**ELK & APM Server Installation and configuration guide**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Name** | **Version** | **Prepared by** | **Reviewed by** |
| ELK & APM server Installation and configuration guide | v.01 | Tarunendra Tripathi | Sumit Malhotra |
|  |  |  |  |

Contents

[Reference URL 2](#_Toc61710011)

[Elastic Search 2](#_Toc61710012)

[RPM 2](#_Toc61710013)

[Other Linux: 2](#_Toc61710014)

[Make sure Elasticsearch is up and running 2](#_Toc61710015)

[Kibana 3](#_Toc61710016)

[MetricBeat 3](#_Toc61710017)

[RPM 3](#_Toc61710018)

[Ship system metrics to Elasticsearch 4](#_Toc61710019)

[RPM 4](#_Toc61710020)

[APM server 4](#_Toc61710021)

[RPM 4](#_Toc61710022)

[LogStash 4](#_Toc61710023)

[url 4](#_Toc61710024)

[step1 4](#_Toc61710025)

[Step2 5](#_Toc61710026)

[Step3 5](#_Toc61710027)

# Reference URL

Use below url for reference to install and configure the ELK and APM server.

[**https://www.elastic.co/guide/en/elastic-stack-get-started/7.10/get-started-elastic-stack.html#install-elasticsearch**](https://www.elastic.co/guide/en/elastic-stack-get-started/7.10/get-started-elastic-stack.html#install-elasticsearch)

# Elastic Search

Download the below rpm file for installation on RHEL server.

## RPM

curl -L -O https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.10.0-x86\_64.rpm

sudo rpm -i elasticsearch-7.10.0-x86\_64.rpm

sudo service elasticsearch start

## Other Linux:

curl -L -O https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.10.0-linux-x86\_64.tar.gz

tar -xzvf elasticsearch-7.10.0-linux-x86\_64.tar.gz

cd elasticsearch-7.10.0

./bin/elasticsearch

tar -xzvf elasticsearch-7.10.0-linux-x86\_64.tar.gz

cd elasticsearch-7.10.0

./bin/elasticsearch

## Make sure Elasticsearch is up and running

To test that the Elasticsearch daemon is up and running, try sending an HTTP GET request on port 9200.

curl http://127.0.0.1:9200

You should see a response similar to this:

{

"name" : "QtI5dUu",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "DMXhqzzjTGqEtDlkaMOzlA",

"version" : {

"number" : "7.10.0",

"build\_flavor" : "default",

"build\_type" : "tar",

"build\_hash" : "00d8bc1",

"build\_date" : "2018-06-06T16:48:02.249996Z",

"build\_snapshot" : false,

"lucene\_version" : "7.3.1",

"minimum\_wire\_compatibility\_version" : "5.6.0",

"minimum\_index\_compatibility\_version" : "5.0.0"

},

"tagline" : "You Know, for Search"

}

# Kibana

curl -L -O https://artifacts.elastic.co/downloads/kibana/kibana-7.10.0-linux-x86\_64.tar.gz

tar xzvf kibana-7.10.0-linux-x86\_64.tar.gz

cd kibana-7.10.0-linux-x86\_64/

./bin/kibana

# MetricBeat

## RPM

curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.10.0-x86\_64.rpm

sudo rpm -vi metricbeat-7.10.0-x86\_64.rpm

# Ship system metrics to Elasticsearch

1. From the Metricbeat install directory, enable the system module:

## RPM

sudo metricbeat modules enable system

1. Set up the initial environment:

Rpm:-

sudo metricbeat setup -e

1. Start Metricbeat:

Rpm:

sudo service metricbeat start

1. Metricbeat runs and starts sending system metrics to Elasticsearch.

****

# APM server

[**url:-**](file:///D:\DevOps\SBI_DevOps\SBI_DevOps\Docs\Devops%20install%20doc\SBI_installation%20docs\Documents\Installation_Documentes_16012021\Installation_Documentes\-)[**https://www.elastic.co/guide/en/apm/server/7.10/installing.html**](https://www.elastic.co/guide/en/apm/server/7.10/installing.html)

## RPM

curl -L -O https://artifacts.elastic.co/downloads/apm-server/apm-server-7.10.0-x86\_64.rpm

sudo rpm -vi apm-server-7.10.0-x86\_64.rpm

# LogStash

## url

use below url for reference.

<https://www.elastic.co/downloads/logstash>

## step1

Download and unzip Logstash

download tar file:- logstash-7.10.0-linux-x86\_64.tar.gz

tar –xzvf logstash-7.10.0-linux-x86\_64.tar.gz

## Step2

Prepare a logstash.conf **[config file](https://www.elastic.co/guide/en/logstash/current/configuration.html)**

Use below url for reference.

<https://www.elastic.co/guide/en/logstash/current/configuration.html>

Let’s step through creating a simple config file and using it to run Logstash. Create a file named "logstash-simple.conf" and save it in the same directory as Logstash

input { stdin { } }

output {

elasticsearch { hosts => ["localhost:9200"] }

stdout { codec => rubydebug }

}

Then, run logstash and specify the configuration file with the -f flag.

bin/logstash -f logstash-simple.conf

## Step3

To Run

bin/logstash -f logstash.conf