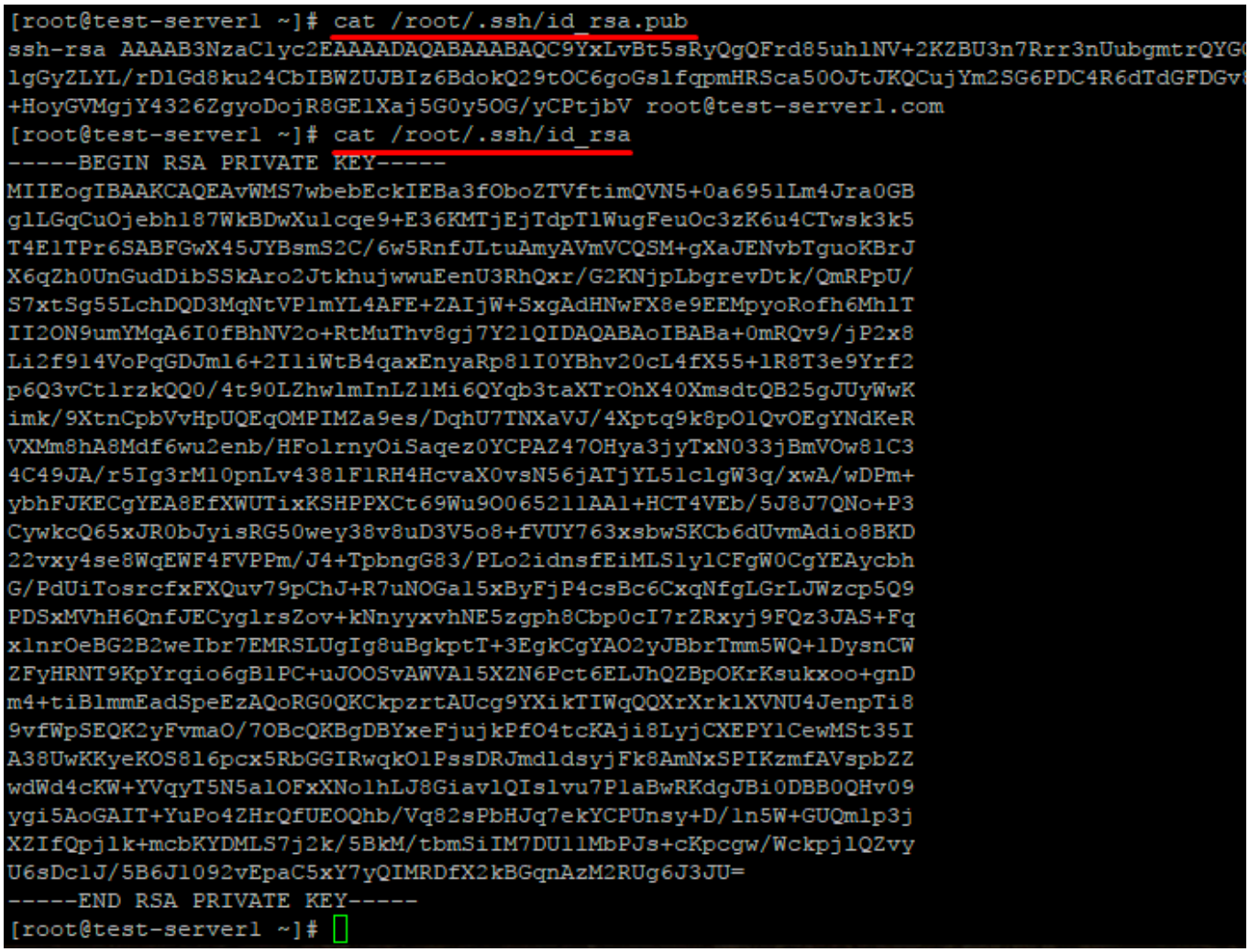
SSH Без Пароля, или Как Настроить SSH-доступ по Ключу в Linux

https://t.me/sysadminof • February 10, 2022



SSH, или Secure Shell — это сетевой протокол с открытым исходным кодом, который можно использовать для входа на серверы и удалённого выполнения команд, что отлично подходит для пользователей VPS.

Есть два способа включить SSH:

- Вход на основе пароля
- Аутентификация на основе открытого ключа

Аутентификация на основе открытого ключа также известна как вход в SSH без пароля, или беспарольный доступ по SSH.

Преимущества Входа в SSH Без Пароля

Защищённое паролем подключение пользователи зачастую находят неудобным. Пароли сложно запоминать, к тому же, если вы работаете в среде, где вам часто приходится вводить пароль, вы просто тратите на это лишнее время.

Здесь можно выделить несколько преимуществ входа в SSH без пароля:

- Простой и не интерактивный вход в систему. Пользователям не нужно вводить пароль для каждого нового сеанса
- Более безопасный по сравнению с паролями, криптографическая защита (открытый/закрытый ключ шифрования)
- Более надёжный
- Лучшее управление аутентификацией и авторизацией
- Подходит, как для маленькой, так и для большой инфраструктуры
- Легко настроить и поддерживать

Чтобы начать использовать SSH без пароля, вам нужно сгенерировать открытый SSH-ключ. В этом руководстве мы сосредоточимся на SSH версии 2, последнем и более безопасном протоколе.

Подключитесь к вашему VPS-серверу по SSH и мы начнём!

Во-первых, нам нужно проверить, существует ли SSH-ключ для клиентского компьютера. Это предотвратит перезапись текущей конфигурации. Чтобы узнать, используйте следующую команду:

```
ls -al ~/.ssh/id_*.pub
```

Если ключ уже существует, вы можете а). пропустить следующий шаг — генерацию SSH-ключа; б). отменить текущую настройку; в). создать резервную копию существующего ключа. Если ключ не существует, вы увидите следующий вывод:

```
ls: cannot access /users/appsadm/.ssh/id_*.pub: No such file or directory
```

Далее мы можем приступить непосредственно к генерации SSH-ключа.

SSH-доступ по Ключу в Ubuntu и CentOS:

Чтобы сгенерировать открытый и закрытый SSH-ключ в Ubuntu или CentOS, используйте команду:

```
ssh-keygen -t rsa
```

Параметр -t означает тип, а RSA — протокол, используемый для генерации ключей. RSA является типом по умолчанию, поэтому вы также можете использовать упрощённую версию команды — ssh-keygen.

Длина ключа по умолчанию — 2048 бит. Однако, если вы хотите усилить защиту, измените значение на 4096 бит. В этом случае команда будет выглядеть так:

```
ssh-keygen -t rsa -b 4096
```

Это интерактивный процесс генерации ключей, и вас попросят выполнить несколько действий, таких как:

- Enter file in which to save the key (/home/.ssh.id_rsa), или «Ввести файл для сохранения ключа (/home/.ssh.id_rsa)»
- Enter passphrase (empty for no passphrase), или «Ввести кодовую фразу (оставьте пустым для отключения кодовой фразы)»

Если вы хотите, чтобы были заданы значения по умолчанию, просто нажмите Enter в ответ на каждый из этих запросов. Кодовая фраза используется для шифрования закрытого ключа; однако она не является обязательной и может быть пропущена. Закрытый ключ будет сохранён в папке по умолчанию — .ssh/id_rsa.

Открытый ключ будет сохранён в файле .ssh/id_rsa.pub. На этом генерация ключа будет завершена. Вы можете проверить файлы с помощью любого редактора.

Копирование Открытого Ключа для Включения Беспарольного SSH

Скопировать открытый ключ на машину предназначения можно тремя способами:

- С помощью команды ssh-copy-id
- С помощью SSH
- Вручную

Первый вариант является наиболее оптимальным и быстрым. Команда ssh-copy-id по умолчанию включена в большинство дистрибутивов Linux. Однако, если вы столкнулись с проблемами при использовании ssh-copy-id или не имеете доступа к этой команде, вы можете попробовать следующие опции.

Метод 1: С Помощью Команды ssh-copy-id

Основной синтаксис этой команды:

```
ssh-copy-id имя_удаленного_пользователя@удаленный_IP_адрес
```

На этом этапе вам нужно будет ввести пароль удалённого компьютера. Если аутентификация пройдёт успешно, сгенерированный открытый ключ SSH будет добавлен в файл author_keys удалённого компьютера. После добавления записи соединение закроется автоматически.

Метод 2: Копирование Закрытого Ключа с Помощью SSH

При этом методе, мы копируем закрытый ключ, используя SSH. Этот вариант сработает только в том случае, если у вас есть SSH-доступ к серверу на основе пароля. Команда ниже сделает всю работу. Вам нужно только ввести имя и IP-адрес удалённого пользователя.

```
cat ~/.ssh/id_rsa.pub | ssh
имя_удаленного_пользователя@удаленный_ip_адрес "mkdir -p ~/.ssh && cat
>> ~/.ssh/authorized_keys"
```

Запись будет добавлена в файл author_keys удалённой машины.

Метод 3: Копирование Открытого Ключа Вручную

Третий метод немного сложнее, так как вам придётся всё делать вручную. Однако, вариант вполне рабочий и вы можете использовать его в отдельных случаях, когда другие методы не работаю. Вам нужно будет вручную добавить содержимое файла id_rsa.pub в файл ~/.ssh/authorized_keys удалённого сервера.

Вы можете посмотреть содержимое файла id_rsa.pub с помощью редактора vi или команды cat:

```
cat ~/.ssh/id_rsa.pub
```

Команда выведет ключ, он начинается с ssh-rsa. Скопируйте эго! Затем на удалённом сервере войдите в систему и создайте файл .ssh, если он не существует.

```
mkdir -p ~/.ssh
```

Также само вы можете создать файл author_keys. Добавьте скопированный открытый SSH-ключ в пустой файл, как показано ниже:

```
echo SSH_public_key >> ~/.ssh/authorized_keys
```

SSH_public_key — это открытый ключ, который вы скопировали с исходного компьютера. Он должен начинаться с ssh-rsa.

После того как ключ будет скопирован, вы сможете настроить необходимые разрешения для каталога .ssh удалённых серверов с помощью команды chmod.

```
chmod -766 ~/.ssh
```

Проверка Входа в SSH Без Пароля

К этому моменту SSH-доступ по ключу должен быть успешно активирован и настроен. Чтобы протестировать эту функцию, можно попробовать подключится к удалённому серверу через исходный сервер. Синтаксис команды будет выглядеть так:

```
ssh имя_удаленного_пользователя@удаленный_IP_адрес
```

Если всё прошло успешно, вы войдёте в систему автоматически без ввода пароля.

Как Отключить SSH-доступ по Ключу

Если вы решите, что беспарольный SSH вам не подходит, вы можете отключить эту функцию, выполнив следующие действия. Для этого откройте файл конфигурации SSH — /etc/ssh/ssh_config. Подойдёт любой текстовый редактор, мы используем nano. Здесь вы найдёте запись с PasswordAuthentication. Измените строки, как показано ниже:

```
PasswordAuthentication no
ChallengeResponseAuthentication no
UsePAM no
```

Чтобы изменения вступили в силу, сохраните файл и перезапустите SSH. Вот как это сделать в Ubuntu 18.04:

```
sudo systemctl restart ssh
```

Команда для CentOS 7:

```
sudo systemctl restart sshd
```

Итоги

На этом мы завершаем наше руководство о том, как настроить вход в SSH без пароля, а также отключить SSH-доступ по ключу, если вы решите, что вам не подходит эта функция. Надеемся, что эта инструкция была полезной! Успехов, берегите себя и свои данные!

источник