



[Главная](#) >> [Сервер](#) >> Авторизация по ключу SSH

Авторизация по ключу SSH

Опубликовано: 8 февраля, 2017 от [admin](#) , 29 комменариев, время чтения: 7 минут

SSH или Secure Shell – это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Если вы захотите что-либо сделать на удаленном сервере, скорее всего, вам придется воспользоваться SSH и работать через терминал.

В SSH существует несколько способов авторизации. Вы можете каждый раз вводить пароль пользователя или использовать более безопасный и надежный способ – ключи SSH. Что самое интересное, он более удобен для применения, вам даже не нужно будет вводить пароль. В этой статье мы рассмотрим как настраивается авторизация по ключу SSH.

Содержание статьи:

- [Как работают ключи SSH?](#)
- [Как создать ключи SSH?](#)
- [Загрузка ключа на сервер](#)
- [Отключение проверки пароля](#)
- [Выводы](#)

Как работают ключи SSH?



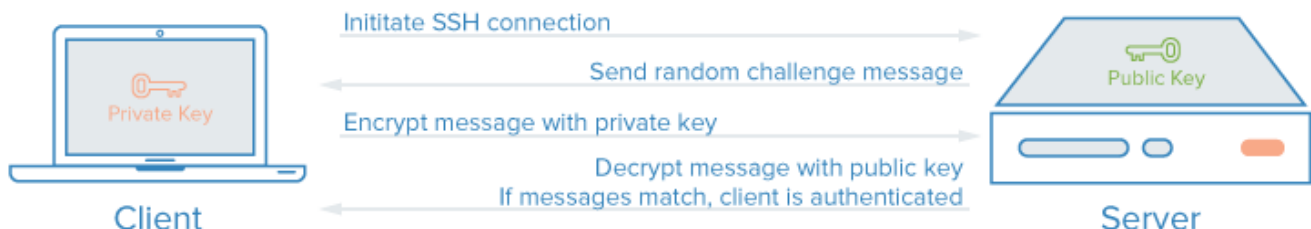
SSH сервер может выполнять аутентификацию пользователей с помощью различных алгоритмов. Самый популярный – это аутентификация по паролю. Он достаточно прост, но не очень безопасный. Пароли передаются по безопасному каналу, но они недостаточно сложны для противостояния попыткам перебора. Вычислительная мощность современных систем в сочетании со специальными скриптами делают перебор очень простым. Конечно, существуют другие способы дополнительной безопасности, например, fail2ban, но аутентификация по ключу SSH более надежна.

Каждая пара ключей состоит из открытого и закрытого ключа. Секретный ключ сохраняется на стороне клиента и не должен быть доступен кому-либо еще. Утечка ключа позволит злоумышленнику войти на сервер, если не была настроена дополнительная аутентификация по паролю.

Открытый ключ используется для шифрования сообщений, которые можно расшифровать только закрытым ключом. Это свойство и используется для аутентификации с помощью пары ключей. Открытый ключ загружается на удаленный сервер, к которому необходимо получить доступ. Его нужно добавить в специальный файл ~/.ssh/authorized_keys.

Когда клиент попытается выполнить проверку подлинности через этот ключ, сервер отправит сообщение, зашифрованное с помощью открытого ключа, если клиент сможет его расшифровать и вернуть правильный ответ – аутентификация пройдена.

SSH Key Authentication

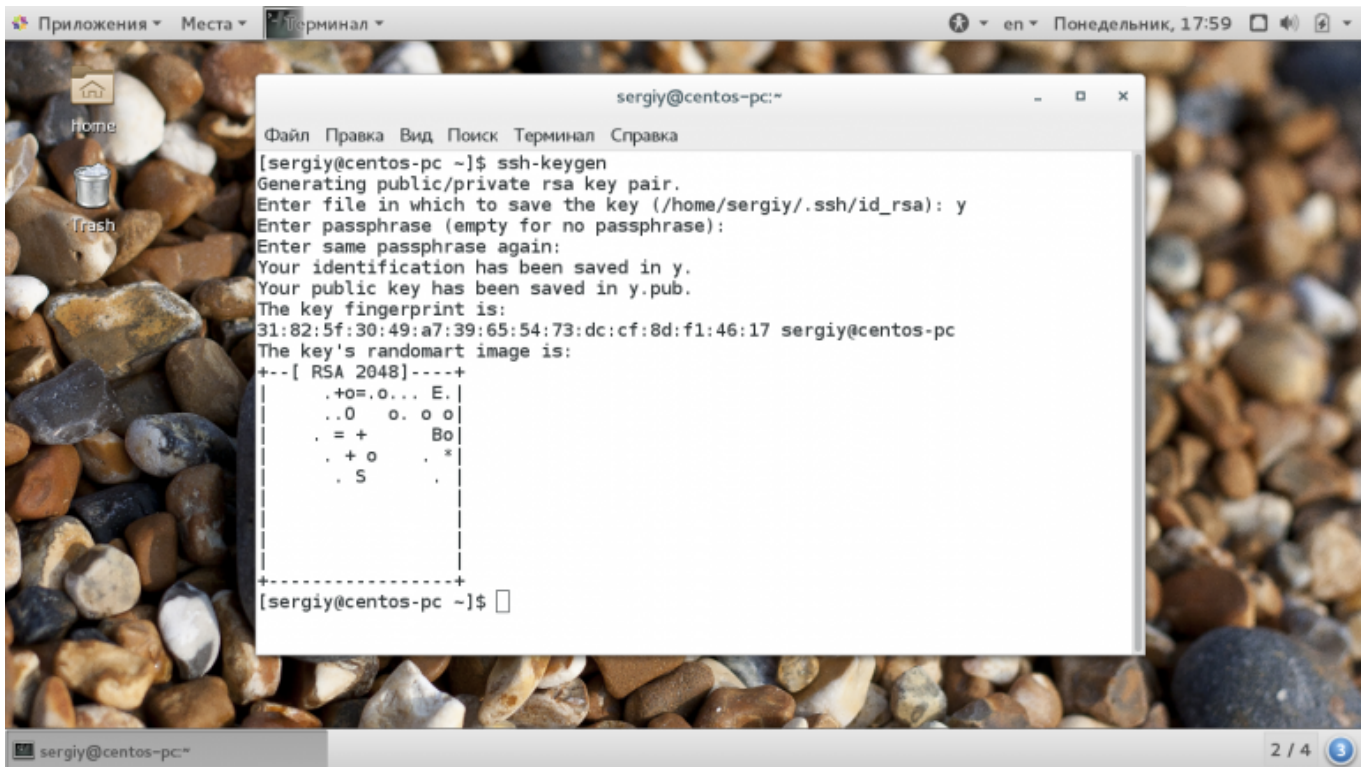


Как создать ключи SSH?

Сначала необходимо создать ключи ssh для аутентификации на локальном сервере. Для этого существует специальная утилита `ssh-keygen`, которая входит в набор утилит OpenSSH. По умолчанию она создает пару 2048 битных RSA ключей, которая подойдет не только для SSH, но и для большинства других ситуаций.

И так, генерация ключей ssh выполняется командой:

```
$ ssh-keygen
```



```
sergiy@centos-pc:~  
Файл Правка Вид Поиск Терминал Справка  
[sergiy@centos-pc ~]$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/sergiy/.ssh/id_rsa): y  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in y.  
Your public key has been saved in y.pub.  
The key fingerprint is:  
31:82:5f:30:49:a7:39:65:54:73:dc:cf:8d:f1:46:17 sergiy@centos-pc  
The key's randomart image is:  
+--[ RSA 2048 ]-----+  
  .+o=.o... E.  
  ..0 o. o o|  
  . = +   Bo|  
  . + o   . *|  
  . S      .  
+-----+  
[sergiy@centos-pc ~]$
```

Утилита предложит вам выбрать расположение ключей. По умолчанию ключи располагаются в папке `~/.ssh/`. Лучше ничего не менять, чтобы все работало по умолчанию и ключи автоматически подхватывались. Секретный ключ будет называться `id_rsa`, а публичный `id_rsa.pub`.

Затем утилита предложит ввести пароль для дополнительного шифрования ключа на диске. Его можно не указывать, если не хотите. Использование дополнительного шифрования имеет только один минус – необходимость вводить пароль, и несколько преимуществ:

- Пароль никогда не попадет в сеть, он используется только на локальной машине для расшифровки ключа. Это значит что перебор по паролю больше невозможен.
- Секретный ключ хранится в закрытом каталоге и у клиента `ssh` нет к нему доступа пока вы не введете пароль;
- Если злоумышленник хочет взломать аутентификацию по ключу `SSH`, ему понадобится доступ к вашей системе. И даже тогда ключевая фраза может стать серьезной помехой на его пути.



Но все же, это необязательное дополнение и если не хотите, то вы можете просто нажать Enter. Тогда доступ по ключу ssh будет выполняться автоматически и вам не нужно будет что-либо вводить.

Теперь у вас есть открытый и закрытый ключи SSH и вы можете использовать их для проверки подлинности. Дальше нам осталось разместить открытый ключ на удаленном сервере.

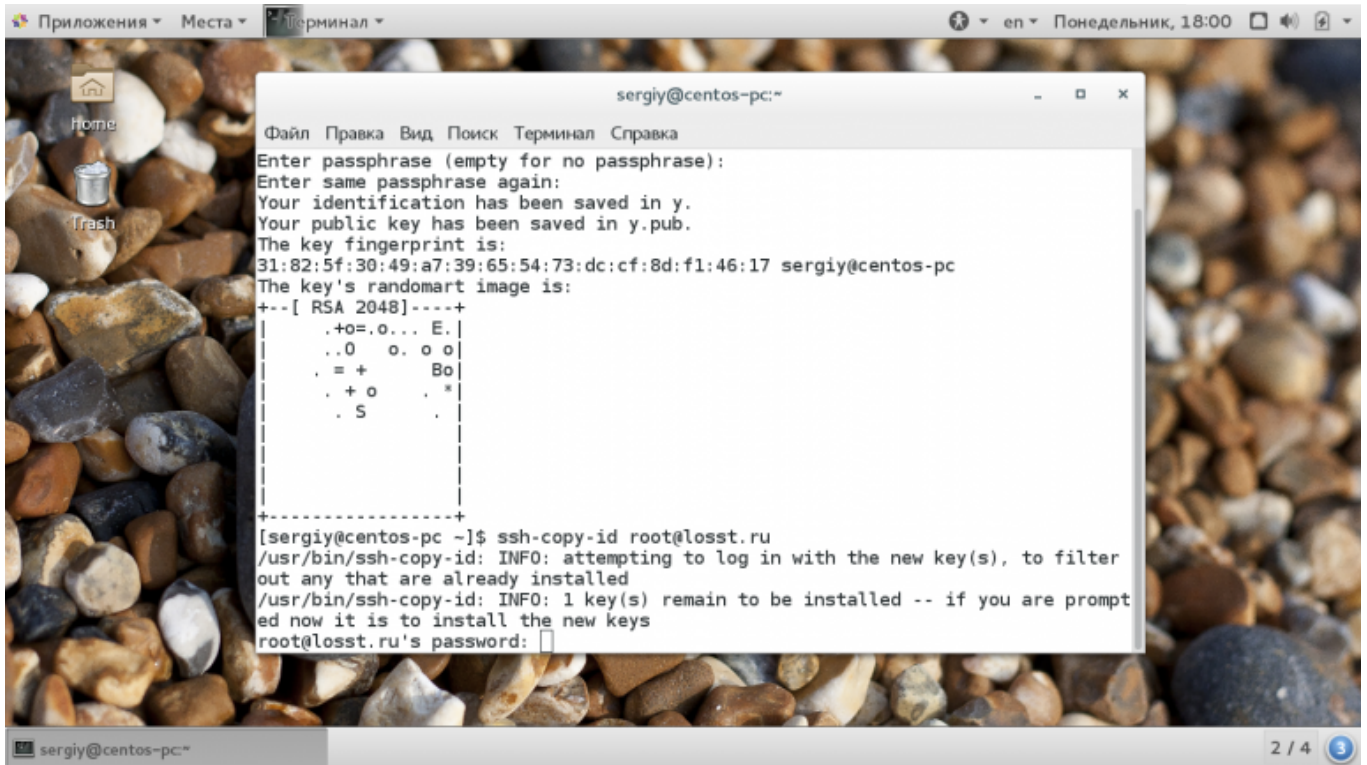
Загрузка ключа на сервер

Когда генерация ключей завершена, нам осталось только загрузить ключ на сервер. Для загрузки ключа можно использовать несколько способов. В некоторых случаях вы можете указать ключ в панели управления сервером, например, cPanel или любой другой. Но мы такой способ рассматривать не будем. Мы рассмотрим ручные способы.

Самый простой способ скопировать ключ на удаленный сервер – это использовать утилиту `ssh-copy-id`. Она тоже входит в пакет программ OpenSSH. Но для работы этого метода вам нужно иметь пароль доступа к серверу по SSH. Синтаксис команды:

```
$ ssh-copy-id username@remote_host
```





При первом подключении к серверу система может его не распознать, поэтому вам нужно ввести `yes`. Затем введите ваш пароль пользователя на удаленном сервере. Утилита подключится к удаленному серверу, а затем использует содержимое ключа `id_rsa.pub` для загрузки его на сервер в файл `~/.ssh/authorized_keys`. Далее вы можете выполнять аутентификацию с помощью этого ключа.

Если такой способ по какой-либо причине для вас не работает, вы можете скопировать ключ по `ssh` вручную. Мы создадим каталог `~/.ssh`, а затем поместим наш ключ в файл `authorized_keys` с помощью символа `>>`, это позволит не перезаписывать существующие ключи:

```
$ cat ~/.ssh/id_rsa.pub | ssh username@remote_host "mkdir -p ~/.ssh && cat >>
~/.ssh/authorized_keys"
```

Здесь вам тоже нужно набрать `yes`, если вы подключаетесь к новому серверу, а затем ввести пароль. Теперь вы можете использовать созданный ключ для аутентификации на сервере:

```
$ ssh username@remote_host
```

Если вы не захотели создать `ssh` ключ с доступом по паролю, то вы сразу же будете авторизованы, что очень удобно. Иначе, сначала вам придется ввести фразу-п

Privacy

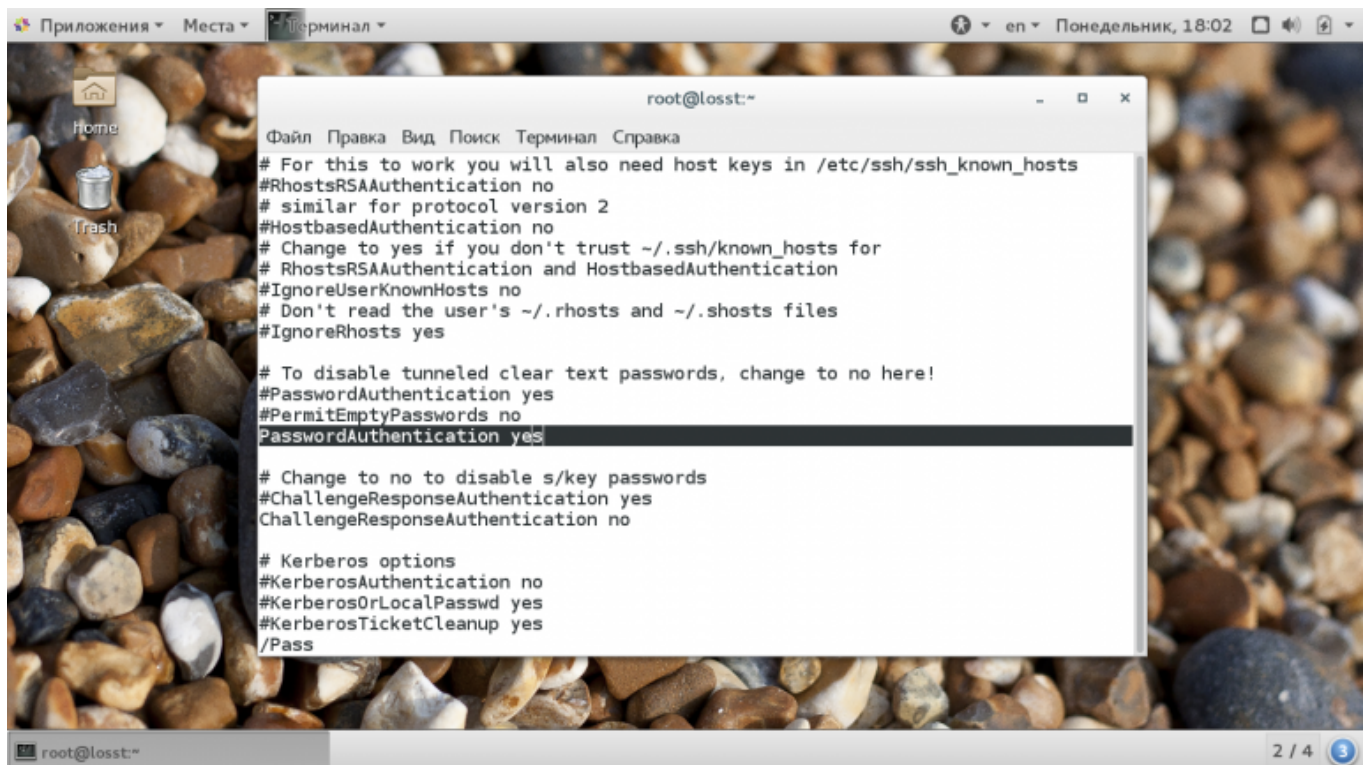
расшифровки ключа.

Отключение проверки пароля

Если пароль больше не будет использоваться, то для увеличения безопасности системы лучше его вовсе отключить. Но убедитесь, что ключ надежно сохранен и вы его не потеряете, потому что по паролю вы больше не войдете. Авторизуйтесь на сервере, затем откройте конфигурационный файл `/etc/ssh/sshd_config` и найдите там директиву `PasswordAuthenticatin`. Нужно установить ее значение в `No`:

```
$ sudo vi /etc/ssh/sshd_config
```

`PasswordAuthentication no`



Теперь сохраните файл и перезапустите службу ssh:

```
$ sudo service ssh restart
```

Дальше будет возможно только подключение по ключу ssh, пароль не будет приниматься.

Выводы

В этой статье мы рассмотрели как выполняется авторизация по ключу ssh, настройка ключей ssh и добавить ssh ключ. Теперь вы можете войти на сервер без ввода пароля. Если у вас остались вопросы, спрашивайте в комментариях!

Обнаружили ошибку в тексте? Сообщите мне об этом. Выделите текст с ошибкой и нажмите Ctrl+Enter.

Похожие записи

Нет похожих записей.

Оцените статью

★★★★★ (30 оценок, среднее: **4,83** из 5)



Статья распространяется под лицензией Creative Commons ShareAlike 4.0 при копировании материала ссылка на источник обязательна .

📁 [Сервер](#)

Об авторе



ADMIN

Основатель и администратор сайта losst.ru, увлекаюсь открытым программным обеспечением и операционной системой Linux. В качестве основной ОС сейчас использую Ubuntu. Кроме Linux, интересуюсь всем, что связано с информационными технологиями и современной наукой.

29 комментариев к “Авторизация по ключу SSH”

**Дима**12 января, 2018 в 10:56 дп

Вы создаёте ключи под пользователем Sergiy? А подключаетесь потом на удалённый сервер под root. Это правильно? Я например, хочу сделать у себя так: отключить вход root на сервер (PermitRootLogin no), и подключаться под своей локальной УЗ на все серверы. После того, как я захожу на сервер, я повышаю свои права до root. Как мне настроить аутентификацию по ключам в таком случае?

[Ответить](#)**Alex**5 февраля, 2018 в 9:36 дп

```
нужно в папке home/.ssh создать файл authorized_keys
туда кинуть ключ
поменять права на папку
# mkdir ~/.ssh
# chmod 0700 ~/.ssh
# touch ~/.ssh/authorized_keys
# chmod 0644 ~/.ssh/authorized_keys
```

[Ответить](#)**garynych**19 мая, 2018 в 8:48 дп

ssh-keygen затем ssh-copy-id username@remote_host далее проверяем работает ли всё как нужно ssh username@remote_host и если пустил сервер не запрашивая пароля то sudo nano /etc/ssh/sshd_config включаем параметр PasswordAuthentication yes (удалив перед ним #) и меняем yes на no сохраняемся и всё, доступ к серверу только по ключу пользователя ,как root`а и как либо ещё уже не пустит ,для получения супер прав, после того как вошли на сервер sudo -i и ввод пароля юзера ну или su и его пароль

[Ответить](#)**garynych**[19 мая, 2018 в 8:51 дп](#)

```
sudo service sshd restart (после редактирования /etc/ssh/sshd_config)
```

[Ответить](#)**ALEX**[31 января, 2018 в 1:09 пп](#)

не совсем понял. вы в команде создания ключей при вводе имени пишете `y`
создаете ключ с именем `y.` и `y.pub`
но при этом потом говорите что у ключа имя :
`id_rsa.`
`id_rsa.pub.`

[Ответить](#)**Andrij**[25 апреля, 2018 в 12:09 пп](#)

Теж спочатку не зрозумів, бо автор вказав ім'я файлу "y", натомість не треба ні чого писати, якщо все робити за статтею, то після вводу "ssh-keygen" просто 3 рази Enter.

[Ответить](#)**Георг**[1 мая, 2018 в 11:07 пп](#)

Здравствуйте. В статье ни слова о файле "PRIVATE KEY". Как без него авторизоваться?

Privacy

[Ответить](#)**Алекс**11 декабря, 2018 в 2:43 пп

Сразу видно "программист" писал... не понятно куда что копировать и как вручную добавить ключ в какой файл на какой машине

[Ответить](#)**Ахмед**21 января, 2019 в 2:33 пп

Проверял несколько раз, через некоторое количество удачных сеансов потом при попытке подключиться к серверу по команде `ssh username@remote_host` - сервер не пускает.

Надо указывать ключ: `ssh -i ~/.ssh/id_rsa username@remote_host`, что не очень удобно.

Проще создать создать конфигурационный файл `~/.ssh/config` такого формата:

=====

```
Host host1 #"имя по желанию"#
```

```
HostName x.x.x.x #"Здесь IP или доменное имя сервера, без разницы"
```

```
User root #"Или другой пользователь, который есть на сервере"
```

```
Port 60000 #"Указываем порт. Лучше, как советовал автор, 22 не использовать"
```

```
IdentityFile ~/.ssh/id_rsa #"Его закрытый ключ"#
```

```
Host host2
```

```
HostName .....
```

```
User .....
```

```
Port 61000
```

```
IdentityFile ~/.ssh/.....
```

```
Host host3
```

```
.....
```

=====

Теперь подключаться можно простой командой, например к первому хосту:

```
ssh host1
```

Важно только, чтобы конфиг назывался именно config и находился в папке ~/.ssh/

[Ответить](#)



admin

[21 января, 2019 в 5:29 пп](#)

Попробуйте добавить ключ с помощью ssh-add. Почему-то ssh не видит ваши ключи, а это странно.

[Ответить](#)



Святослав

[4 марта, 2019 в 5:51 пп](#)

у меня такой вопрос, я сгенерил себе ssh ключ, заказчик попросил публичный ключ, я ему скинул, он сказал что создал мне юзера, но больше никакой инфы, ни что за юзер ни какой хост, тоесть я ему только ключ публичный и все, он говорит что этого достаточно, я не понимаю, как мне подключится, подскажите плиз нубу)

[Ответить](#)



admin

[4 марта, 2019 в 9:12 пп](#)

Узнайте у заказчика ip хоста и имя пользователя, а затем подключайтесь.

[Ответить](#)



Дмитрий

[10 марта, 2019 в 9:03 пп](#)

Спасибо за статью!

Как быть, если нужен доступ к серверу по SSH с 2х компьютеров?

[Ответить](#)



admin

[11 марта, 2019 в 11:18 дп](#)

В идеале нужно для каждого компьютера создавать свой ключ и добавлять его в `~/.ssh/authorized_keys`

[Ответить](#)

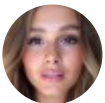


Дмитрий

[27 апреля, 2020 в 10:07 пп](#)

Можно свои ключи скопировать на второй компьютер и затем добавить на сервер.

[Ответить](#)



Sergei

[25 мая, 2019 в 11:41 дп](#)

А SFTP будет работать?

[Ответить](#)



Юра

[30 января, 2020 в 5:45 пп](#)

SFTP точно также будет работать.

Только подключаться через утилиту `sshfs` надо немножко не так, как через `ssh`. Для указания приватного ключа, нужно указывать опцию не `-i`, а `-s`

Privacy

IdentityFile= Пример:

```
sshfs -C -p 9087 -o IdentityFile=~/.ssh/id_rsa_root root@195.95.171.2:/media/vds
```

[Ответить](#)



Илья

6 октября, 2019 в 7:54 пп

а так?

```
mkdir ~/.ssh # это делаем только первый раз)
ssh-keygen -t rsa -b 4096 -q -N 'вашаУжастнаяПарольнаяФраза' -f
~/.ssh/id_rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub логин@вашСервер
```

далее

Are you sure you want to continue connecting (yes/no)? yes

и

входим по паролю

и

вуаля:

Number of key(s) added: 1

[Ответить](#)



Юра

30 января, 2020 в 11:27 дп

Напишите ещё про сеансовый ключ.

[Ответить](#)

**Che Rchill**30 июля, 2020 в 12:01 пп

Парни, как должен выглядеть копируемый текст публичного ключа?
Если я генерирую ключ в Линуксе, то файл .pub содержит такой текст:

```
ssh-rsa AAAAB3NzaC1yc2.....0iP2JqKNoyn valerygl@UBUNTU-530  
(все в одну строку без переносов, заканчивается на имя компа)
```

если я генерирую ключ в Винде (PUTTY), то файл содержит

```
---- BEGIN SSH2 PUBLIC KEY ----  
Comment: "rsa-key-20200730"  
AAAAB3NzaC1yc2EAAAABJQAAAQEA48AQWgzfdPr06UZw8EYH2svNsNKntj1T/CDa  
.....  
9ZmUakRYMjQBJ9okIPGsJRC0Z+z0uUpwh+9RPfZ0GtSiTZZ7+w==  
---- END SSH2 PUBLIC KEY ----
```

вопрос - что из виндового файла нужно перенести в authorized_keys? целиком или вырезать, начиная от "AAA"? Переносы оставлять или вырезать? Провел десяток экспериментов, но пока всё неудачно

[Ответить](#)**NickVG**14 августа, 2020 в 11:34 дп

"Сначала необходимо создать ключи ssh для аутентификации на локальном сервере."

Вот надо же так написать! Что за локальный сервер и чем он отличается от глобального?

У автора каша в голове!

[Ответить](#)

**Mitai**18 сентября, 2020 в 12:27 пп

Как подключится через ssh к своему андроид телефону? там есть пара не понятных моментов, типо имя юзера, куда класть ключ? и еще по мелочи...

[Ответить](#)**kr**24 сентября, 2020 в 4:08 дп

У меня есть одна пара ключей для одного сервера и я генерирую вторую пару для другого. Как мне на указать ssh-copy-id ключ, который я хочу передать на второй сервер? Если ничего не указывать - передается два и не совсем понятно, каким ключом я в итоге авторизуюсь

[Ответить](#)**Илдар**21 ноября, 2020 в 5:53 пп

Приветствую! Создал VM на ORACLE Cloud на образе ОС Canonical-Ubuntu-20.04-2020.11.11-0 с общедоступным IP-адресом. Не получается подключиться к VM через PuTTY (64-bit). IP вписываю, а вот куда ключи SSH вписывать не пойму, может из-за этого не работает. Пишет "Unable to open connection to http. Host does not exist.". Пожалуйста подскажите где подробно описано как пользоваться SSH-клиентами.

[Ответить](#)**KAS**23 ноября, 2020 в 8:02 дп

Там при создании VM ключик для авторизации предлагают скачать. Ещё на VM нужно настраивать iptables. И для Putty нужно конвертировать ключи, вроде бы так

```
openssl rsa -in MyKey.key -out MyKey4PuttyGen.key
```

[Ответить](#)



Андрей

[18 декабря, 2020 в 2:44 пп](#)

Добрый день, а что, если я прописал:

```
PasswordAuthentication no
```

И по какой-то причине потерял ключи.

То я больше никак не попаду на сервак?

[Ответить](#)



Вячеслав

[10 мая, 2021 в 7:49 пп](#)

Дядька, спасибо большое за старания! Хренову кучу раз твои статьи выручали меня когда надо быстро узнать какую-то инфу

[Ответить](#)



Вячеслав

[27 мая, 2021 в 2:46 пп](#)

Добрый день, спасибо за статью, очень интересно, еще бы дополнить ее тем что после того как файл authorized_keys необходимо поменять права на папки "ss

Privacy

файл а то можно много времени потратить на поиск проблемы:

```
chmod go-w ~/
```

```
chmod 700 ~/.ssh
```

```
chmod 600 ~/.ssh/authorized_keys
```

[Ответить](#)**konstantin**[24 июля, 2021 в 11:00 дп](#)

Получается, как предложил Ахмед, если на локальной машине несколько ключей для разных серверов с разными пользователями на серверах, то лучше дополнительно создать ~/.ssh/config с указанием на каком сервере для какого пользователя какой ключ использовать.

Если ключи создаются на сервере, то хранятся в тех же местах, только теперь от сервера нужно пользователю передать приватный ключ.

[Ответить](#)

Оставьте комментарий

☐ Я прочитал и принимаю политику конфиденциальности. Подробнее [Политика конфиденциальности](#) *

[Privacy](#)

Комментировать


Русский

Поиск

ПОИСК ПО КОМАНДАМ

Начните вводить команду

Поиск



Начните изучать
Linux прямо сейчас!

Карта сайта



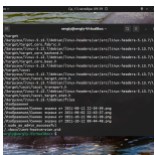
Как пользоваться редактором Vim

Полезно

Лучшие

Свежие

Теги



Команда find в Linux

2021-10-17



Команда chmod Linux

2020-04-13



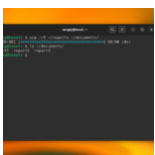
Права доступа к файлам в Linux

2020-10-09



Настройка Cron

2021-10-01



Копирование файлов в Linux

2023-03-03



Privacy

РАССЫЛКА

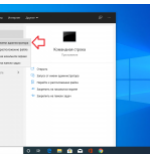
Ваш E-Mail адрес

☐ Я прочитал(а) и принимаю политику конфиденциальности

Sign up

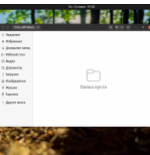
Windows

Списки



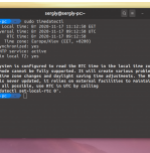
Восстановление Grub после установки Windows 10

2023-05-04



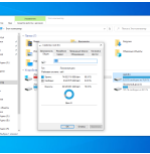
Ошибка Ubuntu не видит сеть Windows

2023-02-19



Сбивается время в Ubuntu и Windows

2023-02-19



Подключение ext4 в Windows

2023-02-19


Смотреть ещё

ОБНАРУЖИЛИ ОШИБКУ?




Privacy

ВКОНТАКТЕ

 >< komYounity

Мы создаём комьюнити, комьюнити создаёт Linux.

13 974 подписчика



Подписаться на новости

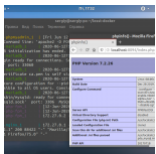
МЕТА

- Регистрация
- Войти
- Лента записей
- Лента комментариев

СЛЕДИТЕ ЗА НАМИ В СОЦИАЛЬНЫХ СЕТЯХ

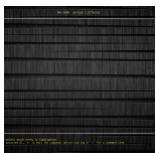


ИНТЕРЕСНОЕ



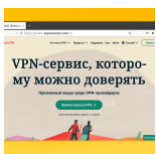
Использование Docker для чайников

2021-04-08



Мультизагрузочная флешка с несколькими ОС Linux

2021-10-01



Лучшие VPN сервисы для Linux

2022-10-11



Линус Торвальдс – человек, создавший Linux

2021-01-28

©Losst 2023 CC-BY-SA [Политика конфиденциальности](#)

