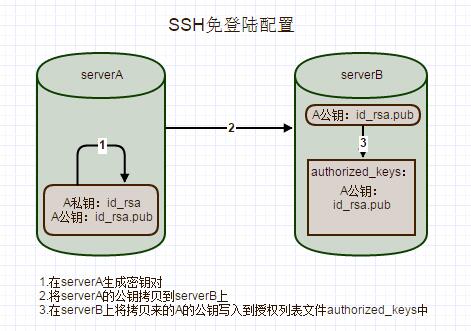
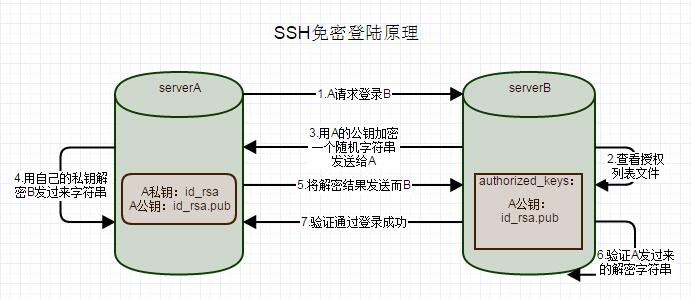
一、SSH免密登录原理

SSH免密登陆配置图示



SSH免密登录原理图示



二、具体配置操作

环境准备

1. 操作系统：centos 6.4
2. serverA： 192.168.100.129
3. serverB： 192.168.100.130

配置

没做任何配置前从serverA上SSH登录到serverB时需要输入密码的（如果是第一次登录，输入密码前还会询问授权yes/no，只管输入yes就行）：

[binxin@serverA ~]$ ssh binxin@serverB

binxin@serverb's password:

Last login: Fri Apr 1 00:35:41 2016 from servera

[binxin@serverB ~]$

下面开始免密登陆的配置：

* 在serveA上生成秘钥对：

[binxin@serverA ~]$ ssh-keygen -t rsa

Generating public/private rsa key pair.

Enter file in which to save the key (/home/binxin/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/binxin/.ssh/id\_rsa.

Your public key has been saved in /home/binxin/.ssh/id\_rsa.pub.

The key fingerprint is:

f2:f1:00:ca:b0:d0:3c:52:ac:9b:b7:0d:7e:62:f3:39 binxin@serverA

The key's randomart image is:

+--[ RSA 2048]----+

| .. |

| +. |

|o.= . |

|.o = . . |

| o. o . S |

|o o o + |

| o + . . |

| \* E. |

| . =o. |

+-----------------+

[binxin@serverA ~]$

查看用户目录下的ssh（隐藏的）文件夹，秘钥对已经生成，公钥id\_rsa.pub，私钥id\_rsa

[binxin@serverA ~]$ cd .ssh/

[binxin@serverA .ssh]$ ls

id\_rsa id\_rsa.pub known\_hosts

[binxin@serverA .ssh]$

* 通过scp命令复制serverA的公钥到serverB上

[binxin@serverA .ssh]$ scp ~/.ssh/id\_rsa.pub binxin@serverB:/home/binxin/id\_rsa.pub

binxin@serverb's password:

id\_rsa.pub 100% 396 0.4KB/s 00:00

[binxin@serverA .ssh]$

* 登录serverB，将上步靠过来的公钥添加到授权列表文件authorized\_keys中，刚开始没有这个文件，追加的时候自动生成了

[binxin@serverB ~]$ cd .ssh/

[binxin@serverB .ssh]$ ls

[binxin@serverB .ssh]$ cat ~/id\_rsa.pub >> ~/.ssh/authorized\_keys

[binxin@serverB .ssh]$ ls

authorized\_keys

[binxin@serverB .ssh]$

* authorized\_keys文件的权限必须为600，ssh目录权限必须为700，手动修改权限

[binxin@serverB ~]$ chmod 700 ~/.ssh

[binxin@serverB ~]$ chmod 600 ~/.ssh/authorized\_keys

* 检验配置是否成功，从serverA通过ssh登陆到serverB，发现不用输密码直接登陆成功了，搞定！

[binxin@serverA .ssh]$ ssh binxin@serverB

Last login: Fri Apr 1 00:46:54 2016 from servera

[binxin@serverB ~]$

三、可能的问题

权限问题

配置完authorized\_keys一直不生效，很可能是因为.ssh目录和下面文件的权限问题导致的，因为目录的权限已经超过了sshd的要求权限。如果希望ssh公钥生效需满足至少下面两个条件：.ssh目录的权限必须是700，.ssh/authorized\_keys文件权限必须是600