ELK Stack Notes

* ELK is an acronym for 3 open-source projects
  + Elasticsearch
    - Search and analytics engine
    - Can search different data types (text/number/geospatial data/etc.)
    - Stores data as schema-free JSON documents
    - Easy to use and scalable
    - Essentially just a database
    - Useful for increasing the manageability of large databases
      * Used for application search/website search/logging and log analytics/geospatial data analysis and visualization/business analytics/etc.
  + Logstash
    - Server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a “stash” like Elasticsearch
    - Can ingest unstructured data from sources such as websites, application servers, and data stores
    - Filters and parses the collected data -> transforms to common format
    - “Collection and transformation agent”
  + Kibana
    - Helps users visualize data with charts and graphs in Elasticsearch
    - Customizable graphics
* Log management solution – ELK forms and end-to-end stack with real time data analytics tools to provide insight on all kinds of data
* Logstash -> Elasticsearch -> Kibana
  + Logstash takes data from different sources and sends the logs into Elasticsearch
  + Elasticsearch allows the user to perform real time search and analysis of the data
  + Kibana provides visual tools to help understand the data better

# Beats

* Beats was another open-source project added in 2015
  + acronym didn’t change now just referred to as the Elastic Stack
* Beats are lightweight, single-purpose data shippers
* There are several distinct beats that are focused on specific types of data
  + Log files/metrics/network packets/Windows events/audit data/cloud data/etc.
* Each Beat has the task of gathering data and shipping it to Elasticsearch
  + Shipped data fits the Elastic Common Schema (ECS)

Chart

Description automatically generated

# Helpful Links

* <https://www.instaclustr.com/elk-stack/> (short summary)
* <https://logz.io/learn/complete-guide-elk-stack/> (longer explanation)