<http://www.cnblogs.com/ggjucheng/archive/2012/08/19/2646346.html>

**前言**

本文基于实际Linux管理工作，实例讲解工作中使用ssh证书登录的实际流程，讲解ssh证书登录的配置原理，基于配置原理，解决实际工作中，windows下使用SecureCRT证书登录的各种问题，以及实现hadoop集群部署要求的无密码跳转问题。

ssh有密码登录和证书登录，初学者都喜欢用密码登录，甚至是root账户登录，密码是123456。但是在实际工作中，尤其是互联网公司，基本都是证书登录的。内网的机器有可能是通过密码登录的，但在外网的机器，如果是密码登录，很容易受到攻击，真正的生产环境中，ssh登录都是证书登录。

**证书登录的步骤**

1.客户端生成证书:私钥和公钥，然后私钥放在客户端，妥当保存，一般为了安全，访问有黑客拷贝客户端的私钥，客户端在生成私钥时，会设置一个密码，以后每次登录ssh服务器时，客户端都要输入密码解开私钥(如果工作中，你使用了一个没有密码的私钥，有一天服务器被黑了，你是跳到黄河都洗不清)。

2.服务器添加信用公钥：把客户端生成的公钥，上传到ssh服务器，添加到指定的文件中，这样，就完成ssh证书登录的配置了。

假设客户端想通过私钥要登录其他ssh服务器，同理，可以把公钥上传到其他ssh服务器。

真实的工作中:员工生成好私钥和公钥(千万要记得设置私钥密码)，然后把公钥发给运维人员，运维人员会登记你的公钥，为你开通一台或者多台服务器的权限，然后员工就可以通过一个私钥，登录他有权限的服务器做系统维护等工作，所以，员工是有责任保护他的私钥的，如果被别人恶意拷贝，你又没有设置私钥密码，那么，服务器就全完了，员工也可以放长假了。

**客户端建立私钥和公钥**

在客户端终端运行命令

ssh-keygen -t rsa

rsa是一种密码算法，还有一种是dsa，证书登录常用的是rsa。

假设用户是blue,执行 ssh-keygen 时，才会在我的home目录底下的 .ssh/ 这个目录里面产生所需要的两把 Keys ，分别是私钥 (id\_rsa) 与公钥 (id\_rsa.pub)。

另外就是私钥的密码了，如果不是测试，不是要求无密码ssh，那么对于passphrase，不能输入空(直接回车),要妥当想一个有特殊字符的密码。

**ssh服务端配置**

ssh服务器配置如下:

[复制代码](javascript:void(0);)

vim /etc/ssh/sshd\_config

#禁用root账户登录，非必要，但为了安全性，请配置

PermitRootLogin no

# 是否让 sshd 去检查用户家目录或相关档案的权限数据，

# 这是为了担心使用者将某些重要档案的权限设错，可能会导致一些问题所致。

# 例如使用者的 ~.ssh/ 权限设错时，某些特殊情况下会不许用户登入

StrictModes no

# 是否允许用户自行使用成对的密钥系统进行登入行为，仅针对 version 2。

# 至于自制的公钥数据就放置于用户家目录下的 .ssh/authorized\_keys 内

RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile %h/.ssh/authorized\_keys

#有了证书登录了，就禁用密码登录吧，安全要紧

PasswordAuthentication no

[复制代码](javascript:void(0);)

配置好ssh服务器的配置了，那么我们就要把客户端的公钥上传到服务器端，然后把客户端的公钥添加到authorized\_keys

在客户端执行命令

scp ~/.ssh/id\_rsa.pub blue@<ssh\_server\_ip>:~

在服务端执行命令

cat id\_rsa.pub >> ～/.ssh/authorized\_keys

如果有修改配置/etc/ssh/sshd\_config，需要重启ssh服务器

/etc/init.d/ssh restart

**客户端通过私钥登录ssh服务器**

ssh命令

ssh -i /blue/.ssh/id\_rsa blue@<ssh\_server\_ip>

scp命令

scp -i /blue/.ssh/id\_rsa filename blue@<ssh\_server\_ip>:/blue

每次敲命令，都要指定私钥，是一个很繁琐的事情，所以我们可以把私钥的路径加入ssh客户端的默认配置里

修改/etc/ssh/ssh\_config

#其实默认id\_rsa就已经加入私钥的路径了,这里只是示例而已

IdentityFile ~/.ssh/id\_rsa

#如果有其他的私钥，还要再加入其他私钥的路径

IdentityFile ~/.ssh/blue\_rsa

**其他应用场景**

**SecureCRT密钥key远连接程ssh证书登录Linux**

  国内大部分人用的系统是windows，而windows下有很多ssh客户端图形工作，最流行，功能最强大的就是SecureCRT了，所以我会单独针对SecureCRT简单讲下实现ssh证书登录Linux的要点,步骤如下:

  1:在SecureCRT创建私钥和公钥:主菜单->工具->创建公钥->选择RSA->填写私钥的密码->密钥长度填为1024->点击完成，生成两个文件,默认名为identity和identity.pub

  2.把私钥和公钥转换为OpenSSH格式:主菜单->工具->转换私钥到OpenSSH格式->选择刚生成私钥文件identity->输入私钥的密码->生成两个文件，指定为id\_rsa,id\_rsa.pub

  3.把公钥id\_rsa.pub上传到ssh服务器，按照之前配置服务器端的证书，再配置一次。

  另外，如果你之前用windows的 SecureCRT的证书登录linux的，有一天你换成了linux，并希望通过原来的私钥登录公司的服务器，那么可以把id\_rsa拷贝倒~/.ssh/目录下，配置ssh客户端参考上文。

  备注:ssh对证书的文件和目录权限比较敏感，要么根据出错提示设置好文件和目录权限，要么是把StrictModes选项设置为no

**hadoop部署的无密码ssh登录**

hadoop要求master要无密码跳转到每个slave,那么master就是上文中的ssh客户端了，步骤如下

   在hadoop master上，生成公钥私钥，这个场景下，私钥不能设置密码。

   把公钥上传到每个slave上指定的目录，这样就完成了ssh的无密码跳转了。

**总结**

ssh证书登录，在实际工作才是最常用的登录方式，本人结合了真正工作的场景普及了ssh证书登录的知识，并根据流行的hadoop部署和windows下最常用的SecureCRT实例讲解了证书登录。