ELK MONITORING

ELASTIC SEARCH, KIBANA, LOGSTASH, & HEARTBEAT.

DEVOPS INTERNSHIP PROGRAM, SEPTEMBER 2019

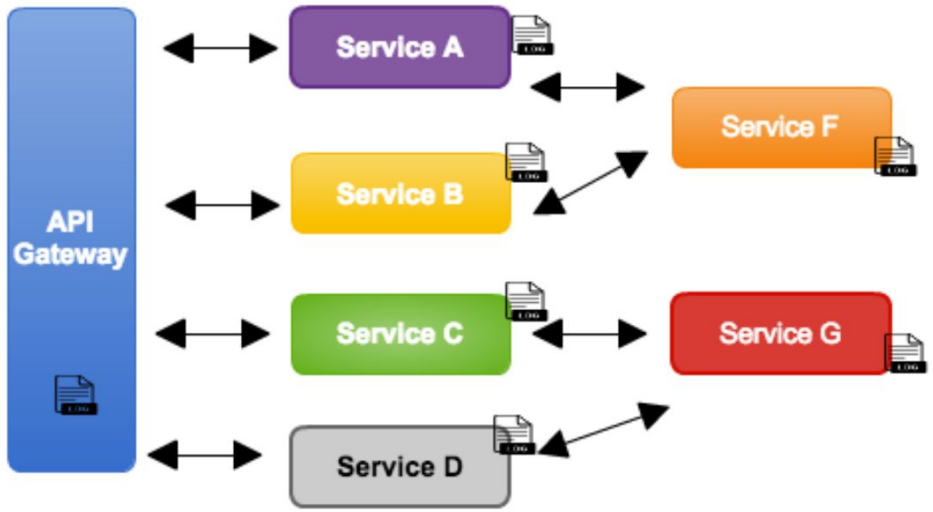
AGENDA

- ELASTIC STACK
- BEATS TOOLS
- HEARTBEAT
- ELK + BEATS
- STACK WORKSHOP

ELASTIC STACK

WHY WE NEED ELK MONITORING?

When we have a microservice-based architecture, one of the main problems we are about to start is how to see the application logs and try to find problems. Even more, when cloud-oriented solutions focus on logs that can be distributed on many machines or providers.



From the outset of the project, the logs should be a concern, and as the project grows, the trail of errors and success should be easily found.

Depending on the organization, a mistake can cost a lot of money or even stop a business's operation for a few hours, causing a lot of damage. Here, the ELK stack comes to the rescue.

ELASTIC STACK

ELASTICSEARCH: THE HEART

Initially released in 2010, Elasticsearch is a modern search and analytics engine which is based on Apache Lucene. Completely open source and built with Java. Categorized as a NoSQL database, its stores data in an unstructured way and that you cannot use SQL to query it.

Unlike most NoSQL databases, though, Elasticsearch has a strong focus on search capabilities and features, the easiest way to get data from Elasticsearch is to search for it using its extensive REST API.

- Is a highly scalable full-text search and analysis engine.
- Allows storing, searching, and analyzing large volumes of data in near real time.
- RESTful distributed search and analysis tool, and it centrally stores data

elasticsearch

ELASTIC STACK

LOGSTASH: THE MANAGER

It is a processing pipeline that ingests data from a multitude of sources at once, transforms it, and then sends it to databases. Data is usually scattered or spread across many systems in various formats.

Supports a variety of entries that draw events from multiple common sources all at the same time. Easily ingest logs, metrics, web applications, data storage, and various services.

As the data arrives, the Logstash filters analyze each event, identify the named fields to build the structure, and transform them to converge in a common format for analysis.

- Responsible for collecting the data.
- Make transformations, like parsing using regular expressions.
- If need it adding fields, and formatting as structures like JSON, etc.
- Sending the data to various destinations, like an ElasticSearch cluster

logstash

ELASTIC STACK

KIBANA: THE VIEW

Basically an analytics and visualization platform, which lets you easily visualize data from Elasticsearch and analyze it to make sense of it. You can assume Kibana as an Elasticsearch dashboard where you can create visualizations such as pie charts, line charts, and many others.

Kibana also provides an interface to manage the authentication and authorization of Elasticsearch. You can literally think of Kibana as a web interface to the data stored on Elasticsearch.

- Web-based application providing a light and easy-to-use dashboard tool.
- Allows you to view your Elasticsearch data and navigate through it.
- Create filters, aggregations, counts, and combinations.

BEATS TOOLS

WHERE BEATS STARTED...

In centralized logging, a data pipeline consists of three main stages: **aggregation, processing, and storage**. In the ELK Stack, the first two stages were traditionally the responsibility of Logstash, the stack's workhorse.

Executing these tasks comes at a cost. Due to inherent issues related to how Logstash was designed, **performance issues became a frequent occurrence**, especially with complicated pipelines that require a large amount of processing.

The idea of outsourcing some of Logstash's responsibilities also came into being, especially the task of data extraction to other tools. The idea first manifested itself in Lumberjack and later in the Logstash forwarder. Eventually, a few cycles of development later, a new and improved protocol was introduced that became the backbone of what is now called **the Beats family**.

endava

HEARTBEAT

UPTIME MONITORING

Beats is basically a collection of data shippers. Data shippers are basically lightweight agents with a particular purpose. You can install one or more data shippers on your server(s) as per the requirements. They then send data to Elasticsearch or Logstash.

There is *n* number of data shippers and each data shipper is called a beat. Each beat or data shipper collects different kinds of data and hence serves different purposes.

Heartbeat monitor services for their availability with active probing. Given a list of URLs, Heartbeat asks the simple question: Are you alive? Heartbeat ships this information and response time to the rest of the Elastic Stack for further analysis.

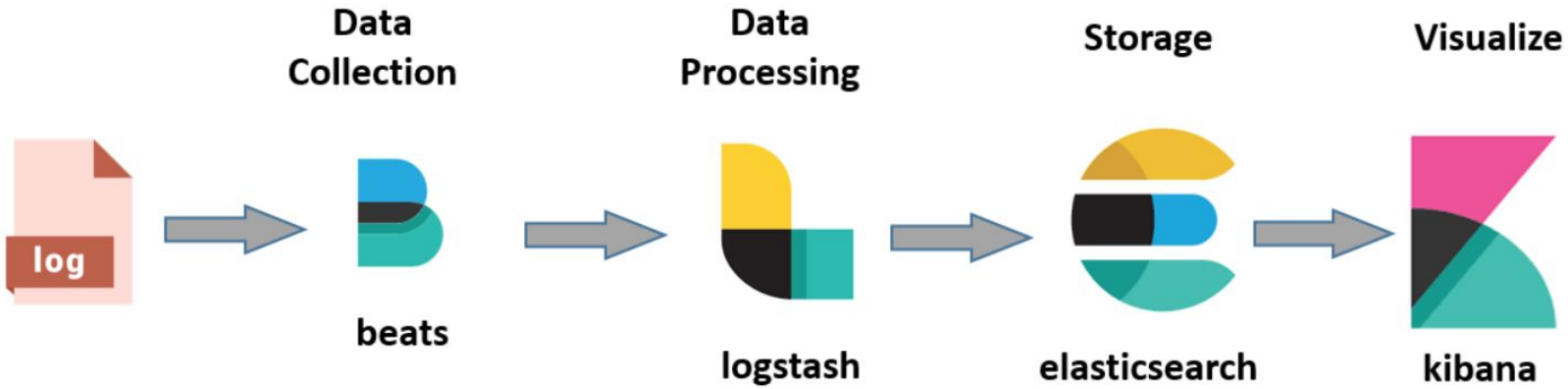
- Pings via ICMP, TCP, and HTTP, and also has support for TLS
- Automate the process of adding and removing monitoring targets by file-based interface.
- Holds onto incoming data and then ships it to Elasticsearch or Logstash when things are back on.

ELK + BEATS

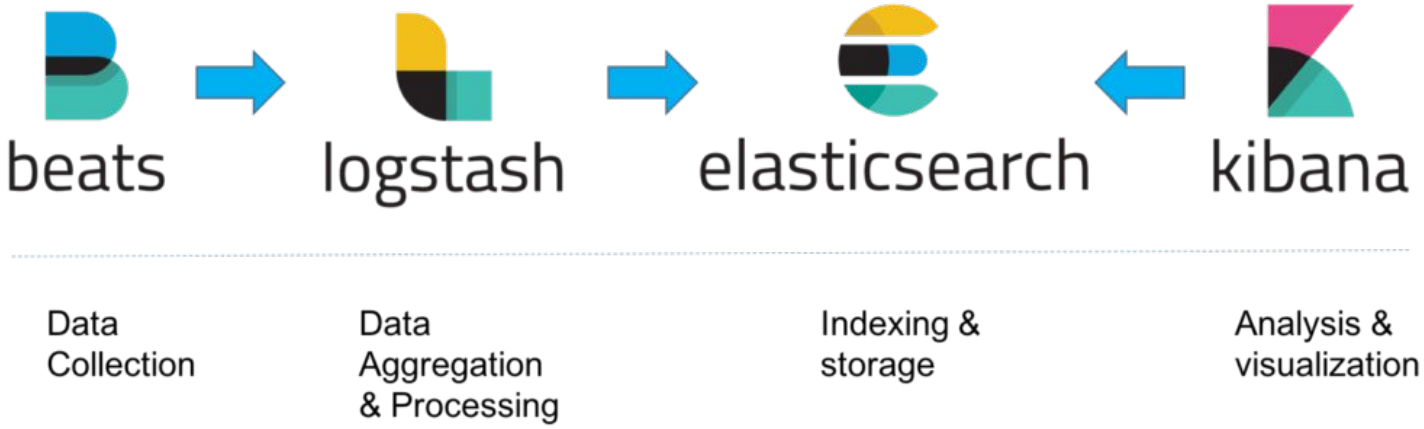
Putting all of the pieces together now. The **center of the Elastic Stack is Elasticsearch**, which contains the data.

Ingesting data into Elasticsearch can be done with Beats and/or Logstash, but also directly through its API.

Kibana is a user interface that sits on top of Elasticsearch and lets you visualize the data that it retrieves from Elasticsearch through the API. It's a wonderful tool that can save a lot of time when building data dashboards.



STACK WORKSHOP



https://github.com/twogg-git/java-elk

- Monitor a Spring Boot application log and API beats with the ELK Stack.
- Practice with Kibana Dashboards and indexing tools.
- Follow each ELK setup and understand connections and events setup.

ELK MONITORING

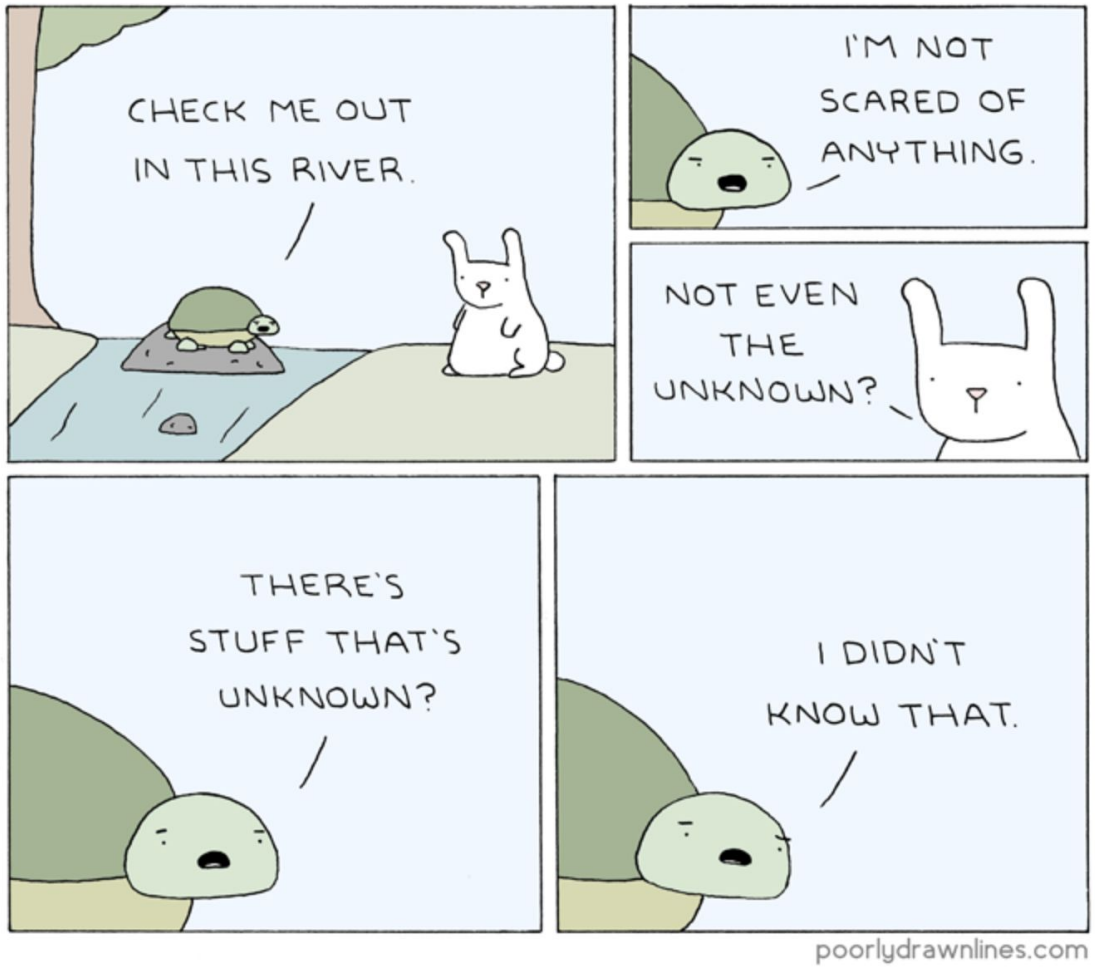
ELK STACK IS THE WORLD'S MOST POPULAR LOG ANALYSIS PLATFORM.

TREAT ALL THE LOG MESSAGES GENERATED AS SOME SORT OF EVENT AND STREAM IT INTO A SINGLE STORAGE, ORDERED BY TIMESTAMP.

Logstash processes the data before sending it to Elasticsearch for indexing and storage.

Kibana is the visualization tool with which you can view the log, create graphs and visualizations.

Beats is not a Logstash replace. Beats acts as a lightweight log shipper for specific use cases, while Logstash is responsible for the heavy lifting, acting as an aggregator and processor.



Thank you!

CATHERINE CRUZ

DEVOPS ENGINEER

https://github.com/twogg-git

catherine.cruz@endava.com