

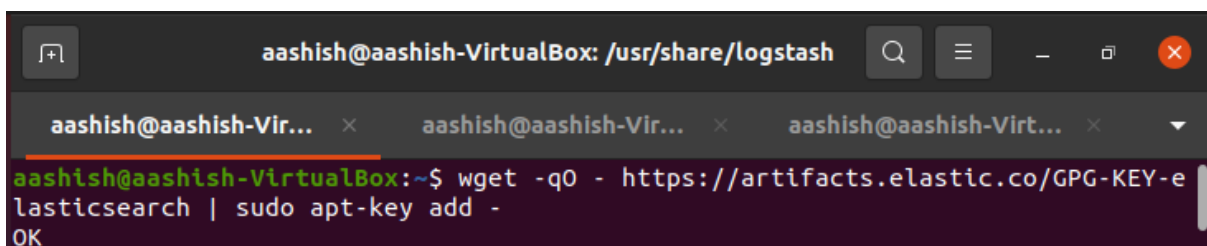
4.

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](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.

**Answer:**

Firstly, we install the public signing key using the following command;

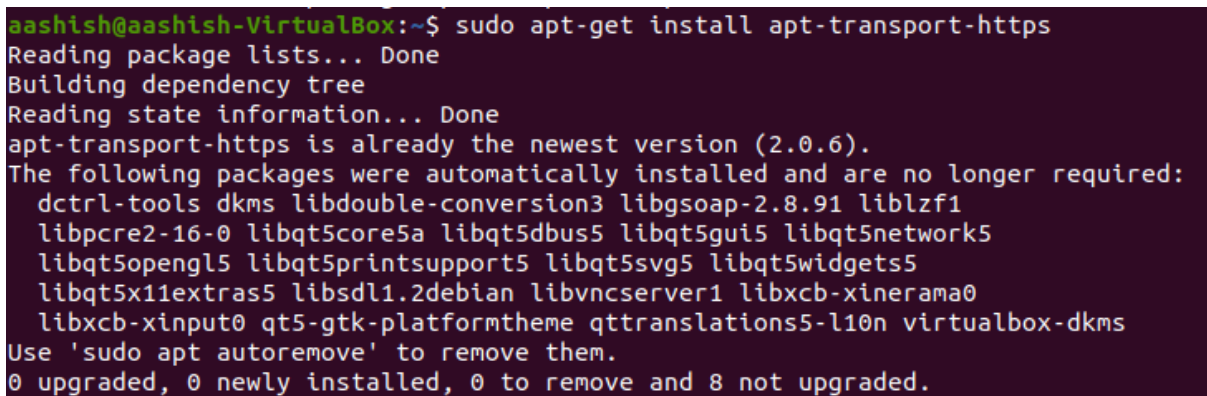
```
- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```



```
aashish@aashish-VirtualBox: /usr/share/logstash
aashish@aashish-Vir... x aashish@aashish-Vir... x aashish@aashish-Virt... x
aashish@aashish-VirtualBox:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
```

Next, we install apt-transport-https as follows;

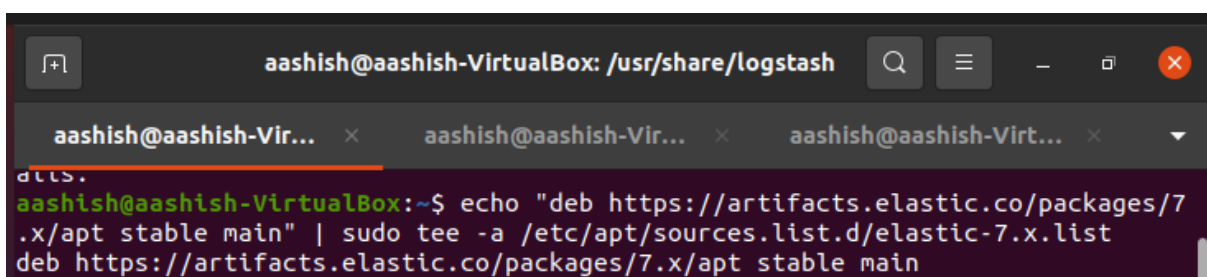
```
- sudo apt-get install apt-transport-https
```



```
aashish@aashish-VirtualBox:~$ 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).
The following packages were automatically installed and are no longer required:
  dctrl-tools dkms libdouble-conversion3 libgsoap-2.8.91 liblzfl
  libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
  libqt5x11extras5 libsdl1.2debian libvncserver1 libxcb-xinerama0
  libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n virtualbox-dkms
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

Then, elastic package repository was added to our repo list as follows;

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



```
aashish@aashish-VirtualBox: /usr/share/logstash
aashish@aashish-Vir... x aashish@aashish-Vir... x aashish@aashish-Virt... x
aashish@aashish-VirtualBox:~$ 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
```

Next, we update apt and install logstash as follows;

- **sudo apt-get update**
- **sudo apt-get install logstash -y**

```
aashish@aashish-VirtualBox: ~  
dctrl-tools dkms libdouble-conversion3 libgsoap-2.8.91 liblzf1  
libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5  
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5  
libqt5x11extras5 libsdl1.2debian libvncserver1 libxcb-xinerama0  
libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n virtualbox-dkms  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  logstash  
0 upgraded, 1 newly installed, 0 to remove and 8 not upgraded.  
Need to get 374 MB of archives.  
After this operation, 640 MB of additional disk space will be used.  
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash  
amd64 1:7.15.2-1 [374 MB]  
Fetched 374 MB in 2min 20s (2,671 kB/s)  
Selecting previously unselected package logstash.  
(Reading database ... 193964 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 v  
ersion 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/pleaser  
un/platform/base.rb:112: warning: constant ::Fixnum is deprecated  
Successfully created system startup script for Logstash  
aashish@aashish-VirtualBox:~$
```

To start and check the logstash status we use;

- **sudo systemctl start logstash**
- **sudo systemctl status logstash**

```
Firefox Web Browser aashish@aashish-VirtualBox: ~  
aashish@aashish-VirtualBox:~$ sudo systemctl start logstash  
aashish@aashish-VirtualBox:~$ sudo systemctl status logstash  
● logstash.service - logstash  
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor pr  
   Active: active (running) since Sun 2021-11-28 17:10:36 +0545; 6s ago  
   Main PID: 9909 (java)  
     Tasks: 14 (limit: 3807)  
    Memory: 207.2M  
    CGroup: /system.slice/logstash.service  
            └─9909 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon  
नवम्बर 28 17:10:36 aashish-VirtualBox systemd[1]: Started logstash.  
नवम्बर 28 17:10:36 aashish-VirtualBox logstash[9909]: Using bundled JDK: /usr/s  
नवम्बर 28 17:10:37 aashish-VirtualBox logstash[9909]: OpenJDK 64-Bit Server VM
```

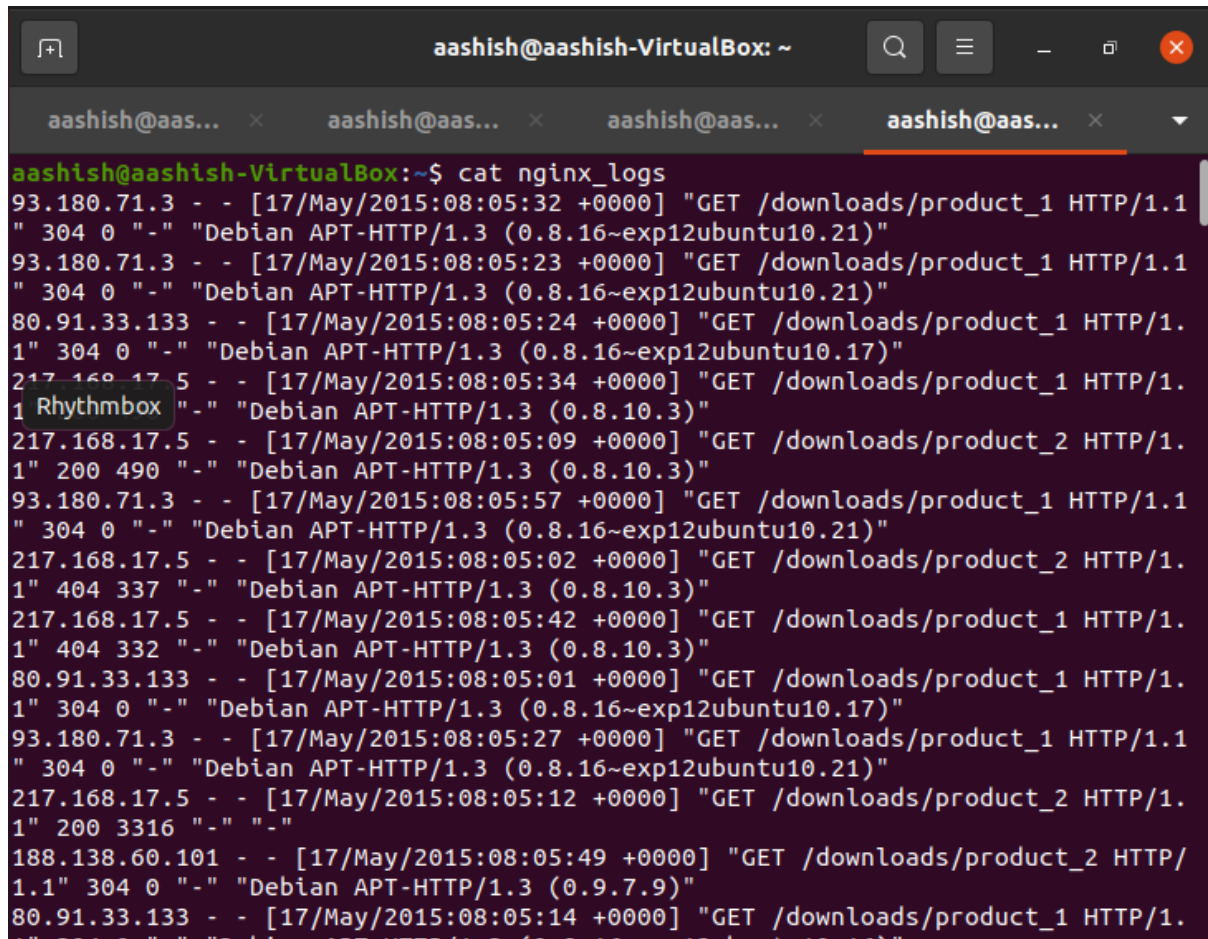
To download nginx log, we use following command;

- **wget**

[https://raw.githubusercontent.com/elastic/examples/master/Common%20Data%20Formats/nginx\\_logs/nginx\\_logs](https://raw.githubusercontent.com/elastic/examples/master/Common%20Data%20Formats/nginx_logs/nginx_logs)

To check the logs downloaded, we use;

- **cat nginx\_logs**



```
aashish@aashish-VirtualBox: ~  
aashish@aas... x aashish@aas... x aashish@aas... x aashish@aas... x  
aashish@aashish-VirtualBox:~$ cat nginx_logs  
93.180.71.3 - - [17/May/2015:08:05:32 +0000] "GET /downloads/product_1 HTTP/1.1  
" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"  
93.180.71.3 - - [17/May/2015:08:05:23 +0000] "GET /downloads/product_1 HTTP/1.1  
" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"  
80.91.33.133 - - [17/May/2015:08:05:24 +0000] "GET /downloads/product_1 HTTP/1.  
1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)"  
217.168.17.5 - - [17/May/2015:08:05:34 +0000] "GET /downloads/product_1 HTTP/1.  
1 Rhythmbbox" "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
217.168.17.5 - - [17/May/2015:08:05:09 +0000] "GET /downloads/product_2 HTTP/1.  
1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
93.180.71.3 - - [17/May/2015:08:05:57 +0000] "GET /downloads/product_1 HTTP/1.1  
" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"  
217.168.17.5 - - [17/May/2015:08:05:02 +0000] "GET /downloads/product_2 HTTP/1.  
1" 404 337 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
217.168.17.5 - - [17/May/2015:08:05:42 +0000] "GET /downloads/product_1 HTTP/1.  
1" 404 332 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
80.91.33.133 - - [17/May/2015:08:05:01 +0000] "GET /downloads/product_1 HTTP/1.  
1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)"  
93.180.71.3 - - [17/May/2015:08:05:27 +0000] "GET /downloads/product_1 HTTP/1.1  
" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"  
217.168.17.5 - - [17/May/2015:08:05:12 +0000] "GET /downloads/product_2 HTTP/1.  
1" 200 3316 "-" "-"  
188.138.60.101 - - [17/May/2015:08:05:49 +0000] "GET /downloads/product_2 HTTP/  
1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.9.7.9)"  
80.91.33.133 - - [17/May/2015:08:05:14 +0000] "GET /downloads/product_1 HTTP/1.  
1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.16)"
```

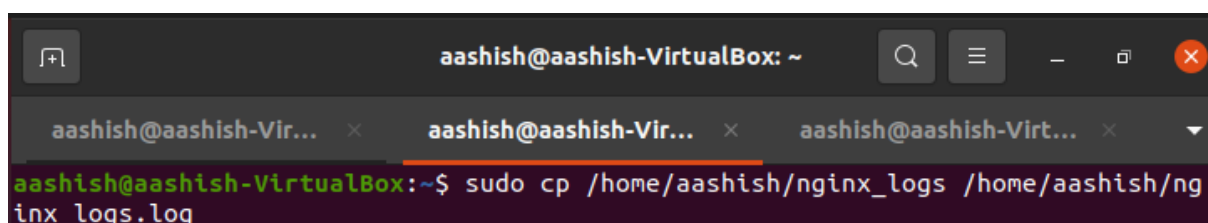
Then, we edit /etc/logstash/logstash.yml file by uncommenting;

- **path.config: /etc/logstash/conf.g**

- **path.data: /var/lib/logstash**

- **path.logs: /var/log/logstash**

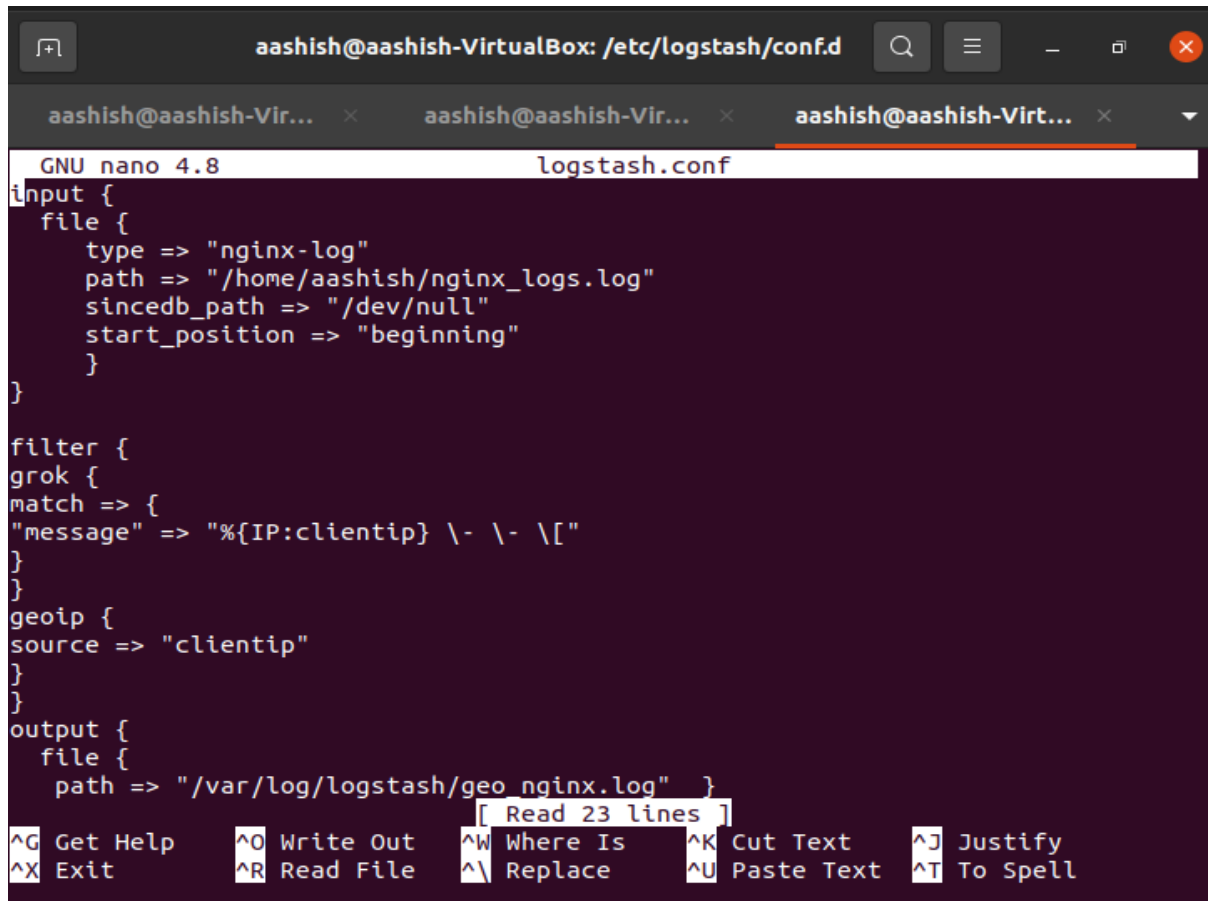
Next, we copied /home/aashish/nginx\_logs to /home/aashish/nginx\_logs.log file as follows;



```
aashish@aashish-VirtualBox: ~  
aashish@aashish-Vir... x aashish@aashish-Vir... x aashish@aashish-Vir... x  
aashish@aashish-VirtualBox:~$ sudo cp /home/aashish/nginx_logs /home/aashish/nginx_logs.log
```

Then, we create logstash configuration file inside `/etc/logstash/conf.d/logstash.conf` as follows;

- **sudo nano /etc/logstash/conf.d/logstash.conf**



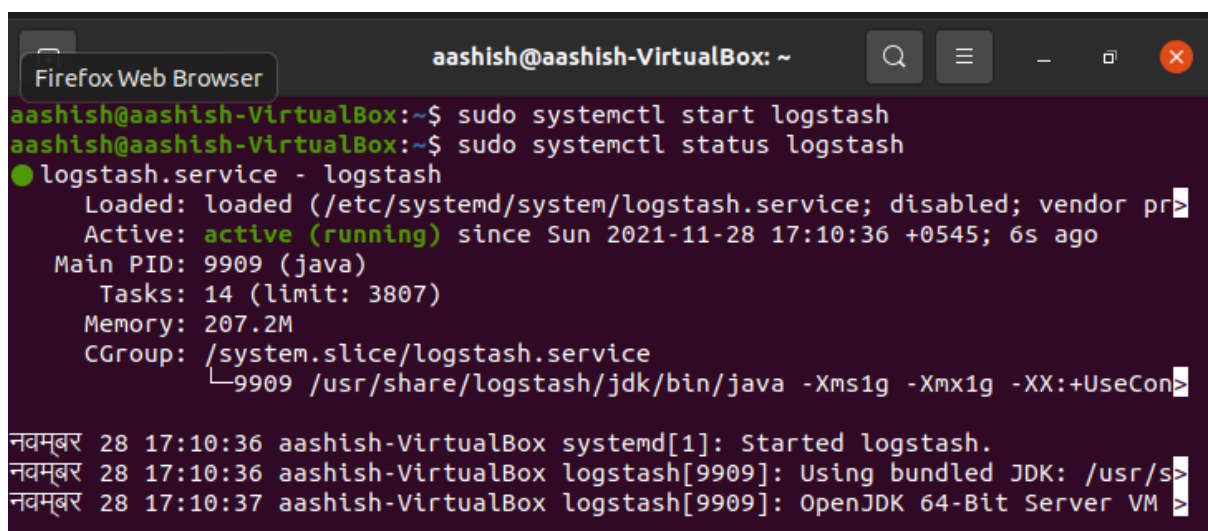
```
GNU nano 4.8 logstash.conf
input {
  file {
    type => "nginx-log"
    path => "/home/aashish/nginx_logs.log"
    sincedb_path => "/dev/null"
    start_position => "beginning"
  }
}

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

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

Next, we restart logstash using the following command;

- **sudo systemctl restart logstash**



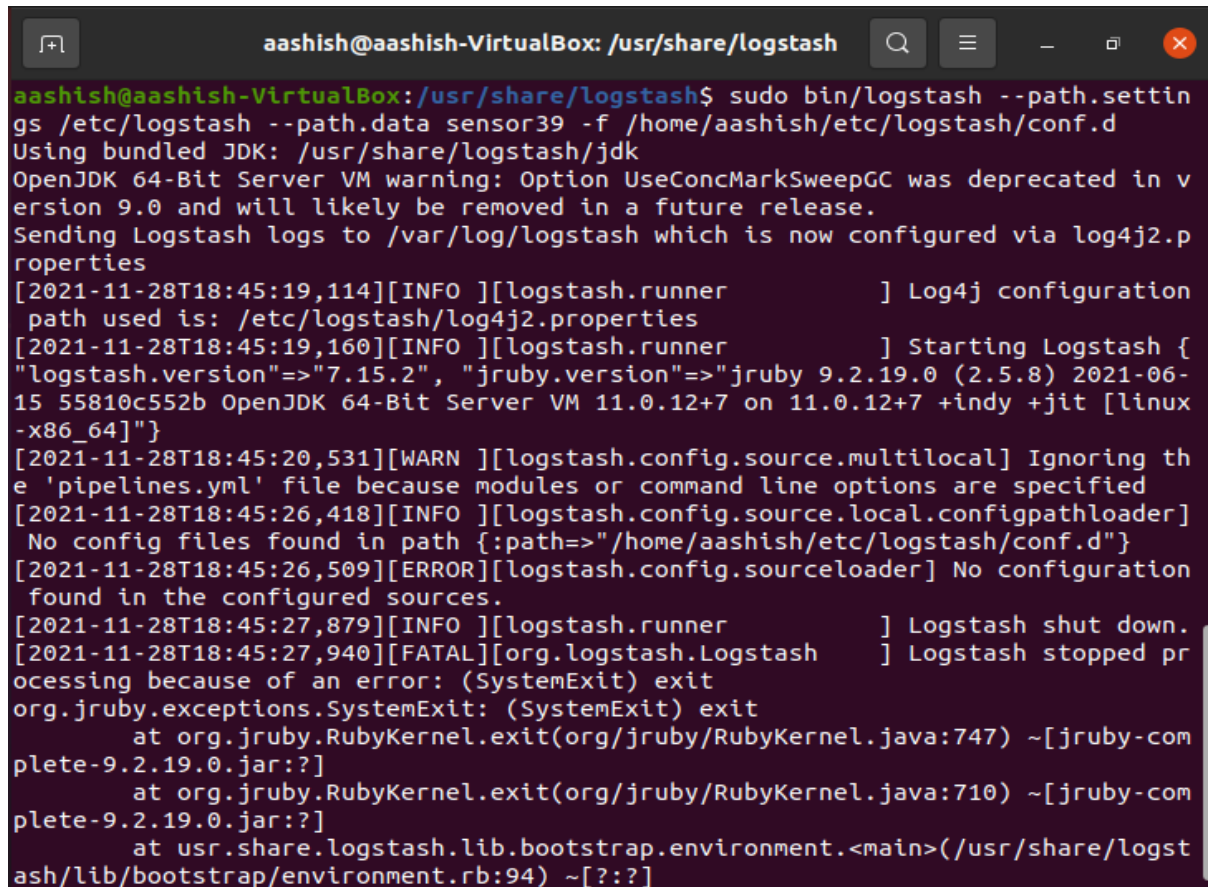
```
aashish@aashish-VirtualBox: ~
aashish@aashish-VirtualBox:~$ sudo systemctl start logstash
aashish@aashish-VirtualBox:~$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor pr>
   Active: active (running) since Sun 2021-11-28 17:10:36 +0545; 6s ago
   Main PID: 9909 (java)
     Tasks: 14 (limit: 3807)
    Memory: 207.2M
    CGroup: /system.slice/logstash.service
            └─9909 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon>

नवम्बर 28 17:10:36 aashish-VirtualBox systemd[1]: Started logstash.
नवम्बर 28 17:10:36 aashish-VirtualBox logstash[9909]: Using bundled JDK: /usr/s>
नवम्बर 28 17:10:37 aashish-VirtualBox logstash[9909]: OpenJDK 64-Bit Server VM >
```



Now, we change the directory to **/usr/share/logstash** and run logstash using the following commands;

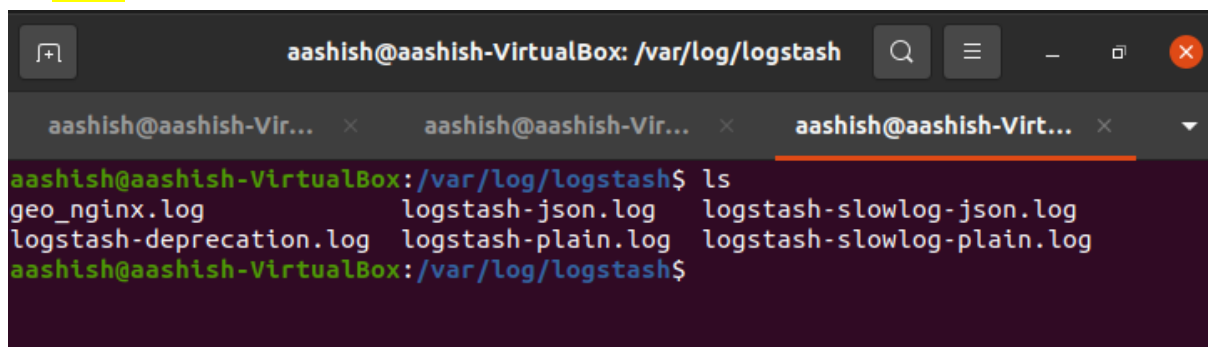
- **cd /usr/share/logstash**
- **sudo bin/logstash --path.settings /etc/logstash --path.data sensor39 -f /home/aashish/etc/logstash/conf.d**



```
aashish@aashish-VirtualBox: /usr/share/logstash
aashish@aashish-VirtualBox:/usr/share/logstash$ sudo bin/logstash --path.settings /etc/logstash --path.data sensor39 -f /home/aashish/etc/logstash/conf.d
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
[2021-11-28T18:45:19,114][INFO ][logstash.runner] Log4j configuration path used is: /etc/logstash/log4j2.properties
[2021-11-28T18:45:19,160][INFO ][logstash.runner] Starting Logstash {"logstash.version"=>"7.15.2", "jruby.version"=>"jruby 9.2.19.0 (2.5.8) 2021-06-15 55810c552b OpenJDK 64-Bit Server VM 11.0.12+7 on 11.0.12+7 +indy +jit [linux-x86_64]"}
[2021-11-28T18:45:20,531][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified
[2021-11-28T18:45:26,418][INFO ][logstash.config.source.local.configpathloader] No config files found in path {:path=>"/home/aashish/etc/logstash/conf.d"}
[2021-11-28T18:45:26,509][ERROR][logstash.config.sourceloader] No configuration found in the configured sources.
[2021-11-28T18:45:27,879][INFO ][logstash.runner] Logstash shut down.
[2021-11-28T18:45:27,940][FATAL][org.logstash.Logstash] Logstash stopped processing because of an error: (SystemExit) exit
org.jruby.exceptions.SystemExit: (SystemExit) exit
    at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:747) ~[jruby-complete-9.2.19.0.jar:?]
    at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:710) ~[jruby-complete-9.2.19.0.jar:?]
    at usr.share.logstash.lib.bootstrap.environment.<main>(/usr/share/logstash/lib/bootstrap/environment.rb:94) ~[?:?]
```

Again, we change the directory to **/var/log/logstash** and list the files as follows;

- **cd /var/log/logstash**
- **ls**



```
aashish@aashish-VirtualBox: /var/log/logstash
aashish@aashish-VirtualBox:/var/log/logstash$ ls
geo_nginx.log          logstash-json.log      logstash-slowlog-json.log
logstash-deprecation.log logstash-plain.log     logstash-slowlog-plain.log
aashish@aashish-VirtualBox:/var/log/logstash$
```

Since, we have named **geo\_nginx.log** to store the generated log file. It was generated successfully as seen from the image above.

To check the file **geo\_nginx.log**, we use;

- **cat geo\_nginx.log**

```
aashish@aashish-VirtualBox: /var/log/logstash
aashish@aashish-Vir... x aashish@aashish-Vir... x aashish@aashish-Virt... x
aashish@aashish-VirtualBox:/var/log/logstash$ cat geo_nginx.log
{"clientip":"93.180.71.3","type":"nginx-log","message":"93.180.71.3 - - [17/May
/2015:08:05:32 +0000] \"GET /downloads/product_1 HTTP/1.1\" 304 0 \"-\" \"Debia
n APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)\"","@timestamp":"2021-11-28T13:00:29.4
85Z","path":"/home/aashish/nginx_logs.log","@version":"1","host":"aashish-Virtu
alBox","geoip":{"country_code3":"NL","ip":"93.180.71.3","continent_code":"EU","
country_name":"Netherlands","timezone":"Europe/Amsterdam","country_code2":"NL",
"latitude":52.3824,"location":{"lat":52.3824,"lon":4.8995},"longitude":4.8995}}
{"clientip":"93.180.71.3","type":"nginx-log","message":"93.180.71.3 - - [17/May
/2015:08:05:23 +0000] \"GET /downloads/product_1 HTTP/1.1\" 304 0 \"-\" \"Debia
n APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)\"","@timestamp":"2021-11-28T13:00:29.5
53Z","path":"/home/aashish/nginx_logs.log","@version":"1","host":"aashish-Virtu
alBox","geoip":{"country_code3":"NL","ip":"93.180.71.3","continent_code":"EU","
country_name":"Netherlands","timezone":"Europe/Amsterdam","country_code2":"NL",
"latitude":52.3824,"location":{"lat":52.3824,"lon":4.8995},"longitude":4.8995}}
{"clientip":"80.91.33.133","type":"nginx-log","message":"80.91.33.133 - - [17/M
```