Introduction

Students, write your response!

Pear Deck Interactive Slide
Do not remove this bar

Table of Contents

- What is ELK?
- Why to choose ELK?
- Logstash
- ElasticSearch
- Kibana
- Beats

1 What is ELK?

What is ELK Stack :

- ELK Stack or more recently called Elastic Stack, is a combination of three open source projects — Elasticsearch, Logstash and Kibana — all developed by Elastic and used for storing and analyzing logs.
- Even though these are three separate products, they compliment each other to the extend that they have come to be recognised as one.

What is ELK Stack :

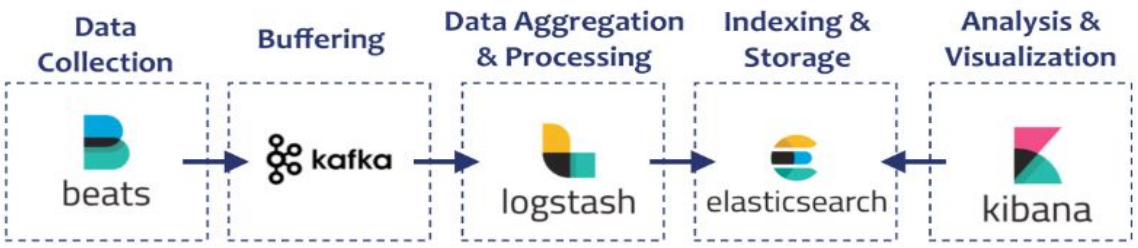
- Logstash collects the logs. It even parses and transforms the data. The data that is transformed by Logstash is stored, searched, and indexed in Elasticsearch. Then we use Kibana to visualize and explore this data indexed in Elasticsearch.

What is ELK Stack :

- There is one more component — Beats — which collects the data and sends it to Logstash. This led Elastic to rename ELK as the Elastic Stack.

What is ELK Stack :

- Further, if we are dealing with very large data, we could provide buffering mechanism using Kafka, RabbitMQ etc to send data from Beats to Logstash.

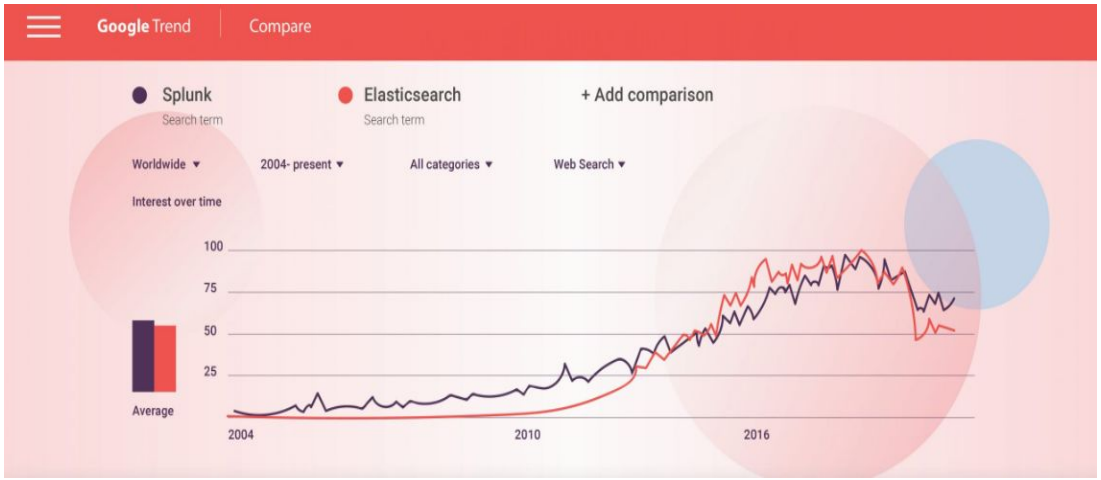


1

Why ELK?

Why ELK?

- ELK vs. Splunk on Google Trend:The ELK Stack is now downloaded 500,000 times every month, making it the world's most popular log management platform.



Why ELK?

- Rapid on-premise (or cloud) installation and easy to deploy
- Scales vertically and horizontally
- Easy and various APIs to use
- Availability of libraries for most programming/scripting languages
- Tools availability
- It's free (open source), and it's quick.

Logstash

- Logstash is the data collection pipeline tool. It collects data inputs and feeds into the Elasticsearch. It gathers all types of data from the different source and makes it available for further use.
- Logstash can unify data from disparate sources and normalize the data into your desired destinations. It allows you to cleanse and democratize all your data for analytics and visualization of use cases.

Logstash

- Managing events and logs
- Collect data
- Parse data
- Enrich data
- Store data
- Open Source:Apache License 2.0

logstash

Logstash

Input

- datastore
- stream
- logfiles
- files
- monitoring
- queues
- network

Filter

logstash

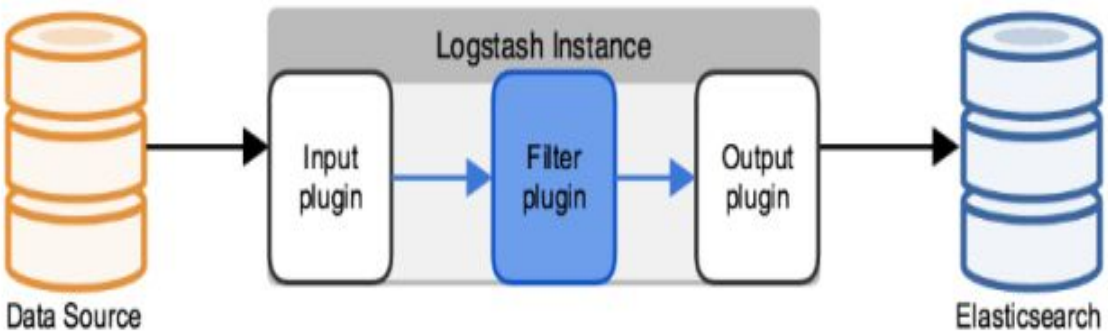
parse,enrich.tag,drop

Output

- datastore
- files
- email
- pager
- monitoring
- chat
- API
- queues

Logstash

Deploying Logstash



Logstash

How logstash works

```
input {
  file {
    path => "/tmp/access_log"
    start_position => "beginning"
  }
}
```

```
filter {
    grok {
        match => { "message" => "%{COMBINEDAPACHELOG}"}
    }
}
```

```
output {
    elasticsearch {
    }
}
```


Logstash

Example: Web server log files

```
      "message" => "83.149.9.216 - - [28/May/2014:16:13:42 -0500] \"GET /
presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1\"
200 203023 \"http://semicomplete.com/presentations/logstash-
monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/
537.36\"",

      "@version" => "1",
    "@timestamp" => "2014-05-28T21:13:42.000Z",
          "host" => "kryptic.local",
      "clientip" => "83.149.9.216",
         "ident" => "-",
          "auth" => "-",
     "timestamp" => "28/May/2014:16:13:42 -0500",
          "verb" => "GET",
       "request" => "/presentations/logstash-monitorama-2013/images/
kibana-search.png",
   "httpversion" => "1.1",
      "response" => "200",
         "bytes" => "203023",
      "referrer" => "\"http://semicomplete.com/presentations/logstash-
monitorama-2013/\"",
         "agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/
537.36\""
```

grok

date

Logstash

Example: Web server log files

ElasticSearch

- Elasticsearch is a NoSQL database. It is based on Lucene search engine, and it is built with RESTful APIS.
- Elasticsearch offers simple deployment, maximum reliability, and easy management. It also offers advanced queries to perform detail analysis and stores all the data centrally. It is helpful for executing a quick search of the documents.
- Elasticsearch also allows you to store, search and analyze big volume of data. Modern web and mobile applications have adopted it in search engine platforms.

ElasticSearch

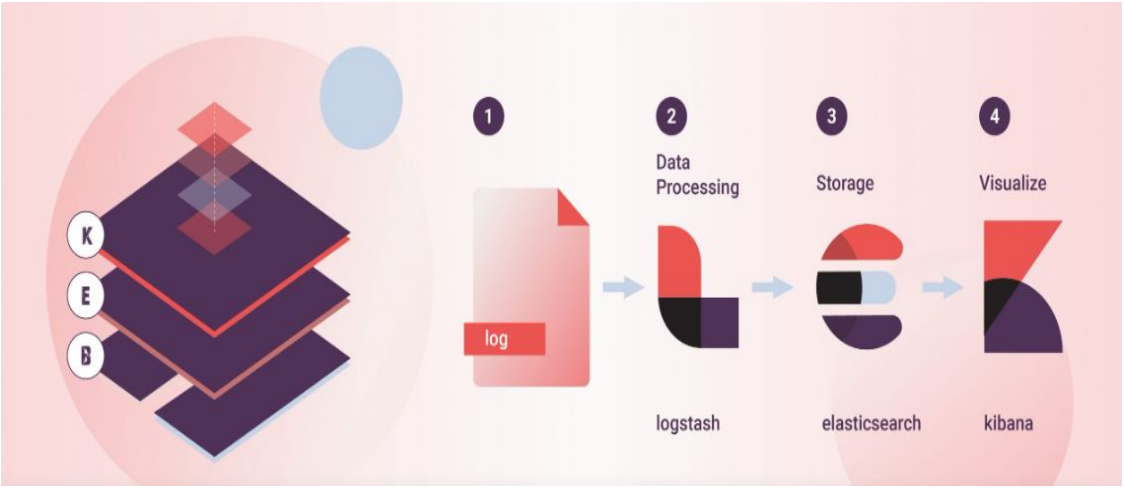
• Wikipedia uses Elasticsearch to provide full-text search with highlighted search snippets, andsearch-as-you-type and did-youmean suggestions

• The Guardian uses Elasticsearch to combine visitor logs with social-network data to provide real-time feedback to its editors about the public's response to new articles

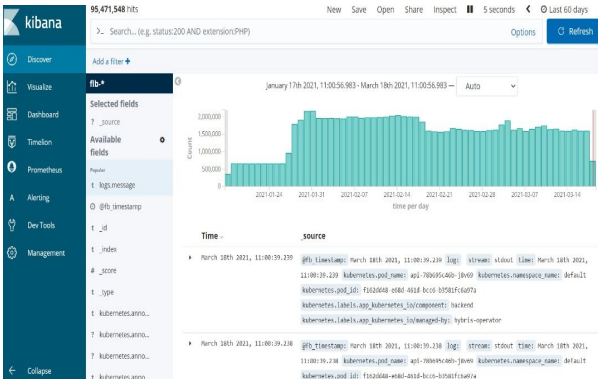
• Stack Overflow combines full-text search with geolocation queries and uses more-like-this to find related questions and answers

• GitHub uses Elasticsearch to query 130 billion lines of code

ElasticSearch



Kibana



Kibana

- Kibana is a data visualization which completes the ELK stack. This tool is used for visualizing the Elasticsearch documents and helps developers to have a quick insight into it. Kibana dashboard offers various interactive diagrams, geospatial data, and graphs to visualize complex queries.

- It is used to search, view, and interact with data stored in Elasticsearch directories and helps you to perform advanced data analysis and visualize your data in a variety of tables, charts, and maps.

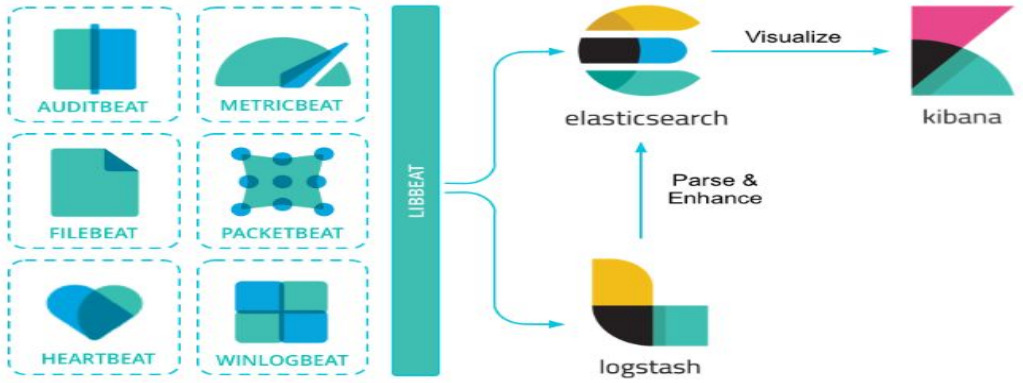
Kibana

- Search, view, and interact with data stored in Elasticsearch indices
- Execute queries on data & visualize results in charts, tables, and maps
- Add/remove widgets
- Share/Save/Load dashboards
- Open Source: Apache License 2.0

Beats

- Beats is a free and open platform for single-purpose data shippers. They send data from hundreds or thousands of machines and systems to Logstash or Elasticsearch.

Beats



Beats

The Beats family

All kinds of shippers for all kinds of data.

Filebeat
Lightweight shipper for logs and other data
→

Metricbeat
Lightweight shipper for metric data
→

Packetbeat
Lightweight shipper for network data
→

Winlogbeat
Lightweight shipper for Windows event logs
→

Auditbeat
Lightweight shipper for audit data
→

Heartbeat
Lightweight shipper for uptime monitoring
→

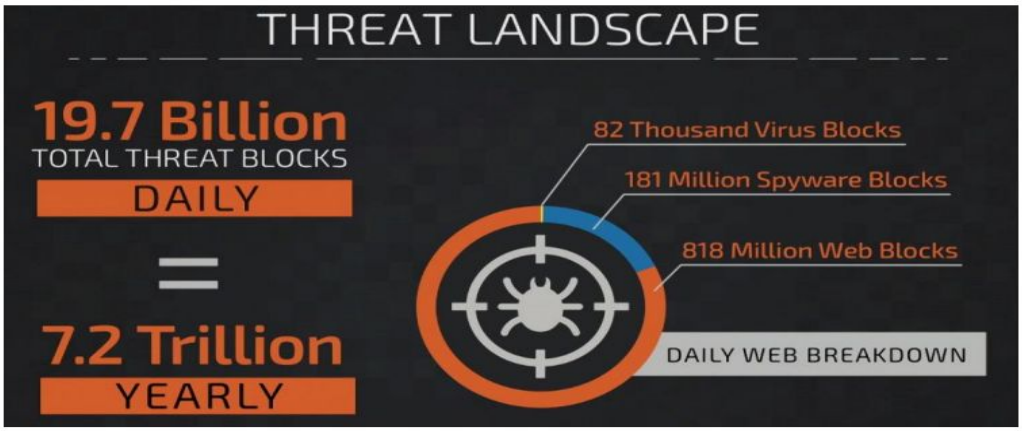
Functionbeat
Serverless shipper for cloud data
→

Use Cases

User Cases

User Cases

Cisco Talos Security Intelligence and Research Group: Hunting for Hackers



THANKS!

Any questions?

You can find me at:

- alex.d@clarusway.com