SPK and Associates

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

How to setup NTOP on a RedHat/CentOS Server

Bradley Tinder, Systems Integrator, SPK and Associates

Prerequisites:

- A working installation of RedHat (with update subscription) or CentOS.
- 2 physical (or virtual) network interface cards (NICs)

Step 1: Prep your operating system for NTOP

There are several packages you'll need to download and install first before compiling NTOP. I'll list out the exact commands you should run as root to get these packages setup first.

```
yum install cairo-devel libxml2-devel pango-devel pango libpng-devel

yum install freetype freetype-devel libart_lgpl-devel wget gcc make

yum install perl-ExtUtils-MakeMaker

cd /opt

wget http://oss.oetiker.ch/rrdtool/pub/rrdtool-1.4.8.tar.gz

tar -zxvf rrdtool-1.4.8.tar.gz

cd rrdtool-1.4.8

./configure –prefix=/usr/local/rrdtool

make

make install
```

This will install all the core requirements for NTOP. Next, we need to download a few more development libraries and the GeoIP tool which will allow you to correlate IP addresses with countries of origin. Run the following commands to get those packages and the GeoIP database installed.

```
yum install libpcap libpcap-devel gdbm gdbm-devel

yum install libevent libevent-devel

wget http://geolite.maxmind.com/download/geoip/api/c/GeoIP-1.4.8.tar.gz

tar -zxvf GeoIP-1.4.8.tar.gz

cd GeoIP-1.4.8

./configure

make

make install
```

Finally, download the automake/autoconf tools and finally, NTOP. I currently run 4.1, but as of this writing, ntopng (NTOP next gen) is the latest and greatest. I have not evaluated that version yet, but expect that in a future blog post. ☺ Run these commands to get those packages and NTOP as well as create a dedicated ntop user account to run the tool.

```
yum install libtool automake autoconf

wget http://downloads.sourceforge.net/project/ntop/ntop/Stable/ntop-4.1.0.tar.gz

tar zxvf ntop-4.1.0.tar.gz

cd ntop-4.1.0

./autogen.sh -prefix=/usr/local/ntop

make

make install

useradd -M -s /sbin/nologin -r ntop

chown ntop:root /usr/local/ntop

chown ntop:ntop /usr/local/ntop/share/ntop
```

Step 2: Configure NTOP for first run

Next, we need to configure NTOP for it’s first run. Issue these commands to launch NTOP in Administrative mode and configure the network interface to be the secondary NIC on the system.

```
cd /usr/local/ntop/bin/
```

```
ntop –A
```

Now you can launch NTOP and begin collecting network data:

```
ntop -d -L -u ntop -P /usr/local/ntop –-skip-version-check –-use –syslog=daemon
```

Access the NTOP web page by heading to:

http://<machine>:3000/

Login with the username and password you chose during the admin mode setup.

Now you should have a working NTOP setup. There’s a lot more to cover about the too, so dig into the tool and check out all of the cool features and stats you can view. Note that it will take about 5-10 minutes for your setup to start collecting meaningful data. Once it does, though, you should be able to see everything that’s going on with your network!