

**A. Create two linux servers, server1 => install and configure kibana and elasticsearch with basic username and password authentication server2
=> install and configure metricbeat.**

Installing ElasticSearch

Download and install the public signing key:

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

```
bibek@bibek-LfTech:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
[sudo] password for bibek:
OK
bibek@bibek-LfTech:~$
```

Install the apt-transport-https package

We have already installed this package during installation of logstash

Save the repository definition to /etc/apt/sources.list.d/elastic-7.x.list:

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

You can install the Elasticsearch Debian package with:

sudo apt-get update && sudo apt-get install elasticsearch

```
Fetched 341 MB in 3min 27s (1,649 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 190803 files and directories currently installed.)
Preparing to unpack ../elasticsearch_7.15.2_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.15.2) ...
Setting up elasticsearch (7.15.2) ...
### NOT starting on installation, please execute the following statements to configure 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) ...
bibek@bibek-LfTech:~$
```

The hostname of server 1 is set to elasticsearch

sudo hostnamectl set-hostname elasticsearch

Configuring Elasticsearch

vi /etc/elasticsearch/elasticsearch.yml

```
discovery.type: single-node
cluster.name: elk-metric-data
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
network.host: 0.0.0.0
```

Starting elasticsearch

systemctl start elasticsearch

```
root@elasticsearch:/usr/share/elasticsearch/bin# systemctl start elasticsearch
root@elasticsearch:/usr/share/elasticsearch/bin# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-11-30 12:54:56 +0545; 33s ago
     Docs: https://www.elastic.co
   Main PID: 6307 (java)
    Tasks: 57 (limit: 2946)
   Memory: 1.6G
    CGroup: /system.slice/elasticsearch.service
            └─6307 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net
               6496 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/elasticsearch
```

Setting up the password

cd /usr/share/elasticsearch/

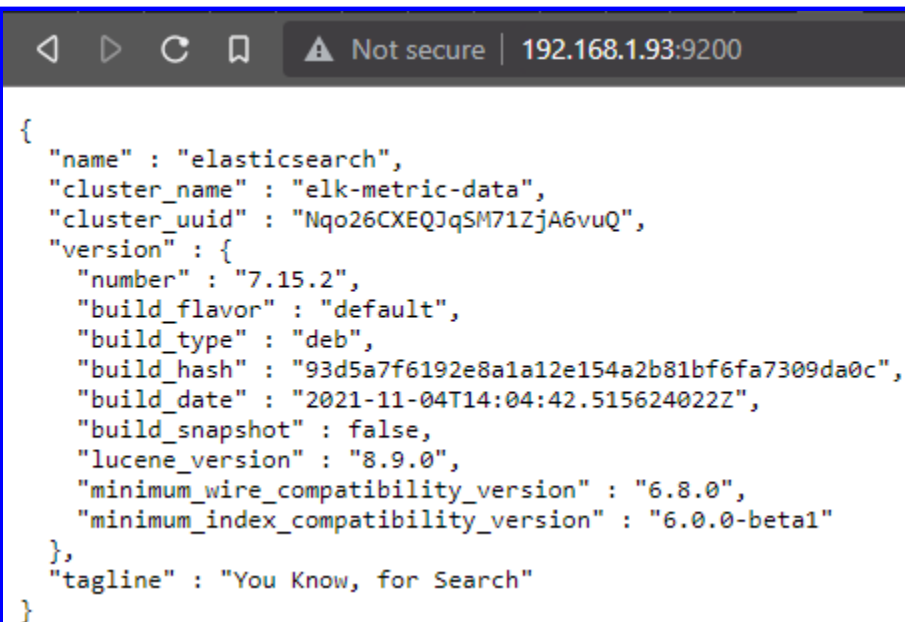
cd bin

./elasticsearch-setup-passwords interactive

```
root@elasticsearch:/usr/share/elasticsearch/bin# ./elasticsearch-setup-passwords
interactive
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,k
ibana_system,logstash_system,beats_system,remote_monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]y

Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana_system]:
Reenter password for [kibana_system]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
root@elasticsearch:/usr/share/elasticsearch/bin#
```

Browsing in web



A screenshot of a web browser window. The address bar shows "Not secure | 192.168.1.93:9200". The main content area displays a JSON object representing the Elasticsearch status. The JSON includes fields for name, cluster_name, cluster_uuid, version (with sub-fields for number, build_flavor, build_type, build_hash, build_date, build_snapshot, lucene_version, minimum_wire_compatibility_version, and minimum_index_compatibility_version), and tagline.

```
{
  "name" : "elasticsearch",
  "cluster_name" : "elk-metric-data",
  "cluster_uuid" : "Nqo26CXEQJqSM71ZjA6vuQ",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Installing Kibana

Download and install the public signing key:

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

Install the apt-transport-https package

We have already installed this package during installation of logstash

Save the repository definition to /etc/apt/sources.list.d/elastic-7.x.list:

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

You can install the Kibana Debian package with:

```
sudo apt-get update && sudo apt-get install kibana
```

```
Fetches 288 MB in 2min 58s (1,616 kB/s)  
Selecting previously unselected package kibana.  
(Reading database ... 191926 files and directories currently installed.)  
Preparing to unpack .../kibana_7.15.2_amd64.deb ...  
Unpacking kibana (7.15.2) ...  
Setting up kibana (7.15.2) ...  
Creating kibana group... OK  
Creating kibana user... OK  
Created Kibana keystore in /etc/kibana/kibana.keystore  
Processing triggers for systemd (245.4-4ubuntu3.13) ...  
bibek@bibek-LfTech:~$
```

Configuring Kibana

```
vi /etc/kibana/kibana.yml
```

```
server.host: "0.0.0.0"  
elasticsearch.username: "elastic"  
elasticsearch.password: "123456"  
xpack.encryptedSavedObjects.encryptionKey: "ajfdhk453jkfa34589afjad43jfaJ538975"
```

```
elasticsearch.hosts: ["http://localhost:9200"]
```

Curl at localhost

```

root@elasticsearch:/etc/kibana# curl --user elastic:123456 -XGET "http://localhost:9200"
{
  "name" : "elasticsearch",
  "cluster_name" : "elk-metric-data",
  "cluster_uuid" : "Nqo26CXEQJqSM71ZjA6vuQ",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

```

Starting the kibana

systemctl restart kibana

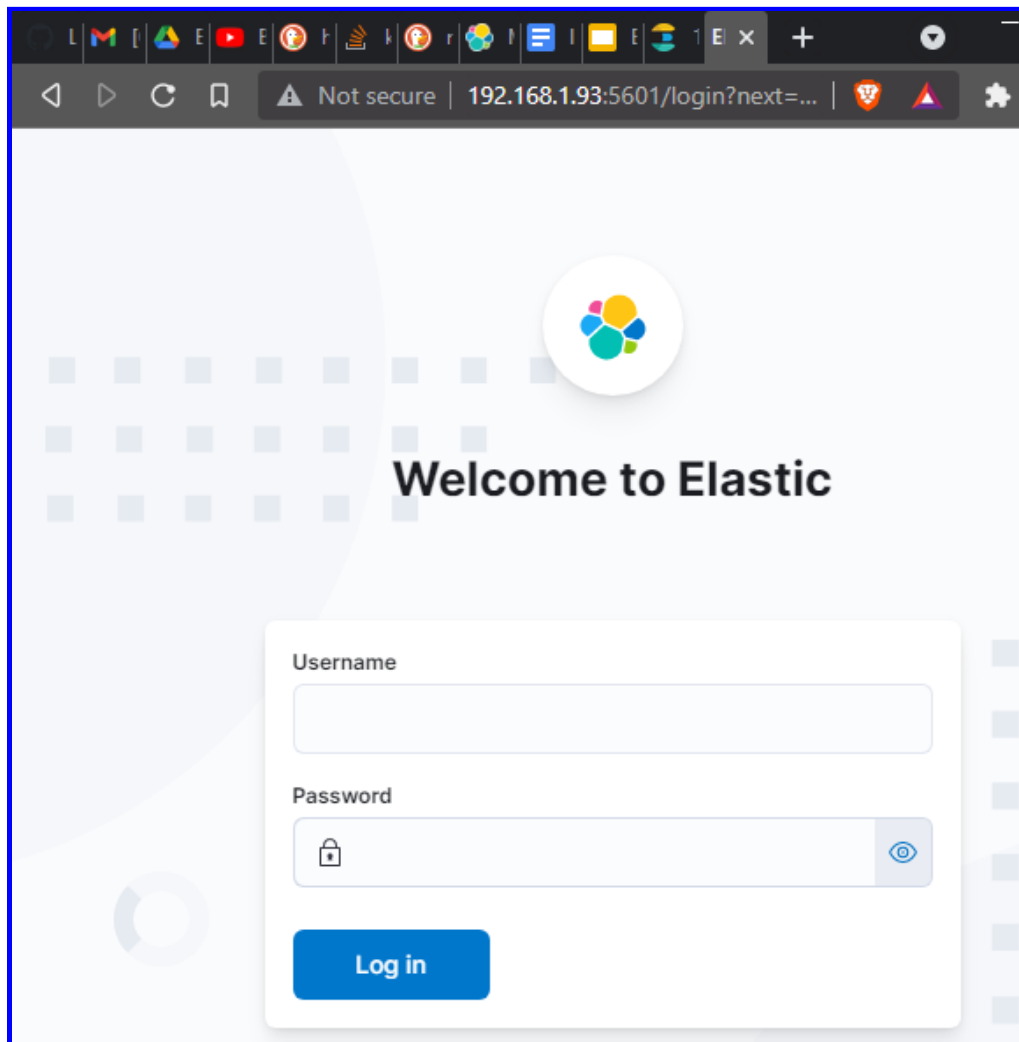
```

root@elasticsearch:/etc/kibana# systemctl restart kibana
root@elasticsearch:/etc/kibana# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor prese
   Active: active (running) since Tue 2021-11-30 14:55:37 +0545; 7s ago
     Docs: https://www.elastic.co
    Main PID: 6872 (node)
      Tasks: 7 (limit: 2946)
     Memory: 53.7M
    CGroup: /system.slice/kibana.service
            └─6872 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bi

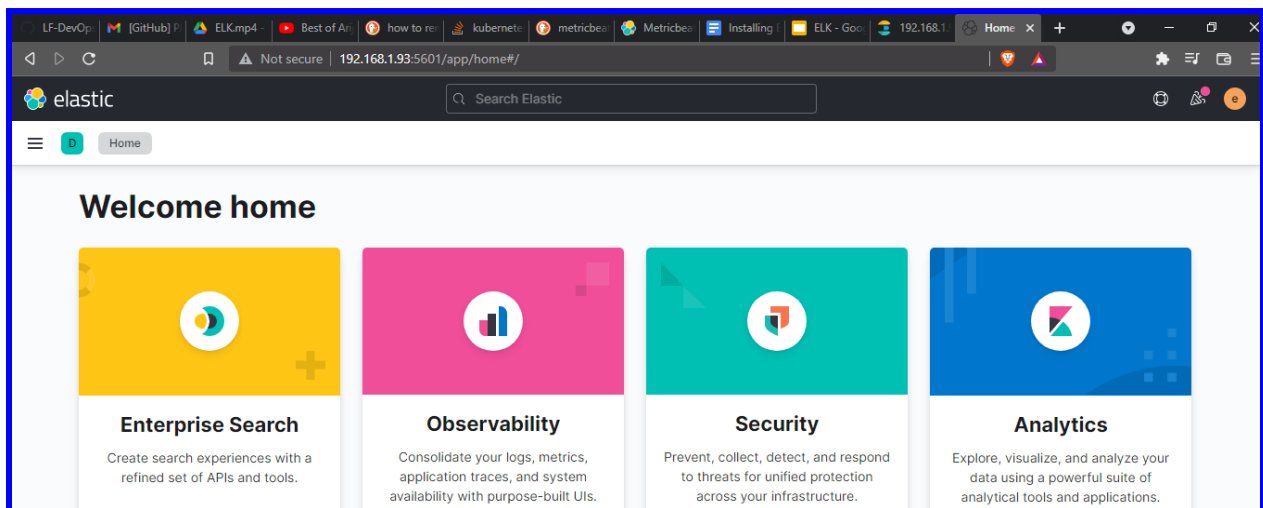
nov 30 14:55:37 elasticsearch systemd[1]: Started Kibana.
lines 1-11/11 (END)

```

Browsing in the web



After login - > Exploring on my own



Installing Metricbeat in Server 2

Server 2 Hostname = metricbeat

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.15.2-amd64.deb
```

```
sudo dpkg -i metricbeat-7.15.2-amd64.deb
```

```
root@metricbeat:/home/bibek# ls
assignment  Downloads  metricbeat-7.15.2-amd64.deb  Public
Desktop    dw         Music                        Templates
Documents  logs.txt  Pictures                     Videos
root@metricbeat:/home/bibek# systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
   Loaded: loaded (/lib/systemd/system/metricbeat.service; disabled; vendor p
   Active: inactive (dead)
     Docs: https://www.elastic.co/beats/metricbeat
lines 1-4/4 (END)
```

Configuring metricbeat for load, disk usage and memory

```
vi /etc/metricbeat/modules.d/system.yml
```

```
# Module: system
# Docs: https://www.elastic.co/guide/en/metricbeat/7.x/module-system.html

- module: system
  period: 10s
  metricsets:
    - cpu
    - load
    - memory
    - network
    - process
    - process_summary
    - socket_summary
  #- entropy
  #- core
  - diskio
  #- socket
  #- service
```

```
vi /etc/metricbeat/metricbeat.yml
```

```
#module
metricbeat.modules:
- module: system
  metricsets:
    - load
  enabled: true
  period: 5s
  index: "server1-metrics-load"

- module: system
  metricsets:
    - memory
  enabled: true
  period: 5s
  index: "server1-metrics-memory"

- module: system
  metricsets:
    - fsstat
  enabled: true
  period: 5s
  index: "server1-metrics-fsstat"

output.elasticsearch:
  hosts: ["192.168.1.93:9200"]
  username: "elastic"
  password: "123456"
  #index: "server1-metrics"

setup.ilm.enabled: false
setup.template.name: "server1-template"
setup.template.pattern: "server1-temp-pattern"

processors:
- add_host_metadata: ~

~
```

Starting metricbeat

systemctl start metricbeat


```

root@metricbeat:/etc/metricbeat# systemctl restart metricbeat
root@metricbeat:/etc/metricbeat# systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
   Loaded: loaded (/lib/systemd/system/metricbeat.service; disabled; vendor
   Active: active (running) since Tue 2021-11-30 16:01:21 +0545; 1s ago
     Docs: https://www.elastic.co/beats/metricbeat
   Main PID: 3161 (metricbeat)
    Tasks: 5 (limit: 2946)
   Memory: 49.1M
   CGroup: /system.slice/metricbeat.service
           └─3161 /usr/share/metricbeat/bin/metricbeat --environment systemd

```

```

नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.064+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.095+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.095+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.096+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.097+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.097+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.098+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.116+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.397+0545
नव सू ३० 16:01:22 metricbeat metricbeat[3161]: 2021-11-30T16:01:22.397+0545

```

Index management in kibana

Index Management

Index M

[Indices](#)
[Data Streams](#)
[Index Templates](#)
[Component Templates](#)

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)
Include rollup indices
Include

Lifecycle status
Lifecycle phase

<input type="checkbox"/>	Name	Health	Status	Primaries	Replicas	Docs count	Storage size
<input type="checkbox"/>	server1-metrics-memory	● yellow	open	1	1	335	936.8kb
<input type="checkbox"/>	server1-metrics-load	● yellow	open	1	1	333	563.9kb
<input type="checkbox"/>	server1-metrics-fsstat	● yellow	open	1	1	207	610kb