**安装NTP包**

检查是否安装了ntp相关包。如果没有安装ntp相关包，使用rpm或yum安装，安装也非常简单方便。

[root@localhost ~]#  rpm -qa | grep ntp

ntpdate-4.2.6p5-1.el6.x86\_64

fontpackages-filesystem-1.41-1.1.el6.noarch

ntp-4.2.6p5-1.el6.x86\_64

**NTP的配置**

**A： 配置/etc/ntp.conf**

NTP Server的主要配置文件为/etc/ntp.conf ,没有修改过的ntp.conf文件内容如下所示，配置选项都有相关注释信息（Linux 版本为Red Hat Enterprise Linux Server release 6.6 ）

[root@localhost ~]# more /etc/ntp.conf

# 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 kod nomodify notrap nopeer noquery

restrict -6 default kod 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 -6 ::1

# Hosts on local network are less restricted.

#restrict 192.168.1.0 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.rhel.pool.ntp.org iburst

server 1.rhel.pool.ntp.org iburst

server 2.rhel.pool.ntp.org iburst

server 3.rhel.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

# 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

**各个选项信息：**

#系统时间与BIOS事件的偏差记录

driftfile /etc/ntp/drift

restrict 控制相关权限。

语法为： restrict IP地址 mask 子网掩码 参数

其中IP地址也可以是default ，default 就是指所有的IP

参数有以下几个：

ignore  ：关闭所有的 NTP 联机服务

nomodify：客户端不能更改服务端的时间参数，但是客户端可以通过服务端进行网络校时。

notrust ：客户端除非通过认证，否则该客户端来源将被视为不信任子网

noquery ：不提供客户端的时间查询：用户端不能使用ntpq，ntpc等命令来查询ntp服务器

notrap ：不提供trap远端登陆：拒绝为匹配的主机提供模式 6 控制消息陷阱服务。陷阱服务是 ntpdq 控制消息协议的子系统，用于远程事件日志记录程序。

nopeer ：用于阻止主机尝试与服务器对等，并允许欺诈性服务器控制时钟

kod ： 访问违规时发送 KoD 包。

restrict -6 表示IPV6地址的权限设置。

**1：设定NTP主机来源（其中prefer表示优先主机），192.168.7.49是本地的NTP服务器，所以优先指定从该主机同步时间。**

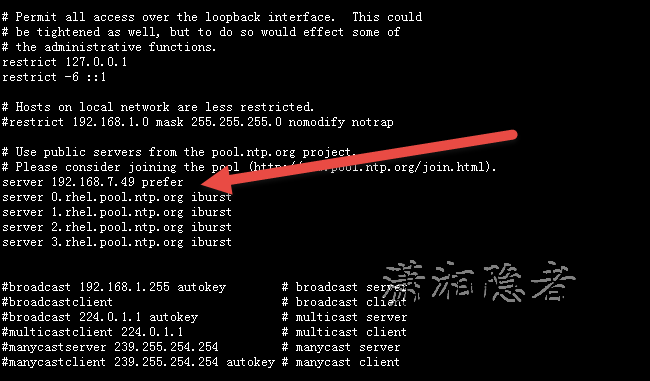
server 192.168.7.49 prefer

server 0.rhel.pool.ntp.org iburst

server 1.rhel.pool.ntp.org iburst

server 2.rhel.pool.ntp.org iburst

server 3.rhel.pool.ntp.org iburst

[](http://images0.cnblogs.com/blog/73542/201508/201228383006536.png)

**2：限制你允许的这些服务器的访问类型,在这个例子中的服务器是不容许修改运行时配置或查询您的Linux NTP服务器**

restrict 192.168.0.0 mask 255.255.255.0 notrust nomodify notrap

在上例中，掩码地址扩展为255，因此从192.168.0.1-192.168.0.254的服务器都可以使用我们的NTP服务器来同步时间

#此时表示限制向从192.168.0.1-192.168.0.254这些IP段的服务器提供NTP服务。

restrict 192.168.0.0 mask 255.255.255.0 notrust nomodify notrap noquery

#设置默认策略为允许任何主机进行时间同步

restrict default ignore

**3：确保localhost（这个常用的IP地址用来指Linux服务器本身）有足够权限.使用没有任何限制关键词的语法：**

restrict 127.0.0.1

restrict -6 ::1

**B：配置/etc/ntp/stpe-tickers文件**

修改/etc/ntp/stpe-tickers文件，内容如下（当ntpd服务启动时，会自动与该文件中记录的上层NTP服务进行时间校对）

[root@localhost ntp]# more /etc/ntp/step-tickers

# List of servers used for initial synchronization.

[root@localhost ntp]# vi /etc/ntp/step-tickers

# List of servers used for initial synchronization.

server 192.168.7.49 prefer

server 0.rhel.pool.ntp.org

server 1.rhel.pool.ntp.org

server 2.rhel.pool.ntp.org

server 3.rhel.pool.ntp.org

关于ntp.conf and step-tickers区别：

step-tickers is used by ntpdate where as ntp.conf is the configuration file for the ntpd daemon. ntpdate is initially run to set the clock before ntpd to make sure time is within 1000 sec. ntp will not run if the time difference between the server and client by more then 1000 sec ( or there about). The start up script will read step-tickers for servers to be polled by ntpdate.

**C：配置/etc/sysconfig/ntpd文件**

ntp服务，默认只会同步系统时间。如果想要让ntp同时同步硬件时间，可以设置/etc/sysconfig/ntpd文件，在/etc/sysconfig/ntpd文件中，添加 SYNC\_HWCLOCK=yes 这样，就可以让硬件时间与系统时间一起同步。

#允许BIOS与系统时间同步，也可以通过hwclock -w 命令

SYNC\_HWCLOCK=yes

**IPTABLES 配置**

由于NTP服务需要使用到UDP端口号123，所以当系统的防火墙（Iptables）启动的情况下，必须开放UDP端口号123。

[root@localhost ~]#  /etc/init.d/iptables status

Table: filter

Chain INPUT (policy ACCEPT)

num  target     prot opt source               destination

1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0

3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0

4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22

5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

num  target     prot opt source               destination

1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

num  target     prot opt source               destination

[root@localhost ~]# /sbin/iptables -I INPUT -p udp --dport 123 -j ACCEPT

[root@localhost ~]#  /etc/init.d/iptables status

Table: filter

Chain INPUT (policy ACCEPT)

num  target     prot opt source               destination

1    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:123

2    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

3    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0

4    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0

5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22

6    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

num  target     prot opt source               destination

1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

num  target     prot opt source               destination

[root@localhost ~]#

[](http://images0.cnblogs.com/blog/73542/201508/201228402221325.png)

如果防火墙没有开放UDP端口号123，有可能出现下面情况。

[root@localhost ~]# /usr/sbin/ntpq -c rv | grep stratum

stratum=16, precision=-24, rootdelay=0.000, rootdisp=3.525, refid=INIT,

[root@localhost~]#

A stratum level of 16 indicates that NTP is not synchronizing correctly.If a stratum level of 16 is detected, wait 15 minutes and issue the command again. It may take this long for the NTP server to stabilize.If NTP continues to detect a stratum level of 16, verify that the NTP port (UDP Port 123) is open on all firewalls between the cluster and the remote machine you are attempting to synchronize to.

**启动NTP服务**

[root@localhost ~]# service ntpd status

ntpd is stopped

[root@localhost ~]# service ntpd start

Starting ntpd: [  OK  ]

[root@localhost ~]#

service ntpd status      #查看ntpd服务状态

service ntpd start           #启动ntpd服务

service ntpd stop            #停止ntpd服务

service ntpd restart         #重启ntpd服务

检查ntp服务是否开机启动，将其设置为开机启动。

[root@localhost ~]# chkconfig --list ntpd

ntpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off

[root@localhost ~]# runlevel

N 3

[root@localhost ~]# chkconfig ntpd on #在运行级别2、3、4、5上设置为自动运行

[root@localhost ~]# chkconfig --list ntpd

ntpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

[root@localhost ~]#

如果要设置在运行级别上自动运行，可以使用下面命令

chkconfig --level 345 ntpd on

可以用下面命令检测NTP服务是否运行

[root@localhost ~]# pgrep ntpd

2639

2641

[root@localhost ~]# netstat -tlunp | grep ntp   #如果看到123端口，说明ntp服务成功启动。

udp        0      0 192.168.7.224:123           0.0.0.0:\*                               2639/ntpd

udp        0      0 127.0.0.1:123               0.0.0.0:\*                               2639/ntpd

udp        0      0 0.0.0.0:123                 0.0.0.0:\*                               2639/ntpd

udp        0      0 fe80::250:56ff:feb3:b5:123  :::\*                                    2639/ntpd

udp        0      0 ::1:123                     :::\*                                    2639/ntpd

udp        0      0 :::123                      :::\*                                    2639/ntpd

[root@localhost ~]#

[](http://images0.cnblogs.com/blog/73542/201508/201228426912512.png)

**查看ntp服务器有无和上层ntp连通**

[root@localhost ~]# ntpstat

synchronised to NTP server (192.168.7.49) at stratum 6

   time correct to within 440 ms

   polling server every 128 s

[root@localhost ~]#

**查看ntp服务器与上层ntp的状态**

[root@localhost ~]# ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter

==============================================================================

192.168.7.49    192.168.7.50     5 u   13   64    3    5.853  1137178   2.696

[root@localhost ~]# ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter

==============================================================================

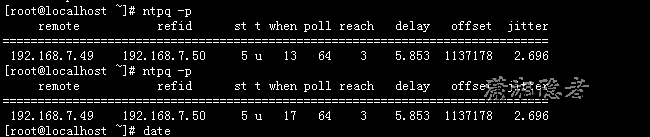
192.168.7.49    192.168.7.50     5 u   17   64    3    5.853  1137178   2.696

[root@localhost ~]# ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter

==============================================================================

192.168.7.49    192.168.7.50     5 u    1   64    1    0.937   -9.570   0.000

[](http://images0.cnblogs.com/blog/73542/201508/201228444419312.png)

remote   - 本机和上层ntp的ip或主机名，“+”表示优先，“\*”表示次优先

refid    - 参考上一层ntp主机地址

st       - stratum阶层

when     - 多少秒前曾经同步过时间

poll     - 下次更新在多少秒后

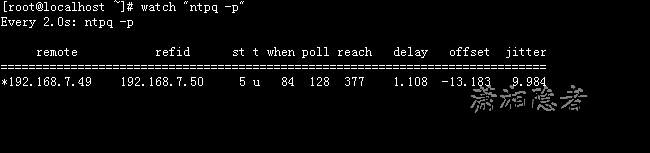
reach    - 已经向上层ntp服务器要求更新的次数

delay    - 网络延迟

offset   - 时间补偿

jitter   - 系统时间与bios时间差

要查看 ntpd 进程的状态，请运行以下命令，按 Ctrl+C 停止查看进程。

[](http://images0.cnblogs.com/blog/73542/201508/201228454723729.png)

第一列中的字符指示源的质量。星号 ( \* ) 表示该源是当前引用。

remote 列出源的 IP 地址或主机名。

when   指出从轮询源开始已过去的时间（秒）。

poll   指出轮询间隔时间。该值会根据本地时钟的精度相应增加。

reach  是一个八进制数字，指出源的可存取性。值 377 表示源已应答了前八个连续轮询。

offset 是源时钟与本地时钟的时间差（毫秒）。

**ntpd、ntpdate的区别**

下面是网上关于ntpd与ntpdate区别的相关资料。如下所示所示：

使用之前得弄清楚一个问题，ntpd与ntpdate在更新时间时有什么区别。ntpd不仅仅是时间同步服务器，它还可以做客户端与标准时间服务器进行同步时间，而且是平滑同步，并非ntpdate立即同步，在生产环境中慎用ntpdate，也正如此两者不可同时运行。

时钟的跃变，对于某些程序会导致很严重的问题。许多应用程序依赖连续的时钟——毕竟，这是一项常见的假定，即，取得的时间是线性的，一些操作，例如数据库事务，通常会地依赖这样的事实：时间不会往回跳跃。不幸的是，ntpdate调整时间的方式就是我们所说的”跃变“：在获得一个时间之后，ntpdate使用settimeofday(2)设置系统时间，这有几个非常明显的问题：

第一，这样做不安全。ntpdate的设置依赖于ntp服务器的安全性，攻击者可以利用一些软件设计上的缺陷，拿下ntp服务器并令与其同步的服务器执行某些消耗性的任务。由于ntpdate采用的方式是跳变，跟随它的服务器无法知道是否发生了异常（时间不一样的时候，唯一的办法是以服务器为准）。

第二，这样做不精确。一旦ntp服务器宕机，跟随它的服务器也就会无法同步时间。与此不同，ntpd不仅能够校准计算机的时间，而且能够校准计算机的时钟。

第三，这样做不够优雅。由于是跳变，而不是使时间变快或变慢，依赖时序的程序会出错（例如，如果ntpdate发现你的时间快了，则可能会经历两个相同的时刻，对某些应用而言，这是致命的）。因而，唯一一个可以令时间发生跳变的点，是计算机刚刚启动，但还没有启动很多服务的那个时候。其余的时候，理想的做法是使用ntpd来校准时钟，而不是调整计算机时钟上的时间。

NTPD 在和时间服务器的同步过程中，会把 BIOS 计时器的振荡频率偏差——或者说 Local Clock 的自然漂移(drift)——记录下来。这样即使网络有问题，本机仍然能维持一个相当精确的走时。