How to troubleshoot NTP issues

SOLUTION VERIFICADA - Actualizado18 de Mayo de 2015 a las 11:42 - English

Medio Ambiente

- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Network time Protocol (NTP)

Cuestión

- How to debug NTP issues
- NTP troubleshooting techniques for accurate and reliable time sync.
- How to check if NTP clients are synchronizing correctly with NTP servers
- What is the purpose of `ntpq` utility and meaning of different paramenters in `ntpq` output
- How to verify whether NTP client and Server configuration is working properly
- How to fix system clock time drift or deviation issue using NTP

Resolución

- The Network Time Protocol (NTP) enables the accurate dissemination of time and date information in order to keep the time clocks on networked computer systems synchronized to a common reference over the network or the Internet.

- In Linux systems, NTP is implemented by a daemon running in user space.

- Ensure that NTP traffic is not blocked by any firewall.

- By default, in Red Hat Enterprise Linux, ntpd uses port 123. NTP traffic consists of UDP packets, hence, port 123 should be open for UDP.

- To use a Network Time Protocol (NTP) client or server on your system you need to have access to port 123 both incoming and outgoing between any client and the server that it is communicating with.

- The startup script for the NTP service should create the firewall holes on your machine automatically. One will have to ensure that all points along the route between the client and the server will allow traffic on port 123.

- After the ntp service is started, the clock selection process takes some time, and it needs 20-30 minutes of exchanging packets with the ntp servers, until the final ntp source is selected.

How ntpq works

```
 ntpq
 ntpq> peers
 remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*time.rhl.       8.16.24.15       2 u  972 1024  377   28.066   -0.181   4.126
+dc1.riu.net     15.15.26.3       3 u  467 1024  377  141.664  -23.531   0.140
mighty.poclabs. .STEP.          16 u    - 1024    0    0.000    0.000   0.000
```

```
*time.rhl.       8.16.24.13       2 u  972 1024  377   28.066   -0.181   4.126
+dc1.riu.net     15.15.26.3       3 u  467 1024  377  141.664  -23.531   0.140
mighty.poclabs. .STEP.          16 u    - 1024    0    0.000    0.000   0.000
LOCAL(0)        .LOCL.          10 l   32   64  377    0.000    0.000   0.001
```

- The "peers" command displays a list showing the DNS name or IP address for each association along with selected status and statistics variables.

- The first character in each line is the tally code, which shows which associations are candidates to set the system clock and of these which one is the system peer.

- During the clock selection process the refid will be .INIT. and the st (stratum) is set to 16.
  The * indicates that this particular association is the chosen ntp source
  The + indicates that this peer is a candidate
  An empty space indicates that the peer unreachable and therefore rejected (stratum 16)

- If no NTP servers get selected, get the output of the following commands for further debugging:

```
ntpq> as
ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 29581  9624   yes   yes  none  sys.peer   reachable  1
  2 29582  9014   yes   yes  none  candidat   reachable  1
  4 29583  8000   yes   yes  none    reject
  5 29584  9024   yes   yes  none    reject   reachable  2
```

- The "as" command displays a list of associations and association identifiers. Note the condition column, which reflects the tally code.

- The associations shown above, correspond to the entries shown in the peer command. Use the "assID" for the following command:

```
ntpq> rv 29583
assID=62236 status=9014 reach, conf, 1 event, event_reach,
srcadr=192.168.23.1, srcport=123, dstadr=192.168.247.11, dstport=123,
leap=00, stratum=3, precision=-6, rootdelay=218.750,
rootdispersion=1381.516, refid=24.1.4.14, reach=377, unreach=0,
hmode=3, pmode=4, hpoll=10, ppoll=10, flash=400 peer_dist, keyid=0,
ttl=0, offset=-29.750, delay=0.316, dispersion=30.400, jitter=1.136,
reftime=d1e4505b.d456f5b0  Thu, Aug  4 2011  0:55:23.829,
org=d1e4c793.e477ba4b  Thu, Aug  4 2011  9:24:03.892,
rec=d1e4c793.ec1fc3ac  Thu, Aug  4 2011  9:24:03.922,
xmt=d1e4c793.ec0b133c  Thu, Aug  4 2011  9:24:03.922,
filtdelay=     0.32    0.40    0.33    0.45    0.42    0.42    0.33    0.38,
filtoffset=  -29.75  -30.89  -29.97  -30.11  -30.15  -29.20  -30.25  -30.36,
filtdisp=     15.63   31.00   46.38   61.75   77.14   92.52  107.91  123.28
```

- To understand the above output of `ntpq> rv assID` refer article What is meaning of different values in " ntpq> rv assID " output .

- From the NTP source, a definition of how peer_distance is measured as this is the most regular error we see:
  NTP Debugging Techniques

- Another useful aid is to run ntpdate with the -d switch:

```
ntpdate -d time.rhl.com
```

- Another useful aid is to run ntpdate with the -d switch.

```
ntpdate -d time.rhl.com
17 Oct 00:20:51 ntpdate[26388]: ntpdate 4.2.2p1@1.1570-o Thu Nov 26 11:34:35 UTC 2009
(1)
 Looking for host time.rhl.com and service ntp
 host found : time.rhl.com
 transmit(66.125.13.54)
 receive(66.125.13.54)
 transmit(66.125.13.54)
 receive(66.125.13.54)
 transmit(66.125.13.54)
 receive(66.125.13.54)
 transmit(66.125.13.54)
 receive(66.125.13.54)
 transmit(66.125.13.54)
 server 66.125.13.54, port 123
 stratum 1, precision -16, leap 00, trust 000
 refid [CDMA], delay 0.32297, dispersion 0.00040
 transmitted 4, in filter 4
 reference time:    d245a5fe.2fdfe09b  Mon, Oct 17 2011  0:20:38.187
 originate timestamp: d245a60c.e2117d1e  Mon, Oct 17 2011  0:20:52.883
 transmit timestamp:  d245a60c.b9c9b413  Mon, Oct 17 2011  0:20:52.725
 filter delay:  0.32361  0.32382  0.32297  0.32619
 0.00000  0.00000  0.00000  0.00000
 filter offset: 0.003892 0.004005 0.003607 0.004972
 0.000000 0.000000 0.000000 0.000000
 delay 0.32297, dispersion 0.00040
 offset 0.003607
17 Oct 00:20:53 ntpdate[26388]: adjust time server 66.187.233.4 offset 0.003607 sec
```

Keyfile Verification

- If you are using secure NTP, your clients will need a keyfile. Occasionally, when setting up a new host, files can be corrupted in copy. Keyfiles are particularly sensitive because any minor flaw can cause the key to be corrupted, denying you access to your NTP service. Best practice here would be to verify the keyfile each time it is copied.

- The easiest method to check for this is to verify the MD5 hash of the original against the copy. This can be done using the following command:

```
md5sum <original_keyfile> > /tmp/origkey.txt
md5sum <keyfile_copy> > /tmp/keycopy.txt
```

- You can verify the hashes manually, or use the 'diff' command to verify the two '.txt' files

```
diff origkey.txt keycopy.txt
```

- How to Configure Authenticated NTP Using Autokey

- How To Configure Authenticated NTP Using Symmetric Keys

Timing issues on virtualized guests

- NTP sometimes fails to synchronize with any NTP time source, and all of the above outputs don't seem to indicate a problem. In that case, check if the system is running on virtual hardware, and use the following articles for resolution:

NTP sometimes fails to synchronize with any NTP time source, and all of the above outputs don't seem to indicate a problem. In that case, check if the system is running on virtual hardware, and use the following articles for resolution:

KVM : Inaccurate time keeping in KVM RHEL guests under 5.4

Xen : XEN VM's unable to synchronise time with NTP on RHEL5.4

RHEV : How to prevent time drift and keep accurate time of Red Hat Enterprise Linux running on Red Hat Enterprise Virtualization?

Hyper-V : Time drift issues in Red Hat Enterprise Linux guests in Microsoft Windows Hyper-V virtualization environment

VMware : VMWare guest time runs fast and jumps ahead on RHEL4 or RHEL5

VMware : How to Tell if VMWare Time Sync is Disabled?

Additional References

- RHEL6 NTP product documentation

- RHEL5 NTP product documentation

Procedimientos para el Diagnóstico

- Is affected NTP client physical or virtual machine and is it running on RHEL?
- Are NTP servers running on RHEL and are they physical or virtual machine?
- Capture updated sosreport , so that we can check version details, configuration and log files for sanity check.
- Collect output of below commands;

```
ntpq
  ntpq> peers
  ntpq> as
  ntpq> rv <asID>   <<--(where <asID> should be replace with the number that is showed
in the previous output, second column)
```

- If there seems to be networking issue then tcpdump file `port123.cap` can be captured using below command for particular time duration of 20-25 minutes.

```
tcpdump -s0 port 123 -vvv -i <NIC> -w port123.cap
```

- You can also confirm debug log about what is going on with following additional settings in /etc/ntp.conf on RHEL6.

```
tinker panic 100000
```

/etc/ntp.conf on RHEL6:

```
tinker panic 100000
enable stats
statsdir /var/log/ntpstats/
statistics clockstats loopstats peerstats sysstats rawstats
filegen clockstats file clockstats type day enable
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen sysstats file sysstats type day enable
filegen rawstats file rawstats type day enable
```