**Elastic Stack Overview:**

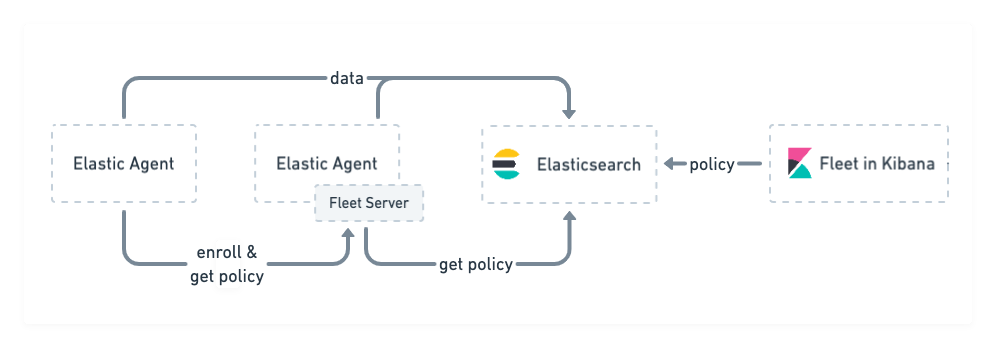
**What is elasticsearch?**

Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured.

Elasticsearch is built on Apache Lucene Known for its simple REST APIs, distributed nature, speed, and scalability.

Elasticsearch is the central component of the Elastic Stack, a set of free and open tools for data ingestion, enrichment, storage, analysis, and visualization.

Elastic stack



Elastic search is the main component of the elastic stack, which stores and ingest data.

Kibana is an UI tool which visualizes the data and tasks to be performed on elasticsearch.

*Elastic Agent & Policy :*

Elastic agent is the package of beats and a unified agent to collect data from host or remote machines. Elastic agents run according to the configurations, which is also called the Agent Policy.

The Agent policy can be modified from kibana as UI.

Integration is a small part of Agent Policy specific to a particular task.

Eg. Docker integration when added to the Agent policy will collect docker metrics.

*Fleet Server:*

The Fleet server is that elastic agent which has fleet server policy attached to it.

The fleet server enrolls to the elastic search and puts the collected data to the elasticsearch.

The elastic agents other than the fleet server collects the data from the different machines and gives it to the fleet server, then the fleet server put the data into elasticsearch.

**Workflow Example of a demo Usecase:**

