liunx 机器之间配置 ssh 免密登陆

作者：kevinBobo
原文链接：https://ld246.com/article/1545993009180
来源网站：链滴

SSH服务简介

root用户的互信在维护监控时可有可无，hadoop用户的互信最好配置上。

1. ssh-keygen 创建公钥（Public Key）和密钥（Private Key）。?

2. ssh-copy-id 把本地主机的公钥复制到远程主机的authorized_keys文件上。也会给远程主机的用主目录（home）和~/.ssh, 和~/.ssh/authorized_keys设置合适的权限?

3. 我们使用client端去登陆server端免密码输入。

lClient 必须制作 Public & Private 这两把 keys，且 Private Key需放到~/.ssh/ 内；

lServer 必须要有 Public Key ，且放置到用户家目录下的~/.ssh/authorized_keys，同时目录的权限 (ssh/) 必须是 700 而目录文件则必须为 644 ，同时文件的拥有者与群组都必须与该账号吻合才行。

安装步骤：

1. 步骤1: 用 ssh-key-gen 在本地主机上创建公钥和密钥　ssh-keygen -t rsa

2. 步骤2: 用 ssh-copy-id 把公钥复制到远程主机上　ssh-copy-id -i ~/.ssh/id_rsa.pub? root@192.68.6.102

3. 步骤3: 直接登录远程主机　ssh 192.168.6.102

示例：

```
[breath@nagios1 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/breath/.ssh/id_rsa): [Enter key]
Enter passphrase (empty for no passphrase): [Enter key]
Enter same passphrase again: [Enter key]
Your identification has been saved in /home/breath/.ssh/id_rsa.
Your public key has been saved in /home/breath/.ssh/id_rsa.pub.
The key fingerprint is:
cd:5a:2a:bb:4a:49:97:8a:2d:70:19:18:60:56:9c:78 breath@nagios1
The key's randomart image is:
+--[ RSA 2048]----+
|+o+..            |
|o+ E             |
|. o              |
|   o   . o       |
|. o . o S +      |
| o + +   +       |
|  o = . o        |
|   o   o         |
|    ..o.         |
```

```
[breath@nagios1 ~]$ cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.80.131 nagios1
192.168.80.132 nagios2
[breath@nagios1 ~]$ ssh-copy-id -i ~/.ssh/id_rsa.pub breath@192.168.80.132
breath@192.168.80.132's password:
Now try logging into the machine, with "ssh 'breath@192.168.80.132'", and check in:
```

原文链接：liunx 机器之间配置 ssh 免密登陆

```
  .ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
[breath@nagios1 ~]$ ssh nagios2
Last login: Mon Sep  1 16:35:04 2014 from nagios1
[breath@nagios2 ~]$ exit
logout
Connection to nagios2 closed.
```

集群统一配置步骤

集群内由于服务器较多，单个设置较繁琐，所以思路是将一台服务器生成密钥公钥然后传输到其他所服务器上去，即可免密。设置之前确认集群内服务器无已经存在的密钥，否则会覆盖，造成已经存在密钥失效。

```
[breath@nagios1 .ssh]$ cd ~/.ssh/
[breath@nagios1 .ssh]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/breath/.ssh/id_rsa): [Enter key]
Enter passphrase (empty for no passphrase): [Enter key]
Enter same passphrase again: [Enter key]
Your identification has been saved in /home/breath/.ssh/id_rsa.
Your public key has been saved in /home/breath/.ssh/id_rsa.pub.
The key fingerprint is:
82:77:58:ca:bb:34:d4:27:4b:89:b0:83:6e:c8:3e:ad breath@nagios1
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|    .   .        |
|   . = * .       |
|  . + O S .      |
| .o   + = +      |
|..+    + .       |
|.o . . o         |
| Eo    .         |
+-----------------+
[breath@nagios1 .ssh]$ ls -lrt
total 8
-rw-r--r-- 1 breath breath  396 Sep  1 16:53 id_rsa.pub
-rw------- 1 breath breath 1675 Sep  1 16:53 id_rsa
[breath@nagios1 .ssh]$ cp id_rsa.pub authorized_keys
[breath@nagios1 .ssh]$ chmod 600 authorized_keys
[breath@nagios1 .ssh]$ scp * nagios2:~/.ssh/
The authenticity of host 'nagios2 (192.168.80.132)' can't be established.
RSA key fingerprint is b8:42:c9:d5:c0:ed:a4:58:4a:bc:92:96:0b:a2:0d:96.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nagios2,192.168.80.132' (RSA) to the list of known hosts.
breath@nagios2's password: [input password for breath@nagios2]
authorized_keys                               100%  396     0.4KB/s   00:00
id_rsa                                        100% 1675     1.6KB/s   00:00
id_rsa.pub                                    100%  396     0.4KB/s   00:00
[breath@nagios1 .ssh]$
[breath@nagios1 .ssh]$ ssh nagios2
Last login: Mon Sep  1 16:53:08 2014 from nagios1
```