IoT Monitoring

ELC Stack

AURIGA
the banking e-volution

THE # NEXTGENBANK

www.aurigaspa.com

Monitoring

Monitor the behavior of the system is important for:

- health checks
- metrics collection (which is important for anomaly detection, root cause analysis, trend detection and capacity planning)

Monitoring systems typically integrate with external alerting systems and analytics tools in order to provide prompt anomaly notifications and useful insights to the interested parties.

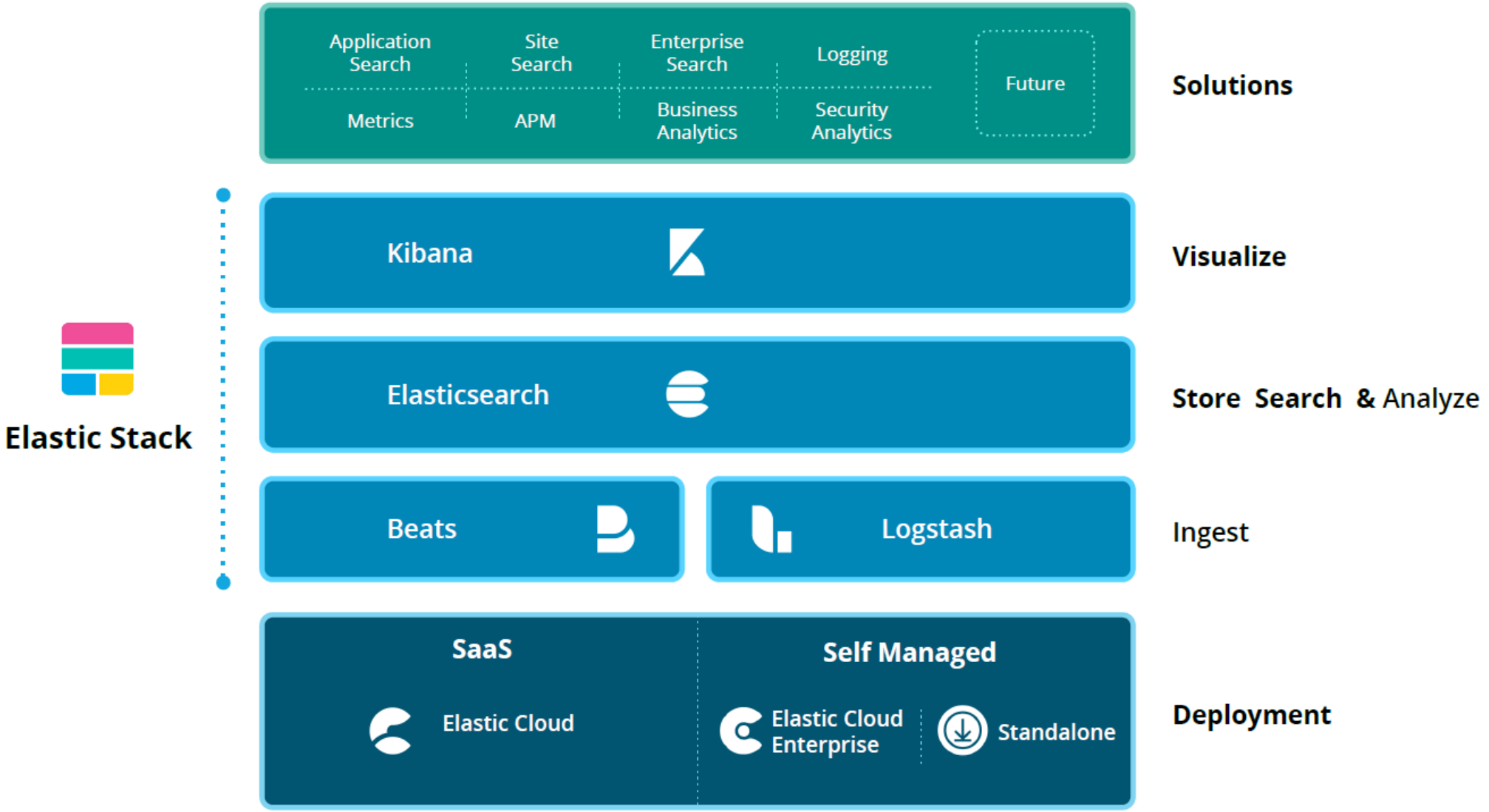
Elastic Stack

Elastic Stack is a group of products that can reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real-time.

Elasticsearch is a distributed, RESTful search and analytics engine that can address a huge number of use cases. Also considered as the heart of the Elastic Stack, it centrally stores user data for high-efficiency search, excellent relevancy, and powerful analytics that is highly scalable.

The core products that define an Elastic stack are:

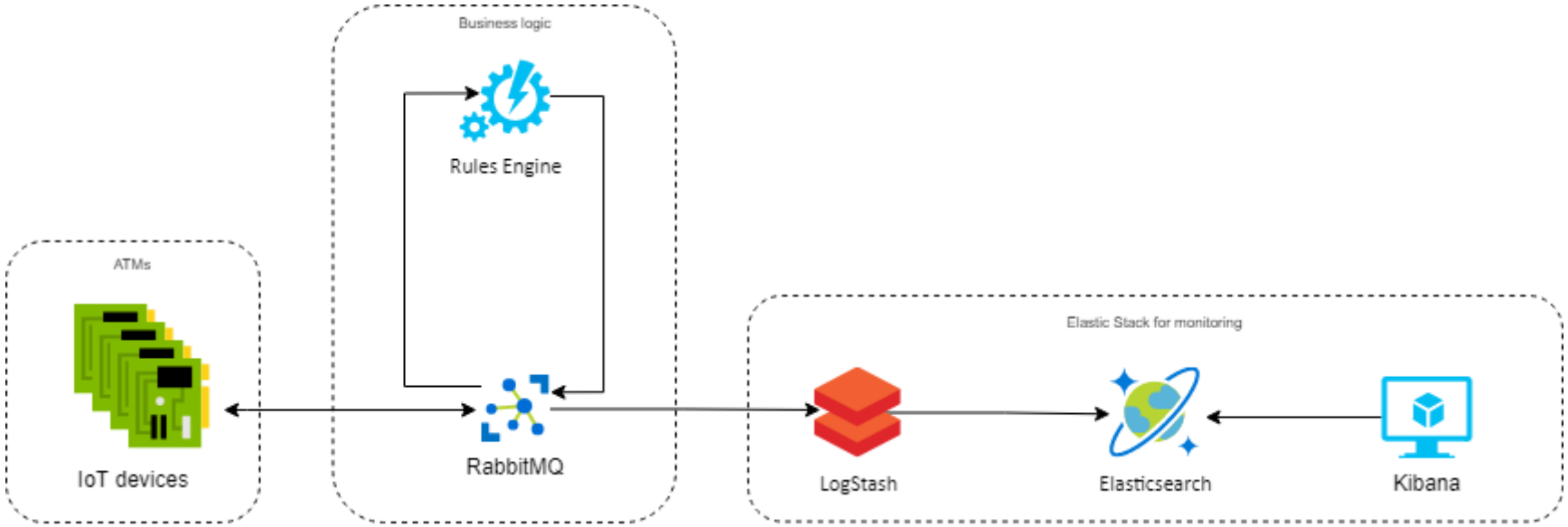
- **Elastic Search** – Search and analytics engine.
- **Logstash** – Data processing pipeline.
- **Kibana** – Dashboard to visualize data.



Why Elastic Stack?

- It is easy to plug
- It is distributed, secure and reliable
- It can be used in different contexts and for different scenarios (monitoring, metrics, business analytics, logging, ...)

Project Architecture



Elastic Search

Elasticsearch is a database that provides distributed, near real-time search and analytics for different types of data. It is based on the Apache Lucene™ library and is developed in Java. It works on structured, unstructured, numerical and geospatial data. The data is stored in the form of schema-less JSON documents.

Some of the major features that Elasticsearch has to offer are:

- Lightening fast full-text search.
- Security analytics and infrastructure monitoring.
- Can be scaled to thousands of servers and can handle petabytes of data.
- Can be integrated with Kibana to provide real-time visualization.
- Use of machine learning to automatically model the behavior of your data

Elastic Search – Main Concepts

Index: It is like a table in a relational database which stores documents having a particular schema in JSON format. In ES versions before 6.0.0, a single index could have multiple types where documents having different schemas could be stored in the same index.

Documents: They are basically the records in an index just like a row in a relational database. Each document has a JSON format, a unique *_id* associated to it and pertains to a specific mapping/schema in the index.

Fields: These are basically the attributes of a document in an index like columns in a table of a relational database.

Elastic Search – Main Concepts

Data types: Elasticsearch supports several data types for the fields in a document (string, numeric, nested, date, bool, geo, ...).

Mapping: It is basically used to specify the schema for an index. It defines the fields within an index, the datatype for each field, and how the field should be handled by Elasticsearch. Mapping is also used to configure metadata associated with the type.

Search API: Allows you to execute a search query and get back search hits that match the query.

Logstash

Logstash is a free and open server-side data processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to your favorite "stash“, usually elasticsearch.

The pipelines use filters to ingest data. Grok filter is a great way to parse unstructured log data into something structured and queryable.

Pipeline example: https://github.com/lorenzokyne/Auriga-IoT-Project/blob/main/Logstash/config/sensors-pipeline.conf

Kibana

Kibana is a data visualization dashboard software for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data.

Kibana also provides a presentation tool, referred to as Canvas, that allows users to create slide decks that pull live data directly from Elasticsearch.

Kibana demo: http://192.168.10.114:5601/app/home#/

Auriga

Thank You

Gaetani Ziri
gaetano.ziri@aurigaspa.com

AURIGA
the banking e-volution

THE # NEXTGENBANK

www.aurigaspa.com