предупреждения до истечения срока действия пароля***

***chage root -M 30 -m 2 -W 7***

***chage root -l***

***chage carys -M 30 -m 2 -W 7***

***chage carys -l***

***$ sudo reboot***

***minlen=10 Минимальная длина пароля***

***ucredit=-1 минимум одна буква в верхнем регистре***

***lcredit=-1 минимум одна буква в нижнем регистре***

***dcredit=-1 минимум одна цифра***

***maxrepeat=3 пароль не должен содержать более 3-х идущих подряд одинаковых символов***

***reject\_username пароль не должен включать имя пользователя***

***difok=7 Количество символов в вашем новом пароле, которые НЕ должны присутствовать в вашем старом пароле***

***$sudo apt-get install libpam-pwquality // устанавливаем утилиту политики***

***$ dpkg -l | grep libpam-pwquality***

***$cp /etc/pam.d/common-password /etc/pam.d/common-password.backup // бэкапим конфиг***

***$vim /etc/pam.d/common-password // правим конфиг***

***password requisite pam\_pwquality.so retry=3 maxrepeat=3 minlen=10 dcredit=-1 ucredit=-1 reject\_username difok=7***

***password requisite pam\_pwquality.so retry=3 maxrepeat=3 minlen=10 dcredit=-1 ucredit=-1 reject\_username enforce\_for\_root***

***// меняем пароли пользователей // в соответствии с политикой:***

***$passwd carys***

***$passwd root***

***passwd сменить свой пароль***

***passwd -aS | grep P Посмотреть все пароли пользователей***

***НАСТРОЙКИ TTY***

***$vim /etc/systemd/logind.conf // правим конфиг tty***

***NAutoVTs=8 // раскомментировать и изменить:***

***ReserveVT=8***

***СОЗДАНИЕ СКРИПТА***

***whereis bash //узнаем где лежит интерпретатор***

***cd "путь к bash"***

***$su user***

***$cd ~/***

***$touch monitoring.sh***

***chmod ugo+x monitoring.sh устанавливаем разрешения chmod 755 monitoring.sh***

***$sudo apt-get install net-tools // для утилиты netstat***

***$vim monitoring.sh // заполняем скрипт командами***

***# !/usr//local/bin/bash***

***wall "***

***#Architecture: $(uname -a)***

***#CPU physical: $( cat /proc/cpuinfo| grep "physical id" | wc -l)***

***#vCPU: $(cat /proc/cpuinfo | grep "^processor" | wc -l)***

***#Memory Usage: $(free -m | awk '{if (FNR == 2) {print $7"/"$2" MB "}}') ($(free -m | awk '(FNR == 2) {printf("%.2f%%"), $3/$2\*100}}’))***

***#Disk Usage: $(df -H | awk '{if (FNR == 4) {printf("%.1f / %.1f Gb (%d%%)"),$3, $2, $5)}}')***

***#CPU load: $(top -b -n 1 | grep ^%Cpu | awk '{printf("%.1f%%"), $2 + $3 +$4 +$6}')***

***#Last boot: $(who -b | awk '{print $3" " $4}')***

***#LVM use: $(if [ $(lsblk | grep lvm | wc -l) -eq 0 ]***

***then***

***echo "no"***

***else***

***echo "yes"***

***fi***

***)***

***#Connections TCP: $(netstat -t | grep tcp |wc -l) ESTABLISHED***

***#User log: $(who | awk '{ print $1 }' | sort -u | wc -l)***

***#Network: IP $(hostname -I) ($(ip link show | awk ' $1 == "link/ether" {print $2}'))***

***#Sudo: $(grep -c 'COMMAND' /var/log/sudo/sudo.log) cmd "***

***НАСТРОЙКА CRON***

***$crontab -e // добавляем скрипт в расписание***

***\*/10 \* \* \* \* sh /home/<user>/monitoring.sh или \*/10 \* \* \* \* ./monitoring.sh***

***crontab -l //Вывод существующих задач в расписании пользователя***

***crontab -r //Удаление файла расписания текущего пользователя***

***crontab -u username //Работа с расписаниями указанных пользователей. Выполняется только от пользователя root***

***\* \* \* \* \* some\_script1***

***#\* \* \* \* \* some\_script2sudo***

***sudo service cron reload //перезапустите сервис***

***/etc/init.d/cron stop //остановить сервис***

***(Вы должны быть пользователем root, чтобы делать эти вещи)***

***$ sudo visudo***

***your\_username ALL=(ALL) NOPASSWD: /usr/local/bin/monitoring.sh***

***$ sudo reboot***

***$ sudo crontab -u root -e***

***\*/10 \* \* \* \* /usr/local/bin/monitoring.sh***

***$ drm:vmw\_host\_log \*ERROR\* Failed to send host log message.***

***$ sudo crontab -u root -l***

***1) Виртуальная машина (ВМ или VM) — это виртуальный компьютер, который использует выделенные ресурсы реального компьютера (процессор, диск, адаптер). Эти ресурсы хранятся в облаке и позволяют ВМ работать автономно. Простыми словами, виртуальная машина позволяет создать на одном компьютере ещё один компьютер, который будет использовать его ресурсы, но работать изолированно.***

***VirtalBox - Программа создающее и эмулиряющая аппаратное обеспечение компьютера, на которую можно накатать свою ОС и использовать как второй компьютер для запуска серверов, облаков и другого ПО.***

***2) LVM — это метод распределения пространства жёсткого диска по логическим томам, размер которых можно легко менять, в отличие от разделов. С LVM пространство жёсткого диска или набора дисков распределяется по физическим томам. Физический том не может располагаться более чем на одном диске. Logical Volume Management (Управление Логическими Томами) - это технология управления устройствами хранения, предоставляющая пользователям возможность объединять и распределять физическое пространство устройств хранения для более простого и гибкого администрирования.***

***1. PV (Physical Volume) — физические тома (это могут быть разделы или целые «неразбитые» диски)***

***2. VG (Volume Group) — группа томов (объединяем физические тома (PV) в группу, создаём единый диск, который будем дальше разбивать так, как нам хочется)***

***3. LV (Logical Volume) — логические разделы, собственно раздел нашего нового «единого диска» ака Группы Томов, который мы потом форматируем и используем как обычный раздел, обычного жёсткого диска.***

***3) Debian и CentOS являются дистрибутивами, серверными операционными системами с открытым исходным кодом. Также не является коммерческой и предоставляется бесплатно для конечных пользователей. Ориентируется на бизнес и корпоративных клиентов.Используется на услугах виртуального выделенного сервера.Debian ОС с открытым исходным кодом, очень хорошо подходящая для новичков, с большим коммьюнити, кучей информацией, а так же обновлениями раз в пару лет (нестабильно). Хороший вариант для частных, небольших проектов. CentOS ОС созданная компанией Red Hat Enterpries Linus так же с открытым исходным кодом, регулярными обновлениями раз в 2-3 года, а так же поддержкой не менее чем на 10 лет.Хороший вариант для больших корпораций, студий и бизнеса.***

***4)SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа. SELinux — функция контроля безопасности, которая ограничивает доступ к определённым модулям ядра. CentOS 7 и RHEL включают её по умолчанию, чтобы обеспечить дополнительный уровень безопасности для системы. Однако функция может быть реализована и в других дистрибутивах Linux, например, Debian.***

***AppArmor — программный инструмент упреждающей защиты, основанный на политиках безопасности (известных также как профили), которые определяют, к каким системным ресурсам и с какими привилегиями может получить доступ то или иное приложение. В AppArmor включён набор стандартных профилей, а также инструменты статического анализа и инструменты, основанные на обучении, позволяющие ускорить и упростить построение новых профилей. AppArmor блокирует уязвимые процессы, ограничивая уязвимость в системе безопасности, которая может возникнуть из-за уязвимости этих процессов. В частности, так же полезен для ограничения работы программ, в которых могут быть экспойты, например, веб-браузера или серверного программного обеспечения. Модель безопасности Apparmor заключается в привязке атрибутов контроля доступа не к пользователям, а к программам. AppArmor обеспечивает изоляцию с помощью профилей, загружаемых в ядро, как правило, при загрузке.AppArmor отличается от остальных реализаций MAC в Linux принципом действия на основе путей, еще он позволяет смешивать профили принудительного исполнения и режима предупреждений. Кроме того AppArmor использует вложенные файлы для облегчения разработки и имеет гораздо более пологий барьер для входа, чем тот же SELinux. В SELinux права доступа определяются самой системой при помощи специально определенных политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux. AppArmor и SELinux обеспечивают безопасность «принудительного контроля доступа» (MAC). SELinux изначально разрабатывался как механизм разграничения доступа, предоставляющий ультимативную безопасность, абсолютный контроль над всей системой и возможность использования гибких политик под разнообразные задачи. У разработчиков не стояло задачи реализовать всё это и еще «чтоб как-нибудь попроще настраивалось и администрировалось». Нет, ни в коем случае! Только безопасность «изо всех сил», только хардкор! Перед AppArmor никогда не стояло подобных задач. Он изначально разрабатывался для удовлетворения требований большинства пользователей. Идея разработчиков заключалась в том, чтобы создать простой, но гибкий механизм, который не доставлял бы больших неудобств при работе с системой.***

***5) UFW (Uncomplicated Firewall) - является самым простым и довольно популярным инструментарием командной строки для настройки и управления брандмауэром в дистрибутивах Ubuntu и Debian. Межсетевой экран, он же firewall служит для автоматической обработки и фильтрации сетевого трафика. Поскольку не все данные, передаваемые по сети, полезны и безопасны, возникла необходимость проверять и обрабатывать их «на лету».Чтобы лучше понять, о чем идет речь, представьте многоквартирный дом. Сотни или даже тысячи людей входят и выходят ежедневно. Среди них есть владельцы квартир, их домочадцы, гости, а также люди, которых никто не приглашал — грабители, мошенники и просто продавцы никому не нужных вещей, надоедающие жителям. Фаервол в данном примере — это строгий консьерж на входе. Он знает и без проблем пропускает каждого жильца, а тех, кого не знает — тщательно проверяет. Имущество и покой обитателей дома при этом находятся в безопасности.***

***6) SSH (Secure Shell — «безопасная оболочка») - это протокол, с помощью которого обеспечивается безопасность удаленного доступа. Методом строгой аутентификации реализуется целостность связи, дополнительно доступ защищен с помощью надежного шифрования. Это самый распространенный способ получения доступа к удаленным серверам Linux. SSH (англ. Secure Shell — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов).***

***7) Sudo (Substitute User and do) - команда которую можно использовать в ситуациях, в которых необходимо повышать привилегии и выполнять команды от имени суперпользователя (root). Root - это пользователь в системах Linux, имеющий полный административный доступ к всей системе.Команда sudo позволяет пользователям без полномочий root запускать команды, которые обычно требуют привилегий суперпользователя, в то время как файл sudoers указывает системе, как обрабатывать команду sudo.***

***8) Обе команды создают нового пользователя в системе. Однако Adduser - утилита для добавления пользователей и групп в систему, а Useradd - это низкоуровневая утилита для добавления пользователей.***

***9) Планировщик заданий Cron - это один из компонентов операционной системы Linux. Он используется для запуска на хостинге определенных скриптов в нужное время, по расписанию. cron — классический демон, использующийся для периодического выполнения заданий в определённое время. Регулярные действия описываются инструкциями, помещенными в файлы crontab и в специальные каталоги. Название cron образовано от греческого слова χρόνος — время.***

***10) GNU — это набор из командной строки и утилит. Linux — это ядро системы. Ядро бесполезно без минимального набора утилит, а утилиты бесполезны без ядра. А GNU/Linux — это уже работоспособная ОС. На основе GNU/Linux делают дистрибутивы, например Debian.***

***11) Команда tty выводит имя специального файла устройства, который ваш ведомый псевдо-телетайп использует для взаимодействия с ведущим устройством. И это, по сути, номер вашего окна терминала.***

***12)Aptitude — оболочка для Advanced Packaging Tool(apt) части системы управления пакетами в операционной системе Debian и её производных. Имеет графический интерфейс (GTK), псевдографический и интерфейс командной строки. apt (advanced packaging tool) — программа для установки, обновления и удаления программных пакетов в операционных системах Debian и основанных на них (Ubuntu, Linux Mint и т. п.), иногда также используется в дистрибутивах, основанных на Mandrake, например Mandriva, ALT Linux и PCLinuxOS. Способна автоматически устанавливать и настраивать программы для UNIX-подобных операционных систем как из предварительно откомпилированных пакетов, так и из исходных кодов.Пакеты берутся из интернет-репозиториев, либо их можно установить с имеющихся носителей. Список источников пакетов хранится в файле /etc/apt/sources.list и в каталоге /etc/apt/sources.list.d/. Графические оболочки для apt позволяют легко добавлять новые и удалять ненужные источники. apt (apt-get) значительно упрощает процесс установки программ в командном режиме. Для пользователей, предпочитающих графический интерфейс, более удобными могут оказаться другие front-end'ы — Synaptic и Adept. Существует текстово‐графический интерактивный пакет (использующий ncurses) — aptitude.***

***aptitude предоставляет интерфейс меню терминала, похожего на терминал в Synaptic, а apt-get не похож. Имеется, правда, несколько незначительных отличий. aptitude автоматически удалит пакеты, тогда как apt-get потребует для этого действия отдельной команды. Команды для обновления вместо dist-upgrade были переименованы в aptitude, возможно, для более точных названий safe-upgrade и full-upgrade соответственно.На самом деле aptitude выполняет функции не только apt-get, но и некоторых сопутствующих инструментов, таких как apt-cache и apt-mark.aptitude имеет немного другой синтаксис запроса для поиска в отличии от apt-cache У aptitude существуют команды why и why-not, которые говорят вам, какие установленные вручную пакеты препятствуют выполнению действия, которое вы, возможно, захотите предпринять.***

***СКРИПТ***

***1) uname -a Самый распространенный способ посмотреть ядро linux - это команда uname. Она выводит информацию о системе в целом, и в том числе о ядре. Чтобы посмотреть всю доступную информацию выполните команду с опцией -a:***

***2) количество физических процессоров:cat /proc/cpuinfo | grep "physical id" | wc -l***

***cat /proc/cpuinfo - эта команда выведет всю инфу о процессоре.***

***Чтобы получить более конкретную информацию, вы можете использовать команду grep – инструмент командной строки для поиска текстовых данных в строках, соответствующих регулярному выражению. Это может помочь вам выводить только имя поставщика, имя модели, количество процессоров, количество ядер и т.д.***

***| - вертикальная черта. Принимает выходные данные одной команды и передает их следующей в качестве входных данных. Количество переданных команд (длина цепочки) произвольно.***

***wc -l считает и выводит количество строк c заданным словом в файле.***

***3) количество виртуальных процессоров:cat /proc/cpuinfo | grep "^processor" | wc -l***

***значок ^ означает, что grep будет принимать в расчет только строчки, где слово processor стоит самым первым.***

***4) Текущая доступная оперативная память RAM на вашем сервере и коэффициент ее использования в процентах:free -m | awk '{if (FNR == 2) {print($7"/"$2"MB")}}' - в МБ***

***free -m | awk '{if (FNR == 2) {printf("%.2f\n"), $3/$2\*100}}')%) - в процентах***

***Команда free - это быстрый и простой способ посмотреть оперативную память linux, получив информацию о её использовании из файла /proc/meminfo. Будет показано общее количество и количество свободной физической памяти и файла подкачки, а также буфера ядра. free -m - это количество памяти в MB. Команда awk - один из самых мощных инструментов для обработки и фильтрации текста. Это не просто утилита, а целый язык разработанный для обработки и извлечения данных. Она читает документ по одной строке за раз, выполняет указанные вами действия и выводит результат на стандартный вывод. Одна из самых частых задач, для которых используется awk - это выборка одной из колонок. Для вывода используем функции-действия:***

***print(строка) - вывод чего либо в стандартный поток вывода;***

***printf(строка) - форматированный вывод в стандартный поток вывода;***

***В функциях-действиях можно использовать различные переменные и операторы:***

***FNR - номер обрабатываемой строки в файле;***

***$ - ссылка на колонку по номеру;***

***5) Текущая доступная память на вашем сервере и коэффициент ее использования в процентах: df -H | awk '{if (FNR == 4) {printf("%.2f / %.2fGb (%d%%)"),$3,$2,$5}}'***

***Команда df позволяет задействовать одноименную утилиту, предназначенную для вывода информации об объеме свободного пространства в каждом из смонтированных разделов.***

***Она выводит имена файлов устройств разделов, полный объем их пространства, объем занятого и свободного пространства, процентный показатель использования разделов, а также точки их монтирования.Базовый синтаксис команды выглядит следующим образом: $ df [параметр] [путь к директории]Утилита поддерживает ряд параметров, а также может выводить данные о разделе, на котором расположена заданная пользователем директория.***

***Параметр -H позволяет выводить числовые значения занятого и свободного пространства на разделах в килобайтах (K), мегабайтах (M) и гигабайтах (G), а не в количестве блоков.***

***6) Текущий коэффициент использования ваших процессоров CPU в процентах:***

***top -b -n 1 | grep ^%Cpu | awk '{printf("%.1f%%\n"), $2 + $3 + $4 + $6}'***

***top (table of processes) — консольная команда, которая выводит список работающих в системе процессов и информацию о них. По умолчанию она в реальном времени сортирует их по нагрузке на процессор. Сама программа top может использоваться в скриптах. Для выполнения команды в этом режиме применяется опция -b. Эта опция полезна для отправки вывода top в другую программу или в файл. В этом режиме top не будет принимать ввод и будет работать до достижения предела повторений, который устанавливается ключом -n. К примеру, запуск команды top в пакетном режиме с одним обновлением информации: 1***

***7) Дата и время последней перезагрузки: who -b | awk '{print $3" "$4}'***

***Команда who служит для получения информации о пользователях, которые подключены к системе, в том числе и об терминальных сессиях, через которые происходит подключение.***

***- b (--boot) — показывает время загрузки операционной системы.***

***8) Активен ли LVM или нет #LVM use: $(if [ $(lsblk | grep lvm | wc -l) -gt 0 ]***

***then echo "yes" else echo "no" fi )***

***Утилита lsblk позволяет отобразить информацию о блочных устройствах. Конкретные возможности утилиты зависят от установленной версии, но в целом команда lsblk может предоставить информацию о самом устройстве, разделении диска и файловой системе.***

***Без аргументов lsblk выведет имя устройства, его размер, права доступа, тип (диск или раздел), точку монтирования и сообщит, является ли устройство съемным (столбец RM).***

***-gt - это оператор сравнения, который обозначает больше, чем .***

***8) количество активных подключений: netstat -t | grep tcp | wc -l***

***Команда netstat выводит данные о сетевых соединениях, таблице маршрутизации, статистику сетевых интерфейсов, маскированных соединений. -t == tcp***

***9)количество пользователей на сервере: who | cut -d " " -f 1 | sort -u | wc -l***

***Команда who служит для получения информации о пользователях, которые подключены к системе, в том числе и об терминальных сессиях, через которые происходит подключение.***

***Команда cut используется, если нужно вырезать часть текста — при этом он может находиться в файле либо быть напечатанным через стандартный ввод.***

***-d (--delimiter=DELIM) — с помощью этой опции пользователь устанавливает свой разделитель вместо стандартного TAB.***

***-f (--fields=LIST) — перечень полей для вырезания.***

***Sort - утилита для вывода текстовых строк в определенном порядке. Проще говоря, для сортировки. Ее можно использовать для сортировки текста из одного или нескольких файлов или c помощью нее может быть выполнена сортировка вывода linux для какой-либо команды.***

***-u - игнорировать повторяющиеся строки***

***10) IP-адрес сервера: hostname -I***

***ip link show | awk '$1 == "link/ether" {print $2}'***

***hostname — это имя, которое присваивается компьютеру, подключенному к сети, которое однозначно идентифицирует в сети и, таким образом, позволяет получить доступ к нему без использования его IP-адреса.Используя имя хоста, вы можете отобразить сетевой адрес (IP-адрес) имени хоста с флагом -i, а параметр -I устанавливает все настроенные сетевые интерфейсы и отображает все сетевые адреса хоста.Утилита ip позволяет посмотреть сетевые интерфейсы и IP адреса им присвоенные, посмотреть и настроить таблицу маршрутизации, включать или отключать сетевые интерфейсы, управлять маршрутизацией и ARP, а также многое другое.Чтобы посмотреть список сетевых интерфейсов используйте объект link:***

***ip link show link или l - физическое сетевое устройство***

***Адрес MAC - это физический адрес, который используется для определения какому устройству надо передать сетевой пакет в локальной сети.***

***11) Как узнать количество команд, выполняемых sudo:***

***grep -c ':' /var/log/sudo/sudo.log -c - подсчитать количество вхождений шаблона;***