

问题解决：重装系统中遇到known_hosts的ssh指纹题

2015年9月27日 星期日 下午12:34

一、简介

问题：测试机重装系统之后，ssh不上自己的机器。

原因：最终发现是ssh中的一个known_hosts会记录历史登录的ssh指纹；在我们重装系统之后，ssh指纹换了，但是known_hosts没改还是旧的，所以出错。

在另一篇笔记"ssh命令及公钥"中，有ssh、known_host中的ssh指纹等相关含义，这里主要记录了实验过程是自己探索过程中的现象，这里分析一下加深理解，最后提了一下更高级配置的方式。

二、含义

1、ssh

是一种远程登陆和远程执行命令的工具。

详见另一篇笔记“ssh命令及公钥”中的一、简介。

2、known_host中的ssh指纹

详见另一篇笔记“ssh命令及公钥”中的二、ssh登录过程及ssh指纹

三、实验过程

1、现象A：重装系统之后，我在secureCRT上登录自己的账户，登录我的机器ssh work@nj01-nlp-test01.nj01.baidu.com登不上。报错：

```
-bash-baidu-ssl$ssh work@nj01-nlp-test01.nj01.baidu.com
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@BILS SUGGESTS YOU RUN COMMAND 'clearknownhost' AND RETRY @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
56:86:ff:8c:bb:51:99:35:11:c4:71:91:b6:6b:03:9b.
Please contact your system administrator.
Add correct host key in /home/tianzhiliang/.ssh/known_hosts to get rid of this message.
Offending key in /home/tianzhiliang/.ssh/known_hosts:1
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
Permission denied (publickey,gssapi-with-mic,password).
-bash-baidu-ssl$ll
-bash: ll: command not found
```

现象B：别人在secureCRT上登录我的账户，登录我的机器，报同

指紋問

样的错误

原因：和1、一起看，说明我的secureCRT账户，也记录了类似know_hosts中ssh指纹的信息。

2、现象A：别人（寰寰）在secureCRT上登录他自己的账户，登录我的机器ssh work@nj01-nlp-test01.nj01.baidu.com没问题

现象B：从别人的一台重装系统之后的机器上，登录我的机器ssh work@nj01-nlp-test01.nj01.baidu.com没问题

原因：别人是第一次登录我的机器，会新建ssh指纹

3、现象：从我之前用过的机器上，登录我的机器ssh work@nj01-nlp-test01.nj01.baidu.com，报同样的错误。

原因：因为我在之前用过的机器上，登录过work@nj01-nlp-test01.nj01.baidu.com，便会在记录know_hosts中记录ssh指纹

4、现象：按照报错，在ssh机器之前，执行clearknownhost，可以ssh我的机器了

原因：clearknownhost清空了我账户下knownhost，重新ssh的时候，会新建一个host的ssh指纹

5、现象：用一台测试机，ssh到我重装系统的机器，失败；按照百度wiki（参考资料2），删除了~/.ssh/known_host中对应的记录，重新ssh，没问题了

原因：与4的原因类似，4是对账户的knownhost做清空，此操作是对本台测试机的knownhost清空

6、现象：对于一台机器的ssh指纹，如cp01-qa2014-junheng2plus103.cp01.baidu.com，重装系统之前所有地方记录的cp01-qa2014-junheng2plus103.cp01.baidu.com的ssh指纹是相同的，重装系统之后所有地方记录的ssh指纹是相同的，但是重装系统之前和之后的不一样。

原因：这说明就是ssh指纹在起作用，如果用的是旧的ssh指纹，就会连接失败。

四、如何配置

1、清空历史的信息

A 对账户的knownhost清空

在ssh机器之前，执行clearknownhost

R 对机器的knownhost清空

按照百度wiki（参考资料2），删除了~/.ssh/known_host中对应的记录

2、如何配置部分有一些高级用法，短时间内用不到，在这里不详细介绍，详见参考资料。

五、参考资料

1、Known_host介绍与忽略他的方法

<http://blog.csdn.net/yasaken/article/details/7348441>

2、百度wiki：重装系统之后，如何重新ssh到自己的机器上

<http://wiki.baidu.com/pages/viewpage.action?pageId=142381081>

3、更新knownhost文件高级用法

<http://junlinux.blog.51cto.com/2521744/1274732>

4、ssh命令讲的不错而且详细推荐 <http://blog.lizhigang.net/archives/249>