

Installation of ELK (Elasticsearch, Logstash, Kibana)

Step1:

```
sudo su
apt-get install openjdk-8-jdk
```

Step2:

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

Step3:

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

Step4:

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

Step5:

```
apt-get install elasticsearch
```

Step6:

```
apt-get install vim
vim /etc/elasticsearch/elasticsearch.yml
```

Edit: Uncomment and put Ur private id:
network.host: private Ip (its Ur private Ip)
http.port: 9200
discovery.seed_hosts: private Ip (its Ur private IP)

```
root@ip-172-31-34-157: /etc/elasticsearch
----- Network -----
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
network.host: 172.31.34.157
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
http.port: 9200
# For more information, consult the network module documentation.
----- Discovery -----
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", ":[::1]"]
discovery.seed_hosts: ["host1", "host2"]
# Bootstrap the cluster using an initial set of master-eligible nodes:
cluster.initial_master_nodes: ["node-1", "node-2"]
# Single node Elastic stack:
discovery.type: single-node
# For more information, consult the discovery and cluster formation module documentation.
----- Various -----
# Require explicit names when deleting indices:
action.destructive_requires_name: true
----- Security -----
*** WARNING ***
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access
# to the cluster. Network connections are also not encrypted.
# To protect your data, we strongly encourage you to enable the Elasticsearch security features.
# Refer to the following documentation for instructions.
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html
```

Step7: Go to

```
vim /etc/elasticsearch/jvm.options(This is to give the size of JVM)
edit:
-Xms512m
-Xmx512m
```

```
#####
##
## JVM configuration
##
#####
## WARNING: DO NOT EDIT THIS FILE. If you want to override the
## JVM options in this file, or set any additional options, you
## should create one or more files in the jvm.options.d
## directory containing your adjustments.
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
## for more information.
##
#####

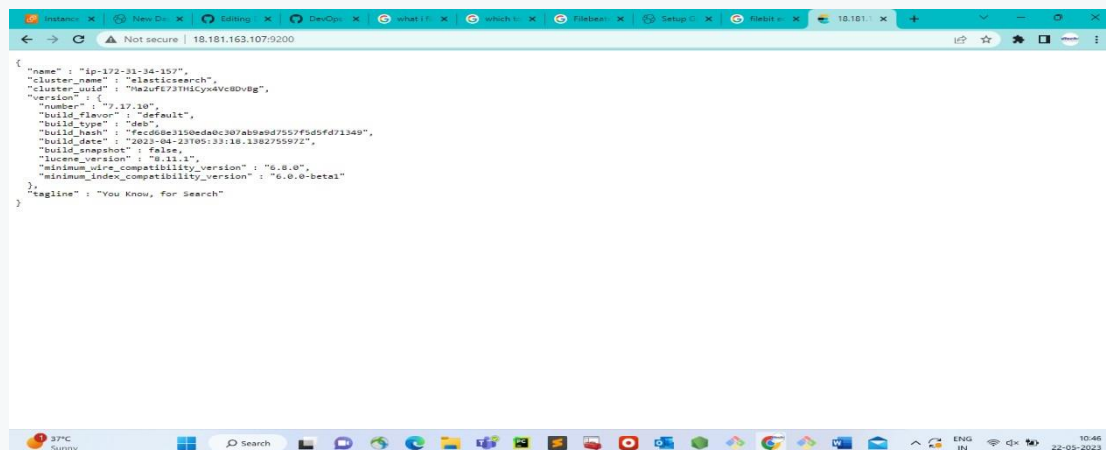
#####
## IMPORTANT: JVM heap size
#####
##
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
##
#####
-Xms512m
-Xmx512m
#####
## Expert settings
#####
##
## All settings below here are considered expert settings. Do
## not adjust them unless you understand what you are doing. Do
## not edit them in this file; instead, create a new file in the
## jvm.options.d directory containing your adjustments.
```

Step8:

```
systemctl start elasticsearch.service
systemctl enable elasticsearch.service
```

Step9:

```
curl -X GET "172.31.34.157:9200"
(or)
ip:9200 (in web)
```



To run the elastic server automatic whenever server starts:

go to

```
cd /systemd/system
touch elastic.service
vim elastic.service
paste below code:
[Unit]
Description=Elasticsearch
Documentation=https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
Wants=network-online.target
After=network-online.target

[Service]
Type=simple
User=elasticsearch
Group=elasticsearch
ExecStart=/usr/share/elasticsearch/bin/elasticsearch
Restart=always
RestartSec=10
StartLimitInterval=0
LimitMEMLOCK=infinity

[Install]
WantedBy=multi-user.target
```

Installation of Kibana on Ubuntu:

Step1:

```
apt-get install kibana
vim /etc/kibana/kibana.yml
```

Step2:

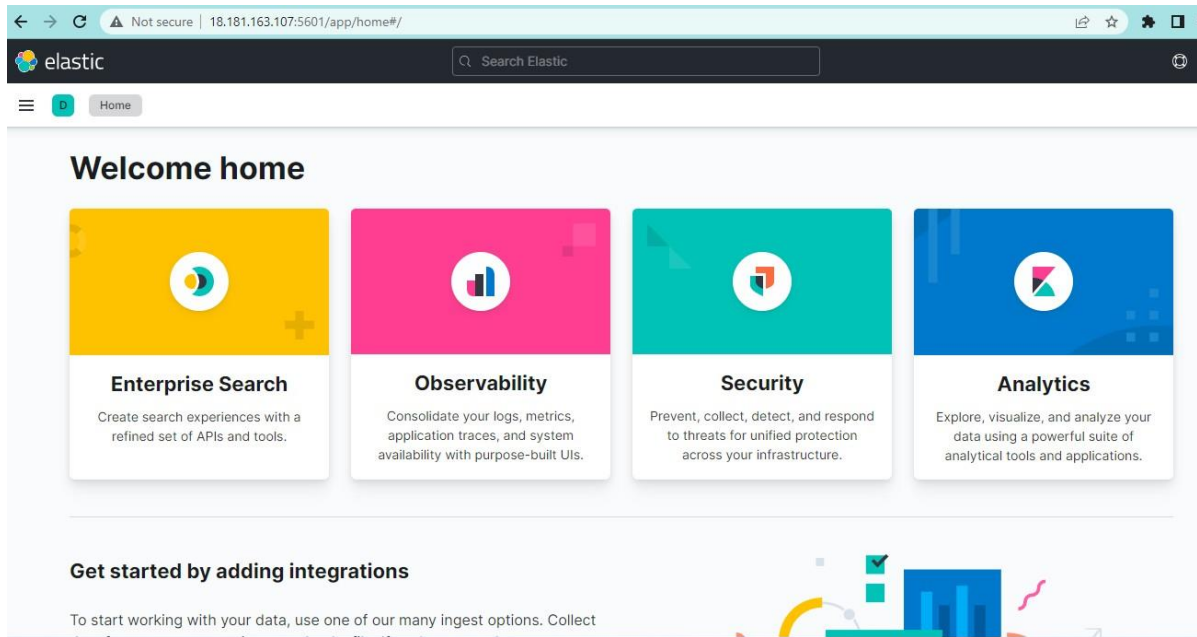
```
Edit:
server.port: 5601
server.host: "private ip"
elasticsearch.hosts: ["http://privateip:9200"]
```

Step3:

```
systemctl start kibana
systemctl enable kibana
```

Step4:

```
allow traffic on port 5601 to access the Kibana dashboard.
ufw allow 5601/tcp
```



Installation of Logstash on Ubuntu:

Installation of Logstash on Ubuntu:

Step1:

```
apt-get install logstash
systemctl start logstash
systemctl enable logstash
systemctl status logstash
```

Step2:

Logstash is a highly customizable part of the ELK stack. Once installed, configure its INPUT, FILTERS, and OUTPUT pipelines according to your own individual use case.

- All logstash files will be stored in:
/etc/logstash/conf.d/.
- Logstash Process:
input-->filter-->output
- apt-get install filebeat

Step3:

```
vim /etc/filebeat/filebeat.yml
Edit:
    output.logstash
    hosts: ["privateip:5044"]
```

Step4:

* What is Filebeat?

```
filebeat modules enable system

one cmd: [ filebeat setup --index-management -E
output.logstash.enabled=false

-E 'output.elasticsearch.hosts=
["172.31.34.157:9200"]' ]
```

```
systemctl start filebeat
systemctl enable filebeat
```

Step5:

```
curl -XGET http://172.31.34.157:9200/\_cat/indices?v
```

Install Connecting the nginx to apache tomcat:

- apt install nginx
- cd /etc/nginx
- vim nginx.conf


```
• then comment 404 all that files
server {
    listen 80;
    server_name 18.216.96.3;(tomcat public id)
    location / {
        proxy_pass http://18.216.96.3:8080/;((tomcat public link)
    }
}
then save & systemctl start nginx
```

← → 🔒 Not secure | 52.193.191.63

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.75

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [First Web Application](#)
- [Realms & AAA](#)
- [JDBC DataSources](#)
- [Examples](#)
- [Servlet Specifications](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. [Read more...](#)

Documentation

[Tomcat 9.0 Documentation](#)
[Tomcat 9.0 Configuration](#)
[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/bin/README.txt
```

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).
- [tomcat-users](#)
User support and discussion