Удалённый доступ к серверу

Стандарт для удалённого доступа — протокол SSH. Он расшифровывается как Secure Shell — «безопасная оболочка».

Наиболее распространённая его реализация — проект OpenSSH.
SSH — это клиент-серверный протокол. Зачастую на каждой машине работает и SSH-клиент (который мы можем использовать для подключения к удалённой машине) и SSH-сервер (принимающий соединения от клиента). Сервер (обычно его процесс называется sshd) по умолчанию слушает на 22-м порту.

Давайте начнём с сервера. Установим SSH-сервер при помощи пакета openssh:

```
sudo apt update
sudo apt install openssh-server
```

Убедимся, что сервер запущен:

```
sudo systemctl status ssh
```

Готово.

Клиент называется просто ssh. Для подключения нужно указать адрес сервера и (опционально) имя пользователя и порт:

```
ssh username@remote_host
ssh victoria 192.168.88.223
```

При первом подключении появится сообщение: «Введите yes в первый раз».
Это нужно для повышения безопасности. При настройке SSH-сервера создаётся уникальная комбинация символов — fingerprint («отпечатки пальцев»). Ваш компьютер запоминает эту комбинацию и сверяет её при каждом новом соединении. Если кто-то переустановит SSH-сервер или всю операционную систему или вообще заменит удалённый компьютер, сохранив его адрес, то при следующем соединении вы узнаете об этом, потому что изменится fingerprint.

Простейший вариант — подключение по паролю. После ввода команды ssh система запросит пароль.

Работа с удалённым сервером

Мы можем настроить авторизацию не по паролю, а по ключу. Дело в том, что пароль относительно просто подобрать. К тому же его необходимо безопасно хранить и менять время от времени.
С ключами весь этот менеджмент требоваться не будет.

Создадим пару ключей:

```
ssh-keygen
```

Программа запустится и спросит, куда сохранять ключи:
Generating public/private rsa key pair.
Enter file in which to save the key (/home/demo/.ssh/id_rsa):

Нажмите Enter для сохранения в стандартное место — директорию .ssh/id_rsa в вашей домашней директории.

Программа запросит passphrase. Это пароль, защищающий ключ.

Можно просто нажать Enter и пропустить этот шаг. Но лучше ввести passphrase — тогда его нужно будет вводить каждый раз, когда используется ключ.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:

Ключи созданы.
Теперь у вас есть два файла:

1) ~/.ssh/id_rsa — **приватный ключ.** Никогда никому и никуда не передавайте его;
2) ~/.ssh/id_rsa.pub — **публичный ключ.** Спокойно распространяйте его.

Для загрузки публичного ключа на сервер нужно добавить публичный ключ на сервер в файл ~/.ssh/authorized_keys.

Первый способ — запустить на локальной машине команду для копирования ключа:

```
ssh-copy-id -i /home/demo/.ssh/id_rsa.pub ivan@52.307.149.244
```

Второй способ — подключиться по паролю, открыть в редакторе файл ~/.ssh/authorized_keys и добавить в конец текст из вашего файла ~/.ssh/id_rsa.pub.

После включения соединений по ключу рекомендуется отключить подключение по паролю. Для этого необходимо поправить конфигурацию сервера ssh.

Откроем конфигурационный файл. Он находится в директории **etc** и, как я и говорила, называется sshd_config. Файлы, которые называются ssh, — это глобальная конфигурация клиента.
Чтобы отключить возможность залогиниться по паролю, откроем файл на редактирование с правами администратора:

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

Заодно запретим логиниться пользователю root:

```
PermitRootLogin no
```

При работе с ключами возможны **две неудобные ситуации:**

1. Если при создании ключа вы указали passphrase (пароль для ключа), то вам придётся вводить пароль при каждом подключении.
2. Если у вас есть несколько ключей для разных целей, то при соединении по ssh придётся указывать нужный ключ вручную — ssh-agent решает эти проблемы. Этот агент аутентификации (authentication agent) работает на фоне в *nix-системах. В зависимости от системы вам, возможно, придётся установить и настроить его автозапуск самостоятельно.

Если добавить ключ к агенту, то:

- для него больше не будет запрашиваться passphrase;
- не нужно будет вводить ключ вручную — он будет автоматически использован при соответствующем подключении;
- ssh-add /home/demo/.ssh/id_rsa добавит ключ id_rsa в запущенный в системе агент.

Если у него есть passphrase, то агент попросит ввести его.
Если запустить ssh-add без аргументов, то будут добавлены ключи ~/.ssh/id_rsa, ~/.ssh/id_dsa, ~/.ssh/id_ecdsa, ~/.ssh/id_ed25519 и ~/.ssh/identity.

Список добавленных в агент ключей можно посмотреть с помощью команды ssh-add -L:

```
ssh-add -L
```

ssh-agent привязан к сессии. Поэтому, например, если перезагрузить компьютер, то ключи нужно будет добавлять в агент заново.