Table Of Contents

Home > Faq > CentOS

Install ntop on Red Hat Enterprise Linux / CentOS Linux

Posted by Vivek Gite <vivek@nixcraft.com>

This entry is part 17 of 2 in the series RRDtool [1]

RRDtool [1]

- Install RRDTool on Red Hat Enterprise Linux [2]
- Install ntop on Red Hat Enterprise Linux / CentOS Linux

Q. ntop is a network probe that shows network usage in a way similar to what top does for processes. How do I install latest version of ntop on RHEL 5.x systems?

[3]

A. ntop is a network and traffic analyzer that provides a wealth of information on various networking hosts and protocols. ntop is primarily accessed via a built-in web interface.

Following instructions are tested on 32/64 bit versions only:
a) RHEL Linux 5.x
b) CentOS Linux 5.x

Download latest ntop

Visit ntop project [4] to grab latest version. You can use wget to grab the same, enter:

```
# cd /opt
# wget http://freshmeat.net/redir/ntop/7279/url_tgz/ntop-3.3.6.tar.gz
```

Untar tar ball, enter:

```
# tar -zxvf ntop-3.3.6.tar.gz
```

Configure and Compile ntop under RHEL

You must have **RRDTool installed** [2]. You also need to install libpcap, enter:

```
# yum install libpcap-devel libpcap
```

Type the following commands to compile and install ntop:

```
# cd ntop
# ./autogen.sh
```

Just type make to compile ntop:

```
# make
```

Just type make install to install ntop:

```
# make install
# make install-data-as
```

Create ntop user

Type the following command to run ntop as ntop user, enter:

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

Setup directory permissions

Next, you need to setup directory permissions, enter:

```
# chown ntop:root /usr/local/var/ntop/
# chown ntop:ntop /usr/local/share/ntop/
```

Setup ntop user admin password

Type the following command to set ntop admin password, enter:

```
# ntop -A
```

Sample output:

```
Mon Jul 28 03:38:34 2008  NOTE: Interface merge enabled by default
Mon Jul 28 03:38:34 2008  Initializing gdbm databases

ntop startup - waiting for user response!

Please enter the password for the admin user:
Please enter the password again:
Mon Jul 28 03:38:42 2008  Admin user password has been set
```

Start ntop

Type the following command to start ntop:

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

Sample output:

```
Mon Jul 28 03:42:19 2008  NOTE: Interface merge enabled by default
Mon Jul 28 03:42:19 2008  Initializing gdbm databases
```

If you have multiple interface (eth0, eth1 and so on), start ntop as follows:

```
# /usr/local/bin/ntop -i "eth0,eth1" -d -L -u ntop -P /usr/local/var/ntop --skip-
version-check --use-syslog=daemon
```

Where,

- **-i "eth0,eth1"** : Specifies the network interface or interfaces to be used by ntop for network monitoring. Here you are monitoring eth0 and eth1.
- **-d** : Run ntop as a daemon.
- **-L** : Send all log messages to the system log (/var/log/messages) instead of screen.
- **-u ntop** : Start ntop as ntop user
- **-P /usr/local/var/ntop** : Specify where ntop stores database files. You may need to backup database as part of your disaster recovery program.
- **--skip-version-check** : By default, ntop accesses a remote file to periodically check if the most current version is running. This option disables that check.
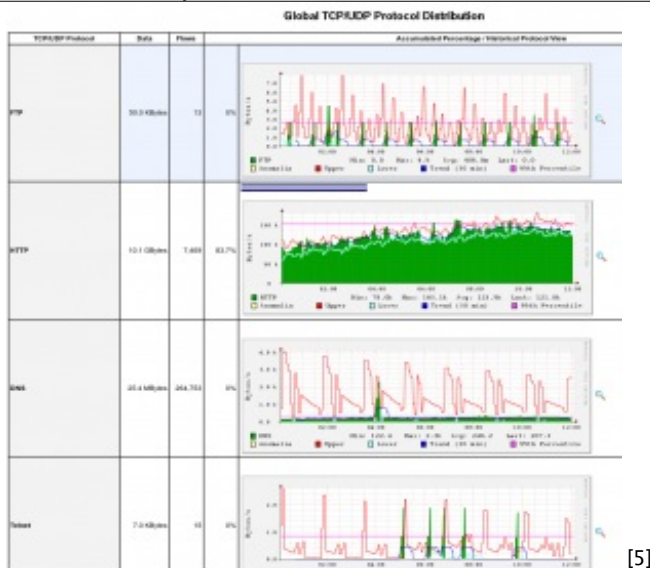- **--use-syslog=daemon** : Use syslog daemon.

How do I view ntop stats?

By default ntop listen on 3000 port. You can view ntop stats by visiting following url:
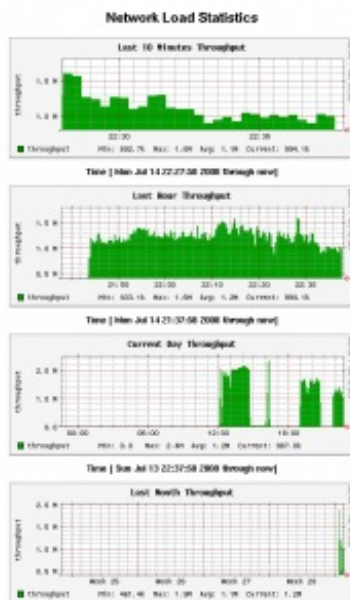
```
http://localhost:3000/
```

OR

```
http://server-ip:3000/
```

(Fig.01: ntop Global TCP/UDP Protocol Distribution Graphs [click to enlarge])

(Fig.02: Network Load Statistics (click to enlarge))

Open port 3000 using iptables

Open /etc/sysconfig/iptables file, enter:

```
# vi /etc/sysconfig/iptables
```

Append following code before final REJECT line:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3000 -j ACCEPT
```

Save and close the file. Restart firewall:

```
# service iptables restart
```

How do I view ntop stats without opening port 3000?

Setup simple tunnel using ssh, enter the following on your local UNIX / Linux desktop system:

```
$ ssh -L 3000:localhost:3000 -N -f user@server.yourcorp.com
```

Now open browser and type the following command:

```
http://localhost:3000/
```

How do I start ntop on boot?

Open /etc/rc.local file, enter:

```
# vi /etc/rc.local
```

Append the following line:

```
/usr/local/bin/ntop -i "eth0,eth1" -d -L -u ntop -P /usr/local/var/ntop --
skip-version-check --use-syslog=daemon
```

Save and close the file.

How do I stop ntop?

Use web interface to shutdown ntop, or use normal kill / killall command:

```
# killall ntop
```

Further readings:

- ntop man page
- ntop project [7]

Series Navigation

«Install RRDTool on Red Hat Enterprise Linux [2]

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/howto-install-ntop-on-rhel-centos-fedora-linux/**

URLs in this post:

[1] RRDtool: **http://www.cyberciti.biz/faq/series/rrdtool/**
[2] Install RRDTool on Red Hat Enterprise Linux: **http://www.cyberciti.biz/faq/howto-install-rrdtool-on-rhel-linux/**
[3] Image: **http://www.cyberciti.biz/faq/faq/category/redhat-and-friends/**
[4] ntop project: **http://freshmeat.net/projects/ntop/**
[5] Image: **http://www.cyberciti.biz/faq/wp-content/uploads/2008/07/ntop-output-1.png**
[6] Image: **http://www.cyberciti.biz/faq/wp-content/uploads/2008/07/network-load-ntop-output-2.png**
[7] ntop project: **http://www.ntop.org/**