How to check who is flooding your Apache, NGinx Webserver - Real time Monitor statistics about IPs doing most URL requests and Stopping DoS attacks with Fail2Ban

Author : admin

If you're **Linux ystem administrator in Webhosting company providing** ***Wordpress / Joomla / Drupal web-sites hosting*** and **your UNIX servers suffer from periodic** ***denial of service attacks*****, because** ***some of the site customers business is a target of competitor company who is trying to ruin your client business sites through DoS or DDOS attacks***, then the best thing you can do is to identify who and how is the Linux server being hammered. If you find out DoS is not on a network level but Apache gets crashing because of *memory leaks* and connections to Apache are so much that the **CPU is being stoned**, the best thing to do is to *check which IP addresses are causing the excessive* ***GET / POST / HEAD*** *requests* in logged.

There is the Apachetop tool that can give you the *most accessed webserver URLs in a refreshed screen like UNIX* **top** command, however Apachetop does not show which IP does most URL hits on *Apache / Nginx* webserver.

1. Get basic information on which IPs accesses Apache / Nginx the most using shell cmds

Before examining the Webserver logs it is useful to get a general picture on who is flooding you on a TCP / IP network level, with netstat like so:

```
# here is howto check clients count connected to your server
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

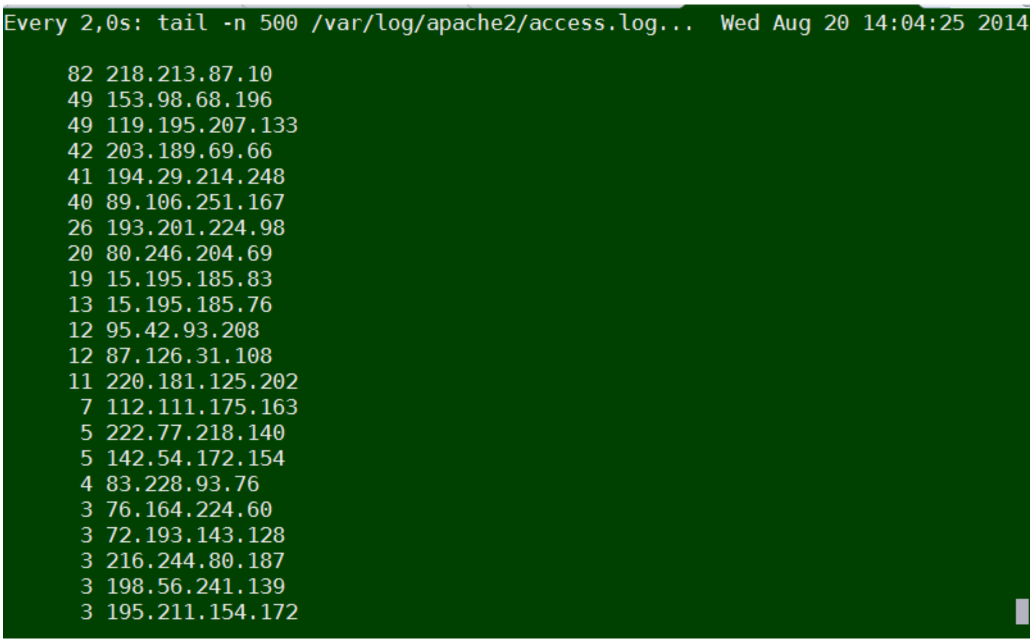
If you get an extensive number of connected various IPs / hosts (like 10000 or something huge as a number), depending on the type of hardware the server is running and the previous scaling planned for the system you can determine whether the count as huge as this can be handled normally by server, if like in most cases the server is planned to serve a couple of hundreds or thousands of clients and you get over 10000 connections hanging, then your server is under attack or if its Internet server suddenly your website become famous like someone posted an article on some major website and you suddenly received a tons of hits.

There is a way using standard shell tools, to **get some basic information on which IP accesses the webserver the most** with:

```
tail -n 500 /var/log/apache2/access.log | cut -d' ' -f1 | sort | uniq -c | sort -gr
```

Or if you want to keep it refreshing periodically every few seconds run it through **watch** command:

```
watch "tail -n 500 /var/log/apache2/access.log | cut -d' ' -f1 | sort | uniq -c | sort -gr"
```



```
Every 2,0s: tail -n 500 /var/log/apache2/access.log...  Wed Aug 20 14:04:25 2014

     82 218.213.87.10
     49 153.98.68.196
     49 119.195.207.133
     42 203.189.69.66
     41 194.29.214.248
     40 89.106.251.167
     26 193.201.224.98
     20 80.246.204.69
     19 15.195.185.83
     13 15.195.185.76
     12 95.42.93.208
     12 87.126.31.108
     11 220.181.125.202
      7 112.111.175.163
      5 222.77.218.140
      5 142.54.172.154
      4 83.228.93.76
      3 76.164.224.60
      3 72.193.143.128
      3 216.244.80.187
      3 198.56.241.139
      3 195.211.154.172
```

Another useful combination of shell commands is to **Monitor POST / GET / HEAD requests number in access.log** :

```
awk '{print $6}' access.log | sort | uniq -c | sort -n
```

1 "alihack