SSH

Luciano Sampaio
lsampaioweb@gmail.com

What Is ssh-keygen?

- ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

Algorithm and Key Size

- rsa - an old algorithm based on the difficulty of factoring large numbers. A key size of at least 2048 bits is recommended for RSA; 4096 bits is better.

- dsa - an old US government Digital Signature Algorithm. It is based on the difficulty of computing discrete logarithms. A key size of 1024 would normally be used with it. DSA in its original form is no longer recommended.

- ecdsa - a new Digital Signature Algorithm standarized by the US government, using elliptic curves. This is probably a good algorithm for current applications. Only three key sizes are supported: 256, 384, and 521 (sic!) bits. We would recommend always using it with 521 bits, since the keys are still small and probably more secure than the smaller keys (even though they should be safe as well).

- ed25519 - this is a new algorithm added in OpenSSH. Support for it in clients is not yet universal. Thus its use in general purpose applications may not yet be advisable.

Algorithm and Key Size

- ssh-keygen -t rsa -b 2048 -f file
- ssh-keygen -t dsa
- ssh-keygen -t ecdsa -b 521 -f file
- ssh-keygen -t ed25519
  - If possible, use this one.

Generate your SSH key

- ssh-keygen -t ed25519

```
lsampaio@DUD-JumpServer:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/lsampaio/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lsampaio/.ssh/id_ed25519
Your public key has been saved in /home/lsampaio/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:ounx1rVkQZVZvy+g4nJDtS+biH59AHTSnro6GrCL+GY lsampaio@DUD-JumpServer
The key's randomart image is:
+--[ED25519 256]--+
|          . ..+.  |
|         o + o  . |
|        . = .    .|
|         . =     .|
|   .    . S+ o.  . |
|    o o .o *. .  .|
|   . =  o.*.+  . .|
|..Eo ++o*o+.o  . |
|o+o o+=*o.o+     |
+----[SHA256]-----+
```

Sharing your key

- Only copy the public key:
  - ssh-copy-id -i ~/.ssh/key.pub user@host

```
lsampaio@DUD-JumpServer:~$ ssh-copy-id -i /home/lsampaio/.ssh/id_ed25519.pub lsampaio@192.168.0.192
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/lsampaio/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
lsampaio@192.168.0.192's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'lsampaio@192.168.0.192'"
and check to make sure that only the key(s) you wanted were added.

lsampaio@DUD-JumpServer:~$ ssh lsampaio@192.168.0.192
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Last login: Sun Sep 25 14:14:34 2022 from 192.168.0.67
lsampaio@ubuntu-server:~$ ls -la .ssh/
total 12
drwx------  2 lsampaio lsampaio 4096 set 25 14:14 .
drwxr-x--- 20 lsampaio lsampaio 4096 set 23 23:06 ..
-rw-------  1 lsampaio lsampaio  105 set 25 14:14 authorized_keys
lsampaio@ubuntu-server:~$ cat .ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIfqpJeJJ7tn27IkV6J9znwU6u0YTAVXR4ZlKVO9Z4PI lsampaio@DUD-JumpServer
```

Connect using SSH

- Specify ssh key if not the default:
  - ssh -i ~/.ssh/key user@host

```
lsampaio@DUD-JumpServer:~$ ssh -i ~/.ssh/id_ed25519 lsampaio@192.168.0.192
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Last login: Sun Sep 25 14:15:01 2022 from 192.168.0.67
lsampaio@ubuntu-server:~$ exit
logout
Connection to 192.168.0.192 closed.
lsampaio@DUD-JumpServer:~$ ssh lsampaio@192.168.0.192
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Last login: Sun Sep 25 14:18:35 2022 from 192.168.0.67
```

Specific config for a host

- cat ~/.ssh/config
- Host DUD-Jump-Server
  - HostName DUD-Jump-Server
  - User lsampaio

- Host switch-01.homelab
  - HostName switch-01.homelab
  - HostKeyAlgorithms +ssh-dss
  - KexAlgorithms +diffie-hellman-group1-sha1
  - Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
  - IdentityFile ~/.ssh/key

References

- How to Use ssh-keygen to Generate a New SSH Key?
- https://www.ssh.com/academy/ssh/keygen

Questions ?

Thank you!

Luciano Sampaio
lsampaioweb@gmail.com