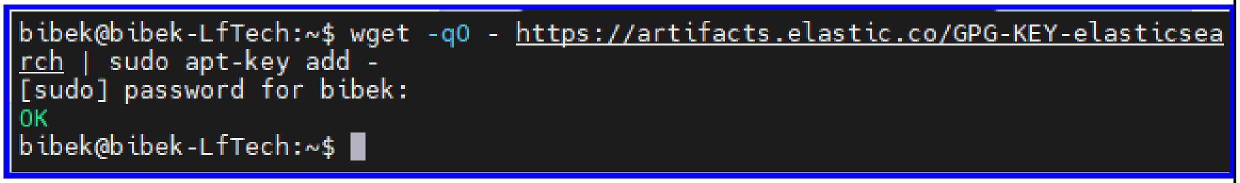
4. Install logstash in your system. download a sample nginx log from https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/nginx_logs/nginx_logs , parse the logs using logstash. The parsed output must contain the geographical information like country, state etc. that the request is originating from. save the parsed output to a file in your system.

Installing Logstash

Download and install the Public Signing Key:

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



```
bibek@bibek-LfTech:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsea
rch | sudo apt-key add -
[sudo] password for bibek:
OK
bibek@bibek-LfTech:~$
```

Install the apt-transport-https package on Debian before proceeding:

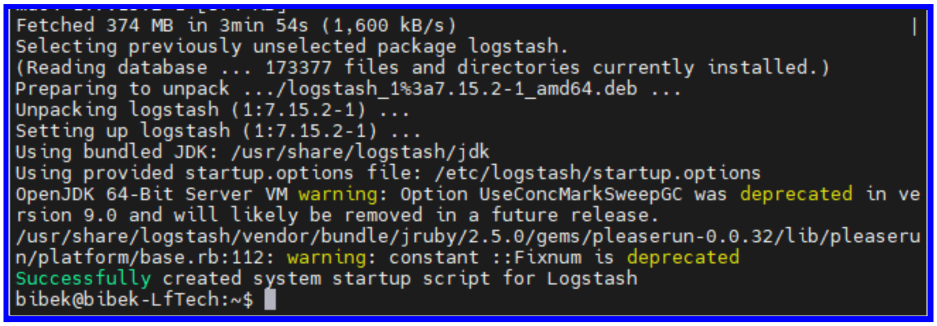
sudo apt-get install apt-transport-https

Save the repository definition to /etc/apt/sources.list.d/elastic-7.x.list:

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

Run sudo apt-get update and the repository is ready for use. You can install it with:

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

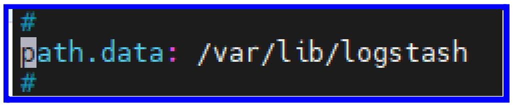


```
Fetched 374 MB in 3min 54s (1,600 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 173377 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.15.2-1_amd64.deb ...
Unpacking logstash (1:7.15.2-1) ...
Setting up logstash (1:7.15.2-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in ve
rsion 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaseru
n/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
bibek@bibek-LfTech:~$
```

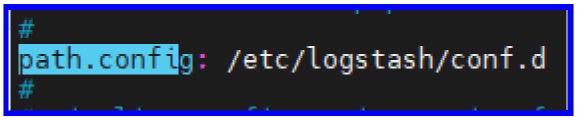
Configuring logstash

sudo vi /etc/logstash

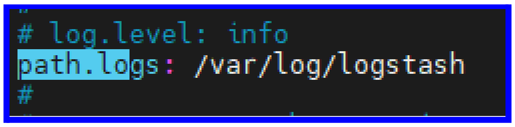
And make these changes



```
#
path.data: /var/lib/logstash
#
```

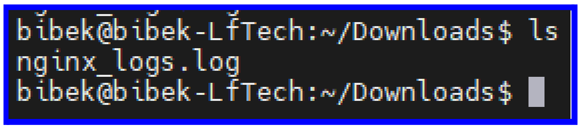


```
#
path.config: /etc/logstash/conf.d
#
```



```
# log.level: info
path.logs: /var/log/logstash
#
```

The nginx log file is downloaded and I renamed it with .log extension



```
bibek@bibek-LfTech:~/Downloads$ ls
nginx_logs.log
bibek@bibek-LfTech:~/Downloads$ 
```

Writing conf file for logstash

sudo vi /etc/logstash/conf.d/logstash-nginx.conf

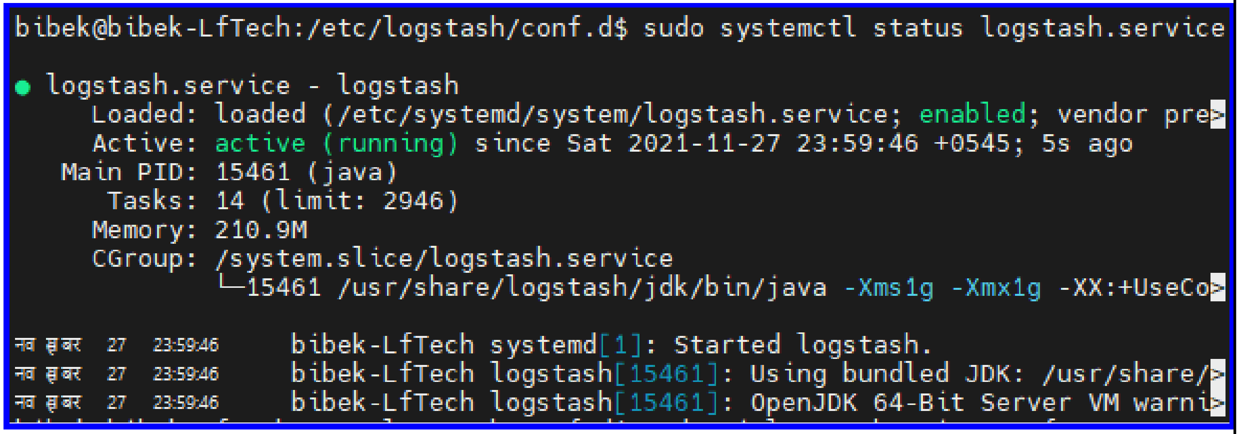
```
input {
 file {
 type => "nginx-log"
 path => "/home/bibek/Downloads/nginx_logs.log"
 sincedb_path => "/dev/null"
 start_position => "beginning"
}
}

filter {
  grok {
    match => { "message" => %{ IPV4 } }
  }
  geoip {
    source => "IPV4"
  }
}

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

Matching **IPV4** because grok filters IP with the name IPv4 and giving same **IPV4** as source to geoip.

Starting the logstash

sudo systemctl start logstash

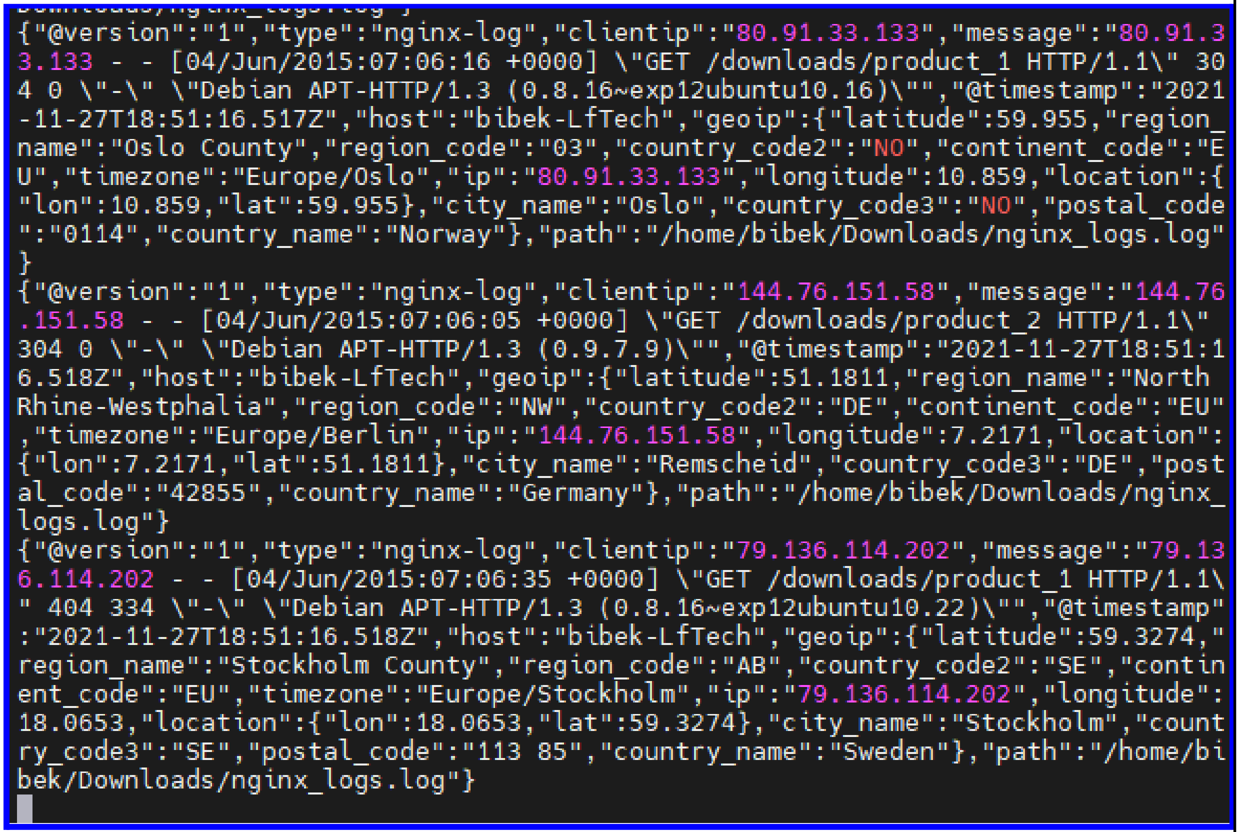
sudo systemctl status logstash



```
bibek@bibek-LfTech:/etc/logstash/conf.d$ sudo systemctl status logstash.service

● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pre>
     Active: active (running) since Sat 2021-11-27 23:59:46 +0545; 5s ago
   Main PID: 15461 (java)
      Tasks: 14 (limit: 2946)
     Memory: 210.9M
     CGroup: /system.slice/logstash.service
             └─15461 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCo>

नव ह्बर 27 23:59:46 bibek-LfTech systemd[1]: Started logstash.
नव ह्बर 27 23:59:46 bibek-LfTech logstash[15461]: Using bundled JDK: /usr/share/>
नव ह्बर 27 23:59:46 bibek-LfTech logstash[15461]: OpenJDK 64-Bit Server VM warni>
```

Checking for the log format in the nginx_log in the /var/log/logstash directory

tail -f /var/log/logstash/logstashnginx.log



```
Downloads/nginx_logs.log"}
{"@version":"1","type":"nginx-log","clientip":"80.91.33.133","message":"80.91.3
3.133 - - [04/Jun/2015:07:06:16 +0000] \"GET /downloads/product_1 HTTP/1.1\" 30
4 0 \"-\" \"Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)\"","@timestamp":"2021
-11-27T18:51:16.517Z","host":"bibek-LfTech","geoip":{"latitude":59.955,"region_
name":"Oslo County","region_code":"03","country_code2":"NO","continent_code":"E
U","timezone":"Europe/Oslo","ip":"80.91.33.133","longitude":10.859,"location":{
"lon":10.859,"lat":59.955},"city_name":"Oslo","country_code3":"NO","postal_code
":"0114","country_name":"Norway"},"path":"/home/bibek/Downloads/nginx_logs.log"
}
{"@version":"1","type":"nginx-log","clientip":"144.76.151.58","message":"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)\"","@timestamp":"2021-11-27T18:51:1
6.518Z","host":"bibek-LfTech","geoip":{"latitude":51.1811,"region_name":"North
Rhine-Westphalia","region_code":"NW","country_code2":"DE","continent_code":"EU"
,"timezone":"Europe/Berlin","ip":"144.76.151.58","longitude":7.2171,"location":
{"lon":7.2171,"lat":51.1811},"city_name":"Remscheid","country_code3":"DE","post
al_code":"42855","country_name":"Germany"},"path":"/home/bibek/Downloads/nginx_
logs.log"}
{"@version":"1","type":"nginx-log","clientip":"79.136.114.202","message":"79.13
6.114.202 - - [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)\"","@timestamp"
:"2021-11-27T18:51:16.518Z","host":"bibek-LfTech","geoip":{"latitude":59.3274,"
region_name":"Stockholm County","region_code":"AB","country_code2":"SE","contin
ent_code":"EU","timezone":"Europe/Stockholm","ip":"79.136.114.202","longitude":
18.0653,"location":{"lon":18.0653,"lat":59.3274},"city_name":"Stockholm","count
ry_code3":"SE","postal_code":"113 85","country_name":"Sweden"},"path":"/home/bi
bek/Downloads/nginx_logs.log"}
```

We can clearly see the country name, city name and other information