ELK:

Client(output) < webserver(app < php) < record(log) < data(info) < file < storage

- Audit

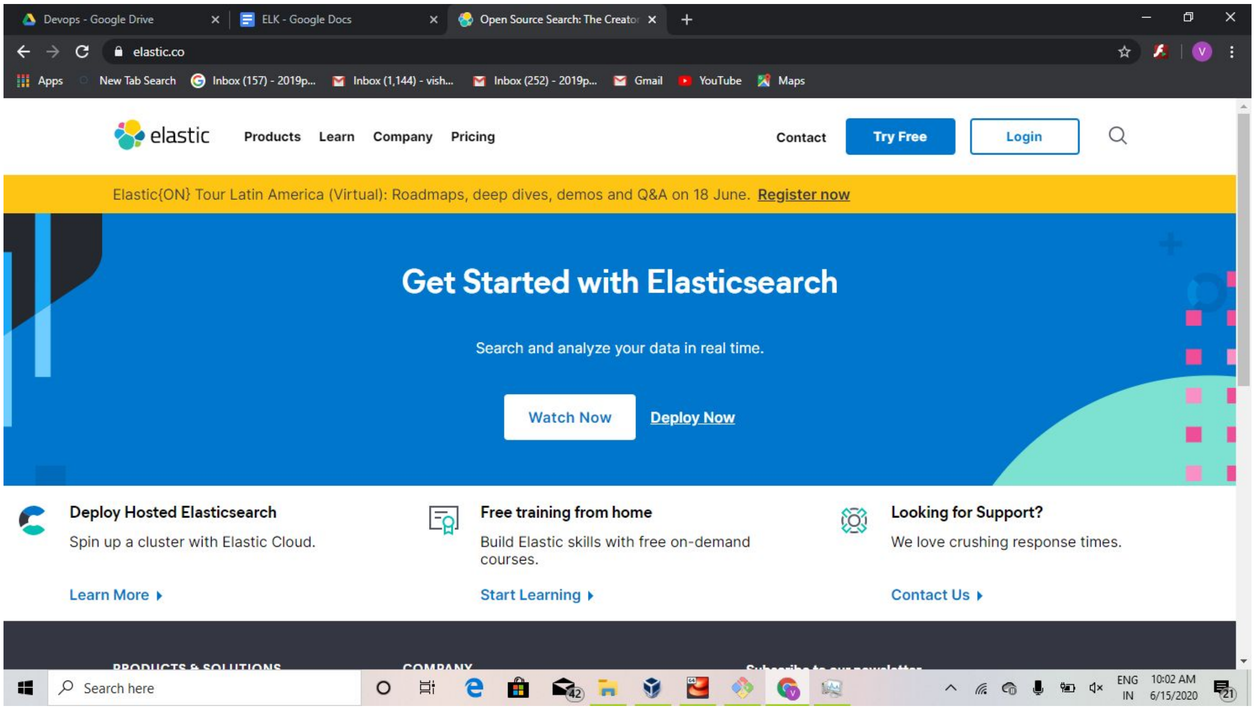
ELK stores data in a database (in form of files)

Prometheus stores in form of metrics

K stands for kibana

L for log stash

E for elastic search



Elastic{ON} Tour Latin America (Virtual): Roadmaps, deep dives, demos and Q&A on 18 June. Register now

Get Started with Elasticsearch

Search and analyze your data in real time.

Deploy Hosted Elasticsearch

Spin up a cluster with Elastic Cloud.

Free training from home

Build Elastic skills with free on-demand courses.

Looking for Support?

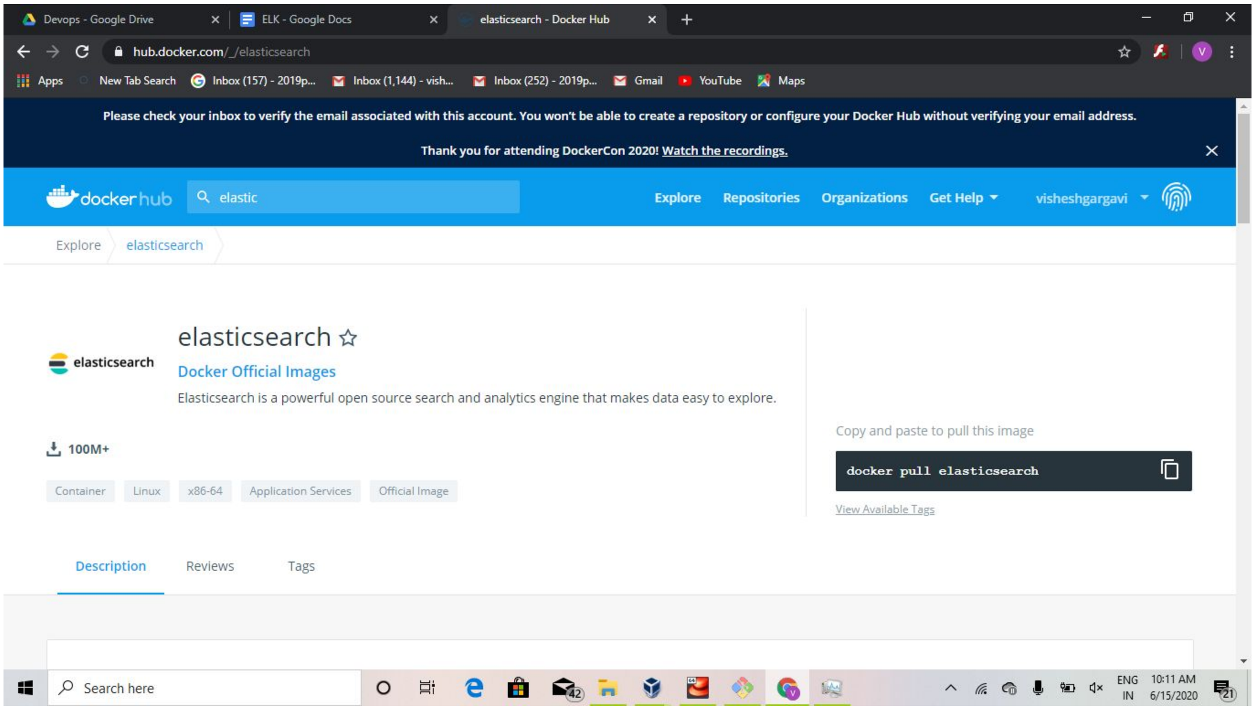
We love crushing response times.

{increase the ram in redhat to 4-8 gb }

Log stash is known as collector

init 0 (helps to reboot system(redhat))

Cpu - 2



Please check your inbox to verify the email associated with this account. You won't be able to create a repository or configure your Docker Hub without verifying your email address.

Thank you for attending DockerCon 2020! Watch the recordings.

elasticsearch ☆

Docker Official Images

Elasticsearch is a powerful open source search and analytics engine that makes data easy to explore.

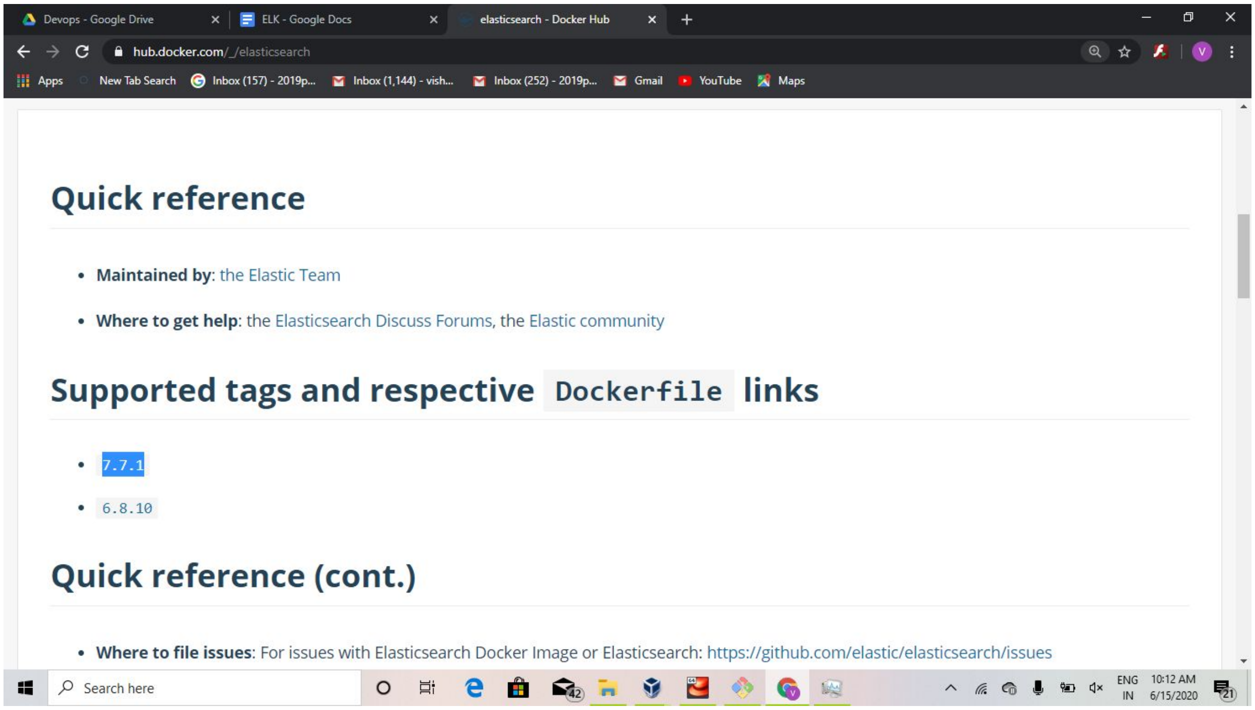
100M+

Container | Linux | x86-64 | Application Services | Official Image

Copy and paste to pull this image

```
docker pull elasticsearch
```

View Available Tags



Quick reference

- **Maintained by**: the Elastic Team
- **Where to get help**: the Elasticsearch Discuss Forums, the Elastic community

Supported tags and respective `Dockerfile` links

- `7.7.1`
- `6.8.10`

Quick reference (cont.)

- **Where to file issues**: For issues with Elasticsearch Docker Image or Elasticsearch: https://github.com/elastic/elasticsearch/issues

```
[root@localhost ~]# docker pull elasticsearch:7.7.1
7.7.1: Pulling from library/elasticsearch
Digest:
sha256:dff614393a31b93e8bbe9f8d1a77be041da37eac2a7a9567166dd5a2abab7c67
Status: Image is up to date for elasticsearch:7.7.1
docker.io/library/elasticsearch:7.7.1
```

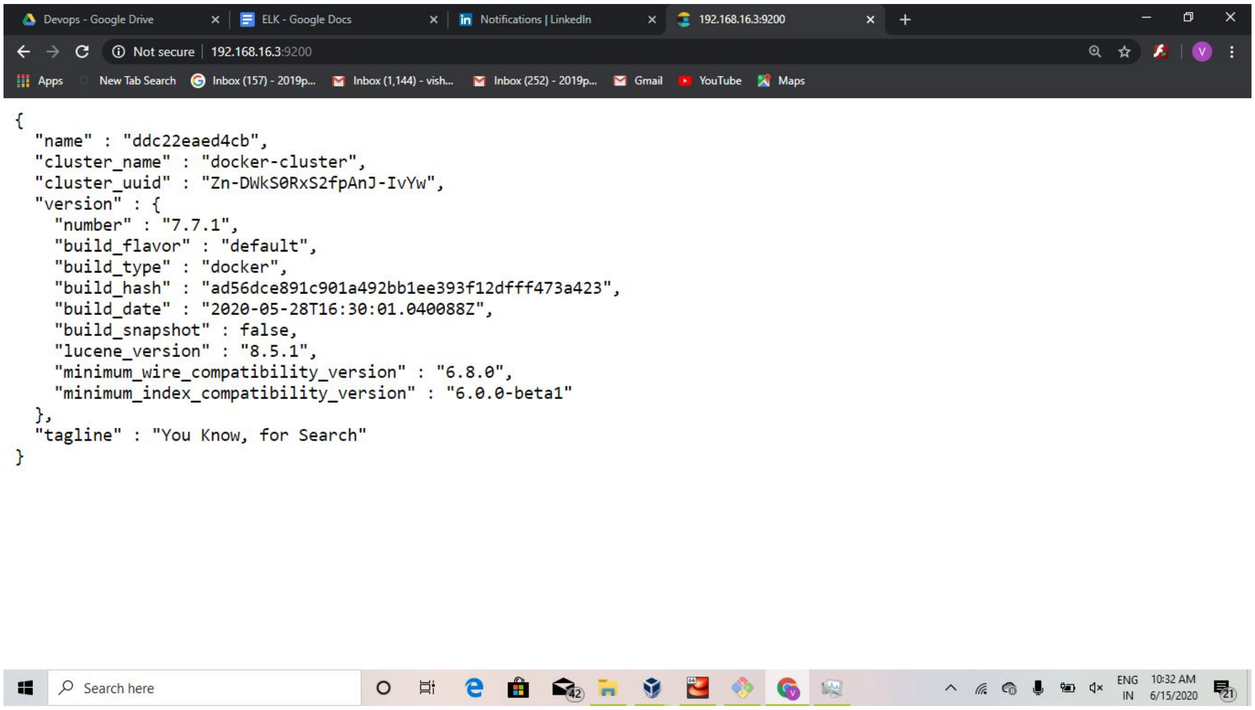
```
[root@localhost ~]# docker network ls
NETWORK ID          NAME                DRIVER              SCOPE
70c37f366ca4        bridge              bridge              local
251e7a1265a7        host                host                local
23c3b1608a33        none                null                local
[root@localhost ~]# docker network create elknetwork
603d9d7cbe8159952f711c01f0d2f6c499333880471b45f2deeab64d91e32da5
```

{Elastic search work on port no. 9200}

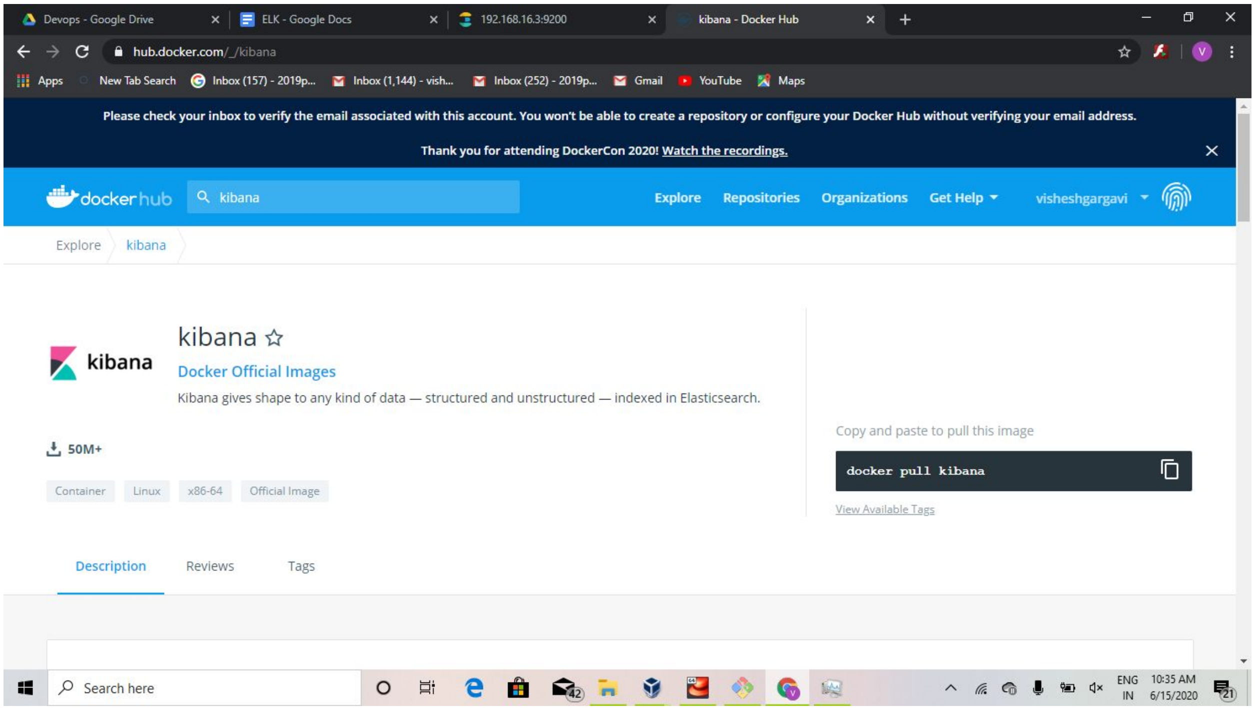
```
[root@localhost ~]# docker run -dit --name elasticsearch --net elknetwork  -p
9200:9200 -p 9300:9300 -e "discovery.type=single-node" elasticsearch:7.7.1
102c10256f0de1052ddcf34b01c8********c5bfe232d1f74de03d7f67f47
```

{Slave connects with (9300) master
And when master connects with client(9200)}

```
[root@localhost ~]# docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS                        PORTS
NAMES
ddc22eaed4cb        elasticsearch:7.7.1   "/tini -- /usr/local…"   About a minute ago   Up About a minute
0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp   elasticsearch
d4645fd28fca        httpd               "httpd-foreground"       17 hours ago         Exited (255) About an hour ago   80/tcp
myos1
b84f55cf8ed9        centos:7            "/bin/bash"              8 days ago           Exited (0) 8 days ago
myos
```



```
{
  "name" : "ddc22eaed4cb",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "Zn-DWkS0RxS2fpAnJ-IvYw",
  "version" : {
    "number" : "7.7.1",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "ad56dce891c901a492bb1ee393f12dfff473a423",
    "build_date" : "2020-05-28T16:30:01.040088Z",
    "build_snapshot" : false,
    "lucene_version" : "8.5.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```



Please check your inbox to verify the email associated with this account. You won't be able to create a repository or configure your Docker Hub without verifying your email address.

Thank you for attending DockerCon 2020! Watch the recordings.

kibana ☆

Docker Official Images

Kibana gives shape to any kind of data — structured and unstructured — indexed in Elasticsearch.

50M+

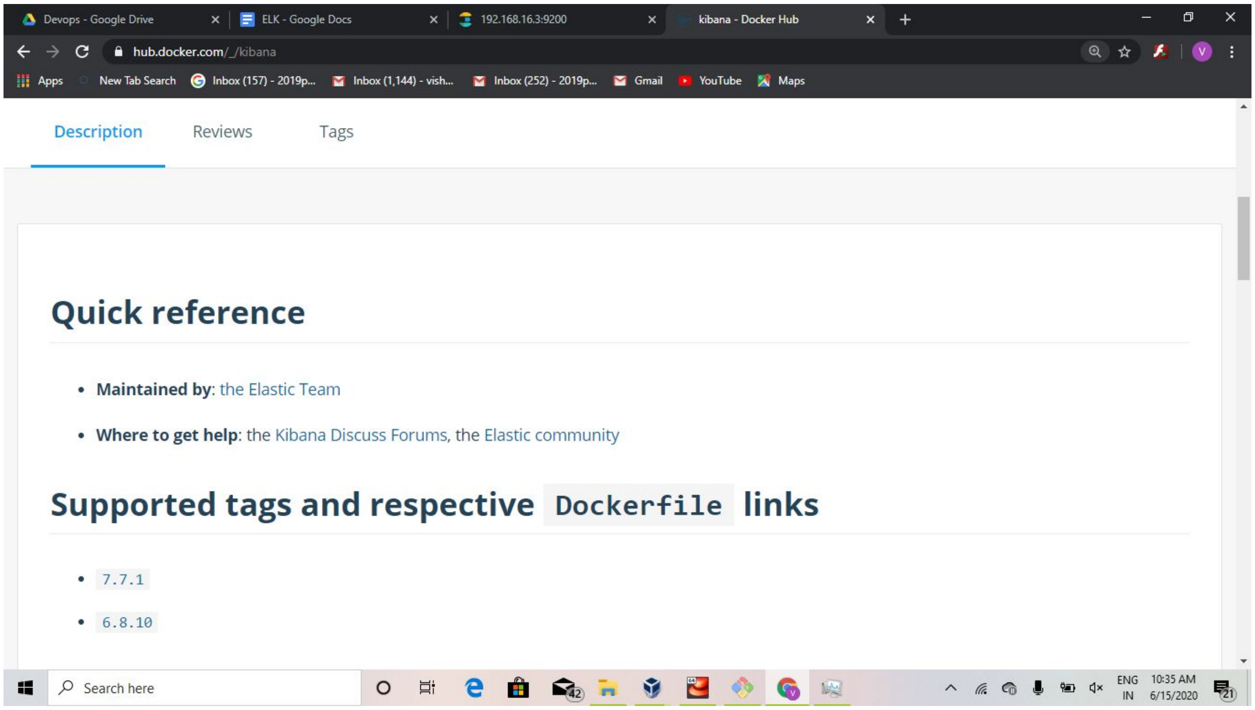
Container | Linux | x86-64 | Official Image

Copy and paste to pull this image

```
docker pull kibana
```

View Available Tags

Description | Reviews | Tags



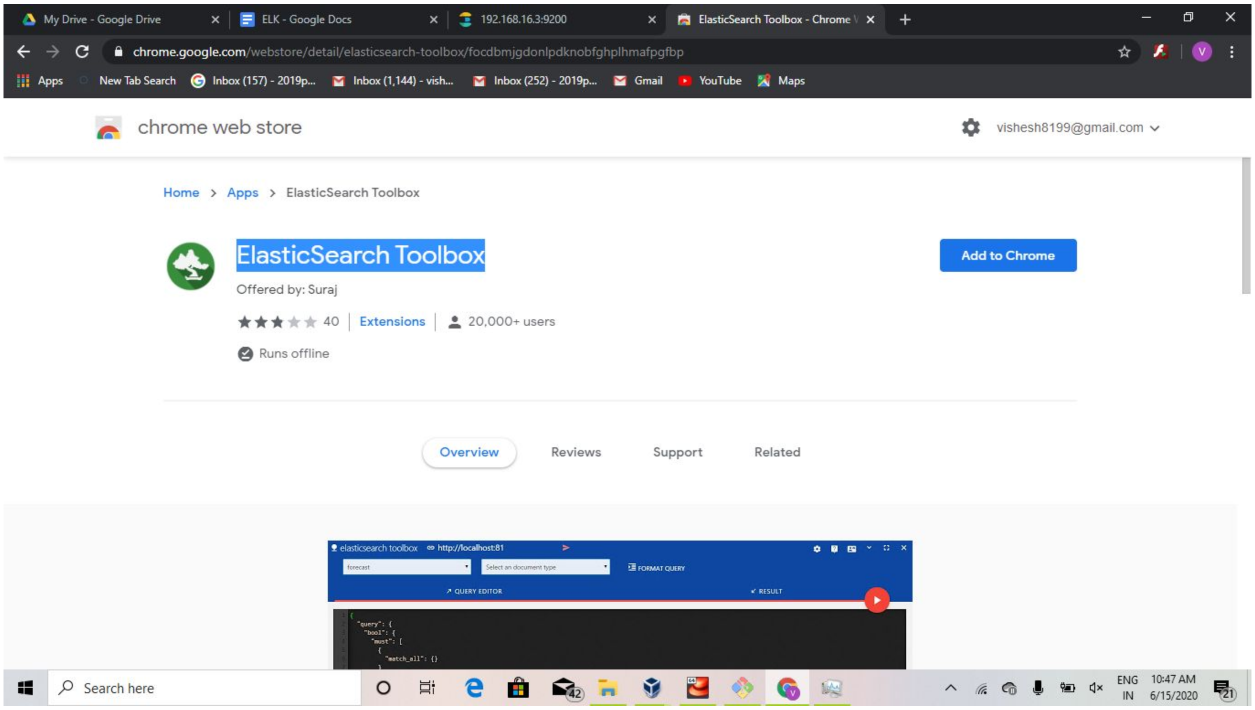
Quick reference

- **Maintained by**: the Elastic Team
- **Where to get help**: the Kibana Discuss Forums, the Elastic community

Supported tags and respective `Dockerfile` links

- `7.7.1`
- `6.8.10`

```
[root@localhost ~]# docker pull kibana:7.7.1
7.7.1: Pulling from library/kibana
524b0c1e57f8: Already exists
103dc10f20b6: Pull complete
e397e023efd5: Pull complete
f0ee6620405c: Pull complete
[root@localhost ~]# docker ps
CONTAINER ID        IMAGE                 COMMAND                  CREATED
STATUS              PORTS                                            NAMES
ddc22eaed4cb        elasticsearch:7.7.1   "/tini -- /usr/local…"   11 minutes ago      Up 11
minutes       0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp   elasticsearch
[root@localhost ~]# curl 192.168.16.3:9200
{
  "name" : "ddc22eaed4cb",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "Zn-DWkS0RxS2fpAnJ-IvYw",
  "version" : {
    "number" : "7.7.1",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "ad56dce891c901a492bb1ee393f12dfff473a423",
    "build_date" : "2020-05-28T16:30:01.040088Z",
    "build_snapshot" : false,
    "lucene_version" : "8.5.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
[root@localhost ~]# curl 192.168.16.3:9200/_cat
=^.^=
/_cat/allocation
/_cat/shards
/_cat/shards/{index}
/_cat/aliases/{alias}
/_cat/thread_pool
/_cat/thread_pool/{thread_pools}
/_cat/plugins
/_cat/fielddata
/_cat/fielddata/{fields}
[root@localhost ~]# curl 192.168.16.3:9200/_cat/master
a3Suuv9DS1ahJnSbiFxu9w 172.18.0.2 172.18.0.2 ddc22eaed4cb
[root@localhost ~]# curl 192.168.16.3:9200/_cat/nodes
172.18.0.2 33 97 16 0.34 1.07 0.80 dilmrt * ddc22eaed4cb
[root@localhost ~]# curl 192.168.16.3:9200/_cat/indices
```



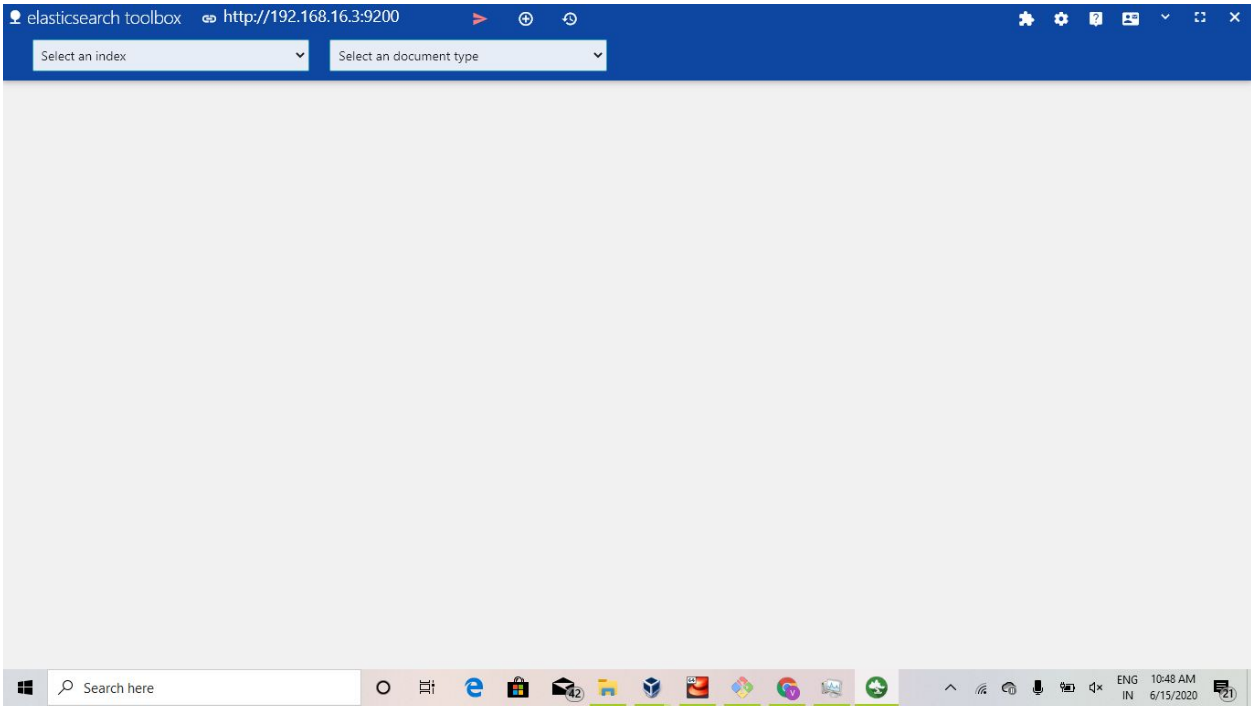
chrome.google.com/webstore/detail/elasticsearch-toolbox/focdbmjgdonlpdknobfghplhmafpgfbp

ElasticSearch Toolbox

Offered by: Suraj

40 | Extensions | 20,000+ users

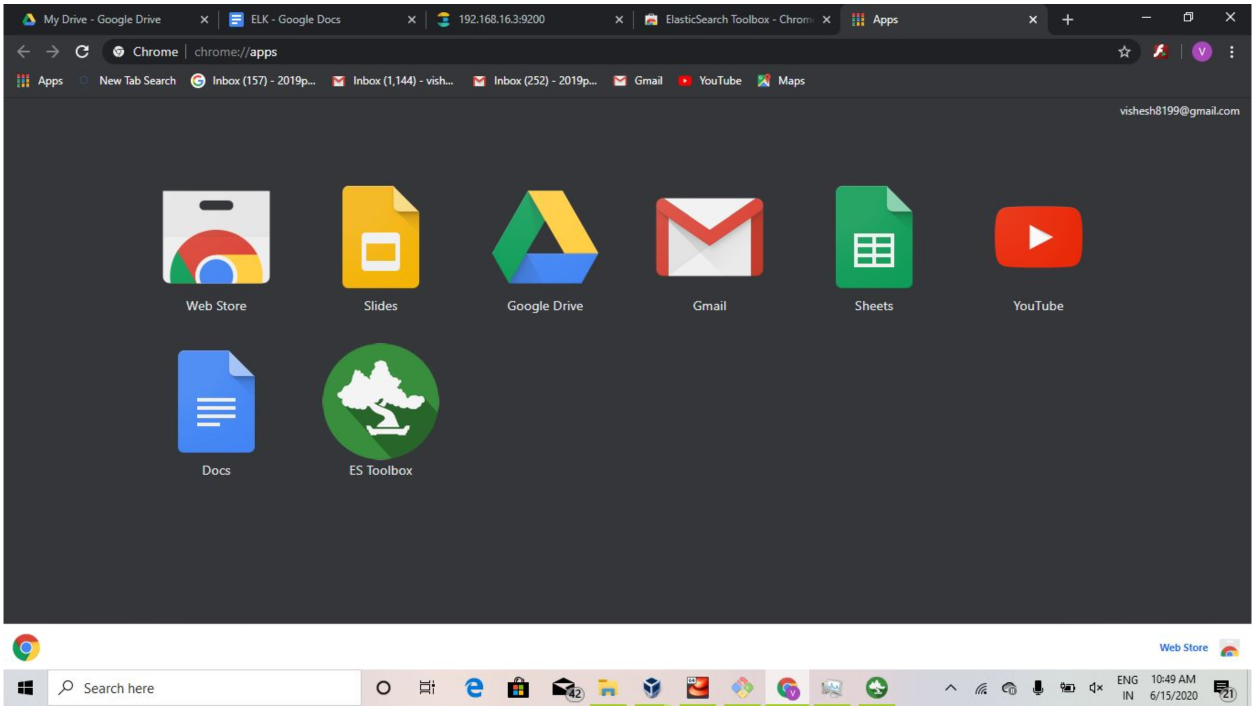
Runs offline

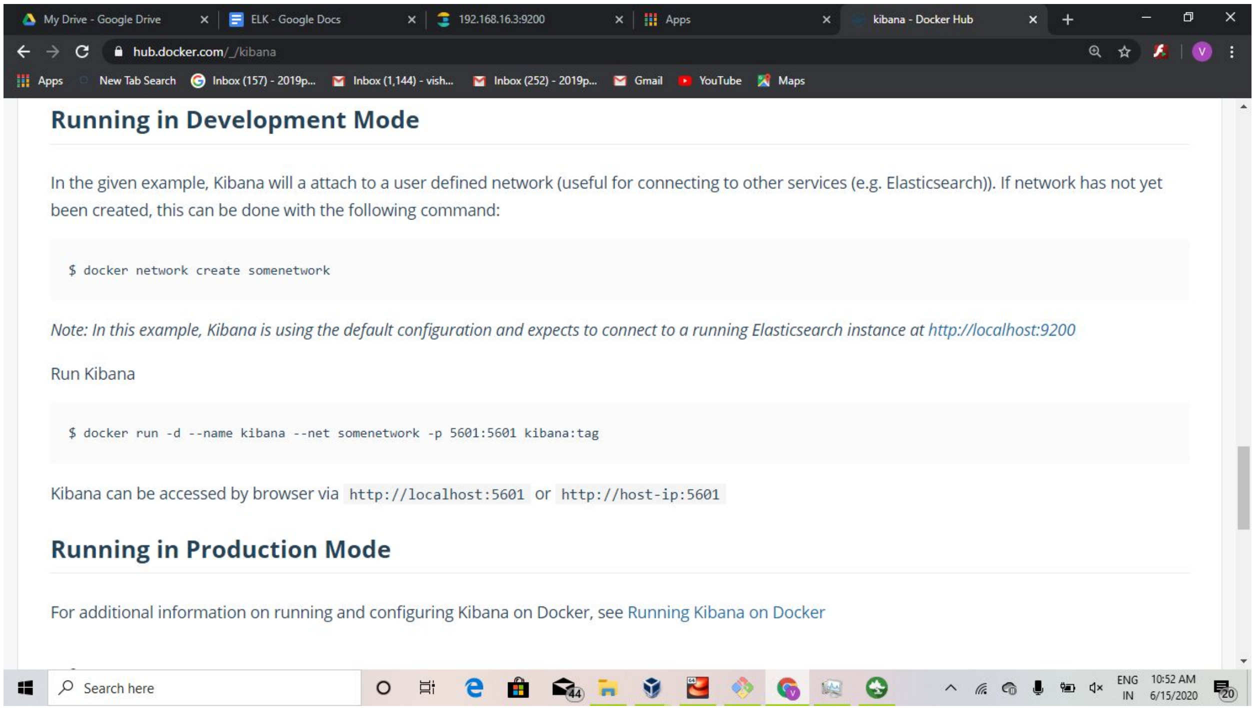


http://192.168.16.3:9200

Select an index

Select an document type





Running in Development Mode

In the given example, Kibana will a attach to a user defined network (useful for connecting to other services (e.g. Elasticsearch)). If network has not yet been created, this can be done with the following command:

```
$ docker network create somenetwork
```

Note: In this example, Kibana is using the default configuration and expects to connect to a running Elasticsearch instance at http://localhost:9200

Run Kibana

```
$ docker run -d --name kibana --net somenetwork -p 5601:5601 kibana:tag
```

Kibana can be accessed by browser via `http://localhost:5601` or `http://host-ip:5601`

Running in Production Mode

For additional information on running and configuring Kibana on Docker, see Running Kibana on Docker

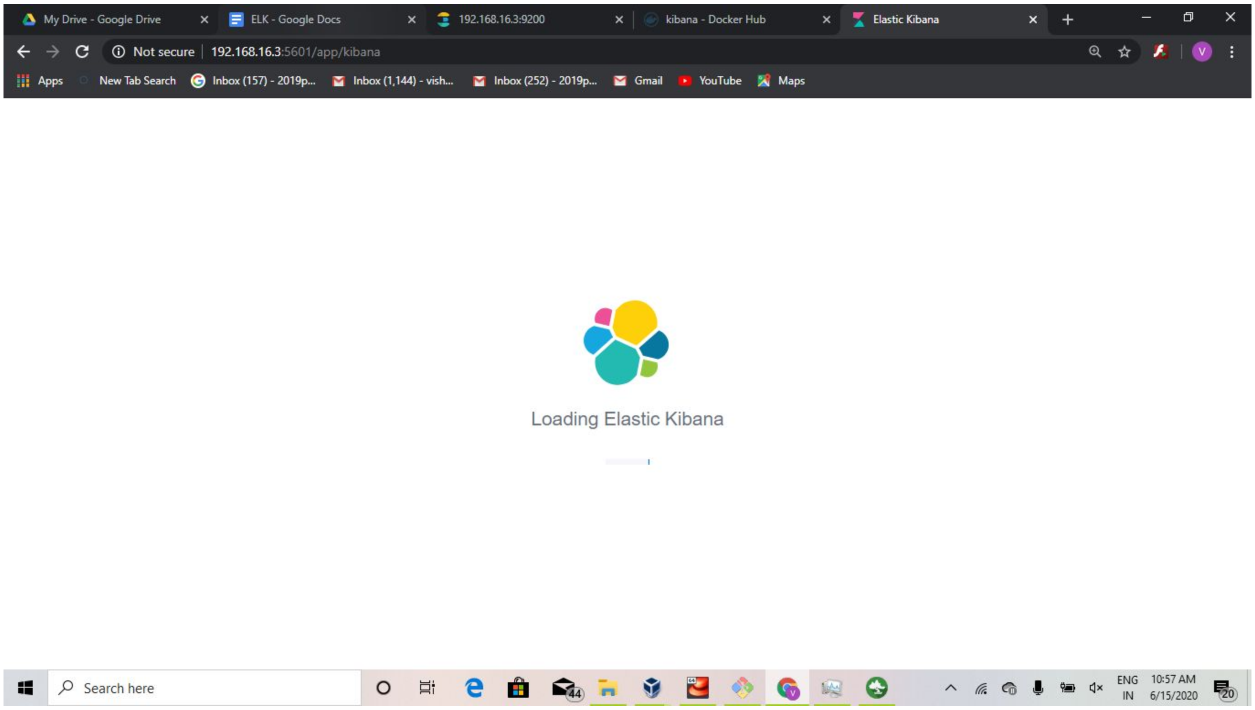
[root@localhost ~]# docker run -dit --name kibana --net elknetwork -p 5601:5601 kibana:7.7.1

660a43510de084e0a715cf822a0420b******5b3d6b7e817b561d7e5e69e5f

[root@localhost ~]# free -m

```
              total        used        free      shared  buff/cache   available
Mem:           3832        2680         154           6         998         865
Swap:          2119          64        2055
```

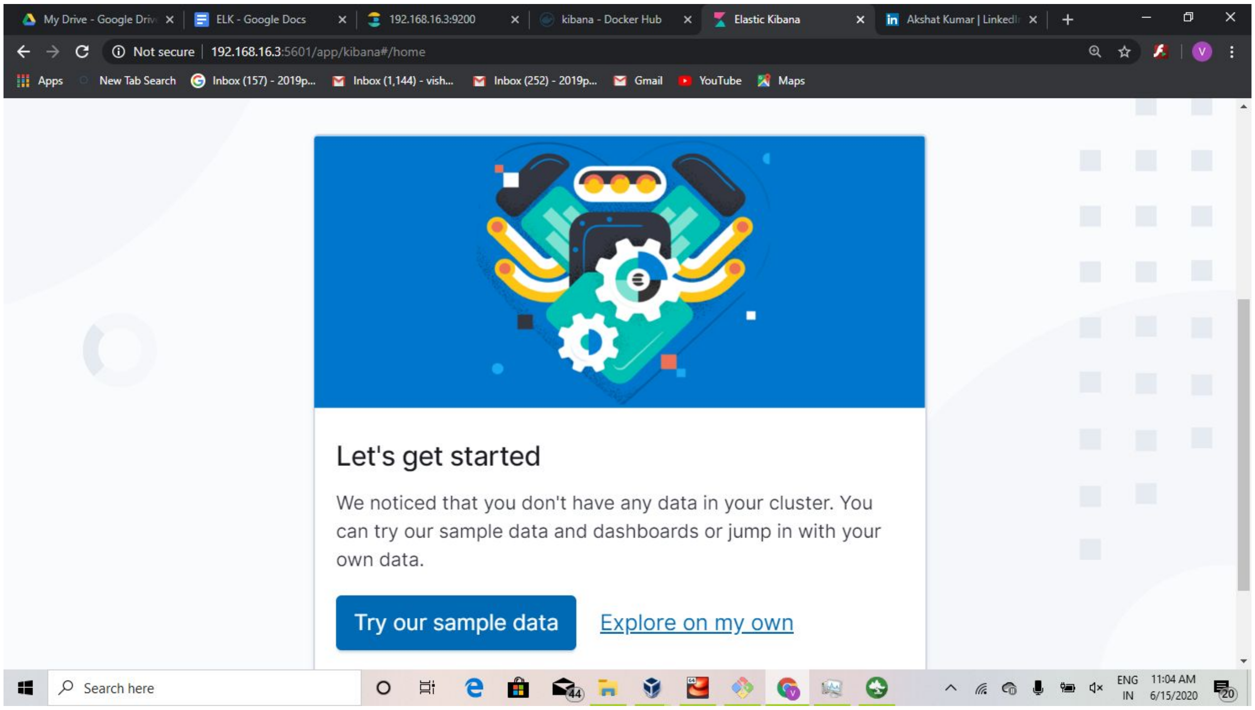
```
[root@localhost ~]# cat /proc/sys/vm/drop_caches
0
[root@localhost ~]# echo 3 > /proc/sys/vm/drop_caches
[root@localhost ~]# cat /proc/sys/vm/drop_caches
3
[root@localhost ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:           3832        2883         679           5         270         724
Swap:          2119          69        2050
```



Loading Elastic Kibana

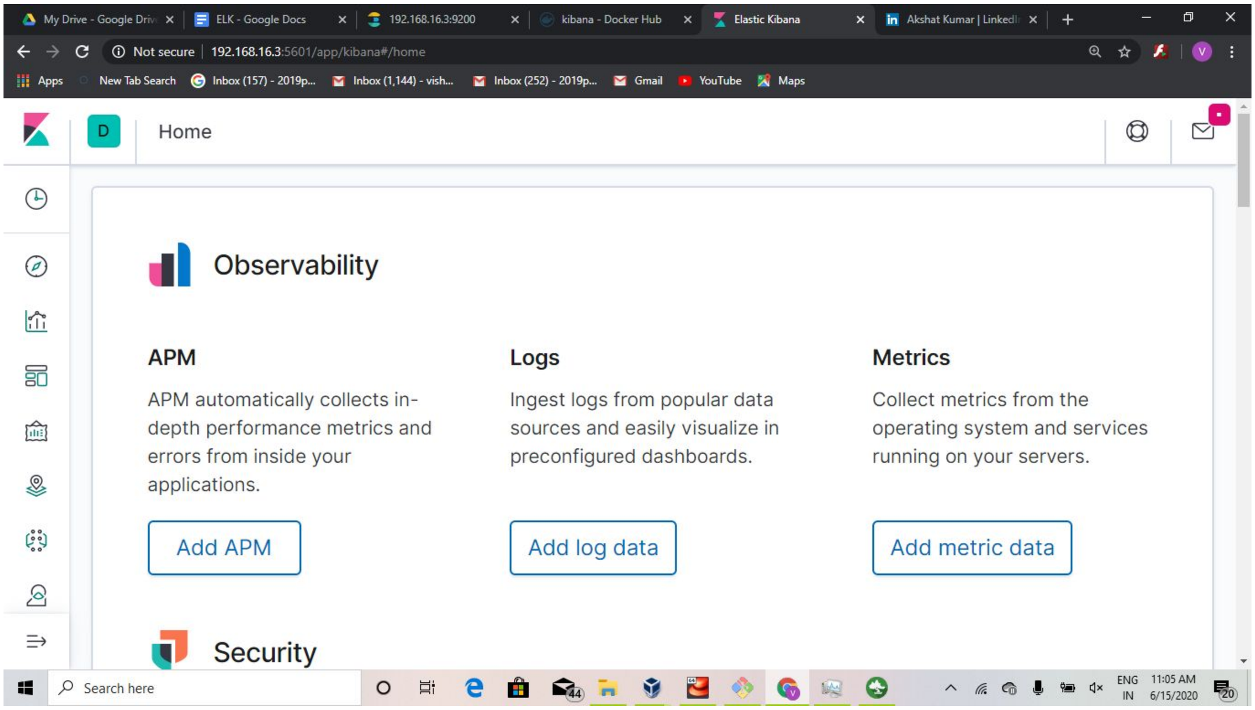
```
[root@localhost ~]# docker ps
CONTAINER ID        IMAGE                 COMMAND                  CREATED
STATUS              PORTS                                            NAMES
660a43510de0        kibana:7.7.1          "/usr/local/bin/dumb…"   2 minutes ago       Up 2
minutes        0.0.0.0:5601->5601/tcp                              kibana
ddc22eaed4cb        elasticsearch:7.7.1   "/tini -- /usr/local…"   26 minutes ago      Up 26
minutes       0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp   elasticsearch
[root@localhost ~]# curl 192.168.16.3:9200/_cat/indices
green open .apm-custom-link          aImMuKMMRxOu6a5SOyXH2A 1 0  0   208b
208b
green open .kibana_task_manager_1   WHwsq46pQ2q3_dFPkozIAg 1 0 5 13 57.7kb
57.7kb
```

```
green open .apm-agent-configuration d_aB0q9IRZWB8UUq1gDS-Q 1 0 0  0   208b
208b
green open .kibana_1               1mZ_rmTKRdmENeNS58SAeQ 1 0 5  1 42.6kb 42.6kb
```



Let's get started

We noticed that you don't have any data in your cluster. You can try our sample data and dashboards or jump in with your own data.



Observability

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

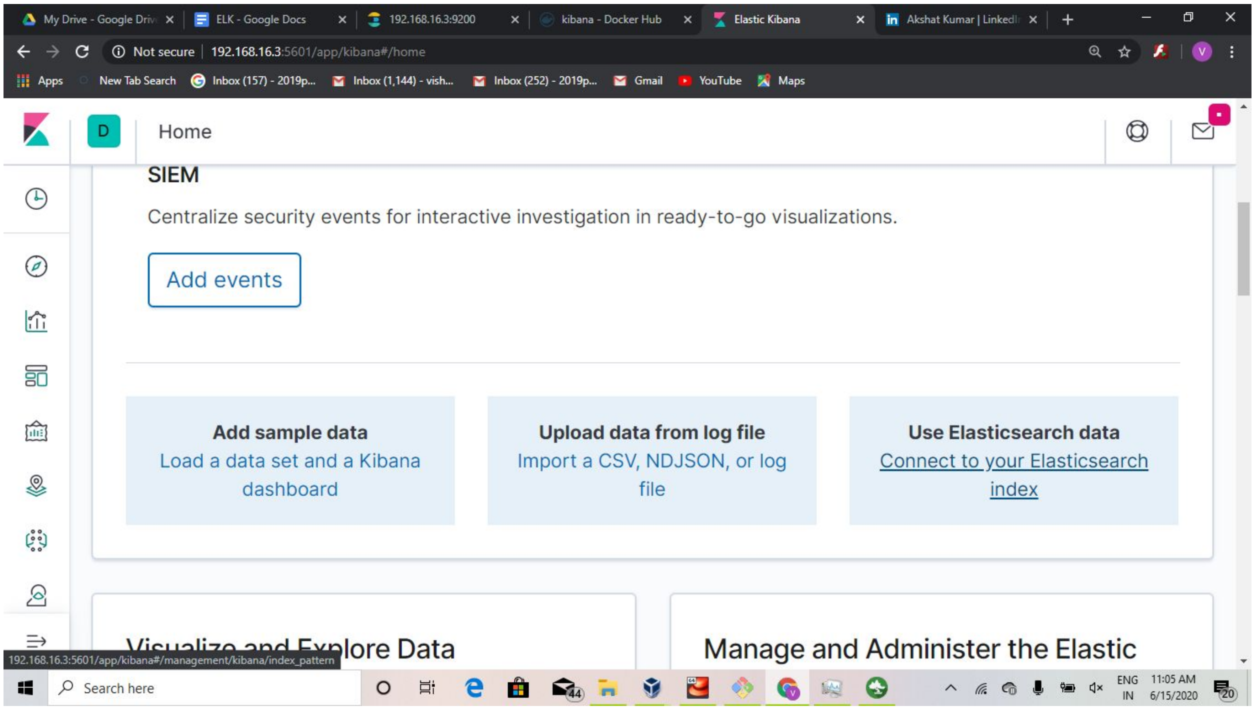
Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

Security



SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add events

Add sample data
Load a data set and a Kibana dashboard

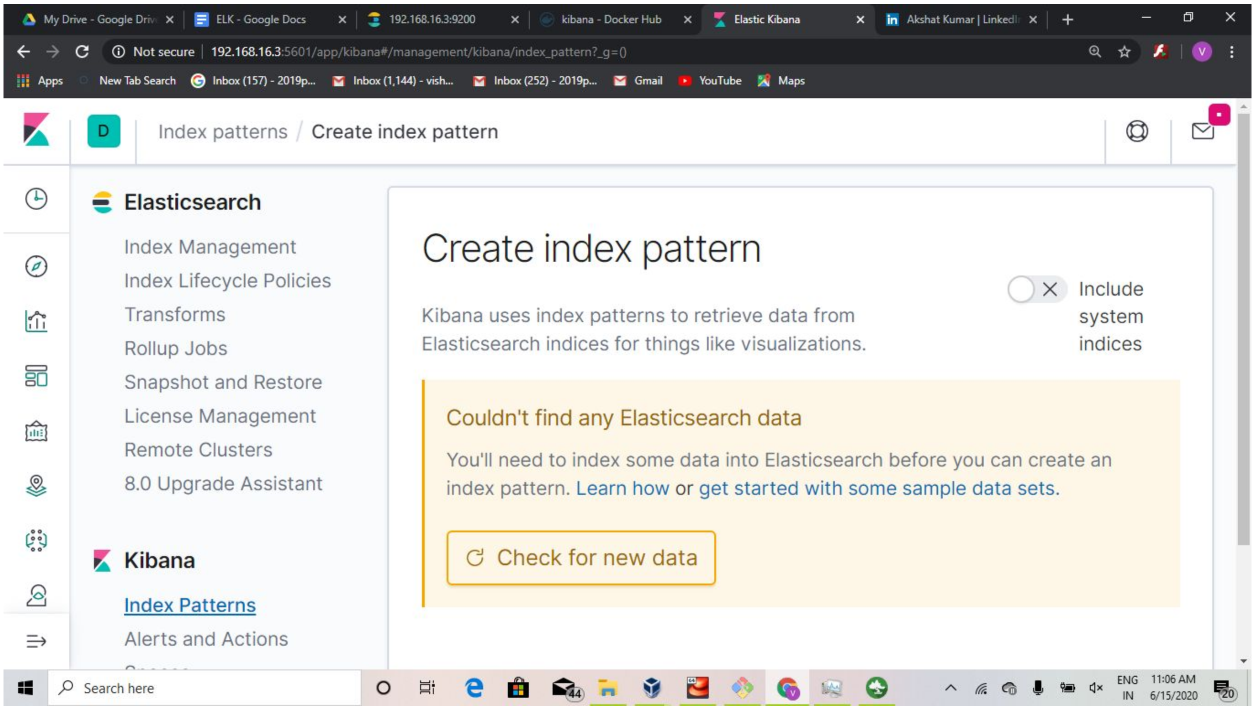
Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Manage and Administer the Elastic

192.168.16.3:5601/app/kibana#/management/kibana/index_pattern
Search here
ENG
IN
11:05 AM
6/15/2020



Create index pattern

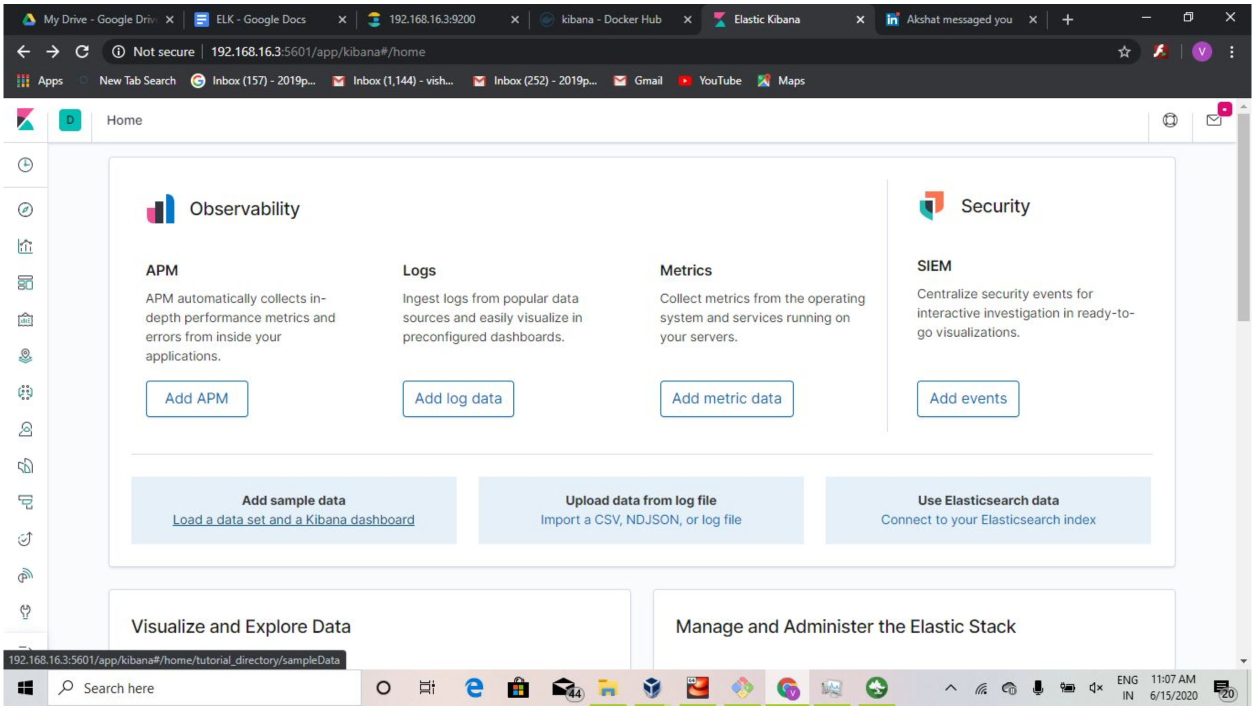
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

Couldn't find any Elasticsearch data

You'll need to index some data into Elasticsearch before you can create an index pattern. Learn how or get started with some sample data sets.

Check for new data



Home

Observability

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

Security

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add events

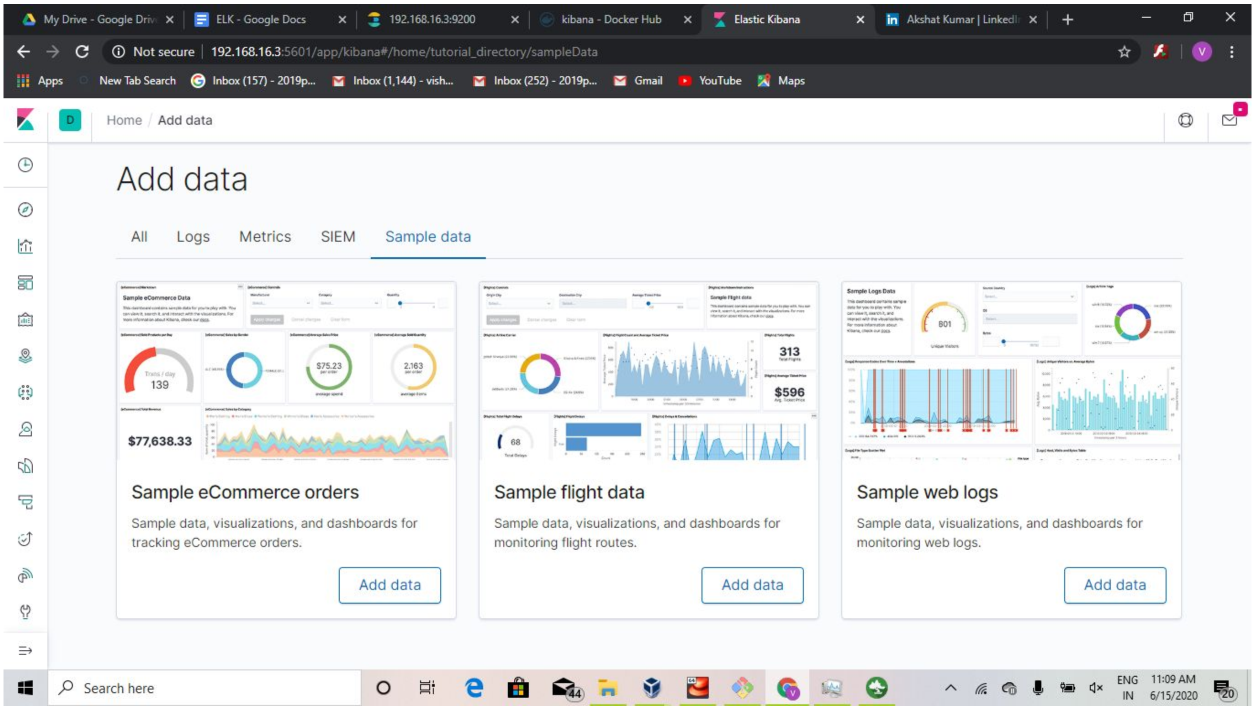
Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Manage and Administer the Elastic Stack



Home / Add data

Add data

All Logs Metrics SIEM Sample data

Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

Add data

Sample flight data

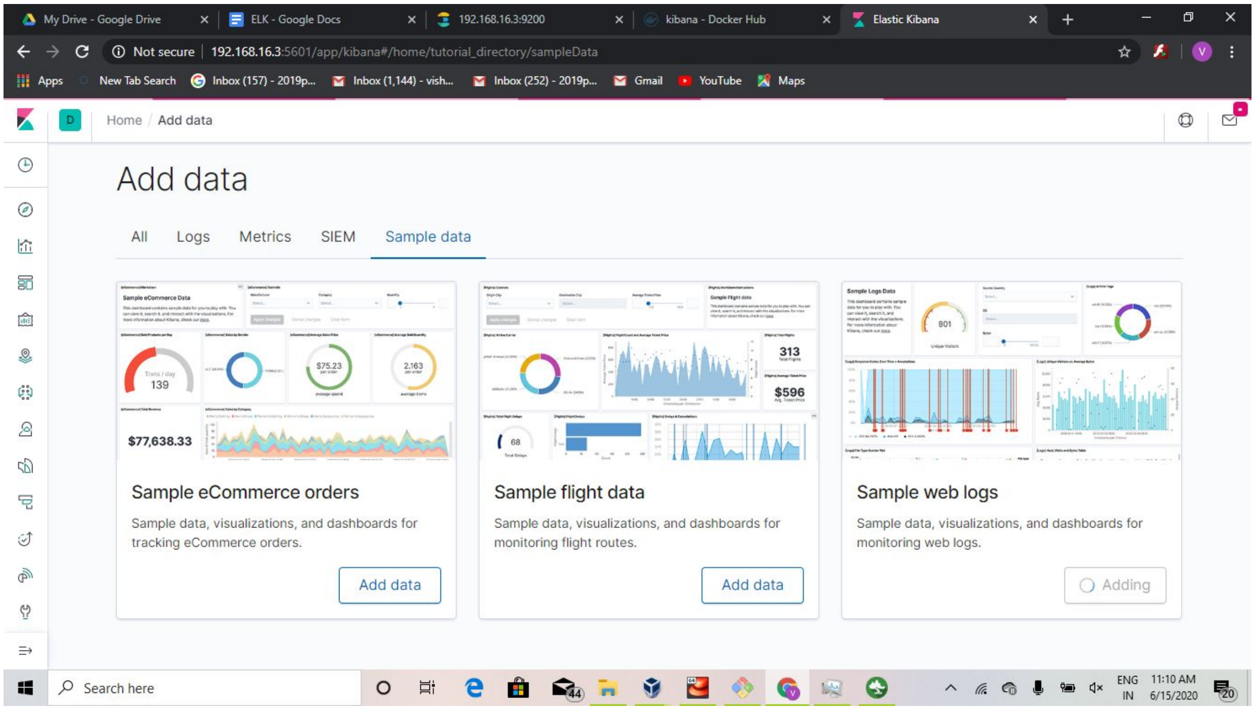
Sample data, visualizations, and dashboards for monitoring flight routes.

Add data

Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.

Add data



Add data

Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

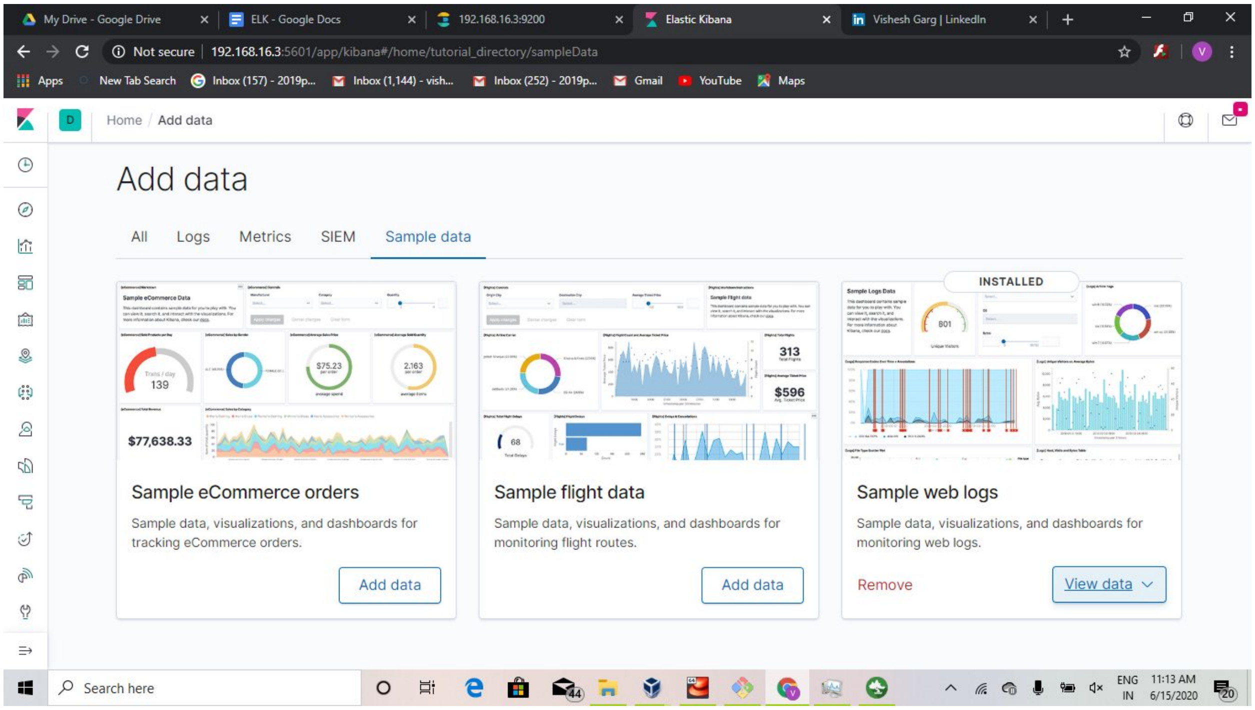
Sample flight data

Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.

```
[root@localhost ~]# curl 192.168.16.3:9200/_cat/indices
green open .apm-custom-link        aImMuKMMRxOu6a5SOyXH2A 1 0    0 0   208b
208b
green open .kibana_task_manager_1   WHwsq46pQ2q3_dFPkozIAg 1 0    5 3 94.9kb
94.9kb
green open .apm-agent-configuration d_aB0q9IRZWB8UUq1gDS-Q 1 0    0 0   208b
208b
green open kibana_sample_data_logs  -PH410dpSVm6nrt4QW10Pg 1 0 7000 0
7.2mb  7.2mb
green open .kibana_1               1mZ_rmTKRdmENeNS58SAeQ 1 0   53 1 57.4kb
57.4kb
[root@localhost ~]# curl 192.168.16.3:9200/kibana_sample_data_logs
{"kibana_sample_data_logs":{"aliases":{},"mapp}
[root@localhost ~]# curl 192.168.16.3:9200/kibana_sample_data_logs/_search
{"took":1792,"timednumber_of_replicas":"0","uuid":"-PH410dpSVm6nrt4QW10Pg","versi
on":{"created":"7070199"}}}}}
```



192.168.16.3:5601/app/kibana#/home/tutorial_directory/sampleData

Add data

Sample eCommerce orders

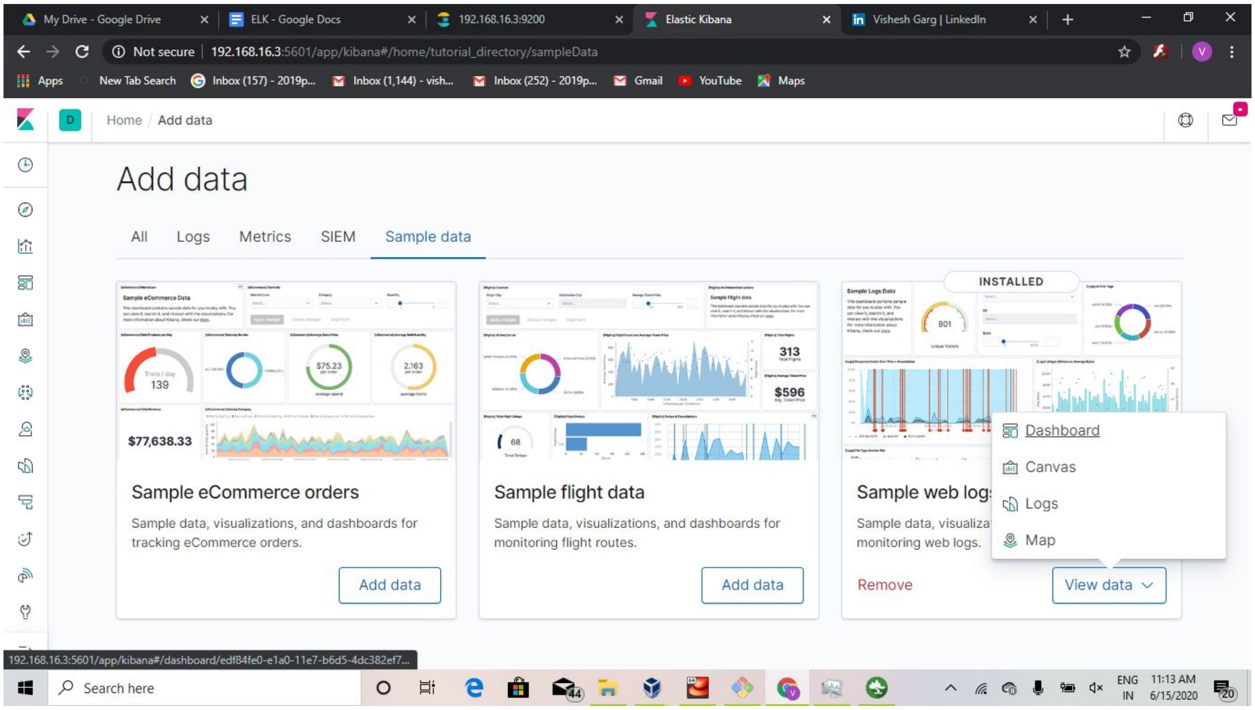
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data

Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.



192.168.16.3:5601/app/kibana#/home/tutorial_directory/sampleData

Add data

Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data

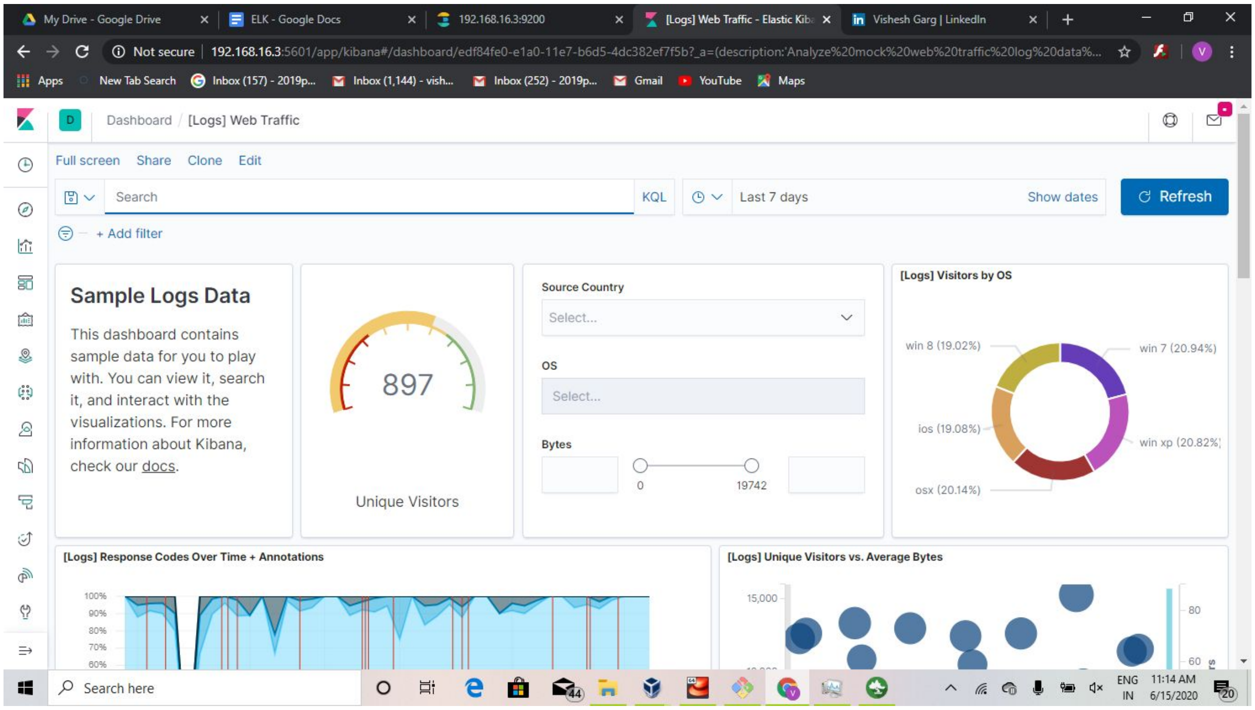
Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs

Sample data, visualiza

monitoring web logs.

192.168.16.3:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7...



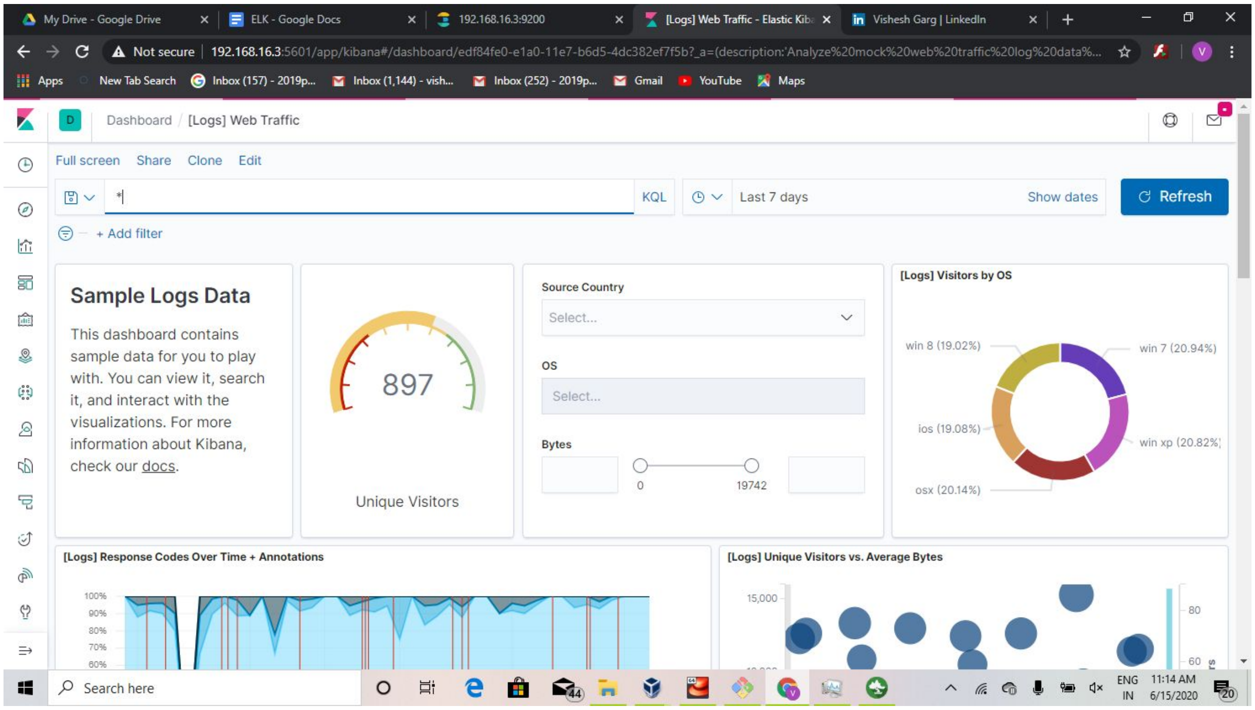
192.168.16.3:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_a=(description:'Analyze%20mock%20web%20traffic%20log%20data%...

Dashboard / [Logs] Web Traffic

Search — KQL — Last 7 days

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.



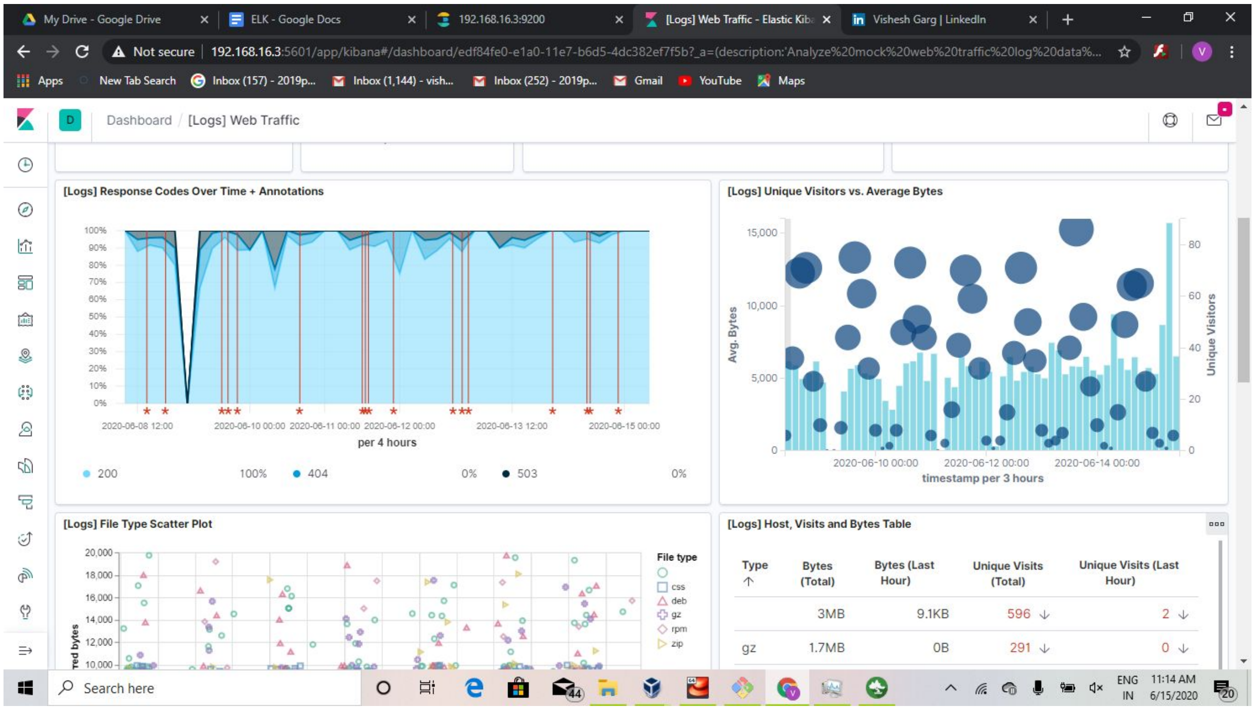
192.168.16.3:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_a=(description:'Analyze%20mock%20web%20traffic%20log%20data%...

Dashboard / [Logs] Web Traffic

*| — KQL — Last 7 days

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.



My Drive - Google Drive
ELK - Google Docs
192.168.16.3:9200
[Logs] Web Traffic - Elastic Kib
Vishesh Garg | LinkedIn
Not secure | 192.168.16.3:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_a=(description:'Analyze%20mock%20web%20traffic%20log%20data%...
Apps
New Tab Search
Inbox (157) - 2019p...
Inbox (1,144) - vish...
Inbox (252) - 2019p...
Gmail
YouTube
Maps
Dashboard / [Logs] Web Traffic

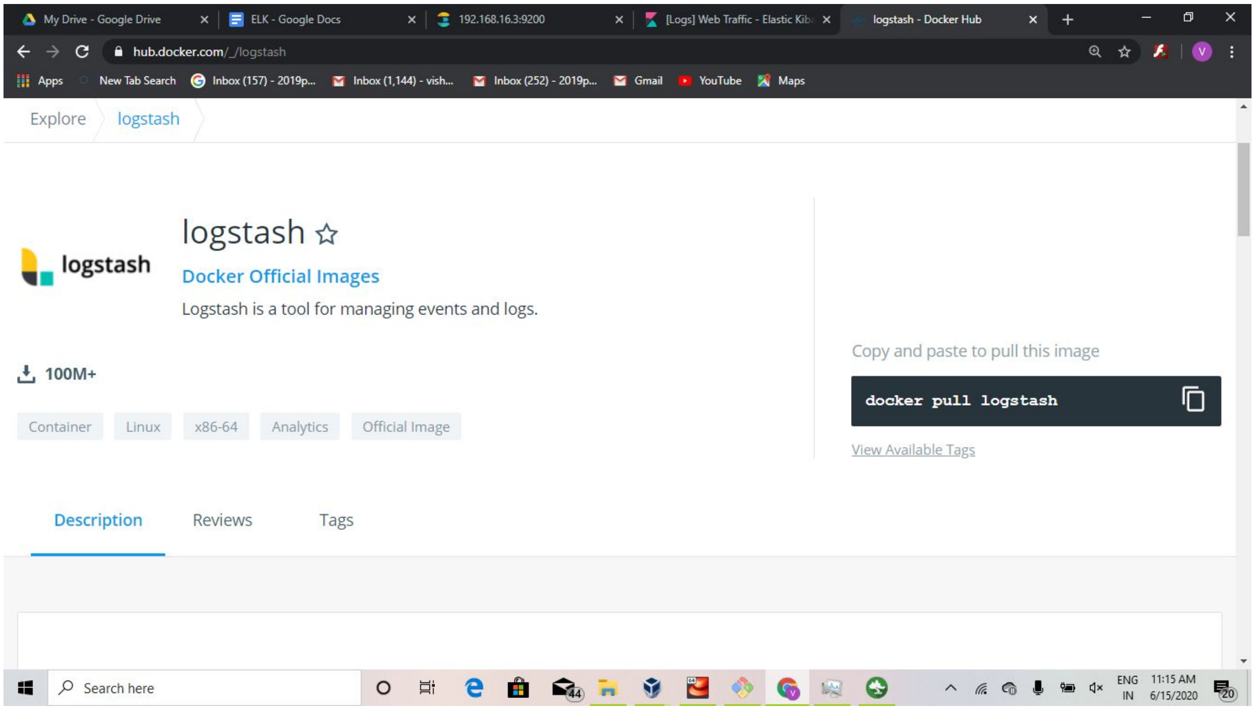
[Logs] Response Codes Over Time + Annotations

[Logs] Unique Visitors vs. Average Bytes

[Logs] File Type Scatter Plot

[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	3MB	9.1KB	596 ↓	2 ↓
gz	1.7MB	0B	291 ↓	0 ↓



logstash ☆

Docker Official Images

Logstash is a tool for managing events and logs.

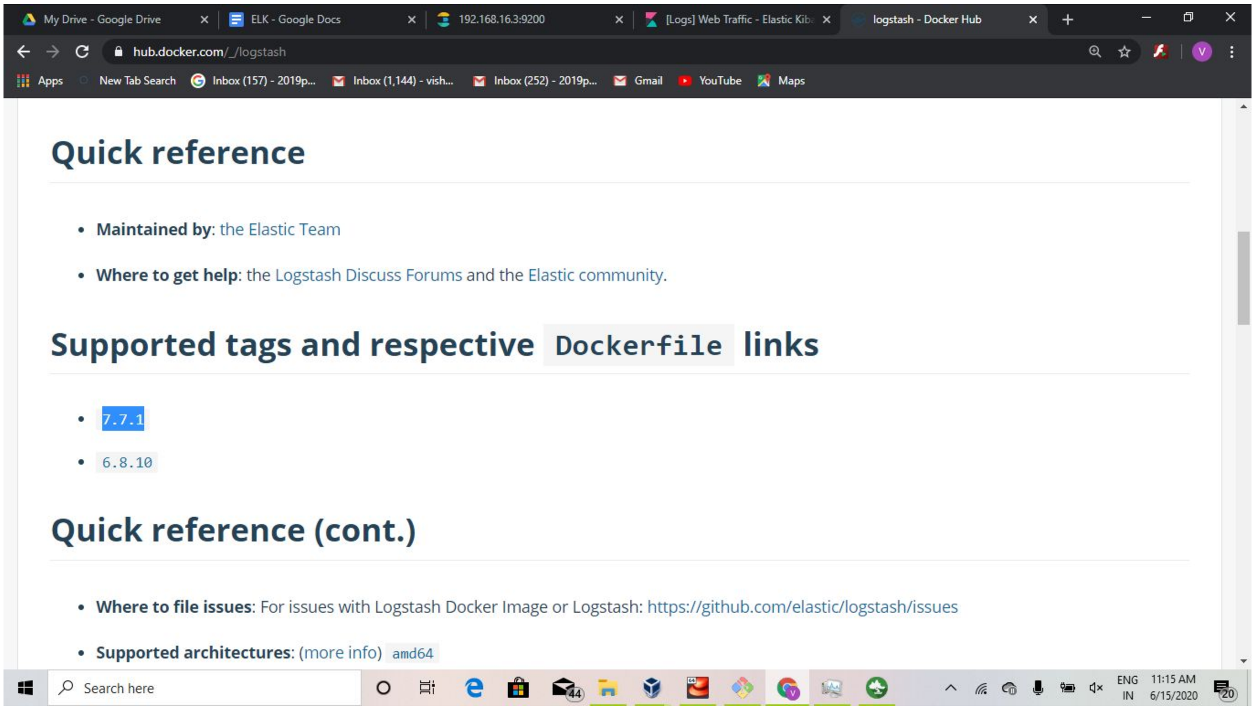
100M+

Container | Linux | x86-64 | Analytics | Official Image

Copy and paste to pull this image

```
docker pull logstash
```

View Available Tags



Quick reference

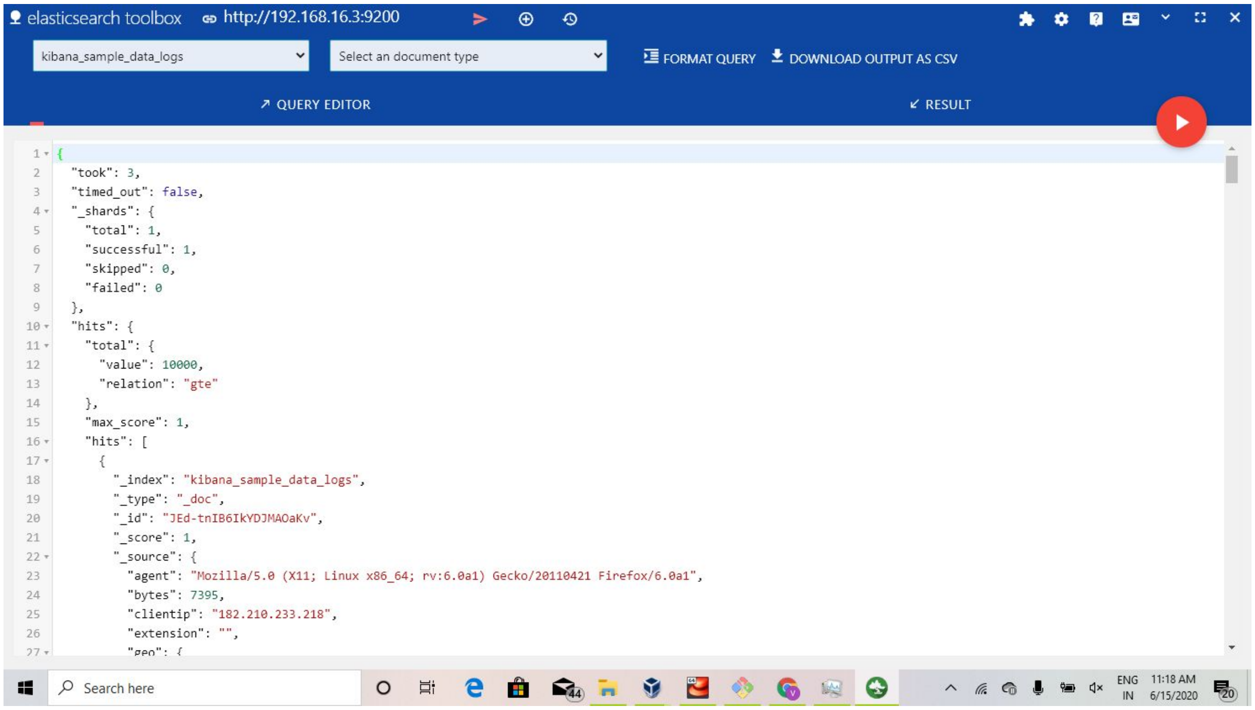
- **Maintained by**: the Elastic Team
- **Where to get help**: the Logstash Discuss Forums and the Elastic community.

Supported tags and respective `Dockerfile` links

- `7.7.1`
- `6.8.10`

Quick reference (cont.)

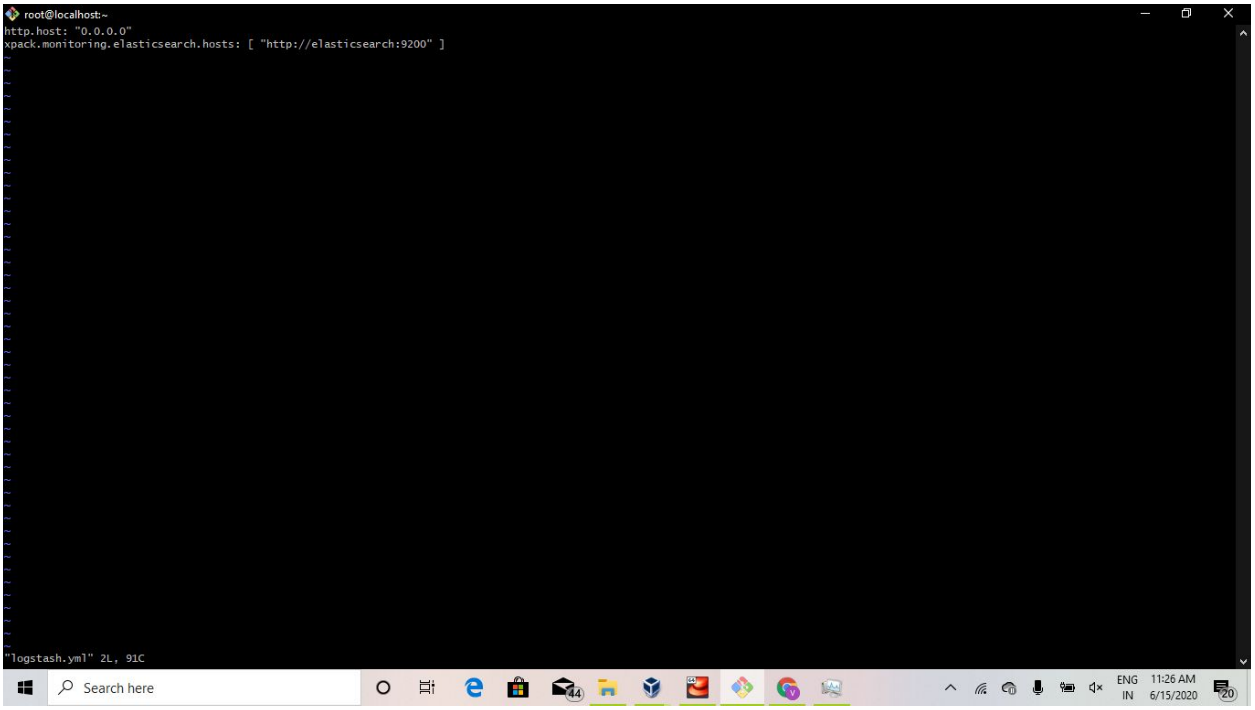
- **Where to file issues**: For issues with Logstash Docker Image or Logstash: https://github.com/elastic/logstash/issues
- **Supported architectures**: (more info) `amd64`



```
{
  "took": 3,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 10000,
      "relation": "gte"
    },
    "max_score": 1,
    "hits": [
      {
        "_index": "kibana_sample_data_logs",
        "_type": "_doc",
        "_id": "JEd-tnIB6IkYDJMAOaKv",
        "_score": 1,
        "_source": {
          "agent": "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",
          "bytes": 7395,
          "clientip": "182.210.233.218",
          "extension": "",
          "geo": {
```

```
[root@localhost ~]# docker pull logstash:7.7.1
7.7.1: Pulling from library/logstash
Digest:
sha256:cf2a17d96e76e5c7a04d85d0f2e408a0466481b39f441e9d6d0aad652e033026
Status: Downloaded newer image for logstash:7.7.1
docker.io/library/logstash:7.7.1
```

```
[root@localhost ~]# docker run -dit --name logstash --net elknetwork
logstash:7.7.1
4215309d346ef06d43571e5d9949b4c2703157e12e5fbc6ad1cb3af25b552
[root@localhost ~]# docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
PORTS                                            NAMES
ec24215309d3        logstash:7.7.1      "/usr/local/bin/dock…"   2 minutes ago       Up About a minute
5044/tcp, 9600/tcp                               logstash
660a43510de0        kibana:7.7.1        "/usr/local/bin/dumb…"   28 minutes ago      Up 28 minutes
0.0.0.0:5601->5601/tcp                           kibana
ddc22eaed4cb        elasticsearch:7.7.1   "/tini -- /usr/local…"   52 minutes ago      Up About an hour
0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp   elasticsearch
[root@localhost ~]# docker exec -it logstash bash
bash-4.2$ ls
bin  config  CONTRIBUTORS  data  Gemfile  Gemfile.lock  lib  LICENSE.txt
logstash-core  logstash-core-plugin-api  modules  NOTICE.TXT  pipeline  tools  vendor
x-pack
bash-4.2$ cd config/
bash-4.2$ ls
jvm.options  log4j2.properties  logstash-sample.conf  logstash.yml  pipelines.yml
startup.options
bash-4.2$ pwd
/usr/share/logstash/config
bash-4.2$ vim logstash.yml
bash: vim: command not found
bash-4.2$ vi logstash.yml
bash-4.2$ ping elasticsearch
PING elasticsearch (172.18.0.2) 56(84) bytes of data.
64 bytes from elasticsearch.elknetwork (172.18.0.2): icmp_seq=1 ttl=64 time=0.113 ms
64 bytes from elasticsearch.elknetwork (172.18.0.2): icmp_seq=2 ttl=64 time=0.154 ms
^C
--- elasticsearch ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.113/0.133/0.154/0.023 ms
```



```
http.host: "0.0.0.0"
xpack.monitoring.elasticsearch.hosts: [ "http://elasticsearch:9200" ]
"logstash.yml" 2L, 91C
```