

Ubuntu和CentOS如何配置SSH使得无密码登陆

在使用Hadoop的时候，一般配置SSH使得我们可以无密码登录到主机，下面分别以Ubuntu和CentOS两个平台来举例说明如何配置SSH使得我们可以无密码登录到主机，当然，你得先安装好SSH服务器，并开启（关于如何在Linux平台下安装好SSH请参加本博客的[《Linux平台下安装SSH》](#)）

在 Ubuntu 平台设置 SSH 无密钥登录

Ubuntu配置步骤如下所示：

```
[wyp@localhost ~]$ ssh-keygen -t dsa -P ""
Generating public/private dsa key pair.
Enter file in which to save the key (/home/wyp/.ssh/id_dsa):
Created directory '/home/wyp/.ssh'.
Your identification has been saved in /home/wyp/.ssh/id_dsa.
Your public key has been saved in /home/wyp/.ssh/id_dsa.pub.
The key fingerprint is:
bd:2c:ed:ab:6d:a9:b2:45:88:32:08:5a:d2:d9:ad:cc wyp@ubuntu
The key's randomart image is:
+--[ DSA 1024]-----+
|          |
| . o .    |
| o + . .   |
| o+ o o . . |
| o o E . S . |
|  o  . o .  |
|    o +.    |
|    .. +o   |
|    .oo++ . |
+-----+
```

这样就会在wyp用户的/home/wyp/.ssh/目录下生成id_dsa和id_dsa.pub两个文件，输出如下：

```
[wyp@ubuntu ~]$ cd /home/wyp/.ssh/
[wyp@ubuntu:~/.ssh]$ ls -l
total 8
-rw----- 1 wyp wyp 668 2013-10-21 02:51 id_dsa
-rw-r--r-- 1 wyp wyp 600 2013-10-21 02:51 id_dsa.pub
```

将id_dsa.pub里面的内容加到用于认证的公钥文件中，命令如下（注意：不要复制，一定要用cat去操作，不信你可以去试试。）：

```
[wyp@ubuntu:~/.ssh]$ cat id_dsa.pub >> authorized_keys
```

可以将这个生成的authorized_keys拷贝到别的机器上面

```
[wyp@ubuntu:~/.ssh]$ cat ~/.ssh/authorized_keys W  
| ssh wyp@192.168.130.141 "cat - >> ~/.ssh/authorized_keys"
```

输入下面命令，如果显示如下类似的信息，就说明配置好了！

```
[wyp@ubuntu:~/.ssh]$ ssh localhost  
The authenticity of host 'localhost (:::1)' can't be established.  
RSA key fingerprint is 22:9b:94:45:dc:f0:c8:02:03:b2:a1:30:d3:04:92:01.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.  
linux ubuntu 2.6.32-38-generic #83-Ubuntu SMP Wed Jan 4 11:12:07 UTC 2012  
x86_64 GNU/Linux  
Ubuntu 10.04.4 LTS
```

```
Welcome to Ubuntu!  
* Documentation: https://help.ubuntu.com/
```

```
242 packages can be updated.  
213 updates are security updates.
```

```
New release 'precise' available.  
Run 'do-release-upgrade' to upgrade to it.
```

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.
```

```
[wyp@localhost ~]$
```

但是实际上，很多人都没有这么顺利的，一般的问题都是文件权限设置的不对，请把.ssh和authorized_keys的访问权限分别设置为755和600（也就是只有自己对上面两个文件有写权限），命令如下：

```
[wyp@localhost ~]$ chmod 755 /home/wyp/.ssh  
[wyp@localhost ~]$ chmod 600 /home/wyp/.ssh/authorized_keys
```

假如这台服务器上面还有test用户，如何使得wyp用户能够无密码登录到test（IP地址为192.168.142.129）呢？执行下面命令

```
[wyp@localhost ~]$ cat /home/wyp/.ssh/id_dsa.pub |  
ssh test@192.168.142.129 'cat - >> ~/.ssh/authorized_keys'
```

之后，在wyp用户下执行下面命令

```
[wyp@localhost ~]$ ssh test@192.168.142.129  
linux ubuntu 2.6.32-38-generic #83-Ubuntu SMP Wed Jan 4 11:12:07  
UTC 2012 x86_64 GNU/Linux  
Ubuntu 10.04.4 LTS
```

```
Welcome to Ubuntu!  
* Documentation: https://help.ubuntu.com/
```

```
240 packages can be updated.  
213 updates are security updates.
```

```
New release 'precise' available.  
Run 'do-release-upgrade' to upgrade to it.
```

```
Last login: Mon Oct 21 02:48:01 2013 from localhost  
[test@localhost ~]$
```

如果出现上述类似的信息，说明成功了！登陆到test用户了。注意上面的信息只有第一次登录的时候才会显示，以后登陆只会显示下面类似的信息：

```
[wyp@localhost ~]$ ssh test@192.168.142.129  
Last login: Mon Oct 21 02:49:51 2013 from localhost  
[test@localhost ~]$
```

上面是以Ubuntu平台为例子。

在 CentOS 平台设置 SSH 无密钥登录

下面来说说怎么在CentOS平台上面配置，（CentOS由于权限比Ubuntu的更加严格，所以配置起来比较麻烦），首先，我们需要设置一下/etc/ssh/sshd_config文件，请将/etc/ssh/sshd_config文件中下面三行的注释去掉：

```
[root@localhost ~]# vim /etc/ssh/sshd_config
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

其余的步骤和开始的一样如下所示：

```
[wyp@localhost ~]$ ssh-keygen -t dsa -P ""
Generating public/private dsa key pair.
Created directory '/home/wyp/.ssh'.
Your identification has been saved in /home/wyp/.ssh/dsa.
Your public key has been saved in /home/wyp/.ssh/dsa.pub.
The key fingerprint is:
15:57:37:f1:ee:05:26:3a:9e:e1:aa:b3:11:27:b3:1a wyp@localhost.localdomain
The key's randomart image is:
+--[ DSA 1024]-----+
|      . ...00 |
|      o  .o |
|     .. o . |
|    .. o o |
|   + S +  o |
|   * o +  .. |
|  E o +  . |
|  o..  |
|  . o+  |
+-----+
[wyp@localhost ~]$ cat ~/.ssh/dsa.pub >> ~/.ssh/authorized_keys
[wyp@localhost ~]$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is f3:f8:0b:26:a1:8e:14:55:34:ec:cb:99:f8:70:2c:d3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
Last login: Fri Aug 9 08:39:32 2013 from 192.168.142.1
[wyp@localhost ~]$
```

好了，配置完成了。

如果登陆失败了，可以通过ssh提供的一个参数查看错误的原因

```
[wyp@localhost ~]$ ssh -v localhost
```

如果/etc/ssh/sshd_config文件内容修改了，.ssh和authorized_keys的权限都做了相应的修改，但是还出现了下面的错误

```
[wyp@localhost ~]$ ssh localhost
Agent admitted failure to sign using the key.
wyp@localhost's password:
```

可以用下面的方法解决

```
[wyp@localhost ~]$ ssh-add ~/.ssh/id_dsa
Identity added: /home/wyp/.ssh/id_dsa (/home/wyp/.ssh/id_dsa)
[wyp@localhost ~]$ ssh localhost
Last login: Fri Oct 25 10:50:46 2013 from localhost.localdomain
```

id_dsa文件是上面ssh-keygen -t dsa -P "生成的。

下一步把生成的 秘钥发到需要无秘钥登录的机器上。比如我想在 192.168.1.113 上无秘钥登录上面机器，可以使用下面命令进行：

```
cat ~/.ssh/authorized_keys | ssh root@192.168.1.113 "cat - >> ~/.ssh/authorized_keys"
```

本博客文章除特别声明，全部都是原创！

原创文章版权归过往记忆大数据（[过往记忆](#)）所有，未经许可不得转载。

本文链接: [【】](#) ()