Linux-CentOS7基础配置记录

1. 修改shell提示符

shell提示符由一个环境变量PS1来控制的，我们可以通过修改这个环境变量的值来修改shell提示符的显示。默认的PS1的值是：`[\u@\h \W]\$ = [username@host dir]#`，我现在想要的shell提示符的效果是这样的：`[username@domain dirwithcolor]\$`，那我们应该怎么修改PS1的值呢？我们可以设置：`PS1='[\u@\H \[\033[0;32m\]\W\[\033[0m\]]\$'`，设置好检测效果，正确，如何让这个变化持久化呢？通过修改.bashrc文件，在.bashrc文件中添加：`PS1='[\u@\H \[\033[0;32m\]\W\[\033[0m\]]\$'`，修改后的.bashrc文件如下：

```
[root@ambari.master ~]# cat .bashrc
# .bashrc

# User specific aliases and functions

alias rm='rm -i'
alias cp='cp -i'
alias mv='mv -i'

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi
PS1='[\u@\H \[\033[0;32m\]\W\[\033[0m\]]\$ '
export PS1
[root@ambari.master ~]#
```

实现的提示符效果：

```
[root@ambari.master local]# _
```

2. 修改网络配置

安装成功操作系统之后的第一件事就是系统联网。那么在centos上怎么进行网络配置呢？

- 找到centos中的网络配置文件(有多个网卡是要配置到正确的上网网卡)：**/etc/sysconfig/network-scritps/ifcfg-eno16777736**这个是centos7上的默认上网网卡配置文件位置。
- 修改配置文件

```
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=6098c618-3cf5-4e1d-9172-f8b72e8a0994
DEVICE=eno16777736
ONBOOT=yes
IPADDR=192.168.146.150
GATEWAY=192.168.146.2
NETMASK=255.255.255.0
DNS1=192.168.146.2
~
~
```

- 重启网络：*service network restart*

```
[root@ambari.master network-scripts]# service network restart
Restarting network (via systemctl):                        [  OK  ]
[root@ambari.master network-scripts]# ping 192.168.146.146
PING 192.168.146.146 (192.168.146.146) 56(84) bytes of data.
64 bytes from 192.168.146.146: icmp_seq=1 ttl=64 time=1.81 ms
64 bytes from 192.168.146.146: icmp_seq=2 ttl=64 time=0.528 ms
64 bytes from 192.168.146.146: icmp_seq=3 ttl=64 time=0.908 ms
64 bytes from 192.168.146.146: icmp_seq=4 ttl=64 time=0.982 ms
^C
--- 192.168.146.146 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.528/1.058/1.816/0.471 ms
```

3. 防火墙配置

centos7中的防火墙有firewalld管理，不再由iptables管理。要修改防火墙的配置，我们可以直接修改**/etc/firewalld/**下面的文件，比如我要开放端口8080的tcp访问，那么只需要在**/etc/firewalld/zones/public.xml**文件中添加：

```
<port protocol="tcp" port="8080"/>
```

修改完配置文件之后，切记重启防火墙，否则修改后的配置不会立刻生效：service firewalld restart

关闭防火墙的方式：*systemctl stop firewalld.service*

关闭开机启动：*systemctl disable firewalld.service*

4. 修改主机名

centos或rhel中，有三种定义的主机名：静态的、瞬态的和灵活的。

centos7中提供了hostnamectl的命令行工具用于修改主机名的相关配置。参考

```
[root@ambari.slaver1 ~]# hostnamectl status
   Static hostname: ambari.slaver1
         Icon name: computer-vm
           Chassis: vm
        Machine ID: db83362f94d44175a85110b3e7471890
           Boot ID: 1bc722337fa447d6b8dd162b930ed68c
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-327.el7.x86_64
      Architecture: x86-64
[root@ambari.slaver1 ~]# hostnamectl status --static
ambari.slaver1
[root@ambari.slaver1 ~]# hostnamectl status --transient
ambari.slaver1
[root@ambari.slaver1 ~]# hostnamectl status --pretty

[root@ambari.slaver1 ~]# hostnamectl set-hostname "ambari.slaver2"
[root@ambari.slaver1 ~]# hostnamectl status
   Static hostname: ambari.slaver2
         Icon name: computer-vm
           Chassis: vm
        Machine ID: db83362f94d44175a85110b3e7471890
           Boot ID: 1bc722337fa447d6b8dd162b930ed68c
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-327.el7.x86_64
      Architecture: x86-64
```

5. 创建用户

创建用户组，用户，设置密码，分配sudo权限

```
groupadd hadoop  #创建用户组
useradd  hadoop  #创建用户
passwd   hadoop  #设置密码
#分配sudo权限
执行visudo修改配置文件/etc/sudoers或者直接使用vim命令编辑/etc/sudoers:
```

```
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
hadoop  ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS
```

执行sudo时，免密码配置：

```
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
hadoop  ALL=(ALL)       NOPASSWD:ALL
## Allows members of the 'sys' group to run networking, software,
```

6. ssh免密码登录配置(用户:hadoop)	HostName

集群环境：

IP	HostName
192.168.146.150	ambari.master
192.168.146.151	ambari.slaver1
192.168.146.152	ambari.slaver2
192.168.146.153	ambari.slaver3
192.168.146.154	ambari.slaver4

1. 配置每台机器的hosts文件，让每台机器可以通过hostname互相访问。

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.146.150 ambari.master
192.168.146.151 ambari.slaver1
192.168.146.152 ambari.slaver2
192.168.146.153 ambari.slaver3
192.168.146.154 ambari.slaver4
~
```

2. 首先配置单台机器免密码登录，在**ambari.master**上切换到hadoop用户，并将工作目录切换到hadoop的家目录下

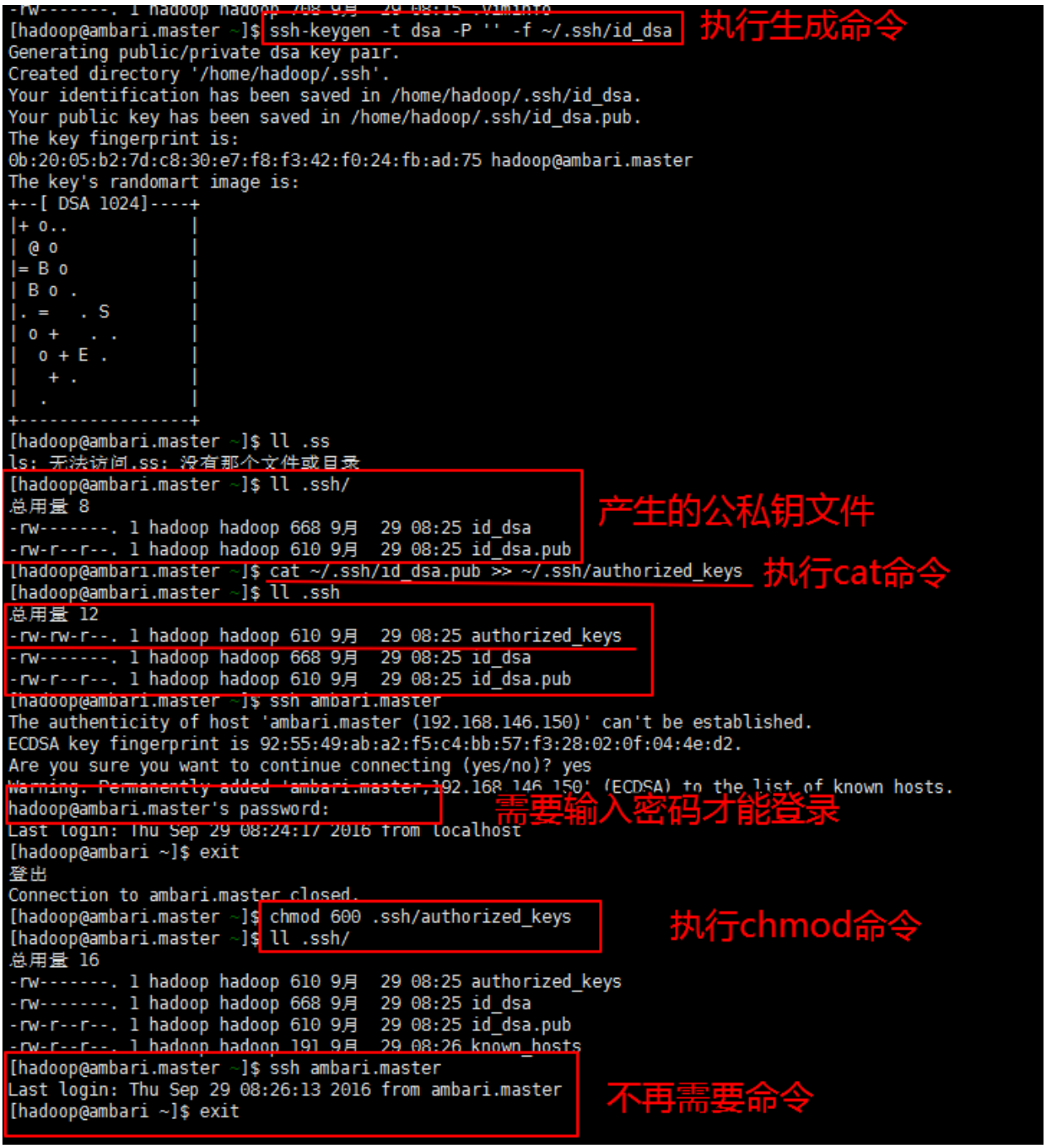
   我们这里选择dsa加密方式来执行ssh登录认证

   执行命令：**ssh-keygen -t dsa -P '' -f ~/.ssh/id_dsa**

   如果不存在ssh-keygen这个命令，请安装ssh命令行工具，执行命令之后再家目录的.ssh目录中会生成两个文件：id_dsa和id_dsa.pub

   执行命令：**cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys**，cat命令执行中的authorized_keys这个文件名是固定的，这个名字必须和**/etc/ssh/sshd_config**这个ssh配置文件中的**AuthorizedKeysFile**属性的值一样，否则上述cat命令执行之后将没有作用。

   在网上的大部分文章说到这里就会结束了，就会认为已经可以ssh免密码登录，然而，当我输入**ssh ambari.master**登录本机时，结果却是不行的，依然要输入密码才能登录，也就是我们的配置没有用。这个因为还缺少一个步骤，必须执行命令：**chmod 600 ~/.ssh/authorized_keys**，再次输入ssh ambari.master成功登录，不再需要输入密码。执行流程截图如下：



使用**rsa**加密方式来配置ssh免密码登录，跟上面的步骤一样的，**而且并不需要修改/etc/ssh/sshd_config/配置文件(网上有说要修改这个配置文件的)。**

/etc/ssh/sshd_config配置文件的部分：

```
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

这里并不需要去掉#号

ssh认证查找的配置文件

3. 单机ssh免密码登录配置成功之后，如法炮制，在其他机器上相应的配置hadoop用户的免密码登录。
4. 将**ambari.master**机器上的**authorized_keys**文件拷贝到ambari.slaver机器上：

   在 ambari.slaver1 上 执 行 命 令 ： **scp hadoop@ambari.master:~/.ssh/authorized_keys ~/.ssh/master_authorized_keys**，将authorized_keys文件拷贝到slaver1上

   再在ambari.slaver1上执行命令：**cat .ssh/master_authorized_keys >> .ssh/authorized_keys**

   在ambari.master上测试ssh ambari.slaver1，免密码登录成功。

```
[hadoop@ambari.slaver1 ~]$ scp hadoop@ambari.master:~/.ssh/authorized_keys ~/.ssh/master_authorized_keys
The authenticity of host 'ambari.master (192.168.146.150)' can't be established.
ECDSA key fingerprint is 92:55:49:ab:a2:f5:c4:bb:57:f3:28:02:0f:04:4e:d2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ambari.master,192.168.146.150' (ECDSA) to the list of known hosts.
hadoop@ambari.master's password:
authorized_keys                                                100%  402     0.4KB/s   00:00
[hadoop@ambari.slaver1 ~]$ ll .ssh/
总用量 20
-rw-------. 1 hadoop hadoop  403 9月  29 19:47 authorized_keys
-rw-------. 1 hadoop hadoop 1679 9月  29 19:47 id_rsa
-rw-r--r--. 1 hadoop hadoop  403 9月  29 19:47 id_rsa.pub
-rw-r--r--. 1 hadoop hadoop  383 9月  29 19:55 known_hosts
-rw-------. 1 hadoop hadoop  402 9月  29 19:55 master_authorized_keys
[hadoop@ambari.slaver1 ~]$ cat .ssh/master_authorized_keys >> .ssh/authorized_keys
```

```
[hadoop@ambari.master ~]$ ssh ambari.slaver1
The authenticity of host 'ambari.slaver1 (192.168.146.151)' can't be established.
ECDSA key fingerprint is 7c:ba:64:01:e6:7f:25:f0:ac:65:a1:e9:1c:32:2e:12.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ambari.slaver1,192.168.146.151' (ECDSA) to the list of known hosts.
Last login: Thu Sep 29 19:48:43 2016 from ambari.slaver1
[hadoop@ambari ~]$ exit
登出
Connection to ambari.slaver1 closed.
```

5. 如法炮制，将**ambari.slaver1**上的**authorized_keys**文件拷贝到**ambari.slaver2**上，依次类推，直到将ambari.slaver3上的authorized_keys文件拷贝到ambari.slaver4上，完成这些步骤之后，ambari.slaver4上的authorized_keys文件将包含集群中所有机器的公钥。
6. 将ambari.slaver4机器上的authorized_keys文件再拷贝到ambari.master、ambari.slaver1、ambari.slaver2和ambari.slaver3上面并覆盖之前的authorized_keys文件，至此集群中各个机器之间的ssh免密码登录完成。
7. **可能出现的问题：**在执行scp命令的时候，可能遇到不能成功拷贝的情况，这是因为hadoop用户对.ssh目录没有操作权限的原因，可以通过赋予权限解决。

7.ip NTP时间同步服务器配置

环境

ip	描述
192.168.146.100	集群中的ntpd服务器，用于与外部公共ntpd服务同步标准时间
192.168.146.170	ntpd客户端，与ntpd服务器同步时间
192.168.146.171	ntpd客户端，与ntpd服务器同步时间
192.168.146.172	ntpd客户端，与ntpd服务器同步时间
192.168.146.173	ntpd客户端，与ntpd服务器同步时间
192.168.146.174	ntpd客户端，与ntpd服务器同步时间

配置ntpd服务器(192.168.146.100)

1. 检查ntpd服务是否安装
   使用rpm命令检查ntp包是否安装：**rpm -qa ntp**
   如果已经安装则略过此步，否则使用yum进行安装：**yum install ntp**
2. 配置ntpd服务器
   配置前先使用命令：**ntpdate -u cn.pool.ntp.org**(中国标准时间服务地址) 同步本机时间
   修改ntp的配置文件：

```
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default nomodify notrap nopeer noquery

# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
# 修改为我们自己的局域网ip
# 我们配置的ntpd服务器如果不加限制也是可以作为全局的ntpd服务器让任何人任何网络来访问我们的服务器同步时间的,但我们现在并不想作为公共服务让别人访问,所以我们要加限制只让我们控制的局域网内ip来访问
# 现在我的局域网网关就是192.168.146.2
restrict 192.168.146.2 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst

# 可以为我们自己的ntpd服务器指定多个外部标准时间服务地址,按顺序获取
server 2.cn.pool.ntp.org  #优先级最高
server 1.asia.pool.ntp.org
server 2.asia.pool.ntp.org

#broadcast 192.168.1.255 autokey        # broadcast server
#broadcastclient                        # broadcast client
#broadcast 224.0.1.1 autokey            # multicast server
#multicastclient 224.0.1.1              # multicast client
#manycastserver 239.255.254.254         # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# 允许上层时间服务器主动修改本机时间
# 注意这里的restrict和上面restrict的区别(这里多了一个noquery)
restrict 2.cn.pool.ntp.org nomodify notrap noquery
restrict 1.asia.pool.ntp.org nomodify notrap noquery
restrict 2.asia.pool.ntp.org nomodify notrap noquery

# 不能同步上层服务器的标准时间时,取本机的时间作为标准时间
server 127.127.1.0  # 注意这里的值不是127.0.0.1
fudge 127.127.1.0 stratum 10
# Enable public key cryptography.

#crypto
```

```
includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

# Disable the monitoring facility to prevent amplification attacks using ntpdc
# monlist command when default restrict does not include the noquery flag. See
# CVE-2013-5211 for more details.
# Note: Monitoring will not be disabled with the limited restriction flag.
disable monitor
```

3. 启动ntpd服务：**systemctl start ntpd**
4. 查看ntpd服务器，同时显示客户端和每个服务器的关系：**ntpq -p**

```
[root@localhost ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*news.neu.edu.cn 202.118.1.47     2 u   46   64  177   52.119    7.550   8.543
+bera.learn.ac.l 62.201.225.9     3 u   45   64  177  306.029  -58.943  10.722
+balthasar.gimas 210.173.160.57   3 u   49   64   77  144.217  -41.092   9.826
 LOCAL(0)        .LOCL.          10 l    -   64    0    0.000    0.000   0.000
```

5. 查看同步结果：

```
[root@localhost ~]# ntpstat
synchronised to NTP server (202.118.1.81) at stratum 3
   time correct to within 7975 ms
   polling server every 64 s
```

配置ntpd客户端(192.168.146.170~192.168.146.174)

1. 其他步骤一样
2. 修改配置文件

```
# For more information about this file, see the man pages
   # ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

   driftfile /var/lib/ntp/drift

   # Permit time synchronization with our time source, but do not
   # permit the source to query or modify the service on this system.
   restrict default nomodify notrap nopeer noquery

   # Permit all access over the loopback interface.  This could
   # be tightened as well, but to do so would effect some of
   # the administrative functions.
   restrict 127.0.0.1
   restrict ::1

   # Hosts on local network are less restricted.
   #restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
   # 这里是上面配置的ntpd服务器的ip地址
   server 192.168.146.100
   restrict 192.168.146.100 mask 255.255.255.0 nomodify notrap

   # Use public servers from the pool.ntp.org project.
   # Please consider joining the pool (http://www.pool.ntp.org/join.html).
   #server 0.centos.pool.ntp.org iburst
   #server 1.centos.pool.ntp.org iburst
   #server 2.centos.pool.ntp.org iburst
   #server 3.centos.pool.ntp.org iburst
```

```
#broadcast 192.168.1.255 autokey        # broadcast server
#broadcastclient                        # broadcast client
#broadcast 224.0.1.1 autokey            # multicast server
#multicastclient 224.0.1.1              # multicast client
#manycastserver 239.255.254.254         # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# 不能同步上层服务器的标准时间时,取本机的时间作为标准时间
server 127.127.1.0  # 注意这里的值不是127.0.0.1
fudge 127.127.1.0 stratum 10
# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

# Disable the monitoring facility to prevent amplification attacks using ntpdc
# monlist command when default restrict does not include the noquery flag. See
# CVE-2013-5211 for more details.
# Note: Monitoring will not be disabled with the limited restriction flag.
disable monitor
```

3. 记住关闭ntpd服务器的防火墙或者是打开ntpd服务的端口，否则不能自动同步