**Install ELK Stack on Linux**

This document outlines the steps involved to install version 6.8.0 of Elasticsearch, Logstash and Kibana.

**Install Java8**

sudo yum install java-1.8.0-openjdk-src.x86\_64

java -version

openjdk version "1.8.0\_212"

OpenJDK Runtime Environment (build 1.8.0\_212-b04)

OpenJDK 64-Bit Server VM (build 25.212-b04, mixed mode)

**Elasticsearch Installation:**

**1. Import the Elasticsearch public GPG key to the rpm package manager:**

sudo rpm --import http://packages.elastic.co/GPG-KEY-elasticsearch

**2. Configure the repo**

sudo vi /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-6.x]

name=Elasticsearch repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

**3. Install the Elasticsearch package.**

sudo yum install -y elasticsearch

**4. Start and enable the service**

sudo systemctl daemon-reload

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

**5. Allow traffic through TCP port 9200 in your firewall:**

sudo firewall-cmd --add-port=9200/tcp

sudo firewall-cmd --add-port=9200/tcp --permanent

If in case, if the above commands does n’t work, then install and start firewalld service

sudo yum install firewalld

sudo systemctl start firewalld

**6. Check if Elasticsearch responds to simple requests over HTTP**

curl -X GET http://localhost:9200

{

"name" : "Mephisto",

"cluster\_name" : "Elasticsearch",

"cluster\_uuid" : "nLTF7EFhR4e\_pC6yyMqocQ",

"version" : {

"number" : "2.4.6",

"build\_hash" : "5376dca9f70f3abef96a77f4bb22720ace8240fd",

"build\_timestamp" : "2017-07-18T12:17:44Z",

"build\_snapshot" : false,

"lucene\_version" : "5.5.4"

},

"tagline" : "You Know, for Search"

}

[root@ip-172-31-23-206 opt]#

**This completes the installation of Elasticsearch!!!**

**Logstash Installation:**

**1. Import the Elasticsearch public GPG key to the rpm package manager:**

sudo rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

**2. Configure the repo for logstash**

sudo vi /etc/yum.repos.d/logstash.repo

[logstash-6.x]

name=Elastic repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

**2. Install the Logstash package:**

sudo yum install -y logstash

3. Add a **SSL** certificate based on the IP address of the ELK server at the following line below the

[ v3\_ca ] section in /etc/pki/tls/openssl.cnf:

[ v3\_ca ]

subjectAltName = IP: <add your ip here>

**3. Generate a self-signed certificate valid for 365 days:**

cd /etc/pki/tls

openssl req -config /etc/pki/tls/openssl.cnf -x509 -days 3650 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/

Generating a RSA private key

.......................+++++

...............+++++

writing new private key to 'private/logstash-forwarder.key'

-----

**4. Configure Logstash input, output, and filter files:**

**Input**: Create /etc/logstash/conf.d/input.conf and insert the following lines into it. This is necessary for Logstash to “**learn**” how to process beats coming from clients. Make sure the path to the certificate and key match the right paths as outlined in the previous step:

[root@ip-172-31-23-206 tls]# vi /etc/logstash/conf.d/input.conf

input {

beats {

port => 5044

ssl => true

ssl\_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"

ssl\_key => "/etc/pki/tls/private/logstash-forwarder.key"

}

}

Output (/etc/logstash/conf.d/output.conf) file:

[root@ip-172-31-23-206 tls]# /etc/logstash/conf.d/output.conf

output {

elasticsearch {

hosts => ["localhost:9200"]

sniffing => true

manage\_template => false

index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"

document\_type => "%{[@metadata][type]}"

}

}

Filter (/etc/logstash/conf.d/filter.conf) file. We will log syslog messages for simplicity:

[root@ip-172-31-23-206 tls]# vi /etc/logstash/conf.d/filter.conf

filter {

if [type] == "syslog" {

grok {

match => { "message" => "%{SYSLOGLINE}" }

}

date {

match => [ "timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]

}

}

}

**5. Verify the Logstash configuration files.**

# [root@ip-172-31-23-206 tls]# service logstash configtest

Configuration OK

**6. Start and enable logstash**

[root@ip-172-31-23-206 tls]# sudo systemctl daemon-reload

[root@ip-172-31-23-206 tls]# sudo systemctl start logstash

[root@ip-172-31-23-206 tls]# sudo systemctl enable logstash

logstash.service is not a native service, redirecting to systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable logstash

[root@ip-172-31-23-206 tls]#

**7. Configure the firewall to allow Logstash to get the logs from the clients (TCP port 5044)**

[root@ip-172-31-23-206 tls]# sudo firewall-cmd --add-port=5044/tcp

success

[root@ip-172-31-23-206 tls]# sudo firewall-cmd --add-port=5044/tcp --permanent

success

[root@ip-172-31-23-206 tls]#

**This completes Logstash Installation!!!**

**Kibana Installation:**

**1. Import the Elasticsearch public GPG key to the rpm package manager:**

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

**2. Configure the repo for Kibana**

[root@ip-172-31-23-206 tls]# sudo vi /etc/yum.repos.d/kibana.repo

[kibana-6.x]

name=Kibana repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

**3. Install the Kibana Package**

[root@ip-172-31-23-206 tls]# sudo yum install -y kibana

**4. Start and enable Kibana**

[root@ip-172-31-23-206 tls]# sudo systemctl daemon-reload

[root@ip-172-31-23-206 tls]# sudo systemctl start kibana

[root@ip-172-31-23-206 tls]# sudo systemctl enable kibana

Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable kibana

Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.

[root@ip-172-31-23-206 tls]#

**5. Make sure you can access access Kibana’s web interface from another computer (allow traffic on TCP port 5601):**

[root@ip-172-31-23-206 tls]# sudo firewall-cmd --add-port=5601/tcp

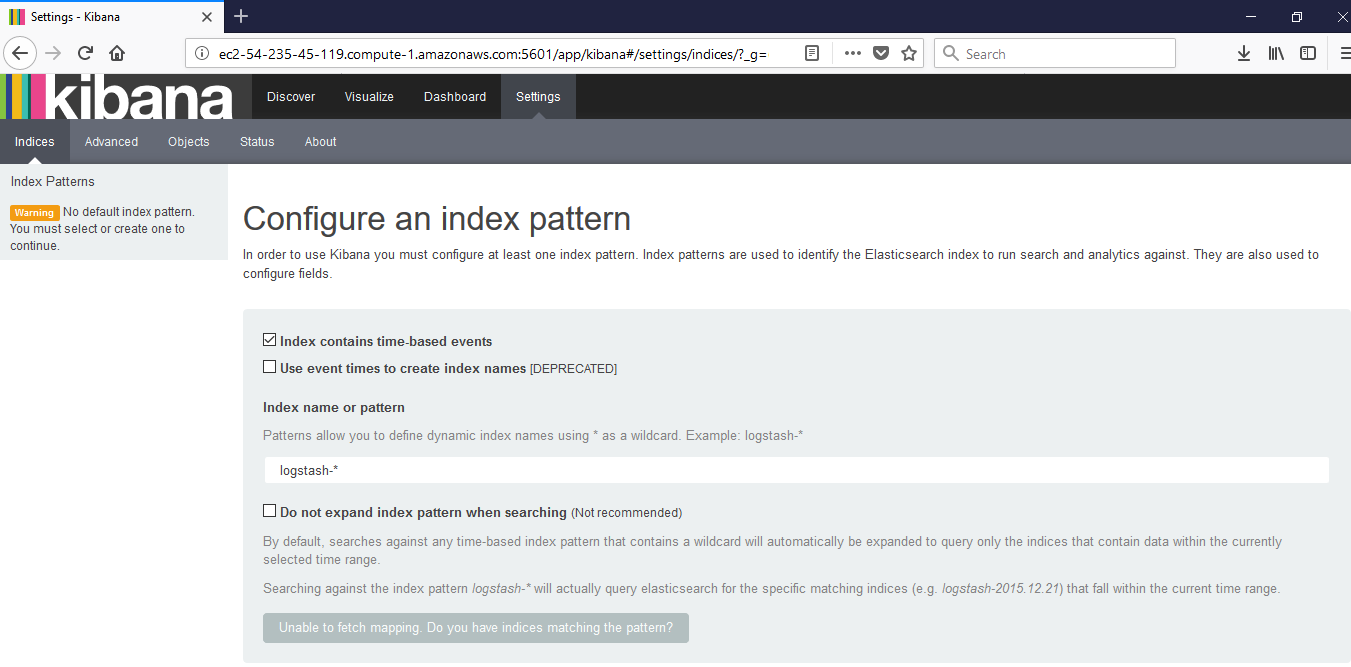
success

[root@ip-172-31-23-206 tls]# sudo firewall-cmd --add-port=5601/tcp --permanent

success

[root@ip-172-31-23-206 tls]#

**6. Launch Kibana (http://192.168.0.29:5601) to verify that you can access the web interface:**



**Install Filebeat on the Client Servers**

We will show you how to do this for **Client #1** (repeat for **Client #2** afterwards, changing paths if applicable to your distribution).

**1.** Copy the SSL certificate from the server to the clients:

[root@ip-172-31-23-206 tmp]# scp /etc/pki/tls/certs/logstash-forwarder.crt [root@3.88.85.40:/etc/pki/tls/certs/](mailto:root@3.88.85.40:/etc/pki/tls/certs/)

2. Import the **Elasticsearch** public GPG key to the rpm package manager

rpm --import http://packages.elastic.co/GPG-KEY-elasticsearch

3. Create a repository for **Filebeat on the Client**

**vi** /etc/yum.repos.d/filebeat.repo

[filebeat]

name=Filebeat for ELK clients

baseurl=https://packages.elastic.co/beats/yum/el/$basearch

enabled=1

gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch

gpgcheck=1

4. Install the **Filebeat** package:

[root@ip-172-31-94-89 ~]# yum install filebeat

5. Start and enable Filebeat:

[root@ip-172-31-94-89 ~]# systemctl start filebeat

[root@ip-172-31-94-89 ~]# systemctl enable filebeat

Created symlink from /etc/systemd/system/multi-user.target.wants/filebeat.service to /usr/lib/systemd/system/filebeat.service.

[root@ip-172-31-94-89 ~]#

#### Configure Filebeat

A word of caution here. **Filebeat** configuration is stored in a **YAML** file, which requires strict indentation. Be careful with this as you edit /etc/filebeat/filebeat.yml as follows:

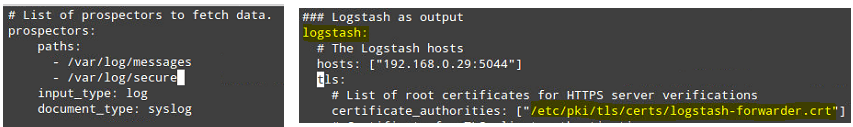
1. Under **paths**, indicate which log files should be “shipped” to the ELK server.
2. Under **prospectors**:

input\_type: log

document\_type: syslog

1. Under **output**:
   1. Uncomment the line that begins with **logstash**.
   2. Indicate the IP address of your ELK server and port where Logstash is listening in **hosts**.
   3. Make sure the path to the certificate points to the actual file you created in **Step I** (**Logstash** section) above.

The above steps are illustrated in the following image:

[](https://www.tecmint.com/wp-content/uploads/2016/09/Configure-Filebeat-in-Client-Servers.png)

Save changes, and then restart **Filebeat** on the clients:

[root@ip-172-31-94-89 ~]# systemctl restart filebeat

#### Testing Filebeat

In order to verify that the logs from the clients can be sent and received successfully, run the following command on the **ELK** server:

# curl -XGET 'http://localhost:9200/filebeat-\*/\_search?pretty'

The output should be similar to (notice how messages from **/var/log/messages** and **/var/log/secure** are being received from **client1** and **client2**):