FIELD NOTE / LINUX

Cara Setting Multiple Private Key pada SSH

Petruknisme · 26 Jan, 2019 · 2 min to read

Pada kasus tertentu, kita akan membutuhkan beberapa private key yang berbeda untuk setiap mesin yang kita autentikasi. Semisal kita memiliki akun github, gitlab dan ssh server dengan autentikasi public key yang berbeda.

Hal tersebut memungkinkan untuk kita implementasikan agar dapat menggunakan *public key* yang sudah ditentukan untuk autentikasi masing-masing platform yang menggunakan ssh sebagai sarana sistem autentikasi.

Kita bisa membuat *private* dan *public key* SSH sebanyak mungkin dengan nama yang berbeda untuk masing-masing platform. Dengan cara:

```
↳ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
```

Pada bagian lokasi penyimpanan key, kita bisa ganti dengan semisal `/home/<namauser>/.ssh/id_rsa_namaplatform` atau dengan penyimpanan yang bebas di mana saja. Tapi saya sarankan ditaruh dalam folder `~/.ssh/` agar lebih mudah.

Jadi, untuk mendapatkan *private key* dan *public key* baru, bisa menggunakan perintah di atas dengan membedakan penyimpanan berkasnya saja.

Jadi semisal kita memiliki 3 private dan public pada `~/.ssh/` yang sudah kita generate untuk masing-masing seperti berikut:

```
↳ tree ~/.ssh
/home/user/.ssh
├── id_rsa
├── id_rsa_github
├── id_rsa_github.pub
├── id_rsa_gitlab
├── id_rsa_gitlab.pub
├── id_rsa_server_lain
```

Licensed under CC BY-SA 4.0

```
├── id_rsa_server_lain.pub
├── id_rsa.pub
├── known_hosts
```

Pada dasarnya, ssh akan menggunakan `~/.ssh/id_rsa` untuk setiap kali melakukan autentikasi terhadap sistem yang melalui ssh.

Nah, pada tulisan kali ini saya akan menjelaskan tentang bagaimana caranya mengkonfigurasi ssh agar bisa menggunakan multiple private key berbeda untuk setiap platform dalam melakukan autentikasi.

Merujuk pada referensi konfigurasi ssh[1], disebutkan bahwa terdapat dua berkas konfigurasi yang di mana bersifat global dan juga hanya lingkup pengguna saja.

- user's configuration file (*~/.ssh/config*)
- system-wide configuration file (*/etc/ssh/ssh_config*)

Agar bisa menggunakan private key berbeda, hal yang harus kita lakukan adalah membuat konfigurasi untuk pengguna pada berkas `~/.ssh/config`, bila berkas tersebut belum terbuat, bisa dibuat terlebih dahulu dengan perintah `touch ~/.ssh/config`. Dan contoh konfigurasinya sebagai berikut:

~/.ssh/config

```
~/.ssh/config

Host github.com-aancw # <-- contoh nama host + github akun
  Hostname github.com # <-- domain/ip yang dipakai
  User git # <-- User yang digunakan untuk login
  IdentityFile ~/.ssh/id_rsa_github

Host server-lain.com # <-- contoh untuk hostname biasa
  Hostname server-lain.com # <-- domain/ip yang dipakai
  User root # <-- user yang digunakan untuk login
  port 22 # <-- gunakan opsi ini bila menggunakan port berbeda
  IdentityFile ~/.ssh/id_rsa_server_lain
```

Pada konfigurasi tersebut dibutuhkan informasi hostname, user, port dan juga IdentityFile. Nah hal yang paling penting adalah `IdentityFile`, konfigurasi berkas tersebut membedakan masing-masing informasi autentikasi yang sudah kita tentukan sebelumnya.

Untuk mengetahui bahwa konfigurasi kita sudah benar adalah dengan melakukan ssh ke server tujuan dan ditambahkan parameter `-vvv` seperti berikut:

Licensed under CC BY-SA 4.0

```
↳ ssh user@server-lain.com -vvvv
OpenSSH_7.9p1, OpenSSL 1.1.1a  20 Nov 2018
debug1: Reading configuration data /home/user/.ssh/config
debug1: /home/user/.ssh/config line 18: Applying options for server-lain.c
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 49: Deprecated option "useroaming"
debug2: resolving "server-lain.com" port 22
debug2: ssh_connect_direct
debug1: Connecting to server-lain.com [xxx.xxx.xxx.xxx] port 22.
debug1: Connection established.
debug1: identity file /home/user/.ssh/id_rsa_server_lain type 0
debug1: identity file /home/user/.ssh/id_rsa_server_lain-cert type -1
```

Nah, bisa kita lihat bahwa konfigurasi yang kita lakukan sudah tepat dengan ditandai oleh informasi tentang identity file yang mengarah pada private key tersebut.

Akhir kata, semoga tulisan kali ini bermanfaat. Karena berbagi itu indah, mari bagikan tulisan ini bila bermanfaat

Referensi

1. https://linux.die.net/man/5/ssh_config (https://linux.die.net/man/5/ssh_config)
2. https://gist.github.com/JoaquimLey/e6049a12c8fd2923611802384cd2fb4a (https://gist.github.com/JoaquimLey/e6049a12c8fd2923611802384cd2fb4a)

Linux # Tutorial

Licensed under CC BY-SA 4.0