Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Redhat Enterprise Linux 5 / CentOS 5 monitor and track TCP connections on the network (eth0)

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I track and monitor connection for eth1 public network interface under Redhat Enterprise Linux (RHEL) 5 server?

A.You can use netstat command or tcptrack command. Both command can show established TCP connection and provides the ability to monitor the same.

[1]

netstat command

netstat command prints information about the Linux networking subsystem. It also works under UNIX and *BSD oses. It can display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships etc.

netstat command to display established connections

Type the command as follows:

```
$ netstat -nat
```

Output:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:2208          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:52459           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1521            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3128            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:31323         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:2207          0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.100:59917     74.86.48.98:291         ESTABLISHED
tcp        0      0 127.0.0.1:3128          127.0.0.1:49413         TIME_WAIT
tcp        0      0 127.0.1.1:54624         127.0.1.1:1521          ESTABLISHED
tcp        0      0 127.0.1.1:1521          127.0.1.1:54624         ESTABLISHED
tcp        0      0 192.168.1.100:55914     74.125.19.147:80        ESTABLISHED
tcp        0      0 127.0.0.1:3128          127.0.0.1:42471         TIME_WAIT
tcp        0      0 192.168.1.100:56357     74.86.48.98:993         ESTABLISHED
tcp        0      0 192.168.1.100:56350     74.86.48.98:993         ESTABLISHED
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

To display client / server ESTABLISHED connections only:

```
$ netstat -nat | grep 'ESTABLISHED'
```

tcptrack command

tcptrack command displays the status of TCP connections that it sees on a given network interface. tcptrack monitors their state and displays information such as state, source/destination addresses and bandwidth usage in a sorted, updated list very much like the top command.

Install tcptrack

Redhat (RHEL) / Fedora / CentOS user, download tcptract here [2]. For example download RHEL 64 bit version:

```
# cd /tmp/
# wget http://dag.wieers.com/rpm/packages/tcptrack/tcptrack-1.1.5-1.2.el5.rf.x86_64.rpm
# rpm -ivh tcptrack-1.1.5-1.2.el5.rf.x86_64.rpm
```

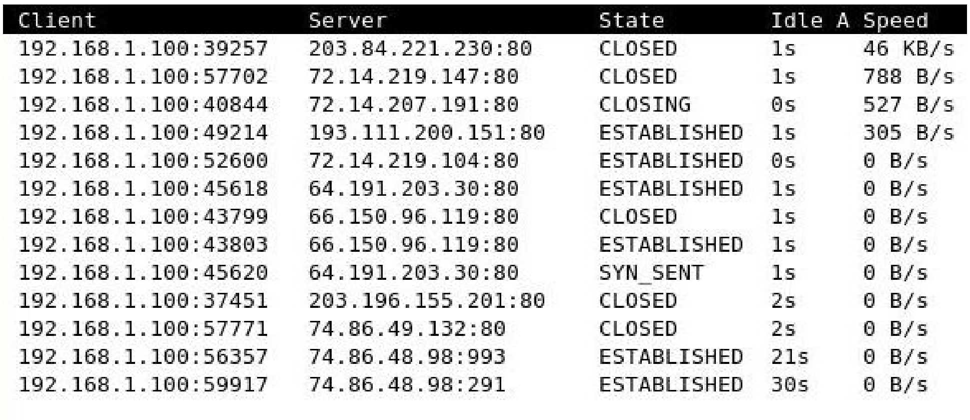
Debian / Ubuntu Linux user use apt-get as follows:

```
$ sudo apt-get install tcptrack
```

How do I use tcptract to monitor and track TCP connections ?

tcptrack requires only one parameter to run i.e. the name of an interface such as eth0, eth1 etc. Use the -i flag followed by an interface name that you want tcptrack to monitor.

```
# tcptrack -i eth0
# tcptrack -i eth1
```



```
 Client                Server                State        Idle A Speed
 192.168.1.100:39257   203.84.221.230:80     CLOSED       1s     46 KB/s
 192.168.1.100:57702   72.14.219.147:80      CLOSED       1s     788 B/s
 192.168.1.100:40844   72.14.207.191:80      CLOSING      0s     527 B/s
 192.168.1.100:49214   193.111.200.151:80    ESTABLISHED  1s     305 B/s
 192.168.1.100:52600   72.14.219.104:80      ESTABLISHED  0s     0 B/s
 192.168.1.100:45618   64.191.203.30:80      ESTABLISHED  1s     0 B/s
 192.168.1.100:43799   66.150.96.119:80      CLOSED       1s     0 B/s
 192.168.1.100:43803   66.150.96.119:80      ESTABLISHED  1s     0 B/s
 192.168.1.100:45620   64.191.203.30:80      SYN_SENT     1s     0 B/s
 192.168.1.100:37451   203.196.155.201:80    CLOSED       2s     0 B/s
 192.168.1.100:57771   74.86.49.132:80       CLOSED       2s     0 B/s
 192.168.1.100:56357   74.86.48.98:993       ESTABLISHED  21s    0 B/s
 192.168.1.100:59917   74.86.48.98:291       ESTABLISHED  30s    0 B/s
```

[3]

(tcptrack in action)

You can just monitor TCP port 25 (SMTP)

```
# tcptrack -i eth0 port 25
```

The next example will only show web traffic monitoring on port 80:

```
# tcptrack -i eth1 port 80
```

tcptrack can also take a pcap filter expression as an argument. The format of this filter expression is the same as that of tcpdump and other libpcap-based sniffers. The following example will only show connections from host 76.11.22.12:

```
# tcptrack -i eth0 src or dst 76.11.22.12
```

For further option please refer to man page of netstat and tcptrack command.

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

URL to article: **http://www.cyberciti.biz/faq/rhel-track-monitor-tcp-connections-on-network/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/networking/**

[2] here: **http://dag.wieers.com/rpm/packages/tcptrack/**

[3] Image: **http://www.cyberciti.biz/faq/wp-content/uploads/2007/08/tcptrack-command-tracking-tcp-connections.jpg**