

Elastic Stack

- [The Elastic Stack](#)
- [Implementing Elastic Search](#)
- [Implementing Fluentd](#)
- [Implementing Kibana](#)
- [Implementing SeriLog](#)

The Elastic Stack

Elastic Search

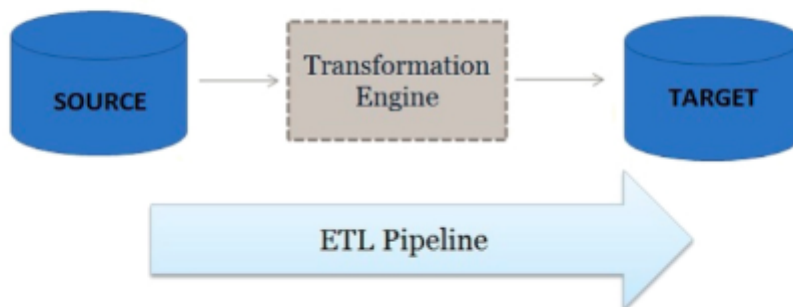
[Elasticsearch](#) is a real-time, distributed storage, RESTful search, and analytics engine. It can be used for many purposes, but one context where it excels is indexing streams of semi-structured data, such as logs or decoded network packets.

Kibana

[Kibana](#) is an open source analytics and visualisation platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualise your data in a variety of charts, tables, and maps.

FluentD

An ETL Pipeline refers to a set of processes extracting data from an input source, transforming the data, and loading into an output destination such as a database, data mart, or a data warehouse for reporting, analysis, and data synchronization.



The letters stand for Extract, Transform, and Load.

Implementing Elastic Search

Packages Required

Configuration

Implementing Fluentd

Packages Required

Configuration

Implementing Kibana

Packages Required

Configuration

Implementing SeriLog

<https://serilog.net/>

<https://github.com/serilog/serilog/wiki/Configuration-Basics>

<https://github.com/serilog/serilog-sinks-elasticsearch>

Packages Required

Configuration