链滴

ssh Host key verification failed 解决方案

作者：weimian

原文链接：https://ld246.com/article/1537361621757

来源网站：链滴

1、问题

配置jenkins 最后一步需要使用scp命令 自动复制war包到服务器。提示:Host key verification failed.

2、原因

ssh连接的时候会验证authorized_keys及known_hosts，首先会验证authorized_keys是否存在本机i_rsa.pub中的公钥信息，如果验证成功会继续验证known_hosts信息，如果是第一次连接或者记录在known_hosts的ip等信息不匹配，ssh无法判断远程的服务端是否是正确的，在这里如果有人中截获了的登录请求，并且模拟ssh服务端的话，你的密码就会泄漏（中间人攻击），所以ssh会询问你：远程务端的指纹是：xxxx，是不是确定登录。

3、Public Key认证

Public Key认证是什么

这是一种认证方法，类似于常见的用户名密码认证方法。不同的是需要在客户端机器上保留一个很长长的加密key，而在服务器端需要做出相应的配置。当客户端想要访问服务器时，服务器则会检查自配置并根据客户端所提供的用户名来识别客户端。说白了就是实现了无密码访问，并同时兼有安全保措施。

认证过程简要说明

Public key对数据进行加密而且只能用于加密，Private key只能对所匹配的Public key加密过的数据行解密。我们把Public key放在远程系统合适的位置，然后从本地开始进行ssh连接。此时，远程的ssd会产生一个随机数并用我们产生的Public key进行加密后发给本地，本地会用Private key进行解密把这个随机数发回给远程系统。最后，远程系统的sshd会得出结论我们拥有匹配的Private key允许们登录

4、解决方案

1、把id_rsa.pub中的公钥复制到服务器authorized_keys中，然后指定不验证known_hosts,第一次功之后本地known_hosts中会自动生成服务器ip等连接信息，然后删除StrictHostKeyChecking 参数可。

scp -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no /app/server/jenkins/jenkns_home/workspace/xxx/target/pac-0.0.1-SNAPSHOT.war appuser@1.1.1.1:/opt/tomcat/webpps/ROOT.war

缺点：SSH登陆时会忽略known_hosts，安全性低 。

2、修改配置文件“~/.ssh/config”，加上，重启服务器。

StrictHostKeyChecking no　UserKnownHostsFile /dev/null

缺点：安全性低，略暴力，不建议使用。

3、客户端和服务器都能手动连接上的情况，直接使用客户端ssh连接服务器，第一次连接之后known hosts中会保存连接信息，下次即可免密登录。

原文链接：ssh Host key verification failed 解决方案

缺点：逼格略低，不建议使用

4、使用expect

expect是提供自动交互的工具。

demo：

```
#!/usr/bin/expect
#set timeout 20 #设置超时时间
spawn ssh root@1.1.1.1
expect "*password:"
send "123\r"
interact
```

解释:

1.#!/usr/bin/expect ： 需要先安装软件，然后来说明用expect来执行

2.spawn ssh root@1.1.1.1 ： spawn是进入expect环境后才可以执行的expect内部命令，用来执行后面的命令。

3.expect "*password:" ： 也是expect的内部命令，用来解惑关键的字符串，如果有，就会立即返回面设置的内容，如果没有就看是否设置了超时时间。

4.send "123\r"：这时执行交互式动作，与手工输入密码等效，在expect截获关键字之后，它就会输send后面的内容。

5.interact ： 执行完毕后把持交互状态，把控制台，这时候就可以进行你想要进行的操作了。如果没这一句，在登陆完成之后就会退出，而不是留在远程终端上。

缺点：第一次执行完之后，注意删掉脚本，没有缺点.

注意

authorized_keys 600权限，.ssh文件夹700权限。

同样适用于SFTP/SSH/SCP/GIT

可以参考

[ssh-the-authenticity-of-host-hostname-cant-be-established] https://stackoverflow.com/questions/3663895/ssh-the-authenticity-of-host-hostname-cant-be-established

[centos7将pub文件加入authorized_keys以后还是要输入密码，解决方法] https://blog.csdn.net/ainloving/article/details/50378049

[unixlinux-setting-up-public-key] http://tutorialgenius.blogspot.com/2012/02/unixlinux-setting-up-public-key.html