Rsync同步

1. **双机ssh互信**

1.在两台机器上生成认证文件，就是ssh互信的认证文件，需要放在用户的home目录中，所以我们需要先创建这个目录，且保证这个目录的全县时755

[root@web-1 ~]# chmod 755 ~/.ssh

[root@web-1 ~]# /usr/bin/ssh-keygen -t rsa ＃下面默认回车就行

[root@web-1 ~]# /usr/bin/ssh-keygen -t dsa

[root@web-2 ~]# chmod 755 ~/.ssh

[root@web-2 ~]# /usr/bin/ssh-keygen -t rsa web1为主机ip，web2为备机ip

[root@web-2 ~]# /usr/bin/ssh-keygen -t dsa

2.必须将每个主机上的公共密钥文件id\_rsa.pub和id\_dsa.pub的内容复制到其他每一个主机的~/.ssh/authorized\_keys文件中。注意，当您第一次使用ssh访问远程主机时，其RSA密钥是未知的，所以提示确认一下，确认完毕后SSH将纪录远程主机的RSA密钥，以后连接该主机将不再做出相应的提示。

[root@web-1 ~]# cat ~/.ssh/id\_rsa.pub >> ~/.ssh/authorized\_keys

[root@web-1 ~]# cat ~/.ssh/id\_dsa.pub >> ~/.ssh/authorized\_keys

[root@web-1 ~]# ssh root@web-2 cat ~/.ssh/id\_rsa.pub >> ~/.ssh/authorized\_keys

[root@web-1 ~]# ssh root@web-2 cat ~/.ssh/id\_dsa.pub >> ~/.ssh/authorized\_keys

3.经过上述两步，在web-1上存了一份完整的key认证文件，我们只需要把这个目录拷贝到web-2这台机器的对应目录里去就可以了，别忘了把authorized\_keys 的权限设置成600

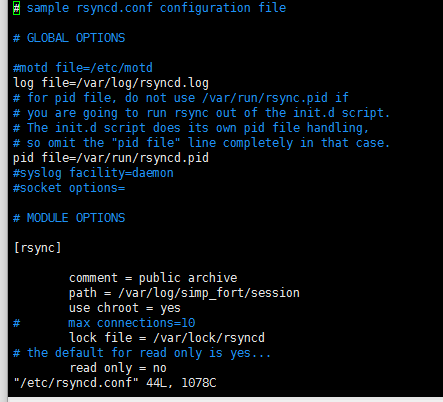
[root@web-1 ~]# scp ~/.ssh/authorized\_keys web-2:~/.ssh/authorized\_keys

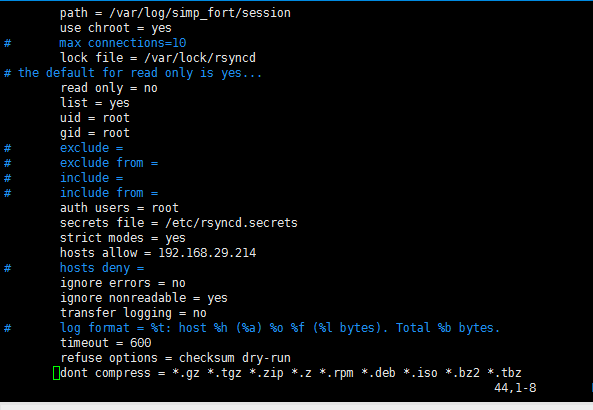
[root@web-1 ~]# chmod 600 ~/.ssh/authorized\_keys

**二．rsync同步配置 server端是备机，client端是主机**

1． 配置server端的/etc/rsyncd.conf文件  
拷贝示例配置文件到/etc目录  
#  cp /usr/share/doc/rsync/examples/rsyncd.conf /etc/

查看rsyncd.conf文件，按需要修改即可





# GLOBAL OPTIONS

#motd file=/etc/motd

log file=/var/log/rsyncd.log

# for pid file, do not use /var/run/rsync.pid if

# you are going to run rsync out of the init.d script.

# The init.d script does its own pid file handling,

# so omit the "pid file" line completely in that case.

pid file=/var/run/rsyncd.pid

#syslog facility=daemon

#socket options=

# MODULE OPTIONS

[rsync]

comment = public archive

path = /var/log/simp\_fort/session

use chroot = yes

# max connections=10

lock file = /var/lock/rsyncd

# the default for read only is yes...

read only = no

list = yes

uid = root

gid = root

# exclude =

# exclude from =

# include =

# include from =

auth users = root

secrets file = /etc/rsyncd.secrets

strict modes = yes

hosts allow = 192.168.29.214 **#备机IP**

# hosts deny =

ignore errors = no

ignore nonreadable = yes

transfer logging = no

# log format = %t: host %h (%a) %o %f (%l bytes). Total %b bytes.

timeout = 600

refuse options = checksum dry-run

dont compress = \*.gz \*.tgz \*.zip \*.z \*.rpm \*.deb \*.iso \*.bz2 \*.tbz

2、在server端创建密码文件/etc/rsyncd.secrets   
# vi /etc/rsyncd.secrets   
  root:m2a1s2u3000 **此处填写username:password**

3、在server端将rsync以守护进程形式启动 **# vi /etc/default/rsync   
RSYNC\_ENABLE=true**

4、启动srync **# /etc/init.d/rsync start**

5、在client端创建密码文件，只填密码即可，**密码要与server端的一致**。  
**# vi /etc/rsyncd.secrets**

**m2a1s2u3000**

**三、添加定时执行**

**# vi /etc/crontab**

**\* \*/1 \* \* \* root /usr/local/bin/sh/change\_rsync.sh**

****