# ssh命令及公钥

2015年9月27日 星期日　　下午3:21

一、简介

ssh命令，是一种远程登陆和远程执行命令。

ssh协议，全称Secure SHell，就是非常安全的shell的意思，SSH协议是IETF（Internet Engineering Task Force）的Network Working Group所制定的一种协议。SSH的主要目的是用来取代传统的telnet和R系列命令（rlogin,rsh,rexec等）远程登陆和远程执行命令的工具。

ssh协议中包含多个工具（详见参考资料1），常用的有ssh和scp。

二、ssh登录过程及ssh指纹

ssh和scp登录/传送文件的过程类似，这里只讲ssh，以A机器ssh到B机器为例。（详见参考资料1）

1、第一次登录

命令行里会看到提示，是否继续，需要输入yes，然后再输入密码

A机器登录B机器，登录成功之后，会把B机器对应的ssh指纹写在A机器的.ssh/known_host文件里，这样的话以后就不用每次输入yes了，但是需要输入密码

2、ssh指纹

顾名思义，每台机器有唯一的指纹，一般不会变。重装系统等操作，会导致ssh指纹变更，需要重新走“1、第一次登录”中的流程，而不能使用旧的指纹。

三、常用的两种登录方式

ssh协议中，比较常用的是代替telnet进行远程登录，支持很多种登入方式Publickey、Keybord Interactive、GSSAPI。但是常用的有下面几种：

1、password方式登录

我们常用的ssh或scp命令，然后输入密码，是常用的方式

2、public key的方式登录

不用输入密码的方式登录

每台机器可以生成一个公钥，可以理解为代替password方式密码，把待登录机器的公钥存在发起ssh机器的特定文件中。发起ssh命令

时，会自动去找待登录机器的公钥，找到之后就可以不输入密码的ssh/scp了。

四、public key使用方式（不输入密码）

我想从A机器，通过ssh/scp方式登录/发送文件 到B 机器上，在这个过程中不想输入密码。需要按照下面的步骤建立信任：

1、在B机器上生成B机器的公钥

A 公钥会生成在.ssh/id_rsa.pub 中（私钥生成在id_rsa中，先别管私钥），一般机器都有可以直接看到

B 如果没有，可以手动生成

```
[root@mail ~]# ssh-keygen -b 1024 -t dsa -C gucuiwen@myserver.com
Generating public/private dsa key pair.
#提示正在生成，如果选择4096长度，可能需要较长时间
Enter file in which to save the key (/root/.ssh/id_dsa):
#询问把公钥和私钥放在那里，回车用默认位置即可
Enter passphrase (empty for no passphrase):
#询问输入私钥密语，为了实现自动登陆，应该不要密语，直接回车
Enter same passphrase again:
#再次提示输入密语，再次直接回车
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
#提示公钥和私钥已经存放在/root/.ssh/目录下
The key fingerprint is:
71:e5:cb:15:d3:8c:05:ed:05:84:85:32:ce:b1:31:ce gucuiwen@myserver.com
#提示key的指纹
```

说明：

-b 1024　采用长度为1024字节的公钥/私钥对，最长4096字节，一般1024或2048就可以了，太长的话加密解密需要的时间也长。

-t dsa　　采用dsa加密方式的公钥/私钥对，除了dsa还有rsa方式，rsa方式最短不能小于768字节长度。

-C gucuiwen@myserver.com 对这个公钥/私钥对的一个注释和说明，一般用所有人的邮件代替。可以省略不写，更多其他参数请man ssh-keygen。

执行ssh-keygen -b 1024 -t rsa 命令，（注意，我看我们的测试机用的是rsa，所以不是dsa而是rsa）

后面一直回车就行

能看到.ssh/ 下，会有id_rsa.pub文件，这个就是B机器的公钥

2、把B机器上生成的公钥，写在A机器的.sssh/authorized_keys 文件里，添加新的一行就行。现在就可以用了。

3、上述的示例可以参考
work@nj01-nlp-test01.nj01.baidu.com、work@cp01-qa2014-junheng2plus103.cp01.baidu.com、work@szwg-rp-nlp349.szwg01.baidu.com文件的.ssh文件夹

五、参考资料

1、ssh命令讲的不错而且详细推荐 http://blog.lizhigang.net/archives/249
2、和上面的博客差不多，作为其补充，公钥部分讲的好
http://www.ruanyifeng.com/blog/2011/12/ssh_remote_login.html
3、公钥的生成和配置方式https://git-scm.com/book/zh/v1/%E6%9C%8D%E5%8A%A1%E5%99%A8%E4%B8%8A%E7%9A%84-Git-%E7%94%9F%E6%88%90-SSH-%E5%85%AC%E9%92%A5