Check the count and monitor of established / time_wait TCP, UDP connections on Linux and Windows with netstat command

Author : admin

For me as a **GNU / Linux sysadmin** it is intuitive to **check on a server the number of established connections / connections in time_wait state** and so on .

I will not explain why this is necessery as every system administrator out there who had a performance or network issues due to server / applications connection overload or have been a target of Denial of Service (DoS)
or Distributed Denial of Service attacks (DDoS) **is well aware that a number of connections in different states such as SYN_ACK / TIME_WAIT or ESTABLISHED state could be very nasty thing and could cause a productive application or Infrastructure service to be downed for some time causing from thousands of Euros to even millions to some bussinesses as well as some amount of data loss ...**

To prevent this therefore **sysadmins should always take a look periodically on the Connection states on the adminned server** (and in **this number I say not only sys admins but DevOps guys who are deploying micro-services for a customer in the Cloud - yes I believe *Richard Stallman* is right here they're clouding your minds :).**

Even though cloud services could provide a very high amount of Hardware (CPU / Memory / Storage) resources, often for custom applications migrating the application in the Cloud does not solve it's design faults or even problems on a purely classical system administration level.

1. Get a statistic for FIN_WAIT1, FOREIGN, SYNC_RECV, LAST_ACK, TIME_WAIT, LISTEN and ESTABLISHED Connections on GNU / Linux

On **GNU / Linux and other Linux like UNIXes the way to do it is to grep out the TCP / UDP connection type you need via netstat a very useful cmd** in that case is:

```
root@pcfreak:~# netstat -nat | awk '{print $6}' | sort | uniq -c | sort -n
   1 established)
   1 FIN_WAIT1
   1 Foreign
   1 SYN_RECV
   3 LAST_ACK
   4 FIN_WAIT2
   8 TIME_WAIT
  45 LISTEN
 147 ESTABLISHED
```

2. Netstat 1 liner to Get only established and time_wait connections state

Other ways to check only TCP ESTABLISHED connections on Linux I use frequently are:

```
root@pcfreak:~# netstat -etna|grep -i establi|wc -l
145
```

```
root@pcfreak:~# netstat -nat | awk '{print $6}' | sort | uniq -c | sort -n
      1 established)
      1 FIN_WAIT2
      1 Foreign
      2 LAST_ACK
      2 SYN_RECV
      2 SYN_SENT
      4 CLOSE_WAIT
      7 TIME_WAIT
     45 LISTEN
    138 ESTABLISHED
root@pcfreak:~#
```

Or to get whole list of connections including the ones who are about to be esatablished in *FIN_WAIT2, TIME_WAIT, SYN_RECV* state:

```
root@pcfreak:~# netstat -tupen |wc -l
164
```

3. Other Linux useful one liner commands to track your connection types

```
netstat -n -p | grep SYN_REC | sort -u
```

List out the all IP addresses involved instead of just count.

```
netstat -n -p | grep SYN_REC | awk '{print $5}' | awk -F: '{print $1}'
```

List all the unique IP addresses of the node that are sending SYN_REC connection status.

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

Use netstat command to calculate and count the number of connections each IP address makes to the server.

```
netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

List count of number of connections the IPs are connected to the server using TCP or UDP protocol.

```
netstat -ntu | grep ESTAB | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr
```

Check on ESTABLISHED connections instead of all connections, and displays the connections count

for each IP.

```
netstat -plan|grep :80|awk {'print $5'}|cut -d: -f 1|sort|uniq -c|sort -nk 1
```

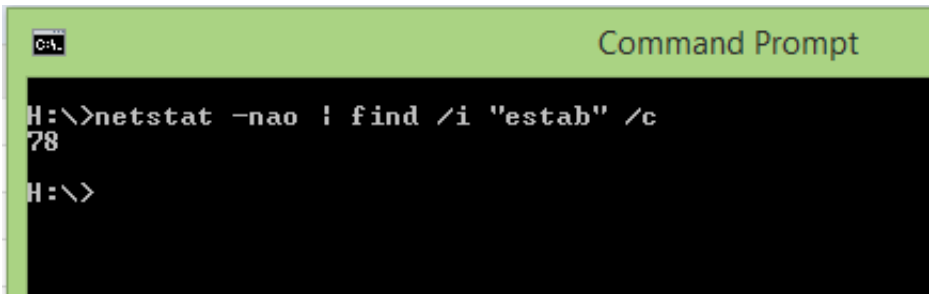
Show and list IP address and its connection count that connect to port 80 on the server. Port 80 is used mainly by HTTP web page request.

Examples are taken from this nice blog post

4. Check the count of esatblished connections on M$ Windows

As I'm forced to optimize a couple of Microsoft Windows DNS servers which are really slow to resolve the
The logical question for me was how the *Established* and *TIME_WAIT* state connections then could be checked on Windows OS, after a quick investigation online I've come up with this:

```
C:\Users\admin> netstat -nao | find /i "estab" /c
78
```



C:\Users\admin> netsatt -nao | find /i "time_wait" /c
333

If you're used to Linux watch command, then to do same on Windows OS (e.g. check the output of netstat) command every second
and print output use:

netstat –an 1 | find “3334”

Below commands will show stats for services listening on TCP port 3334

To find out which process on system sends packets to remote destination:

netstat –ano 1 | find “Dest_IP_Addr”

The -o parameter outputs the process **ID (PID**) responsible for the connection.
then if you need further you can find the respective process name with tasklist