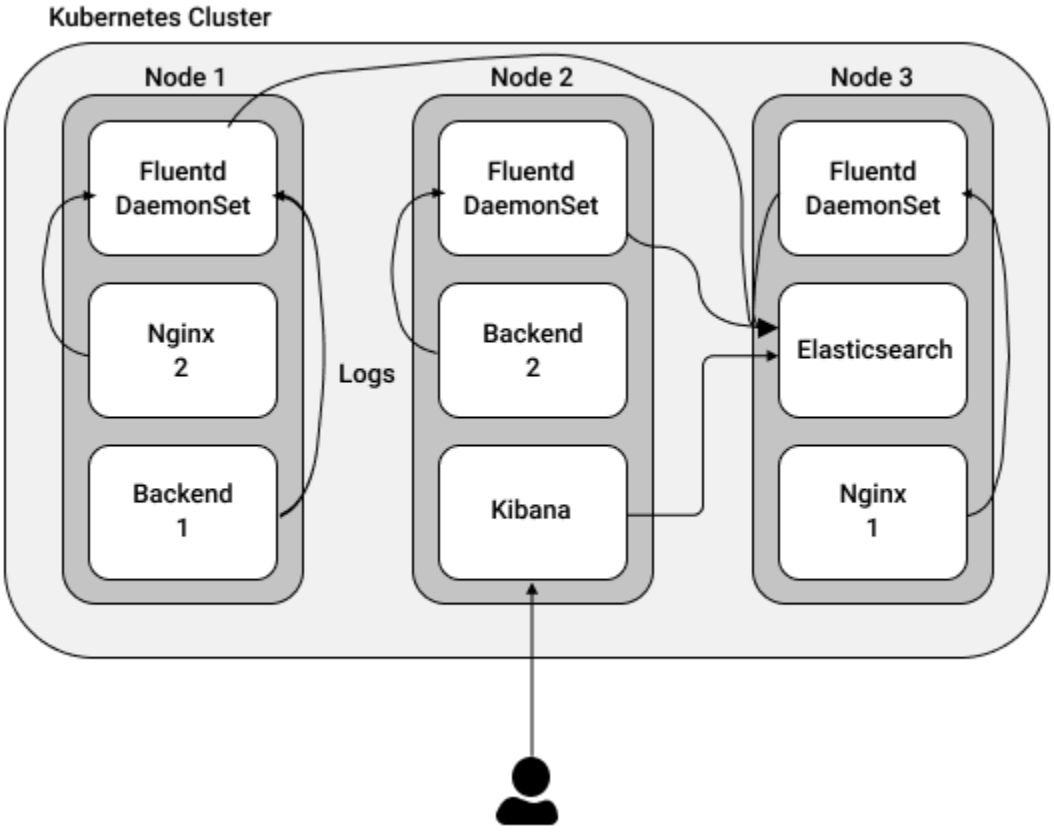
KUB 34: Сбор логов в кластере Kubernetes

Описание:

Для понимания ситуации нужны не только метрики, но и логи. Обычно в Kubernetes используют стек ElasticSearch + Fluentd + Kibana. Fluentd в этой связке используется вместо ожидаемого Logstash за счет модульности, гибкости в плане конфигурации и интеграции с системами оркестрации (и в Docker есть плагин, и для Kubernetes есть плагин для сбора метаданных). Это ничем не отличается от сбора логов с обычных машин, кроме как централизацией — в случае, когда у вас развесистая микросервисная архитектура, подключение к логам через kubectl logs становится нереальным. Важный момент — получение дополнительных меток с контейнеров, подов, неймспейсов. Все это покрывает Fluentd с плагинами для работы с ElasticSearch и Kubernetes metadata.



Как правило, ElasticSearch запускают либо на выделенной ноде, либо вообще вне кластера, так как из-за количества съедаемых ресурсов (CPU/RAM/Disk IO) практически ничего не выживает рядом с ним при серьезных нагрузках.
Давайте попробуем установить стек для сбора логов с нашего кластера.

Задание:

1. Установите kibana, elasticsearch, fluent-bit в namespace logging.

- fluent-bit должен собирать логи со всех подов кластера
- fluent-bit должен отправлять логи в elasticsearch
- kibana должна подключаться и читать данные из elasticsearch

2. Настройте basic authentication для kibana ingress (вы можете использовать выданное вам доменное имя для настройки ingress)
3. Отправьте задание на проверку.