1. **Install and configure file beat in application server**
2. **Install and configure logstash to collect logs from filebeat**
3. **Install and configure elastic search cluster**
4. **Install and configure kibana server**
5. **Generate self signed certificates and configure in Kibana server**

**Steps to deploy ELK stack in Single Ubuntu server :**

1. Build EC2 instance with Ubuntu in AWS
2. Login to EC2 server and run below command to update the package repo

apt-get update

1. File beat installation
2. Download and install the Public Signing Key:

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

1. You may need to install the apt-transport-https package on Debian before proceeding:

sudo apt-get install apt-transport-https

1. Save the repository definition to /etc/apt/sources.list.d/elastic-6.x.list:

echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list

1. Run apt-get update, and the repository is ready for use. For example, you can install Filebeat by running:

sudo apt-get update && sudo apt-get install filebeat

1. To configure the Beat to start automatically during boot, run:

sudo update-rc.d filebeat defaults 95 10

<https://github.com/elastic/puppet-elasticsearch>

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

yum install java-1.8.0-openjdk-devel

Kibana server installation :

# 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: "ec2-35-165-77-205.us-west-2.compute.amazonaws.com"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This only affects

# the URLs generated by Kibana, your proxy is expected to remove the basePath value before forwarding requests

# to Kibana. This setting cannot end in a slash.

#server.basePath: ""

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

#server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.

#server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.

#elasticsearch.url: "http://localhost:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host

# setting. When the value of this setting is false, Kibana uses the hostname of the host

# that connects to this Kibana instance.

#elasticsearch.preserveHost: true

# 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: "user"

#elasticsearch.password: "pass"

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.

# These settings enable SSL for outgoing requests from the Kibana server to the browser.

server.ssl.enabled: true

server.ssl.certificate: /etc/ssl/certs/kibana-selfsigned.crt

server.ssl.key: /etc/ssl/private/kibana-selfsigned.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.

# These files validate that your Elasticsearch backend uses the same key files.

#elasticsearch.ssl.certificate: /path/to/your/client.crt

#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the certificate

# authority for your Elasticsearch instance.

#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.

#elasticsearch.ssl.verificationMode: full

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of

# the elasticsearch.requestTimeout setting.

#elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value

# must be a positive integer.

#elasticsearch.requestTimeout: 30000

# List of Kibana client-side headers to send to Elasticsearch. To send \*no\* client-side

# headers, set this value to [] (an empty list).

#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten

# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.

#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.

#elasticsearch.shardTimeout: 0

# Time in milliseconds to wait for Elasticsearch at Kibana startup before retrying.

#elasticsearch.startupTimeout: 5000

# Specifies the path where Kibana creates the process ID file.

#pid.file: /var/run/kibana.pid

# Enables you specify a file where Kibana stores log output.

#logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.

#logging.silent: false

# Set the value of this setting to true to suppress all logging output other than error messages.

#logging.quiet: false

# Set the value of this setting to true to log all events, including system usage information

# and all requests.

#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance

# metrics. Minimum is 100ms. Defaults to 5000.

#ops.interval: 5000

# The default locale. This locale can be used in certain circumstances to substitute any missing

# translations.

#i18n.defaultLocale: "en"

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/kibana-selfsigned.key -out /etc/ssl/certs/kibana-selfsigned.crt

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.2.2-amd64.deb

sudo dpkg -i filebeat-6.2.2-amd64.deb