Elasticsearch & Kibana

Mobina Noori - Zahra Gandomi

Introduction To Elasticsearch & Kibana

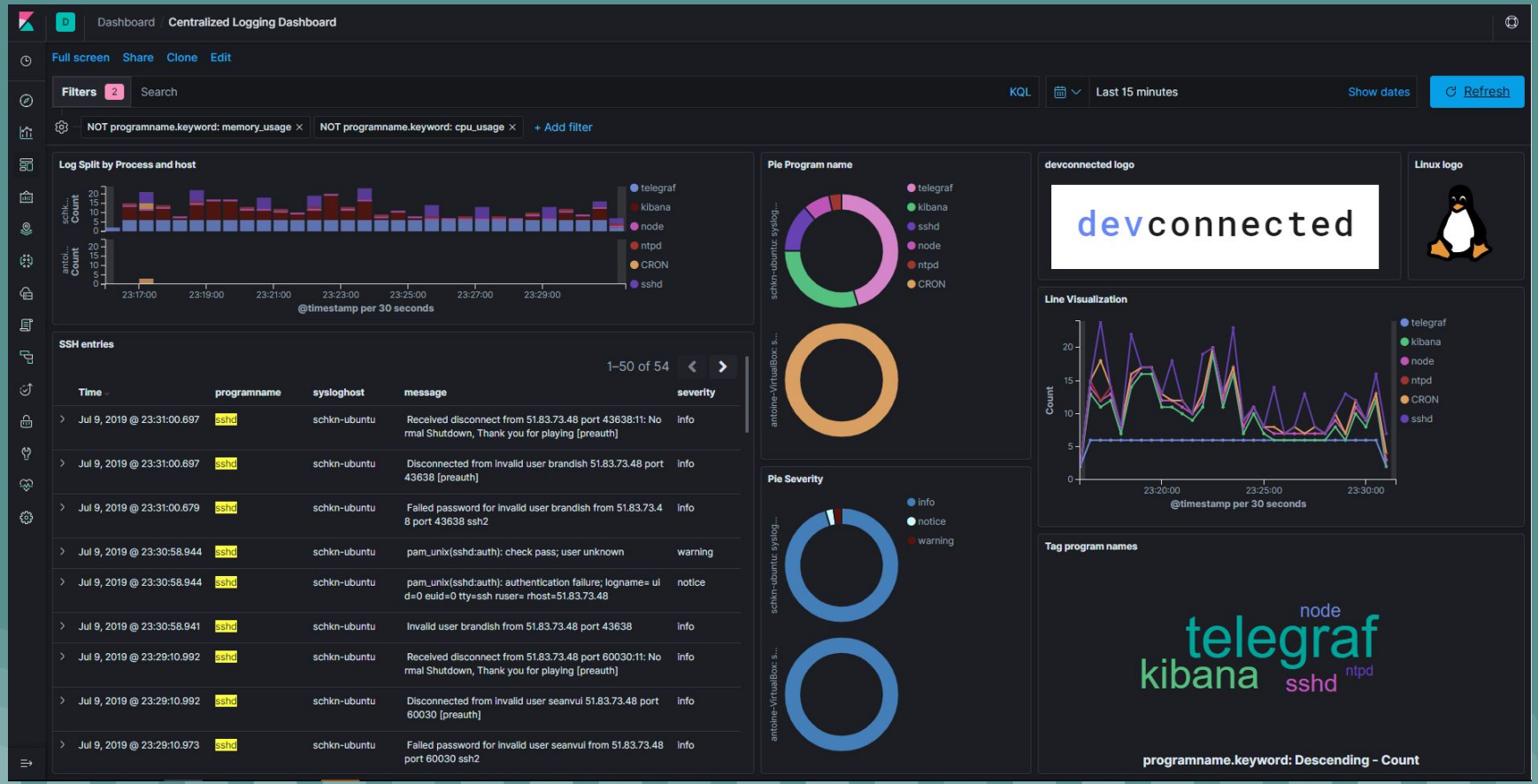
- **Elasticsearch is a document oriented database.**
- **Elasticsearch can be used to search any kind of documents.**
- **According to the DB-Engines ranking, Elasticsearch is the most popular enterprise search engine.**
- **Elasticsearch is great at analyzing lots of data.**

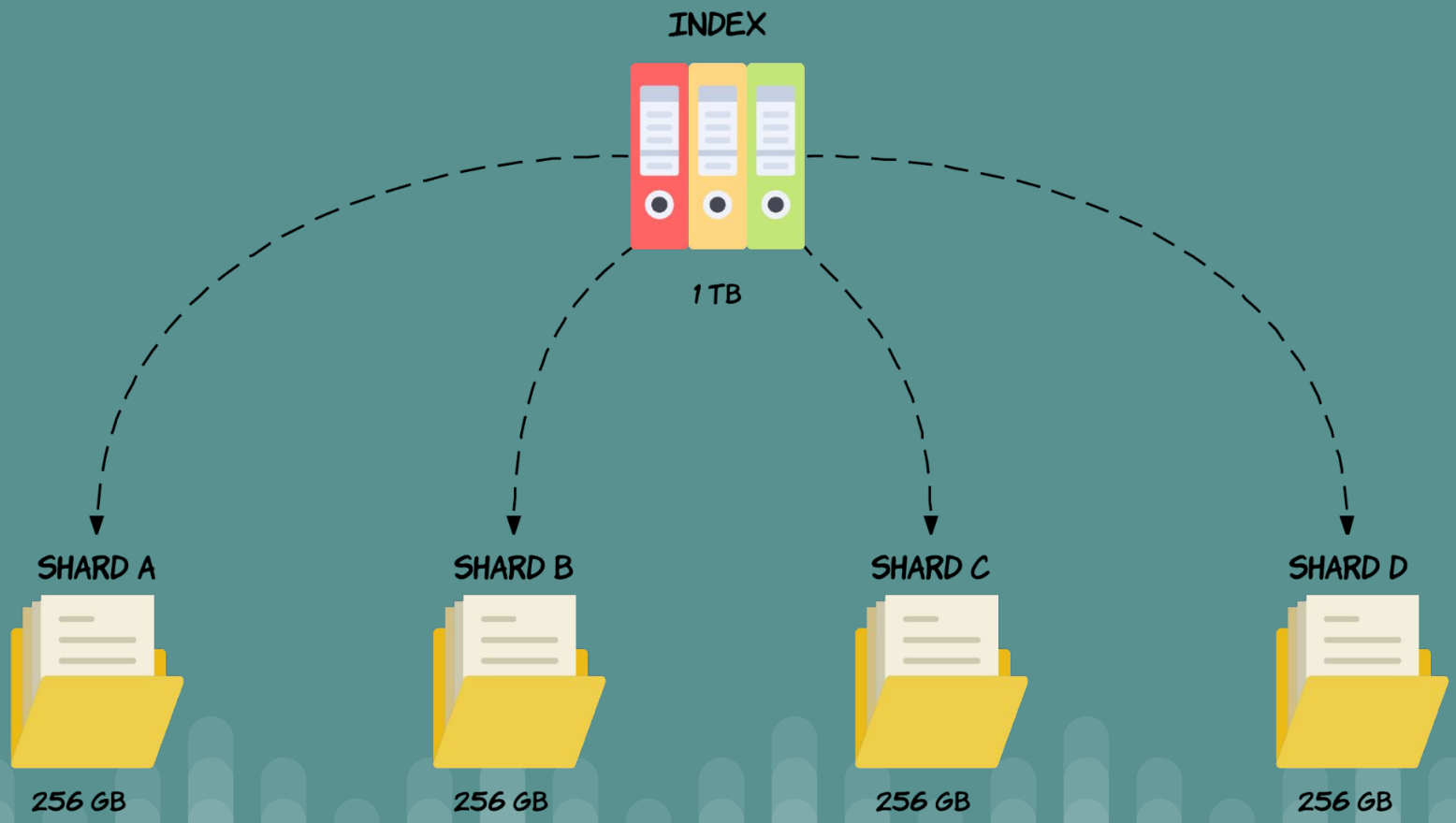
Introduction To Elasticsearch & Kibana

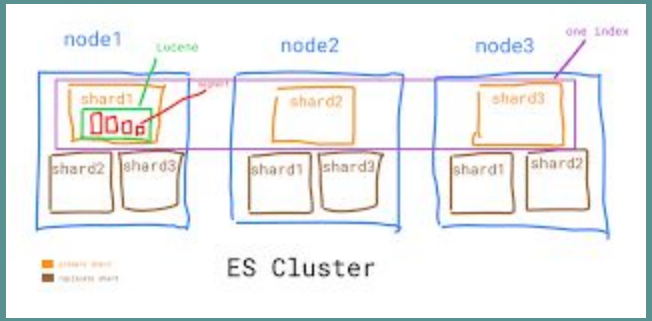
- **Kibana is a proprietary data visualization dashboard software for Elasticsearch, whose open source successor in OpenSearch is OpenSearch Dashboards.**

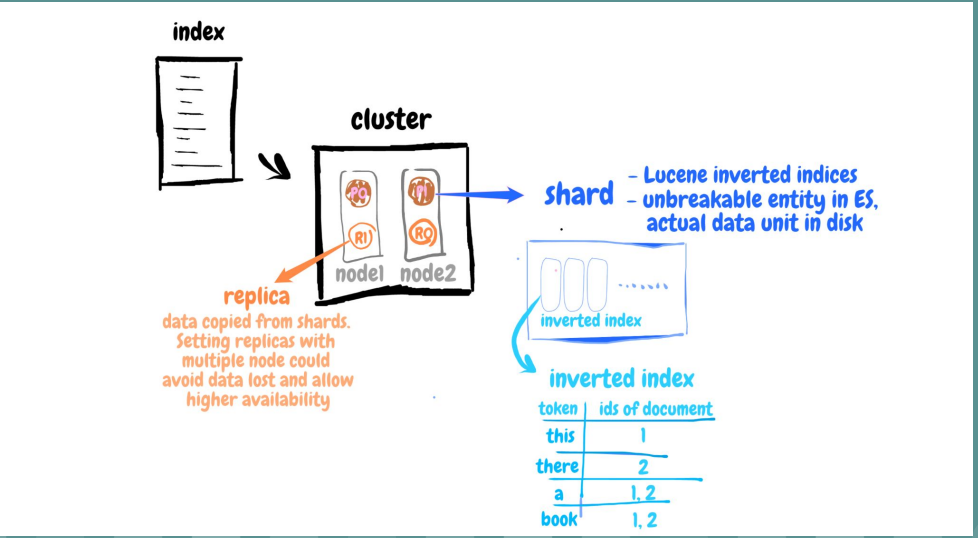
- **Elasticsearch is distributed, which means that indices can be divided into shards and each shard can have zero or more replicas.**

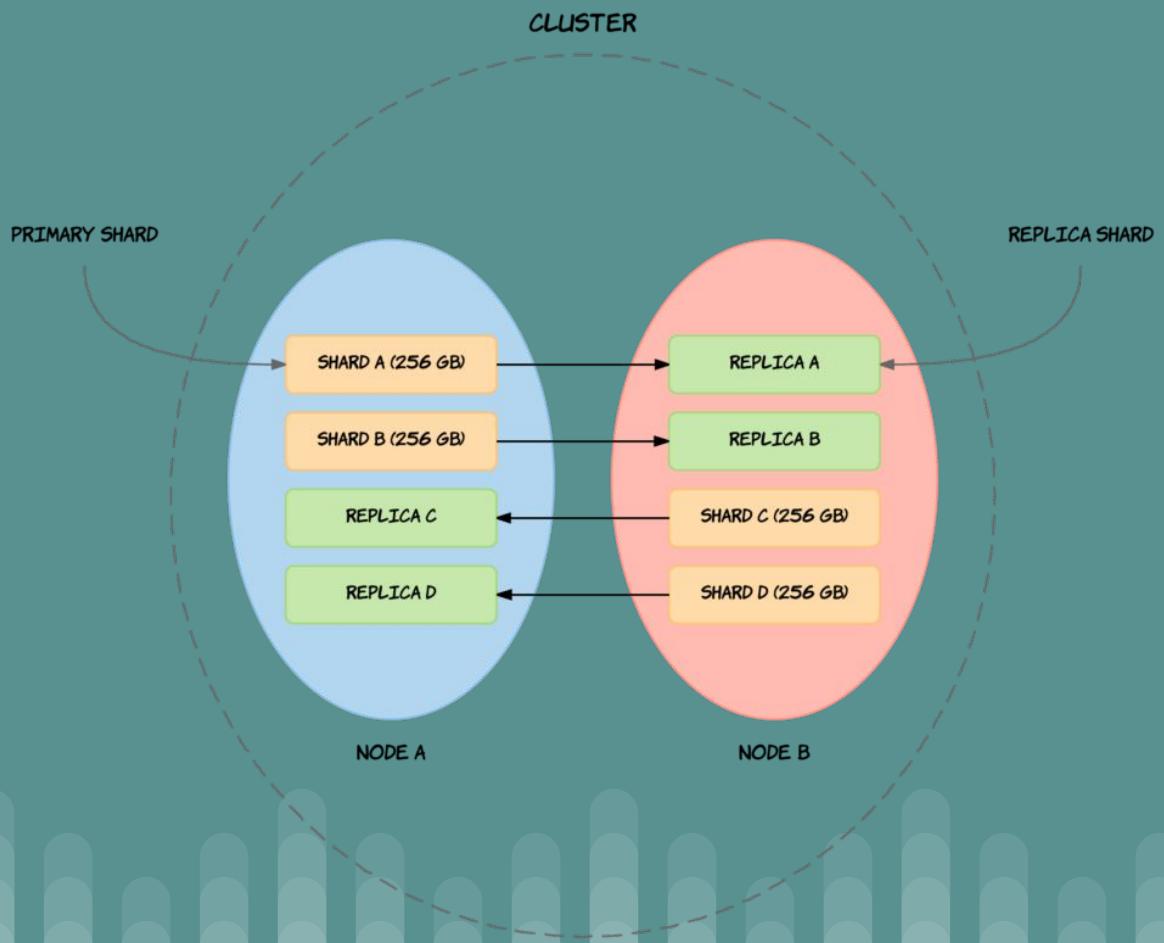
Kibana Dashboard




INDEX
1 TB
SHARD A
256 GB
SHARD B
256 GB
SHARD C
256 GB
SHARD D
256 GB


node1
Lucene
node2
node3
one index
shard1
shard2
shard3
shard2
shard3
shard1
shard2
shard1
shard2
ES Cluster


index
cluster
PQ
RI
RI
RQ
node1
node2
shard
- Lucene inverted indices
- unbreakable entity in ES, actual data unit in disk
replica
data copied from shards. Setting replicas with multiple node could avoid data lost and allow higher availability
inverted index
inverted index
token | ids of document
this | 1
there | 2
a | 1, 2
book | 1, 2


CLUSTER
PRIMARY SHARD
REPLICA SHARD
SHARD A (256 GB)
SHARD B (256 GB)
REPLICA C
REPLICA D
REPLICA A
REPLICA B
SHARD C (256 GB)
SHARD D (256 GB)
NODE A
NODE B

Elasticsearch Applications

1. Full-text searches (Build complex search functionality)
2. Write queries that aggregate data
3. Get valuable information out of the data (Logs, Errors)
4. Send events to Elasticsearch
5. Use machine learning to forecast sales based on historical data
6. Anomaly detection (You can set up alerting for this and be notified whenever something unusual happens, such as receiving an e-mail or a message on Slack.)

You can build complex search functionality with Elasticsearch. Google search, for instance.

- Suppose we want to implement searching for a webshop.
- Besides searching through product names and other full-text fields, we might want to take a number of factors into account when sorting the results.
- If the products have ratings, we probably want to boost the relevance of highly rated products.
- We also might want to allow users to filter results, such as by price range, brand, size, color, etc., and to sort by price or relevance, for instance.

You can also query structured data such as numbers and aggregate data, and use Elasticsearch.

- Full-text searches is not the only thing Elasticsearch can do, though.

- You can write queries that aggregate data and use the results for making pie charts, line charts, or whatever you might need.

Get valuable information out of the data that you store within Elasticsearch.

- An example would be to store logs from applications and various server system metrics and then analyze these, perhaps with alerting set up.

- You might want to keep track of the number of errors for a web application or the CPU and memory usage of servers, and then show that on a line chart, for instance.

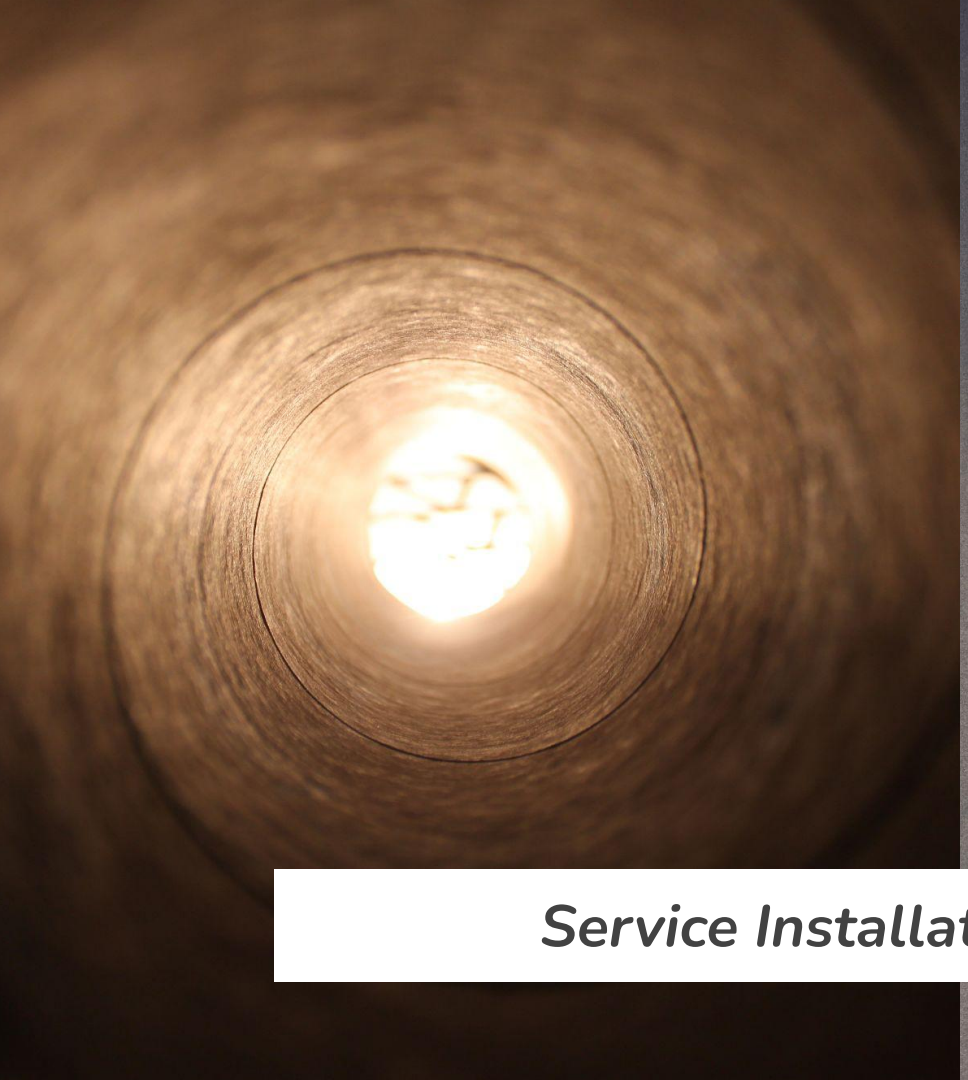
- This is referred to as Application Performance Management - or APM - and is a quite common use case of Elasticsearch and the Elastic Stack.

Another common thing to do, is to send events to Elasticsearch, which can be anything you want.

- Perhaps we are sending sales from physical stores to Elasticsearch, in which case we can analyze which stores sell the most.

- We can do that with something called aggregations, which you may know from relational databases.

- But we can do much more than that, so Elasticsearch is great at analyzing lots of data.



Service Installation Steps

- Since Elasticsearch runs on top of Java, you need to install the Java Development Kit (JDK).
- To allow access to your repositories via HTTPS, you need to install an APT transport package.
- After you confirm Java and apt-transport-https installed successfully, proceed with steps to install Elasticsearch.
- update the GPG key for the Elasticsearch repository.
- Use the wget command to pull the public key

- use this command to add the repository to your system:
  echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

- Install Elasticsearch.

- Once the installation is finished, Elasticsearch does not run until you start it. Also, when you reboot the machine, you need to rerun the Elasticsearch service as it does not start automatically.
-
- To have Elasticsearch automatically reload when the system restarts, use the following commands (First, reload the systemd configuration): sudo systemctl daemon-reload

- Then, enable the Elasticsearch service.

- And finally, after the service is enabled, start Elasticsearch.

- Now, Elasticsearch will start every time you turn on or reboot the system.

- If you make changes to configuration files, or need to restart Elasticsearch for any reason, use:

```
sudo systemctl restart elasticsearch.service
```

- Once you finish using the commands to start, restart, and stop Elasticsearch, you can also check the status of the service.

```
service elasticsearch status
```

- The default configuration does not allow your machine to be accessed by other hosts. To allow remote access, use a text editor of your choice and open the elasticsearch.yml file.

- Scroll down to the Network section. Find the line that says #network.host.

- Uncomment the line (remove the pound (#) sign), set the IP address to 0.0.0.0, and add these lines:

  transport.host: localhost

  transport.tcp.port: 9300

  http.port: 9200

- Now that the Elasticsearch service is active you can use curl to test if the tool works.

```
mobina@mobina-X542URR:~$ sudo apt install apt-transport-https
[sudo] password for mobina:
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:
  libcublas10 libfltk1.1
Use 'sudo apt autoremove' to remove them.
```

To allow access to your repositories via HTTPS, you need to install an APT transport package:

sudo apt install apt-transport-https

```
mobina@mobina-X542URR:~$ java -version
openjdk version "11.0.13" 2021-10-19
OpenJDK Runtime Environment (build 11.0.13+8-Ubuntu-0ubuntu1.20.04)
OpenJDK 64-Bit Server VM (build 11.0.13+8-Ubuntu-0ubuntu1.20.04, mixed mode, sharing)
mobina@mobina-X542URR:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
mobina@mobina-X542URR:~$ 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
mobina@mobina-X542URR:~$
```

- To install default JDK, run the following command:
  sudo apt install openjdk-8-jdk

- Use the wget command to <u>pull the public key</u>:
  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

- use this command to <u>add the repository to your system</u>:
  echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

```
mobina@mobina-X542URR:~$ sudo apt install elasticsearch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcublas10 libfltk1.1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 344 MB of archives.
After this operation, 552 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.16.2 [344 MB]
Fetched 325 MB in 9min 39s (561 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 318540 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.16.2_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.16.2) ...
Setting up elasticsearch (7.16.2) ...
### NOT starting on installation, please execute the following statements to con
figure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
Processing triggers for systemd (245.4-4ubuntu3.13) ...
```

mobina@mobina-X542URR: ~

```
  GNU nano 4.8                    /etc/elasticsearch/elasticsearch.yml                    Modified
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# 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
Files
# 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"]
#
# 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

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket M-Q Previous   ^B Back        ^← Prev Word
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^W Where Was   M-W Next       ^F Forward     ^→ Next Word
```

```
#
#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
```

```
mobina@mobina-X542URR:~$ service elasticsearch status
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: failed (Result: timeout) since Wed 2022-01-05 12:52:58 +0330; 19mi>
       Docs: https://www.elastic.co
   Main PID: 1661 (code=killed, signal=TERM)

Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/s>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/s>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/s>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/s>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/j>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/j>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/j>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at java.base/j>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at org.elastic>
Jan 05 12:53:01 mobina-X542URR systemd-entrypoint[2181]:         at org.elastic>
lines 1-16/16 (END)
```

```
mobina@mobina-X542URR:~$ sudo systemctl start elasticsearch.service
mobina@mobina-X542URR:~$ sudo systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script wit
h /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
mobina@mobina-X542URR:~$
```

```
mobina@mobina-X542URR:~$ sudo systemctl enable elasticsearch.service
[sudo] password for mobina:
Synchronizing state of elasticsearch.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
mobina@mobina-X542URR:~$ sudo systemctl start elasticsearch.service
mobina@mobina-X542URR:~$ service elasticsearch status
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Wed 2022-01-05 13:14:36 +0330; 9s ago
       Docs: https://www.elastic.co
   Main PID: 7921 (java)
      Tasks: 85 (limit: 9327)
     Memory: 4.1G
     CGroup: /system.slice/elasticsearch.service
             ├─7921 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─8119 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Jan 05 13:13:41 mobina-X542URR systemd[1]: Starting Elasticsearch...
Jan 05 13:14:36 mobina-X542URR systemd[1]: Started Elasticsearch.
lines 1-13/13 (END)
```

```
mobina@mobina-X542URR:~$ sudo systemctl start elasticsearch
mobina@mobina-X542URR:~$ curl -X GET "localhost:9200"
{
  "name" : "mobina-X542URR",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "7hf-ezTDQVqsv5nEoz0S5A",
  "version" : {
    "number" : "7.16.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "2b937c44140b6559905130a8650c64dbd0879cfb",
    "build_date" : "2021-12-18T19:42:46.604893745Z",
    "build_snapshot" : false,
    "lucene_version" : "8.10.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
mobina@mobina-X542URR:~$
```

```
mobina@mobina-X542URR:~$ sudo apt install kibana
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcublas10 libfltk1.1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 285 MB of archives.
After this operation, 767 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.16.2 [285 MB]
Fetched 285 MB in 9min 59s (476 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 319665 files and directories currently installed.)
Preparing to unpack .../kibana_7.16.2_amd64.deb ...
Unpacking kibana (7.16.2) ...
Setting up kibana (7.16.2) ...
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
Processing triggers for systemd (245.4-4ubuntu3.13) ...
mobina@mobina-X542URR:~$
```

```
  GNU nano 4.8                                                    /etc/kibana/kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
#elasticsearch.username: "kibana_system"
#elasticsearch.password: "pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# If may use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket  M-Q Previous   ^B Back        ^◀ Prev Word
```

```
mobina@mobina-X542URR:~$ sudo systemctl start elasticsearch.service
mobina@mobina-X542URR:~$ sudo systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script wit
h /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
mobina@mobina-X542URR:~$
```

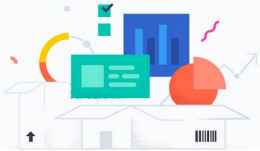
```
mobina@mobina-X542URR:~$ sudo systemctl start kibana
mobina@mobina-X542URR:~$ sudo systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
mobina@mobina-X542URR:~$
```

Firefox Web Browser Jan 3 9:48 PM en

Home - Elastic

localhost:5601/app/home#/

Welcome to Elastic

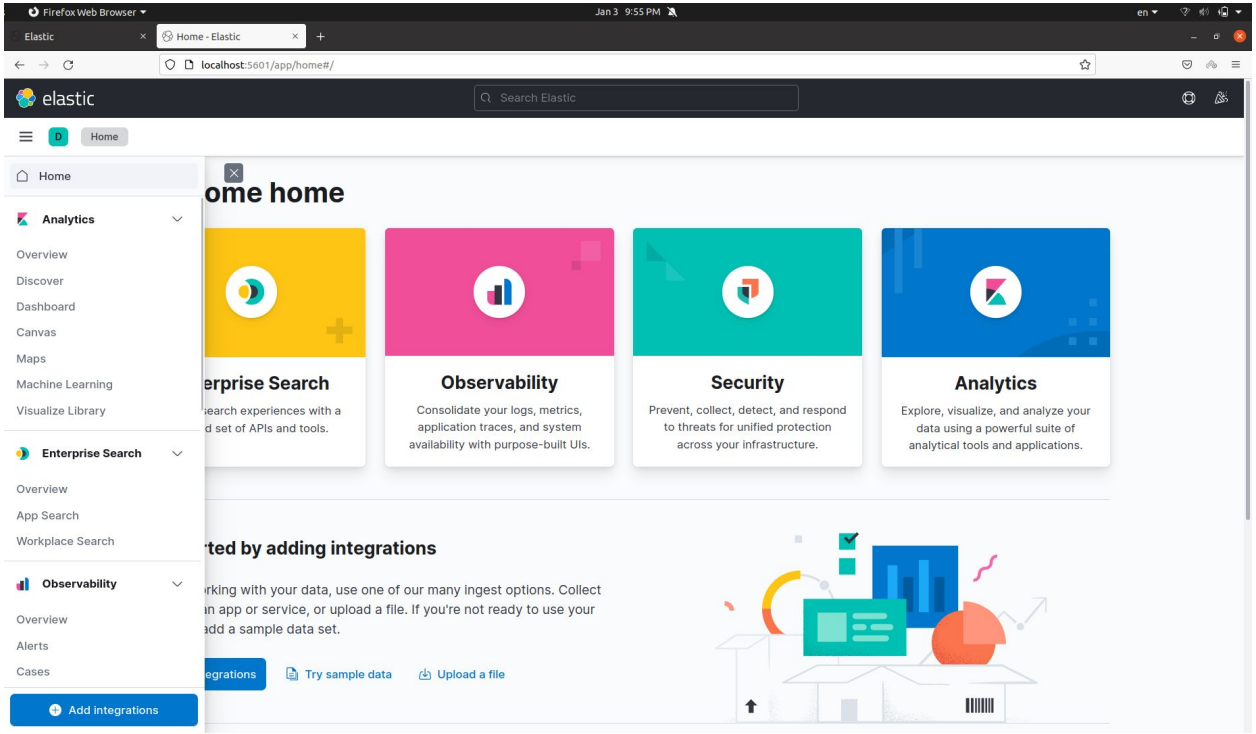


Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

Add integrations Explore on my own

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.


Firefox Web Browser
Jan 3 9:55 PM
en
Elastic
Home - Elastic
localhost:5601/app/home#/
elastic
Search Elastic
D
Home
Home
Analytics
Overview
Discover
Dashboard
Canvas
Maps
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Alerts
Cases
Add integrations
ome home
erprise Search
earch experiences with a
d set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
ted by adding integrations
rking with your data, use one of our many ingest options. Collect
n app or service, or upload a file. If you're not ready to use your
dd a sample data set.
egrations
Try sample data
Upload a file

Firefox Web Browser Jan 3 9:49 PM en

Elastic

localhost:5601/status

Kibana status is Green

mobina-X542URR

2.05 GB	360.85 MB	1.91, 1.93, 1.50
Heap total	Heap used	Load
0.00 ms	**0.00 ms**	**0.00**
Response time avg	Response time max	Requests per second

Plugin status

BUILD **46307** COMMIT **9b678a13a6a3f45286f1d21856a7536a9297f42f**

ID	Status
core:elasticsearch	Elasticsearch is available
core:savedObjects	SavedObjects service has completed migrations and is available
plugin:advancedSettings	All dependencies are available
plugin:bfetch	All dependencies are available
plugin:expressionMetricVis	All dependencies are available
plugin:expressionTagcloud	All dependencies are available
plugin:charts	All dependencies are available
plugin:console	All dependencies are available
plugin:customIntegrations	All dependencies are available
plugin:dashboard	All dependencies are available

kibana

Dev Tools

History Settings Help

Discover
Visualize
Dashboard
Timelion
Dev Tools
Management

Console

```
PUT person
{
  "mappings": {
    "doc": {
      "properties": {
        "title":    { "type": "text"  },
        "name":     { "type": "text"  },
        "age":      { "type": "integer" },
        "created":  {
          "type":   "date",
          "format": "strict_date_optional_time||epoch_millis"
        }
      }
    }
  }
}


POST /person/doc/
{
  "title": "Mrs",
  "name": "Jenny Doe",
  "age": 34
}
```

```
{
  "_index": "person",
  "_type": "doc",
  "_id": "0NHVAmQBMUgnU5StsKLd",
  "_version": 1,
  "result": "created",
  "_shards": {
    "total": 1,
    "successful": 1,
    "failed": 0
  },
  "_seq_no": 0,
  "_primary_term": 1
}
```

Thanks For Your Attention.