|  |  |
| --- | --- |
| 1. Как установить Ubuntu Server на физический сервер или виртуальную машину? | 1. Выбираем пункт “Создать “. 2. Выбираем имя и путь до директории хранения образа Ubuntu 3. Настраиваем все и устанавливаем 4. Указываем имя пользователя, его пароль, hostname виртуалки и проводим установку OpenSSH 5. Можно выбрать дополнительное ПО. Можно установить все вручную, а можно установить при помощи систем автоматизации (Ansible) |
| 1. Как настроить сетевое подключение и управлять сетевыми интерфейсами в Ubuntu Server? | 1. Запускаем виртуальную машину, логинимся там и вводим команду ip a. Нам выведет айпишник нашей машины. 2. Далее в консоли прописываем такую команду: **ssh имямашины@айпишник** 3. Подтверждаем и готово |
| 1. Как установить и настроить SSH-сервер для удаленного доступа к Ubuntu Server? | Установка SSH  sudo apt install openssh-client  Использовать SSH на сервере  sudo apt install openssh-server  Конфигурация  Получить инфу о директивах информации используемых в файле:  man sshd\_config  Проверить конфигурацию после ее изменения и перед запуском сервера:  **sudo sshd -t -f /etc/ssh/sshd\_config**  После внесения изменений нужно сохранить файл и перезапустить приложение sshd  **sudo systemctl restart sshd.service** |
| 1. Как настроить брандмауэр Ubuntu Server для защиты сервера от несанкционированного доступа? | UFW — это простой интерфейс управления брандмауэром  Нужно настроить UFW для протокола IPv6 (он так же подходит для протокола IPv4), нужно прописать эту команду  **sudo nano /etc/default/ufw**  Нужно убедиться, что параметр IPv6 имеет значене yes  **IPv6=yes**  Далее сохраняем и закрываем файл  Для восстановления настроек по умолчанию для UFW необходимо использовать следующие команды:  **sudo ufw default deny incoming**  **sudo ufw default allow outgoing**  Далее нужно разрешить подключаться к SSH:  **sudo ufw allow ssh**  Потом можно поключиться к порту 22:  **sudo ufw allow 22**    Далее, чтобы активиировать UFW нужно ввести команду:  **Sudo ufw enable** |
| 1. Как установить и настроить веб-сервер Apache на Ubuntu Server? | Apache - это веб-сервер с открытым исходным кодом.  Чтобы установить apache2, нужно выполнить следующие команды:  **sudo apt update**  **sudo apt install apache2** |
| 1. Как установить и настроить веб-сервер Nginx на Ubuntu Server? | Сначала нужно установить программу:   1. sudo apt update 2. sudo apt install nginx   Далее нужно настроить брандмауэр:  Для вывода списка конфигрураций приложений, которые известны ufw, необходимо ввести следущую команду:   1. sudo ufw app list   Есть три профиля, доступных для Nginx:   * **Nginx Full**: этот профиль открывает порт 80 и порт 443 * **Nginx HTTP**: этот профиль открывает только порт 80 * **Nginx HTTPS**: этот профиль открывает только порт 443   Если нам нужен 80 порт, то нам нужно ввести следующую команду:   1. sudo ufw allow 'Nginx HTTP'   Для того, чтобы посмотреть на работоспособность, Нужно ввести следущую команду:   1. systemctl status nginx   C помощью инструмента [icanhazip.com](http://icanhazip.com/) можно узнать свой IP-адрес сервера   1. curl -4 icanhazip.com   Когда мы узнали свой ип-адрес, нужно ввести его в адресную строку  http://your\_server\_ip |
| 1. Как настроить доступ к файловой системе на Ubuntu Server, используя Samba? | Чтобы установить Samba, нужно ввести следующие команды:  **Sudo apt update**  **Sudo apt install samba**  Теперь, когда Samba установлена, нам нужно создать каталог для ее совместного использования:  **Mkdir /home/<username>/sambashare/**  Чтобы добавить новый каталог в качестве общего ресурса, мы редактируем файл, выполнив:  **Sudo nano /etc/samba/smb.conf**  В нижней части файла добавьте следующие строки:  **[sambashare]**  **comment = Samba on Ubuntu**  **path = /home/username/sambashare**  **read only = no**  **browsable = yes** |
| 1. Как настроить доступ к файловой системе на Ubuntu Server, используя NFS? | Устанавливаем на хосте:   1. sudo apt update 2. sudo apt install nfs-kernel-server   Затем на клиенте:   1. sudo apt update 2. sudo apt install nfs-common   Далее создаем общие каталоги на хосте  Далее настраиваем экспорт NFS на хосте  Далее настраиваем брандмауэр на хосте  Далее создаем точки монтирования  Тестируем доступ NFS  NFS (сетевая файловая система) – это протокол файловой системы, который позволяем монтировать на сервер удаленные каталоги. |
| 1. Как установить и настроить базу данных MySQL на Ubuntu Server? | MySQL - это быстрый, многопоточный, многопользовательский и надежный сервер баз данных SQL.  Установка MySQL > **sudo apt install mysql-server**  После завершения установки MySQL должен быть запущен автоматически.  /  Чтобы проверить текущее состояние:  **Sudo service mysql status**  /  Если сервер работает некорректно: **Sudo service mysql restart**  /  \  Отредактировать файл mysql.cnf. Там нужно изменить директиву bind-addres на IP-адрес сервера:  **Bind-adress = 192.168.0.5**  192.168.0.5 нужно заменить на свой адрес, который можно определить с помощью команды> **ip addres show** |
| 1. Как настроить удаленный доступ к базе данных Mysql? | Для начала нужно настроить сервер MySQL на прослушивание определенного IP-адреса:  Отредактировать файл mysql.cnf. Там нужно изменить директиву bind-addres на IP-адрес сервера:  **Bind-adress = 192.168.0.5**  192.168.0.5 нужно заменить на свой адрес, который можно определить с помощью команды> **ip addres show**  Далее Нужно перезапустить сервер:  **Sudo systemctl restart mysql**  Предоставление доступа пользователю с удаленного компьютера: 1.Войдите на сервер MySQL как пользователь root:  **Sudo mysql**  2.Если вы используете старый собственный плагин аутентификации MySQL для входа в систему как root, выполните следующую команду:  **Mysql –uroot -p** |
| 1. Как управлять службами Ubuntu Server, включая запуск, остановку и перезагрузку сервисов? | Сначала нужно получить список всех служб:  **service –status-all**  Он покажет полный список сервисов на вашем компьютере.  Далее нужно вводить следующие команды чтобы:  Запустить службу:  **sudo systemctl start ufw**  Остановить службу:  **sudo systemctl stop ufw**  Перезапустить службу:  **sudo systemctl restart ufw**  Проверить статус служб:  **sudo systemctl status ufw** |
| 1. Как настроить и использовать системный журнал Ubuntu Server для отслеживания событий и проблем? | Systemd нужен для того, чтобы управлять журналами.  Чтобы посмотреть журналы, нужно ввести команду > **journalctl**l  Если вы хотите вывести временные метки в формате UTC, нужно ввести следующую команду> **journalctl --utc**  Чтобы вывести для просмотра все записи журнала, нужно ввести следующую команду > **journalctl –b**  Чтобы инфа о сеансах загрузки не удалялась, вы можете создать каталог для хранения журналов > **sudo mkdir –p /var/log/journal**  Так же можно отредактировать файл журнальной системы>  **Sudo nano /etc/system/journal.conf**  В разделе [journal] установите для опции Storage= значение persistent, чтобы включить постоянное хранение журналов:  **[journal]**  **Storage=persistent** |
| 1. Как установить и настроить базу данных PostgreSQL на Ubuntu Server? | Установка > **sudo apt install postgresql**  Файлы конфигурации PostgreSQL хранятся в **/etc/postgresql/<version>/main**  По умолчанию разрешены только подключения из локальной системы, чтобы разрешить всем другим компьютерам подключаться к вашему серверу PostgreSQL, отредактируйте файл /etc/postgresql/\*/main/postgresql.conf.   Найдите строку: *#listen\_addresses* = ‘localhost’ и измените ее на \*:  **listen\_addresses = '\*'**  Теперь, когда мы можем подключиться к нашему серверу PostgreSQL, следующим шагом будет установка пароля для пользователя *postgres*. Выполните следующую команду в командной строке терминала для подключения к базе данных шаблонов PostgreSQL по умолчанию:  **sudo -u postgres psql template1** |
| 1. Как настроить удаленный доступ к базе данных PostgreSQL? | Для начала посмотрим путь расположения конфигурационного файла **postgresql.conf**  **/db/pgsql/postgresql.conf —**это путь расположения нужного нам конфигурационного файла.  Находим и редактируем следующее:  **listen\_addresses = '\*'**  После открываем на редактирование следующий конфигурационный файл: pg\_hba.conf  и внизу добавляем следующую строку:  host     all     all     192.168.0.10/32     password  Далее перезагружаем PostgreSQL |
| 1. Как настроить и использовать утилиту rsync для резервного копирования и синхронизации данных на Ubuntu Server? | Rsync – утилита командной строки.  Для того, чтобы установить, нужно ввести следующую команду:  apt-get install rsync  Далее открываем следующий файл  **Sudo nano /etc/defaut/rsync.conf**  Находим запись:  RSYNC\_ENABLE=false  И меняем на:  RSYNC\_ENABLE=true  Запускаем:  /etc/init.d/rsync start  Настройка:  1.Копирование и синхронизация файлов на локальном компьютере  2.Синхронизация папок на локальной машине  3.Синхронизация с удаленным сервером  4.Синхронизация файлов по SSH  5. Просмотр прогресса при синхронизации  6.Синхронизация не всех файлов в rsync  7. Удаление при синхронизации  8.Максимальный размер файлов  9.Удаление исходны данных  10.Режим симуляции rsync  11.Ограничить скорость передачи  12. Автоматическая синхронизация папок rsync |
| 1. Как настроить и использовать инструменты мониторинга, такие как htop или btop, на Ubuntu Server? | **btop** — монитор ресурсов системы который выводит статистку использования процессора, памяти, сети и дисков.  Установка btop:  sudo apt install btop  Загружаем на сервер последнюю версию и распаковываем архив:  sudo make install  Для запуска программы необходимо выполнить команду:  btop  htop – монитор ресурсов.  Установка:  **apt-get install htop**  Далее необходимо выполнить команду htop, чтобы запустить программу |
| 1. Как установить и использовать систему контроля версий Git на Ubuntu Server? | Сначала нужно установить git:   1. sudo apt update 2. sudo apt install git   Далее нужно убедиться, что программа установилась:   1. git --version   Настройка может быть достигнута с помощью git config команды. В частности, нам нужно указать наше имя и адрес электронной почты, потому что Git встраивает эту информацию в каждый коммит, который мы делаем. Мы можем продолжить и добавить эту информацию, введя:   1. git config --global user.name "Your Name" 2. git config --global user.email "youremail@domain.com"   Мы можем отобразить все элементы конфигурации, которые были установлены, введя:   1. git config --list |
| 1. Как настроить и использовать программное обеспечение для виртуализации, такое как KVM или VirtualBox, на Ubuntu Server? | Для установки KVM на Ubuntu Server нужно выполнить следующие шаги:  1. Установить пакеты для работы с виртуализацией:  sudo apt-get install qemu-kvm libvirt-bin virtinst bridge-utils  2. Добавить пользователя в группу libvirtd:  sudo adduser <имя\_пользователя> libvirtd  3. Перезагрузить компьютер:  sudo reboot  4. После перезагрузки проверить, что KVM установлен и работает:  sudo virsh list --all  Для установки VirtualBox на Ubuntu Server нужно выполнить следующие шаги:  1. Добавить репозиторий VirtualBox:  sudo add-apt-repository "deb [arch=amd64] <https://download.virtualbox.org/virtualbox/debian> $(lsb\_release -cs) contrib"  2. Скачать и добавить ключ репозитория:  wget -q <https://www.virtualbox.org/download/oracle_vbox_2016.asc> -O- | sudo apt-key add -  3. Обновить список пакетов и установить VirtualBox:  sudo apt-get update sudo apt-get install virtualbox-6.0  4. Добавить пользователя в группу vboxusers:  sudo adduser <имя\_пользователя> vboxusers  5. Перезагрузить компьютер:  sudo reboot  6. После перезагрузки проверить, что VirtualBox установлен и работает:  VBoxManage --version |
| 1. Как установить и настроить сервер Ansible на Ubuntu Server? | 1. Установка 2. 1. sudo apt update 3. sudo apt install ansible   2.Настройка файла инвентаризации   1. sudo nano /etc/ansible/hosts   Если вы хотите проверить файл инвентаризации   1. ansible-inventory --list -y   3.Тестирование подклчения   1. ansible all -m ping -u root   4.Запуск ситуативных команд |
| 1. Как настроить и использовать систему управления пакетами apt для управления установкой и обновлением программного обеспечения на Ubuntu Server? | Установка apt:  **Sudo apt install nmap**  Обновление пакетов:  **Sudo apt update** |
| 1. Как установить и настроить веб-приложения, такие как Nextcloud, на Ubuntu Server? | Установка:   1. sudo snap install nextcloud   Проверить, Установлен ли он:   1. snap changes nextcloud   Настройка:  Послеустановки NextCloud создаем аккаунт с логином и паролем.  Следом приходит сообщение, что запись настроена правильно. Теперь все права для работы с базой данных переданы пользователю username.  Переходим к настройке доменного имени. Допустим, сервер доступен по адресу 192.168.0.15, но мы хотим, чтобы он был доступен по адресу «mycloud.com». Для этого мы изменяем запись trusted\_domains в файле config.php. По умолчанию адрес домена в NextCloud дополняется файлом с расширением**«**index.php». |
| 1. Как настроить утилиту iperf3 и проверить пропускную способность сети между двумя серверами? | При помощи данной команды можно установить iperf3 в Ubuntu Linux:  **sudo apt install iperf3**  **Запуск серверной версии**  Запустите iperf3 на сервере командой:  **iperf3 -s**  После этого сервер iperf3 начнет слушать порт 5201 на всех сетевых интерфейсах.  Пока идет тестирование, придется держать iperf3 запущенным.  Как уже отмечалось, iperf3 будет слушать все сетевые интерфейсы. Однако можно забиндить его на определенный IP командой:  **iperf3 -s -D -B ip.add.re.ss**  **Запуск клиентской версии**  На клиенте iperf3 запускается так:  **iperf3 -c <хост>**  При выполнении данной команды iperf3 будет инициировать сетевой соединение на указанный адрес хоста (домен либо IP) через порт 5021. Будет начато тестирование. |
| 1. Как изменить файлы конфигурация php для увеличения производительности сервера? | Открыть файл php.ini  Значение max\_execution\_time в файле php.ini используется для установки максимального времени выполнения отдельного процесса PHP до его завершения. Эта настройка по умолчанию составляет 30 секунд, рекомендуется установить значение 5 секунд:  **max\_execution\_time = 5**  Лучше установить максимальный размер файла, который можно загрузить. Кроме того, лучше всего указать, сколько файлов может быть загружено одновременно: **file\_uploads = 1**  **upload\_max\_filesize = 10M**   1. **max\_file\_uploads = 3**   По умолчанию PHP позволяет загружать 20 файлов за один запрос. Максимальный размер файла для загрузки составляет 2 МБ. Здесь я настроен на загрузку максимум 3 файлов в одном запросе. Максимальный размер файла для каждого файла составляет 10 МБ. Не устанавливайте это значение слишком много. Большой, иначе произойдет тайм-аут. |
| 1. Какое назначение утилиты netplan? | Netplan - это утилита для простой настройки сети в системе Linux. Вы просто создаете описание на языке YAML требуемых сетевых интерфейсов и того, для чего каждый из них должен быть настроен. Исходя из этого описания, Netplan сгенерирует всю необходимую конфигурацию для выбранного вами инструмента визуализации. |
| 1. Что такое Ansible и для чего он используется? | Это ПО с открытым исходным кодом, которое автоматизирует поставку ПО, управление конфигурацией и развертывание приложений |
| 1. Как написать простой плейбук для развертывания веб-сервера с использованием Ansible? | Создаем файл > playbook.yaml  Добавим следущее в этот файл:  **-** **name:** My first play  **hosts:** virtualmachines  **tasks:**  **-** **name:** Ping my hosts  **ansible.builtin.ping:**  **-** **name:** Print message  **ansible.builtin.debug:**  **msg:** Hello world  И далее вводим следущую команду, чтобы запустить установку. > **ansible-playbook** |
| 1. Как управлять группами хостов и использовать переменные в Ansible? | Для управления группами хостов в Ansible нужно создать файл inventory, в котором будут указаны все хосты и их группы. Например:  [web] webserver1 webserver2  [db] dbserver1 dbserver2  [all:vars] ansible\_user=ubuntu  В этом примере созданы две группы хостов "web" и "db", а также указана переменная "ansible\_user", которая будет использоваться для всех хостов.  Чтобы использовать переменные в Ansible, нужно создать файл переменных (vars) и указать их значения. Например:  # vars.yml --- web\_port: 80 db\_port: 5432  Затем можно использовать эти переменные в плейбуках Ansible. Например:  # playbook.yml --- - name: Configure web server   hosts: web   vars\_files:     - vars.yml   tasks:     - name: Install Apache       apt:         name: apache2         state: present     - name: Configure Apache       template:         src: templates/apache.conf.j2         dest: /etc/apache2/apache.conf       notify: restart apache  В этом примере переменная "web\_port" будет использована в шаблоне конфигурации Apache. |
| 1. Что такое Шлюз/Gateway? | Проводник для передачи информации между компьютерными сетями с разными протоколами данных (глобальной и локальной) |
| 1. Что такое dns? | Компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста |
| 1. Что такое права пользователей и зачем они нужны в Ubuntu? | Зачем нужны права пользователя:   1. Получить доступ к папкам и файлам, которые не доступны обычному пользователю 2. Доступ к редактированию файлов, изменение параметров конфигурации   Права пользователя – это права, которые определяют, что может делать пользователь, а что нет |
| 1. Как создать нового пользователя в Ubuntu Server и назначить ему права на доступ к файлам и директориям? | Выполните вход через подключение SSH на ваш сервер как **root** user:   1. ssh root@your\_server\_ip\_address   Затем добавляем нового пользователя:   1. adduser isp21    Вам будет предложено создать и проверить пароль пользователя.  Далее вам будет предложено ввести определенную информацию о вашем новом пользователе. Вы можете принимать значения по умолчанию или оставить их пустыми.  Воспользуйтесь командой usermod для добавления пользователя в группу **sudo**:   1. usermod -aG sudo isp21   Чтобы проверить, что новые разрешения sudo доступны, сначала нужно воспользоваться командой su для переключения на новую учетную запись пользователя:   1. su – isp21   Далее мы можем добавить sudo |
| 1. Как изменить пароль пользователя и разрешить ему доступ к конкретным файлам и директориям в Ubuntu? | Чтобы поменять пароль надо ввести следущую команду  **Passwd –d пользователь**  **-d** – удалить пароль пользователя.  А чтобы поставить другой пароль, нужно ввести команду:  **Passwd**  Чтобы узнать права на файл linux выполните такую команду, в папке где находится этот файл:  **ls -l**  Есть такой флаг прав > **rwx** < который дает все права |
| 1. Как создать группу пользователей и назначить им права на доступ к определенным файлам и директориям в Ubuntu? | Все группы, созданные в системе, находятся в файле /etc/group  **nano /etc/group**  Mы сами вручную можете менять группы файлов для этого есть команда chgrp:  **chgrp имя\_группы имя\_файла**  Например создадим файл test:  **touch test**  И изменим для него группу:  **chgrp adm test**  Если вы хотите создать группу linux, это можно сделать командой newgrp:  **sudo groupadd test** |
| 1. Как использовать команду sudo для выполнения команд от имени другого пользователя или суперпользователя в Ubuntu? | Для этого достаточно написать sudo перед именем программы: sudo whoami. Если вы хотите выполнить программу не от имени root, а от имени другого пользователя, то можно использовать опцию –u,  например: **sudo –u isp21 whoami 2** |
| 1. Как изменить права доступа к файлам и директориям, используя команду chmod в Ubuntu? | Эта команда имеет типичный для команд linux синтаксис:  **Chmod опции права /путь/к/файлу**   * **r** - чтение; * **w** - запись; * **x** - выполнение; * **s** - выполнение  от имени суперпользователя (дополнительный); * u+x - разрешить выполнение для владельца; * ugo+x - разрешить выполнение для всех; * ug+w - разрешить запись для владельца и группы; * o-x - запретить выполнение для остальных пользователей; * ugo+rwx - разрешить все для всех; |
| 1. Как изменить владельца файла или директории и назначить права доступа для других пользователей в Ubuntu? | Вы можете изменить владельца папки с помощью файлового менеджера, например в Nautilus. Но для этого надо запустить файловый менеджер от имени суперпользователя. Откройте терминал с помощью сочетания клавиш**Ctrl+Alt+T**и выполните команду:  sudo nautilus  Затем найдите нужную папку, и кликните по ней правой кнопкой мыши. В открывшемся контекстном меню выберите пункт **Свойства**:  В появившемся окне перейдите на вкладку Права. Здесь можно изменить владельца папки и группу владельца с помощью выпадающего списка напротив соответствующего пункта:  Если вам нужно чтобы эти изменения были применены для всех вложенных папок и файлов, нажмите внизу окна кнопку**Изменить права на вложенные файлы...** |
| 1. Как настроить ACL (Access Control Lists) для определенных файлов и директорий в Ubuntu? | Для настройки ACL в Ubuntu нужно выполнить следующие шаги:  1. Установить пакеты для работы с ACL:  sudo apt-get install acl  2. Создать файл или директорию, для которых нужно настроить ACL.  3. Установить права доступа для файла или директории:  sudo chmod <права\_доступа> <имя\_файла\_или\_директории>  4. Настроить ACL для файла или директории:  sudo setfacl -m u:<имя\_пользователя>:<права\_доступа> <имя\_файла\_или\_директории>  5. Проверить настройки ACL:  sudo getfacl <имя\_файла\_или\_директории>  Пример:  Создадим директорию "test" и настроим ACL для пользователя "user1" так, чтобы он имел права на чтение, запись и выполнение файлов в этой директории:  1. Создать директорию "test":  sudo mkdir /test  2. Установить права доступа для директории "test":  sudo chmod 755 /test  3. Настроить ACL для директории "test":  sudo setfacl -m u:user1:rwx /test  4. Проверить настройки ACL:  sudo getfacl /test  Результат должен быть следующим:  # file: test/ # owner: root # group: root user::rwx user:user1:rwx group::r-x mask::rwx other::r-x |
| 1. Как настроить SUID и SGID для файлов и директорий в Ubuntu? | Для настройки SUID и SGID для файлов и директорий в Ubuntu нужно выполнить следующие шаги:  1. Установить права доступа для файла или директории:  sudo chmod <права\_доступа> <имя\_файла\_или\_директории>  2. Настроить SUID для файла или директории:  sudo chmod u+s <имя\_файла\_или\_директории>  3. Настроить SGID для директории:  sudo chmod g+s <имя\_директории>  Пример:  Создадим директорию "test" и настроим SGID, чтобы все новые файлы и директории в этой директории наследовали группу от родительской директории:  1. Создать директорию "test":  sudo mkdir /test  2. Установить права доступа для директории "test":  sudo chmod 2775 /test  Обратите внимание, что здесь установлен SGID для группы.  3. Создать новую директорию "subdir" внутри "test":  sudo mkdir /test/subdir  4. Проверить права доступа для директории "subdir":  ls -ld /test/subdir  Результат должен быть следующим:  drwxrwsr-x 2 root root 4096 Oct 28 10:00 /test/subdir  Обратите внимание, что здесь установлен SGID для группы и новая директория "subdir" унаследовала группу от родительской директории "test". |
| 1. Что такое группы пользователей и зачем они нужны в Ubuntu? | Группы в линукс – это совокупность пользователей. Основная цель групп- определить набор привелегий, таких как разрешение на чтение, запись или выполнение для данного ресурса, которые могут быть совместно использованы пользователями внутри группы. |
| 1. Как создать новую группу пользователей в Ubuntu Server и добавить пользователей в нее? | **sudo groupadd testgroup**  groupad – команда для создания группы  Чтобы добавить пользователя в группу:  **Usermod -aG** |
| 1. Как изменить принадлежность пользователя к группе и разрешить ему доступ к определенным файлам и директориям в Ubuntu? | Для изменения принадлежности пользователя к группе в Ubuntu нужно выполнить следующие шаги: 1. Проверить, к какой группе принадлежит пользователь: groups <имя\_пользователя> 2. Если нужно добавить пользователя в другую группу, выполнить команду: sudo usermod -a -G <имя\_группы> <имя\_пользователя> 3. Проверить, что пользователь добавлен в группу: groups <имя\_пользователя> 4. Настроить права доступа для файлов и директорий: sudo chown <имя\_пользователя>:<имя\_группы> <имя\_файла\_или\_директории> 5. Установить права доступа для файлов и директорий: sudo chmod <права\_доступа> <имя\_файла\_или\_директории> Пример: Добавим пользователя "user" в группу "www-data", чтобы он мог редактировать файлы веб-сервера: 1. Проверить, к какой группе принадлежит пользователь "user":  groups user  Результат должен быть следующим:  user : user  2. Добавить пользователя "user" в группу "www-data":  sudo usermod -a -G www-data user  3. Проверить, что пользователь добавлен в группу "www-data":  groups user  Результат должен быть следующим:  user : user www-data  4. Настроить принадлежность пользователя "user" к группе "www-data" для директории "/var/www":  sudo chown -R user:www-data /var/www  5. Установить права доступа для директории "/var/www": sudo chmod -R 775 /var/www |
| 1. Как изменить права доступа для определенной группы пользователей в Ubuntu? | ------------------------------------------------------------------------------------------  Для изменения прав доступа для определенной группы пользователей в Ubuntu нужно выполнить следующие шаги:  1. Определить группу, для которой нужно изменить права доступа.  2. Использовать команду chmod для изменения прав доступа для определенной группы пользователей.  Например, если нужно установить права доступа на чтение и запись для группы "www-data" для директории "/var/www", выполните следующую команду:  sudo chmod -R g+rw /var/www  Эта команда установит права на чтение и запись для группы "www-data" для всех файлов и поддиректорий в директории "/var/www".  Если нужно установить права на выполнение, добавьте букву "x" к команде chmod, например:  sudo chmod -R g+rwx /var/www  Эта команда установит права на чтение, запись и выполнение для группы "www-data" для всех файлов и поддиректорий в директории "/var/www". |
| 1. Как использовать команду chgrp для изменения владельца группы файлов и директорий в Ubuntu? | **chgrp [параметры] новая\_группа имя\_файла**   чтобы изменить группу имени файла filename на www-data вы должны запустить:  chgrp www-data filename |
| 1. Как настроить sudo для разрешения выполнения команд суперпользователя только для определенной группы пользователей в Ubuntu? | Для настройки sudo для разрешения выполнения команд суперпользователя только для определенной группы пользователей в Ubuntu нужно выполнить следующие шаги:  1. Отредактировать файл конфигурации sudoers командой:  sudo visudo  2. Найти строку, начинающуюся с "%sudo" и заканчивающуюся словом "ALL".  3. Заменить слово "ALL" на имя группы пользователей, которым нужно разрешить выполнение команд суперпользователя.  Например, если нужно разрешить выполнение команд суперпользователя только для группы "admins", строка должна выглядеть так:  %sudo ALL=(ALL:ALL) ALL  заменить на  %admins ALL=(ALL:ALL) ALL  4. Сохранить изменения и закрыть файл.  Теперь только пользователи, входящие в группу "admins", смогут выполнять команды суперпользователя с помощью sudo. |
| 1. Как использовать setgid для создания файлов и директорий, которые наследуют права группы в Ubuntu? | Для использования setgid для создания файлов и директорий, которые наследуют права группы в Ubuntu, нужно выполнить следующие шаги:  1. Создать группу, которой будут принадлежать пользователи, имеющие доступ к файлам и директориям:  sudo groupadd examplegroup  2. Установить setgid для директории, в которой будут создаваться файлы и директории:  sudo chmod g+s /path/to/directory  3. Установить права на директорию и ее содержимое:  sudo chown -R username:examplegroup /path/to/directory sudo chmod -R 775 /path/to/directory  Где "username" - имя пользователя, который будет создавать файлы и директории.  Теперь при создании новых файлов и директорий в этой директории они будут автоматически наследовать права группы "examplegroup". |
| 1. Как использовать инструменты мониторинга групп пользователей, такие как Group Policy, в Ubuntu? |  |
| 1. Как создать вложенную группу пользователей и назначить ей права доступа в Ubuntu? | Создаем группу test > **sudo groupadd test**  Создаем пользователя > **sudo useradd isp21**  Добавляем в группу пользователя, которому хотим выдать права на работу с папкой.  **Sudo usermod –aG названиеГруппы имяПользователя**  Устанавливаем связь между папкой и группой:  **Sudo chgrp test test**  Теперь выдаем права:  **Chmod g+rw** |
| 1. Как настроить ACL для групп пользователей в Ubuntu и разрешить доступ к определенным файлам и директориям? |  |