ssh-агент

ssh-агент — программа, хранящая в ОЗУ приватные ключи, используемые для публичной (по ключу) аутентификации (RSA, DSA).

---

ssh-агент может запускать *графическая оболочка*

1094 ? Ssl 2:28 _ **xfce4-session**

1215 ? Ss 0:06 _ /usr/bin/**ssh-agent** /usr/bin/im-launch startxfce4

или *скрипт* в ~/.bashrc:

eval "$(ssh-agent -s)" — выполнить строку как команды оболочки

(выполняются следующие команды):

SSH_AUTH_SOCK=/tmp/ssh-XXXXXXxvPknT/agent.388521; export SSH_AUTH_SOCK; - переменная экспортируется для всех потомков (это файл-сокет)

SSH_AGENT_PID=388522; export SSH_AGENT_PID;

echo Agent pid 388522;

ssh-агент висит в памяти

проверить наличие идентификаторов в ssh-агенте:

$ ssh-add -l

4096 SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 atereshchenko@twlinux206 (RSA)

удалить все идентификаторы из ssh-агента:

$ ssh-agent -D

добавить идентификатор:

$ ssh-add /home/kostushka/.ssh/timeweb

ssh-add устанавливает связь с агентом и **загружает данные ключа**

ssh-add ~/.ssh/id_rsa

ssh смотрит ключи в ssh-агенте (не на диске)

Чем полезен ssh-агент:

1. **Можно использовать запароленный ключ**

без агента ssh каждый раз будет просить пароль для ключа

ssh-агент хранит в ОЗУ незашифрованный ключ (потому пароль каждый раз при ssh подключении вводить не требуется, однако на диске посмотреть ключ без пароля будет нельзя).

2. **Можно пробрасывать ключ**

ForwardAgent yes в конфиге ssh позволяет автоматически пробрасывать ключ из ssh-агента в удаленный хост

Или можно пробросить ключ вручную, если использовать ключ -A при подключении по ssh:

kostushka@laptop:~/.ssh$ **ssh -A serv1**

Без ssh-агента проброс ключей работать не будет (с диска ключ не берется).

Для проброса ключей надо добавить ключи в ssh-agent:

1) прописать команду:

ssh-add /home/kostushka/.ssh/id_ed25519

2) или добавить в ~/.bashrc:

ssh-add ~/.ssh/timeweb

ssh-add ~/.ssh/id_ed25519

После можно подключиться на сервер с пробросом ключей из ssh-agent:

kostushka@laptop:~/.ssh$ **ssh-add -l**

4096 SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 atereshchenko@twlinux206 (RSA)

256 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w nastyatery47@yandex.ru (ED25519)

kostushka@laptop:~/.ssh$ **ssh serv1**

nastya@2280611-lq52427:~$ **ssh-add -l**

4096 SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 atereshchenko@twlinux206 (RSA)

256 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w nastyatery47@yandex.ru (ED25519)

В «Will attempt key» видим два ключа из агента и прочие файлы с ключами

nastya@2280611-lq52427:~$ **ssh -v nastya@serv2.inastris.ru**

debug1: Will attempt key: atereshchenko@twlinux206 RSA SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 agent

debug1: Will attempt key: nastyatery47@yandex.ru ED25519 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w agent

debug1: Will attempt key: /home/nastya/.ssh/id_rsa

debug1: Will attempt key: /home/nastya/.ssh/id_dsa

debug1: Will attempt key: /home/nastya/.ssh/id_ecdsa

debug1: Will attempt key: /home/nastya/.ssh/id_ecdsa_sk

debug1: Will attempt key: /home/nastya/.ssh/id_ed25519

debug1: Will attempt key: /home/nastya/.ssh/id_ed25519_sk

debug1: Will attempt key: /home/nastya/.ssh/id_xmss

...

debug1: Offering public key: /home/kostushka/.ssh/id_ed25519 ED25519 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w **agent**

debug1: Server accepts key: /home/kostushka/.ssh/id_ed25519 ED25519 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w agent

Authenticated to serv2.inastris.ru ([193.124.113.44]:22) using "publickey".

Если ключа нет в ssh-agent, то мы увидим, что ключ берется из локального файла (если он есть) или же запрашивается пароль:

kostushka@laptop:~$ **ssh -v nastya@serv2**

debug1: Offering public key: atereshchenko@twlinux206 RSA SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 agent

debug1: Authentications that can continue: publickey,password

debug1: Trying private key: /home/kostushka/.ssh/id_rsa

debug1: Trying private key: /home/kostushka/.ssh/id_ecdsa

debug1: Trying private key: /home/kostushka/.ssh/id_ecdsa_sk

debug1: Offering public key: /home/kostushka/.ssh/id_ed25519 ED25519 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w

debug1: Server accepts key: /home/kostushka/.ssh/id_ed25519 ED25519 SHA256:kB0lg/L40Owkv3rWrXn/OSiSTgDLQKFGPAxQ4qiJQ7w

Authenticated to serv2.inastris.ru ([193.124.113.44]:22) using "publickey".

При подключении к хосту по SSH родителем терминала будет sshd сервис, а не графическая оболочка. А ssh-agent запускается либо графической оболочкой, либо командой в ~/.bashrc. Таким образом, не будет переменных среды, которые содержат информацию о запущенном в графической оболочке ssh-агенте:
kostushka@laptop:~$ **env | fgrep ssh**
SSH_AUTH_SOCK=/tmp/ssh-WzAJ9QW46mJE/agent.1441 — этих переменных не будет
OLDPWD=/home/kostushka/.ssh
следовательно, ssh-agent будет недоступен.

Например, если подключиться по SSH на localhost, то ssh-agent доступен не будет:
$ ssh localhost
$ ssh-add -l
Could not open a connection to your authentication agent.

Но можно самостоятельно определить все эти значения вручную, задав путь к сокету в переменную среды, и всё заработает.
kostushka@laptop:~$ **export SSH_AUTH_SOCK=**/tmp/ssh-WzAJ9QW46mJE/agent.1441
kostushka@laptop:~$ **ssh-add -l**
4096 SHA256:KYYwbC9e2OqrbcK6EE1jdw9F9VL1GbZiAJ5SwywzgD4 atereshchenko@twlinux206 (RSA)