Clock Synchronization

It is important that the system clocks in the Linux workstations of the RFPK Software Team be closely synchronized to the clock in the server which hosts the CVS repository, or to the time standard to which that server is synchronized, because the CVS application, as well as the backup process which runs on the same server, depend for their proper operation on the comparison of timestamps of files residing on different.machines. This tutorial explains how to configure your workstation so that it stays synchronized within a fraction of a second with that server.

Table of Contents

Network Time Protocol

The Network Time Protocol (NTP) allows computers connected to the Internet to keep their clocks synchronized. Certain host computers equipped with accurate clocks make the NTP service available to other, less well endowed, hosts. A machine with an accurate clock which is offering an NTP service is known as a *level one* NTP server. Other machines, which may not be equipped with accurate clocks but which nevertheless have accurate time due to the fact that they are synchronized to one or more *level one* NTP servers, can offer an NTP service over the Internet as *level two* NTP servers, and so on.

The host bigben.cac.washington.edu is a *level one* NTP server equipped with a clock that gets its time from GPS satellites. The RFPK CVS server is synchronized to bigben and several other *level one* NTP servers. This document describes the way to configure your RedHat Linux 8.0 workstation to synchronize to to one or the other of these servers.

If your machine is on the LAN behind the SPK firewall, it can be synchronized to the the CVS server, which is located on the LAN. If it is not on the LAN, it can be synchronized to bigben.cac.washington.edu or to some other external time server.

Defining Timeserver

The following instructions will be easier to follow if we define a system alias for the time server we are going to use. This will also allow us to move machines from one network to another, only having to change the alias definition in a single file rather than references in a number of files.

The changes will be made to the `/etc/hosts` file. There are the following cases:

i. Your machine is outside the firewall. Add the following line to `/etc/hosts`:

```
140.142.16.34    bigben.cac.washington.edu   timeserver
```

ii. Your machine is behind the firewall and there is already an entry for the CVS server (IP address 192.168.1.2) in your `/etc/hosts` file. In this case, simply add *timeserver* to the end of that line.

iii. Your machine is behind the firewall, but there is no entry for the CVS server. Add the following line to `/etc/hosts`

```
192.168.1.2 timeserver
```

iv. The machine is one of the computational (not frontend) nodes in the cluster topology that contains a frontend. The entry in `/etc/hosts` should look like this

```
192.168.3.1    timeserver frontend
```

Configuring RFPK Software Development Clients

This section covers the configuration of RFPK software development workstations and the cspk server. We must edit several configuration files. To do this, you will need root privilege.

```
su -
cd /etc
```

Edit `ntp.conf` with your favorite editor, setting the default behavior to *nomodify* rather than *ignore*.

```
restrict default ignore

 should be changed to

restrict default nomodify
```

Next specify that timesever is a trusted time server by making this change:

```
 after

# restrict mytrustedtimeserverip mask 255.255.255.255 nomodify notap noquery
# server mytrustedtimeserverip

 insert the following pair of lines

restrict timeserver nomodify notrap noquery
server timeserver
```

Save the file, after you have made your changes.

Finally, we need to recreate the `/etc/ntp/step-tickers` file, which is a list of time servers queried by your system when it boots.

```
cd /etc/ntp
echo timeserver > step-tickers
echo time.nist.gov >> step-tickers
```

Daemon Setup

We need to start the ntp daemon, if it is not already running, and make sure that it is started automatically whenever the system reboots. As root, input the following commands:

```
/etc/rc.d/init.d/ntpd restart
/sbin/chkconfig --level 2345 ntpd on
```

You should now check that your ntp daemon is working. Wait a few minutes after restarting ntpd, then issue this command:

```
/usr/sbin/ntpq -p
```

You should see output that looks something like this:

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        LOCAL(0)        10 l   63   64  377    0.000    0.000   0.008
*whitechuck.rfpk bigben.cac.wash  2 u  192  256  377    0.684    0.075   0.024
```

If delay, offset, and jitter are not small numbers, the clock has not synchronized, which may indicate that there is an error your configuration.

Extra Configuration for Webserver

Webserver is on the orange LAN. The rest of the RFPK workstations and servers are either on the green LAN or on the public internet. The firewall greatly restricts network traffic between the green and orange LANs. The NTP setup for *webserver* is the same as for the rest of the clients with the exception that additional configuration must be done to the firewall. It is necessary to use the firewall administration interface to create a pinhole between the IP address of *webserver* and the IP address of *timeserver* on port 123 for the TCP protocol, and another one on the same port for the UDP protocol.

Configuring the RFPK Timeserver

The RFPK time server needs to be set up somewhat differently from the workstations.

Just as for workstations, the default should be edited to read

```
restrict default nomodify
```

The list of trusted servers, should read as follows:

```
restrict bigben.cac.washington.edu nomodify notrap noquery
restrict time.nist.gov nomodify notrap noquery
restrict tick.uh.edu nomodify notrap noquery
restrict tick.usno.navy.mil nomodify notrap noquery

server bigben.cac.washington.edu
server time.nist.gov
server tick.uh.edu
server tick.usno.navy.mil
```

Unlike the workstation case, the server must be open to clients. Just following the commented CLIENT NETWORK section, add the following

```
restrict 192.168.0.0 mask 255.255.0.0 notrust nomodify notrap
```

which enables service requests coming from any of the IP addresses behind the firewall in the lab at AERL 241.

Additional lines, similar to the one above, can be added to accommodate RFPK machines with IP addresses that fall into other address ranges.