**Centralised Logging Service**

**Using Elastic Stack**

# Concept :

There is a vast amount of information hiding inside the log files on our servers, but visualising and exploring such a large amount of textual data can be difficult. There are a few problems you must first overcome.These log files are often distributed over many machines or cluster of Machine, so we must first aggregate them into a single location. Next, we'll need to find the information we are looking for (which can involve doing a fair bit of command-line magic), and even then it may be difficult to visualise without the aid of some graphical tools.

**Logstash** directly addresses these common pain points by: aggregating log files, parsing them, inserting them into a searchable database (**Elastic Search**), and providing a number of ways to visualise the data (**Kibana**).

# Technology :

Elastic Stack comprised of Various modules , we will be using Elastic Search , Logstash & Kibana widely know as ELK stack

1. **Logstash :**

**Logstash** is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favourite “stash.” (Ours is Elastic Search, naturally.)

1. **Elastic Search :**

**Elastics Search** is a [search engine](https://en.wikipedia.org/wiki/Search_engine_(computing)) based on [Lucene](https://en.wikipedia.org/wiki/Lucene). It provides a distributed, [multitenant](https://en.wikipedia.org/wiki/Multitenancy)-capable [full-text search](https://en.wikipedia.org/wiki/Full-text_search) engine with an [HTTP](https://en.wikipedia.org/wiki/HTTP) web interface and schema-free [JSON](https://en.wikipedia.org/wiki/JSON) documents. Elastic Search is developed in [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) and is released as [open source](https://en.wikipedia.org/wiki/Open_source_software) under the terms of the [Apache License](https://en.wikipedia.org/wiki/Apache_License).

1. **Kibana :**

**Kibana** is an open source data visualisation plugin for Elastic Search. It provides visualisation capabilities on top of the content indexed on an Elastic search cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data.



Architectural Diagram

# Partical Application :

**Nomura** has many application which are running in cluster on different Machine where each application generate their respective logs at the time of debugging any anomaly in the application it becomes very difficult for the respective team to track each logs files. This System will give them the Visualisation dash board which PS or the concern team can you to detect and monitor the Issue . Apart from Application log it can also help in tracking various System logs and Database logs which again can be a added advantage at time of System failure .

# Plan of the Day :

Generate a Application Log files from multiple system and push them into LogStash for Parsing the logs and storing them Elastic Search and perform few query to demonstrate the retrieval of the data and few graphical data generated using logs file.

# Requirement :

Unix/Linux Server to deploy the Elastic Stack and a System to perform the demo