Файлы ключей SSH.

Category: GNU/Linux,ssh,ssh-keygen
2026-03-06

Host-ключи (серверные).

Используются сервером **SSH** для идентификации себя перед клиентом. Когда клиент подключается к серверу, то он ищет в своём ~/.ssh/known_hosts открытый ключ сервера. Затем решает, доверяет ли он этому серверу. Если клиент подключается к серверу первый раз, то нужно будет согласиться на добавление открытого ключа сервера в файл ~/.ssh/known_hosts на клиенте.

Файлы в /etc/ssh/.

Файл	Назначение
/etc/ssh/ssh_host_rsa_key	Приватный RSA host-ключ
/etc/ssh/ssh_host_rsa_key.pub	Публичный RSA host-ключ
/etc/ssh/ssh_host_ecdsa_key	Приватный ECDSA host-ключ
/etc/ssh/ssh_host_ecdsa_key.pub	Публичный ECDSA host-ключ
/etc/ssh/ssh_host_ed25519_key	Приватный ED25519 host-ключ
/etc/ssh/ssh_host_ed25519_key.pub	Публичный ED25519 host-ключ

На хосте смотреть так:

sudo ls /etc/ssh/ -la

Ответ:

```
[hamster@ems ~]$ sudo ls /etc/ssh/ -lo
итого 620
-rw-r--r--  1 root 592446 дек 10 05:00 moduli
-rw-r--r--  1 root   1916 дек 10 05:00 ssh_config
drwxr-xr-x. 2 root   4096 фев 27 05:00 ssh_config.d
-rw-------  1 root   3834 дек 10 05:00 sshd_config
drwx------. 2 root   4096 фев 27 05:00 sshd_config.d
-rw-------. 1 root    480 дек 26  2023 ssh_host_ecdsa_key
-rw-r--r--. 1 root    162 дек 26  2023 ssh_host_ecdsa_key.pub
-rw-------. 1 root    387 дек 26  2023 ssh_host_ed25519_key
-rw-r--r--. 1 root     82 дек 26  2023 ssh_host_ed25519_key.pub
-rw-------. 1 root   2578 дек 26  2023 ssh_host_rsa_key
-rw-r--r--. 1 root    554 дек 26  2023 ssh_host_rsa_key.pub
[hamster@ems ~]$
```

У **SSH** сервера разные ключи (**ECDSA**, **ED25519**, **RSA**) для совместимости с разными клиентами. Так как разные клиенты могут поддерживать разные алгоритмы.

Эти файлы генерируются командой:

```
sudo dpkg-reconfigure openssh-server
```

Клиентские ключи (для входа без пароля).

Генерируются на клиенте и обычно хранятся в ~/.ssh/.

Файл	Назначение
id_rsa / id_rsa.pub	Приватный и публичный RSA ключи
id_ecdsa / id_ecdsa.pub	Приватный и публичный ECDSA-ключи
id_ed25519 / id_ed25519.pub	Приватный и публичный ED25519-ключи

Генерируются командами:

```
sudo ssh-keygen -t rsa
sudo ssh-keygen -t ecdsa
sudo ssh-keygen -t ed25519
```

Файл авторизованных ключей.

Находится на сервере. Содержит публичные ключи, которым разрешено входить без пароля.

Файл	Назначение
~/.ssh/authorized_keys	Список доверенных публичных ключей

Важно: При добавлении публичного ключа в этот файл, SSH будет разрешать доступ его владельцу, если у него приватный ключ.

Known Hosts (на стороне клиента).

Хранятся публичные **host-ключи** серверов, к которым ранее подключались.

Файл на клиенте:

Файл	Назначение
~/.ssh/known_hosts	Хэш или список хостов и их публичных ключей

Позволяет клиенту проверить подлинность сервера (и избегать **MITM-атак**).

Атака «человек посередине» (англ. *man-in-the-middle attack*, наиболее известна как **MITM-атака**) — вид атаки в криптографии и компьютерной безопасности, при котором злоумышленник тайно ретранслирует и при необходимости изменяет соединение между двумя сторонами, которые ошибочно считают, что обмениваются данными напрямую друг с другом.

Оригиналы источников информации.

1. ru.wikipedia.org «Атака посредника.»
2. Alexandr Semenenko «Файлы ключей SSH.»