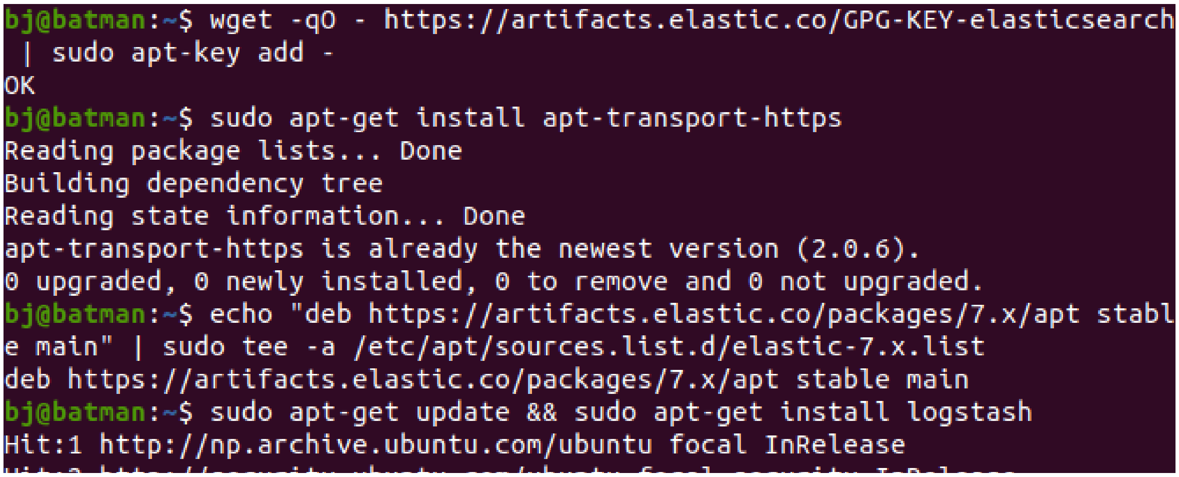
Install logstash in your system. download a sample nginx log from https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/nginx_logs/nginx_logs , parse the logs using logstash. The parsed output must contain the geographical information like country, state etc. that the request is originating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

First of all, to install logstash, following commands are used:

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

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

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



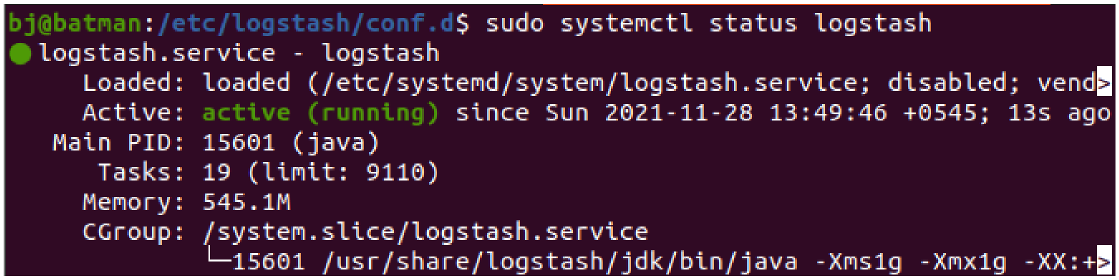
```
bj@batman:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch
 | sudo apt-key add -
OK
bj@batman:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
apt-transport-https is already the newest version (2.0.6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
bj@batman:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stabl
e main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
bj@batman:~$ sudo apt-get update && sudo apt-get install logstash
Hit:1 http://np.archive.ubuntu.com/ubuntu focal InRelease
```

And logstash is not started by default so, it is started using command:

Sudo systemctl start logstash

To check the status,

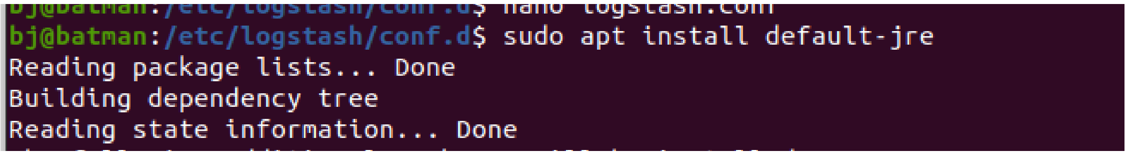
Sudo systemctl status logstash



```
bj@batman:/etc/logstash/conf.d$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vend>
     Active: active (running) since Sun 2021-11-28 13:49:46 +0545; 13s ago
   Main PID: 15601 (java)
      Tasks: 19 (limit: 9110)
     Memory: 545.1M
     CGroup: /system.slice/logstash.service
             └─15601 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+>
```

Now, java runtime environment should be installed which is installed using command:

Sudo apt install default-jre

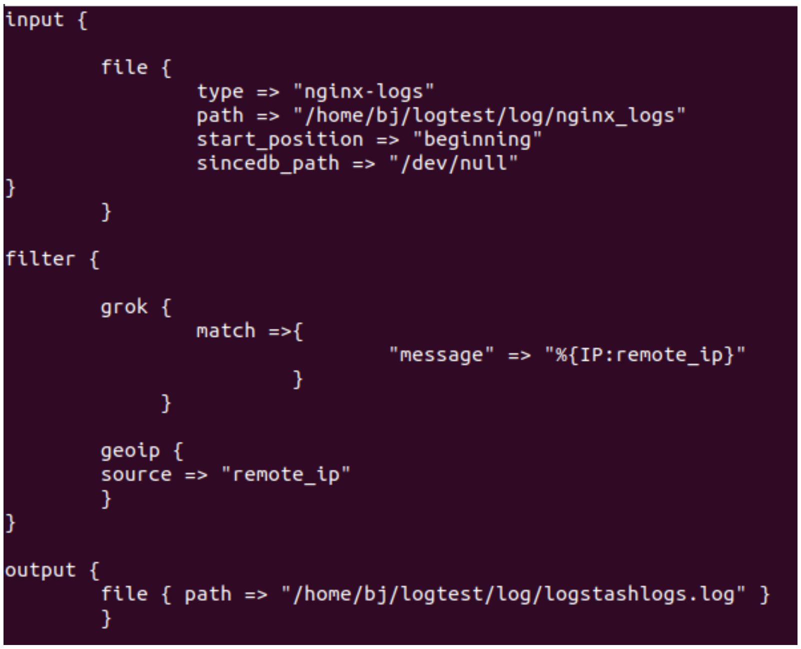


```
bj@batman:/etc/logstash/conf.d$ nano logstash.conf
bj@batman:/etc/logstash/conf.d$ sudo apt install default-jre
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

In the directory /etc/logstash/conf.d a file is made, *logstash.conf* with content shown in figure:

Cd /etc/logstash/conf.d

Nano logstash.conf

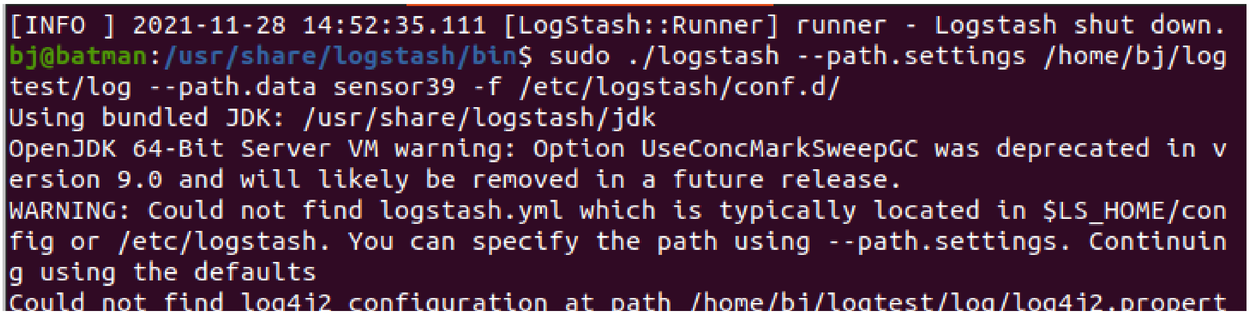


```
input {

        file {
                type => "nginx-logs"
                path => "/home/bj/logtest/log/nginx_logs"
                start_position => "beginning"
                sincedb_path => "/dev/null"
}
        }

filter {

        grok {
                match =>{
                                "message" => "%{IP:remote_ip}"
                        }
             }

        geoip {
        source => "remote_ip"
        }
}

output {
        file { path => "/home/bj/logtest/log/logstashlogs.log" }
        }
```

Now we run a logstash script from within the /usr/share/logstash/bin directory:

Cd /usr/share/logstash/bin

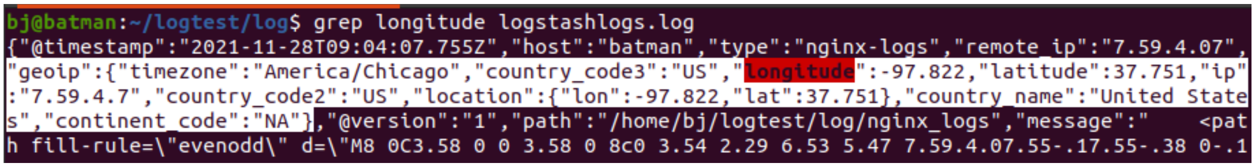
Sudo ./logstash --path.settings /home/bj/logtest/log --path.data sensor39 -f /etc/logstash/conf.d/



```
[INFO ] 2021-11-28 14:52:35.111 [LogStash::Runner] runner - Logstash shut down.
bj@batman:/usr/share/logstash/bin$ sudo ./logstash --path.settings /home/bj/log
test/log --path.data sensor39 -f /etc/logstash/conf.d/
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in v
ersion 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/con
fig or /etc/logstash. You can specify the path using --path.settings. Continuin
g using the defaults
Could not find log4j2 configuration at path /home/bj/logtest/log/log4j2.propert
```

After this process is completed: we can use grep to view the longitude information in the logstashlogs.log file, which is specified in the above configuration file.

Here, we can see country code, ip address, location (with longitude and latitude) and other geo information for that specific IP.



```
bj@batman:~/logtest/log$ grep longitude logstashlogs.log
{"@timestamp":"2021-11-28T09:04:07.755Z","host":"batman","type":"nginx-logs","remote_ip":"7.59.4.07",
"geoip":{"timezone":"America/Chicago","country_code3":"US","longitude":-97.822,"latitude":37.751,"ip"
:"7.59.4.7","country_code2":"US","location":{"lon":-97.822,"lat":37.751},"country_name":"United State
s","continent_code":"NA"},"@version":"1","path":"/home/bj/logtest/log/nginx_logs","message":"    <pat
h fill-rule=\"evenodd\" d=\"M8 0C3.58 0 0 3.58 0 8c0 3.54 2.29 6.53 5.47 7.59.4.07.55-.17.55-.38 0-.1
```