Continuous Monitoring – Part 3

This lesson discusses ELK stack monitoring logs in distributed systems.

We'll cover the following

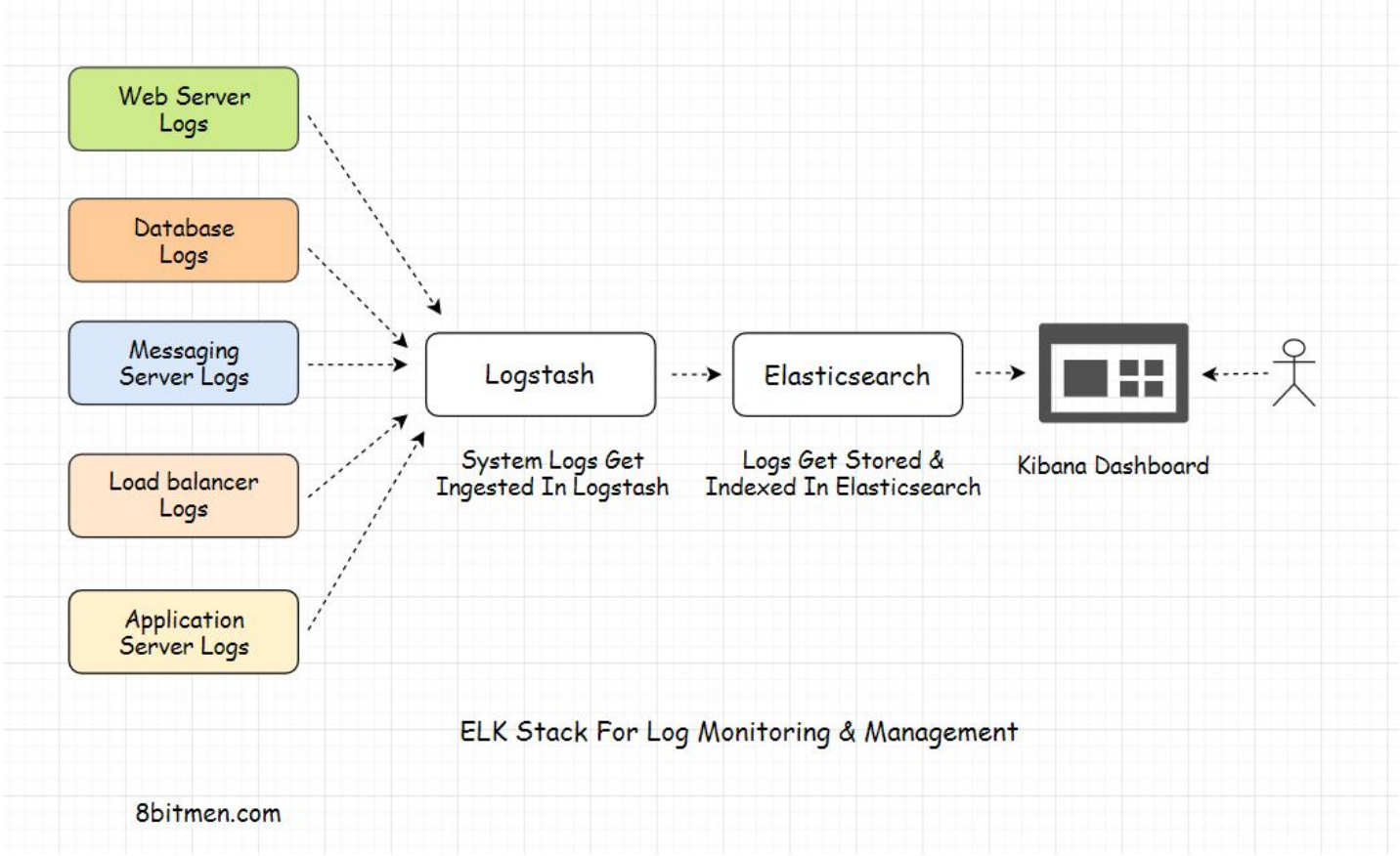
Monitoring logs with ELK

ELK stands for *Elastic Logstash Kibana*. *Elasticsearch* was the first and product originally released by the developers of the *ELK* stack. It's a search and analytics engine. *Logstash* and *Kibana* were released later.

Logstash is a data processing pipeline that ingests data from multiple sources and then converts the ingested data into a standard format to be stored in the *Elasticsearch* datastore. The *Elasticsearch* store is a *document-oriented* store.

In our use case, *Logstash* will ingest logs in different formats from various components in our application, such as *database, application server, web server, message server*, and so on, and will convert all the logs in a single standard format to be stored in the *Elasticsearch* datastore.

Kibana is the visual dashboard that acts as a centralized log dashboard for all the logs that are ingested from the different components in the application. With the help of *Kibana*, developers can easily debug the issues in any component of the application by going through the log details of that component in the *Kibana* dashboard.



To build a more customized and complex pipeline intended to handle a large amount of data, we can also set up a message queue like *RabbitMQ* or *Kafka* before the *Logstash* component.

Again, there is no standard rule for setting up a data ingestion pipeline, we can always set it up according to our business requirements.

AWS and *Google Cloud* both provide managed *ELK* stack service.

Though the *ELK* stack is primarily used for log analysis, it's not limited to just that. The *Elasticsearch* ecosystem provides a complete application observability solution that entails *log monitoring, infrastructure monitoring, application performance monitoring*, and so on.

So, this was pretty much it on application monitoring. In the next lesson, let's talk about *DevOps*.