CNCon / KubeCon China 2019

Fluentd Project Intro

CLOUD NATIVE
COMPUTING FOUNDATION

Masahiro Nakagawa
Senior Software Engineer

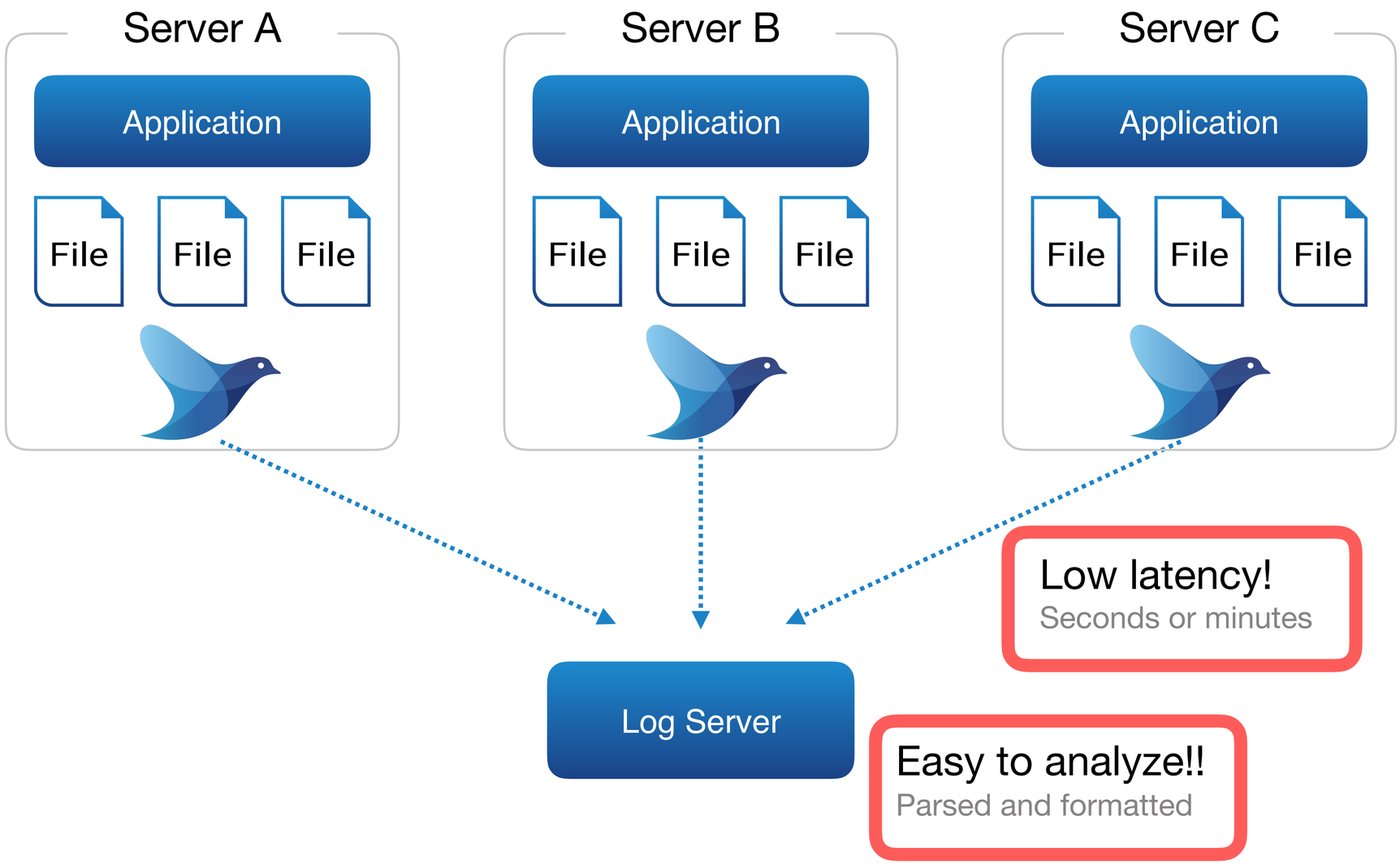
arm
TREASURE DATA

Fluentd Overview

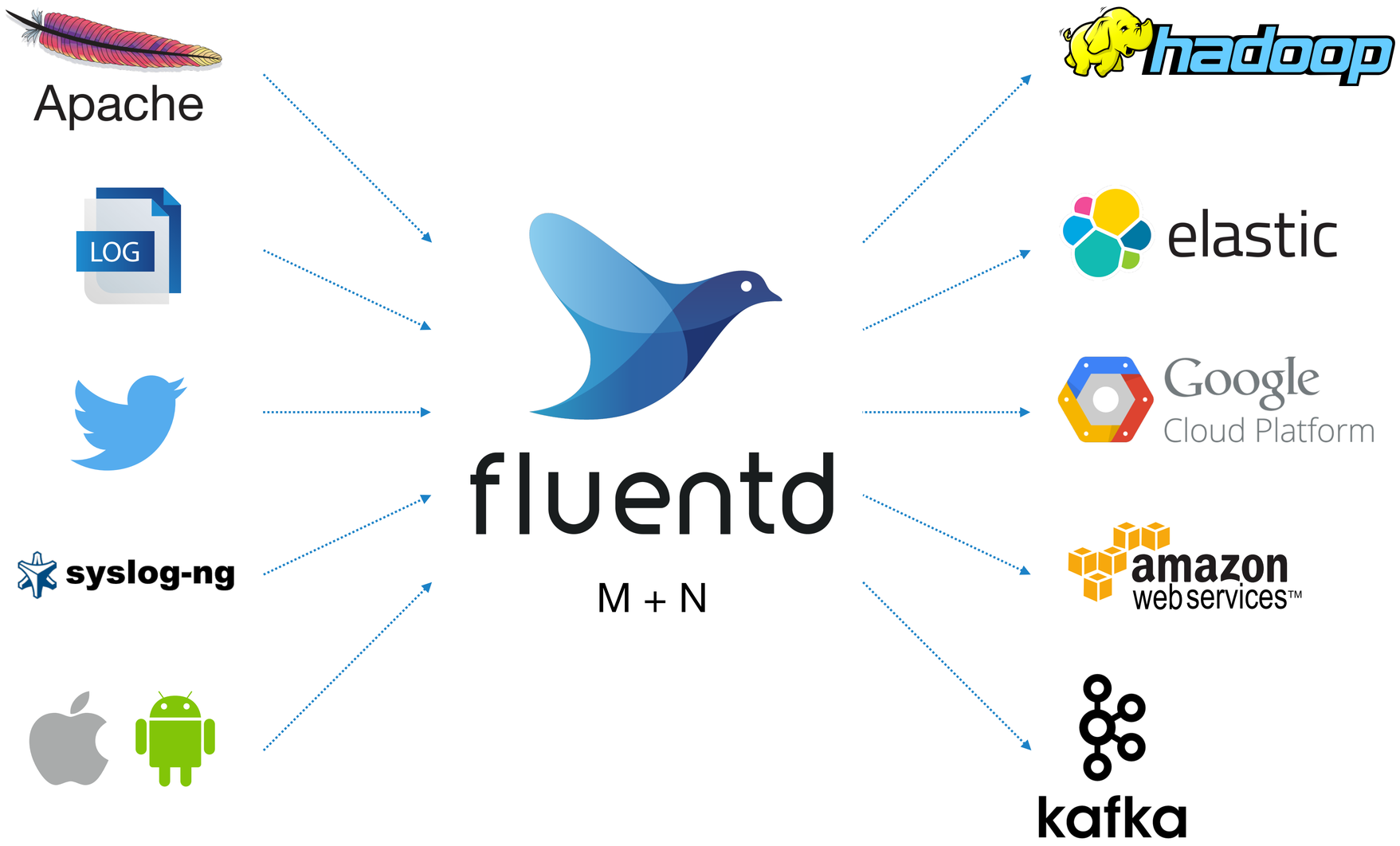
What’s Fluentd

- Streaming data collector for unified logging
  - Core + Plugins
- RubyGems based various plugins
  - Follow Ruby’s standard way
- Several setup ways
  - https://docs.fluentd.org/installation
- Latest version: v1.5.2
- Logging part in CNCF and Graduated at 2019

Streaming way with Fluentd



Unified logging layer



Fluentd Architecture

Design

Core

- Buffering & Retrying
- Error handling
- Event routing
- Parallelism
- Helper for plugins

Plugins

- Read / receive data
- Parse data
- Filter / enrich data
- Buffer data
- Format data
- Write / send data

Event structure

Time

- Nano-second unit
- from logs

Tag

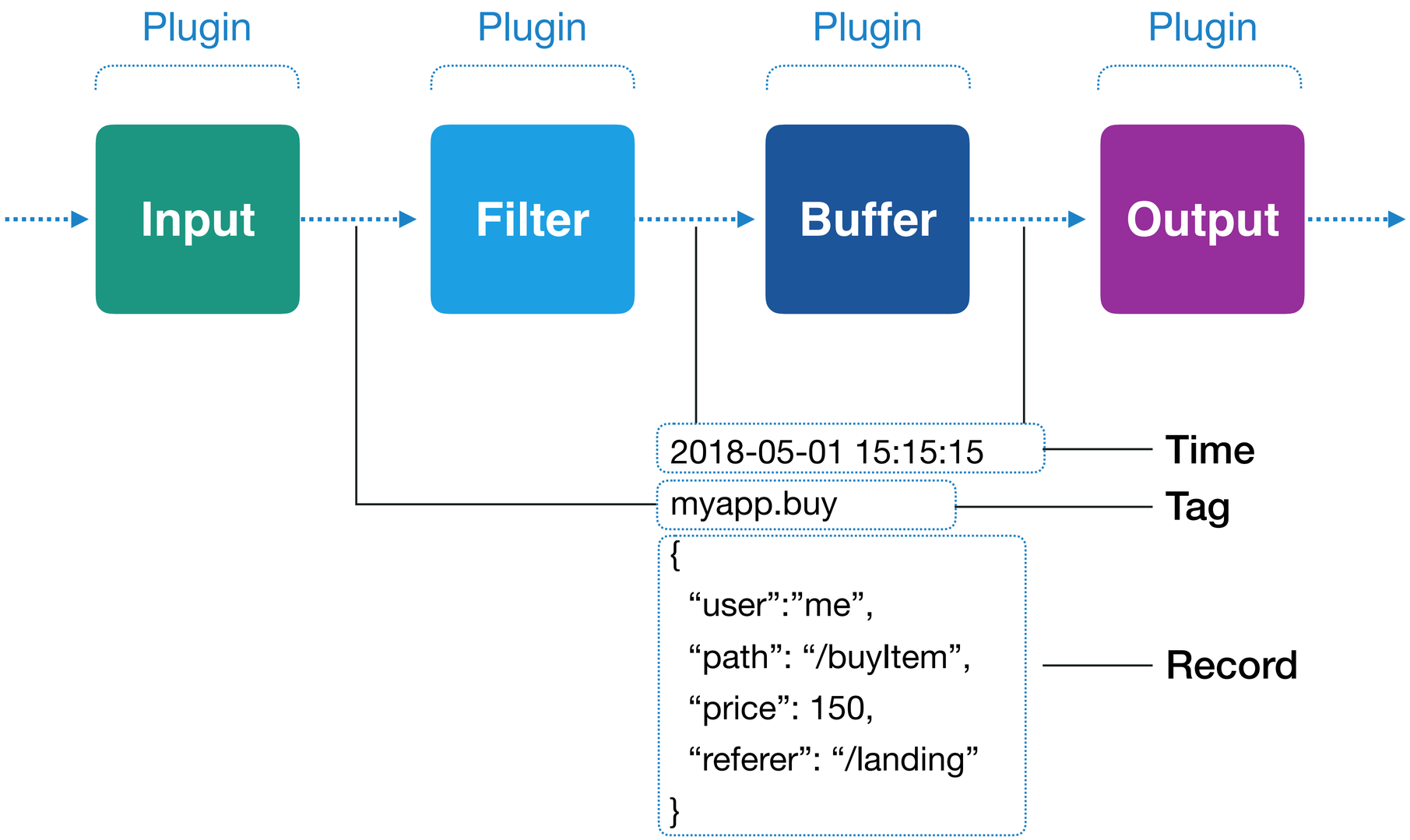
- for event routing
- Identify data source

Record

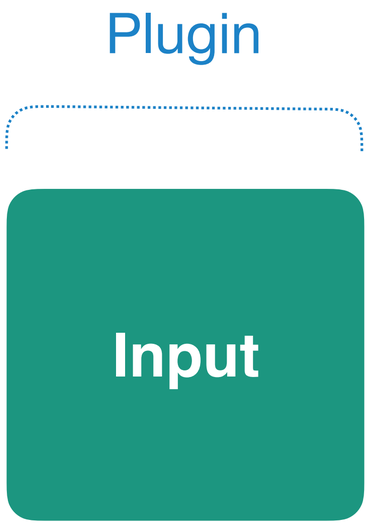
- JSON object,
  not raw string

```
{
  “str_field”:”hey”,
  “num_field”: 100,
  “bool_field”: true,
  “array_field”: [“elem1”, “elem2”]
}
```

Data pipeline (simplified)



Architecture: Input Plugins



- Receive or pull logs from data sources
- Emit logs to data pipeline
- Parse incoming logs for structured logging

HTTP+JSON (in_http)
Local files (in_tail)
Syslog (in_syslog)
…

Architecture: Filter Plugins

- Transform logs
- Filter out unnecessary logs
- Enrich logs

Modify logs (record_transformer)

Filter out logs (grep)

Parse field (parser)

…

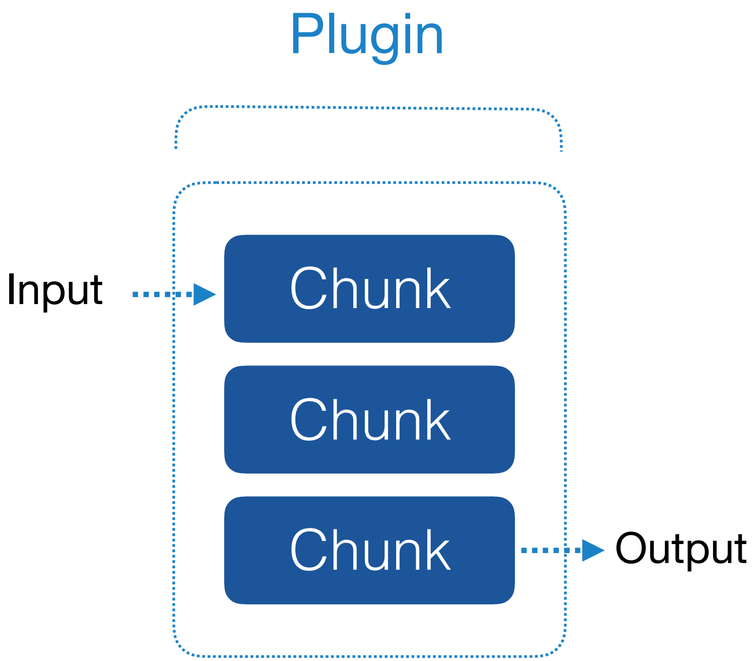
Architecture: Buffer Plugins

- Improve performance
- Provide reliability
- Provide thread-safety

Memory (buf_memory)

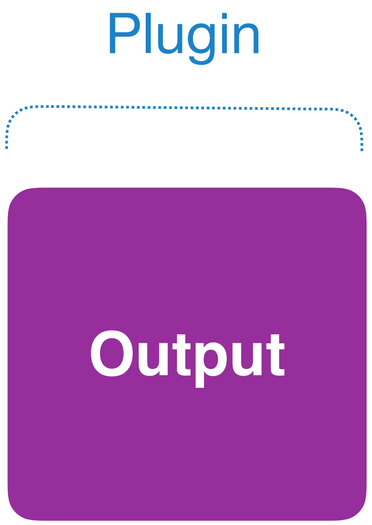
File (buf_file)

Architecture: Buffer Plugins



- Improve performance
- Provide reliability
- Provide thread-safety

Architecture: Output Plugins



- Write or send event logs
- Sync or Async

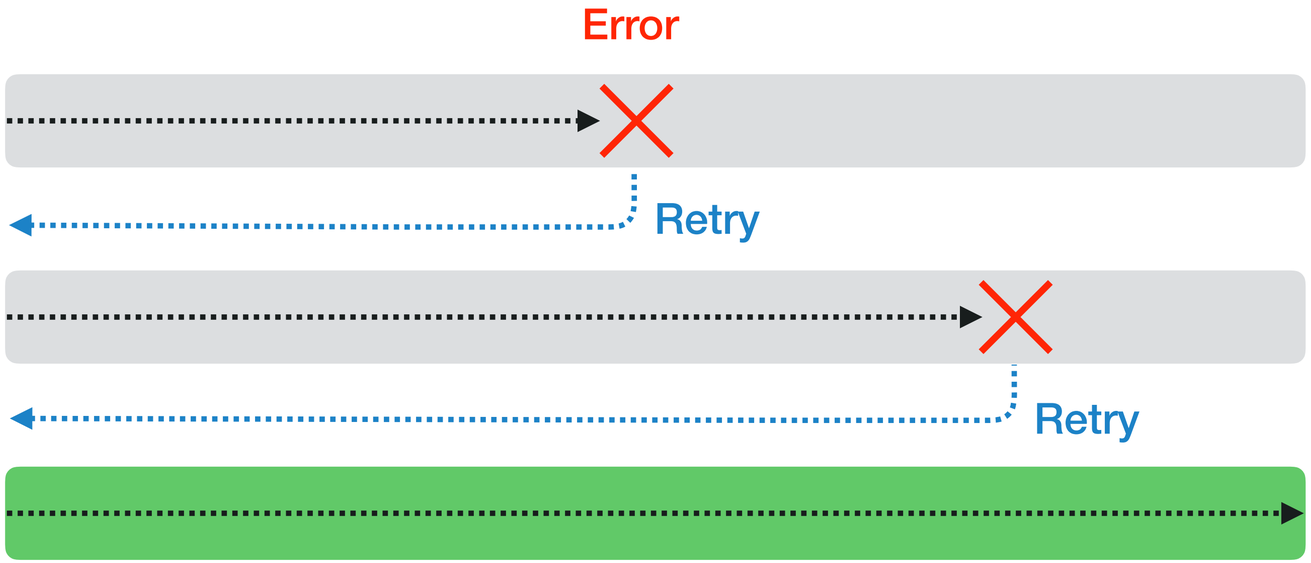
Local File (out_file)

Amazon S3 (out_s3)

Forward to other fluentd (out_forward)

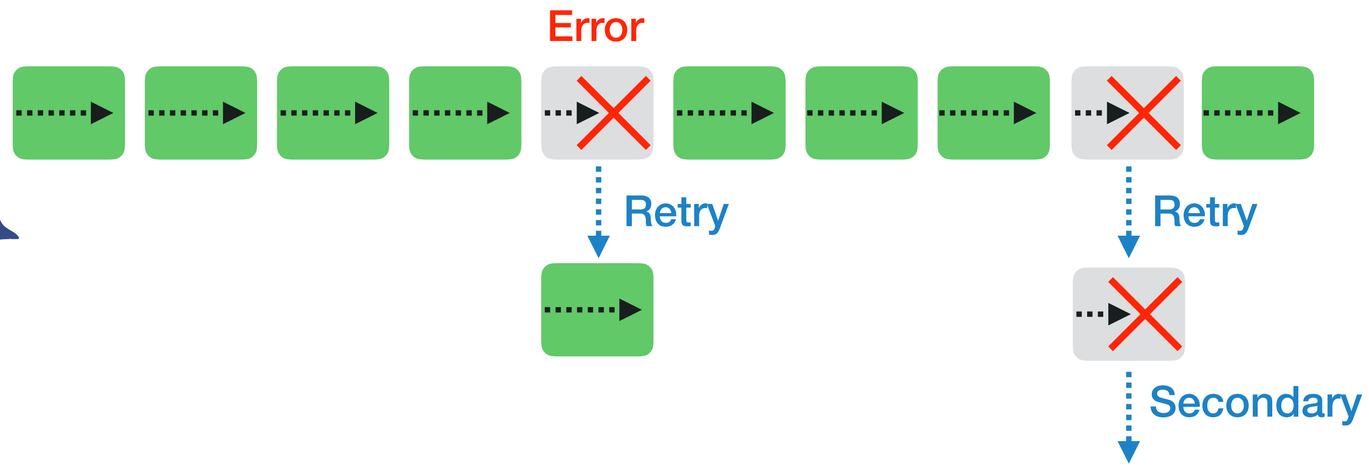
…

Divide & Conquer for retry

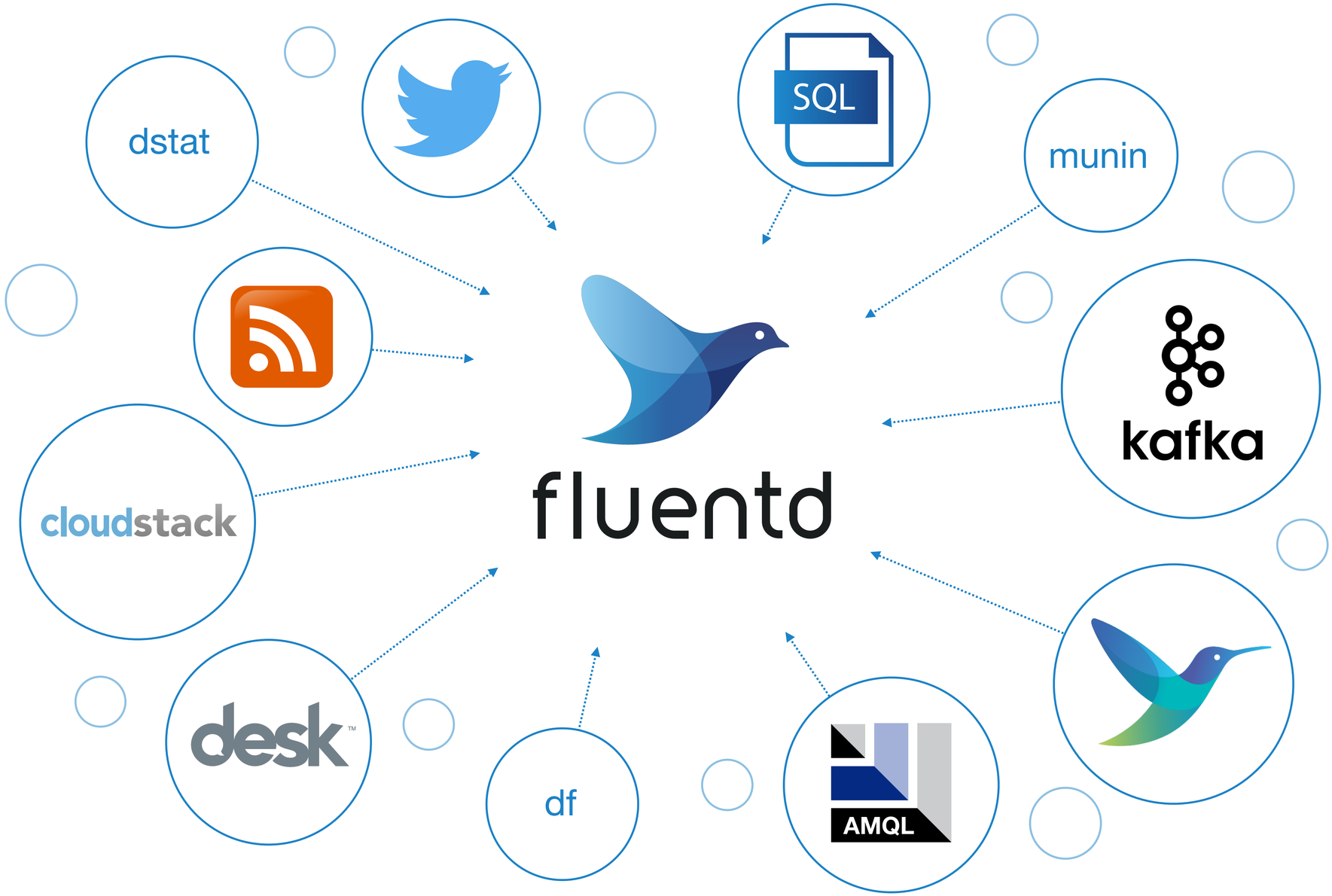


Batch

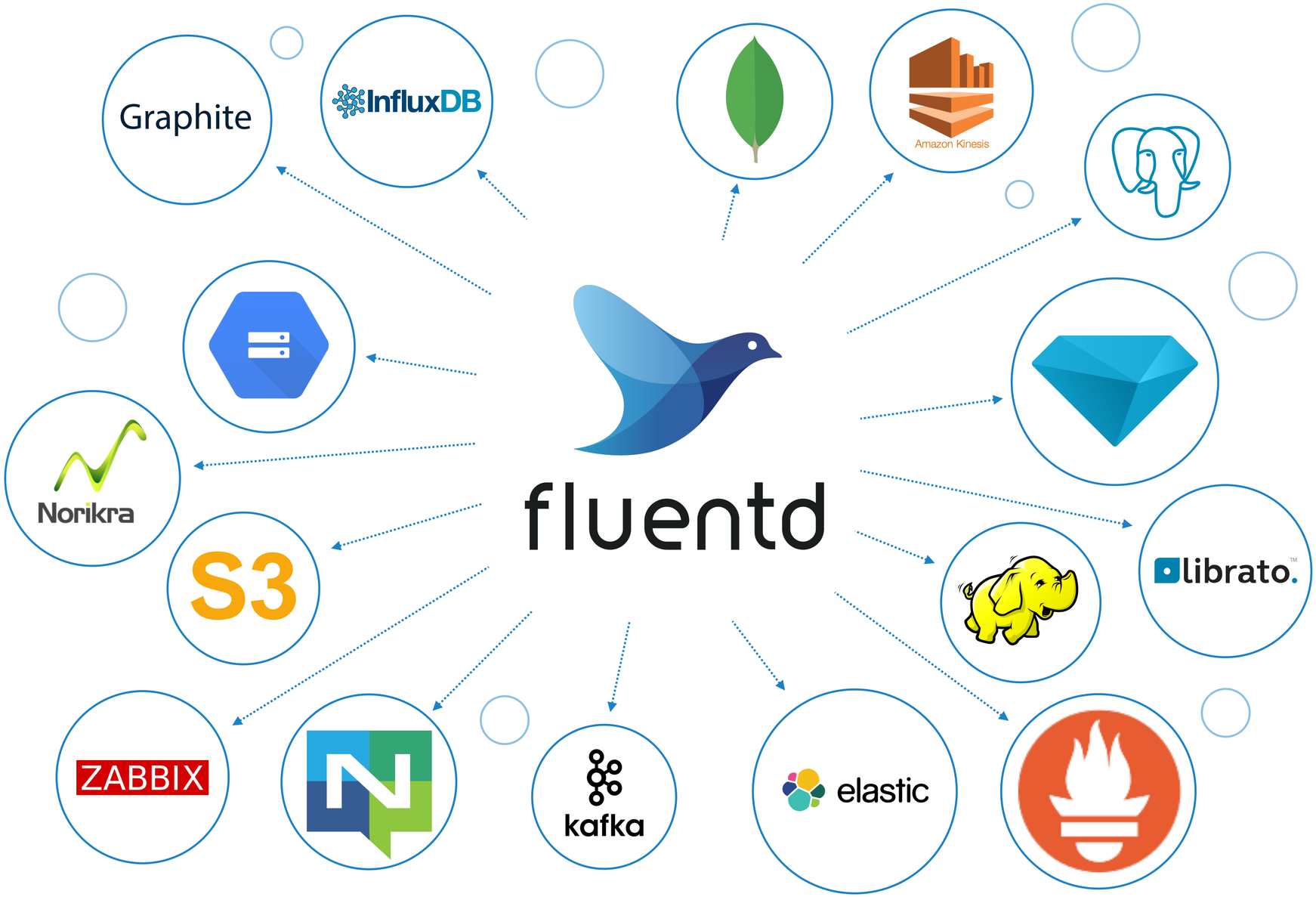
Stream



3rd party input plugins

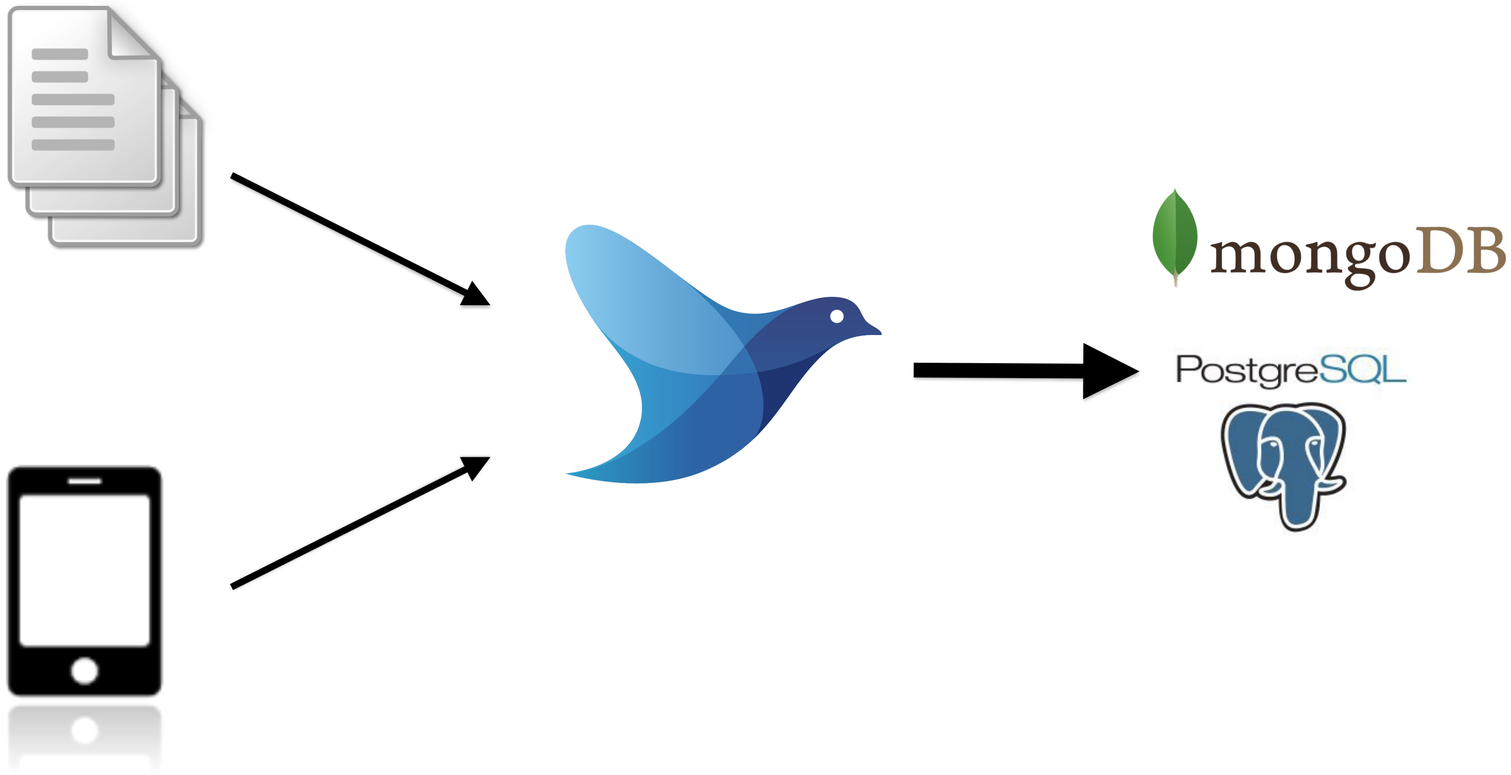


3rd party output plugins



Use-cases with Configuration Example

Simple forwarding

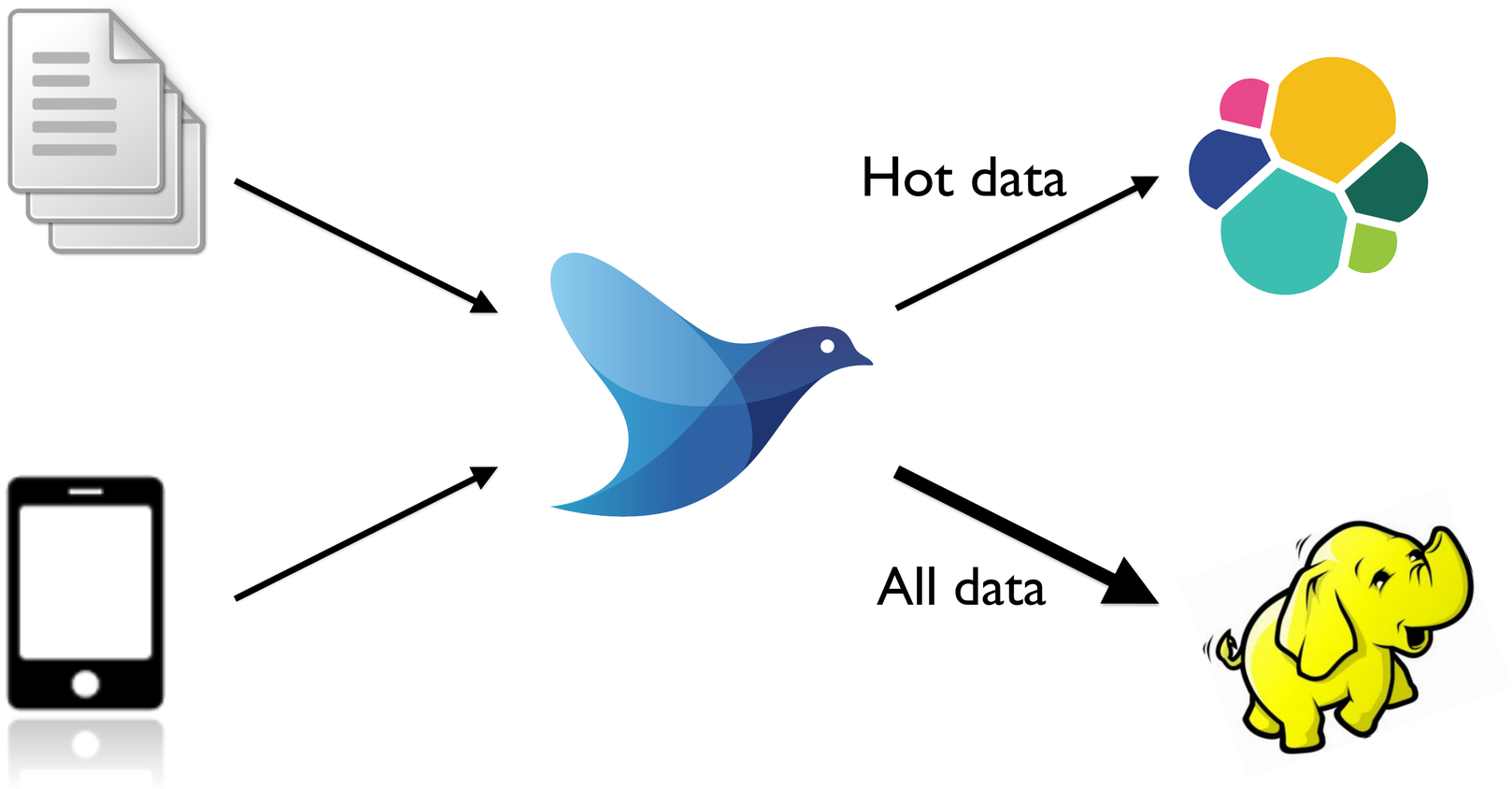


```
# logs from a file
<source>
  @type tail
  path /var/log/httpd.log
  pos_file /tmp/pos_file
  <parse>
    @type apache2
  </parse>
  tag app.apache
</source>

# logs from client libraries
<source>
  @type forward
  port 24224
</source>
```

```
# store logs to MongoDB
<match app.**>
  @type mongo
  database fluent
  collection logs
  <buffer tag>
    @type file
    path /tmp/fluentd/buffer
    flush_interval 30s
  </buffer>
</match>
```

Multiple destinations

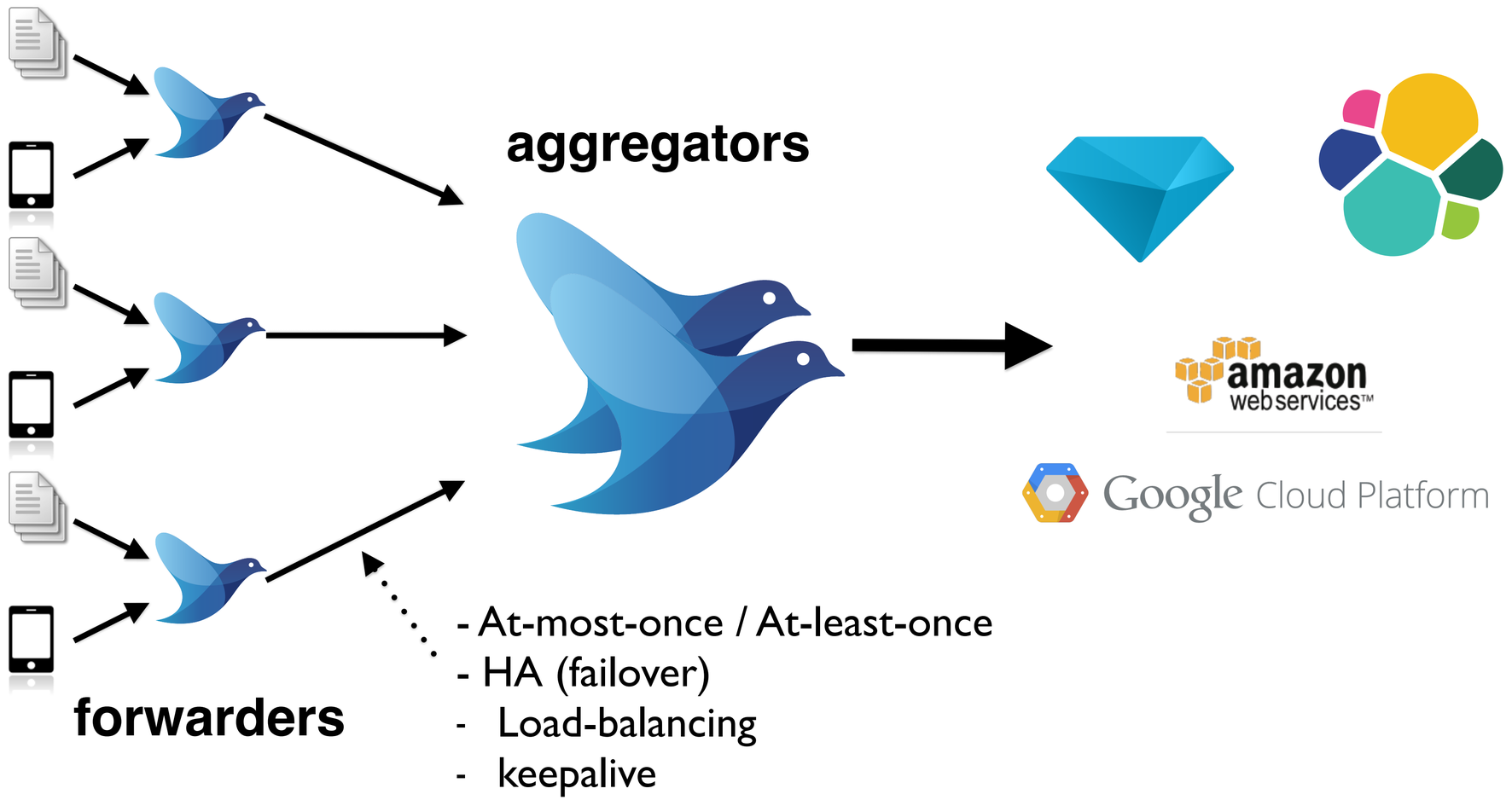


```
# logs from a file
<source>
  @type tail
  path /var/log/httpd.log
  pos_file /tmp/pos_file
  <parse>
    @type apache2
  </parse>
  tag app.access
</source>

# logs from client libraries
<source>
  @type forward
  port 24224
</source>
```

```
# store logs to ES and HDFS
<match app.**>
  @type copy
  <store>
    @type elasticsearch
    logstash_format true
  </store>
  <store>
    @type webhdfs
    host namenode
    port 50070
    path /path/on/hdfs/
  </store>
</match>
```

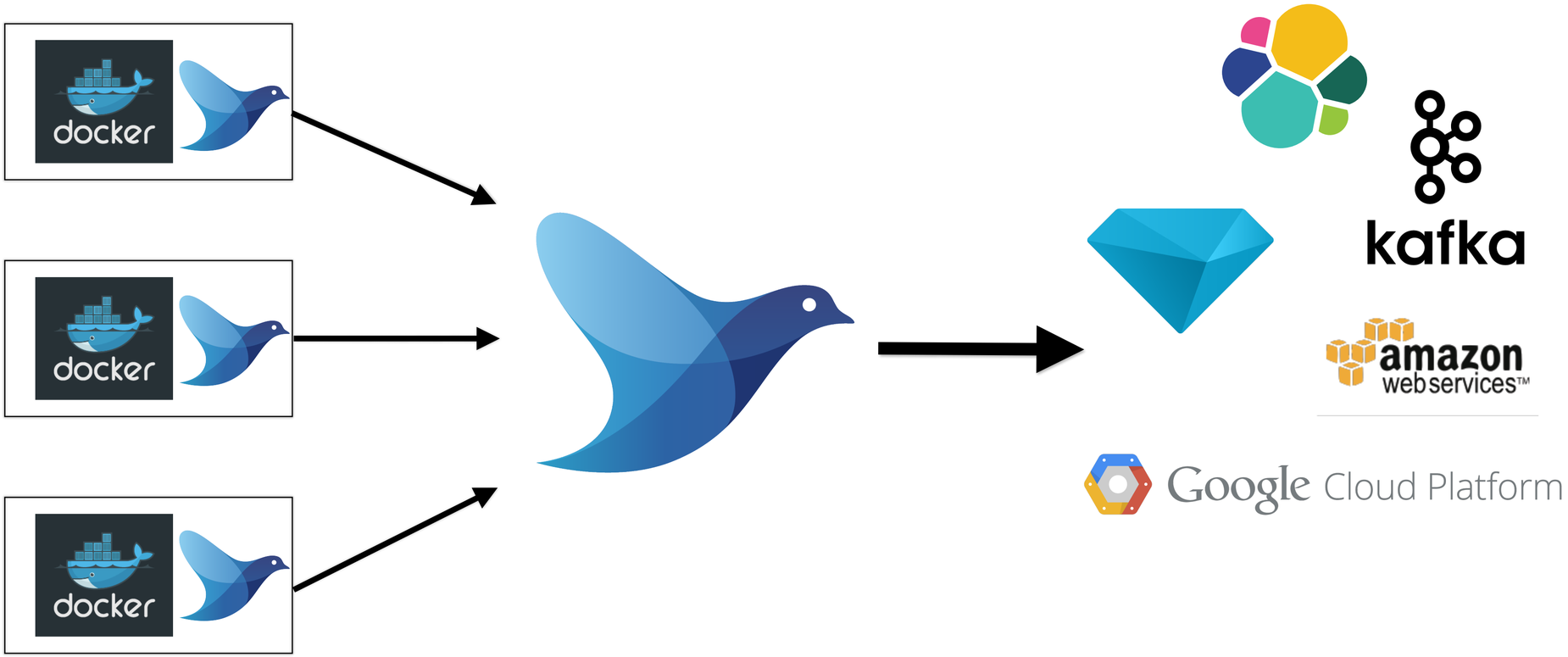
Multi-tier Forwarding



https://www.slideshare.net/repeatedly/fluentd-and-distributed-logging-at-kubecon

Container and Kubernetes

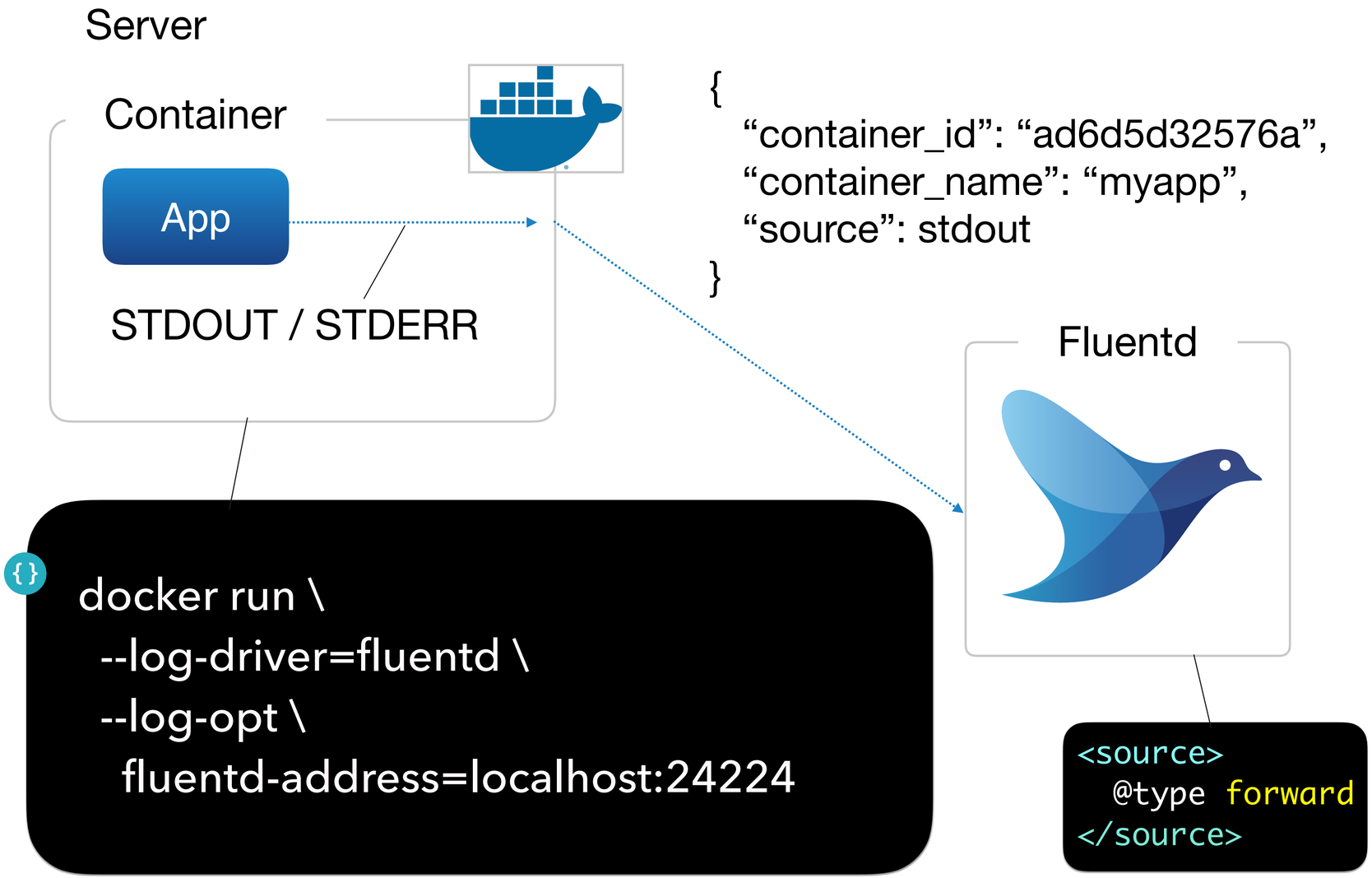
Container Logging



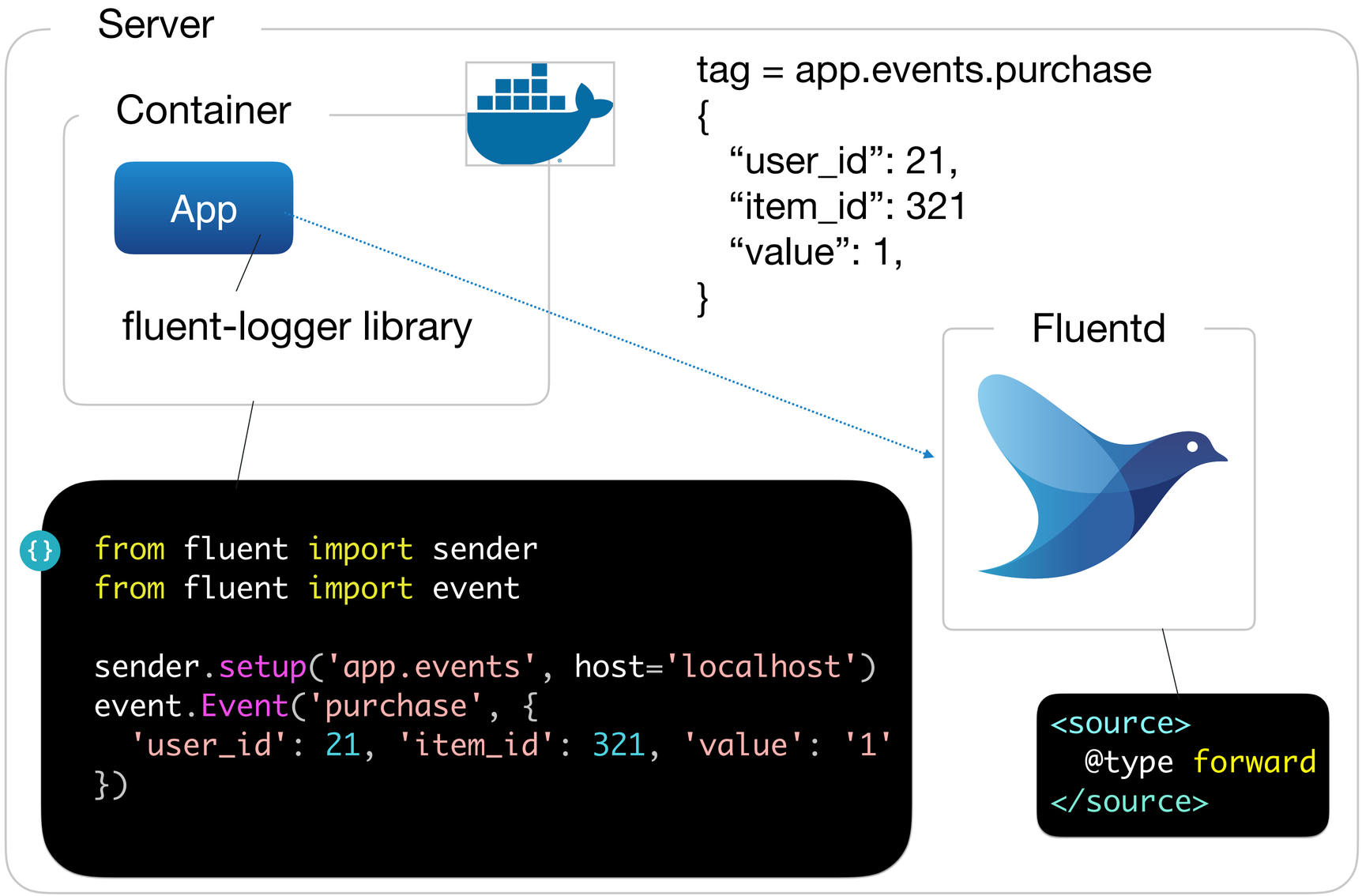
Resources

- Docker : fluentd-docker-image
  - Alpine / Debian images
  - x86, Arm, PowerPC, etc support by Docker official
- Kubernetes : fluentd-kubernetes-daemonset
  - Debian images
  - Some built-in destinations, ES, kafka, graylog, etc…
- Helm chart
  - https://github.com/helm/charts/tree/master/stable/fluentd

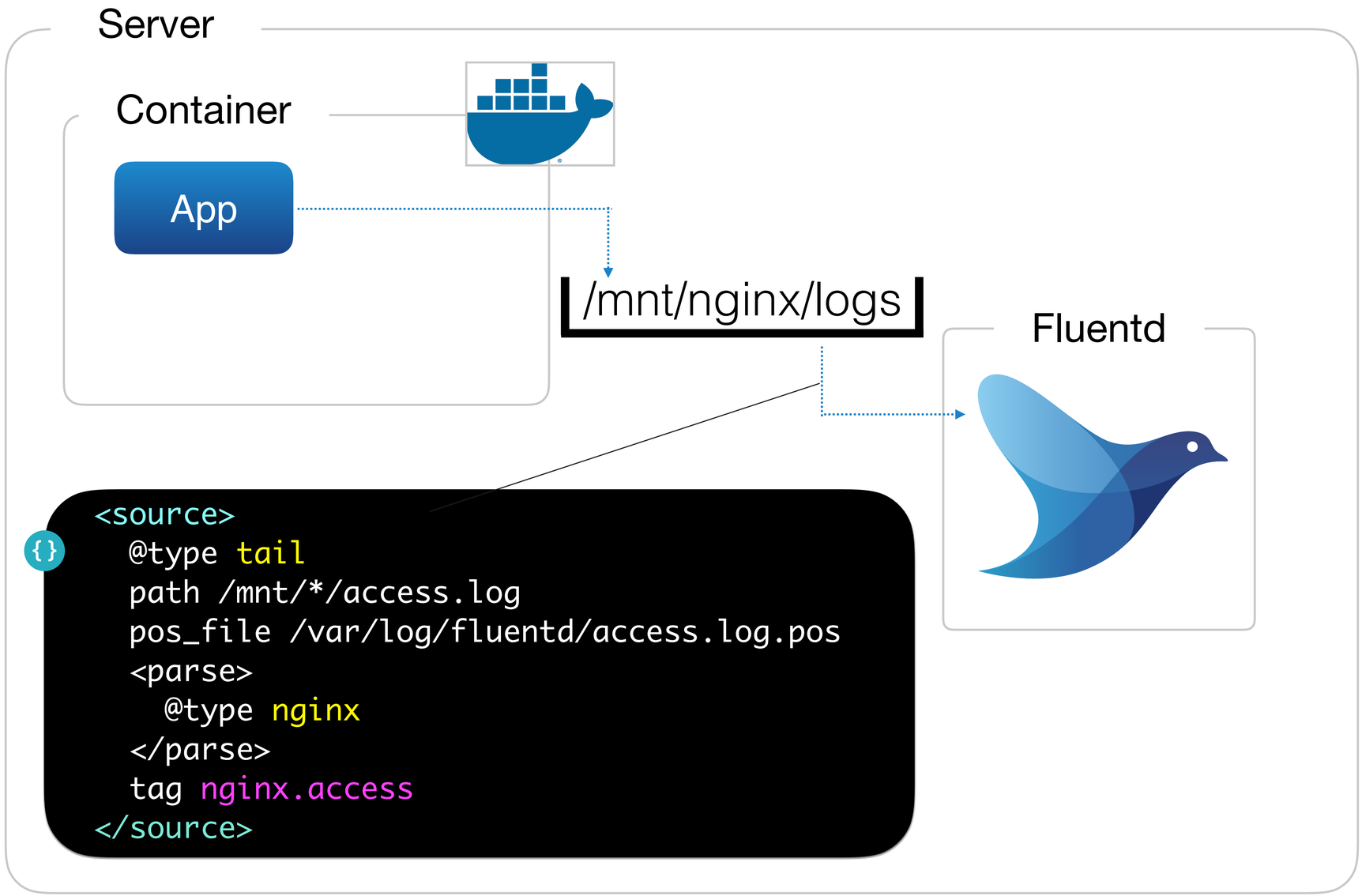
Docker logging with --log-driver=fluentd



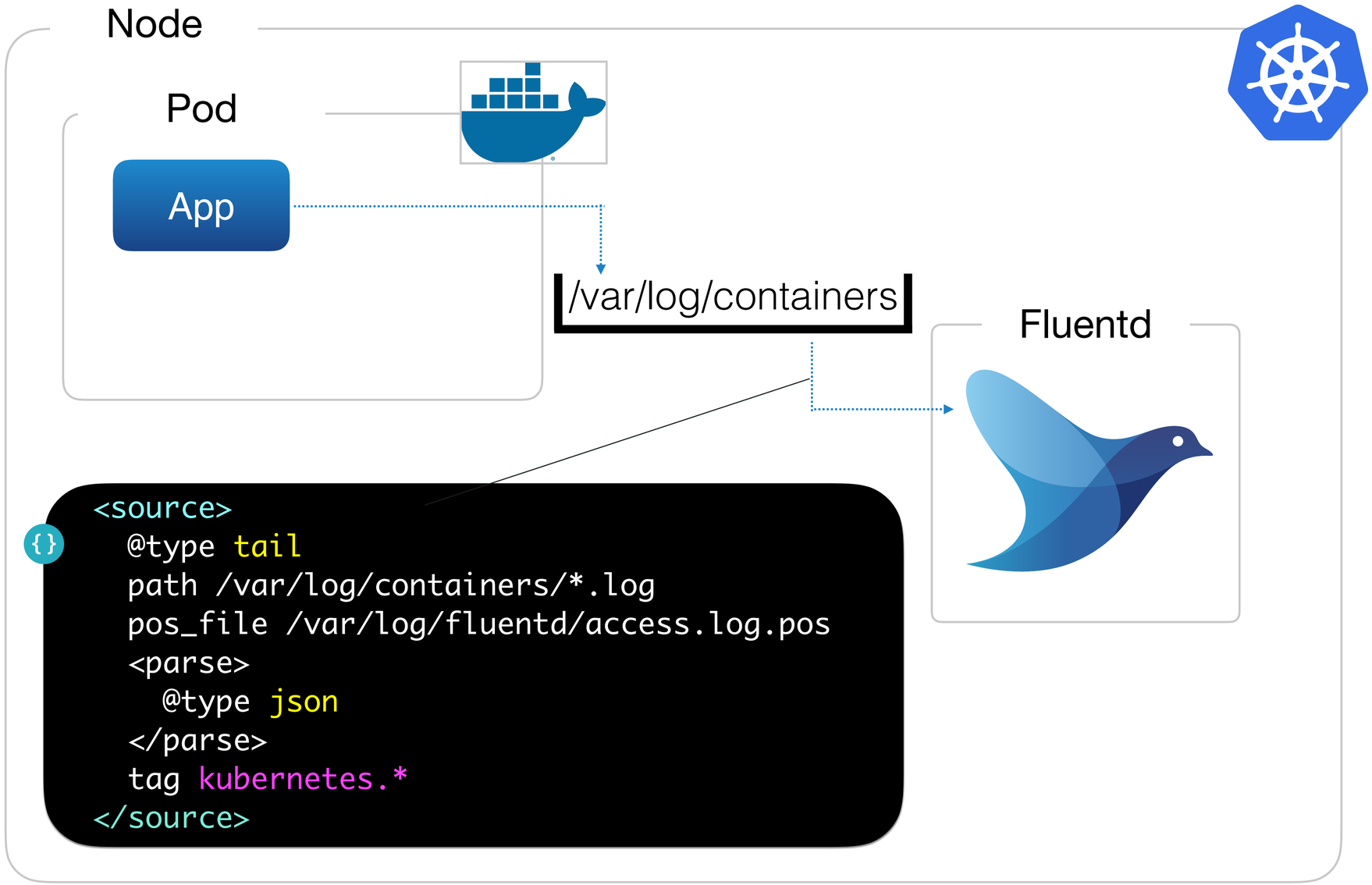
Data collection with fluent-logger



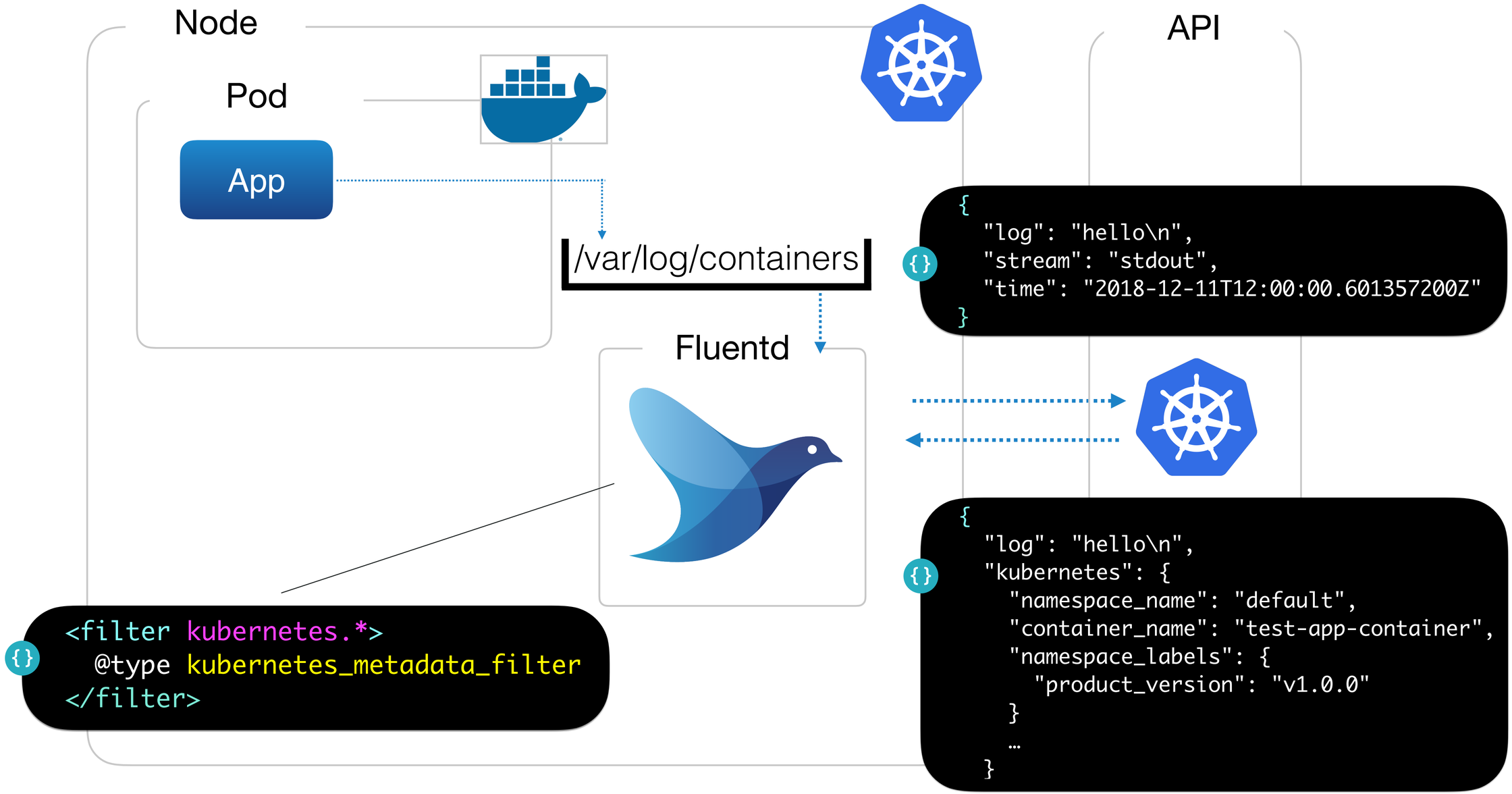
Shared data volume and tailing



Kubernetes Daemonset



Kubernetes Daemonset & metadata



Container Logging approach summary

- Collect log messages with docker
  - --log-driver=fluentd
- Application data/metrics
  - fluent-logger
- Access logs, logs from middleware
  - Shared data volume with in_tail
- Kubernetes Daemonset
  - Collect container logs from /var/log/containers/*
  - Add kubernetes metadata to logs

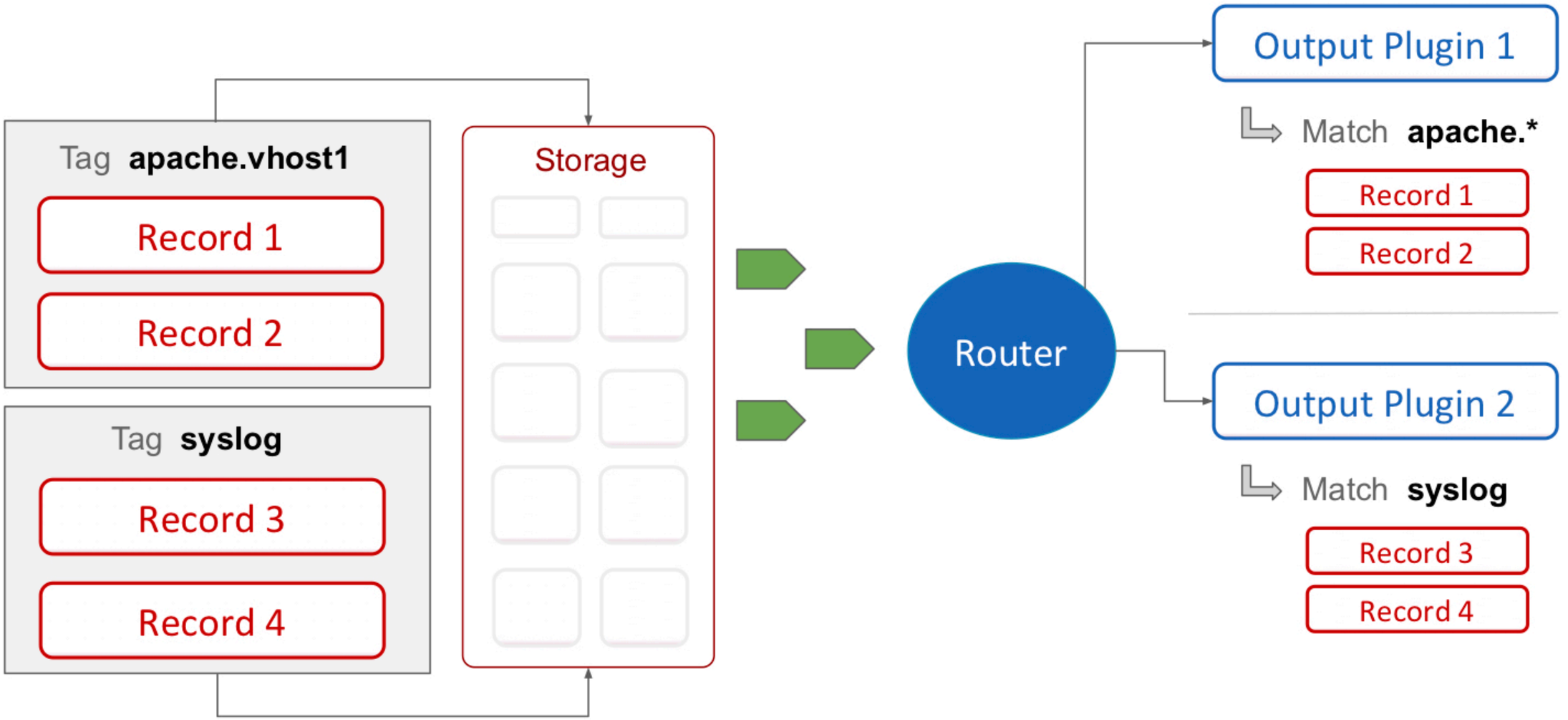
Fluent-bit

Fluentd and Fluent-bit

	Fluentd	Fluent-bit
Implementation	Ruby + C	C
Focus	Flexibility and Robustness	Performance and footprint
Design	Pluggable	Pluggable
Target	Forwarder / Aggregator	Forwarder / Edge

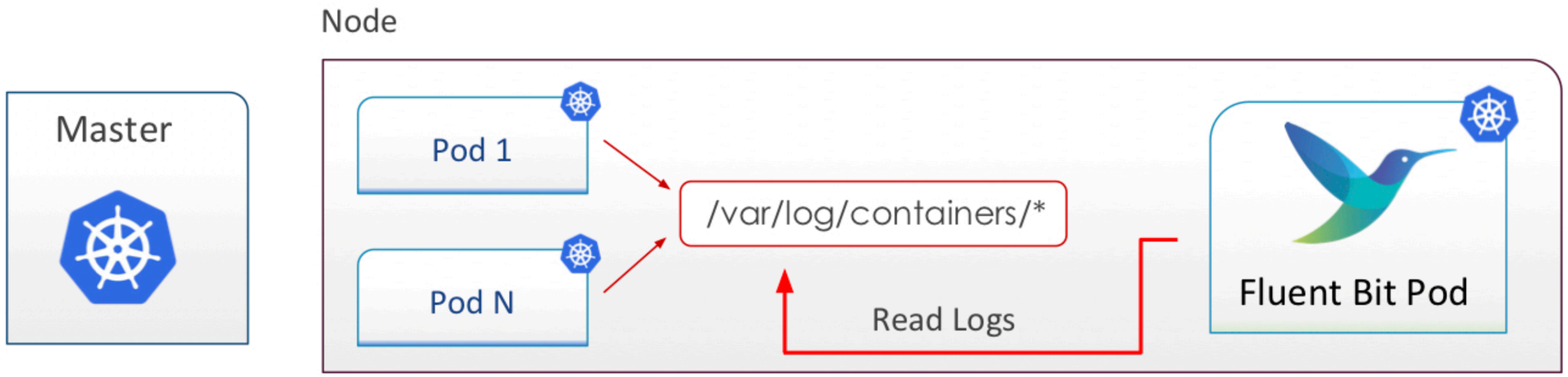
Forward logs from fluent-bit to fluentd is popular pattern

Logging & Routing

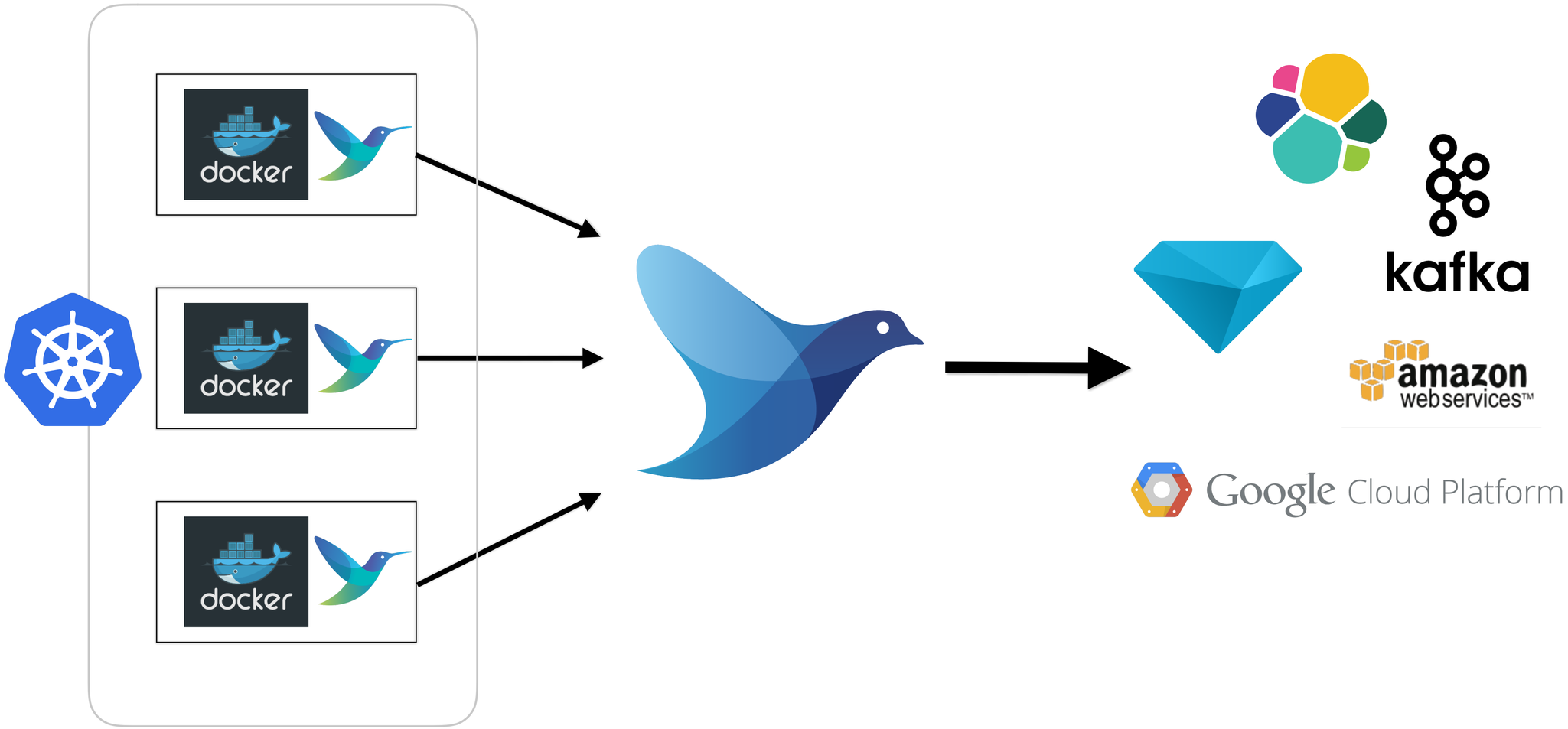


Logging Processing in Kubernetes

Read Logs from the Filesystem or Journald



Container Logging with fluent-bit



Stream Processing on the Edge

Use cases

- Data selection, filtering by patterns or values
- Data Aggregation using windows
- Create new Streams based on query results

Stream Processing Capabilities

- Structured Query Language (SQL)
- Fluent Bit Input plugins are STREAMS of data
- Data Aggregation

https://docs.fluentbit.io/stream-processing/

Enjoy logging