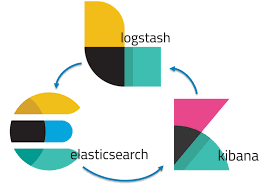
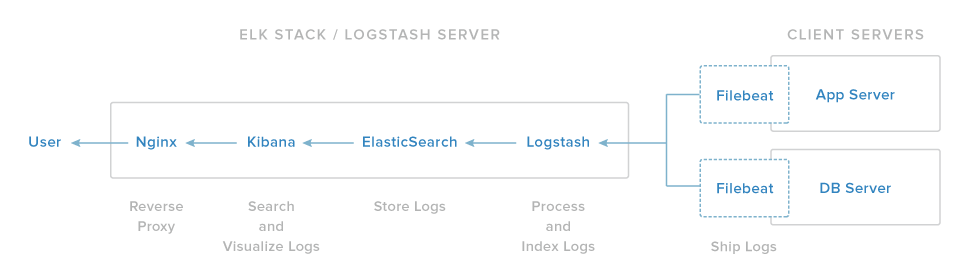
**ELK STACK IMPLEMENTATION ON A DOCKER BASED PLATFORM**



Our ELK stack setup has four main components:

* Logstash : The server component of Logstash that processes incoming logs or you can use Fluentd without using logstash for Log collections and parsing engine ([https://www.fluentd.org/](https://www.youtube.com/redirect?event=video_description&v=MNId4HG0wV8&redir_token=QUFFLUhqbm1fWlg4Sk9EUko1N0Fmd0oxVVV5b0JSS3M2UXxBQ3Jtc0tsd1ZlSXJOeHQxNmdUeEF6eE0tMDFpOS1VZkJXLXM2bDVOR2ZrVk9xVS1xTHdNdnExOFo5SDJRMjlaWmlGZlliLXptN3lKYnE5YVVWVk8yQnlOWlNZTjExUU14V2NMXzFXMFd6ek1WY2Rtc1NaMGprdw%3D%3D&q=https%3A%2F%2Fwww.fluentd.org%2F))
* Elasticsearch : Stores all of the logs
* Kibana :Web interface for searching and visualizing logs, which will be proxied through Nginx
* Filebeat : Installed on client servers that will send their logs to Logstash, Filebeat serves as a log shipping agent that utilizes the lumberjack networking protocol to communicate with Logstash



***Elastic Search***

***Apache lucene***

•*“Information retrieval software library”*

•Free/open source

•Supported by Apache Foundation

•Created by Doug Cutting

•Written in 1999

**Open source search server written in java**

•Used to index any kind of heterogeneous data

•Enables real-time ability to search through index

•Has REST API web-interface with JSON output

•**RESTfull** Service

•JSON API over HTTP

•Want to use it from PHP?

* CURL Requests, as if you’d do requests to the Facebook Graph API.

•**High Availability & Performance**

•Clustering

•Long Term **Persistency**

•Write through to persistent storage system.

• Based on top Lucence

• Multi-language support

• Geolocation support

• Full-text search

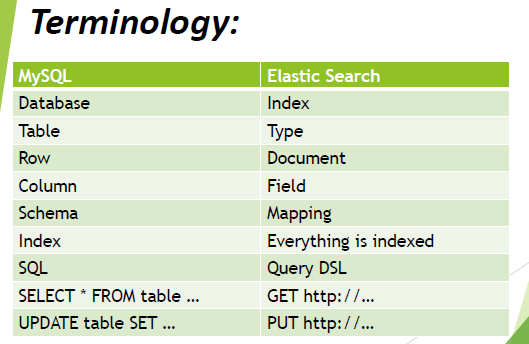
• Did-you-mean suggestions

• Extremely speed

• Support **RESTful**

• Text and number

• Scoring



**Logstash**

•Framework for managing logs

•Founded by Jordan Sissel

•Mainly consists of 3 components:

* Input : passing logs to process them into machine understandable format(file, lumberjack).
* filters: set of conditionals to perform specific action on a event(grok, geoip).
* output: decision maker for processed event/log(elasticsearch, file)

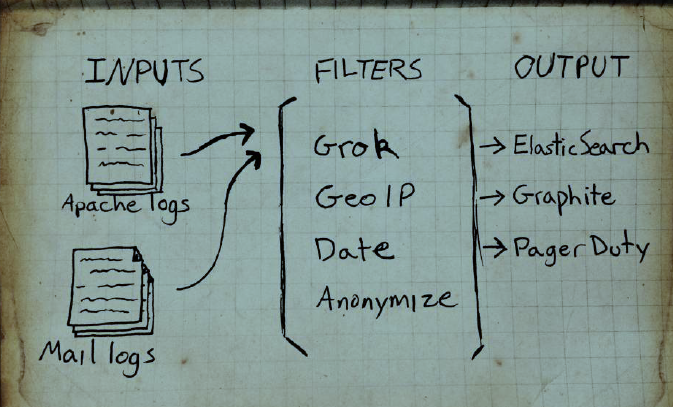
• Multiple Input / MultipleOutput

• Centralize Logs

• Collect

• Parse

• Store /Forward



Processing example

127.0.0.1 - - [05/Feb/2014:17:11:55 +0000] "GET /css/main.css HTTP/1.1" 200 140

"http://www.onet.pl" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:2.0.1)

Gecko/20100101 Firefox/4.0.1"

{

"host" : "127.0.0.1",

"@timestamp" : "2014-02-05T17:11:55+0000",

..."verb" : "GET"

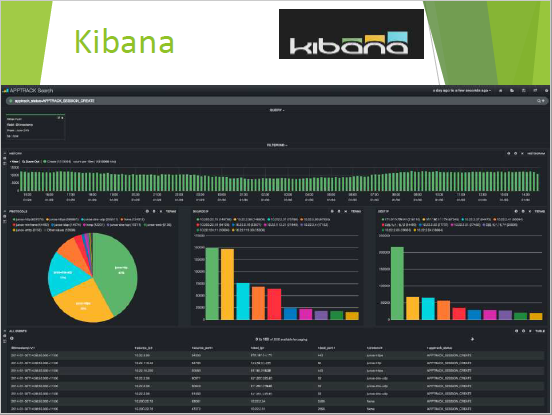
}

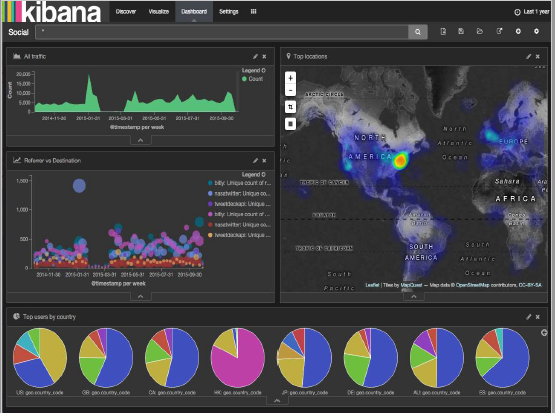
**Kibana**

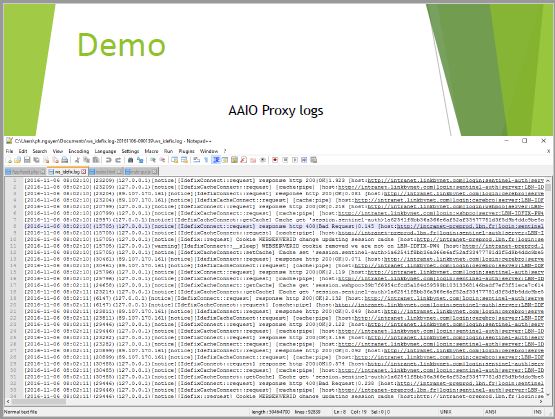
•Powerful front-end dashboard for visualizing indexed information from elastic cluster.

•Capable to providing historical data in form of graphs, charts, etc.

•Enables real-time search of indexed information.



****





**Filebeat**

**APT**

To add the Beats repository for APT:

1. 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-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

The package is free to use under the Elastic license. An alternative package which contains only features that are available under the Apache 2.0 license is also available. To install it, use the following sources list:

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

To add the Elastic repository, make sure that you use the echo method shown in the example. Do not use add-apt-repository because it will add a deb-src entry, but we do not provide a source package.

If you have added the deb-src entry by mistake, you will see an error like the following:

Unable to find expected entry 'main/source/Sources' in Release file (Wrong sources.list entry or malformed file)

Simply delete the deb-src entry from the /etc/apt/sources.list file, and the installation should work as expected.

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 Filebeat to start automatically during boot, run:

sudo systemctl enable filebeat

or download deb package of 6.5.4 from

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.5.4-amd64.deb

**ELK stack setup with docker run command**

Scope: Using 3 different Docker images (official Elastic docker images)

- Step 1: Setup Elasticsearch container and verify elastic its working

**docker run -d -p 9200:9200 -p 9300:9300 -it -h elasticsearch --name elasticsearch elasticsearch**

curl http://localhost:9200/

eg: *docker run -d -p 192.168.50.112:9200:9200 -p 192.168.50.112:9300:9300 -it -h elasticsearch --name elasticsearch elasticsearch:6.5.4*

- Step 2: Setup Kibana container

**docker run -d -p 5601:5601 -h kibana --name kibana --link elasticsearch:elasticsearch kibana**

curl <http://localhost:9200/_cat/indices>

eg: *docker run -d -p 192.168.50.112:5601:5601 -h kibana --name kibana --link elasticsearch:elasticsearch kibana:6.5.4*

- Step 3: Create logstash config file and use it to setup Logstash container

**docker run -h logstash --name logstash --link elasticsearch:elasticsearch -it --rm -v "$PWD":/config-dir logstash -f /config-dir/logstash.conf**

curl http://localhost:9200/\_cat/indices

**docker run -d -p 9500:9500 -h logstash2 --name logstash2 --link elasticsearch:elasticsearch --rm -v "$PWD":/config-dir logstash -f /config-dir/logstash2.conf**

Logstash:

Once the Elasticsearch is up and running, we will now ready to run the Logstash container. Before starting the Logstash container, create a configuration file to receive the logs from the beats.

Create the directory and configuration file on the Docker host.

mkdir /logstash

vi /logstash/logstash.conf

Below configuration file is to receive the logs with log type “**syslog**” on port “**5044** “and send them to Elasticsearch for indexing.

input {

 beats {

 port => 5044

 }

 }

filter {

if [type] == "syslog" {

    grok {

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

    }

    date {

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

}

  }

}

output {

 elasticsearch {

  hosts => ["elasticsearch:9200"]

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

       }

stdout {

    codec => rubydebug

       }

}

In the above configuration file, if you see the output section; elasticsearch host is defined as **elasticsearch:9200**. You might think that how the Logstash will resolve that host to send logs, do not worry; Docker linking (**–link**) will take care of that.

cd /logstash/

Create a Logstash container by issuing the following command.

Where,

**–link elasticsearch-container-name:hostname-in-config-file**

docker run -d --name logstash -p 5044:5044 --link elasticsearch:elasticsearch -v "$PWD":/logstash logstash -f /logstash/logstash.conf

eg: ***docker run -d --name logstash -p 5044:5044 --link elasticsearch:elasticsearch -v "$PWD":/logstash logstash:6.5.4 -f /logstash/logstash.conf***

**Kibana configuration for logstash-filebeat module**

*Infrastructure > setup instructions > add data to kibana > logging > logstash logs> self managed > deb*

1. Download and install Filebeat

**curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.5.4 amd64.deb**

***sudo dpkg -i filebeat-6.5.4-amd64.deb***

1. Edit the configuration

Modify **/etc/filebeat/filebeat.yml** to set the connection information:

output.elasticsearch:

hosts: ["<es\_url>"]

username: "elastic"

password: "<password>"

setup.kibana:

host: "<kibana\_url>"

*Where <password> is the password of the elastic user, <es\_url> is the URL of Elasticsearch, and <kibana\_url> is the URL of Kibana*.

1. Enable and configure the logstash module

***sudo filebeat modules enable logstash***

1. Modify the settings in the /etc/filebeat/modules.d/logstash.yml file.

Configure the module

* You can further refine the behavior of the logstash module by specifying [variable settings](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-logstash.html#logstash-settings) in the modules.d/logstash.yml file, or overriding settings at the command line.
* The following example shows how to set paths in the modules.d/logstash.yml file to override the default paths for Logstash logs and set the format to json

- module: logstash

log:

enabled: true

var.paths: ["/path/to/log/logstash.log\*"]

var.format: json

slowlog:

enabled: true

var.paths: ["/path/to/log/logstash-slowlog.log\*"]

var.format: json

To specify the same settings at the command line, you use:

-M "logstash.log.var.paths=[/path/to/log/logstash/logstash-server.log\*]" –M "logstash.slowlog.var.paths=[/path/to/log/logstash/logstash-slowlog.log\*]"

1. Start Filebeat

The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

***sudo filebeat setup***

***sudo service filebeat start***

***filebeat –e***

1. Module status

Check that data is received from the Filebeat logstash module

Check status

When all steps are complete, you're ready to explore your data.

**Logstash logs dashboard**

**Docker compose for ELK stack and Jenkins**

**Readme**

Installations should be done in an order

\* Elastic search

\* Kibana

\* Logstash

\* File beats

\*\*Filebeat can be installed in host and it can be configured to input data to logstash for further process

* *wget*[*https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.8.0-amd64.deb*](https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.8.0-amd64.deb)
* *dpkg -i filebeat-7.8.0-amd64.deb*
* *systemctl enable filebeat*
* *systemctl start filebeat*
* ***edit the /etc/filebeat/filebeat.yml***

Change the filebeat.input section

**- type: log**

enabled: true

**paths:**

"specify the path where the logs to be fetched"

Change the output section of logstash

**output.logstash**

**hosts: ["192.168.50.112:5044"]**

* *systemctl restart filebeat*

Work flow : **Filebeat(ship logs)-->Logstash(Process and Index logs)-->Elastic Search(store logs)-->Kibana(search and visualize logs)-->Nginx(reverse proxy) -->user**

If you want to test this docker compose files in your pc, kindly change ip's mentioned in it to your local host ip.

ELK stack implementation on a docker based platform for monitoring.

* **Elastic Search Docker compose**

version: '2.2'

services:

es:

image: docker.elastic.co/elasticsearch/elasticsearch:7.8.0

container\_name: es

environment:

- node.name=es

- cluster.name=es-docker-cluster

- cluster.initial\_master\_nodes=es

- bootstrap.memory\_lock=true

- "ES\_JAVA\_OPTS=-Xms512m -Xmx512m"

ulimits:

memlock:

soft: -1

hard: -1

volumes:

- data01:/usr/share/elasticsearch/data

ports:

- 9200:9200

networks:

- elastic

volumes:

data01:

driver: local

networks:

elastic:

driver: bridge

* **Kibana Docker compose**

version: '2'

services:

kibana:

image: docker.elastic.co/kibana/kibana:7.8.0

ports:

- 5601:5601

environment:

SERVER\_NAME: kibana.ccs.org

ELASTICSEARCH\_HOSTS: <http://192.168.50.112:9200>

* **Logstash docker compose**

version: "3.3"

services:

logstash:

image: docker.elastic.co/logstash/logstash:7.8.0

volumes:

- type: bind

source: ./config/logstash.yml

target: /usr/share/logstash/config/logstash.yml

- type: bind

source: ./pipeline

target: /usr/share/logstash/pipeline

ports:

- "192.168.50.112:5044:5044/tcp"

- "192.168.50.112:5000:5000/udp"

- "192.168.50.112:9600:9600"

environment:

LS\_JAVA\_OPTS: "-Xmx256m -Xms256m"

***Config and pipeline should be in the same folder where docker-compose.yml is located***

**Config file (logstash.yml)**

## Default Logstash configuration from Logstash base image. https://github.com/elastic/logstash/blob/master/docker/data/logstash/config/logstash-full.yml

#

http.host: "0.0.0.0"

xpack.monitoring.elasticsearch.hosts: [ "http://192.168.50.112:9200" ]

## X-Pack security credentials

#

xpack.monitoring.enabled: true

**Pipeline(logstash.conf and Jenkins.conf)**

**logstash.conf**

input {

beats {

port => 5044

}

}

output {

elasticsearch {

hosts => ["192.168.50.112:9200"]

index => "appdata"

}

}

**jenkins.conf**

input {

beats {

port => 5044

}

}

output {

elasticsearch {

hosts => ["192.168.50.112:9200"]

index => "jenkins"

}

}

* **Filebeats**

**Configurations in /etc/filebeat/filebeat.yml**

* **Jenkins docker compose**

version: "3.2"

services:

jenkins:

image: cd14cecfdb3a

ports:

- "192.168.50.112:8080:8080"

- "192.168.50.112:50000:50000"

volumes:

- /apps/data/jenkins-data:/var/jenkins\_home

- /var/run/docker.sock:/var/run/docker.sock

restart: always