CentOS6 ssh 配置无密码访问

周永强

June 22, 2014

1 说明

1.1 目的

本文档讲述如何设置 ssh 无密码访问，环境为两台装有 CentOS 6.4 的计算机，每台计算机至少有一块以太网卡，二者可以通过网络相互访问，即通过主机名可以相互 ping 通，二者的主机名分别为 node01 和 node02。

`root@node01` 表示： 位于主机 `node01` 上的 `root` 用户。
`root@node01` 表示： 位于主机 `node02` 上的 `root` 用户。

更准备的表述为：通过设置 ssh 使得 root@node01 可以无密码访问 root@node02。

1.2 原理

root@node01 产生自己的公钥和私钥，并将自己的公钥上传到 root@node02 的信任文件里面，这样 root@node01 用户每次通过 ssh 登录到 root@node02 时便可通过 rsa 进行验证，免去输入密码的麻烦。

2 配置过程

1. root@node02 : 编辑/etc/ssh/sshd_config 文件，去掉如下条目的内容前的注释符号 #

```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile     .ssh/authorized_keys
```

2. root@node02 : 重启 sshd 服务

```
service sshd restart
```

3. root@node01 : 生成自己的密钥和私钥，直接 enter 按照默认设置即可，不需要输入任何内容，正常情况下这一步执行完成后，应该在 /.ssh 目录下生成两个文件 id_rsa(私钥) 和 id_rsa.pub（公钥）

```
ssh-keygen -t rsa
```

4. root@node01 : 将自己的公钥加入 root@node02 的信任区，并设置权限

```
ssh root@node02 'mkdir -p /root/.ssh'
scp /root/.ssh/id_rsa.pub root@node02:/root/.ssh/authorized_keys
ssh root@node02 'chmod  700 /root/.ssh'
ssh root@node02 'chmod  600 /root/.ssh/*'
```

5. root@node01 : 完成上述步骤已经可以无密码访问了，但是 CentOS 6.4 比较乖张，在其 Bug Tracker 上看到导致原因是当设置 selinux 为 enforcing 时，所有客户端的认证都被忽略。解决方法是，运行下列命令。

```
ssh root@node02 'restorecon -R -v /root/.ssh'
```