



# Telemetry on K8S

---

임성국 issac.lim 송지현 jenny.ssong  
Cloud.Telemetry @ 카카오

01 - 04 Prologue

---

05 - 09 KOCOON-HERMES

# 01 Who We Are?

if(kakao) dev 2019

# Telemetry?

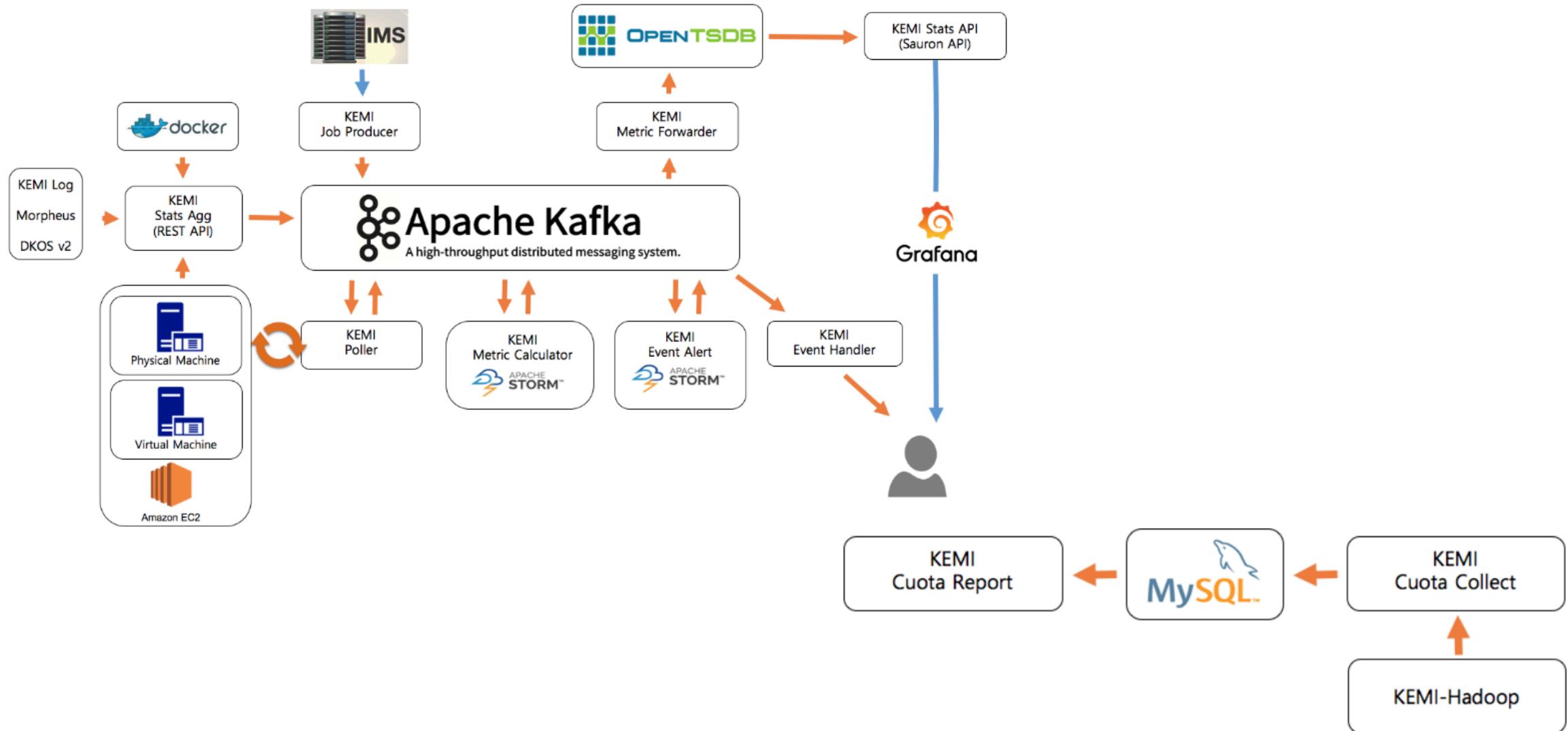
Telemetry is an **automated communications process** by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

# Cloud Telemetry?

- **Remote & Inaccessible points**
  - Baremetal, IaaS, CaaS ...
- **We Develop & Provide automated communications process**
  - MaaS (Monitoring as a Service)
    - KEMI (Kakao Event Metering and monitoring)
    - KOCOON?

## 02 Previous Stage

# KEMI Stats Overview

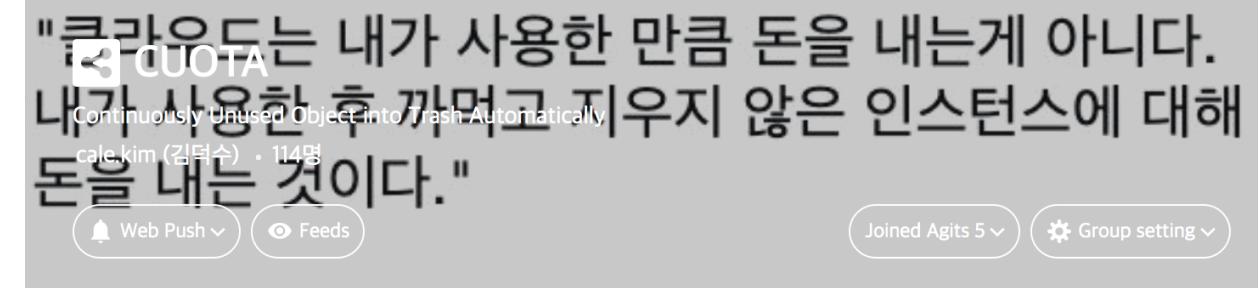


# KEMI Stats Provide ...

9rum 클라우드 포탈

issac.lim

- 9rum 포탈
- 애자로
- 레코드 관리
- 비용
  - 나의 비용
  - 부서 비용
- KRANE
  - 프로젝트 관리
  - 내 소유 VM 관리
- SSO
- 클라이언트 관리
- 클라우드 서비스
- 컴퓨팅
- KRANE
- DKOS-V2



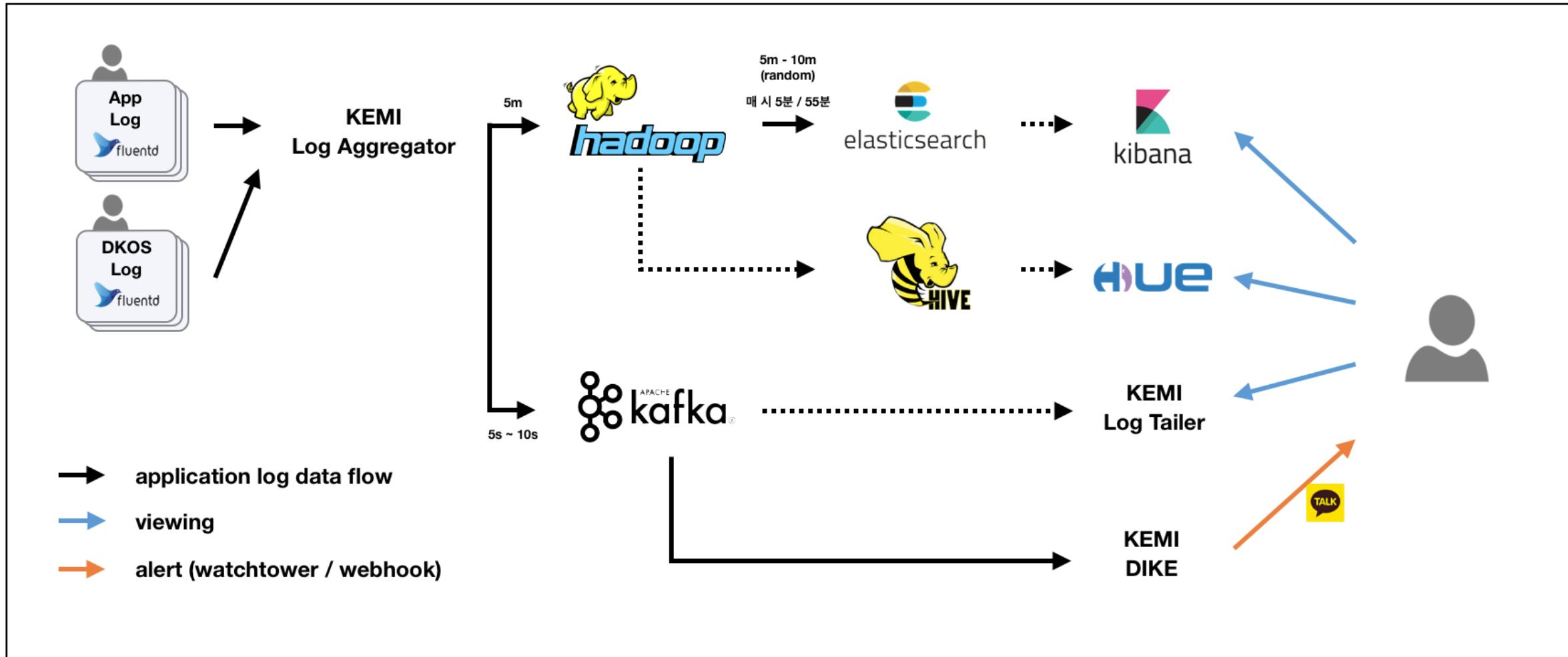
Continuously Unused Object into Trash Automatically

KRANE DEV 인스턴스들은 CUOTA 시스템을 통해 관리 되고 있습니다. 유휴 자원으로 판단 되는 인스턴스를 대상으로 검색/공지/정지/삭제 진행 되며, 인스턴스를 화이트 리스트에 등록한 경우에 관리 대상에서 제외 됩니다.

- 공용으로 관리해야하는 VM 들은 멤버 모두 프로젝트 참여해주시길 부탁드립니다.
- 화이트 리스트 등록 가이드 : <https://kakao.agit.in/g/300008675/wall/320944751>
- 공지/정지/삭제 이력 확인 가이드 : <https://kakao.agit.in/g/300008675/wall/320945034>

Thx Joanne

# KEMI Logs Overview



# KEMI Logs Provide ...

**[IMS\_API] Dashboard**

**[IMS\_API] category call pie**

**[ims\_api] Client\_Top10**

**[IMS\_API] 각 api서버 요청**

**[IMS\_API] category call cnt**

filters	Count
*	13,314,864
serverViews	10,729,316
svc_categories	1,643,593
etc	914,845
servers	32,871
securitys	25,501
security_policy	6,914
bookedips	5,942
networks	608
code AND asset	62

**[IMS\_API] Client call list**

call   host    Q	Count
10.194	3,213,138
10.194	3,153,683
10.194	2,937,252
10.42.2	773,076
10.42.2	762,101
10.60.7	596,013
10.61.2	591,444
10.197	184,526
10.194	158,985
10.197	127,148

**[IMS\_API] code:500**

**HUE**

**Hive**

```

1 select
2   get_json_object(regexp_replace(`data`, '@timestamp', 'timestamp'), '$.timestamp'), data
3 from kemi.k_public_test_src
4 where
5   dt = '20180518' and
6   hr = '09'
7 limit 1;
  
```

**Job** Job Queue Hive Add a name... 설명 추가...

**도우미** 도우미 함수

**Hive** Search...

- Aggregate
- Analytic
- Collection
- Complex Type
- Conditional
- Date
- Mathematical
- Misc
- String
- Data Masking
- Table Generating
- Type Conversion

**쿼리 기록** **저장된 쿼리** **결과 (1)**

**\_c0** **data**

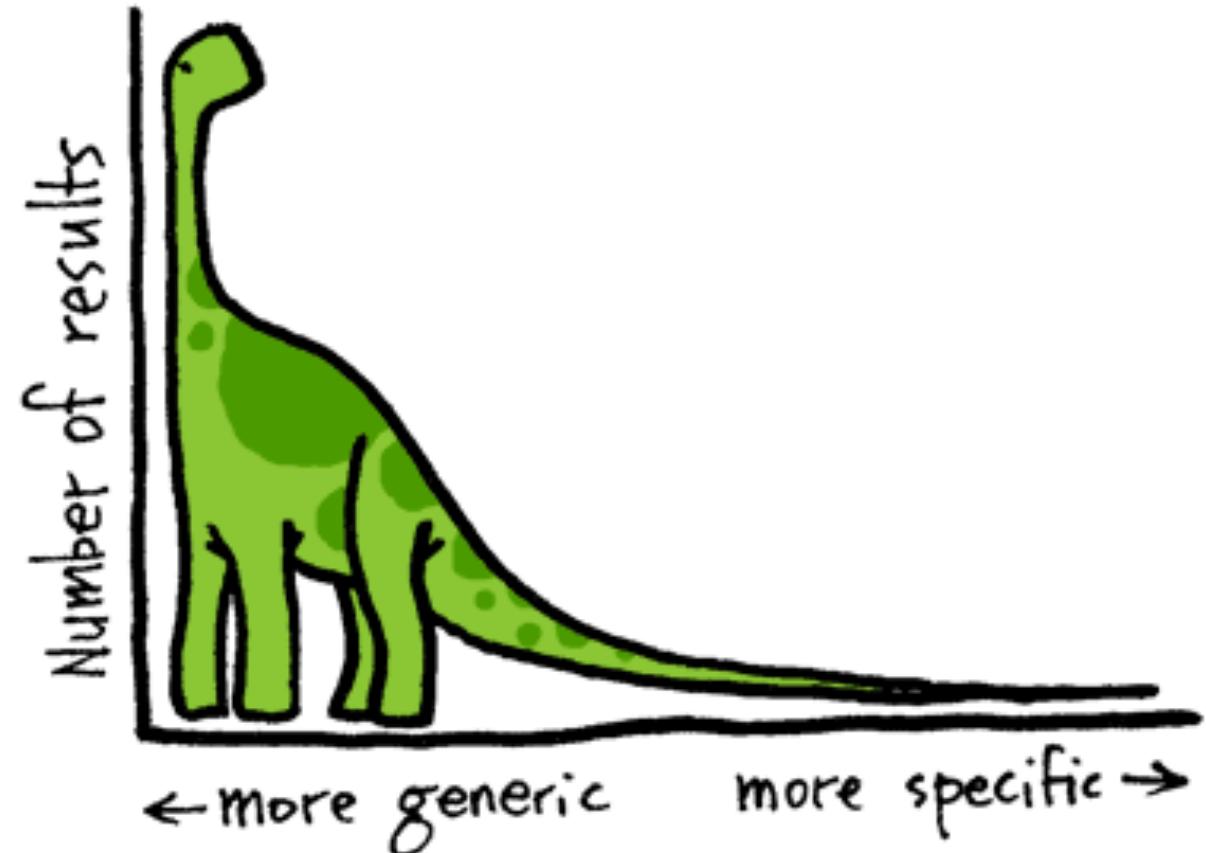
```

1 2018-05-18T09:30:27+09:00 {
  
```

# 03 Is It Enough?

**Head: KEMI-\***

**Longtail: ?**



ref: <https://mgcabral.wordpress.com/2012/03/04/thelongtaileconomics/>

# Longtail

## Users want

- Own Resource
- To deal with resources in their own way  
realtime(< 1m) & heavy query
- To Customize everything

## We think

- Divide resources by services
- Provide self-monitoring & self-healing
- Provide more values (services)

# New CaaS (DKOSv3)

## DKOSv3

- k8s based container orchestrator
- ifkakao 2019 day1 15:00 ~

카카오톡 적용 사례를 통해 살펴보는 카카오 클라우드의 KaaS

The screenshot shows the DKOS web interface with a blue header bar. Below it is a search bar and a user profile section. The main content area is titled "Cluster List". It displays two clusters:

- kemi-staging**: Kubernetes version v1.9.5 | kakao/v2.5.0. Status: Dev\_Zone, VM Only. Description: kemi poc staging cluster. Buttons: 상세 보기, 삭제, KUBECTL 설정, 대쉬보드 토큰, 사용자 관리.
- kc-pro-prod**: Kubernetes version v1.11.5 | kakao/v2.7.0. Status: Prod\_Zone, VM Only. Description: kc-pro-prod. Buttons: 상세 보기, 삭제, KUBECTL 설정, 대쉬보드 토큰, 사용자 관리.

Each cluster card has a "Kube Dashboard" button with a toggle switch labeled "Enabled" and a "새 창 열기" (Open in new window) link. The background of the interface is white.



# Telemetry on Own Resource

====

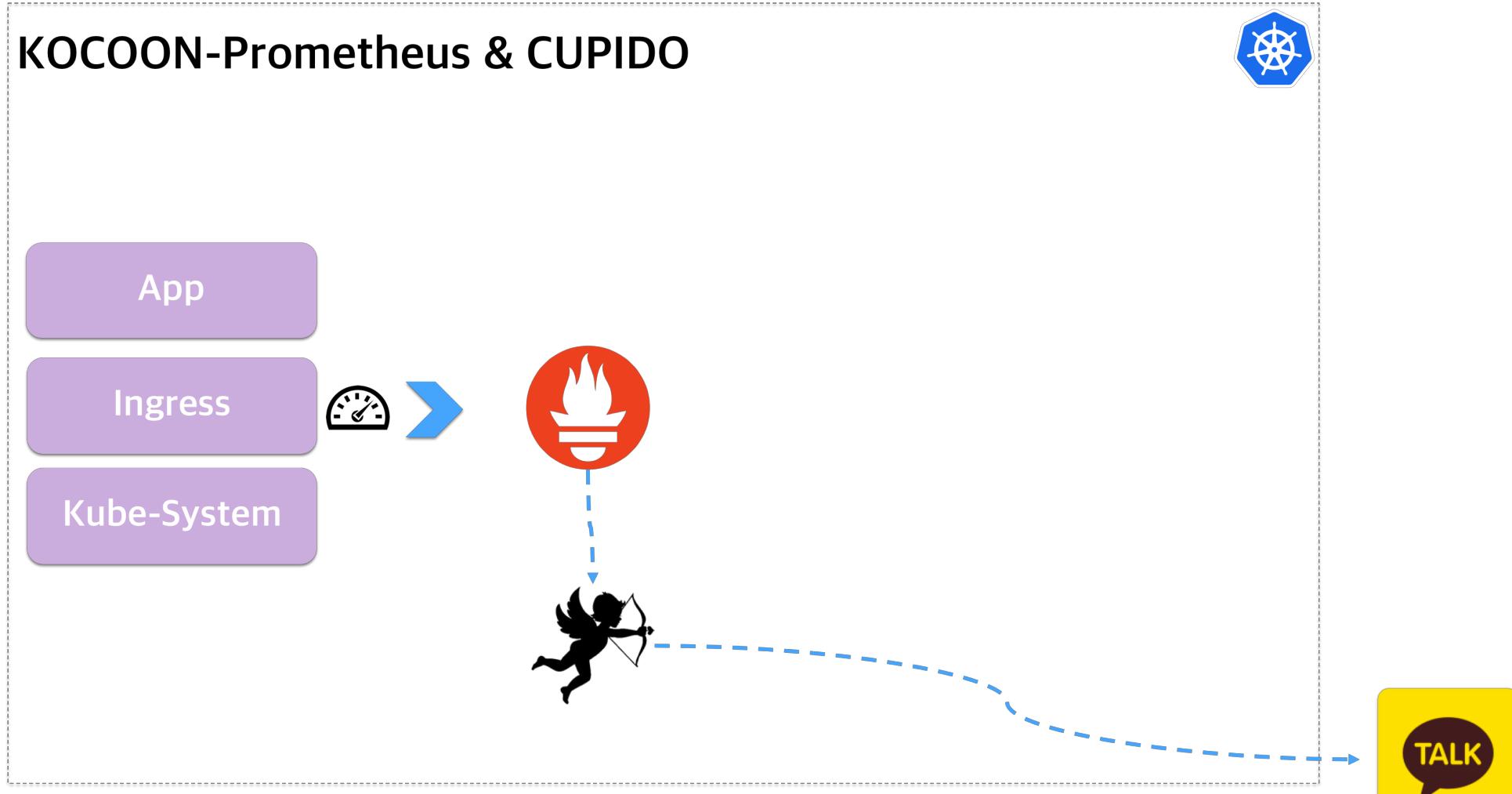
# Telemetry on k8s

## **KakaO COntainer based service mONitoring**

# 04 KOCOON-\*

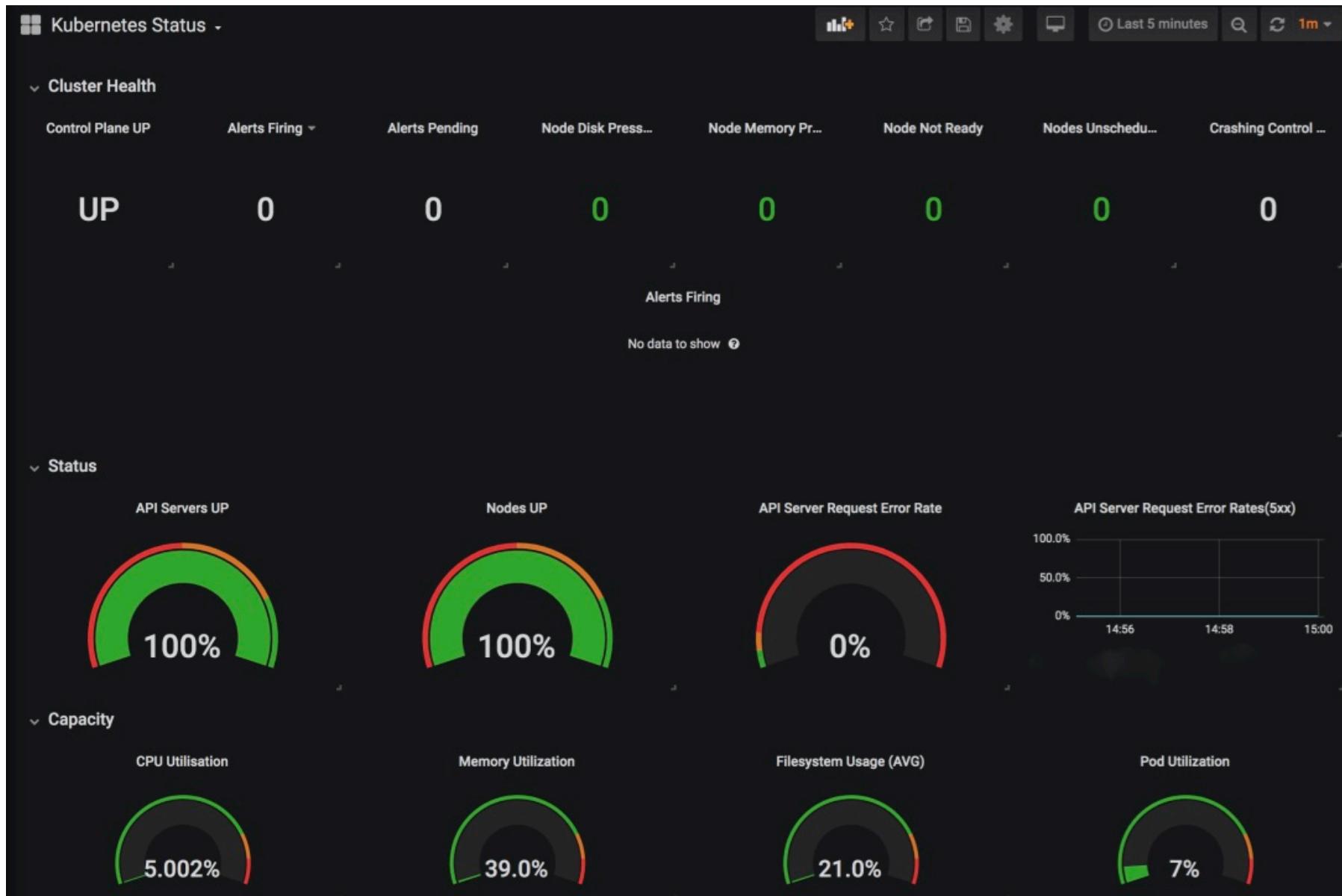
if(kakao) dev 2019

# Metric based Self Monitoring

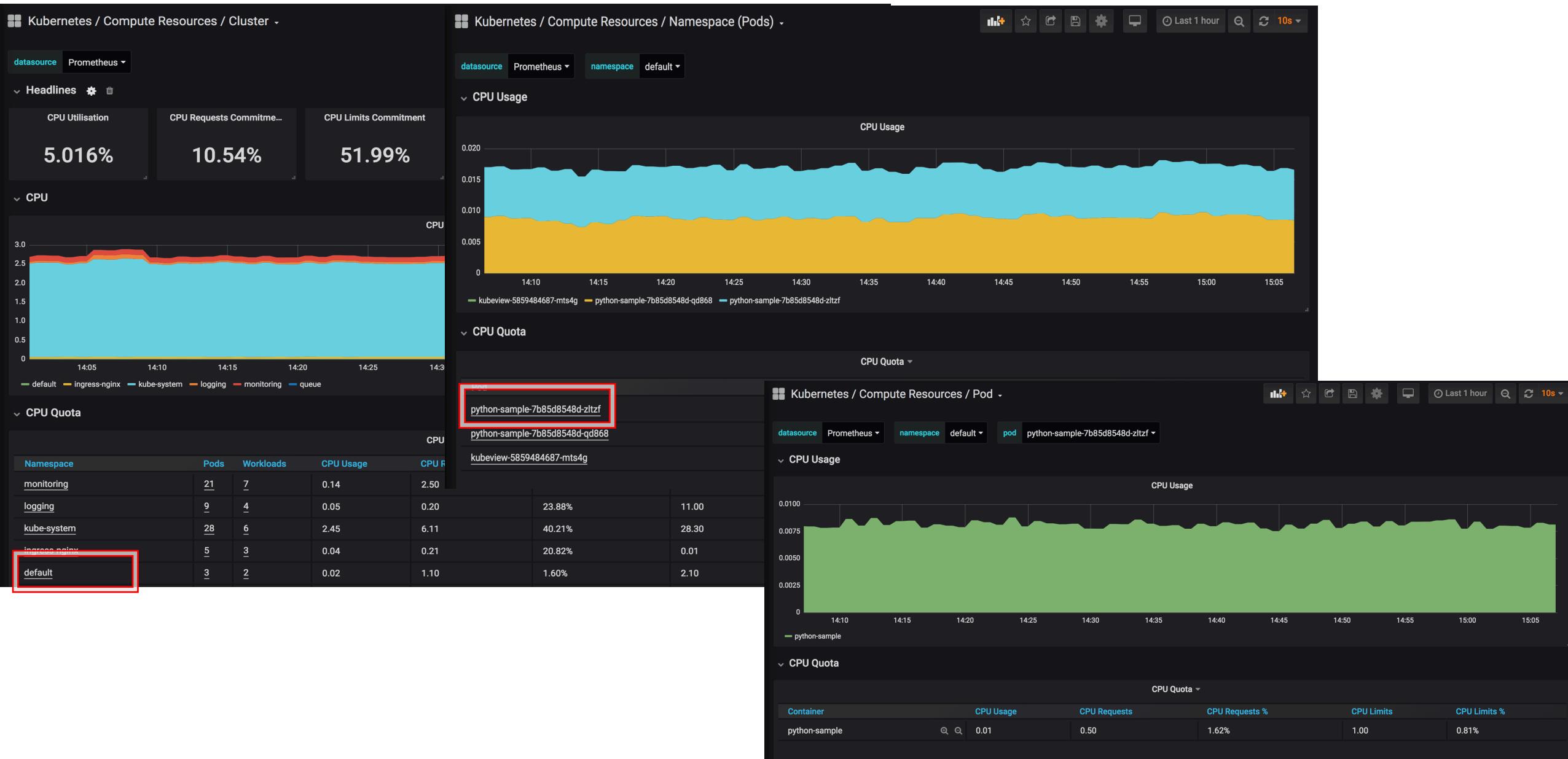


➤ : Pulling    - - ➤ : Push

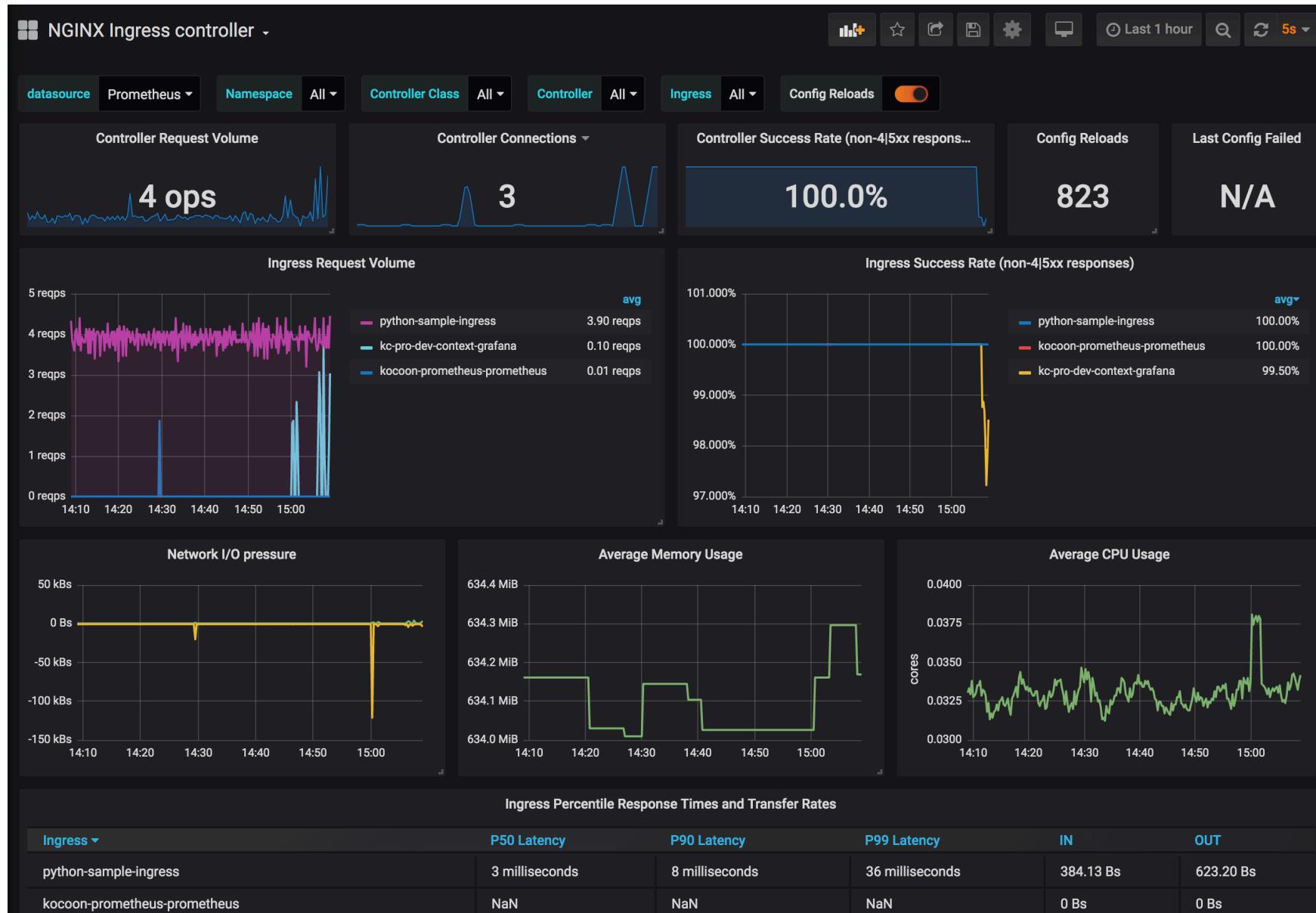
# k8s Status View



# k8s DrillDown View



# k8s Ingress Controller View



# k8s ETCD View



# KOCOON-Cupido Alarm

Watchtower

[ kocoon cupido ]

AlertName:  
KubeDaemonSetRolloutStuck

Status: 🔥 firing 🔥

StartsAt: 2019-05-28  
05:58:31.571433492 +0000 UTC

Message: Only 78.8% of the desired Pods of DaemonSet kube-system/cilium are scheduled and ready.

[http://64-prometheus.dev.9rum.cc/graph?  
g0.expr=kube\\_daemonset\\_status number ready%7Bjob%3D%22kube-state-metrics%22%7D+  
%2F+kube\\_daemonset\\_status desired number scheduled%7Bjob%3D%22kube-state-metrics%22%7D+  
%2A+100+%3C+100&g0.tab=1](http://64-prometheus.dev.9rum.cc/graph?g0.expr=kube_daemonset_status_number_ready%7Bjob%3D%22kube-state-metrics%22%7D+%2F+kube_daemonset_status_desired_number_scheduled%7Bjob%3D%22kube-state-metrics%22%7D+%2A+100+%3C+100&g0.tab=1)

2:59 PM

Watchtower

[ kocoon cupido ]

AlertName:  
KubeDaemonSetRolloutStuck

Status: 🌈 resolved 🌈

StartsAt: 2019-05-28  
05:58:31.571433492 +0000 UTC

EndsAt: 2019-05-28  
05:59:31.571433492 +0000 UTC

Message: Only 78.8% of the desired Pods of DaemonSet kube-system/cilium are scheduled and ready.

# Default SLA for KOCOON-Prometheus

- **Resource Request & Limit**
  - CPU 1~4 Core, Memory 4~6 GB

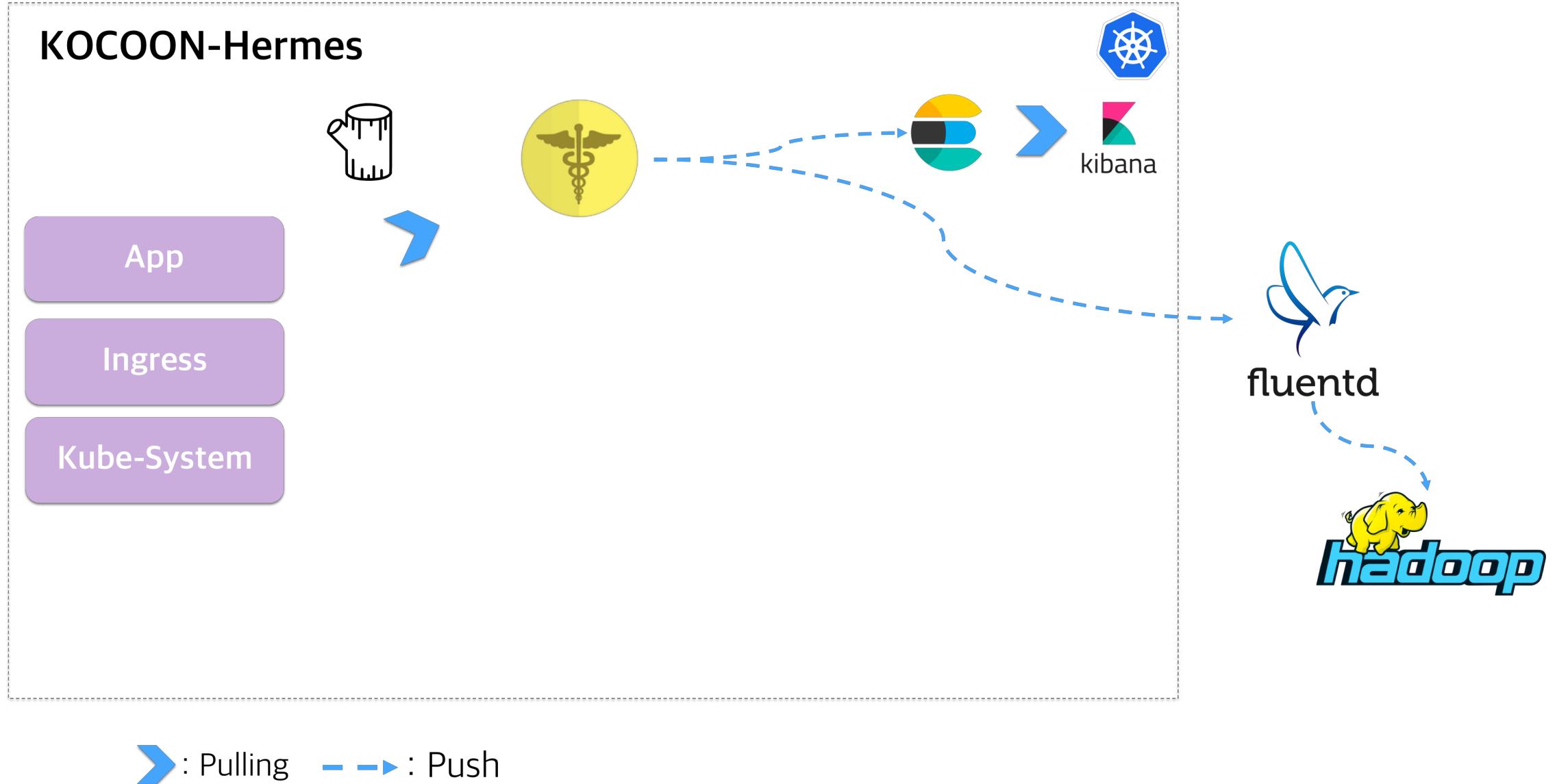
# Default SLA for KOCOON-Prometheus

- Metric 보관 기간 : 3 days
- Metric 수집 주기 : Every 60s
- Alarm 주기: 5~15M동안 이벤트가 반복되면 1시간에 한 번 알림
- ~ 200 nodes, ~ 1500 pods, ~ 10,000 metrics/sec

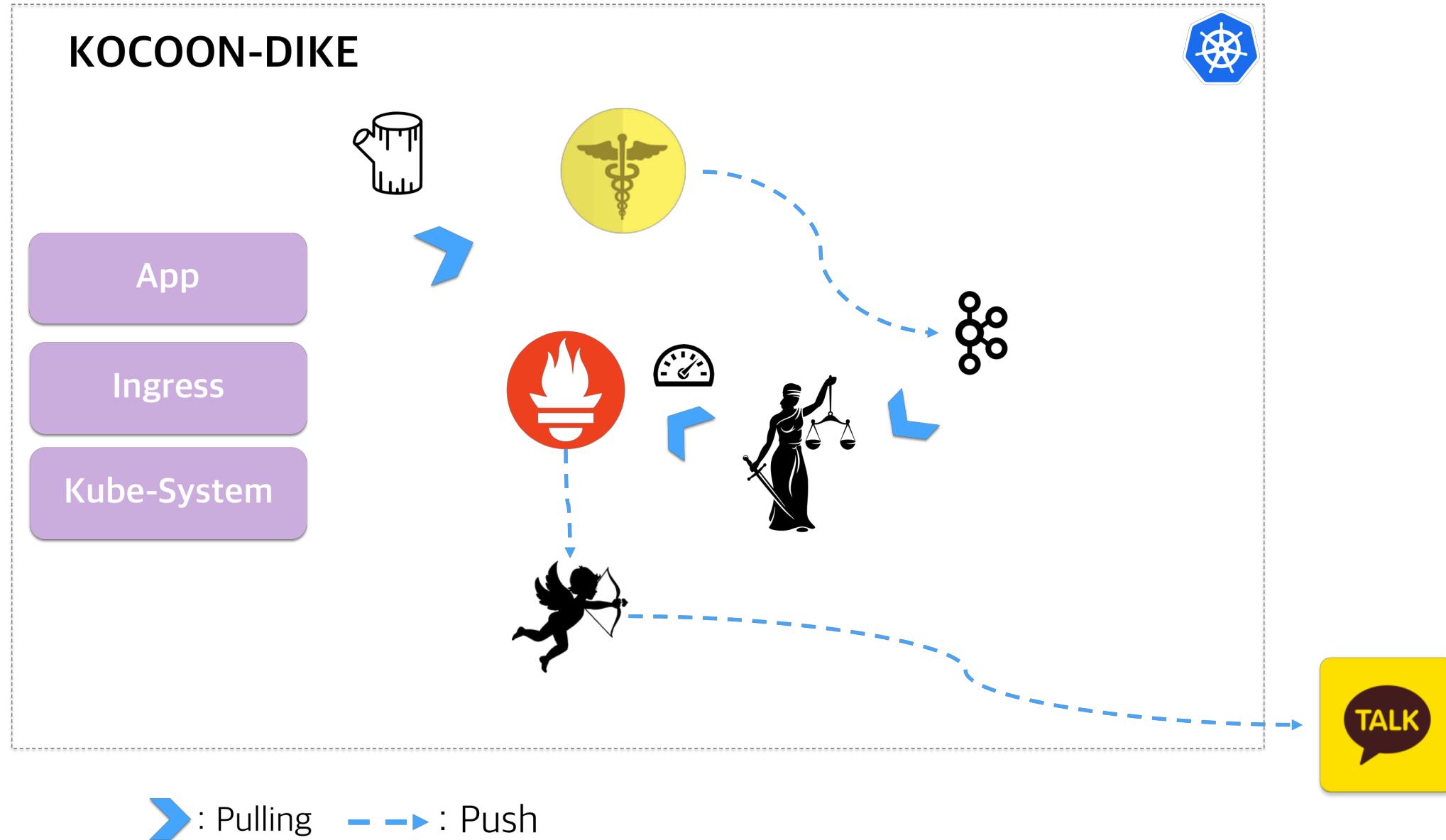
# More About for KOCOON-Prometheus

[2019-kocoon-kakao-automatic-k8s-monitoring](#)  
by templer7 @sildeshare

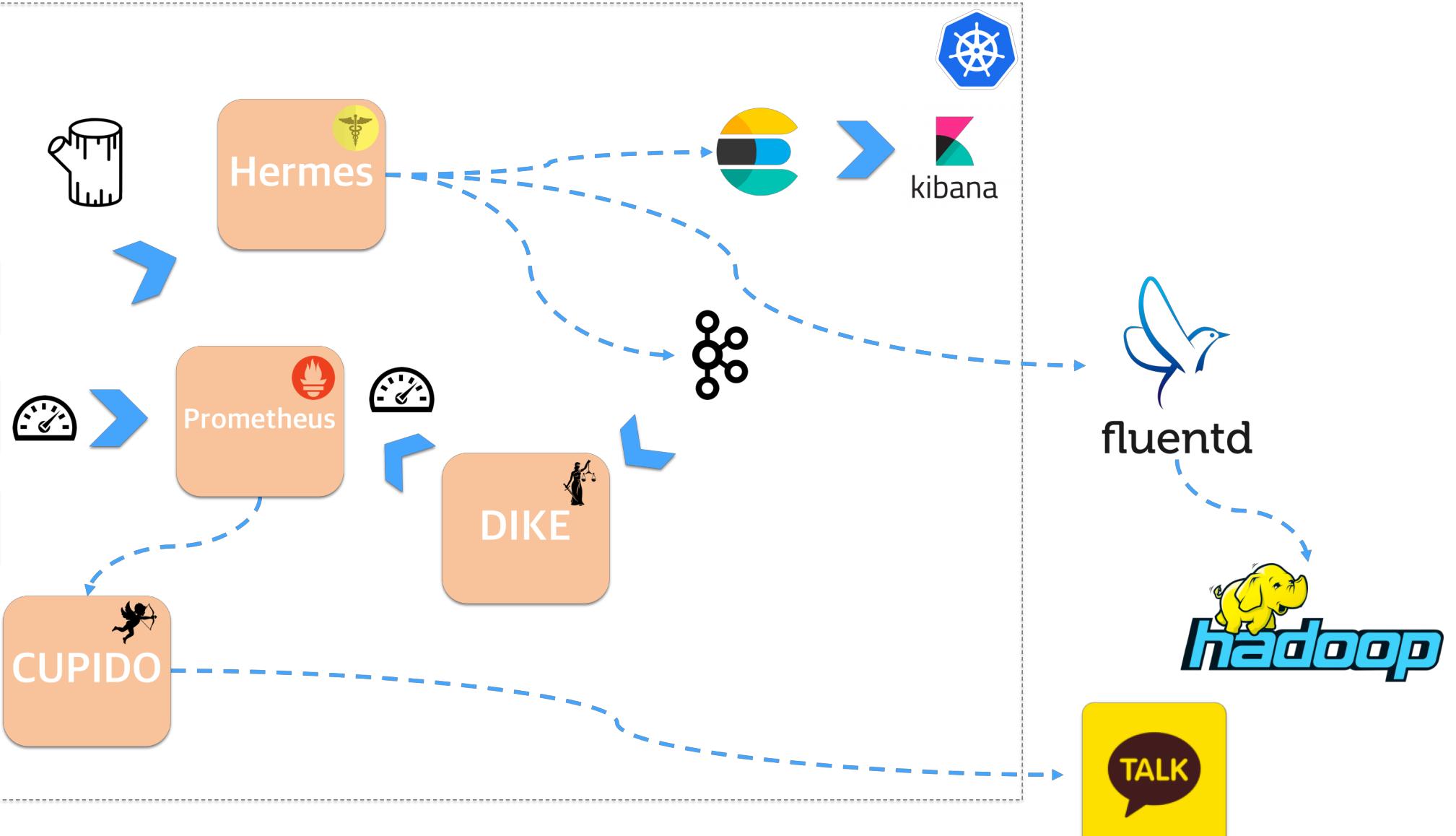
# Log Routing



# Rule based Log Event



# KOCOON-\*



➤ : Pulling    ➡ : Push

# 05 KOCOON-HERMES



# Why Hermes?



## Users want

- **Own Resource**
- **To deal with resources in their own way**  
**realtime(< 1m) & heavy query**
- **To Customize everything**

## Hermes provide

- **Kubernetes Log Customizing**
- **Sink to own cluster**
  - **kafka cluster, elasticsearch cluster ...**
- **Self-monitoring (TOBE)**

## We think

- **Divide resources by services**
- **Provide self-monitoring & self-healing**
- **Provide more values (services)**

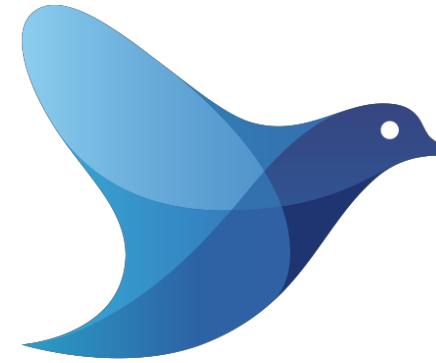
# Dive Into Hermes - Fluentd

## Why fluentd?

- Many plugins
- Stable
- CNCF
- fast PR & merge

### Compose of

- Input
- Filter
- Output



fluentd

# Why do not using fluent-bit?

Because, fluent-bit does not support tag-rewrite



**jihyun.song** Aug 8th at 6:04 PM

Hi, Is there any plugin for rewrite tag name in fluent-bit? like  
"match record\_modifier or rewrite\_tag\_filter" in fluentd (edited)

---

2 replies



**eduardo** 3 days ago

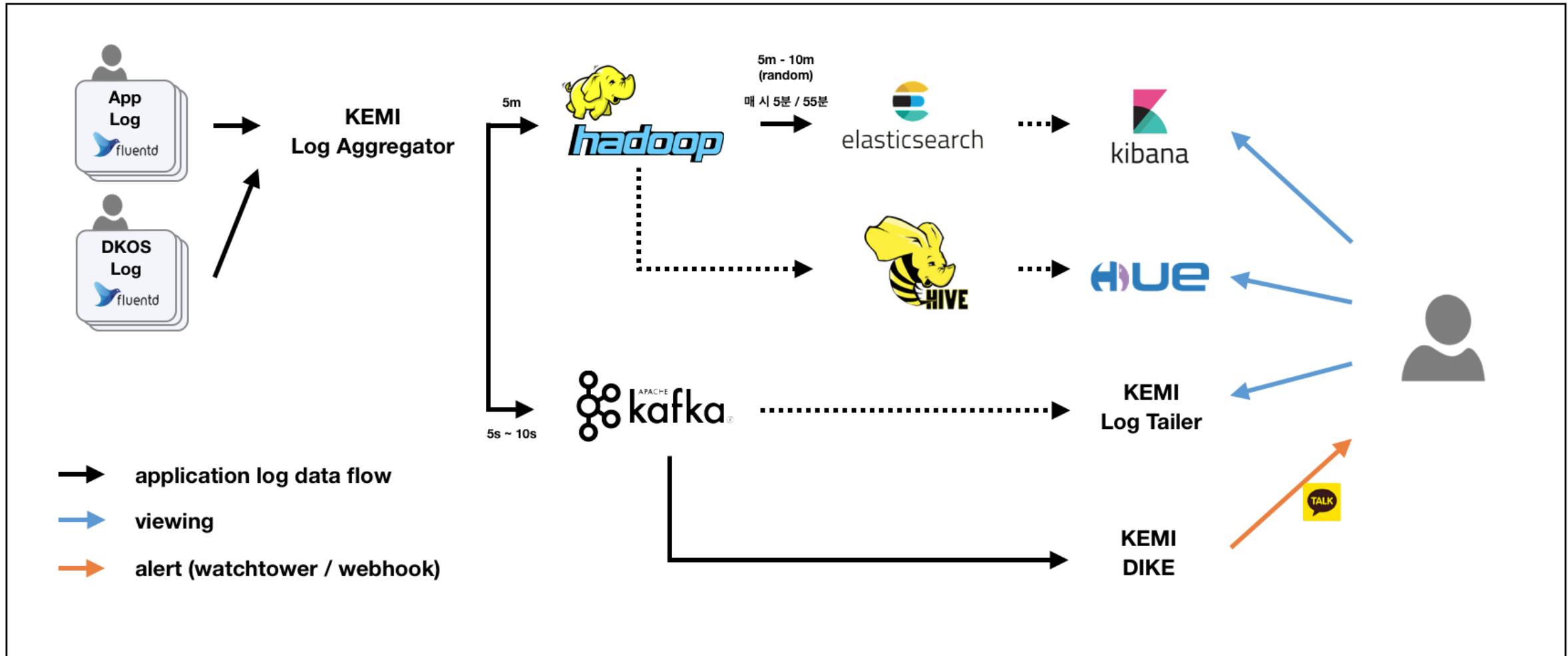
that plugin is currently in "work in process"



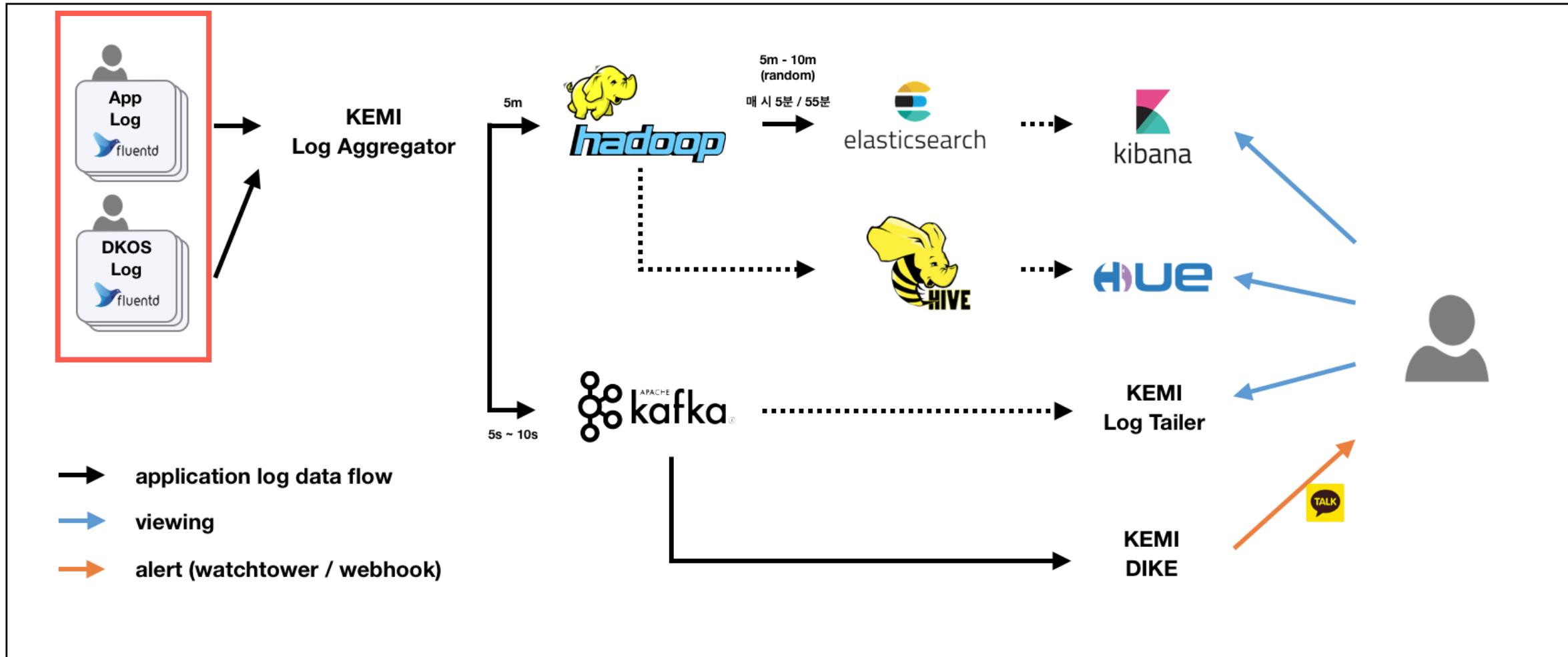
**jihyun.song** 3 days ago

@eduardo That sounds good! Thank you for the answer!

# Dive Into Hermes - KEMI Logs Overview



# Dive Into Hermes - KEMI Logs Overview



# Dive Into Hermes – Hermes goal

- **Running on k8s**
  - **as docker file**
- **Using helm**
  - **easy to setup**
  - **ifkakao 2019 day1 11:00 ~ 카카오에서 컨테이너를 사용하는 방법**
- **User can customize the logging configuration**
  - **log customizing**
  - **routing log to own kafka & elasticsearch cluster**

# 06 Goals for work



# Goals for work – running on k8s

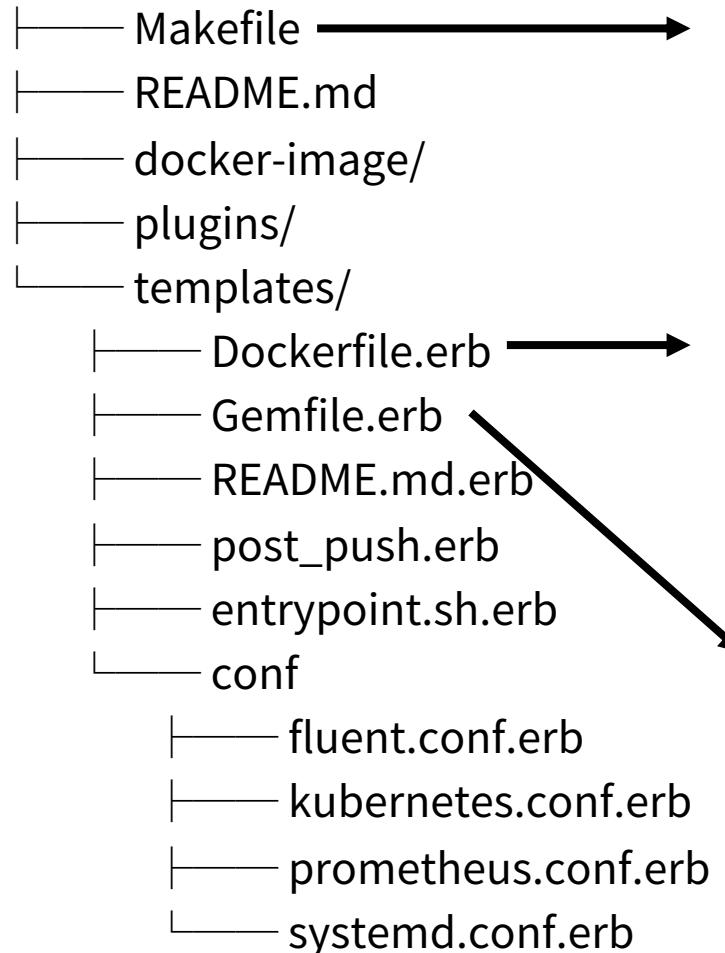
- use **DaemonSet** resource type
  - k8s ensures that all Nodes run a copy of a Pod
- [fluentd-kubernetes-daemonset](#)
  - slim ruby 2.6 image
  - install fluentd gem and others
  - does not support multiple destination (ex. kafka & elasticsearch)

## Debian

- v1.4.2-debian-elasticsearch-1.1,v1.4-debian-elasticsearch-1 [docker-image/v1.4/debian-elasticsearch/Dockerfile](#)
- v1.4.2-debian-loggly-1.1,v1.4-debian-loggly-1 [docker-image/v1.4/debian-loggly/Dockerfile](#)
- v1.4.2-debian-logentries-1.1,v1.4-debian-logentries-1 [docker-image/v1.4/debian-logentries/Dockerfile](#)
- v1.4.2-debian-cloudwatch-1.1,v1.4-debian-cloudwatch-1 [docker-image/v1.4/debian-cloudwatch/Dockerfile](#)
- v1.4.2-debian-stackdriver-1.1,v1.4-debian-stackdriver-1 [docker-image/v1.4/debian-stackdriver/Dockerfile](#)
- v1.4.2-debian-s3-1.1,v1.4-debian-s3-1 [docker-image/v1.4/debian-s3/Dockerfile](#)
- v1.4.2-debian-syslog-1.1,v1.4-debian-syslog-1 [docker-image/v1.4/debian-syslog/Dockerfile](#)
- v1.4.2-debian-forward-1.1,v1.4-debian-forward-1 [docker-image/v1.4/debian-forward/Dockerfile](#)
- v1.4.2-debian-gcs-1.1,v1.4-debian-gcs-1 [docker-image/v1.4/debian-gcs/Dockerfile](#)
- v1.4.2-debian-graylog-1.1,v1.4-debian-graylog-1 [docker-image/v1.4/debian-graylog/Dockerfile](#)
- v1.4.2-debian-papertrail-1.1,v1.4-debian-papertrail-1 [docker-image/v1.4/debian-papertrail/Dockerfile](#)
- v1.4.2-debian-logzio-1.1,v1.4-debian-logzio-1 [docker-image/v1.4/debian-logzio/Dockerfile](#)
- v1.4.2-debian-kafka-1.1,v1.4-debian-kafka-1 [docker-image/v1.4/debian-kafka/Dockerfile](#)
- v1.4.2-debian-kinesis-1.1,v1.4-debian-kinesis-1 [docker-image/v1.4/debian-kinesis/Dockerfile](#)

# Goals for work – fluentd-kubernetes-daemonset

if(kakao) dev 2019



```
14 ALL_IMAGES := \
15     v1.4/debian-elasticsearch:v1.4.2-debian-elasticsearch-1.1,v1.4-debian-elasticsearch-1 \
16     v1.4/debian-logzio:v1.4.2-debian-logzio-1.1,v1.4-debian-logzio-1 \
17     v1.4/debian-kafka:v1.4.2-debian-kafka-1.1,v1.4-debian-kafka-1 \
18     v1.4/debian-kinesis:v1.4.2-debian-kinesis-1.1,v1.4-debian-kinesis-1
19
20 #      <Dockerfile>:<version>,<tag1>,<tag2>,...
21
22 COPY Gemfile* /fluentd/
23
24 RUN buildDeps="sudo make gcc g++ libc-dev libffi-dev
25             <% elsif target == "kafka" %> build-essential
26                 automake libtool pkg-config<% end %> •••
27             && apt-get update \
28             •••
29
30
31 <% case target when "elasticsearch" %>
32 <% if is_v1 %>
33   gem "fluent-plugin-elasticsearch", "~> 3.4.2"
34 <% else %>
35   gem "fluent-plugin-elasticsearch"
36 <% end %>
37 <% when "logentries" %>
38   #gem "fluent-plugin-logentries"
```

# Goals for work – fluentd-kubernetes-daemonset

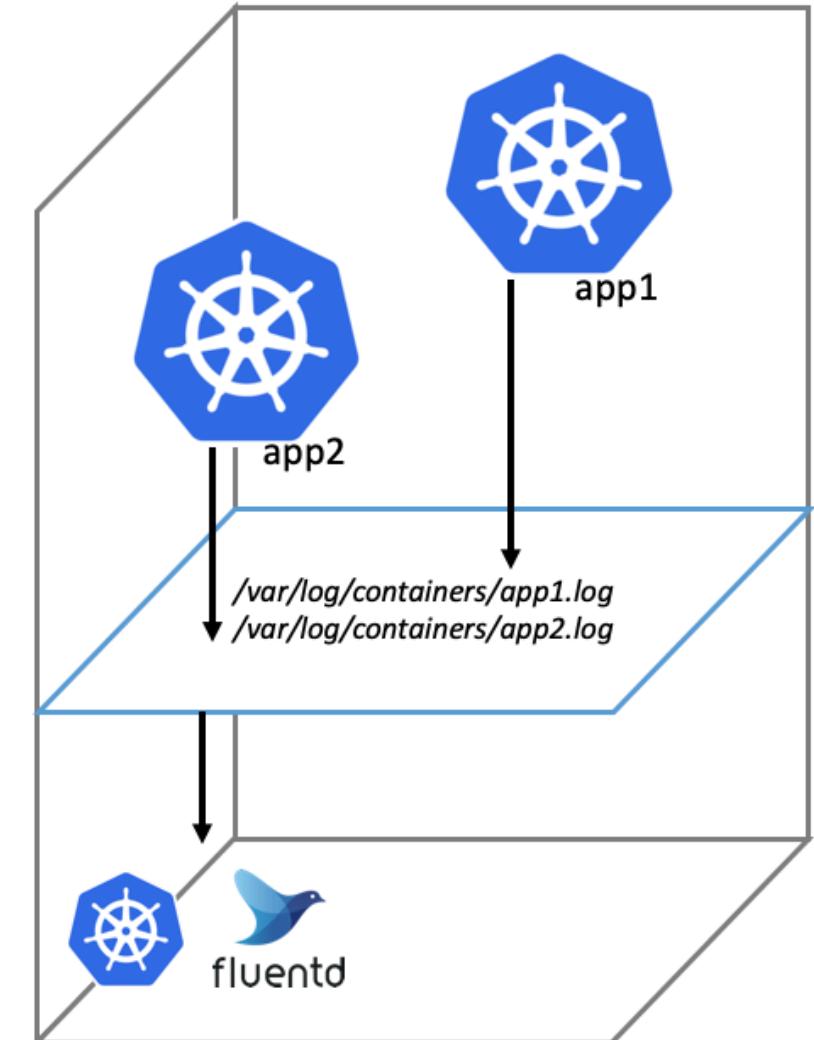
```
├── Makefile →  
├── README.md  
├── docker-image/  
├── plugins/  
└── templates/  
    ├── Dockerfile.erb →  
    ├── Gemfile.erb →  
    ├── README.md.erb  
    ├── post_push.erb  
    ├── entrypoint.sh.erb  
    └── conf  
        ├── fluent.conf.erb  
        ├── kubernetes.conf.erb  
        ├── prometheus.conf.erb  
        └── systemd.conf.erb
```

```
26 ALL_IMAGES := \  
27     v1.4/debian-hermes:v1.4.2-debian-hermes-1.0,v1.4-debian-hermes-1  
28 #     <Dockerfile>:<version>,<tag1>,<tag2>,...  
^  
  
|<% elsif target == "hermes" %> build-essential autoconf automake libtool pkg-config<% end %>  
29 |<% when "hermes" %>  
30 |gem "fluent-plugin-kafka", "~> 0.9.0"  
31 |gem "zookeeper", "~> 1.4.11"  
32 |gem "snappy", "~> 0.0.15"  
33 |gem "fluent-plugin-elasticsearch", "~> 3.4.2"  
34 |gem "fluent-plugin-record-modifier"
```

# Goals for work – using Helm

## Helm Chart for In-house

k8s resource type	Worker node	Ingress node
daemonset	fluentd	fluentd-ingress
configmap	fluentd-cm	fluentd-ingress-cm
clusterrole	fluentd	fluentd-ingress
clusterrolebindings	fluentd	fluentd-ingress
serviceaccount	fluentd	fluentd-ingress



# Goals for work – daemonset (1/2)

- Use customized fluentd docker
- Resource limit
- Environments

```
1 apiVersion: extensions/v1beta1
2 kind: DaemonSet
3 metadata:
4 ...
5 spec:
6   template:
7     spec:
8       containers:
9         image: /kocoon/fluentd-kubernetes-daemonset:
10        imagePullPolicy: IfNotPresent
11        name: kocoon-hermes
12        resources:
13          limits:
14            memory: 400Mi
15          requests:
16            cpu: 100m
17            memory: 200Mi
18        - env:
19          - name: K8S_NODE_NAME
20            valueFrom:
21              fieldRef:
22                apiVersion: v1
23                fieldPath: spec.nodeName
24          - name: KEMI_TAG
25            value: dkos_v3_jenny
```

# Goals for work – daemonset (2/2)

- Mount hostpath
  - timezone,  
application log path
- Mount configmap
  - fluentd configuration

```
26      volumeMounts:  
27        - mountPath: /var/log  
28          name: varlog  
29        - mountPath: /var/lib/docker/containers  
30          name: varlibdockercontainers  
31          readOnly: true  
32          name: tz-config  
33          readOnly: true  
34        - mountPath: /fluentd/etc/  
35          name: fluentd-config  
36      volumes:  
37        - hostPath:  
38          path: /var/log  
39          type: ""  
40          name: varlog  
41        - hostPath:  
42          path: /var/lib/docker/containers  
43          type: ""  
44          name: varlibdockercontainers  
45        - hostPath:  
46          path: /etc/localtime  
47          type: ""  
48          name: tz-config  
49        - configMap:  
50          defaultMode: 420  
51          name: fluentd-configmap  
52          name: fluentd-config
```

# Goals for work – daemonset (2/2)

- Mount hostpath
  - timezone,  
application log path
- Mount configmap
  - fluentd configuration

```
26      volumeMounts:  
27        - mountPath: /var/log  
28          name: varlog  
29        - mountPath: /var/lib/docker/containers  
30          name: varlibdockercontainers  
31          readOnly: true  
32          name: tz-config  
33          readOnly: true  
34        - mountPath: /fluentd/etc/  
35          name: fluentd-config  
36      volumes:  
37        - hostPath:  
38          path: /var/log  
39          type: ""  
40          name: varlog  
41        - hostPath:  
42          path: /var/lib/docker/containers  
43          type: ""  
44          name: varlibdockercontainers  
45        - hostPath:  
46          path: /etc/localtime  
47          type: ""  
48          name: tz-config  
49        - configMap:  
50          defaultMode: 420  
51          name: fluentd-configmap  
52          name: fluentd-config
```

# Goals for work – configmap

- Fluentd configmap
- Compose of 3 files
  - **input-kubernetes.conf**
  - **filter-kubernetes.conf**
  - **fluent.conf**

```
1 apiVersion: v1
2 kind: ConfigMap
3 metadata:
4 ...
5 data:
6   input-kubernetes.conf: |
7   ...
8   filter-kubernetes.conf: |
9   ...
10  fluent.conf: |
11  ...
12  @include input-kubernetes.conf
13  @include filter-kubernetes.conf
14  ...
```

# Goals for work

- L10-12  
:: too many logs
- L15  
:: avoid OOM
- L20, L22, L24  
:: docker log driver  
:: time zone setup

```

1  input-kubernetes.conf: |
2      <match fluent.**>
3          @type null
4      </match>
5
6      <source>
7          @type tail
8          @id in_tail_container_logs
9          path /var/log/containers/*.log
10         exclude_path ["/var/log/containers/*_kube-system_*.log",
11                         "/var/log/containers/*_monitoring_*.log",
12                         "/var/log/containers/fluentd*.log"]
13         pos_file /var/log/fluentd-containers.log.pos
14         tag kubernetes.-
15         read_from_head "#{ENV['FLUENTD_INPUT_READ_FROM_HEAD'] || 'false'}"
16         rotate_wait 0
17         enable_stat_watcher false
18
19         # Json Log Example:
20         #
21         # "log":"[info:2016-02-16T16:04:05.930-08:00] Some log text here\n",
22         # "stream":"stdout",
23         # "time":"2016-02-17T00:04:05.931087621Z"
24         #
25         <parse>
26             @type "#{ENV['K8S_FORMAT_PARSER'] || 'json' }"
27             time_format %Y-%m-%dT%H:%M:%S.%NZ
28             time_key time
29             keep_time_key true
30             timezone "+00:00"
31         </parse>
32     </source>

```

# Goals for work

- L10-12  
:: too many logs
- L15  
:: avoid OOM
- L20, L22, L24  
:: docker log driver  
:: time zone setup

```

1  input-kubernetes.conf: |
2      <match fluent.**>
3          @type null
4      </match>
5
6      <source>
7          @type tail
8          @id in_tail_container_logs
9          path /var/log/containers/*.log
10         exclude_path [
11             "/var/log/containers/*_kube-system_*.log",
12             "/var/log/containers/*_monitoring_*.log",
13             "/var/log/containers/fluentd*.log"
14         ]
15         pos_file /var/log/fluentd-containers.log.pos
16         tag kubernetes.*
17         read_from_head "#{ENV['FLUENTD_INPUT_READ_FROM_HEAD']} || 'false'"
18         rotate_wait 0
19         enable_stat_watcher false
20
21         # Json Log Example:
22         # {
23         #     "log": "[info:2016-02-16T16:04:05.930-08:00] Some log text here\n",
24         #     "stream": "stdout",
25         #     "time": "2016-02-17T00:04:05.931087621Z"
26         # }
27         <parse>
28             @type "#{ENV['K8S_FORMAT_PARSER']} || 'json' "
29             time_format %Y-%m-%dT%H:%M:%S.%NZ
30             time_key time
31             keep_time_key true
32             timezone "+00:00"
33         </parse>
34     </source>

```

# Goals for work – filter-kubernetes.conf (1/2)

```
/var/log/containers$ ls
elasticsearch-data-3_logging_chown-d999f3ebde6806426ca4b87166bc2b4f4cae4769068f32758283e53bce75bc50.log
elasticsearch-master-1_logging_chown-9ae026b63f15021f6d81982d25e64d3893f63fd99ad2667c5fbffc0598533622.log
fluentd-c9hcv_kube-system_kocoon-hermes-ea57791cf432fb0bb6c6a2e75f026b6a67b58619cc5f254cc5139d50ef78de5f.log
```

```

1 filter-kubernetes.conf: |
2   <match kubernetes.**>
3     @type record_modifier
4     prepare_value @kube_file_regex = 'kubernetes\\.var\\.log\\.containers\\.(?<pod_na
5     @regexp_compiled = Regexp.compile(@kube_file_regex)
6     tag "#{{ENV['KEMI_TAG']}}"
7     <record>
8       @timestamp ${Time.at(time).strftime('%Y-%m-%dT%H:%M:%S.%L+09:00')}
9       cluster_name "#{{ENV['CLUSTER_NAME']}}"
10      hostname "#{{ENV['K8S_NODE_NAME']}}"
11      kubernetes ${tag.match(@regexp_compiled).named_captures}
12    </record>
13  </match>
14
```

- L4-5, L11

**:: replace kubernetes-metadata-plugin**

It use too many resources on master

=> pod\_name, namespace, container\_name, docker\_id

# Goals for work – filter-kubernetes.conf (2/2)

```
15 # log에 해당하는 부분을 파싱하기 위한 부분
16 # Json Log Example:
17 #
18 #   "log": "{\"some\":\"log\"}",
19 #   "stream": "stdout",
20 #   "time": "2016-02-17T00:04:05.931087621Z"
21 #
22 # 만약에 @type json이면서, 해당하는 time_key가 존재하지 않는경우, 이 필터에 도착한 시간으로 event_time이 바뀐다.
23 <filter **>
24   @type parser
25   key_name log
26   reserve_data true
27   emit_invalid_record_to_error false
28   remove_key_name_field true
29   <parse>
30     @type      "#{ENV['APP_LOG_FORMAT'] || 'none'}"
31     expression "#{ENV['APP_LOG_EXPRESSION'] || '/.*$/'}"
32     types     "#{ENV['APP_LOG_FORMAT_TYPES'] || nil}"
33     keep_time_key true
34     time_key   "#{ENV['APP_LOG_TIME_KEY'] || '_time_log_agent_'}"
35     time_format "#{ENV['APP_LOG_TIME_KEY_FORMAT'] || '%Y-%m-%d %H:%M:%S.%NZ'}"
36     message_key log
37   </parse>
38 </filter>
```

# Goals for work – fluent.conf

- L7,8
  - import configurations
- L10 – 25
  - forward to KEMI Log-aggregator

@type can be replaced with  
kafka or elasticsearch

```
1 fluent.conf: |
2   @include input-kubernetes.conf
3   @include filter-kubernetes.conf
4
5   <match **>
6     @type copy
7     <store>
8       @type           forward
9       @id             out_forward
10      expire_dns_cache 60s
11      <server>
12        host          "#{ENV['KEMI_LOG.Aggregator']}"
13      </server>
14      <buffer>
15        @type           memory
16        flush_interval  5s
17        flush_at_shutdown true
18      </buffer>
19    </store>
20  </match>
```

# Which issue?

**case 1. w/ fluentd-metadata-plugin**

**using memory with K8S node counts & metadata information**

**⇒ fluentd supervisor (PID 1) OOM killed (docker restart)**

**⇒ drop pos file**

**case 2. w/o fluentd-metadata-plugin**

**⇒ fluentd worker (PID 2) got SIGKILL**

**⇒ drop data which in output buffer memory (before flushed)**

**⇒ using same pos file**

# SLA?

**sensitive with memory  
using only worker's resource**

**1000 lines / sec is ok (under 4K/msg)**

```
resources:  
limits:  
  memory: 400Mi  
requests:  
  cpu: 100m  
  memory: 200Mi
```

# Use Case? ... 000+ cluster

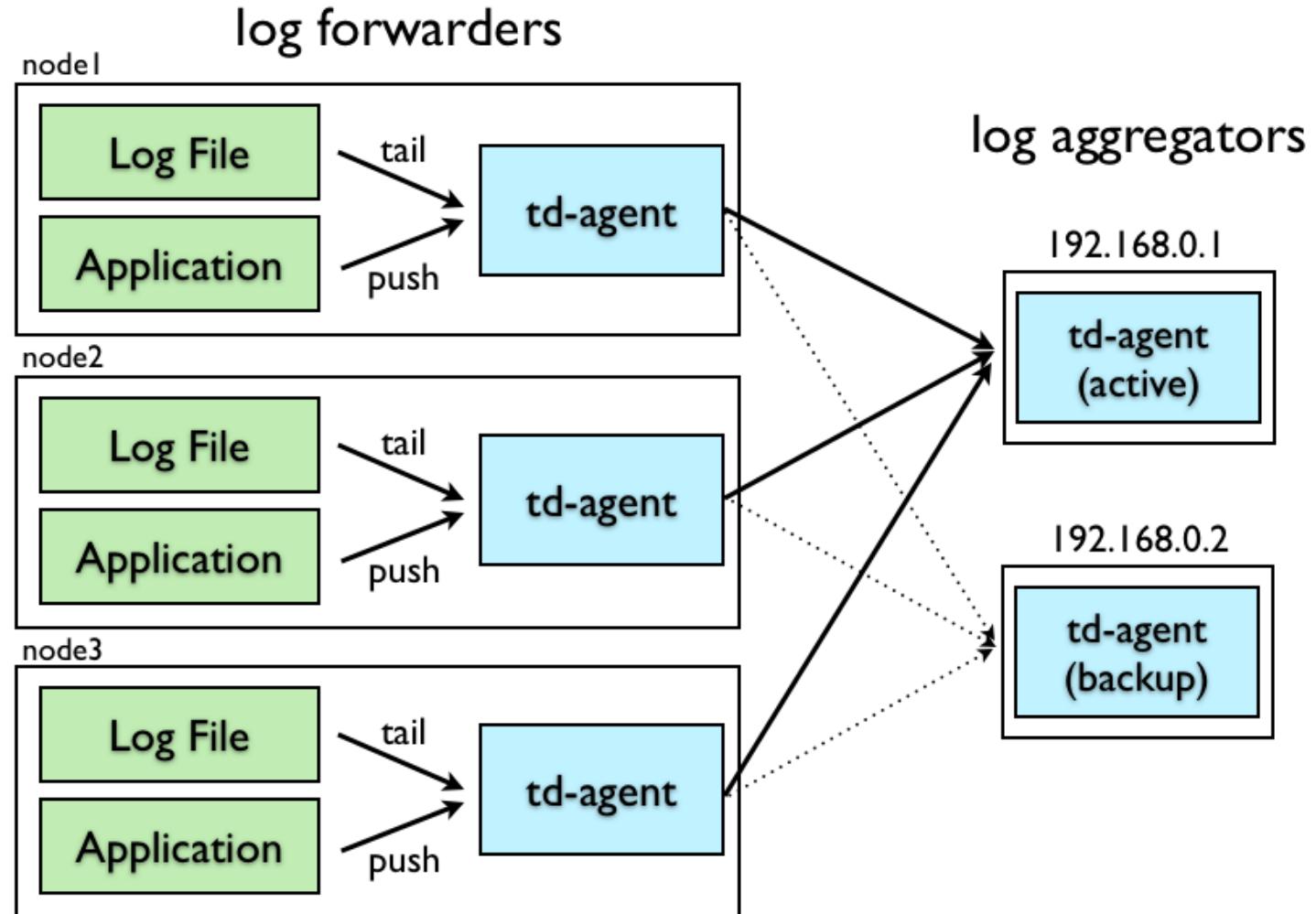
if(kakao) dev 2019

차트명	클러스터	Version	AppVersion	KubesprayVersion	K8sVersion
kocoon-hermes	██████████	1.0.3	1.4.2	kakao/v2.5.0	v1.9.5
kocoon-hermes	██████████	1.0.3	1.4.2	kakao/v2.5.0	v1.9.5
kocoon-hermes	██████████	1.0.3	1.4.2	kakao/v2.5.0	v1.9.5
kocoon-hermes	██████████	1.0.3	1.4.2	kakao/v2.5.0	v1.9.5
kocoon-hermes	██████████	1.0.3	1.4.2	v2.7.3	v1.11.5
kocoon-prometheus	██████████	0.0.6	5.7.0	v2.7.3	v1.11.3
kocoon-prometheus	██████████	0.0.6	5.7.0	v2.7.3	v1.11.5
kocoon-prometheus	██████████	0.0.6	5.7.0	v2.7.3	v1.11.5
kocoon-prometheus	██████████	0.0.7	5.7.0	v2.7.3	v1.11.5

# 07 KEMI Log-aggregator

if(kakao) dev 2019

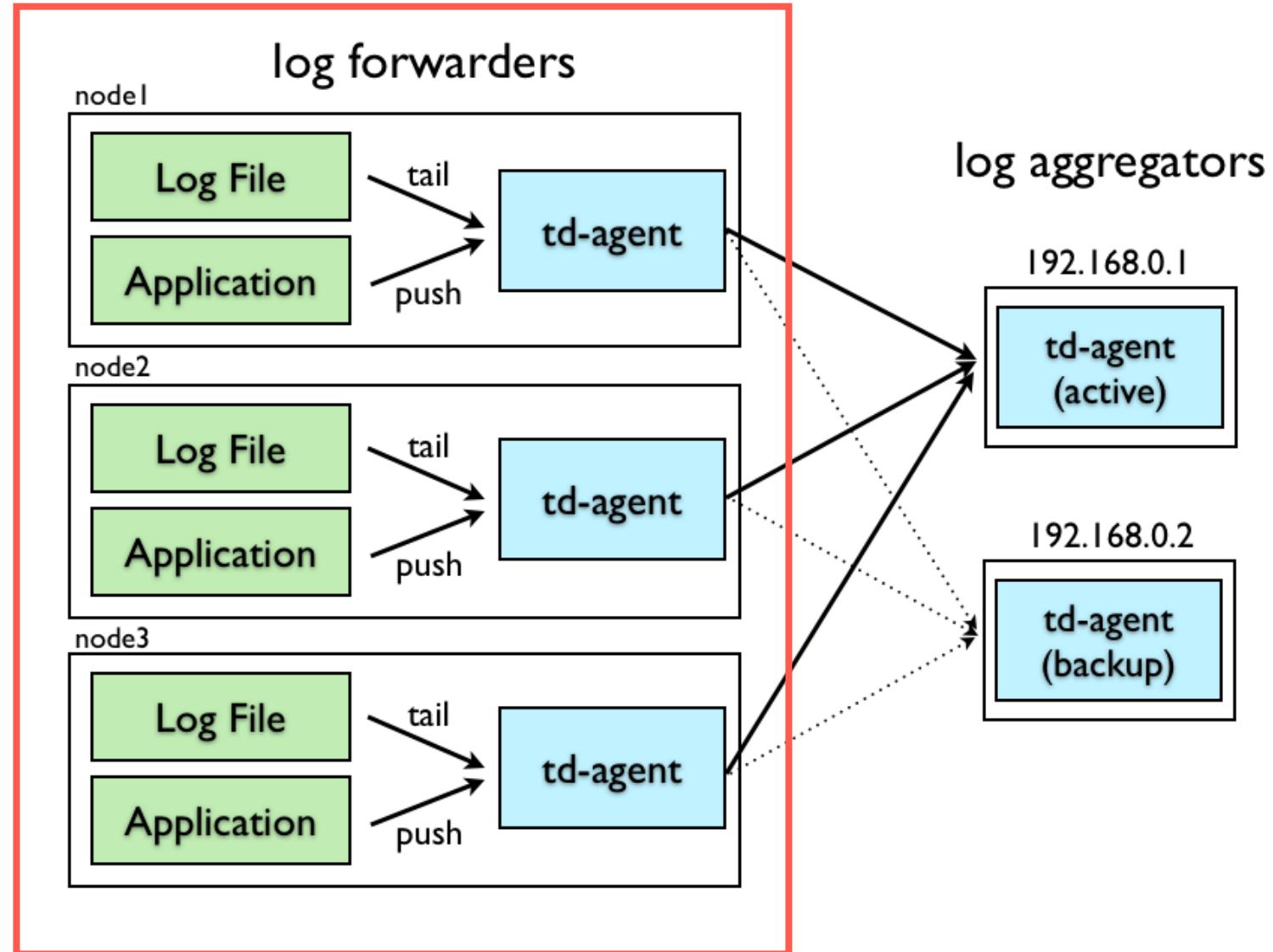
# HA reference in fluentd official documents



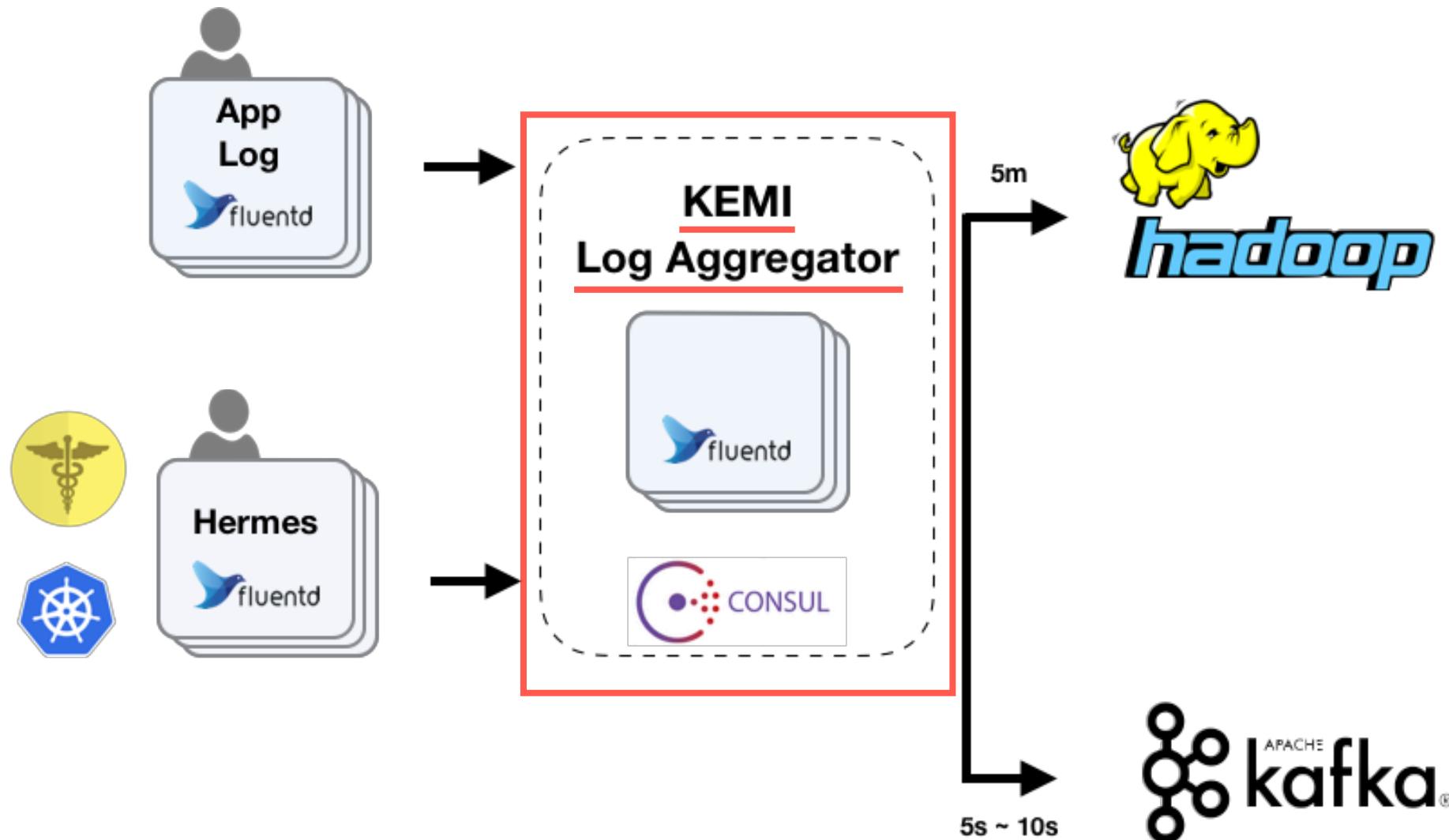
# HA reference in fluentd official documents



Hermes



# KEMI Log-aggregator – architecture



# KEMI Log-aggregator – consul?



if (kakao) dev 2019

## Health Checks

Pairing service discovery with health checking prevents routing requests to unhealthy hosts and enables services to easily provide circuit breakers.

```
$ dig web-frontend.service.consul. ANY  
  
; <>> DiG 9.8.3-P1 <>> web-frontend.service.consul. ANY  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29981  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDIT  
  
;; QUESTION SECTION:  
;web-frontend.service.consul. IN ANY  
  
;; ANSWER SECTION:  
web-frontend.service.consul. 0 IN A 10.0.3.83  
web-frontend.service.consul. 0 IN A 10.0.1.109
```

A screenshot of the HashiCorp Consul UI. The top navigation bar includes tabs for dc1, Services, Nodes (which is selected), Key/Value, ACL, and Intentions. On the right, there are links for Documentation and Settings, and a search bar labeled "Search by name". The main content area is titled "Nodes" and shows a summary: All (38), Passing (32), Warning (2), Critical (4). Below this is a section for "Unhealthy Nodes" containing six entries, each with a node name, IP, and a list of failing checks. To the right is a section for "Healthy Nodes" containing three entries. Each entry shows the node name, IP, and a list of passing checks.

## DNS Query Interface

Consul enables service discovery using a built-in DNS server. This allows existing applications to easily integrate, as almost all applications support using DNS to resolve IP addresses. Using DNS instead of a static IP address allows services to scale up/down and route around failures easily.

# KEMI Log-aggregator – Health Check

## Health check

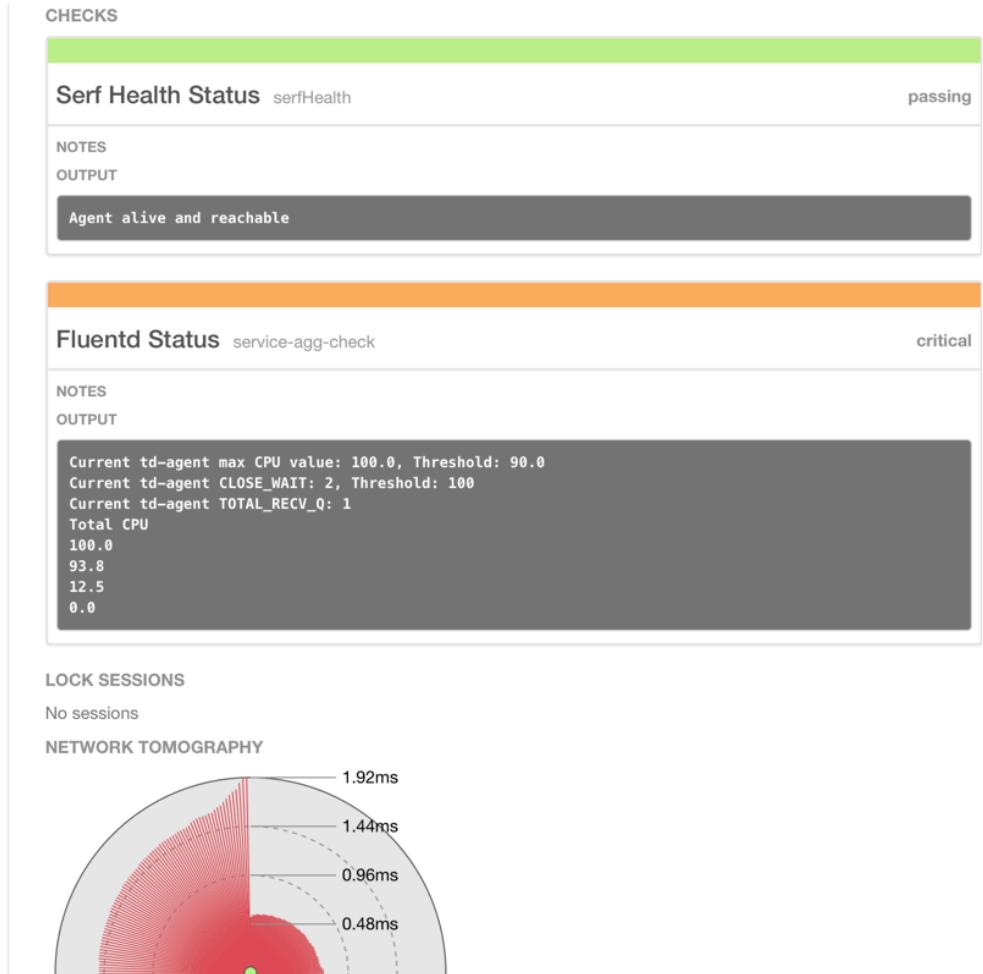
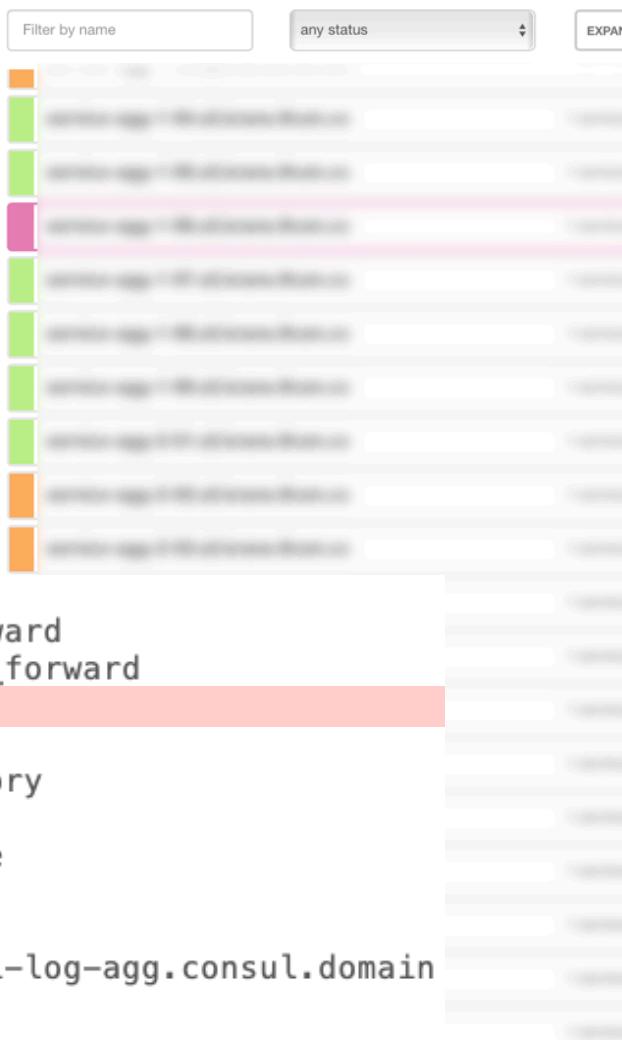
- CPU
- CLOSE\_WAIT (for kafka)

```

<store>
  @type
  @id
  expire_dns_cache
  <buffer>
    @type
    flush_interval
    flush_at_shutdown
  </buffer>
  <server>
    host
  </server>
</store>

```

	forward	
	out_forward	
expire_dns_cache	60s	
<buffer>	memory	
	5s	
	true	
		kemi-log-agg.consul.domain

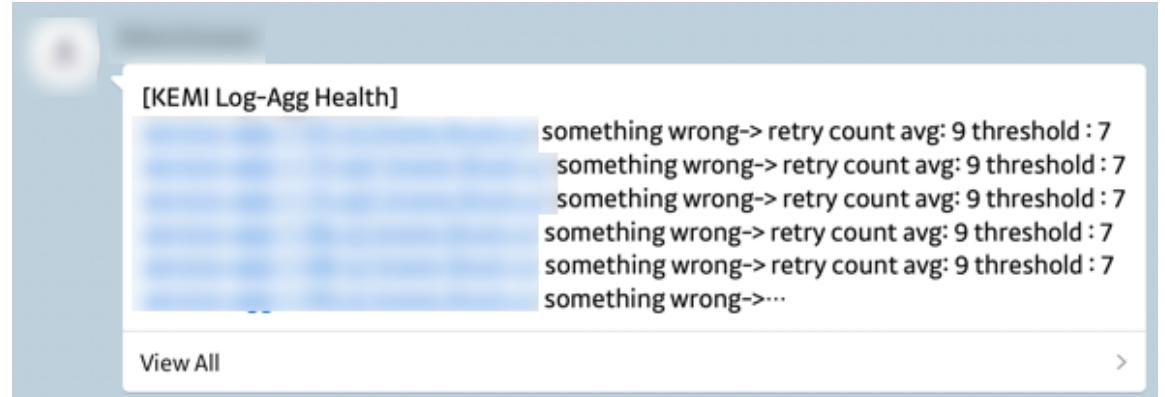


# KEMI Log-aggregator – Monitoring

- monitoring with monitor agent

Usually alert by ...

- HDFS namenode failover



```
curl -s :24420/api/plugins
plugin_id:input_forward plugin_category:input type:forward output_plugin:false retry_count:
plugin_id:object:3fa7efec8ae8 plugin_category:input type:syslog output_plugin:false retry_count:
plugin_id:object:3fa7f011ee78 plugin_category:input type:syslog output_plugin:false retry_count:
plugin_id:input_http plugin_category:input type:http output_plugin:false retry_count:
plugin_id:object:3fa7ef7d8274 plugin_category:input type:monitor_agent output_plugin:false retry_count:
plugin_id:object:3fa7eff77188 plugin_category:output type:rewrite_tag_filter output_plugin:true retry_count:0
plugin_id: group_copy_plugin plugin_category:output type:copy output_plugin:false retry_count:0
plugin_id: webhdfs_kemi_hadoop plugin_category:output type:webhdfs output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: kafka_common plugin_category:output type:kafka2 output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _alpha_group_copy_plugin plugin_category:output type:copy output_plugin:false retry_count:0
plugin_id: _alpha_webhdfs_kemi_hadoop plugin_category:output type:webhdfs output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _alpha.kafka_common plugin_category:output type:kafka2 output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _group_copy_plugin plugin_category:output type:copy output_plugin:false retry_count:0
plugin_id: _webhdfs_kemi.hadoop plugin_category:output type:webhdfs output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _kafka_common plugin_category:output type:kafka2 output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _alpha_group_copy_plugin plugin_category:output type:copy output_plugin:false retry_count:0
plugin_id: _alpha_webhdfs_kemi_hadoop plugin_category:output type:webhdfs output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
plugin_id: _alpha.kafka_common plugin_category:output type:kafka2 output_plugin:true buffer_queue_length:0 buffer_total_queued_size:0 retry_count:0
```

# KEMI Log-aggregator – is stability?

- connection management
- fluentd file buffering is very powerful (v1.0>)
  - reprocess is also good

```
:/var/log/td-agent/buffer/webhdfs_kemi_hadoop/ $ ls -al *
worker0:
total 25892
drwxr-xr-x 2 td-agent td-agent 12288 Aug 12 10:43 .
drwxr-xr-x 5 td-agent td-agent 4096 Nov 1 2018 ..
-rw-r--r-- 1 td-agent td-agent 14144 Aug 12 10:43 buffer.b58fe198d95a3d0271ae26af46c95e08a.log
-rw-r--r-- 1 td-agent td-agent 97 Aug 12 10:43 buffer.b58fe198d95a3d0271ae26af46c95e08a.log.meta
-rw-r--r-- 1 td-agent td-agent 19223 Aug 12 10:42 buffer.b58fe199077698c5af074eb0227d17cbb.log
-rw-r--r-- 1 td-agent td-agent 86 Aug 12 10:42 buffer.b58fe199077698c5af074eb0227d17cbb.log.meta
-rw-r--r-- 1 td-agent td-agent 3717 Aug 12 10:40 buffer.b58fe19cfcfa11cc7cd6492956cb0eb3c3.log
-rw-r--r-- 1 td-agent td-agent 86 Aug 12 10:40 buffer.b58fe19cfcfa11cc7cd6492956cb0eb3c3.log.meta
-rw-r--r-- 1 td-agent td-agent 4998 Aug 12 10:40 buffer.b58fe19d02f93c781585c1c4c4ec0e5f9.log
-rw-r--r-- 1 td-agent td-agent 93 Aug 12 10:40 buffer.b58fe19d02f93c781585c1c4c4ec0e5f9.log.meta

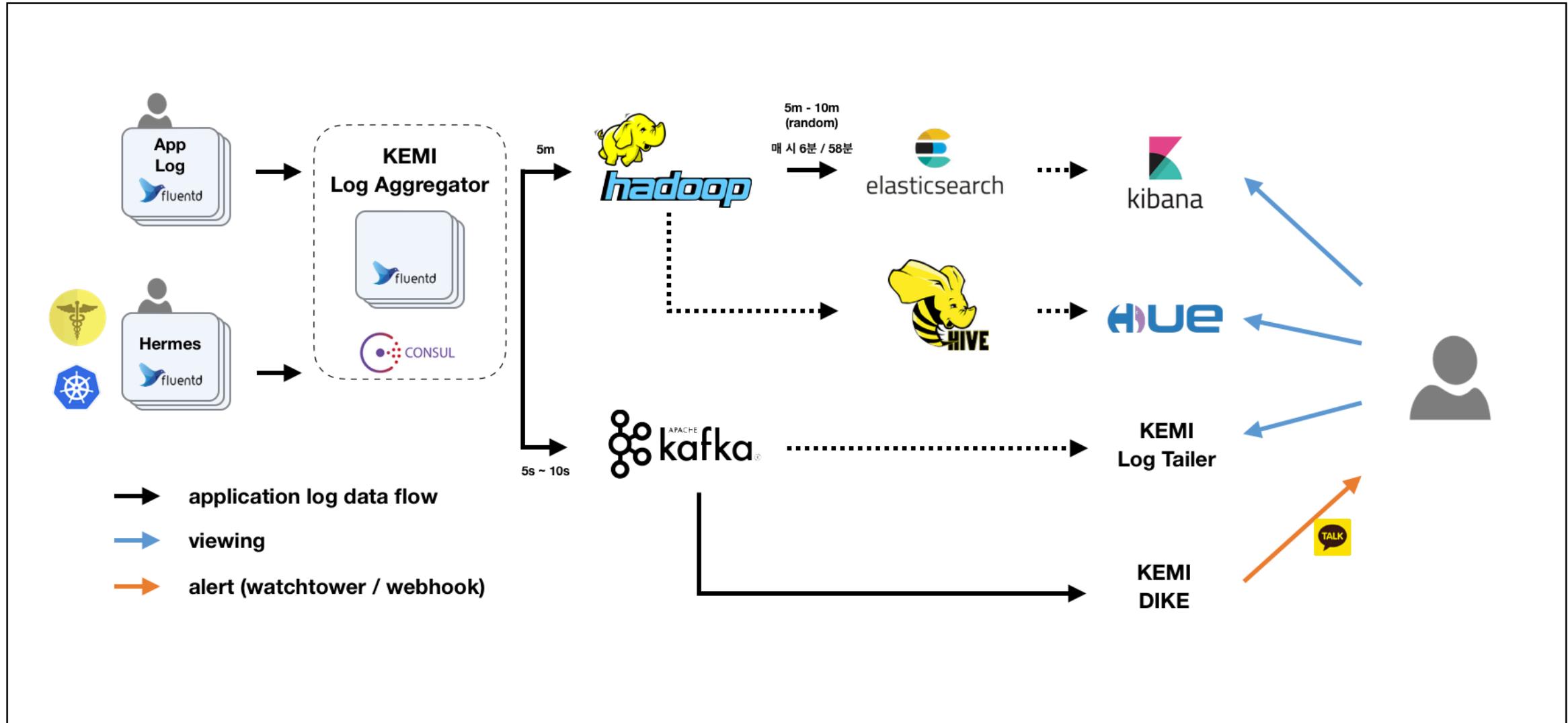
worker1:
total 14068
drwxr-xr-x 2 td-agent td-agent 12288 Aug 12 10:43 .
drwxr-xr-x 5 td-agent td-agent 4096 Nov 1 2018 ..
-rw-r--r-- 1 td-agent td-agent 29860 Aug 12 10:44 buffer.b58fe19d840862cbf9cdf0b8b3dbf4afa.log
-rw-r--r-- 1 td-agent td-agent 86 Aug 12 10:44 buffer.b58fe19d840862cbf9cdf0b8b3dbf4afa.log.meta
-rw-r--r-- 1 td-agent td-agent 32532 Aug 12 10:41 buffer.b58fe19dc98cb3bf5f7ad0e67b2a86870.log
-rw-r--r-- 1 td-agent td-agent 93 Aug 12 10:41 buffer.b58fe19dc98cb3bf5f7ad0e67b2a86870.log.meta
-rw-r--r-- 1 td-agent td-agent 7041 Aug 12 10:41 buffer.b58fe19e2e06cfacd77790b221bbd73c6.log
-rw-r--r-- 1 td-agent td-agent 86 Aug 12 10:41 buffer.b58fe19e2e06cfacd77790b221bbd73c6.log.meta
-rw-r--r-- 1 td-agent td-agent 17243 Aug 12 10:41 buffer.b58fe19e5d822e49a8fb934913ac9e71.log
-rw-r--r-- 1 td-agent td-agent 92 Aug 12 10:41 buffer.b58fe19e5d822e49a8fb934913ac9e71.log.meta
-rw-r--r-- 1 td-agent td-agent 1643 Aug 12 10:41 buffer.b58fe19eb752d7f5cdc6a63f0dfe47daa.log
-rw-r--r-- 1 td-agent td-agent 91 Aug 12 10:41 buffer.b58fe19eb752d7f5cdc6a63f0dfe47daa.log.meta
-rw-r--r-- 1 td-agent td-agent 9392 Aug 12 10:41 buffer.b58fe19ebfef3ff2cfa9e4882a5d9d28d.log
-rw-r--r-- 1 td-agent td-agent 82 Aug 12 10:41 buffer.b58fe19ebfef3ff2cfa9e4882a5d9d28d.log.meta
-rw-r--r-- 1 td-agent td-agent 29117 Aug 12 10:41 buffer.b58fe19f2c1bb9a2863298456a0da6de7.log
-rw-r--r-- 1 td-agent td-agent 96 Aug 12 10:41 buffer.b58fe19f2c1bb9a2863298456a0da6de7.log.meta

worker2:
total 24396
drwxr-xr-x 2 td-agent td-agent 12288 Aug 12 10:44 .
drwxr-xr-x 5 td-agent td-agent 4096 Nov 1 2018 ..
-rw-r--r-- 1 td-agent td-agent 770097 Aug 12 10:39 buffer.b58fe198bf5cbf8ce21311b187c35ea01.log
-rw-r--r-- 1 td-agent td-agent 85 Aug 12 10:39 buffer.b58fe198bf5cbf8ce21311b187c35ea01.log.meta
-rw-r--r-- 1 td-agent td-agent 10672 Aug 12 10:43 buffer.b58fe19945d4525f6bae63e8e3a19bd2a.log
-rw-r--r-- 1 td-agent td-agent 97 Aug 12 10:43 buffer.b58fe19945d4525f6bae63e8e3a19bd2a.log.meta
```

# 08 AS-IS ...

if(kakao) dev 2019

# AS-IS ...

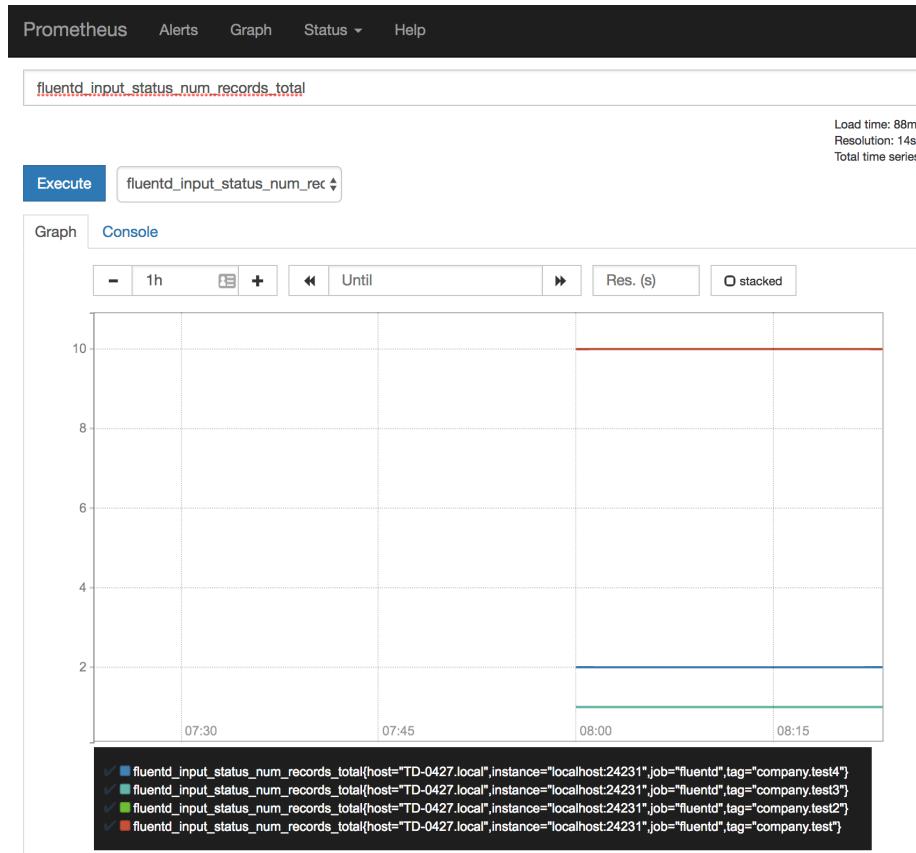


# 09 TOBE ...

if(kakao) dev 2019

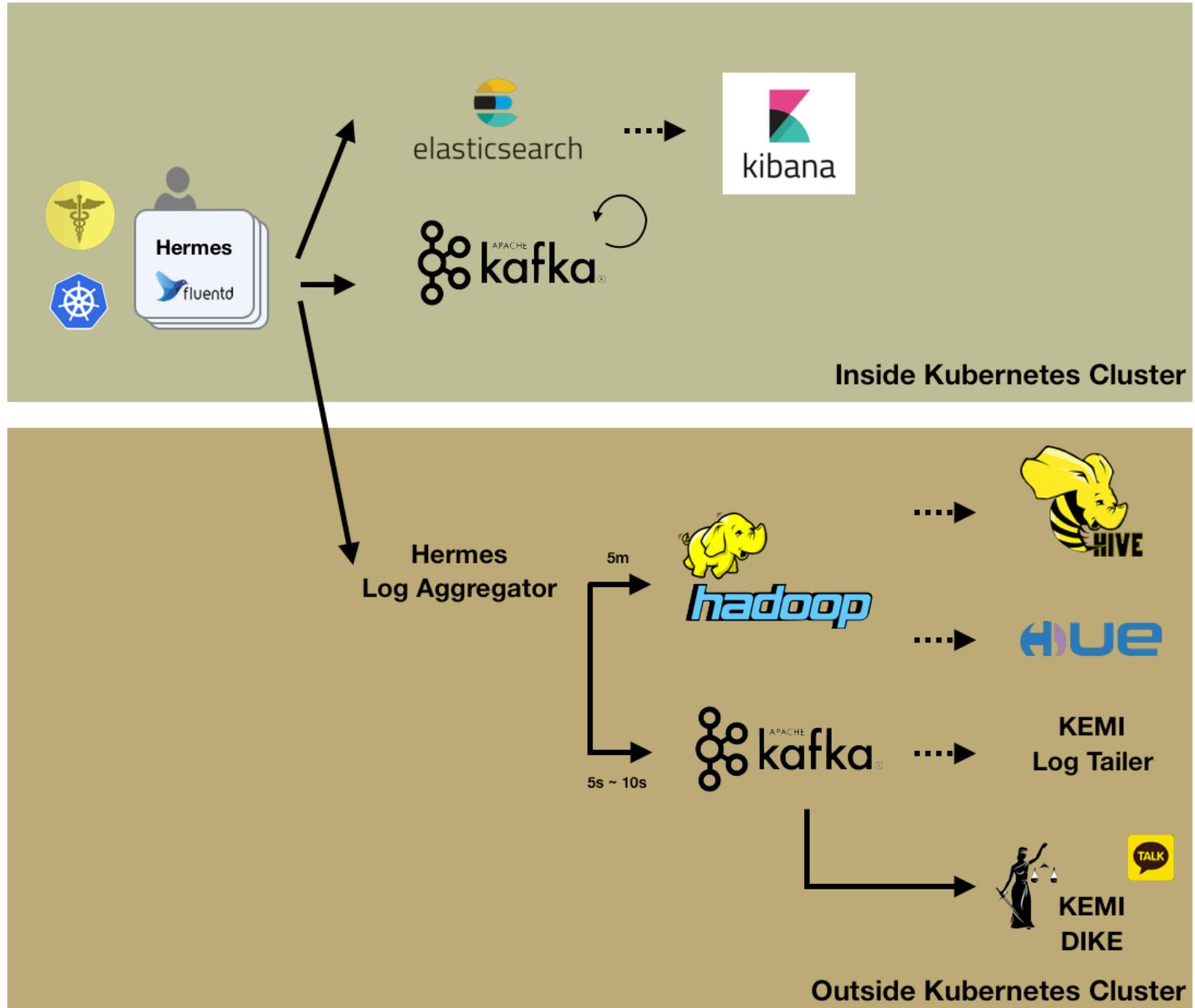
# TOBE ...

## - hermes fluentd self-monitoring with [fluent-plugin-prometheus](#) @ kocoon



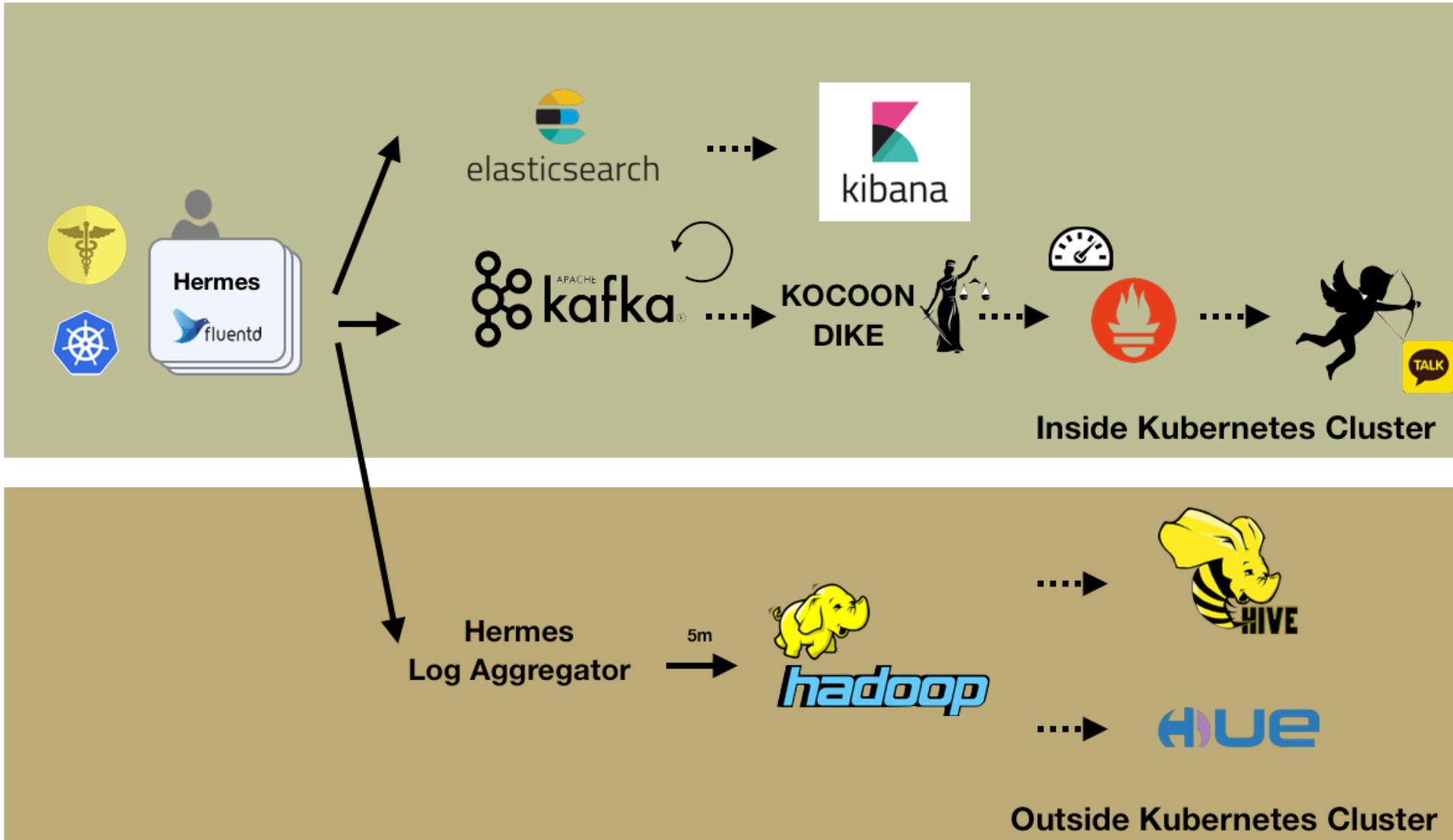
# TOBE ...

## Phase 1



# TOBE ... Phase 2

if (kakao) dev 2019



# 00 Q&A

if(kakao) dev 2019

# 09 Thank you

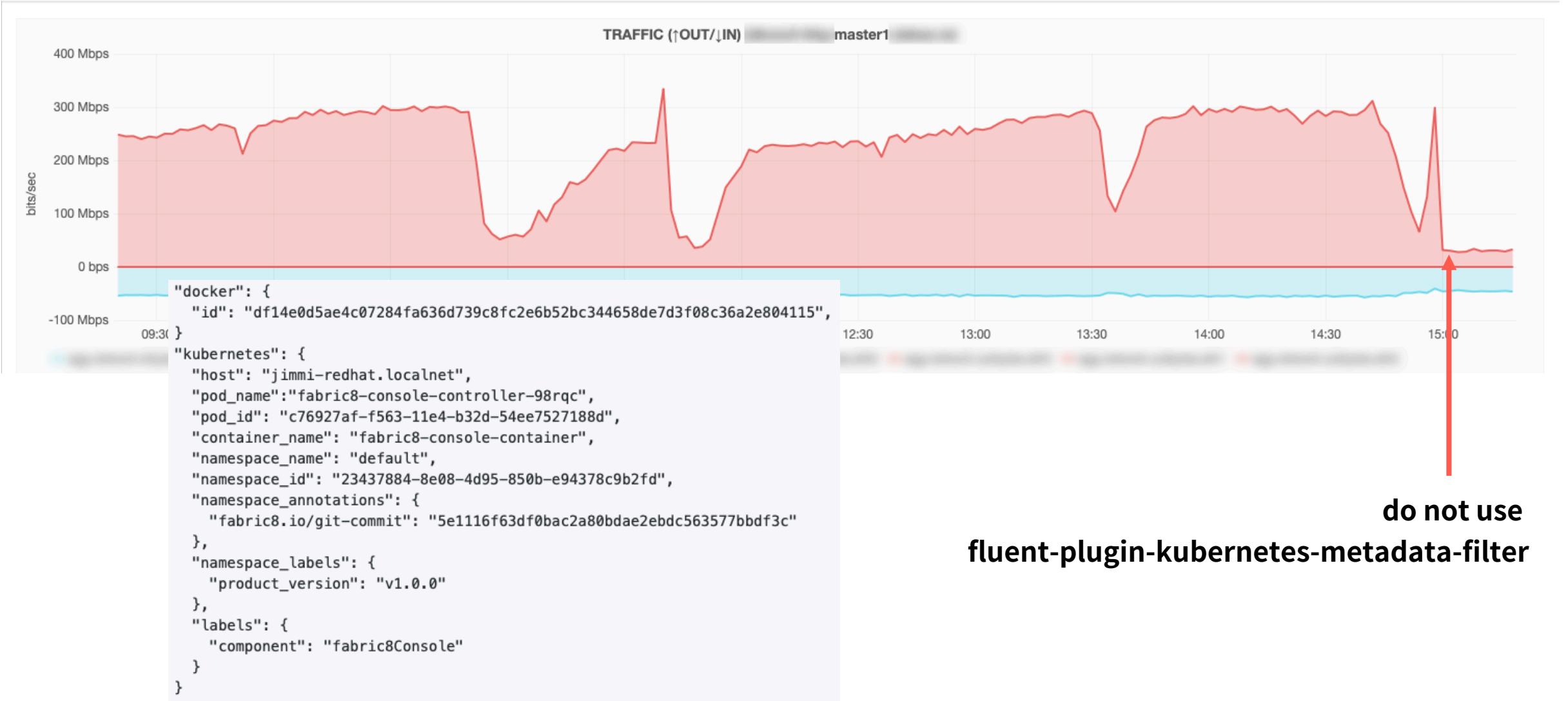
---

also Thanks to `cloud.telemetry`

# 00 Appendix

if(kakao) dev 2019

# Too many resources on master



# AS-IS ...

if(kakao) dev 2019

# compare log monitor

	O/KAFKA	O/HDFS	O/ES	Service name mgmt	HA
fluentd	O	O	O	O	fluentd
fluent-bit	O	X	O	X	fluentd
filebeat	O	X	O	Δ	logstash