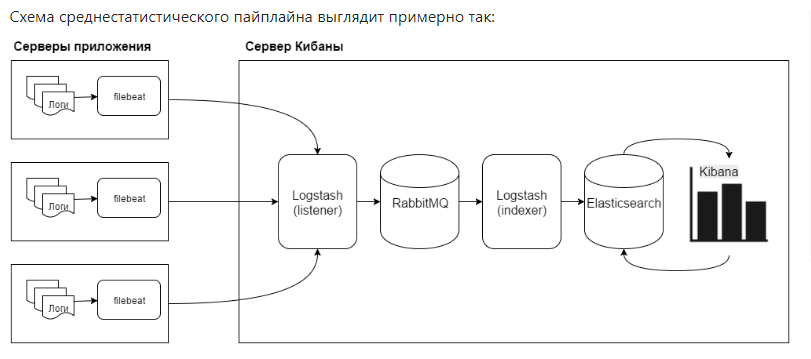
При логировании с нескольких машин и размере лог файлов достигающих 50 гб имеет смысл использовать централизованную систем логирования и СУБД для хранения логов и писка по ним.



Заменим Logstash на Fluentd, уберем RbbitMQ:

Почему Fluentd?

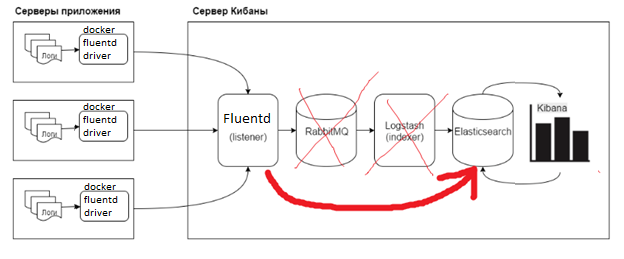
-Обрабатывает 13 000 строк в секунду при потреблении памяти 40 мб. Можно обойтись без реббита.

-Умеет обрабатывать логи асинхронно

-Есть стандартный докер-драйвер для сбора логов.

-Поддерживает буферизацию.

-Есть возможность через плагин вычитвать логи из файлов нпрямую (более 300 различных плагинов)



при потреблении оперативной памяти около 40 мегабайт обрабатывается 13 000 строк в секунду

Инструкция по настройке Elasticsearch + Fluentd + Kibana в докере

<https://docs.fluentd.org/v/0.12/articles/docker-logging-efk-compose>

Инструкция по настройке драйвера логгирования в docker

<https://docs.docker.com/config/containers/logging/fluentd/>

Что для чего?

Fluentd – для сбора, фильтрации, форматирования и передачи в СУБД логов в формате json

Elasticsearch – NoSql СУБД

Kibana – Удобный просмотр, фильтры, поиск, графики, и куча всего.

В Kibana создал 4 фильтра по кол-ву контейнеров. Есть свой язык запросов, но базовые возможности по просмотру и поиску вроде просто делаются.

Можно тыкнуть по фильтру- и нажать включить его или отключить.

