Авторизация ssh на хостах по ключу

РЕД ОС
Windows
Putty

Окружение

- **Версия РЕД ВИРТ:** 7.3

РЕД ОС

Сгенерируйте ключ утилитой ssh-keygen:

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

Утилита информирует о каталоге размещения сгенерированных ключей. Каталог можно изменить, указав другой путь (не рекомендуется):

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
```

Далее будет предложено установить пароль на ключ для защиты от несанкционированного доступа третьих лиц. Опция не является обязательной. Если оставить поле пустым, пароль не будет установлен:

```
Created directory '/home/admin/.ssh'.
Enter passphrase (empty for no passphrase):
```

После этого происходит генерация ключей. По завершении процесса генерации будут указаны каталоги хранения **id_rsa** (приватная часть ключа) и **id_rsa.pub** (публичная часть ключа).

Передача открытой части ключа на сервер

Открытую часть ключа передайте на сервер при помощи утилиты **ssh-copy-id** в формате вида:

```
ssh-copy-id -i <путь_до_ключа> root@<IP-адрес_сервера_или_FQDN>
```

Например:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.100.61
```

При первом подключении к серверу будет предложено проверить отпечаток ключа **fingerprint**. Для подтверждения наберите **yes**. Отпечаток ключа будет сохранен в файл **~/.ssh/known_hosts**.

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.100.61 (192.168.100.61)' can't be established.
ED25519 key fingerprint is
SHA256:q3oeMFb4bpE4SMd39cH5QqShw3yFmMXi4Wh5VfS260g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Далее будет предложено ввести пароль пользователя **root** хоста:

```
root@192.168.100.61's password: <пароль_root>
```

Выполните проверку подключения к серверу с помощью команды вида:

```
ssh root@<IP-адрес_сервера>
```

Настройка поведения клиента SSH

Для упрощения доступа к различным серверам можно настроить псевдонимы. Для этого создайте файл настроек:

```
touch ~/.ssh/config
```

Заполните файл, указав псевдоним (Alias) и параметры подключения, следующим образом:

```
Host <Alias>
  Hostname <IP-адрес_или_FQDN_сервера>
  User <Имя_пользователя>
  IdentityFile <путь_до_закрытого_ключа>
```

Последовательно можно указать несколько псевдонимов. В дальнейшем можно будет подключаться только по Alias:

```
ssh <Alias>
```

Windows

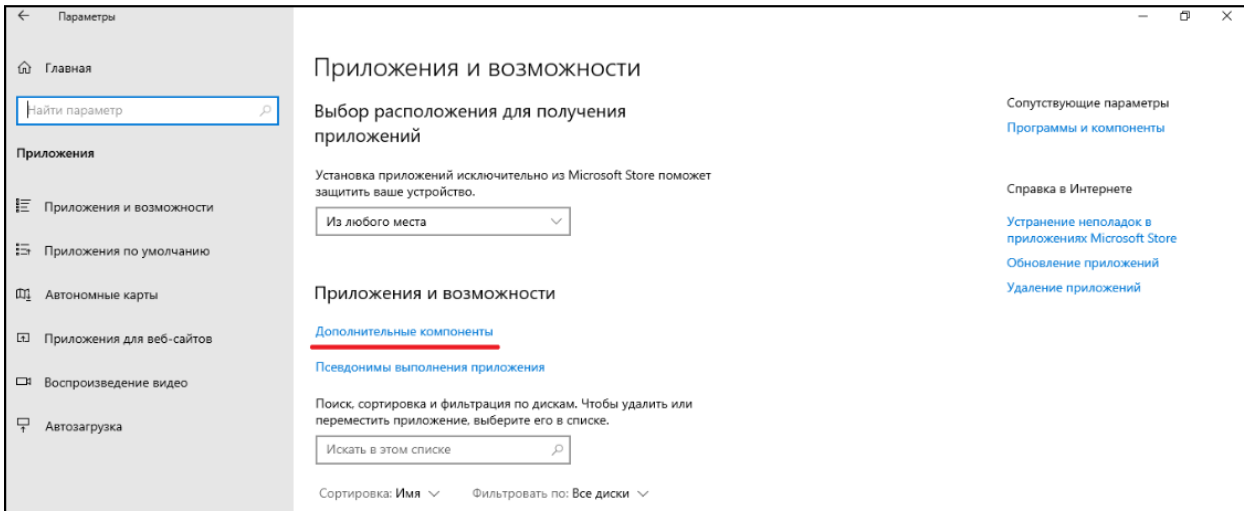
Установка ssh

Чтобы убедиться, что клиент OpenSSH уже установлен, в Windows 10 выполните следующие действия:
Откройте **Командную строку** или **PowerShell**: нажмите Win + R, введите cmd (для командной строки) или powershell, и нажмите **Enter**.
В открывшемся окне выполните команду:

```
ssh -V
```

Если в ответе будет отображена версия клиента, значит OpenSSH уже установлен.
Если OpenSSH отсутствует, его можно добавить через настройки Windows. Для этого:

1. Откройте Параметры Windows.
2. Перейдите в раздел **Приложения** и **Дополнительные компоненты**.



3. Нажмите на **Добавить компонент** и выберите **OpenSSH Client**.

   Сгенерируйте ключ утилитой ssh-keygen:

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

   Утилита информирует о каталоге размещения сгенерированных ключей. Каталог можно изменить, указав другой путь (не рекомендуется):

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (C:\Users\admin\.ssh\id_rsa):
   ```

   Далее будет предложено установить пароль на ключ для защиты от несанкционированного доступа третьих лиц. Опция не является обязательной.

Если оставить поле пустым, пароль не будет установлен:

```
Enter passphrase (empty for no passphrase):
```

После этого происходит генерация ключей. По завершении процесса генерации будут указаны каталоги хранения **id_rsa** (приватная часть ключа) и **id_rsa.pub** (публичная часть ключа).

Передача открытой части ключа на сервер

Открытую часть ключа передайте на сервер при помощи утилиты **ssh-copy-id** в формате вида:

```
ssh-copy-id -i <путь_до_ключа> root@<IP-адрес_сервера_или_FQDN>
```

Например:

```
ssh-copy-id -i C:\Users\admin\.ssh\id_rsa.pub root@192.168.100.61
```

При первом подключении к серверу будет предложено проверить отпечаток ключа **fingerprint**. Для подтверждения наберите **yes**. Отпечаток ключа будет сохранен в файл **~/.ssh/known_hosts**.

```
The authenticity of host '192.168.100.61 (192.168.100.61)' can't be established.
ED25519 key fingerprint is
SHA256:q3oeMFb4bpE4SMd39cH5QqShw3yFmMXi4Wh5VfS260g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Далее будет предложено ввести пароль пользователя **root** хоста:

```
root@192.168.100.61's password: <пароль_root>
```

При недоступности утилиты **ssh-copy-id**, можно выполнить:

```
type <путь_до_ключа> | plink.exe root@<IP-адрес_сервера_или_FQDN> -pw
<Пароль_для_пользователя> "umask 077; test -d .ssh || mkdir .ssh ; cat >>
.ssh/authorized_keys"
```

Выполните проверку подключения к серверу с помощью команды вида:

```
ssh root@<IP-адрес_сервера>
```

PuTTY

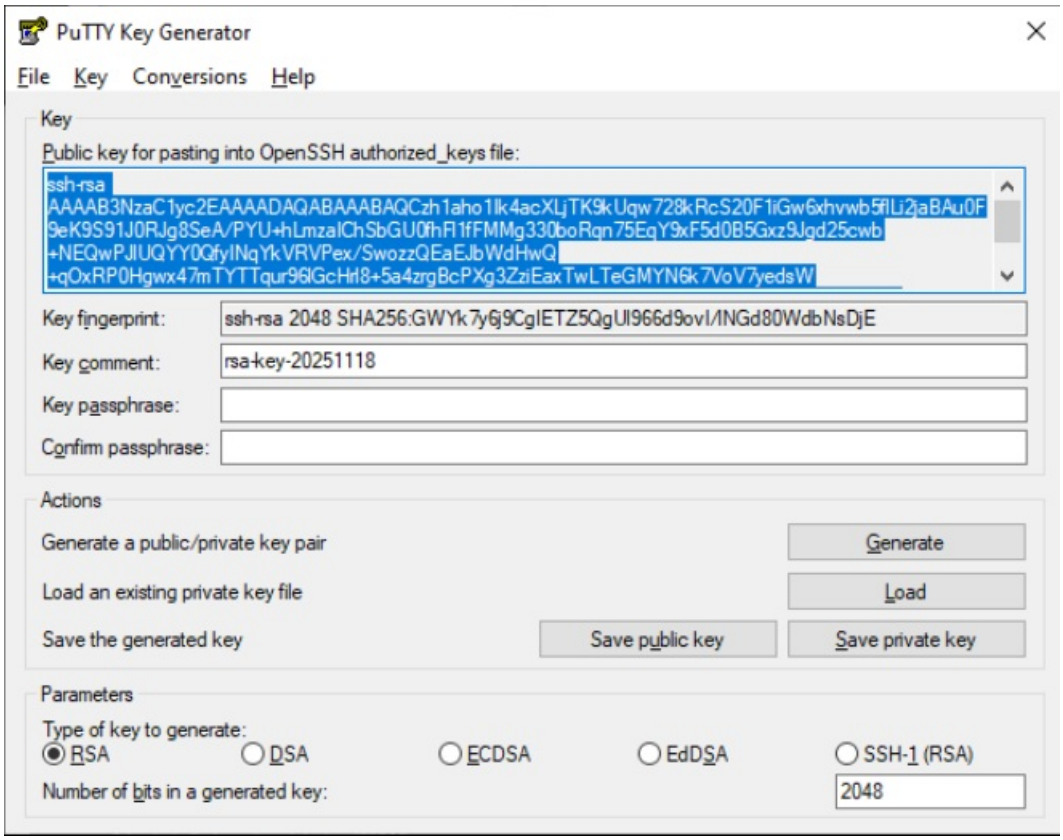
Установка

Для начала загрузите **PuTTY** с официального сайта и установите его на свой ПК. **PuTTYgen** поставляется в комплекте с **PuTTY**.

Генерация SSH-ключа

Чтобы создать SSH-ключ с помощью **PuTTYgen**, нужно выполнить следующие шаги:

1. Откройте программу **PuTTYgen**.
2. В разделе **Parameters** выберите тип ключа (например, RSA), и задайте его длину.
3. Нажмите кнопку **Generate** и перемещайте курсор мыши в пустом поле окна для создания случайных данных – это необходимо для усиления криптографической стойкости ключа.



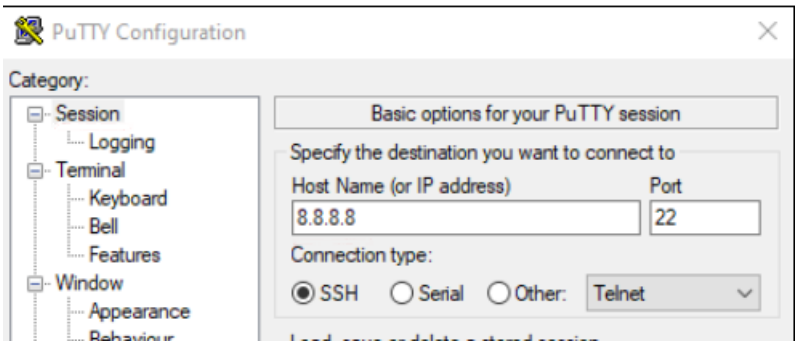
4. Сохраненный ключ имеет другой формат. Скопируйте текстовую строку из поля Public key for pasting into OpenSSH authorized_key file.
5. Создайте (или добавьте новую строку в существующий) файл **authorized_keys** на сервере в папке **~/.ssh**, и вставьте содержимое одной строкой.
6. Сохраните ключи с помощью кнопок **Save private key** (для закрытого ключа) и **Save public key** (для открытого ключа).

Закрытый ключ остается на клиенте.

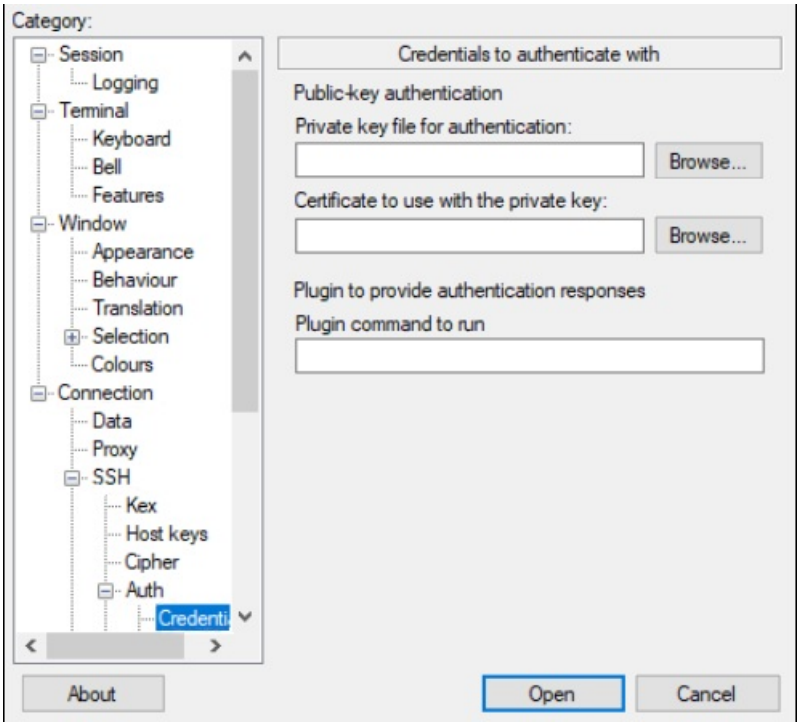
Использование SSH-ключа с PuTTY

Чтобы подключиться к серверу с помощью сгенерированного SSH-ключа, выполните следующие действия:

1. Откройте PuTTY, в разделе **Session** введите адрес сервера в поле **Host Name (or IP address)**.



2. Перейдите в раздел **Connection→SSH→Auth→Credentials** и укажите путь к вашему закрытому ключу в поле Private key file for authentification: .



3. Укажите имя пользователя, от имени которого будет производиться подключение. Для этого в разделе **Connection→Data** в поле **Auto-login username** пропишите имя пользователя.

Вы можете подключиться сразу, нажав кнопку **Open** или сохранить как сессию, чтобы в дальнейшем использовать сохранённые параметры.
Для сохранения сессии перейдите в раздел **Session**, в поле **Saved Sessions** введите имя, которое будет отображаться в списке и нажмите кнопку **Save**.
Чтобы открыть необходимую сессию, выделите её в списке и нажмите кнопку **Load**, затем кнопку **Open** или сделайте двойной клик по имени сессии в списке.

Источник: https://redvirt.red-soft.ru/base/knowledge-base/ssh-auth/