LOGGING AS A SERVICE

GROUP 10

Aditya Harit   Akshay Bhandiwad   Shweta Iyer

INTRODUCTION

Motivation

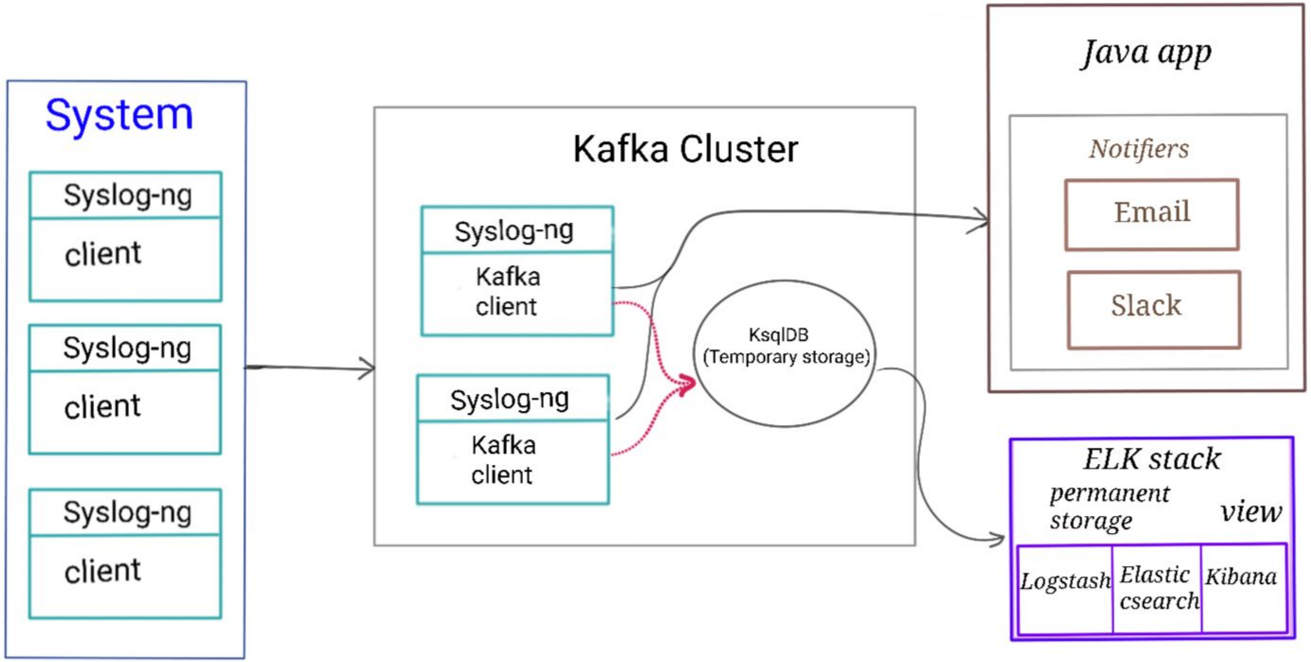
- There has been a massive increase in the amount of data produced in recent times
- Logs make up a significant fraction of this data
- The microservice architecture is adopted by a majority of organizations today
- In this scenario, each application generates several logs
- This necessitates the need for log parsing, transformation and storage systems
- Log notifications systems and real time log monitoring is very essential for the system admins

Basic Idea

- Providing logging as a service to multiple clients
- Generate email or slack notifications to the client’s system admins when errors occur
- Provide a real time log visualization platform for the client’s system admins to monitor their systems
- Distribute this client log processing across multiple servers for parallelism

DESIGN

Architecture



Implementation details

- The Kafka destination feature of Syslog-ng is used to send data from Syslog-ng to Kafka on the servers.
- A round-robin load balancing of client’s logs is done among the servers for the processing of the logs.
- One Kafka topic is created per client organization
- KSQL is used to generate tags for the logs
- Email and slack notifier applications subscribe to changes to the required Kafka topic

Technologies used

- ❏ Google Cloud Platform
- ❏ Syslog-ng
- ❏ Kafka and KSQL
- ❏ Elasticsearch and Kibana (ELK Stack)
- ❏ Email and Slack

DEMO TIME!

THANK YOU