为了让两个linux机器之间使用ssh不需要用户名和密码。所以采用了数字签名RSA或者DSA来完成这个操作。

模型分析

假设 A （192.168.20.59）为客户机器，B（192.168.20.60）为目标机；

要达到的目的：

A机器ssh登录B机器无需输入密码；

加密方式选 rsa|dsa均可以，默认dsa

ssh-keygen -t rsa #使用rsa加密

二、具体操作流程

单向登陆的操作过程（能满足上边的目的）：

1、登录A机器

2、ssh-keygen -t [rsa|dsa]，将会生成密钥文件和私钥文件 id\_rsa,id\_rsa.pub或id\_dsa,id\_dsa.pub

3、将 .pub 文件复制到B机器的 .ssh 目录， 并 cat id\_dsa.pub >> ~/.ssh/authorized\_keys

4、大功告成，从A机器登录B机器的目标账户，不再需要密码了；（直接运行 #ssh 192.168.20.60 ）

双向登陆的操作过程：

1、ssh-keygen做密码验证可以使在向对方机器上ssh ,scp不用使用密码.具体方法如下:

2、两个节点都执行操作：#ssh-keygen -t rsa

然后全部回车,采用默认值.

3、这样生成了一对密钥，存放在用户目录的~/.ssh下。

将公钥考到对方机器的用户目录下 ，并将其复制到~/.ssh/authorized\_keys中（操作命令：#cat id\_dsa.pub >> ~/.ssh/authorized\_keys ）。

4、设置文件和目录权限：

设置authorized\_keys权限

$ chmod 600 authorized\_keys

设置.ssh目录权限

$ chmod 700 -R .ssh

5、要保证.ssh和authorized\_keys都只有用户自己有写权限。否则验证无效。（今天就是遇到这个问题，找了好久问题所在），其实仔细想想，这样做是为了不会出现系统漏洞。

我从20.60去访问20.59的时候会提示如下错误：

The authenticity of host '192.168.20.59 (192.168.20.59)' can't be established. RSA key fingerprint is 6a:37:c0:e1:09:a4:29:8d:68:d0:ca:21:20:94:be:18. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '192.168.20.59' (RSA) to the list of known hosts. root@192.168.20.59's password: Permission denied, please try again. root@192.168.20.59's password: Permission denied, please try again. root@192.168.20.59's password: Permission denied (publickey,gssapi-with-mic,password).

三、总结注意事项

1、文件和目录的权限千万别设置成chmod 777.这个权限太大了，不安全，数字签名也不支持。我开始图省事就这么干了

2、生成的rsa/dsa签名的公钥是给对方机器使用的。这个公钥内容还要拷贝到authorized\_keys

3、linux之间的访问直接 ssh 机器ip

4、某个机器生成自己的RSA或者DSA的数字签名，将公钥给目标机器，然后目标机器接收后设定相关权限（公钥和authorized\_keys权限），这个目标机就能被生成数字签名的机器无密码访问了

ssh-keygen设置ssh无密码登录

ssh-keygen - 生成、管理和转换认证密钥，包括 RSA 和 DSA 两种密钥

密钥类型可以用 -t 选项指定。如果没有指定则默认生成用于SSH-2的RSA密钥

配置：

1、在本地机器中的~/.ssh/目录下执行下命令

ssh-keygen -t dsa

将生成两个文件,id\_dsa和id\_dsa.pub

2、将id\_dsa.pub拷贝到远程机器,并且将id\_dsa.pub的内容添加到~/.ssh/authorized\_keys中

cat id\_dsa.pub >>authorized\_keys

注意:目录.ssh和文件authorized\_keys的权限必须是600

完成以上操作之后，用户从本地机器到远程机器就不需要用密码了

几个文件的作用说明，摘自http://lamp.linux.gov.cn/OpenSSH/ssh-keygen.html

~/.ssh/identity

该用户默认的 RSA1 身份认证私钥(SSH-1)。此文件的权限应当至少限制为"600"。

生成密钥的时候可以指定采用密语来加密该私钥(3DES)。

ssh将在登录的时候读取这个文件。

~/.ssh/identity.pub

该用户默认的 RSA1 身份认证公钥(SSH-1)。此文件无需保密。

此文件的内容应该添加到所有 RSA1 目标主机的 ~/.ssh/authorized\_keys 文件中。

~/.ssh/id\_dsa

该用户默认的 DSA 身份认证私钥(SSH-2)。此文件的权限应当至少限制为"600"。

生成密钥的时候可以指定采用密语来加密该私钥(3DES)。

ssh将在登录的时候读取这个文件。

~/.ssh/id\_dsa.pub

该用户默认的 DSA 身份认证公钥(SSH-2)。此文件无需保密。

此文件的内容应该添加到所有 DSA 目标主机的 ~/.ssh/authorized\_keys 文件中。

~/.ssh/id\_rsa

该用户默认的 RSA 身份认证私钥(SSH-2)。此文件的权限应当至少限制为"600"。

生成密钥的时候可以指定采用密语来加密该私钥(3DES)。

ssh将在登录的时候读取这个文件。

~/.ssh/id\_rsa.pub

该用户默认的 RSA 身份认证公钥(SSH-2)。此文件无需保密。

此文件的内容应该添加到所有 RSA 目标主机的 ~/.ssh/authorized\_keys 文件中。

/etc/ssh/moduli

包含用于 DH-GEX 的 Diffie-Hellman groups

BG2BLT01 is on, BG2BLT02 is power off. They’re too noisy L

When and how to move them to data center?

Please update SSH key in .33 server for git repo access.

ssh-keygen -t dsa

scp ~/.ssh/id\_dsa.pub [YOUR\_USER\_NAME]@10.38.116.33:authorized\_keys

ssh [YOUR\_USER\_NAME]@ 10.38.116.33

skip below 3 steps if you already have .ssh and .ssh/authorized\_keys

mkdir -m 700 .ssh

touch .ssh/authorized\_keys

chmod 600 .ssh/authorized\_keys

cat authorized\_keys >> .ssh/authorized\_keys;exit

vi ~/.ssh/config

add lines and save quit

host 10.38.116.33

user [YOUR\_USER\_NAME]

————————————————

版权声明：本文为CSDN博主「wh\_19910525」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/wh\_19910525/article/details/7433164