Нубские дела

- Смена имени хоста и IP
- Пользователи
- Добавление ssh ключа - id_rsa.pub
- Команда sudo без пароля в LINUX
- Как сбросить root-пароль в CentOS 6 и CentOS 7
- Linux iptables delete prerouting rule command
- Как просмотреть историю команд другого пользователя в Linux?
- Open VPN
- Запуск с несколькими конфиг файлами...
- Секреты Notepad++

Смена имени хоста и IP

`hostname` - Вывод имени хоста

`sudo hostname servername` - изменяет имя хоста на *servername.* Так же рекомендуется подкорректировать файл *hosts* и сделать перезапуск

`ifconfig` - отображает IP адреса

`ip addr` or `ip a` - список интерфейсов, адресов и статуса

`ls /etc/netplan/` - необходимо отредактировать файл заканчивающийся на *.yaml* по адресу */etc/netplan.* Если файла нет вводим `sudo netplan generate` . Название файла конфигурации в *netplan* может отличаться, *“00-installer-config.yaml”*, у вас скорей всего будет иное название.

`sudo nano /etc/netplan/00-installer-config.yaml` - открывает файл *00-installer-config.yaml* в редакторе *nano*

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [10.0.2.15/24]
      gateway4: 10.0.2.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

> Не используйте табуляцию - клавишу `Tab` , интерпретатор файла реагирует на отступы!

Пользователи

Введение

Команда `sudo` служит механизмом для предоставления прав администратора, которые обычно доступны только пользователю **root** user, для обычных пользователей. Из этого руководства вы узнаете, как создать нового пользователя с привилегиями `sudo` в Ubuntu 18.04 без изменения файла `/etc/sudoers` на вашем сервере. Если вы хотите настроить `sudo` для существующего пользователя, перейдите к шагу 3.

Шаг 1 — Выполнение входа на ваш сервер

Выполните вход через подключение SSH на ваш сервер как **root** user:

```
ssh root@your_server_ip_address
```

Шаг 2 — Добавление нового пользователя в систему

Используйте команду `adduser` для добавления нового пользователя в вашей системе:

```
adduser sammy
```

Обязательно замените `sammy` на имя пользователя, которое вы хотите использовать. Вам будет предложено создать и проверить пароль пользователя:

```
Output
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Далее вам будет предложено ввести определенную информацию о вашем новом пользователе.

```
utput
Changing the user information for sammy
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
```

Шаг 3 — Добавление пользователя в группу *sudo*

Воспользуйтесь командой `usermod` для добавления пользователя в группу **sudo**:

```
usermod -aG sudo sammy
```

Не забудьте заменить `sammy` на имя пользователя, которое вы только что добавили. По умолчанию в Ubuntu все участники группы **sudo** имеют полный набор привилегий `sudo`.

Отображение групп пользователя

`id -Gn имя_пользователя`

Шаг 4 — Тестирование доступа к *sudo*

Чтобы проверить, что новые разрешения `sudo` доступны, сначала нужно воспользоваться командой `su` для переключения на новую учетную запись пользователя:

```
su - sammy
```

Используя нового пользователя, убедитесь, что вы можете использовать `sudo`, добавив `sudo` перед командой, которую вы хотите запустить с привилегиями суперпользователя:

```
sudo command_to_run
```

Например, вы можете вывести список содержимого директории `/root`, которое обычно доступно только для пользователя root user:

```
sudo ls -la /root
```

При первом использовании `sudo` в сеансе вам будет предложено ввести пароль учетной записи данного пользователя. Введите пароль, чтобы продолжить:

```
Output:
[sudo] password for sammy:
```

> **Примечание:** это *не* запрос пароля **root**! Введите пароль пользователя с привилегиями sudo, а не пароль **root**.

Если ваш пользователь находится в соответствующей группе и вы ввели правильный пароль, команда с `sudo` будет запущена с правами **root**.

Добавление ssh ключа - id_rsa.pub

Копирование публичного ключа вручную

Необходимо убедиться, что директория *~/.ssh* существует (в папке пользователя)

`mkdir -p ~/.ssh` - Если ее нет то данная команда создаст. Далее можно создать или отредактировать файл *authorized_keys*, это можно сделать командой `echo` **`строка_публичного_ключа`** `>> ~/.ssh/authorized_keys` Строка должна начинаться с *ssh-rsa AAAA...*

Далее убедимся, что директория *~/.ssh* и файл *authorized_keys* имеют подходящие права доступа: `chmod -R go= ~/.ssh`

`chmod 700 ~/.ssh` - ограничьте права доступа к этому каталогу только себе!

Эта команда удаляет права доступа для “group” и “other” для директории *~/.ssh/.*

Если вы используете аккаунт *root* для настройки ключей для аккаунта пользователя, важно, чтобы директория *~/.ssh* принадлежала этому самому пользователю, а не пользователю *root* :

`chown -R yuzer:yuzer ~/.ssh`

В нашем руководстве мы используем пользователя с именем ***yuzer*** , вам же следует использовать имя своего пользователя в команде выше.

Аутентификация на сервере Ubuntu с использованием ключей SSH

`ssh username@remote_host` - вход на сервер по *ssh*

Если вы заходите на удалённый хост по SSH в первый раз, вы можете увидеть вывод следующего вида:

```
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
```

Это означает, что ваш локальный компьютер не узнал удалённый хост. Напечатайте “*yes*” и нажмите `ENTER` для продолжения.

Отключение аутентификации по паролю на вашем сервере

вход на сервер с использованием пароля всё есть активен, что означает, что сервер уязвим для атак с перебором пароля (brute-force attacks). Вход *ssh* по паролю можно отключить отредактировав файл *sshd_config*

`sudo nano /etc/ssh/sshd_config`

Внутри файла найдите директиву *PasswordAuthentication*. Она может быть закомментирована. Раскомментируйте её при необходимости и установите её значение в “*no* ”. Это отключит возможность входа на сервер по паролю.

```
...
PasswordAuthentication no
...
```

Для применения внесённых изменений нам необходимо перезапустить сервис *sshd* - `sudo systemctl restart ssh`

В качестве меры предосторожности откроем новое окно терминала и проверим, что соединение по *ssh* работает корректно, перед тем, как закрывать текущую сессию.

Скопировать ключ так же можно с помощью scp (с одного хоста на другой)

`scp -p /home/yuzer/.ssh/authorized_keys yuzer@10.0.10.48:/home/yuzer/.ssh/`

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2   #Пример синтакса
```

> SCP - перезапишет уже сущесвующий файл!

Команда sudo без пароля в LINUX

Чтобы отключить пароль sudo, надо добавить к строчке настройки пользователя или группы директиву NOPASSWD. Синтаксис такой:

имя_пользователя ALL=(ALL) NOPASSWD: ALL

Для того чтобы отключить пароль sudo для определенного пользователя нужно открыть файл конфигурации sudo и отключить запрос пароля следующей строчкой, например для пользователя losst:

```
 sudo visudo
```

```
losst ALL=(ALL) NOPASSWD: ALL
```

Сохраните изменения и закройте файл, на всякий случай напомню что в vi для перехода в режим вставки используется клавиша **i**, для сохранения команда **:w** и команда **:q** для выхода. Теперь sudo не будет запрашивать пароль у выбранного пользователя при выполнении любых команд.

Для того чтобы разрешить пользователю выполнять только некоторые команды без пароля (например apt и reboot) добавьте следующую строчку:

```
losst ALL=(ALL) NOPASSWD: /usr/bin/apt, /sbin/reboot
```

Чтобы отключить пароль для группы пользователей используйте следующий код:

```
%имя_группы ALL=(ALL) NOPASSWD: ALL
```

Теперь у пользователей группы имя_группы утилита sudo не будет спрашивать пароль, а у всех остальных будет.

Как сбросить root-пароль в CentOS 6 и CentOS 7

Общий алгоритм сброса пароля

- Откройте VNC-консоль сервера
- Перезагрузите сервер и измените параметры загрузки ядра для загрузки в однопользовательский режим
- Установите новый пароль root без необходимости ввода старого

1. Доступ к VNC-консоли

Этот шаг одинаков для всех разновидностей Linux. Для облачного сервера найдите свой сервер в разделе "Облачные серверы > Создание и управление" в панели управления. Для выделенного сервера зайдите в "Выделенные серверы > Управление", соответственно. Откройте VNC-консоль с помощью одноименной кнопки:

54f9b2bc86ec3da8afe661c8758eabe7.png

Вид VNC-консоли может немного отличаться в зависимости от типа сервера и ОС.

2. Перезагрузка сервера и редактирование параметров загрузки ядра

Чтобы загрузить сервер в однопользовательский режим, вам потребуется отредактировать параметры загрузки ядра с помощью меню загрузчика GRUB. Поведение меню и параметры загрузки зависят от версии ОС и от того, является сервер облачным или выделенным.

2.1. CentOS 6, выделенный сервер

Перезагрузите сервер, нажав CTRL + ALT + DEL в окне VNC-консоли.

После меню BIOS, перед запуском ОС, появляется таймер. Нажмите ESC, чтобы остановить таймер и войти в меню загрузки GRUB.

11f1eadbdcc46f43538823ba8bd0f057.png

Используйте клавиши ↓ и ↑ для перемещения по меню. Выберите загрузочную строку и нажмите "e", чтобы отредактировать ее.

338100ab3da5ba5896da71d098791aba.png

Выберите строку, начинающуюся с "kernel /vmlinuz- ". Нажмите "e", чтобы отредактировать ее.

7619c18d4f450fda7f196dec9be2cc0d.png

Добавьте параметр "single" после пробела в конце строки.

5c4ec12d20c649ec100e94a0d115077d.png

Нажмите ENTER, чтобы сохранить изменения. Изменения будут сохранены до следующей перезагрузки.

Нажмите "b", чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

2.2. CentOS 6, облачный сервер

Перезагрузите сервер, нажав кнопку "Send CtrlAltDel" в окне VNC-консоли. Загрузочное меню с таймером появится сразу после меню BIOS.

Нажмите TAB, чтобы остановить таймер и отредактировать параметры загрузки. Изменения будут сохранены до следующей перезагрузки.

ddeec4ea727061773b8cfc845b2a82a6.png

Удалите параметры, выделенные красным цветом на рисунке ниже. Добавьте "1" (без кавычек и через пробел) в конце строки.

4540dd57c0762eae45aabed440e4d68b.png

Строка параметров должна выглядеть следующим образом:

6e45f8d0dfbaccdebfc33d2177dda0be.png

Нажмите ENTER, чтобы чтобы запустить систему в однопользовательском режиме.

Перейдите к разделу "Установка нового пароля root" в этой статье.

2.3. CentOS 7, выделенный сервер

Перезагрузите сервер, нажав CTRL + ALT + DEL в VNC-консоли. После меню BIOS, перед запуском ОС, появляется меню GRUB.

6b11b0562eae117a965828044bb4c801.png

Используйте клавиши ↓ и ↑ для навигации по меню, выберите свою загрузочную строку и нажмите "e", чтобы отредактировать ее.

Найдите строку, которая начинается с "linux" в 64-разрядной версии IBM Power Series или "linux16" в системах на базе BIOS x86-64 или "linuxefi" в системах UEFI. Измените параметр "ro" на "rw", удалите параметры "rhgb" и "quiet"; добавьте "rd.break enforcing=0" в конце строки.

22b4ac28da366b0790a1473056c63b16.png

0aac8bbae746dd3c252fdaaed857c267.png

Нажмите CTRL + X, чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

2.3. CentOS 7, облачный сервер

Перезагрузите сервер, нажав кнопку "Send CtrlAltDel" в окне VNC-консоли. После меню BIOS, перед запуском ОС, появляется загрузочное меню.

Используйте клавиши ↓ и ↑ для навигации по меню, выберите загрузочную строку и нажмите "e", чтобы отредактировать ее.

02364966866b1e20225ad9a11b7cbf95.png

Найдите строку, которая начинается с "linux" в 64-разрядной версии IBM Power Series или "linux16" в системах на базе BIOS x86-64 или "linuxefi" в системах UEFI. Измените параметр "ro" на "rw", удалите параметры, отмеченные красным на изображении ниже:

a7ec5fc253e55595a8b9e86bb4ef2b24.png

Добавьте "rd.break enforcing=0" в конце строки. Строка параметров должна выглядеть следующим образом:

77024959610bb9c8aa853cdb90b8b332.png

Нажмите CTRL + X, чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

3. Установка нового пароля root

В однопользовательском режиме вы работаете с правами пользователя root. Выполните следующие команды для изменения пароля root и перезагрузки:

3.1 **CentOS 6**

```
passwd root
reboot
```

3.2 **CentOS 7**

```
chroot /sysroot
passwd root
touch /.autorelabel
exit
reboot
```

Linux iptables delete prerouting rule command

Step 1 – List the pretrouting rules

The syntax is as follows:
`sudo iptables -t nat -v -L PREROUTING -n --line-number`
OR
`sudo iptables -t nat -v -L -n --line-number`
Iptables list the pretrouting rules on Linux
Where,

- **`-t nat`** : Select nat table.
- **`-v`** : Verbose output.
- **`-L`** : List all rules in the selected chain. In other words, show all rules in nat table.
- **`-L PREROUTING`** – Display rules in PREROUTING chain only.
- **`-n`** : Numeric output. IP addresses and port numbers will be printed in numeric format.
- **`--line-number`** : When listing rules, add line numbers to the beginning of each rule, corresponding to that rule's position in the chain. You need to use line numbers to delete nat rules.

Step 2 – Iptables delete prerouting nat rule

The syntax is:
`sudo iptables -t nat -D PREROUTING {rule-number-here}`
To delete rule # 1 i.e. the following rule:

```
1    15547  809K DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
tcp dpt:80 to:10.147.164.8:80
```

Type the following command:
`sudo iptables -t nat -D PREROUTING 1`

OR

```
sudo iptables -t nat --delete PREROUTING 1
```

Verify that rule has been deleted from the PREROUTING chain , enter:

```
sudo iptables -t nat -v -L PREROUTING -n --line-number
```

Linux iptables remove prerouting command

Here is another DMZ rule:

```
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

To remove prerouting command, run:

```
sudo iptables -t nat -D PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

Make sure you save updated firewall rules, either modifying your shell scripts or by running iptables-save command as described here.

Alternate syntax to remove specific PREROUTING rules from iptables

Say, you execute the following iptables PREROUTING command for port redirection:

```
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

To delete, run the same above command but replace the "`-A`" with "`-D`":

```
sudo iptables -t nat -D PREROUTING -i eth0 -p tcp -m tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

Another example, run the same command but replace the "`-I" with "-D". For example, say you have the following rule that redirect SSH (TCP 22) from port 2222 to port 22:`

```
sudo iptables -t nat -I PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

Becomes:

```
sudo iptables -t nat -D PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

OR

```
sudo iptables -t nat --delete PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

Как просмотреть историю команд другого пользователя в Linux?

```
sudo vim /home/USER_YOU_WANT_TO_VIEW/.bash_history
```

Open VPN

Игнорировать маршрут прописанным сервером.

Добавить в конфиг клиента:

```
pull-filter ignore "route 10.0.10.0 255.255.255.0"
```

Гоним весь трафик через впн.

```
redirect-gateway def1
```

Запуск с несколькими конфиг файлами...

```
/usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.adv.cfg -f /etc/haproxy/listen.cfg -f
/etc/haproxy/wildcard.cfg -f /etc/haproxy/backends.cfg -f /etc/haproxy/userlists.cfg
```

выполняет следующее:

- **Исполняемый файл**:
  Запускает бинарный файл HAProxy, расположенный по пути `/usr/sbin/haproxy`.
- **Используемые параметры**:
  - Флаг `-W` указывает HAProxy работать в однопроцессном режиме.
  - Флаг `-s` часто используется в сочетании с другими флагами для указания режима работы HAProxy (например, в некоторых версиях он может относиться к сигналам для мастер-рабочего режима); точное поведение может варьироваться в зависимости от версии HAProxy. Рекомендуется ознакомиться с документацией HAProxy или выполнить команду `haproxy -h`, чтобы получить подробности для вашей версии.
- **Конфигурационные файлы**:
  Команда указывает несколько конфигурационных файлов с помощью опции `-f`.
  HAProxy загрузит эти конфигурационные файлы в порядке, указанном в команде:
  - `/etc/haproxy/haproxy.adv.cfg`: Вероятно, содержит продвинутые или глобальные настройки.
  - `/etc/haproxy/listen.cfg`: Содержит определения для секции `listen` (объединяющей настройки frontend и backend).
  - `/etc/haproxy/wildcard.cfg`: Может определять правила или настройки, связанные с wildcard-доменами.
  - `/etc/haproxy/backends.cfg`: Определяет пул серверов backend.
  - `/etc/haproxy/userlists.cfg`: Содержит определения списков пользователей, часто используемых для базовой аутентификации или контроля доступа.

Как это работает

HAProxy читает и объединяет эти конфигурационные файлы последовательно. Такой подход полезен для организации конфигурации по различным аспектам (глобальные настройки, фронтенды, бэкенды и т. д.), что упрощает управление и обновление.

Дополнительные заметки

- **Порядок имеет значение**: Поскольку HAProxy обрабатывает конфигурационные файлы в указанном порядке, настройки в более поздних файлах могут переопределять предыдущие, если есть конфликтующие директивы.
- **Отладка/Проверка**: Если вам нужно проверить загруженную конфигурацию и возможные ошибки, вы можете использовать

Секреты Notepad++

Искать ^((?!\b(?:\d{1,3}\.){3}\d{1,3}\b).)*$\R? заменить на "NULL-пустое значение" - Оставит в файле только строки с IP-адресами

Искать - -.* заменить на "NULL-пустое значение" - Удаляет указанный текс (- -) и все после него в строке