Q4)

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

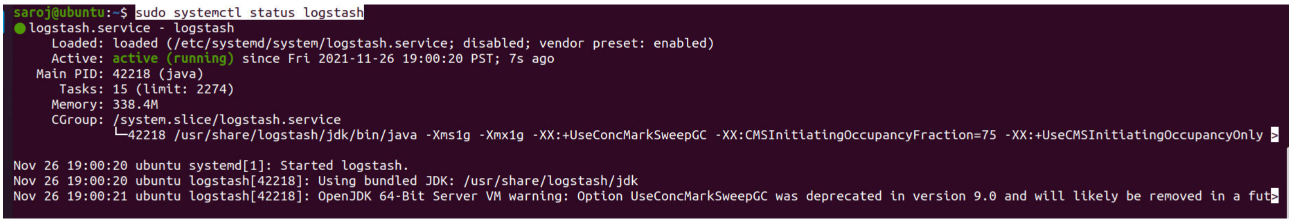
sudo apt-get install apt-transport-https

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main

sudo apt-get update && sudo apt-get install logstash

sudo systemctl start logstash

sudo systemctl status logstash

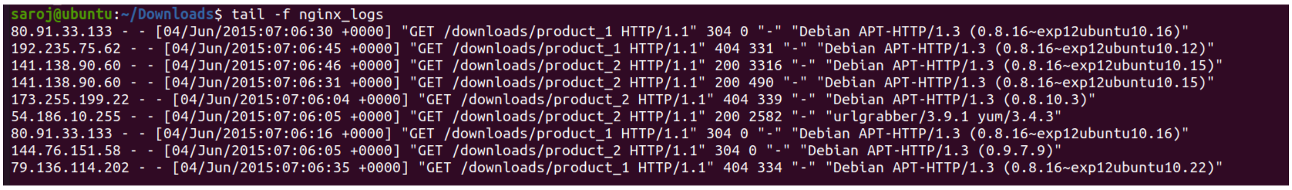


```
saroj@ubuntu:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset: enabled)
     Active: active (running) since Fri 2021-11-26 19:00:20 PST; 7s ago
   Main PID: 42218 (java)
      Tasks: 15 (limit: 2274)
     Memory: 338.4M
     CGroup: /system.slice/logstash.service
             └─42218 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly >

Nov 26 19:00:20 ubuntu systemd[1]: Started logstash.
Nov 26 19:00:20 ubuntu logstash[42218]: Using bundled JDK: /usr/share/logstash/jdk
Nov 26 19:00:21 ubuntu logstash[42218]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a fut>
```

downloading logs from https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/nginx_logs/nginx_logs

cd Downloads/
paste the content with name nginx_logs



```
saroj@ubuntu:~/Downloads$ tail -f nginx_logs
80.91.33.133 - - [04/Jun/2015:07:06:30 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)"
192.235.75.62 - - [04/Jun/2015:07:06:45 +0000] "GET /downloads/product_1 HTTP/1.1" 404 331 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.12)"
141.138.90.60 - - [04/Jun/2015:07:06:46 +0000] "GET /downloads/product_2 HTTP/1.1" 200 3316 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.15)"
141.138.90.60 - - [04/Jun/2015:07:06:31 +0000] "GET /downloads/product_2 HTTP/1.1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.15)"
173.255.199.22 - - [04/Jun/2015:07:06:04 +0000] "GET /downloads/product_2 HTTP/1.1" 404 339 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"
54.186.10.255 - - [04/Jun/2015:07:06:05 +0000] "GET /downloads/product_2 HTTP/1.1" 200 2582 "-" "urlgrabber/3.9.1 yum/3.4.3"
80.91.33.133 - - [04/Jun/2015:07:06:16 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)"
144.76.151.58 - - [04/Jun/2015:07:06:05 +0000] "GET /downloads/product_2 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.9.7.9)"
79.136.114.202 - - [04/Jun/2015:07:06:35 +0000] "GET /downloads/product_1 HTTP/1.1" 404 334 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.22)"
```

```
cd //etc//logstash//conf.d//
sudo nano logstash.conf
input {
  file {
    type => "nginx-log"
    path => "/home/saroj/Downloads/nginx_logs"
    sincedb_path => "/dev/null"
    start_position => "beginning"
  }
}

filter {
grok{
match=>{
"message"=>"%{IP:clientip} \- \- \["
}
}
geoip {
source => "clientip"
 }
}

output {
  file {
    path => "/var/log/logstash/testnginx.log"
  }
}
```

```
cd //etc//logstash//
sudo nano logstash.yml
```

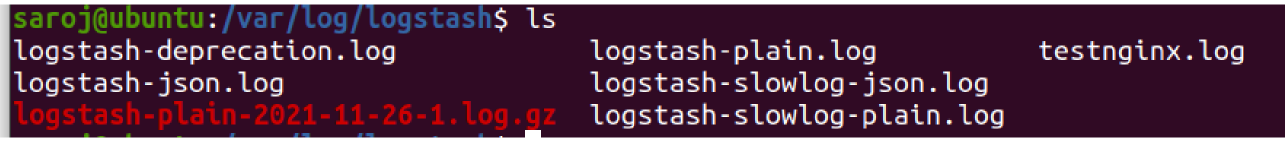
uncomment path.config //home/saroj/Downloads/nginx_logs

save it

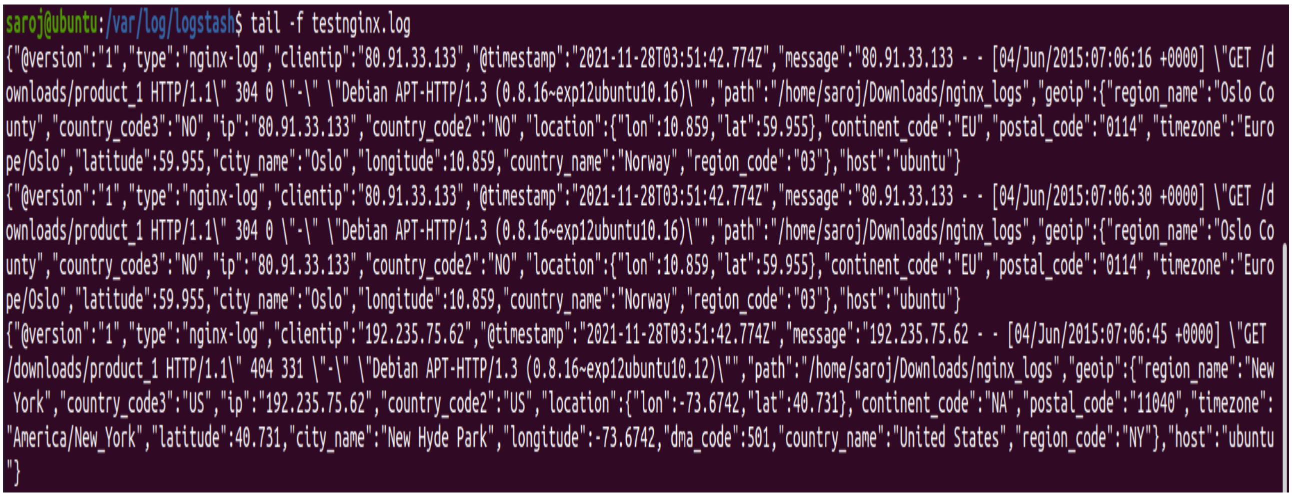
```
sudo systemctl stop logstash
sudo systemctl start logstash

cd //usr/share/logstash

sudo bin/logstash --path.settings /etc/logstash --path.data sensor39 -f /etc/logstash/conf.d
```



```
saroj@ubuntu:/var/log/logstash$ ls
logstash-deprecation.log          logstash-plain.log          testnginx.log
logstash-json.log                 logstash-slowlog-json.log
logstash-plain-2021-11-26-1.log.gz  logstash-slowlog-plain.log
```



```
saroj@ubuntu:/var/log/logstash$ tail -f testnginx.log
{"@version":"1","type":"nginx-log","clientip":"80.91.33.133","@timestamp":"2021-11-28T03:51:42.774Z","message":"80.91.33.133 - - [04/Jun/2015:07:06:16 +0000] \"GET /d
ownloads/product_1 HTTP/1.1\" 304 0 \"-\" \"Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)\"","path":"/home/saroj/Downloads/nginx_logs","geoip":{"region_name":"Oslo Co
unty","country_code3":"NO","ip":"80.91.33.133","country_code2":"NO","location":{"lon":10.859,"lat":59.955},"continent_code":"EU","postal_code":"0114","timezone":"Euro
pe/Oslo","latitude":59.955,"city_name":"Oslo","longitude":10.859,"country_name":"Norway","region_code":"03"},"host":"ubuntu"}
{"@version":"1","type":"nginx-log","clientip":"80.91.33.133","@timestamp":"2021-11-28T03:51:42.774Z","message":"80.91.33.133 - - [04/Jun/2015:07:06:30 +0000] \"GET /d
ownloads/product_1 HTTP/1.1\" 304 0 \"-\" \"Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)\"","path":"/home/saroj/Downloads/nginx_logs","geoip":{"region_name":"Oslo Co
unty","country_code3":"NO","ip":"80.91.33.133","country_code2":"NO","location":{"lon":10.859,"lat":59.955},"continent_code":"EU","postal_code":"0114","timezone":"Euro
pe/Oslo","latitude":59.955,"city_name":"Oslo","longitude":10.859,"country_name":"Norway","region_code":"03"},"host":"ubuntu"}
{"@version":"1","type":"nginx-log","clientip":"192.235.75.62","@timestamp":"2021-11-28T03:51:42.774Z","message":"192.235.75.62 - - [04/Jun/2015:07:06:45 +0000] \"GET
/downloads/product_1 HTTP/1.1\" 404 331 \"-\" \"Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.12)\"","path":"/home/saroj/Downloads/nginx_logs","geoip":{"region_name":"New
 York","country_code3":"US","ip":"192.235.75.62","country_code2":"US","location":{"lon":-73.6742,"lat":40.731},"continent_code":"NA","postal_code":"11040","timezone":
"America/New_York","latitude":40.731,"city_name":"New Hyde Park","longitude":-73.6742,"dma_code":501,"country_name":"United States","region_code":"NY"},"host":"ubuntu
"}
```