Logging at Scale

using **Graylog**

billion+ messages, 100k+ msg/sec

Rohit Gupta

@rohit01

www.rohit.io

Production Engineer II, OlaCabs

What is Graylog?

- Open source **log management** that actually works
- Search, analysis, alerting and a lot more

Ola Logging Requirements

- **Volume:** Billion+ logs per day
- **Velocity:** 100k+ messages per sec
- **Variety:** Hundreds of micro-services

Why not ELK?

- ELK Clusters are **maintenance intensive**
- We often end-up building on top of ELK

But why Graylog?

Great UI, best for viewing logs

graylog | Search | Streams | Dashboards | Sources | System | In **251,232** / Out **251,454** msg/s | Help | Rohit Gupta

Search in the last 1 day | Not updating | Saved searches

`application:heka-docker-logs-kafka`

Search result

Found **4,997 messages** in 136 ms, searched in 77 indices.

Add count to dashboard | Save search criteria | More actions

Fields

Default | All | None | Filter fields

- application
- container_id
- log
- logbucket
- logtime
- message
- source
- stack
- stream
- time
- version

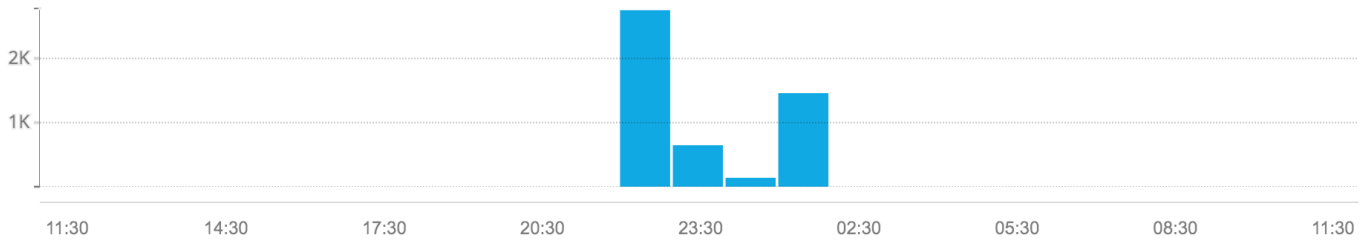
List fields of **current page** or all fields.

Highlight results

Histogram

Add to dashboard

Year, Quarter, Month, Week, Day, **Hour**, Minute



Messages

Previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Next

Timestamp	source	log
2016-07-21 01:52:36.000	devops-applications	2016/07/20 20:22:36 Input 'dockerlogs' error: record exceeded MAX_RECORD_SIZE 65794 and was dropped
2016-07-21 01:52:36.000	devops-applications	2016/07/20 20:22:36 Input 'dockerlogs' error: record exceeded MAX_RECORD_SIZE 65794 and was dropped
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:20 Pre-loading: [DashboardOutput]
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:20 Loading: [HekaFramingSplitter]
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:20 Loading: [ProtobufDecoder]
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:21 Starting hekad...
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:20 Pre-loading: [KafkaOutput-app_devops]
2016-07-21 01:52:21.000	devops-applications	2016/07/20 20:22:20 Pre-loading: [ProtobufEncoder]

Dashboard

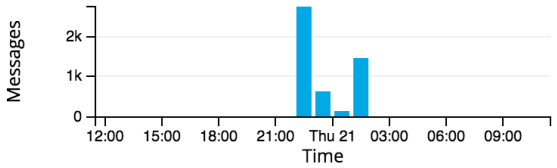
heka

heka

Drag widgets to any position you like in unlock / edit mode.

heka message trend

a few seconds ago



One day message count

a few seconds ago

4,997

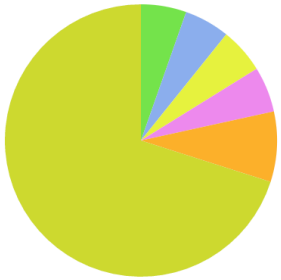
Cardinality

a few seconds ago

821

Quick values

a few seconds ago



Value	%	Count
Top values		
2016/07/20 18:32:40 Input 'dockerlogs' error: record exceeded MAX_RECORD_SIZE 65794 and was dropped	3.28%	164
heka:INFO [Step 4.1] Processing module file (gelf_log_bucket.lua) with template	2.12%	106
heka:INFO [Step 3] config file updated from template	2.12%	106
heka:INFO [Step 2] Generating config file from template	2.12%	106
heka:INFO [Step 1] Reading config file: /heka/etc/docker_to_kafka.toml	2.12%	106
Others		
heka:INFO [Step 5] Starting Heka	2.12%	106
heka:INFO [Step 4.2] gelf_log_bucket.lua) updated	2.12%	106
heka:INFO [Step 4] checking config file for custom modules	2.12%	106

Easy manageability of Elasticsearch indexes

Indices

This is an overview of all indices (message stores) Graylog is currently taking in account for searches and analysis.

You can learn more about the index model in the documentation

Maintenance

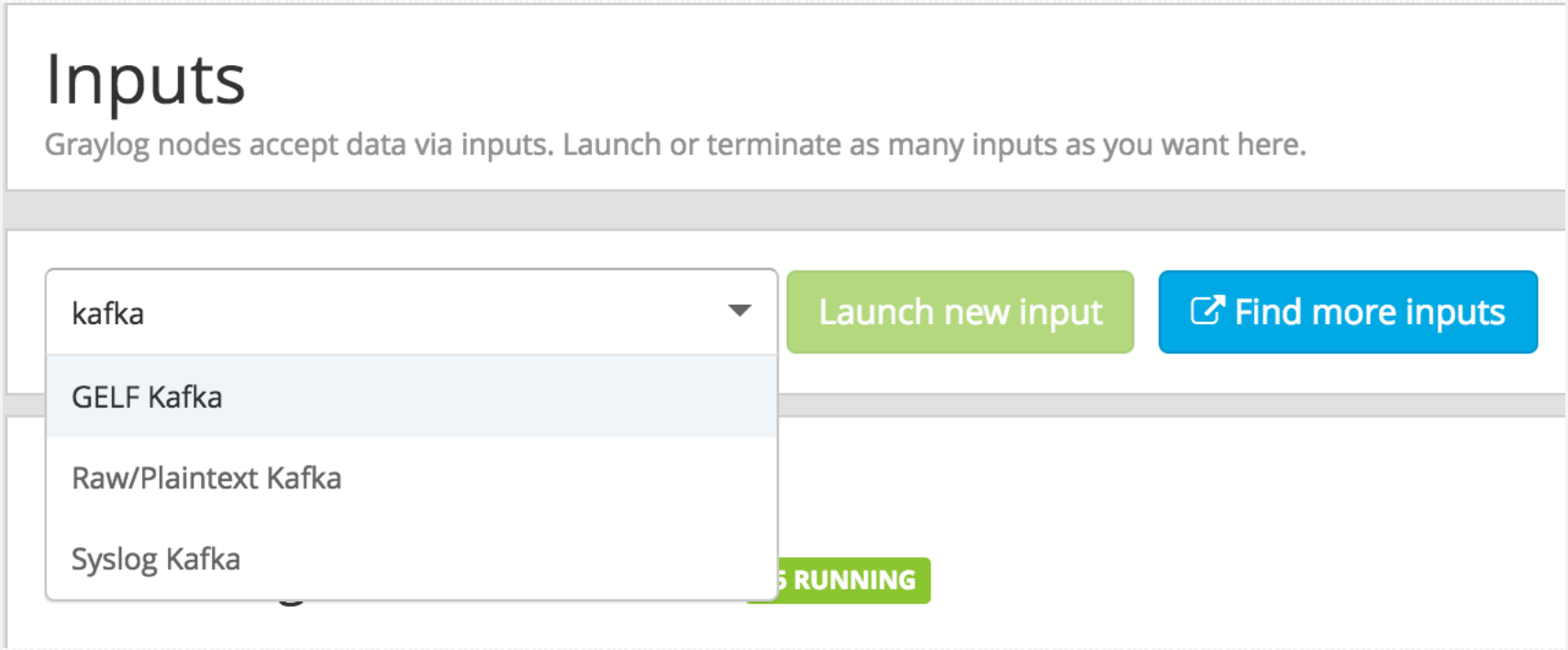
Settings

Index rotation strategy: Message Count
Max docs per index: 40000000

Index retention strategy: Delete
Max number of indices: 250

Update configuration

Several input & output options



Stream **IN** logs from anywhere

Stream **OUT** logs to anywhere

Real-time log analysis & alerts

Streams

You can route incoming messages into streams by applying rules against them. If a message matches all rules of a stream it is routed into it. A message can be routed into multiple streams. You can for example create a stream that contains all SSH logins and configure to be alerted whenever there are more logins than usual. Read more about streams in the documentation.

Take a look at the Graylog stream dashboards for wall-mounted displays or other integrations.

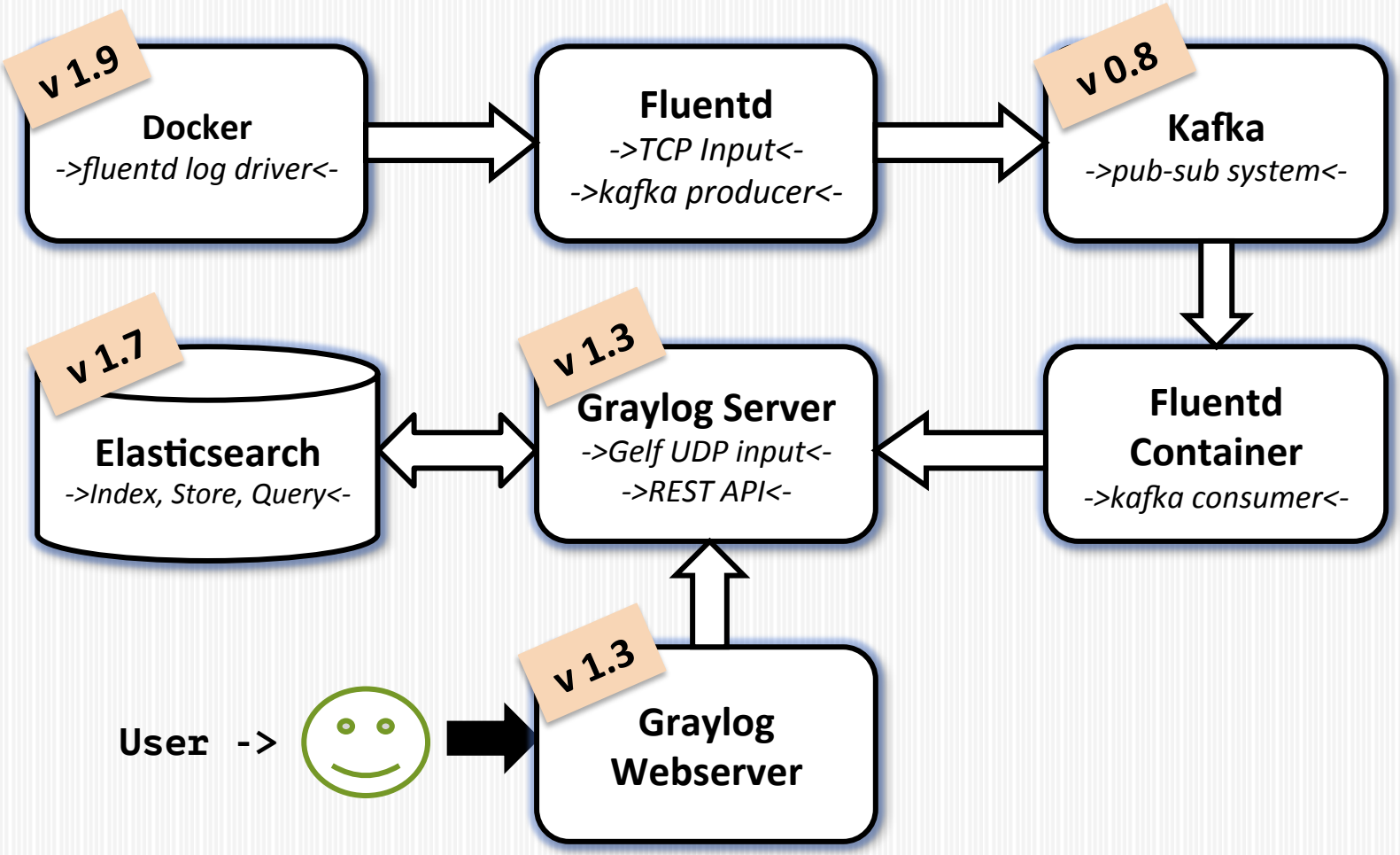
Create Stream

- **Define criteria for streams**
- **Analyze and configure alerts**
- **Create pipelines & dashboards**

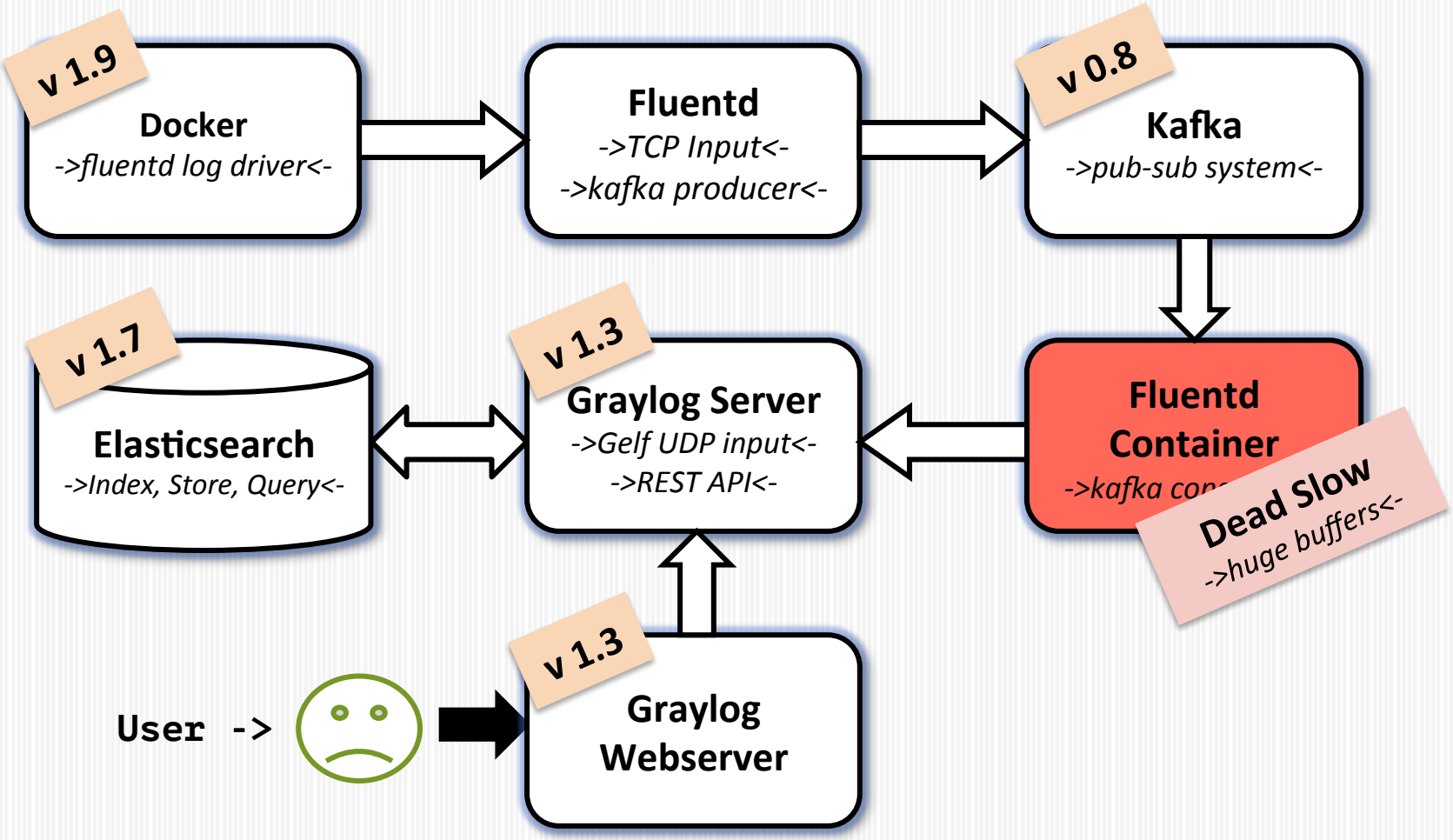
Problems & learning's

the *Ola* story!

#1: Initial Pipeline

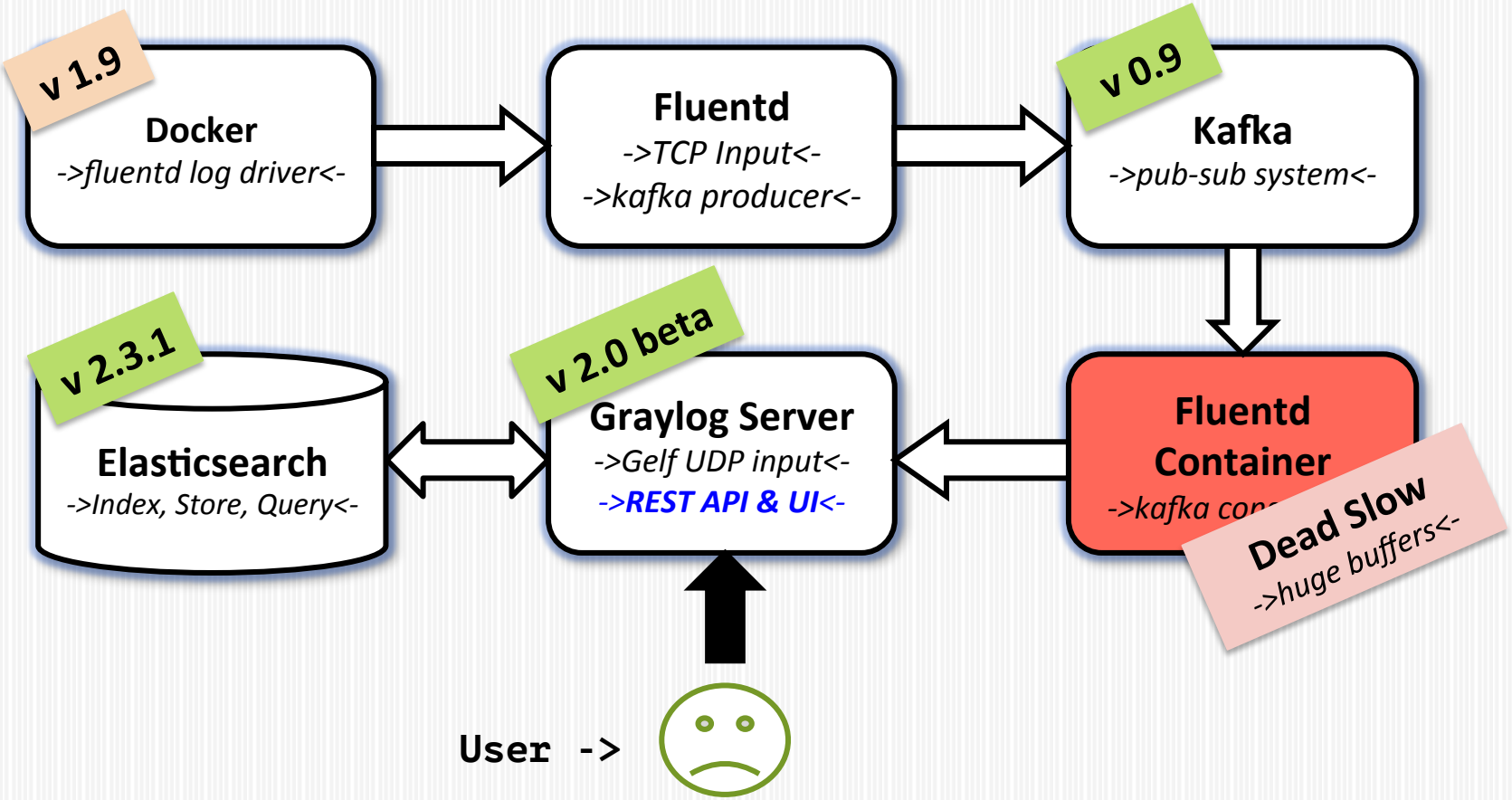


#1: Initial Pipeline



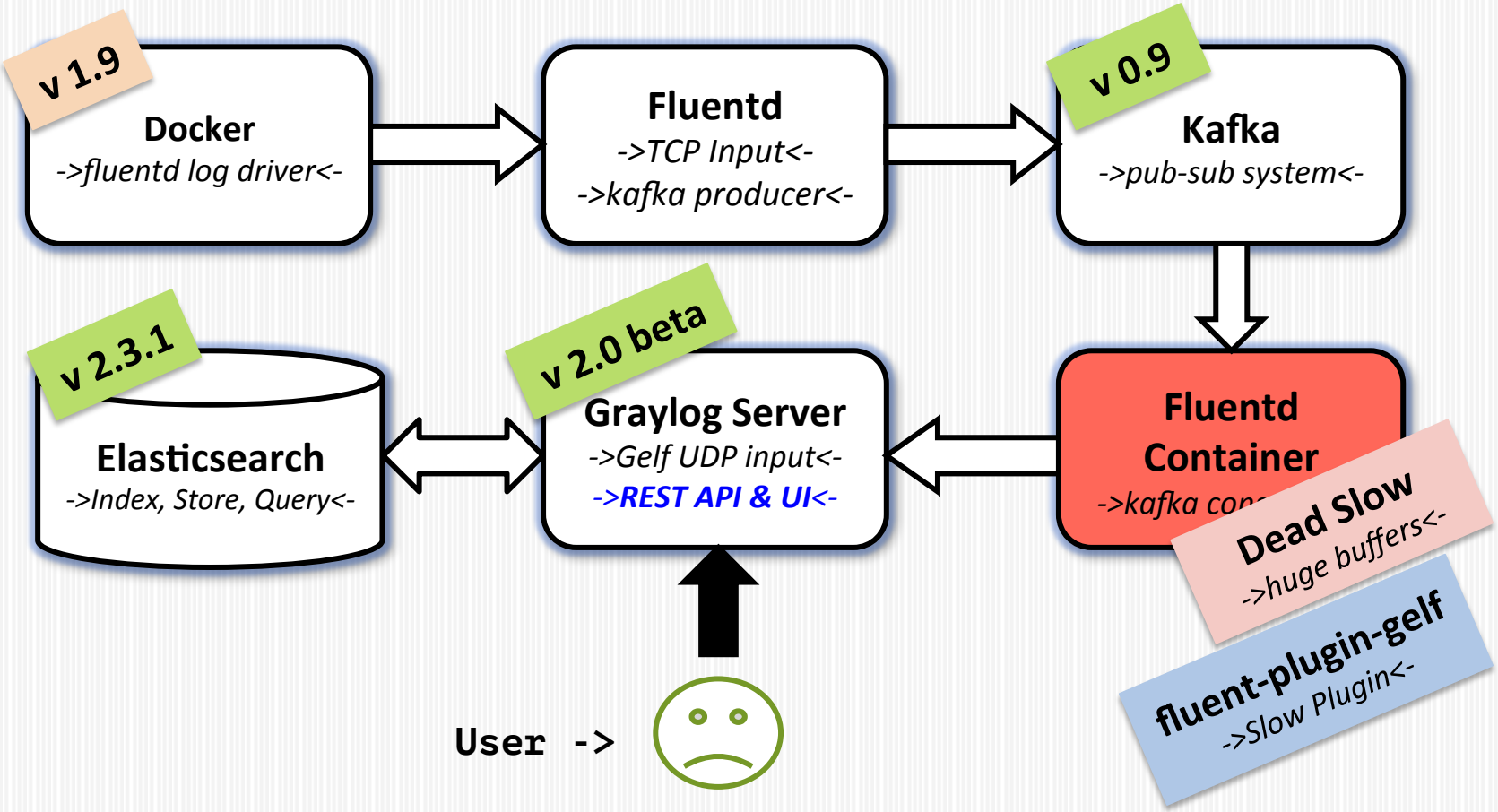
Huge lag for app logs in Graylog UI

#1: Initial Pipeline



Huge lag for app logs in Graylog UI

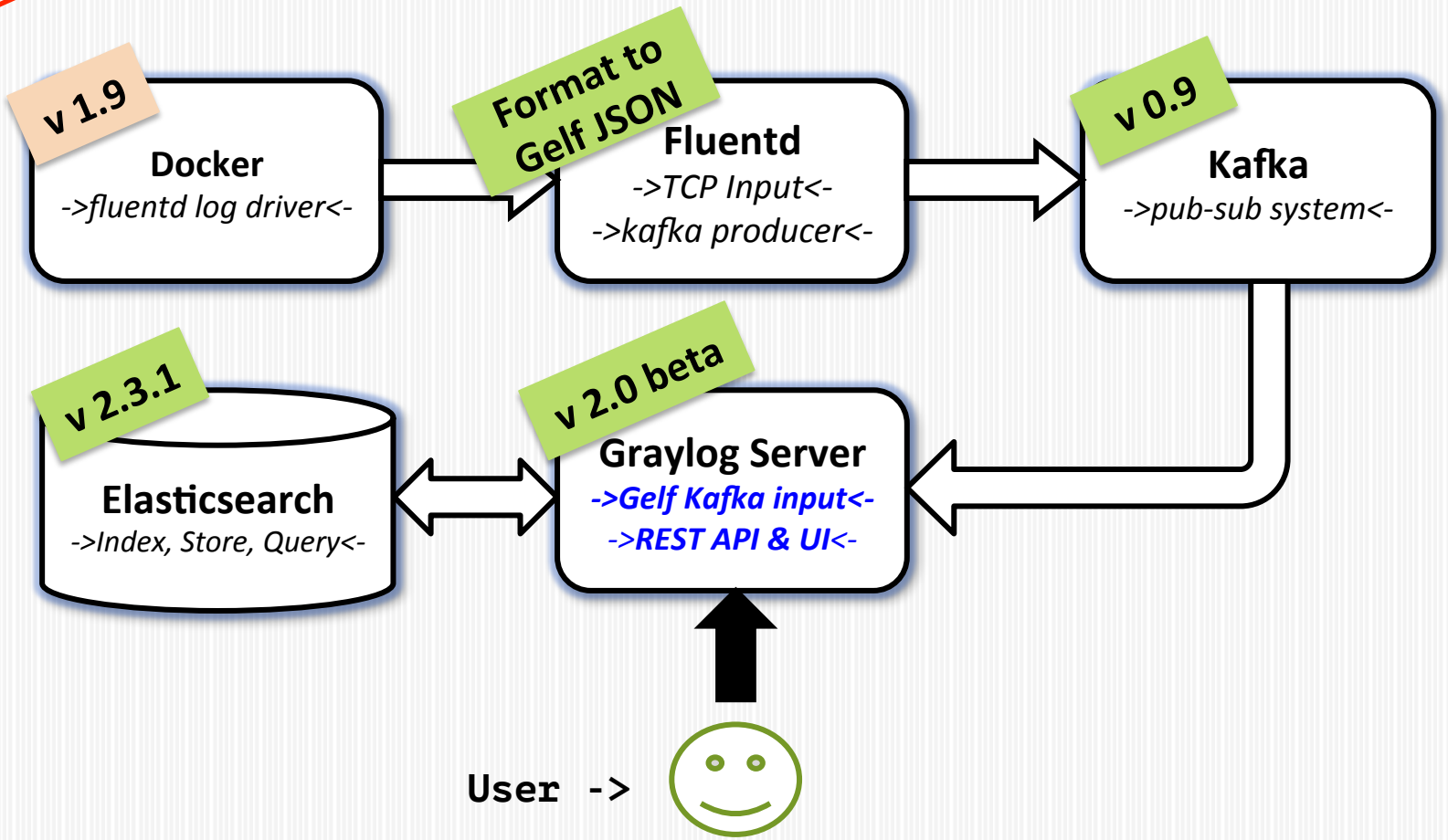
#1: Initial Pipeline



Huge lag for app logs in Graylog UI

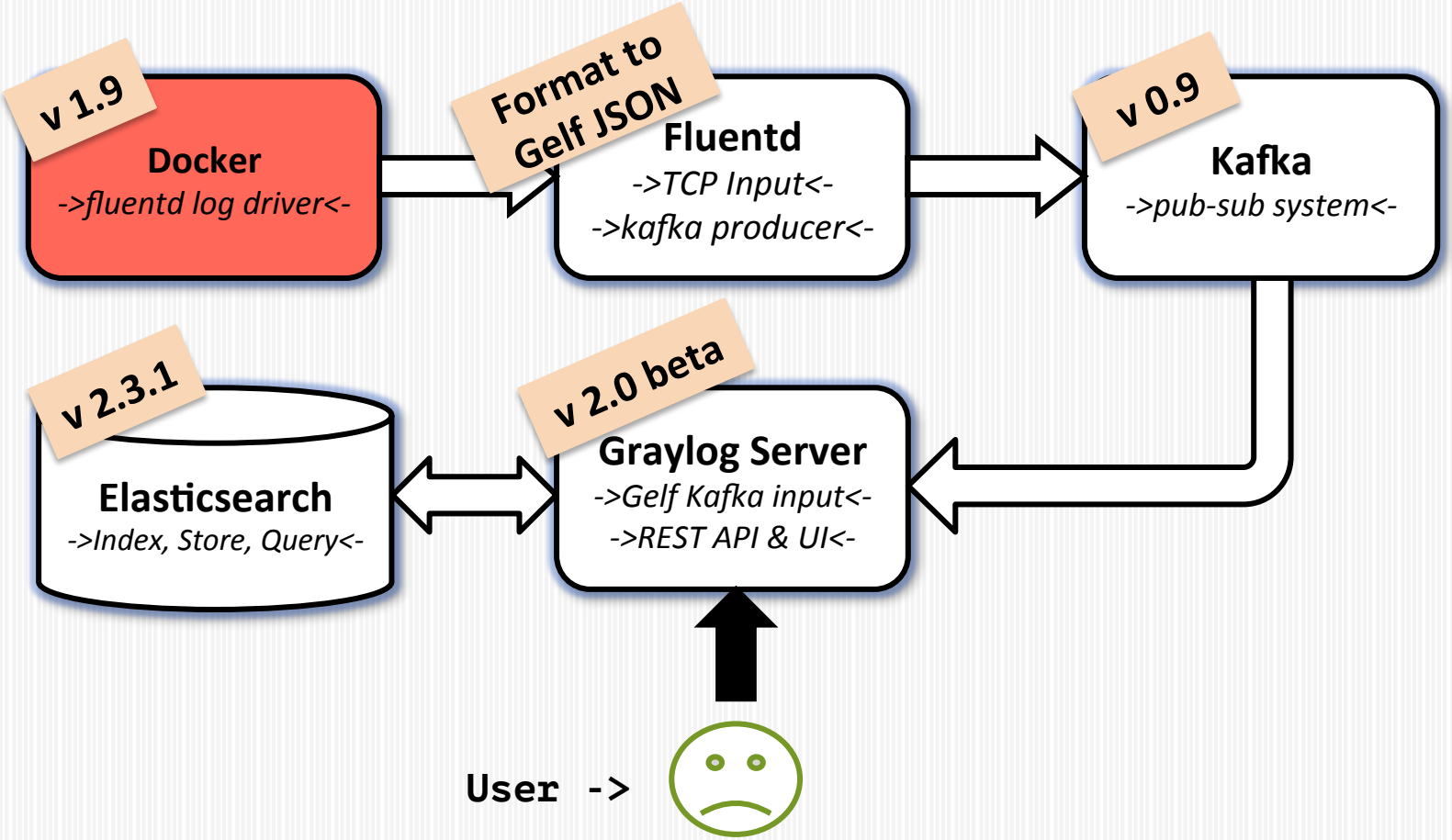
CASE SOLVED

#1: Initial Pipeline

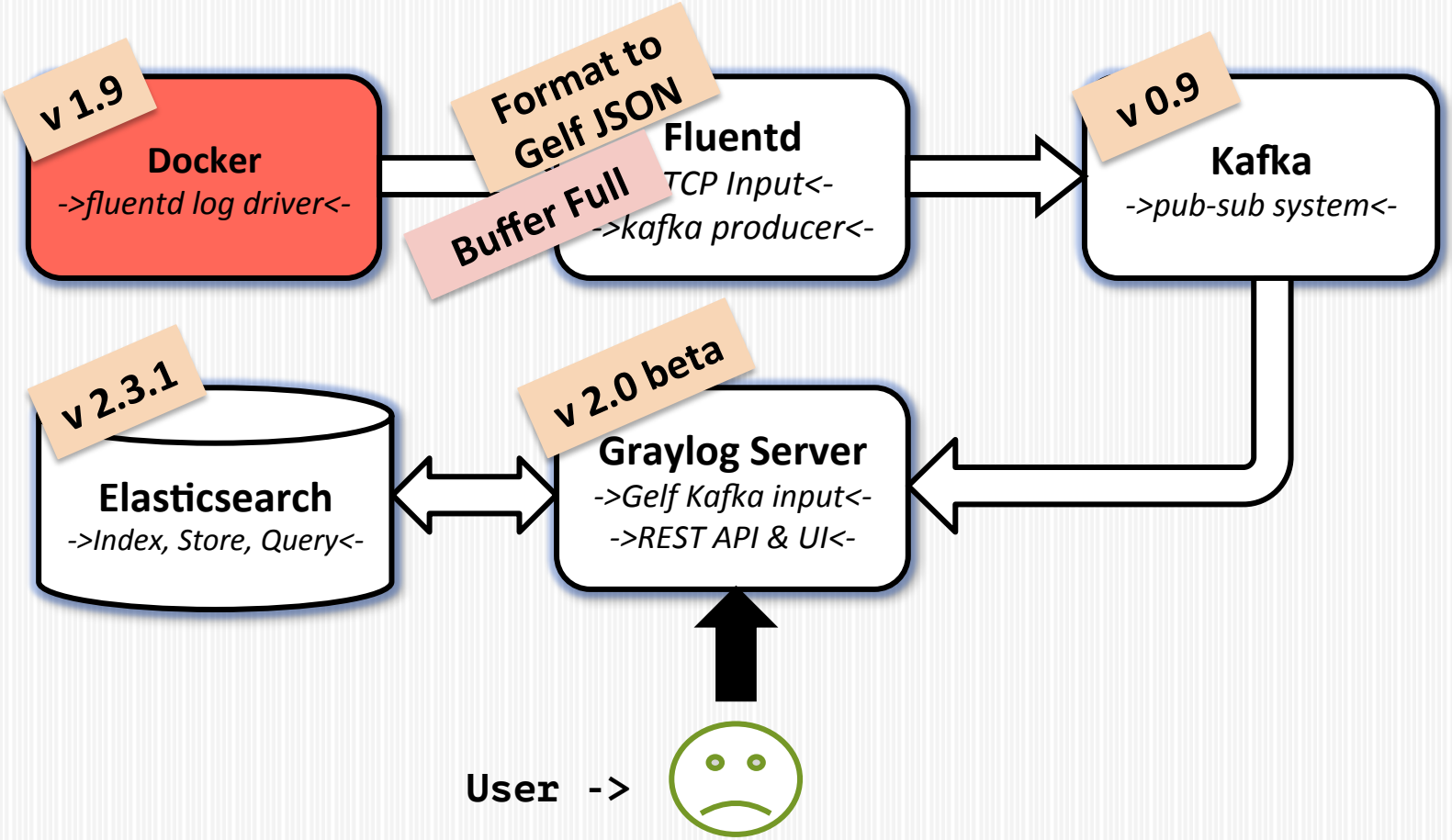


~~Huge lag for~~ app logs in Graylog UI

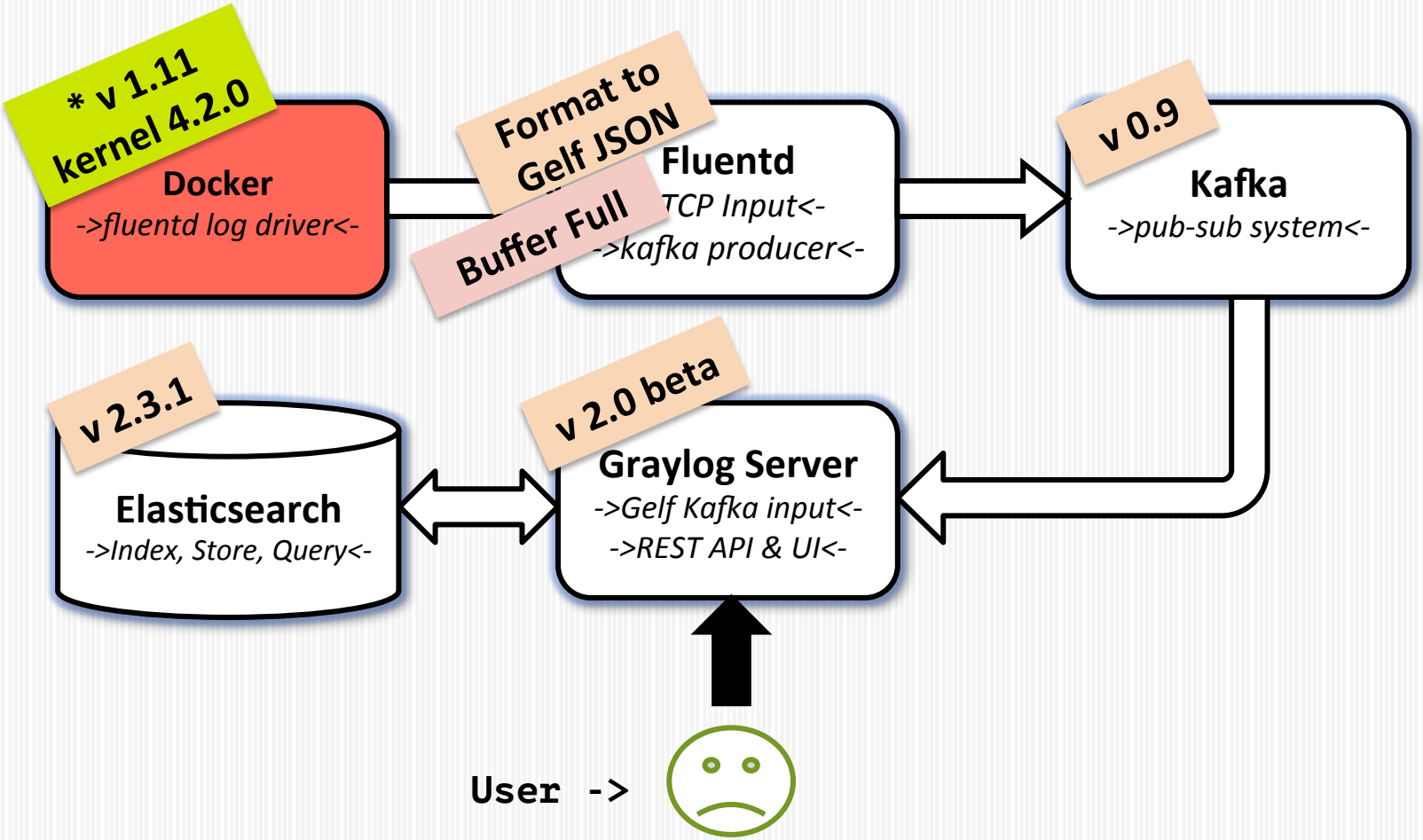
#2: Docker Service Crash



#2: Docker Service Crash

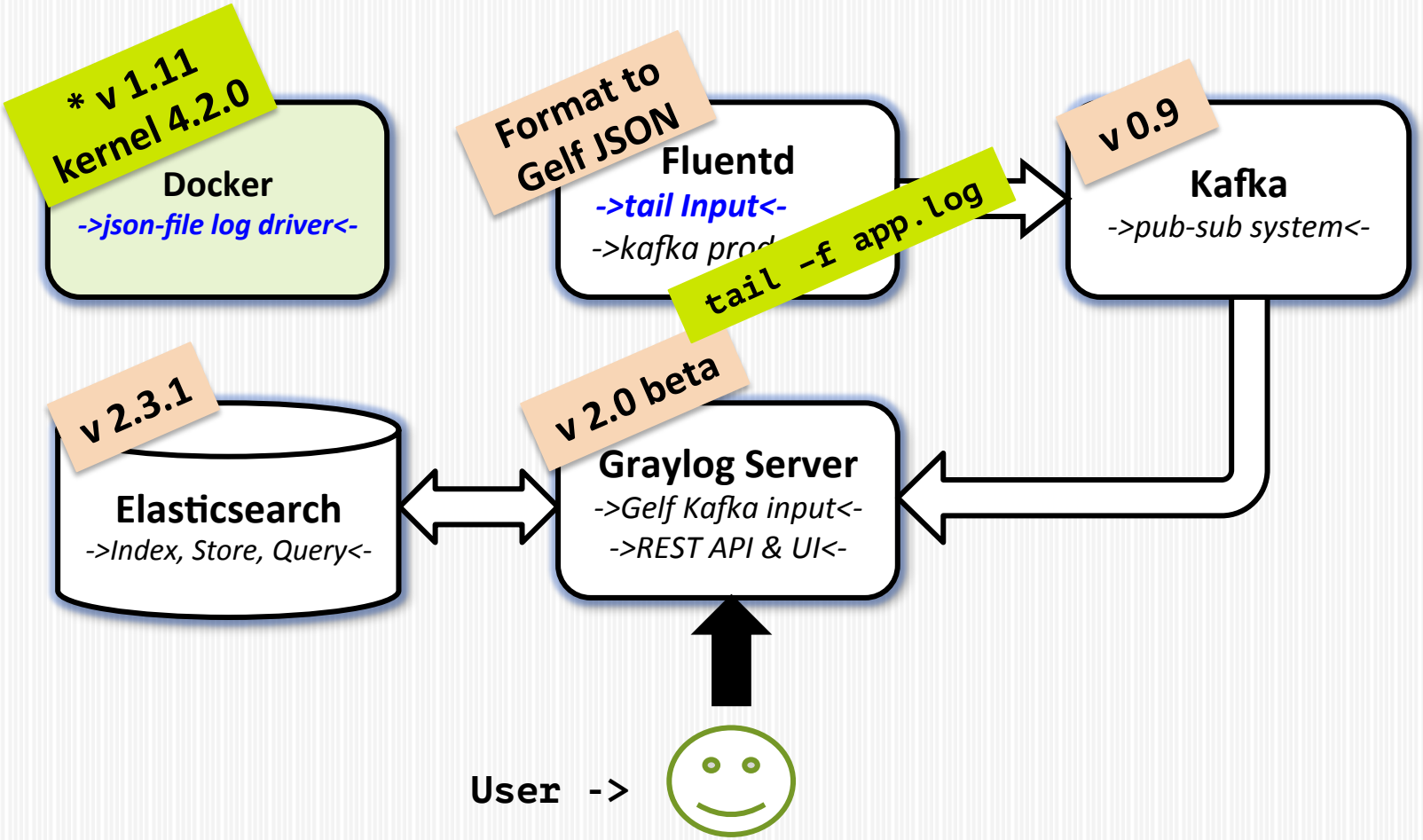


#2: Docker Service Crash



*** Docker should not crash due to log-driver**

#2: Docker Service Crash

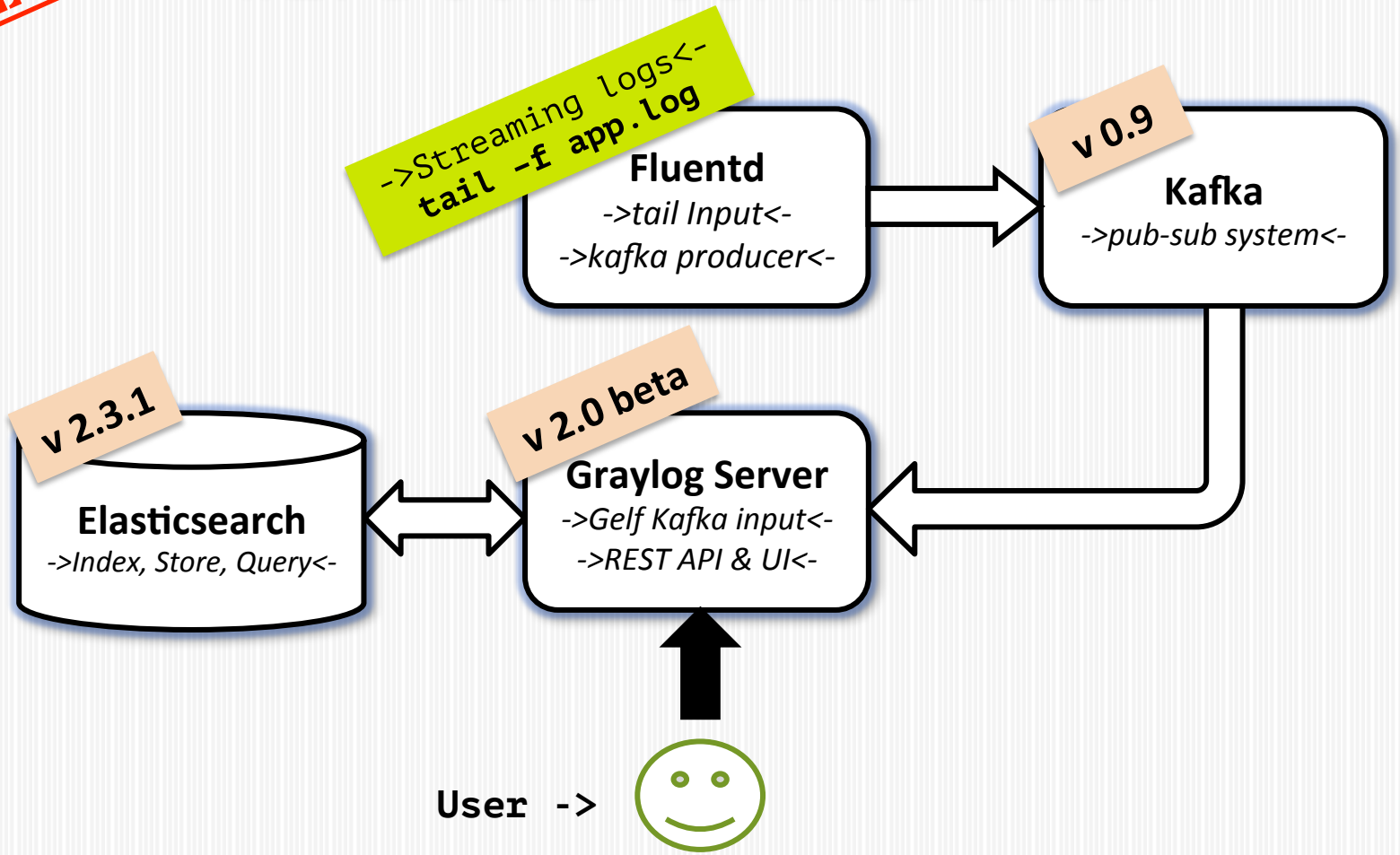


*** Docker should not crash due to log-driver**

Use default docker logging driver: json-driver

CASE SOLVED

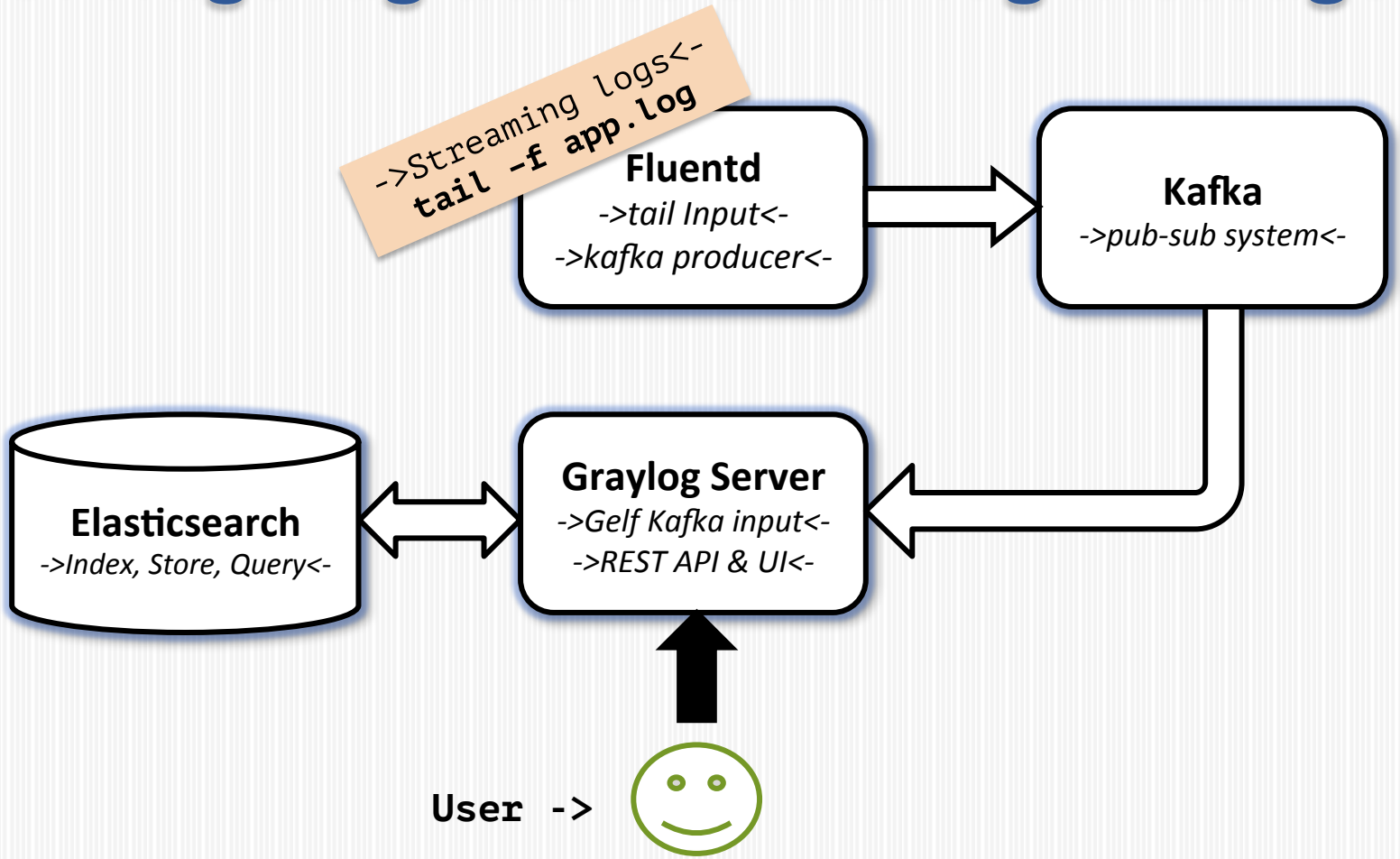
#2: Docker Service Crash



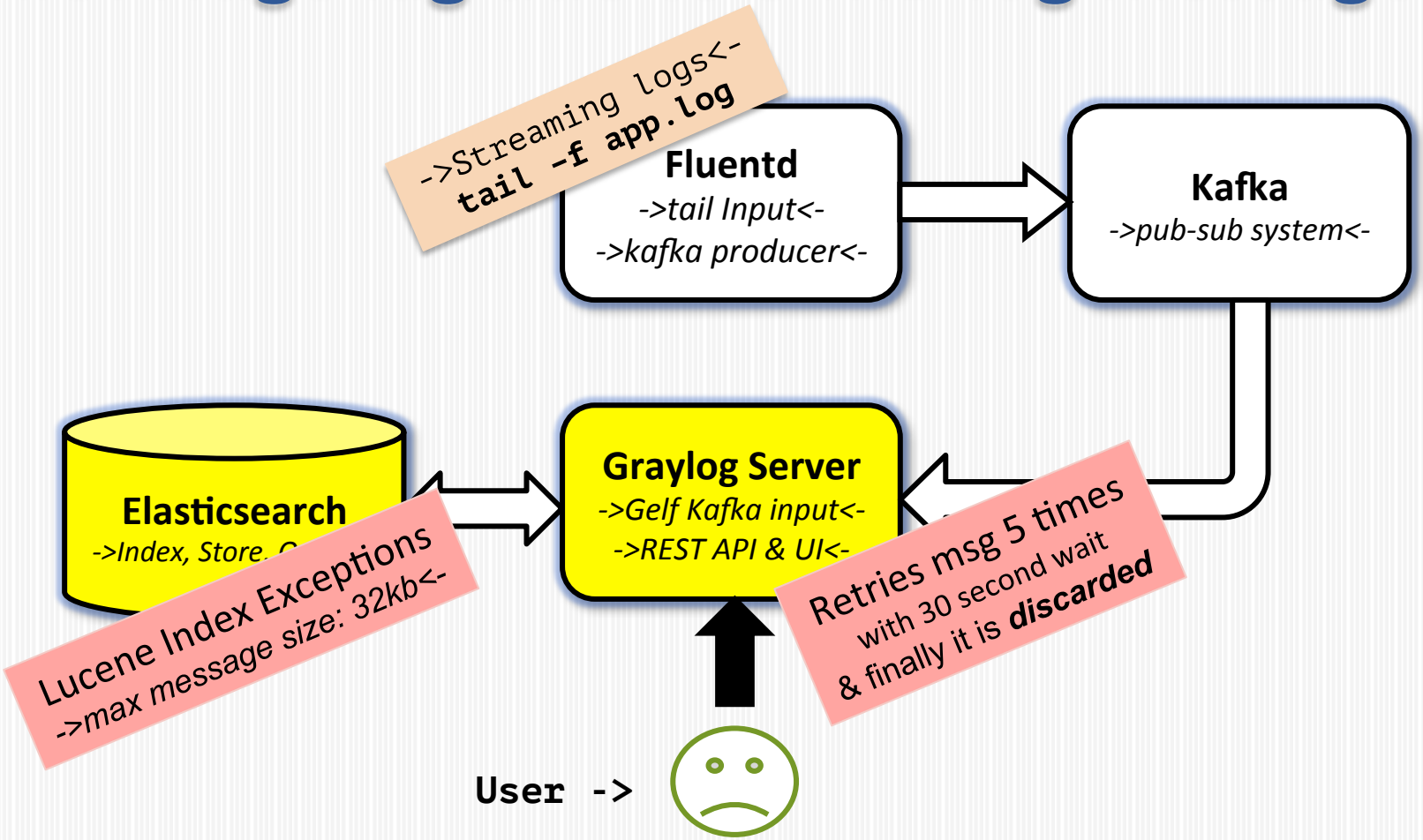
*** Docker should not crash due to log-driver**

Use default docker logging driver: json-driver

#3: Huge lag due to 3 MB log messages



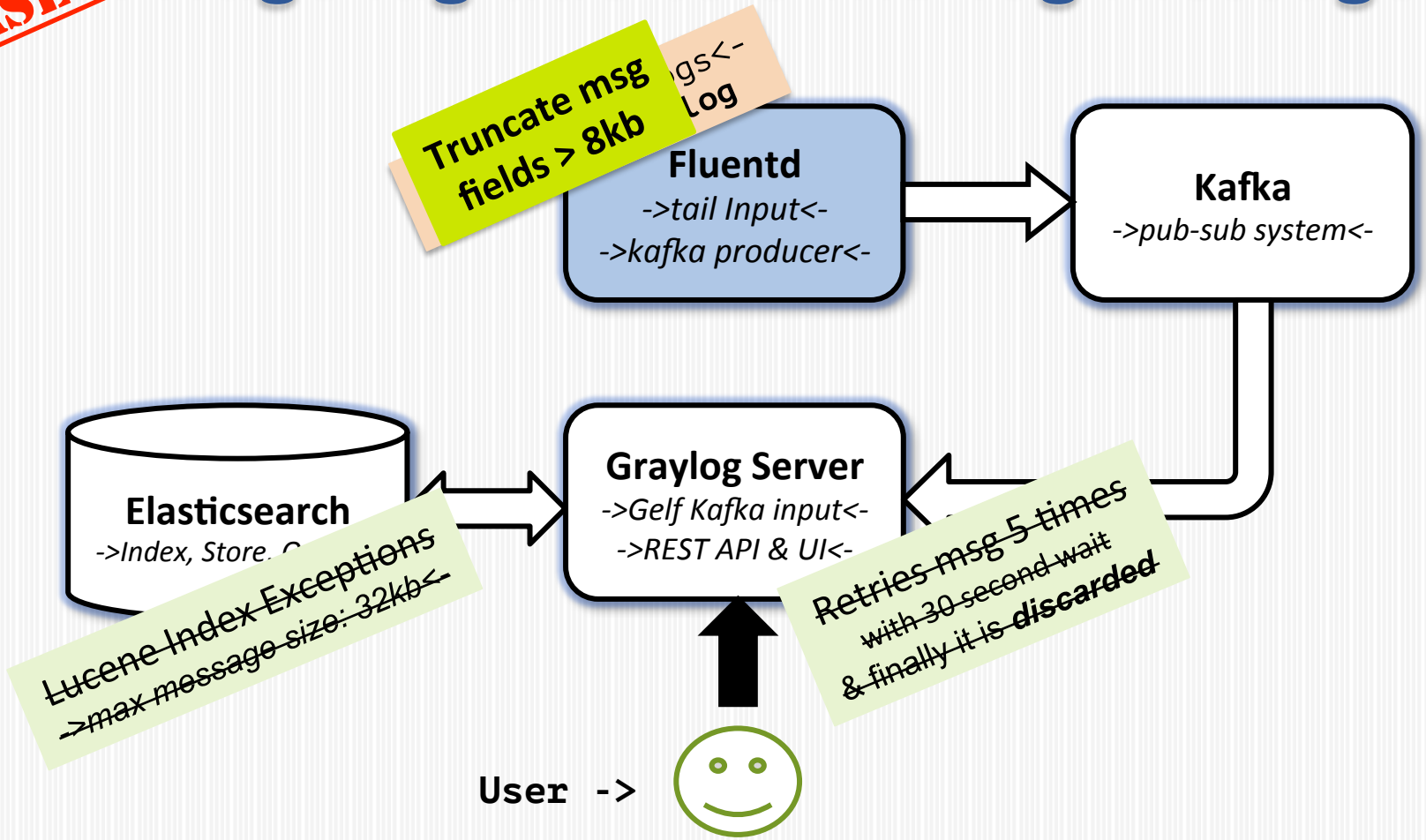
#3: Huge lag due to 3 MB log messages



Unable to index huge log messages!

#3. Huge lag due to 3 MB log messages

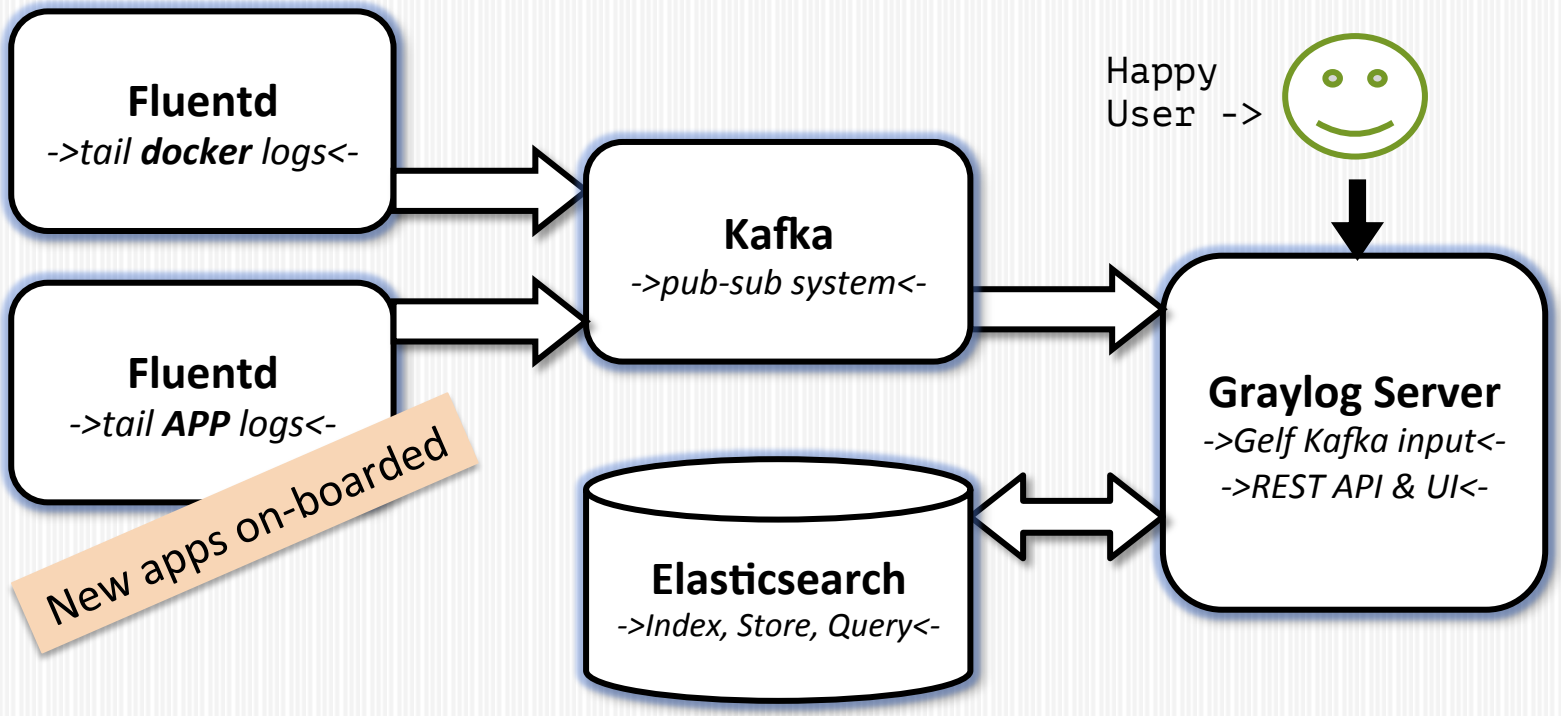
CASE SOLVED



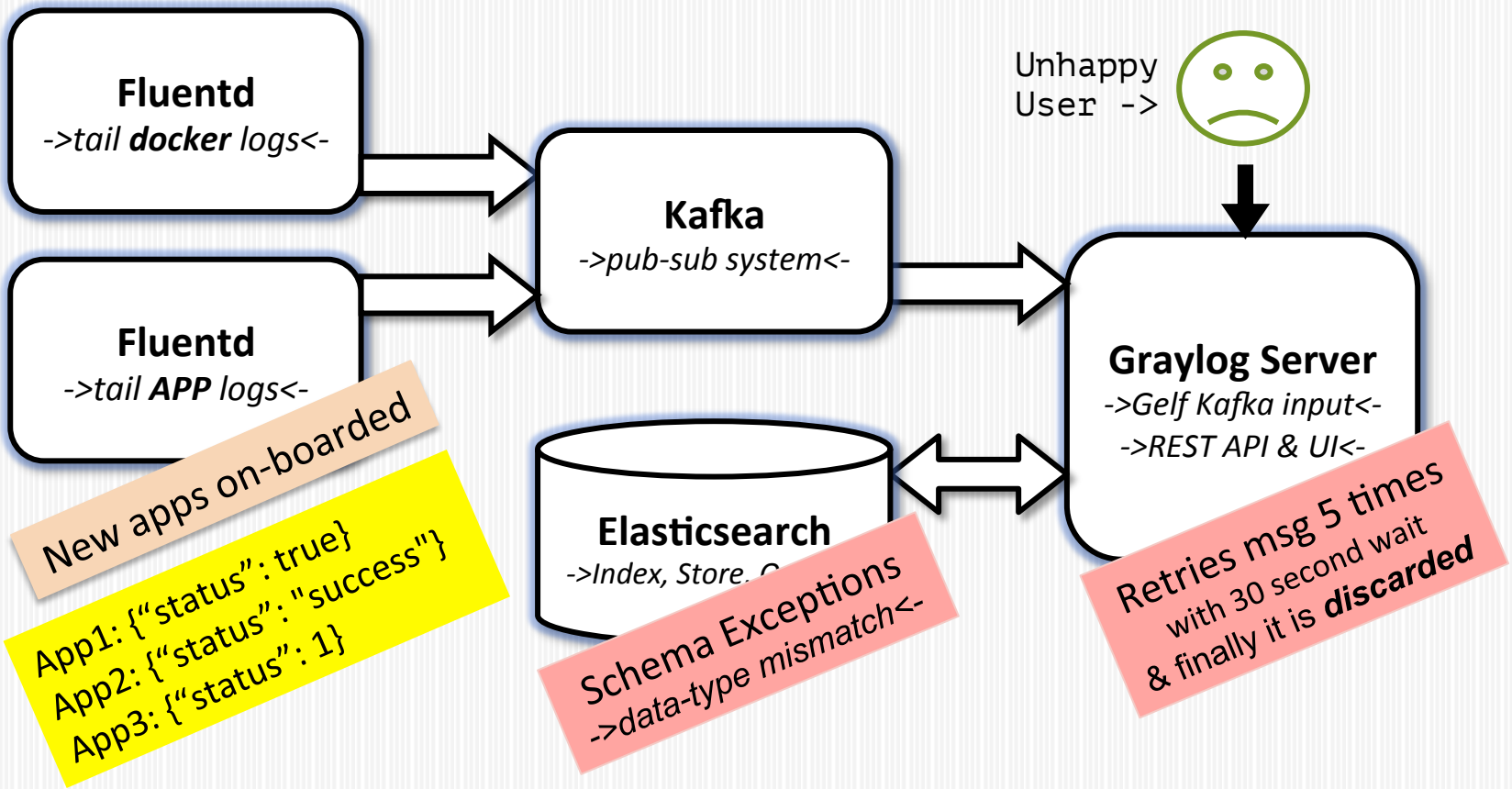
~~Unable to index huge log messages!~~

Able to index small log messages!

#4: Inconsistent schema problem



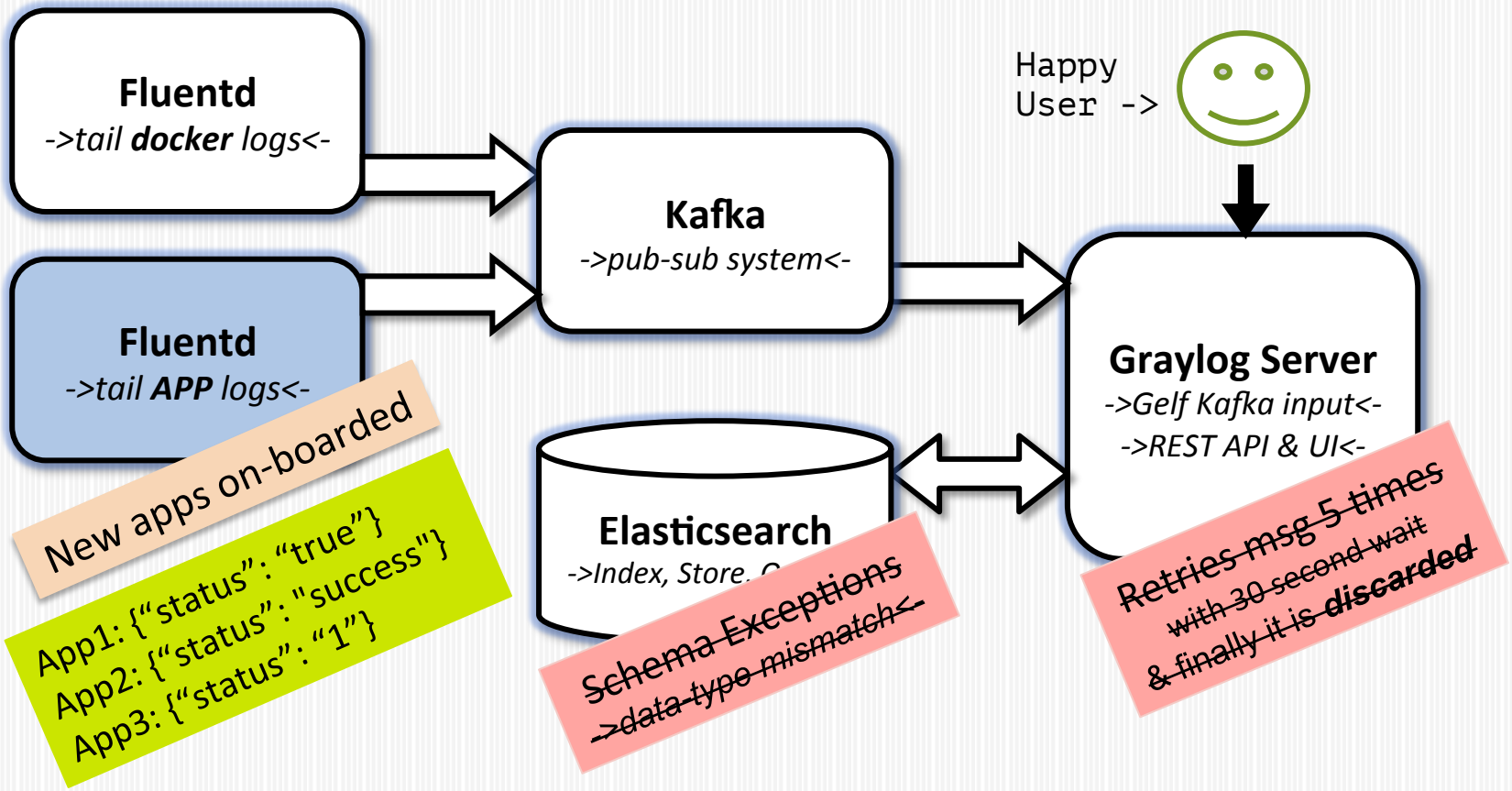
#4: Inconsistent schema problem



Elasticsearch maps field data-type for every key!

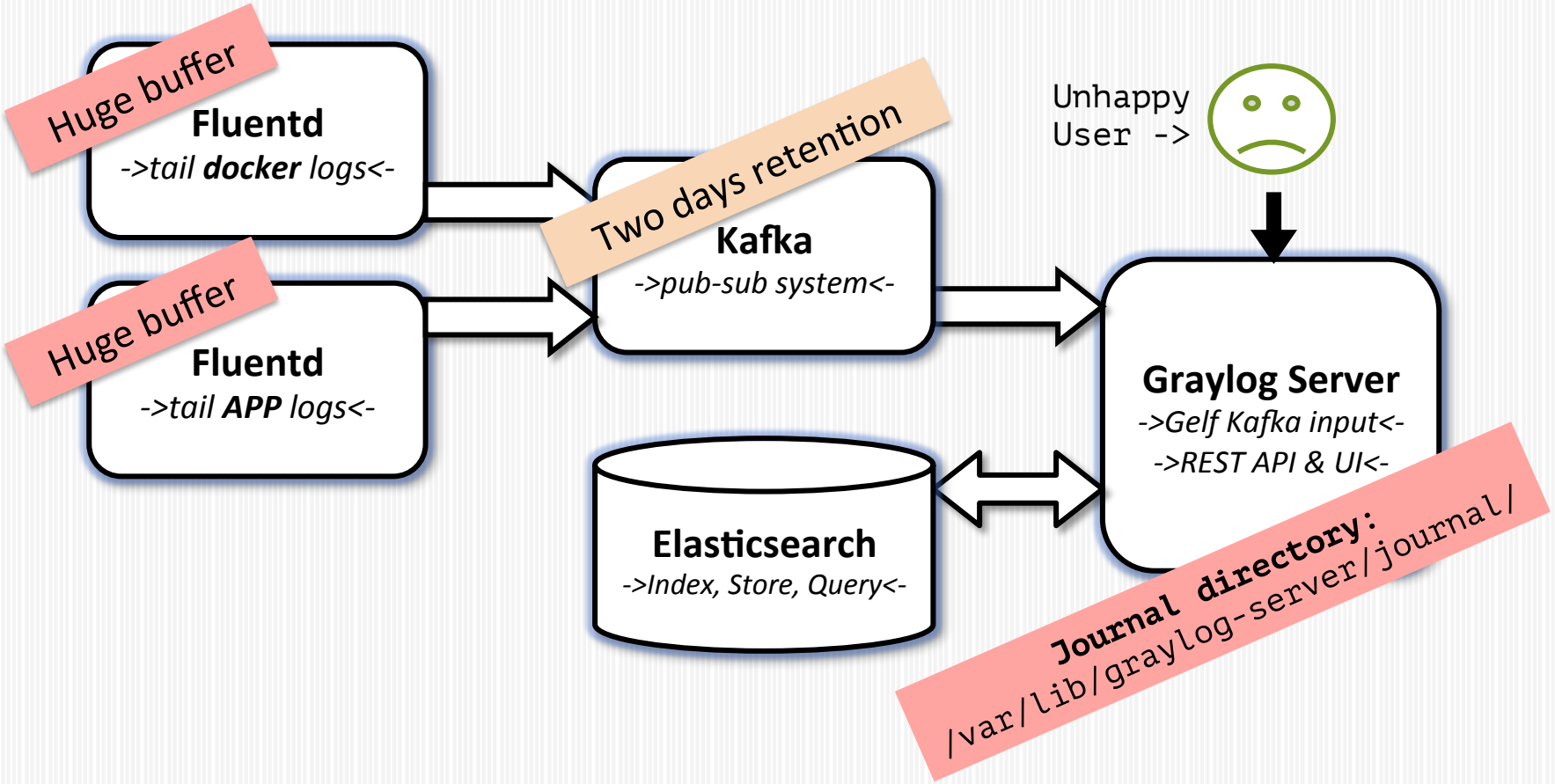
#4: Inconsistent schema problem

CASE SOLVED



Elasticsearch maps field data-type for every key!

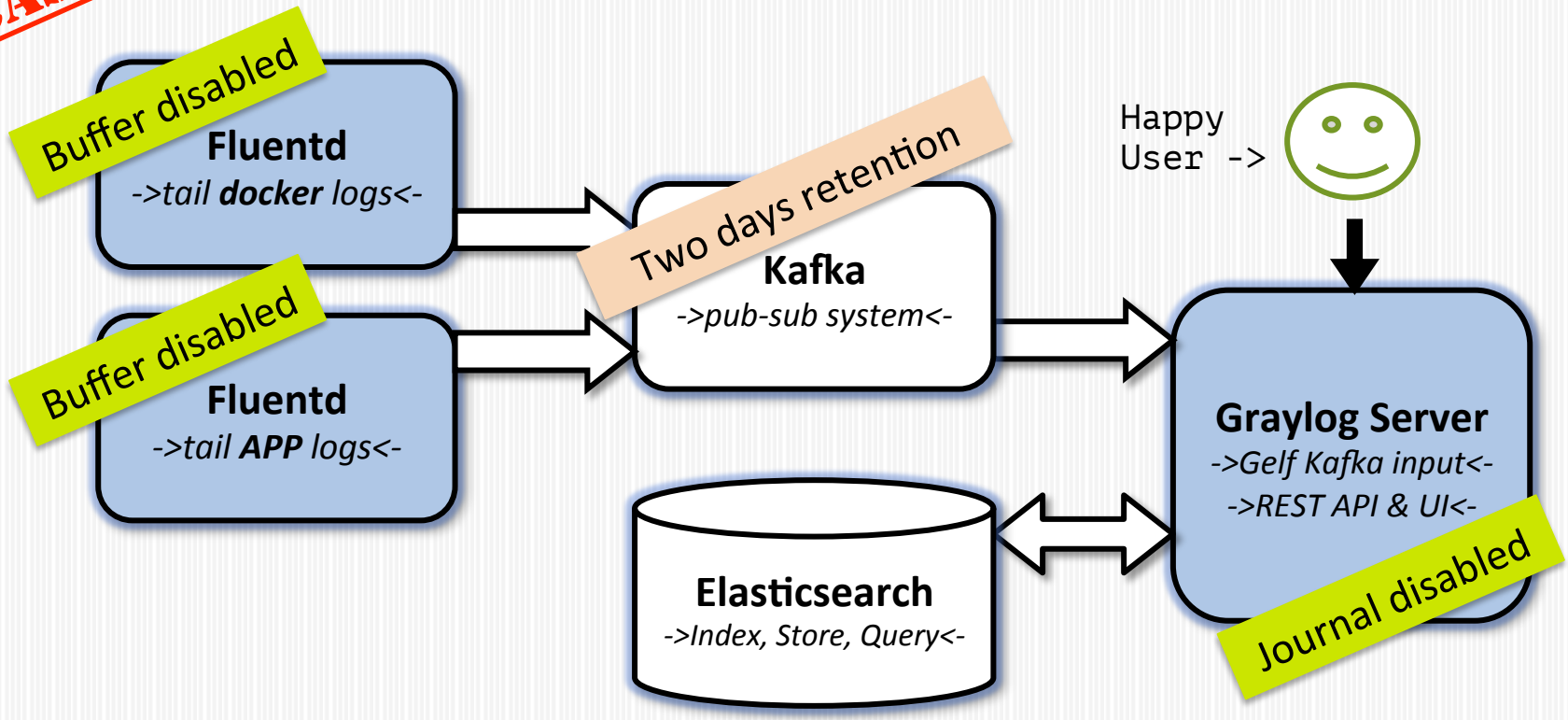
#5: Journal/Buffer utilization too high



Q. Are buffers at each level necessary?

#5. Journal/Buffer utilization too high

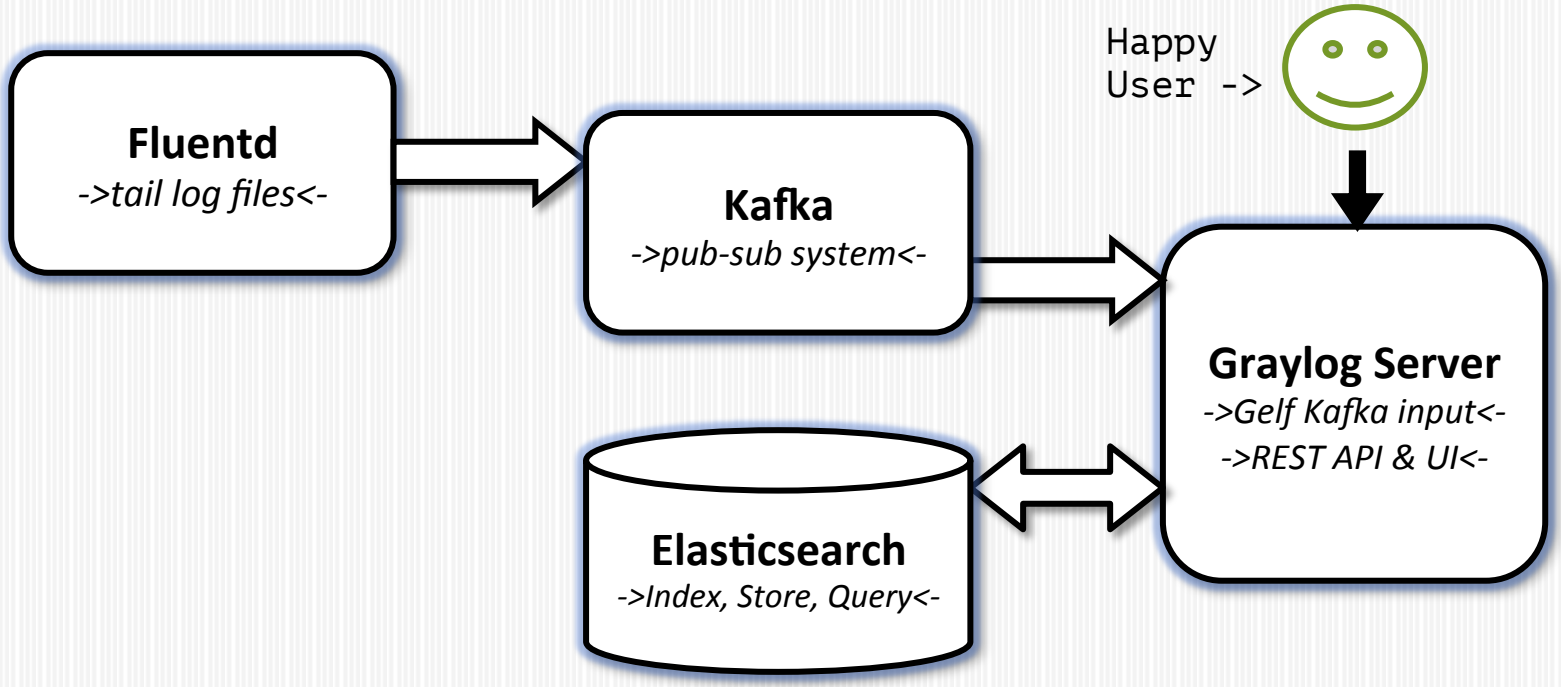
CASE SOLVED



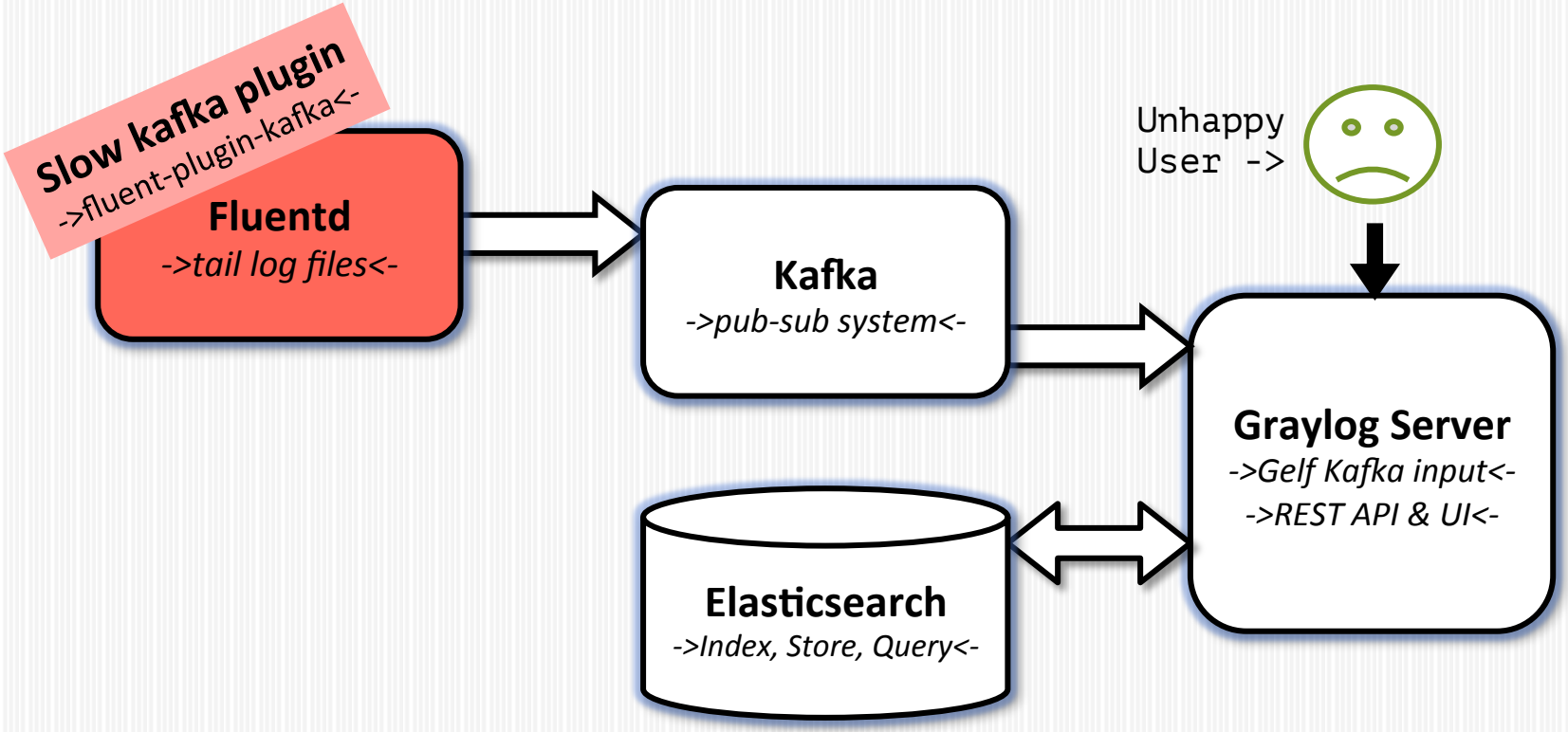
Q. Are buffers at each level necessary?

Ans. No. Log files & Kafka retention is enough.

#6: Missing/delayed docker logs



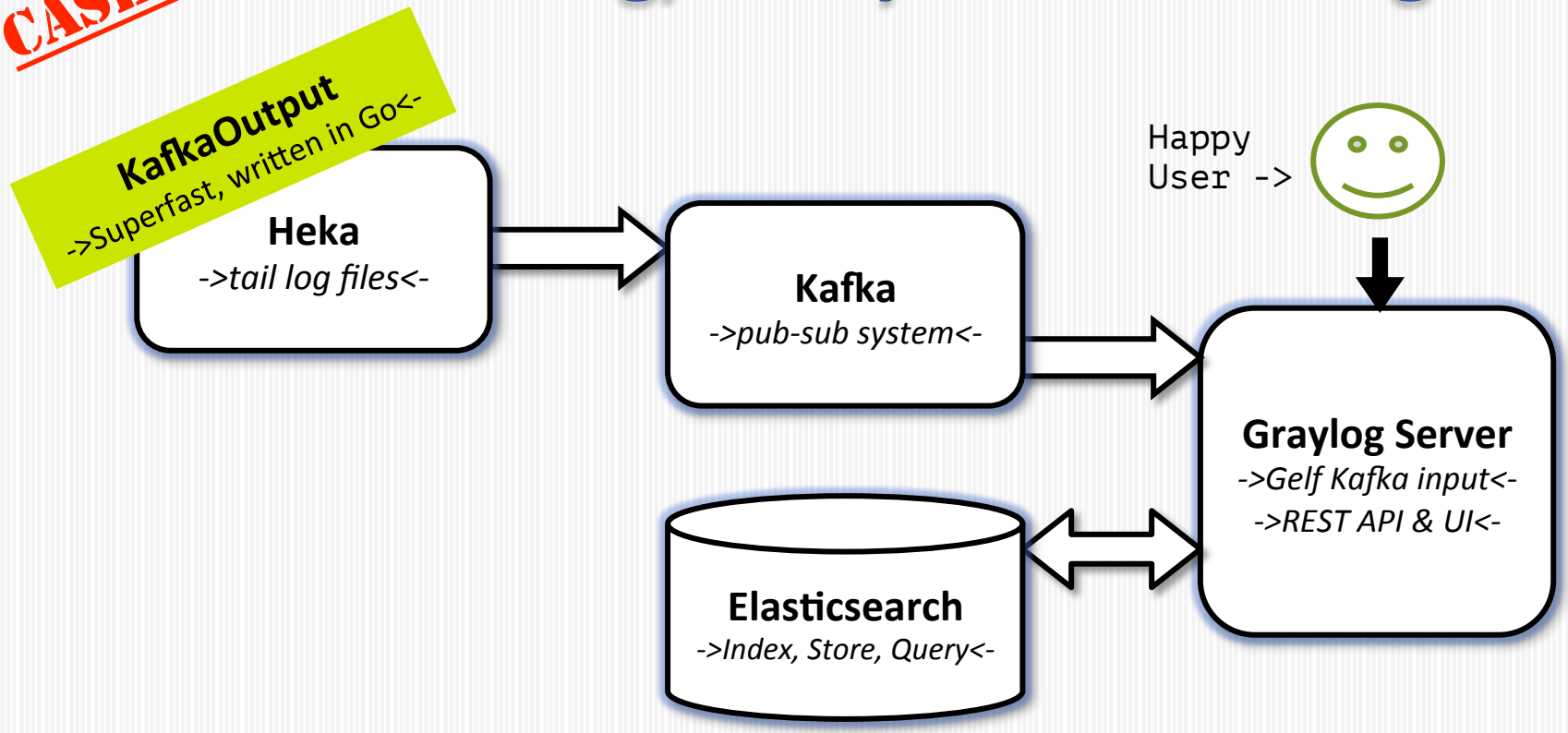
#6: Missing/delayed docker logs



Slow plugin, adding CPU/RAM did not help!

#6: Missing/delayed docker logs

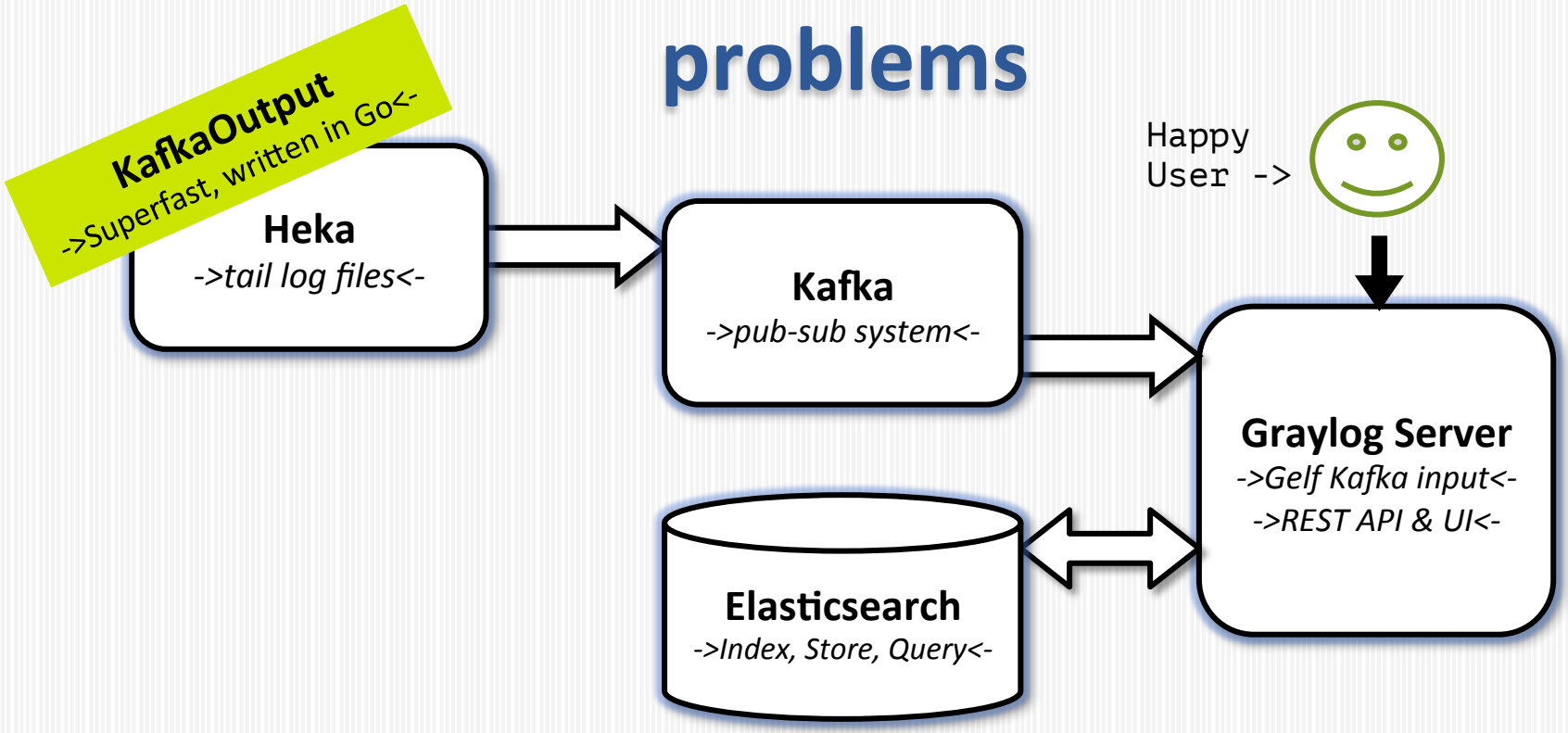
CASE SOLVED



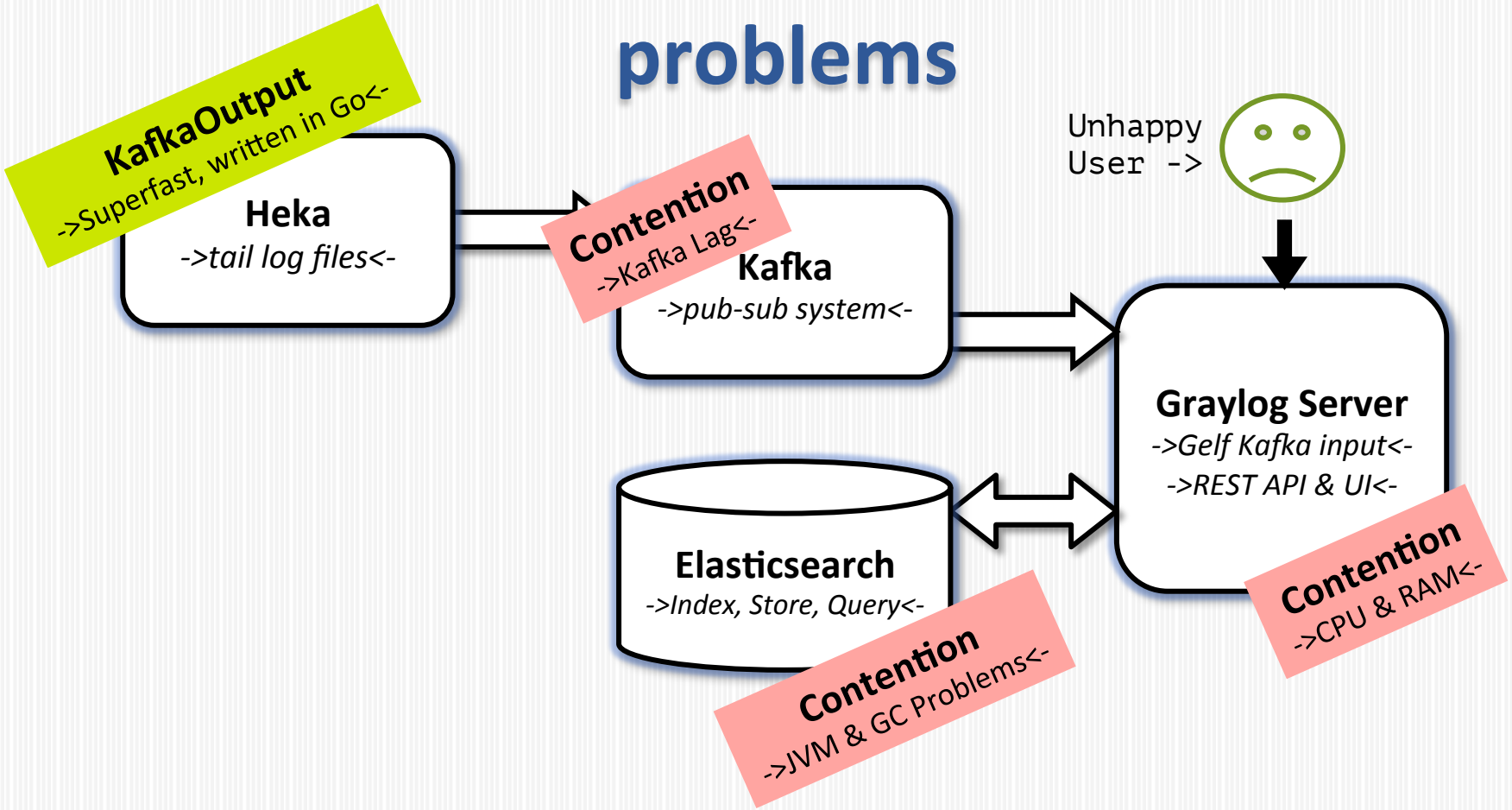
Fluentd vs. Heka

Written in Ruby	Written in Go (10x CPU, 5x mem friendly)
Easy & very good plugin ecosystem	Learning curve, few community plugins
Simple configuration	Feature rich configuration

#7: Centralized solution, Centralized problems

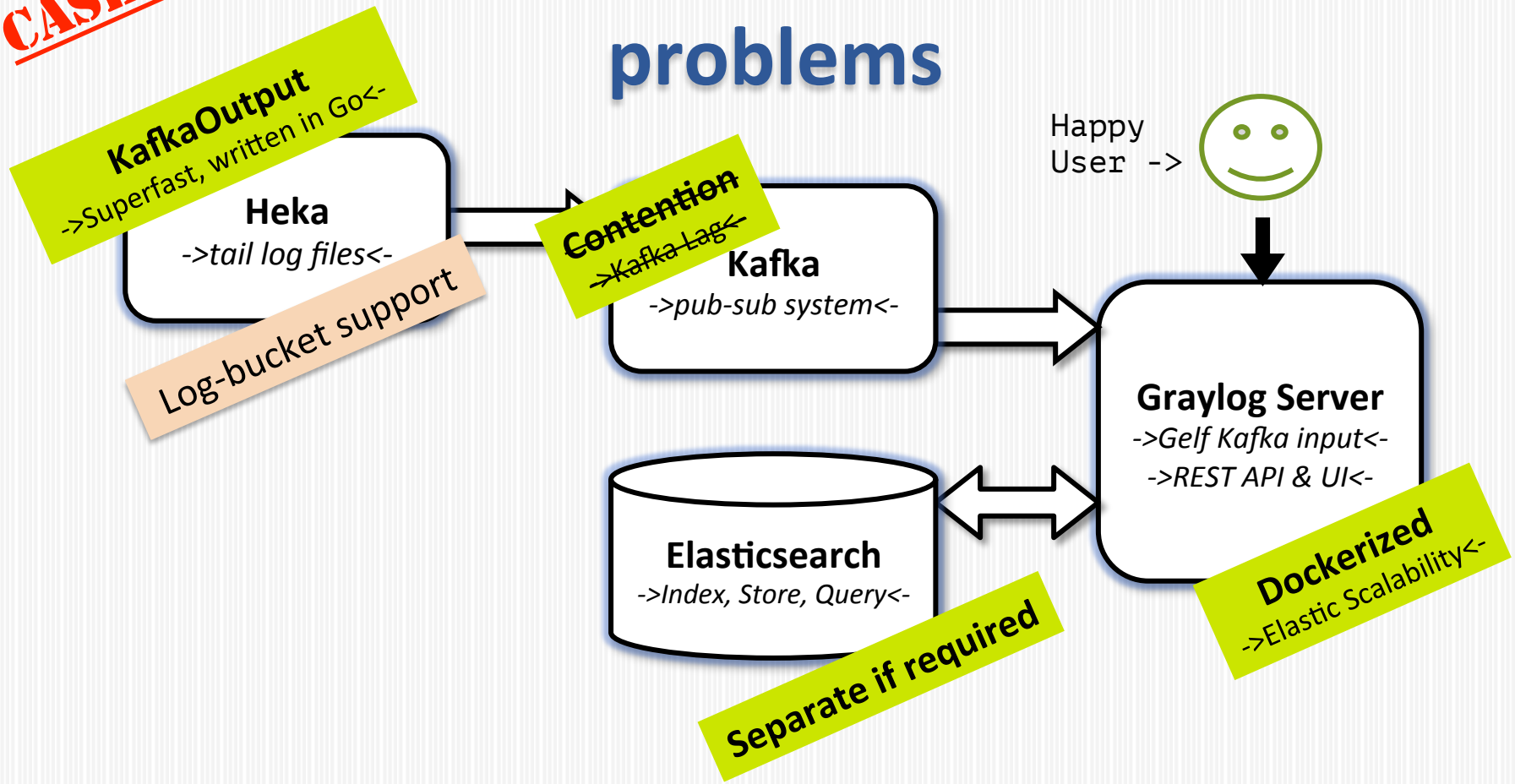


#7: Centralized solution, Centralized problems



#7: Centralized solution, Decentralized problems

CASE SOLVED



Logs are sent to different kafka topics based on log-bucket

Mesos + docker provides elastic scaling for Graylog

Who likes it?

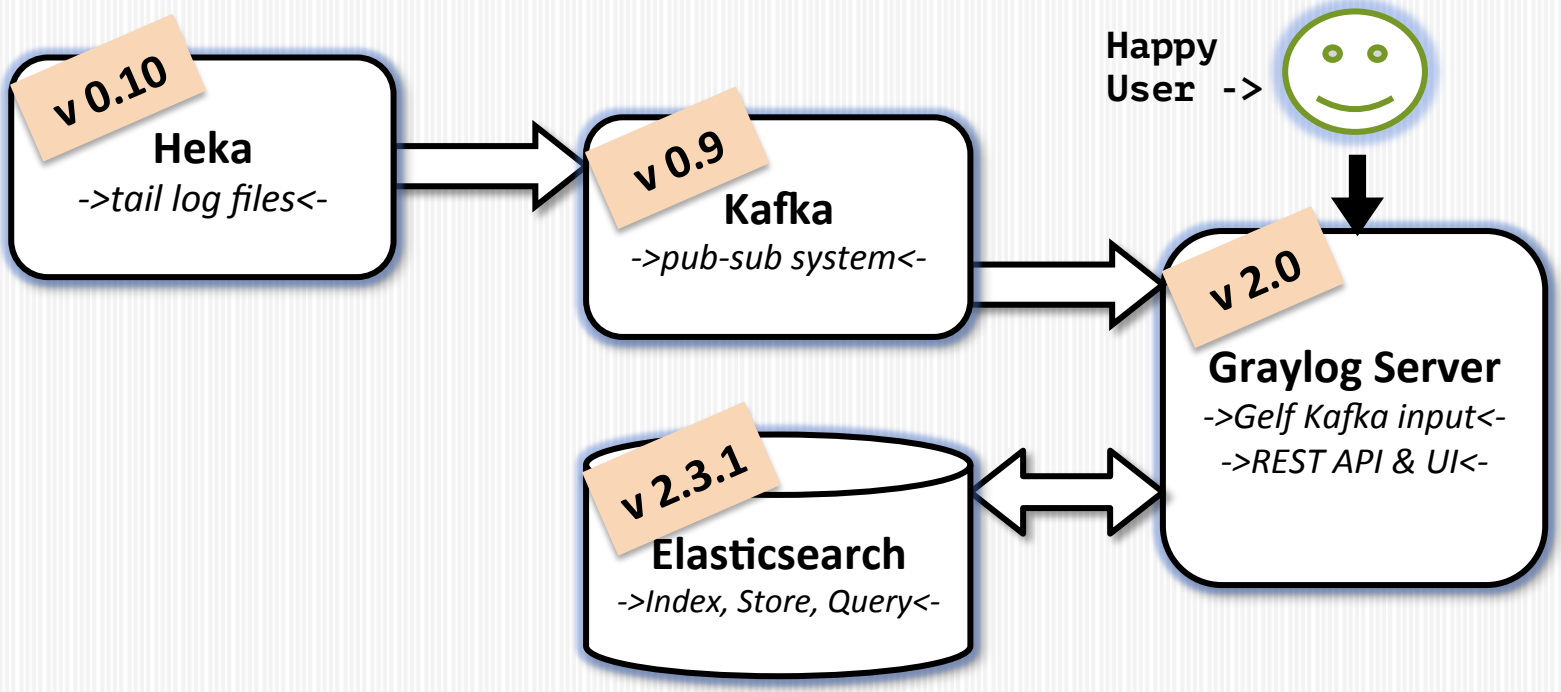
- **Developers:** Quick RCAs
- **Devops:** More time to sleep
- **Management:** Lovely dashboards

Try it yourself

```
# docker run -d --name elasticsearch elasticsearch
# docker run -d --name mongo mongo
# docker run -p 9000:9000 -d \
        --name graylog \
        --link mongo:mongo \
        --link elasticsearch:elasticsearch \
        -e GRAYLOG_PASSWORD=admin \
        rohit01/graylog
```

Now open: http://localhost:9000 (admin/admin)

Questions?



Thank You!