

SSH密钥创建分发(端口号非22)&脚本实现自动创建分发密钥

惨绿少年 Linux运维, 安全, 自动化, 运维基本功 0评论 来源: 本站原创 35°C 字体: 小 中 大

1.1 服务端端口号变化了, 如何基于秘钥连接

1.1.1 环境准备

实验环境:

```
[root@test ~]# cat /etc/redhat-release
CentOS release 6.9 (Final)
```

将一台服务器的ssh服务端口修改为63389

```
[root@test ~]# netstat -lntup|grep sshd
tcp        0      0 0.0.0.0:63389 0.0.0.0:*        LISTEN      5083/sshd
tcp        0      0 :::63389    :::*              LISTEN      5083/sshd
```

1.1.2 通过另外一台服务器创建并分发密钥

第一个里程碑: 现创建密钥使用 ssh-keygen

```
[root@backup ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): #指定密钥对的保存路径
Enter passphrase (empty for no passphrase): #为密钥对创建密码
Enter same passphrase again: #确认为密钥对创建的密码
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
72:48:65:1d:25:69:e1:4c:ae:2b:6f:a5:aa:70:96:1e root@backup
The key's randomart image is:
+--[ RSA 2048 ]-----+ #2048表示加密的位数为2048位
|      o.==.          |
|      o =+.          |
|      . .+           |
|      . . .          |
|      o S            |
|      . o ..         |
|      . E . .o        |
|      = . oo         |
|      o..o.          |
+-----+

```

第二个里程碑: 分发密钥, 注意ssh的端口

```
[root@backup ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub "-p63389 172.16.1.250"
The authenticity of host '[172.16.1.250]:63389 ([172.16.1.250]:63389)' can't be established.
RSA key fingerprint is d3:41:bb:0d:43:88:da:a3:2c:e8:36:91:11:c9:e4:9c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.16.1.250]:63389' (RSA) to the list of known hosts.
root@172.16.1.250's password:
Now try logging into the machine, with "ssh '-p63389 172.16.1.250'", and check in:
```

```
.ssh/authorized_keys    #分发到对端服务器后进行改名
```

to **make** sure we haven't **added extra keys that you weren't** expecting.

说明:

通过 man 手册找到密钥分发的命令格式。

-i 参数指定 公钥文件的存放位置

[use@]表示使用的用户，默认使用当前登陆的用户

-p 指定端口，主要要在双引号之间（通过cat `which ssh-copy-id` 命令脚本内容得知）

```
[root@backup ~]# man ssh-copy-id
Formatting page, please wait...
SSH-COPY-ID(1)                      SSH-COPY-ID(1)
NAME
    ssh-copy-id - install your public key in a remote machine's autho-
    rized_keys
SYNOPSIS
```

第三个里程碑：测试密钥登陆

```
[root@backup ~]# ssh 172.16.1.250 -p 63389
Last login: Wed Oct 18 15:42:05 2017 from 10.0.0.41

[root@test ~]#
```

1.2 如何实现自动创建密钥对，同时分发公钥（编写脚本实现）

脚本内容：

```
[root@m01 ~]# vim /server/scripts/piliang_fenfa.sh
1 #!/bin/bash
2
3 #make key
4 \rm -f /root/.ssh/id_dsa
5 ssh-keygen -t dsa -f /root/.ssh/id_dsa -P "" -q
6
7 #fengfagongyao
8 for ip in 8 31 41
9 do
10 echo ====fenfa key to host 172.16.1.$ip====
11 sshpass -p123456 ssh-copy-id -i /root/.ssh/id_dsa.pub "-o StrictHostKeyChecking=no root@172.
12 echo =====fenfa end=====
13 echo ""
14 done
```

脚本说明:

```
ssh-keygen -t dsa -f /root/.ssh/id_dsa -P "" -q
```

创建密钥, -f指定存放位置, -P 密钥加密的密码 -q 减少信息输出

```
sshpass -p123456 ssh-copy-id -i /root/.ssh/id_dsa.pub "-o StrictHostKeyChecking=no root@172.16.1
```

这里需要安装一个软件 yum install sshpass -y 用来提供中户密码

ssh-copy-id 命令来分发密钥 -i 指定密钥本地存放的路径

-o StrictHostKeyChecking=no 在登陆其他服务器是不选择yes/no

```
for ip in 8 31 41
```

这里使用for循环来对ip地址进行变化。

附录: CentOS 7密钥分发脚本

```
1 #!/bin/bash
2 . /etc/rc.d/init.d/functions
3
4 yum install sshpass -y >/dev/null
5 # 创建密钥
6 \rm ~/.ssh/id_rsa* -f
7 ssh-keygen -t rsa -f ~/.ssh/id_rsa -N "" -q
8 # 分发公钥
9 for ip in 61 21 51 31 41 8 7 9 5 6
10 do
11 sshpass -p123456 ssh-copy-id -o "StrictHostKeyChecking no" -i /root/.ssh/id_rsa.pub 172.16.1
12 if [ $? -eq 0 ];then
13 action "fenfa 172.16.1.$ip" /bin/true
14 else
15 action "fenfa 172.16.1.$ip" /bin/false
16 fi
17 echo ""
18 done
```

本文出自“惨绿少年”，欢迎转载，转载请注明
出处! <http://blog.znix.top>

赞0

如无特殊说明，文章均为本站原创，转载请注明出处

- 转载请注明来源: ssh密钥创建分发(端口号非22)&脚本实现自动创建分发密钥
- 本文永久链接地址: <https://www.nmtui.com/clsn/lx918.html>

该文章由 惨绿少年 发布



惨绿少年Linux www.nmtui.com