SSH免密码登陆

|  |  |  |  |
| --- | --- | --- | --- |
| 编写 | 刘化罗 | 编写时间 | 2015-1-16 |
| 审核 |  | 审核时间 |  |
| 审批 |  | 审批时间 |  |

**文档修订历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **作者** | **工作描述** | **修订历史** | **修改日期** |
| V1.0 | 刘化罗 | 根据网络安装文档改编 |  | 2015-1-16 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1 实现原理

使用一种被称为"公私钥"认证的方式来进行ssh登录。"公私钥"认证方式简单的解释是：

首先在客户端上创建一对公私钥（公钥文件：~/.ssh/id\_rsa.pub；私钥文件：~/.ssh/id\_rsa），然后把公钥放到服务器上 （~/.ssh/authorized\_keys），自己保留好私钥。当ssh登录时，ssh程序会发送私钥去和服务器上的公钥做匹配。如果匹配成功就可 以登录了。

# 2. 实验环境

A机：TS-DEV/10.0.0.163

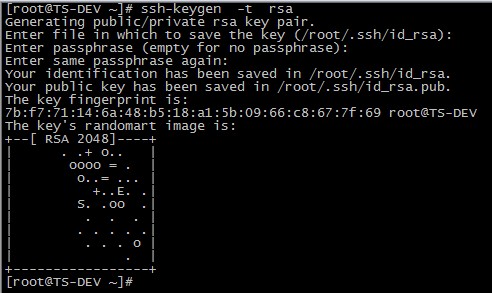
B机：CS-DEV/10.0.0.188

# 3. Linux/Unix双机建立信任

1. 在A机生成证书

在A机root用户下执行ssh-keygen命令，在需要输入的地方，直接回车，生成建立安全信任关系的证书。

# ssh-keygen  -t  rsa

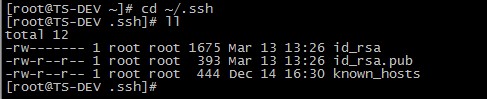


注意：在程序提示输入passphrase时直接输入回车，表示无证书密码。  
　　　上述命令将生成私钥证书id\_rsa和公钥证书id\_rsa.pub，存放在用户家目录的.ssh子目录中。

1. 查看~/.ssh生成密钥的文件

# cd ~/.ssh

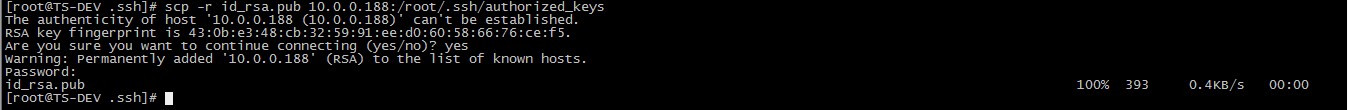
# ll



1. A对B建立信任关系

将公钥证书id\_rsa.pub复制到机器B的root家目录的.ssh子目录中，同时将文件名更换为authorized\_keys，此时需要输 入B机的root用户密码（还未建立信任关系）。建立了客户端到服务器端的信任关系后，客户端就可以不用再输入密码，就可以从服务器端拷贝数据了。

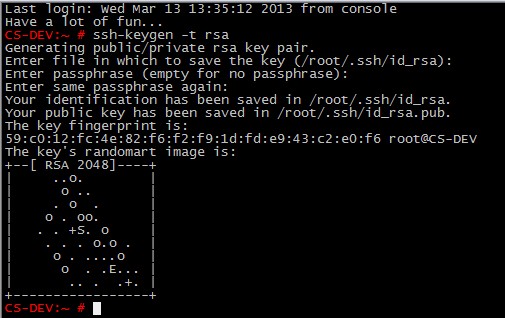
# scp -r id\_rsa.pub 10.0.0.188:/root/.ssh/authorized\_keys



1. B对A建立信任关系

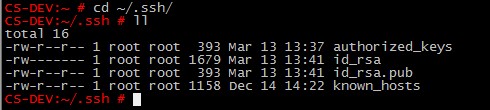
在B机上执行同样的操作，建立B对A的信任关系。

# ssh-keygen -t rsa

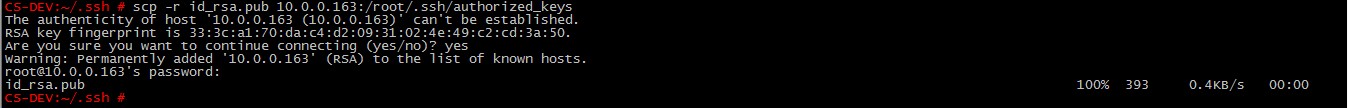


# cd ~/.ssh/

# ll



# scp -r id\_rsa.pub 10.0.0.163:/root/.ssh/authorized\_keys



如果想让B，C同时可以scp不输入密码，传输A中的数据；

则要把B、C的公钥都给 A；  
操作步骤：把两机器的id\_rsa.pub中的数据都拷贝到A的/root/.ssh/authorized\_keys文件中，一行表示一条；

A: scp -r id\_rsa.pub 10.0.0.163:/root/.ssh/authorized\_keys

B: scp -r id\_rsa.pub 10.0.0.188:/root/.ssh/authorized\_keys

测试 ssh root@10.0.0.188 'hostname'  ///  ssh root@10.0.0.163 'hostname'

如果连接反应慢，请修改以下两参数

/etc/ssh/sshd\_config  
GSSAPIAuthentication no  
UseDNS no  
然后重启service sshd restart