ssh-keygen 基本用法

作者：fjun
原文链接：https://ld246.com/article/1546486474689
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

ssh 公钥认证是ssh认证的方式之一。通过公钥认证可实现ssh免密码登陆，git的ssh方式也是通过公进行认证的。

在用户目录的home目录下，有一个.ssh的目录，和当前用户ssh配置认证相关的文件，几乎都在这个录下。

ssh-keygen 可用来生成ssh公钥认证所需的公钥和私钥文件。

使用 ssh-keygen 时，请先进入到 ~/.ssh 目录，不存在的话，请先创建。并且保证 ~/.ssh 以及所有目录的权限不能大于 711

生成的文件名和文件位置

使用 ssh-kengen 会在~/.ssh/目录下生成两个文件，不指定文件名和密钥类型的时候，默认生成的个文件是：

- id_rsa
- id_rsa.pub

第一个是私钥文件，第二个是公钥文件。

生成ssh key的时候，可以通过 -f 选项指定生成文件的文件名，如下:

```
[huqiu@101 .ssh]$ ssh-keygen -f test   -C "test key"
                      ~~文件名   ~~~~ 备注
```

如果没有指定文件名，会询问你输入文件名:

```
[huqiu@101 .ssh]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/huqiu/.ssh/id_rsa):
```

你可以输入你想要的文件名，这里我们输入test。

密码

之后，会询问你是否需要输入密码。输入密码之后，以后每次都要输入密码。请根据你的安全需要决是否需要密码，如果不需要，直接回车:

```
[huqiu@101 .ssh]$ ssh-keygen -t rsa -f test -C "test key"
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

结果

如果文件名是test，结果是:

```
[huqiu@101 .ssh]$ ll test*
```

```
-rw------- 1 huqiu huqiu 1675 Sep 15 13:24 test
-rw-r--r-- 1 huqiu huqiu  390 Sep 15 13:24 test.pub
```

备注

上面生成的命令中，-C选项是公钥文件中的备注:

```
[huqiu@101 .ssh]$ cat test.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAlgjiMw7Askxbvp QY9rmZPQxQBzh9laxFvbaini2EgmQkN
XBA9WJOXn2YBJauoiVsdUKBWA97avjsobrTxsCYvFr1yQQvTfTlbqlqGNIhQc/3HjTl2pIkClpDWv
rRN+jpyESS4MNbfOL1qjT4c/QhGvj6U6HrN6kUyn58oyyJpTzOLG74AZELJ2Led57QvTw1yJXZu
MWioR0A3BGd25fdocLX3ebux6ya8AsloOVYfsAqGlggrARe6FXjLfMH4a/nxaAdiDYVXU/Vr1ybK
P7SfyEDGJi3JtgiPUlA6vPxUC
E+9IJPQaqqeqCGzrJ6G/XO7om1v9YLLG/H/ZN2tQ== test key
                                    ~~~~备注
```

文件的权限

为了让私钥文件和公钥文件能够在认证中起作用，请确保权限正确。

对于.ssh 以及父文件夹，当前用户用户一定要有执行权限，其他用户最多只能有执行权限。

对于公钥和私钥文件也是: 当前用户一定要有执行权限，其他用户最多只能有执行权限。

对于利用公钥登录，对其他用户配置执行权限是没有问题的。但是对于git，公钥和私钥, 以及config相关文件的权限，其他用户不可有任何权限。