

SSH 目录

目录

- [ssh-keygen](#)
- [ssh-agent](#)
- [ssh-add](#)
- [ssh CA 目录](#)
- [CA 目录](#)
- [CA 目录](#)
- [目录](#)
- [目录 CA 目录](#)
- [目录](#)
- [目录 CA 目录](#)
- [目录](#)
- [目录](#)

SSH 目录

目录 SSH
目录
目录

目录

目录

目录

目录
目录

目录


~~~~~ ~/.ssh ~~~~~ user\_ca ~~~~~ user\_ca.pub ~~~~~

~~~~~

- -t rsa ~~~~~ RSA
- -b 4096 ~~~~~ 4096 ~~~~~
1024
- -f ~/.ssh/user_ca ~~~~~
- -C user_ca ~~~~~

~~~~~ host\_ca

```
# CA
$ ssh-keygen -t rsa -b 4096 -f host_ca -C host_ca
```

~~~~~ ~/.ssh ~~~~~ host\_ca ~~~~~ host\_ca.pub ~~~~~

~~~ ~/.ssh ~~~~~

- ~/.ssh/user\_ca
- ~/.ssh/user\_ca.pub
- ~/.ssh/host\_ca
- ~/.ssh/host\_ca.pub

# CA ~~~~~

~~~ CA ~~~~~

~~~~~ CA ~~~~~ SSH ~~~~~ sshd  
~~~~~ /etc/ssh/ssh\_host\_rsa\_key ~~~~~

```
$ sudo ssh-keygen -f /etc/ssh/ssh_host_rsa_key -b 4096 -t rsa
```

~~~~~ /etc/ssh ~~~~~ ssh\_host\_rsa\_key ~~~~~ ssh\_host\_rsa\_key.pub  
~~~~~ ssh\_host\_rsa\_key.pub ~~~~~ CA ~~~~~

~~~~~ CA ~~~~~ host\_ca ~~~~~ ssh\_host\_rsa\_key.pub ~~~~~

```
$ ssh-keygen -s host_ca -I host.example.com -h -n host.example.com -V +52w  
ssh_host_rsa_key.pub
```

~~~~~ ssh\_host\_rsa\_key-cert.pub ~~~~~ -cert  
~~~~~

- `-s` `CA`
- `-I`
- `-h`
- `-n host.example.com`
- `-V +52w` `52`
- `ssh_host_rsa_key.pub`

```
$ ssh-keygen -L -f ssh_host_rsa_key-cert.pub
```

```
$ chmod 600 ssh_host_rsa_key-cert.pub
```

## CA

`CA`

```
$ ssh-keygen -f ~/.ssh/user_key -b 4096 -t rsa
```

`~/.ssh` `user_key` `user_key.pub`

`user_key.pub` `CA` `CA` `user_ca`

```
$ ssh-keygen -s user_ca -I user@example.com -n user -V +1d user_key.pub
```

`user_key-cert.pub` `-cert`

- `-s` `CA`
- `-I`
- `-n user`
- `SSH`

- 

--	--	--	--	--	--	--

--	--	--	--	--	--	--

--	--	--	--

--	--	--	--	--

CA 

user\_ca.pub

--	--	--	--	--	--	--

```
/etc/ssh
```



