The basics of Fluentd

Masahiro Nakagawa

Treasuare Data, Inc.
Senior Software Engineer

fluentd

Structured logging

Reliable forwarding

Pluggable architecture

http://fluentd.org/

Agenda

> Background

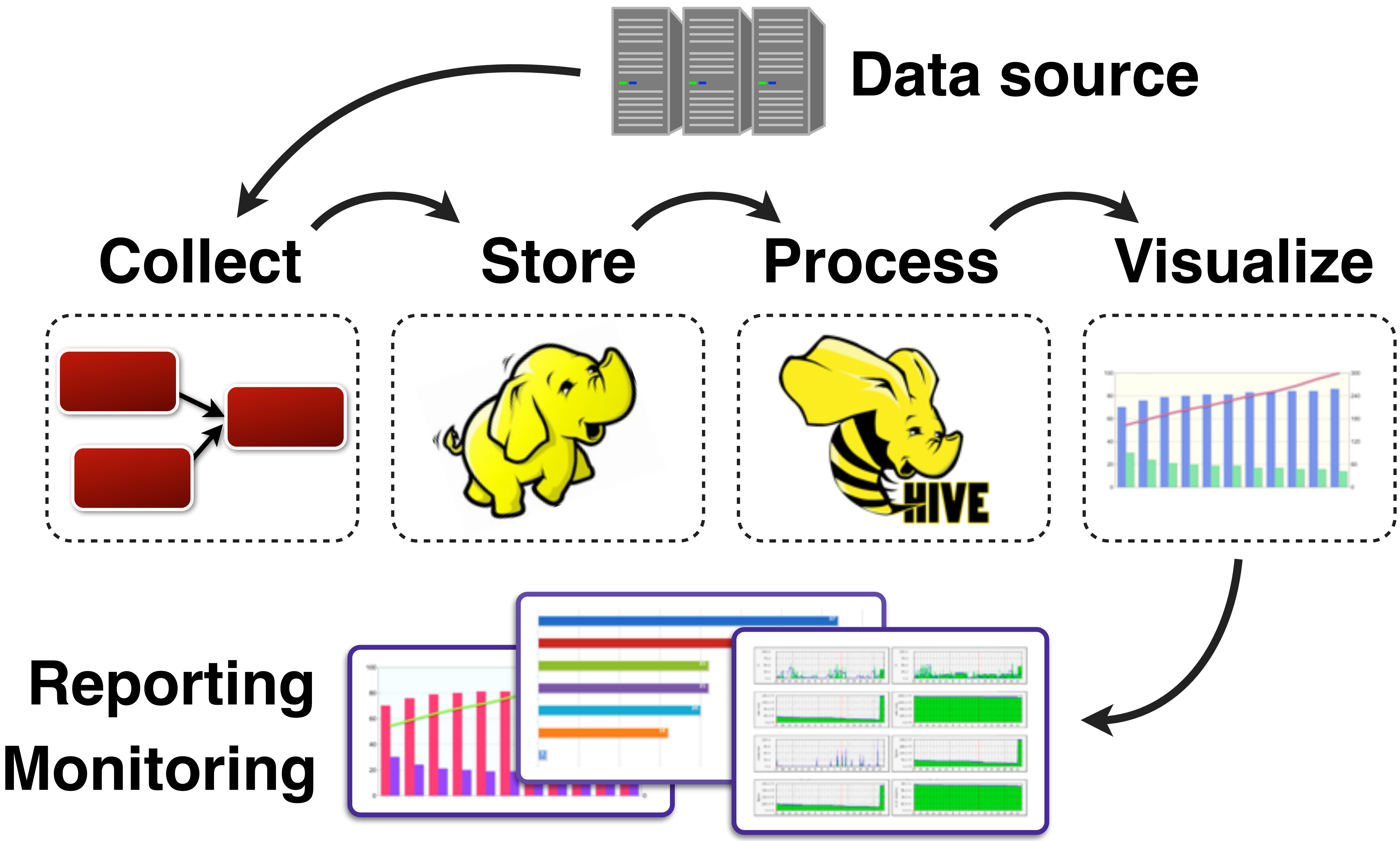
> Overview

> Product Comparison

> Use cases

Background

Data Processing



Data source

Collect

Store

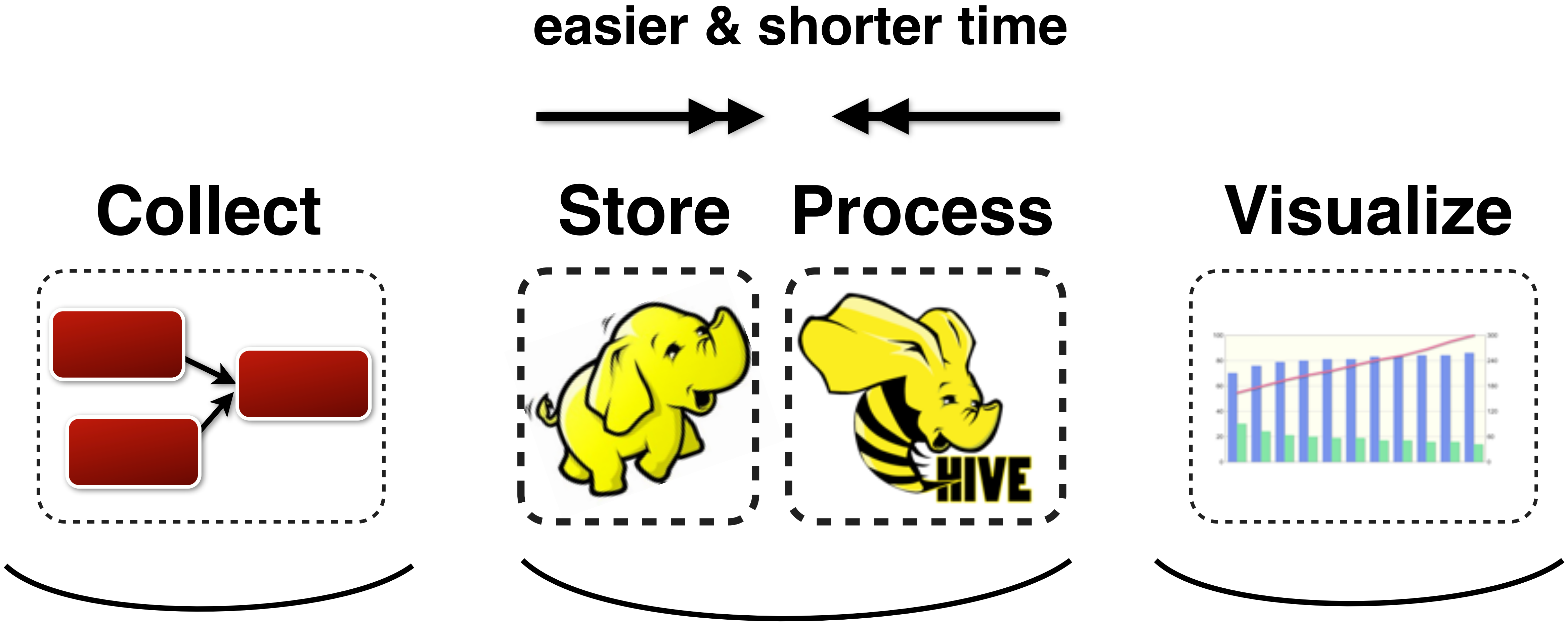
Process

Visualize

Reporting

Monitoring

Related Products



easier & shorter time

Collect

Store

Process

Visualize

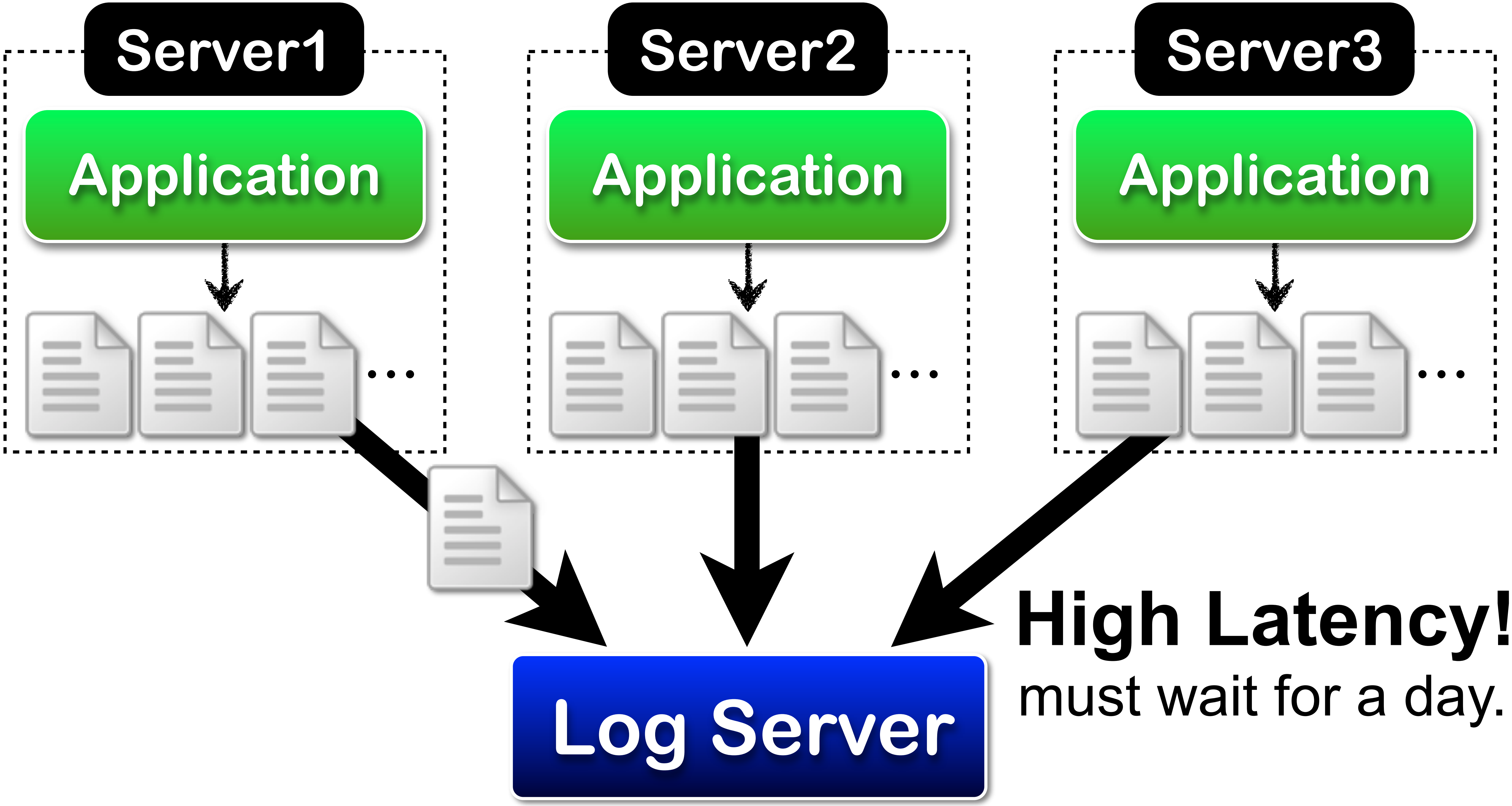
???

Cloudera
Horton Works
Treasure Data

Excel
Tableau
R

fluentd

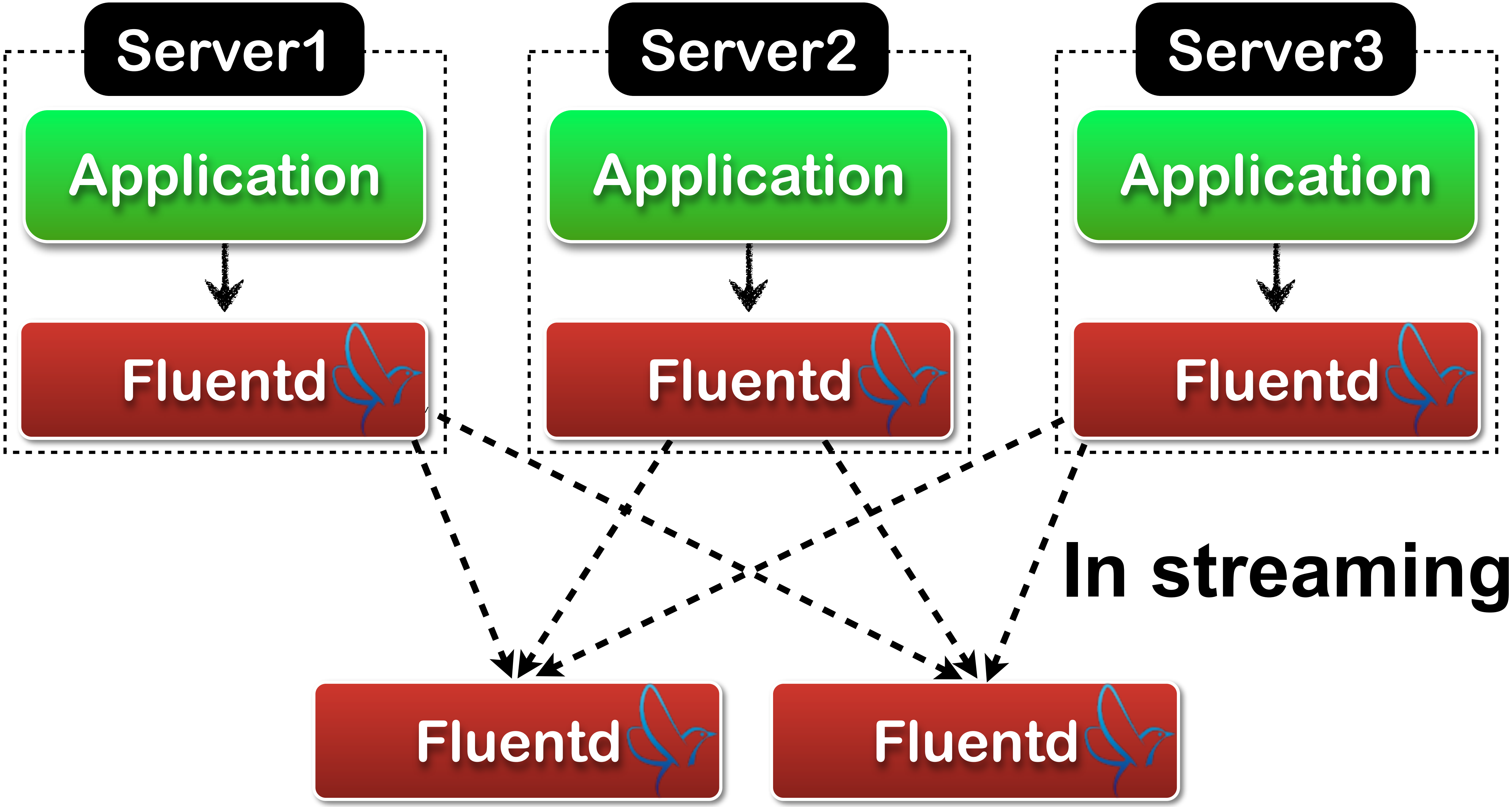
Before Fluentd



High Latency!

must wait for a day...

After Fluentd



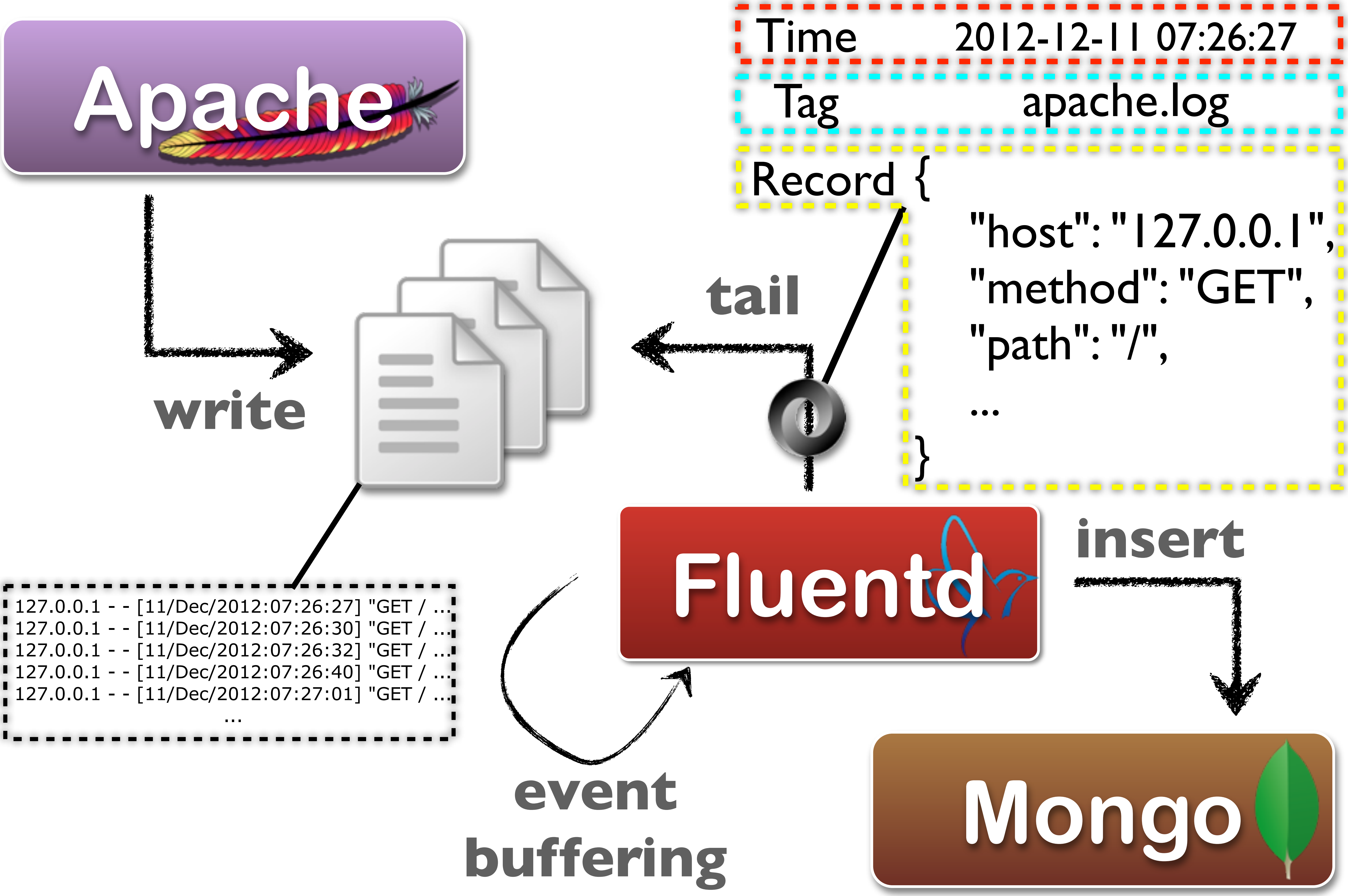
In streaming!

Overview

In short

- Open sourced log collector written in Ruby
- Using rubygems ecosystem for plugins

It’s like syslogd, but
uses JSON for log messages



Apache

write

tail

Time 2012-12-11 07:26:27

Tag apache.log

```
Record {
    "host": "127.0.0.1",
    "method": "GET",
    "path": "/",
    ...
}
```

```
127.0.0.1 - - [11/Dec/2012:07:26:27] "GET / ...
127.0.0.1 - - [11/Dec/2012:07:26:30] "GET / ...
127.0.0.1 - - [11/Dec/2012:07:26:32] "GET / ...
127.0.0.1 - - [11/Dec/2012:07:26:40] "GET / ...
127.0.0.1 - - [11/Dec/2012:07:27:01] "GET / ...
                     ...
```

Fluentd

insert

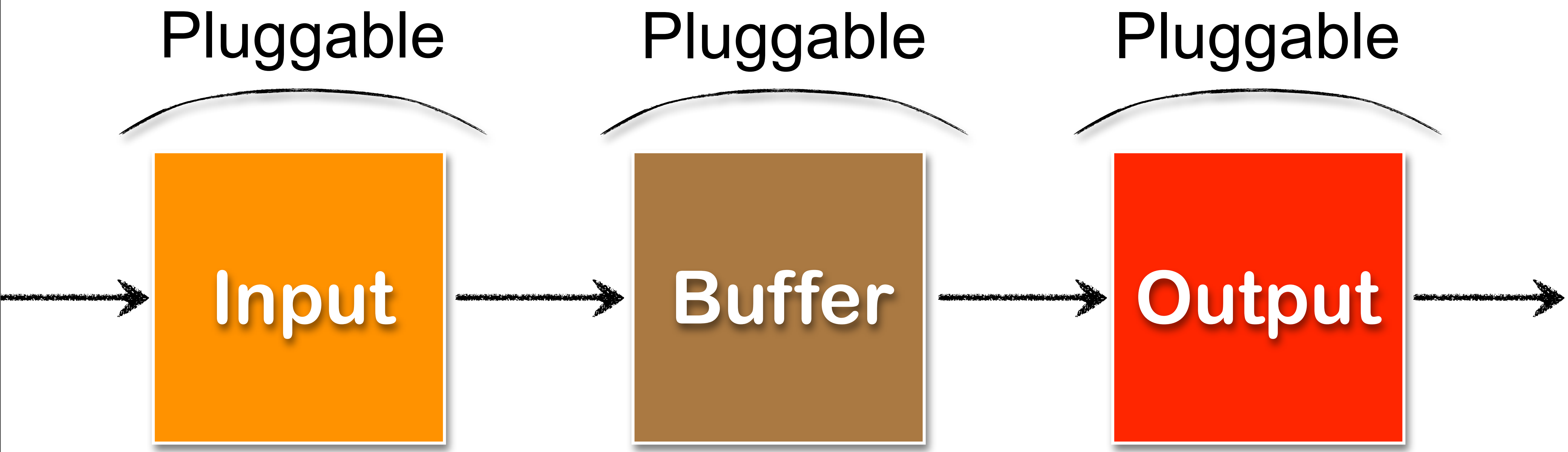
event buffering

Mongo

Event structure(log message)

- ✓ Time
  - > second unit
  - > from data source or adding parsed time
- ✓ Tag
  - > for message routing
- ✓ Record
  - > JSON format
    - > MessagePack internally
    - > non-unstructured

Architecture



Pluggable

Input

Pluggable

Buffer

Pluggable

Output

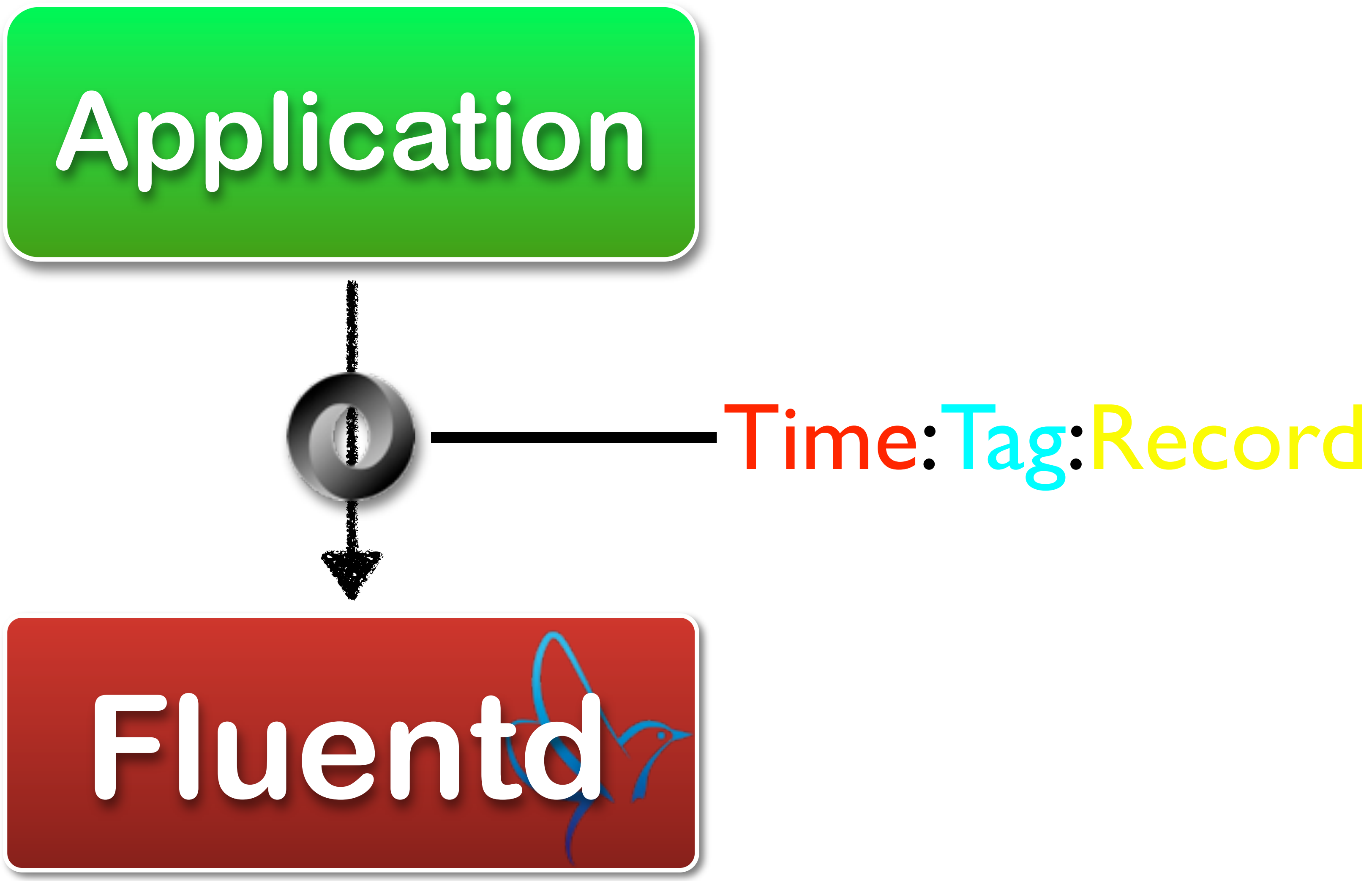
- > **Forward**
- > **HTTP**
- > **File tail**
- > **dstat**
- > ...

- > **Memory**
- > **File**

- > **Forward**
- > **File**
- > **Amazon S3**
- > **MongoDB**
- > ...

Client libraries

> Ruby
> Java
> Perl
> PHP
> Python
> D
> Scala
> ...



Application

Time:Tag:Record

Fluentd

```
# Ruby
Fluent.open(“myapp”)
Fluent.event(“login”, {“user” => 38})
#=> 2012-12-11 07:56:01 myapp.login  {“user”:38}
```

Configuration and operation

- **No central / master node**
  - **HTTP include** helps conf sharing
- **Operation depends on your environment**
  - Use your deamon management
  - Use **chef** in Treasure Data
- **Scribe like syntax**

```
# receive events via HTTP
<source>
  type http
  port 8888
</source>

# read logs from a file
<source>
  type tail
  path /var/log/httpd.log
  format apache
  tag apache.access
</source>

# save access logs to MongoDB
<match apache.access>
  type mongo
  database apache
  collection log
</match>
```

```
# save alerts to a file
<match alert.**>
  type file
  path /var/log/fluent/alerts
</match>

# forward other logs to servers
<match **>
  type forward
  <server>
    host 192.168.0.11
    weight 20
  </server>
  <server>
    host 192.168.0.12
    weight 60
  </server>
</match>

include http://example.com/conf
```

Reliability (core + plugin)

- Buffering
  - Use file buffer for persistent data
  - buffer chunk has ID for idempotent
- Retrying
- Error handling
  - transaction, failover, etc on forward plugin
  - secondary

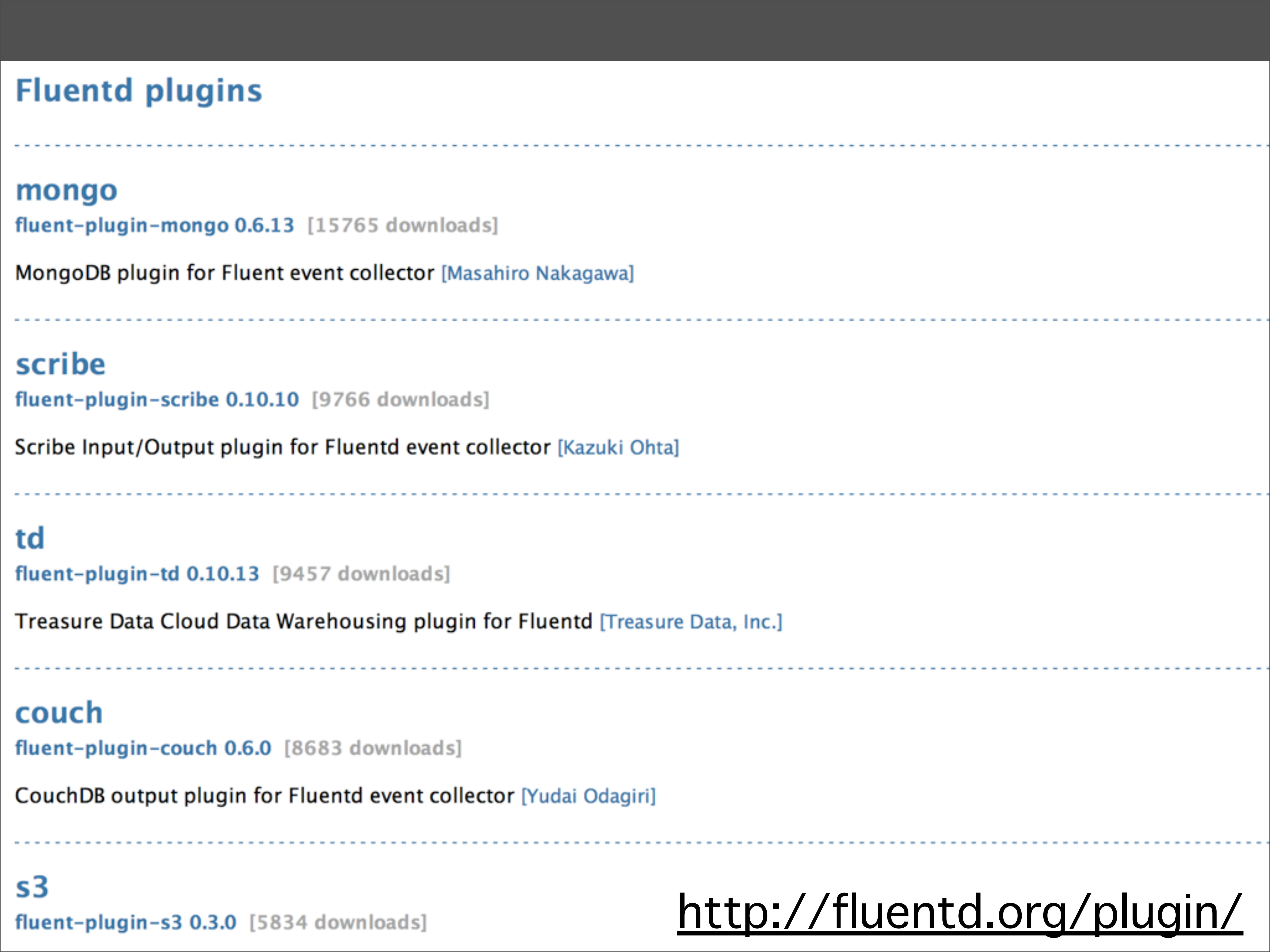
Plugins – use rubygems

```
$ fluent-gem search -rd fluent-plugin
```

```
$ fluent-gem search -rd fluent-mixin
```

```
$ fluent-gem install fluent-plugin-mongo
```

※ Today, don’t talk the plugin development



Fluentd plugins

mongo

fluent-plugin-mongo 0.6.13 [15765 downloads]

MongoDB plugin for Fluent event collector [Masahiro Nakagawa]

scribe

fluent-plugin-scribe 0.10.10 [9766 downloads]

Scribe Input/Output plugin for Fluentd event collector [Kazuki Ohta]

td

fluent-plugin-td 0.10.13 [9457 downloads]

Treasure Data Cloud Data Warehousing plugin for Fluentd [Treasure Data, Inc.]

couch

fluent-plugin-couch 0.6.0 [8683 downloads]

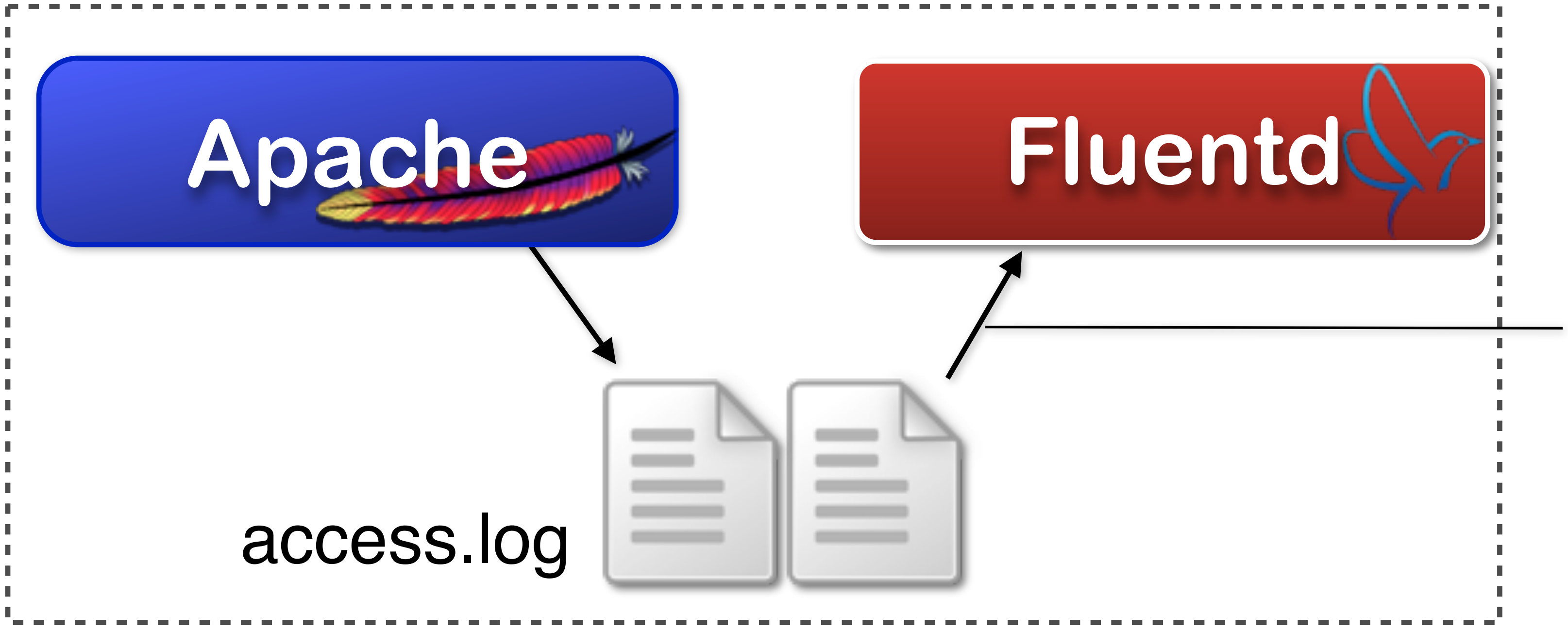
CouchDB output plugin for Fluentd event collector [Yudai Odagiri]

s3

fluent-plugin-s3 0.3.0 [5834 downloads]

http://fluentd.org/plugin/

in_tail

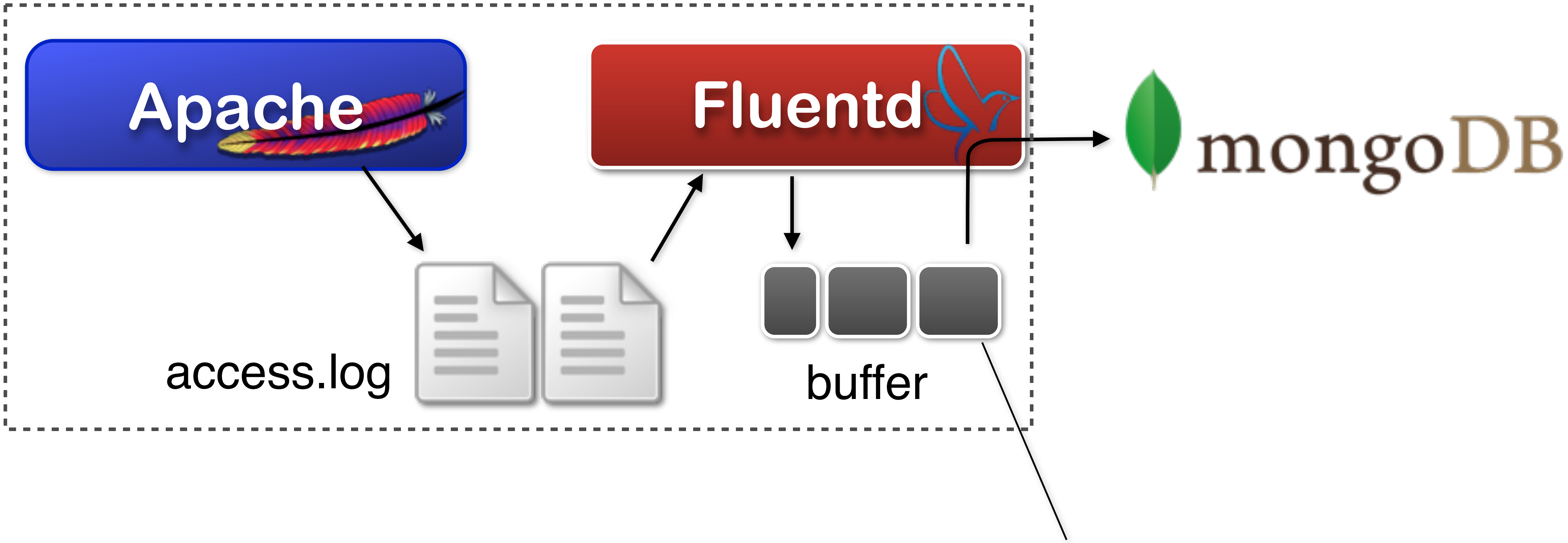


✓ read a log file
✓ custom regexp
✓ custom parser in Ruby

Supported format:

- apache
- apache2
- syslog
- nginx
- json
- csv
- tsv
- ltsv (since v0.10.32)

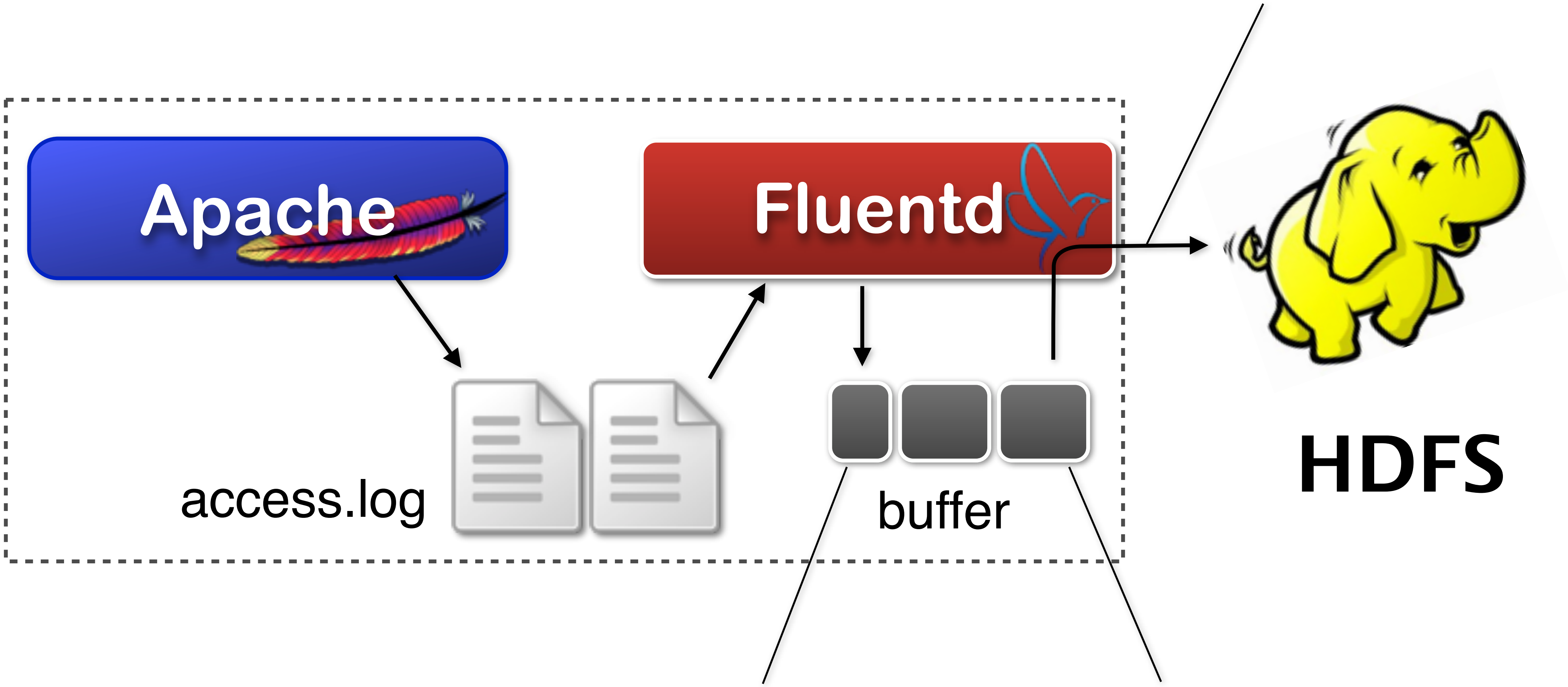
out_mongo



✓ retry automatically
✓ exponential retry wait
✓ persistent on a file

out_webhdfs

✓ custom text formatter

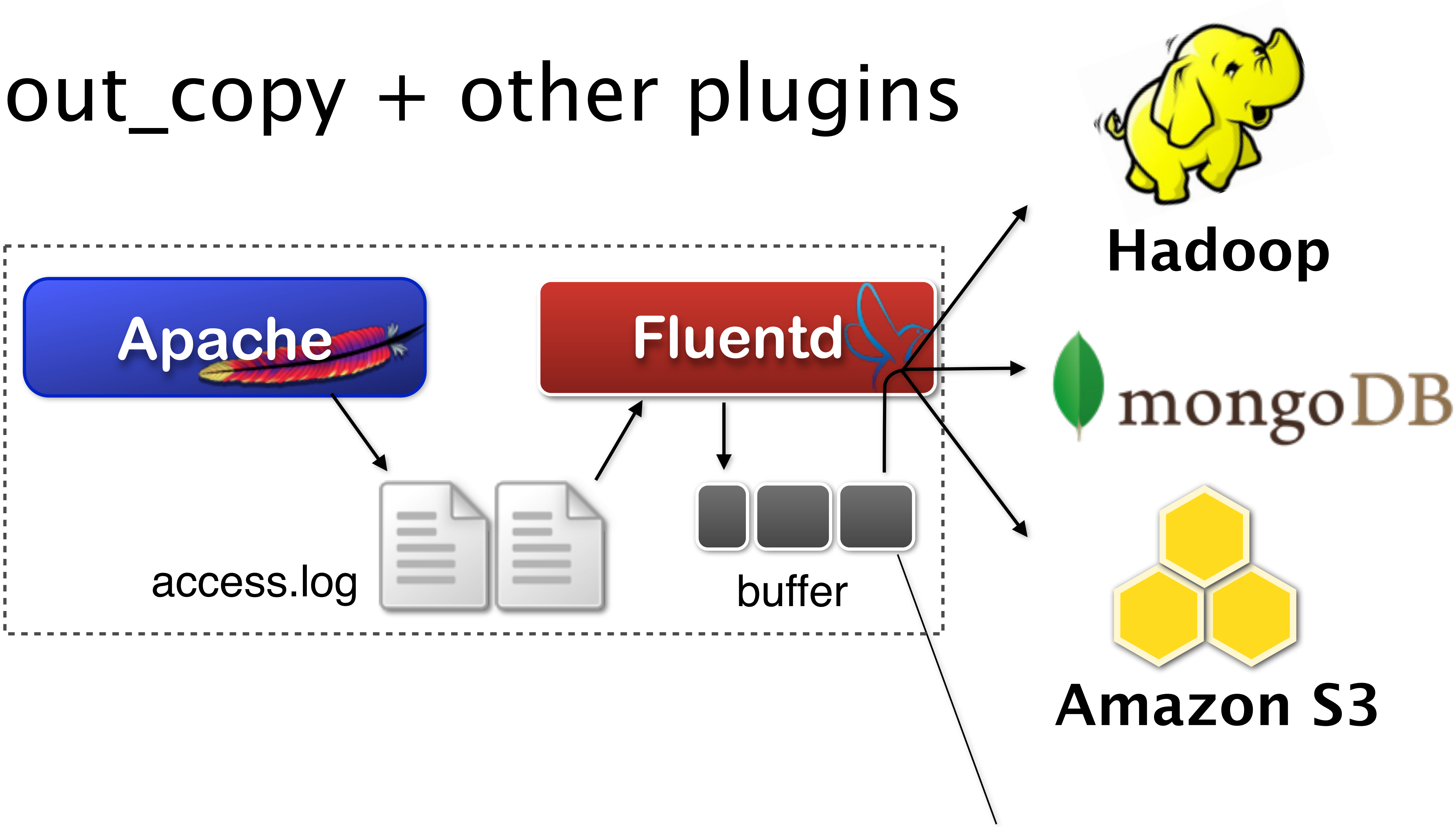


✓ slice files based on time

2013-01-01/01/access.log.gz
2013-01-01/02/access.log.gz
2013-01-01/03/access.log.gz
...

✓ retry automatically
✓ exponential retry wait
✓ persistent on a file

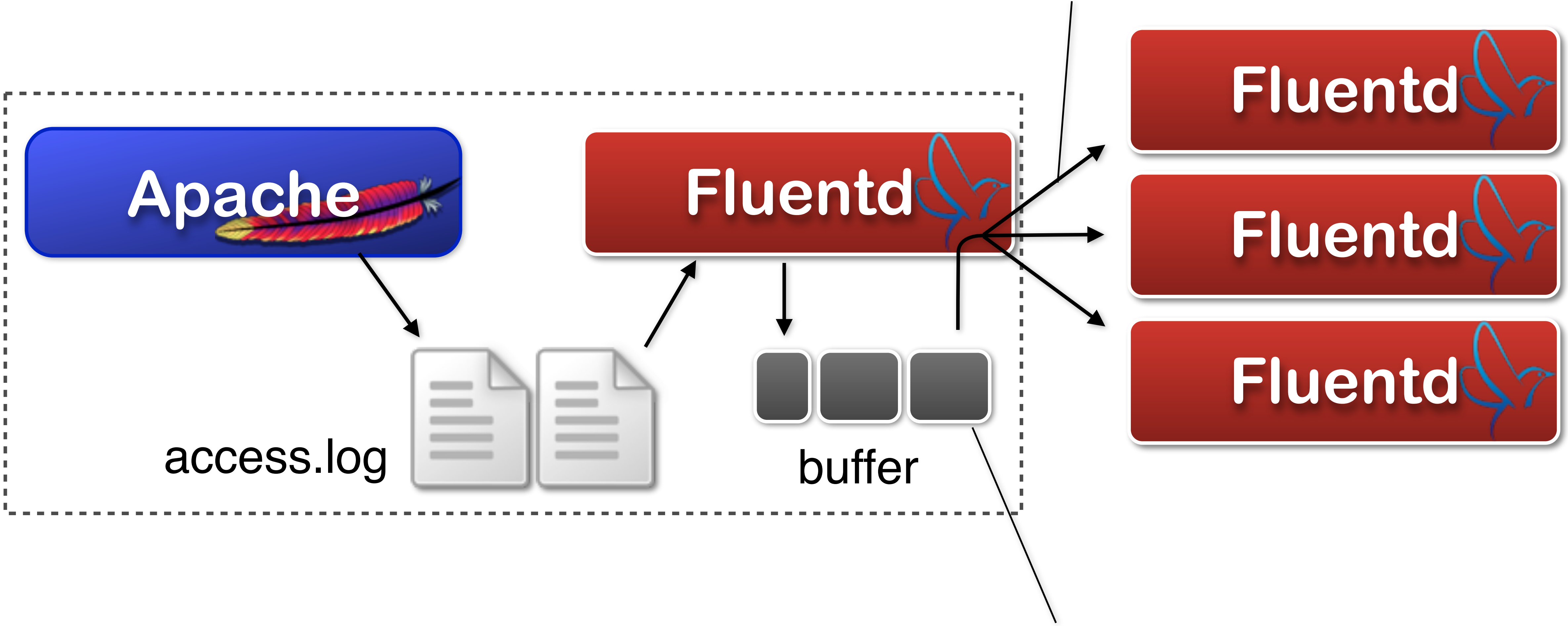
out_copy + other plugins



✓ routing based on tags
✓ copy to multiple storages

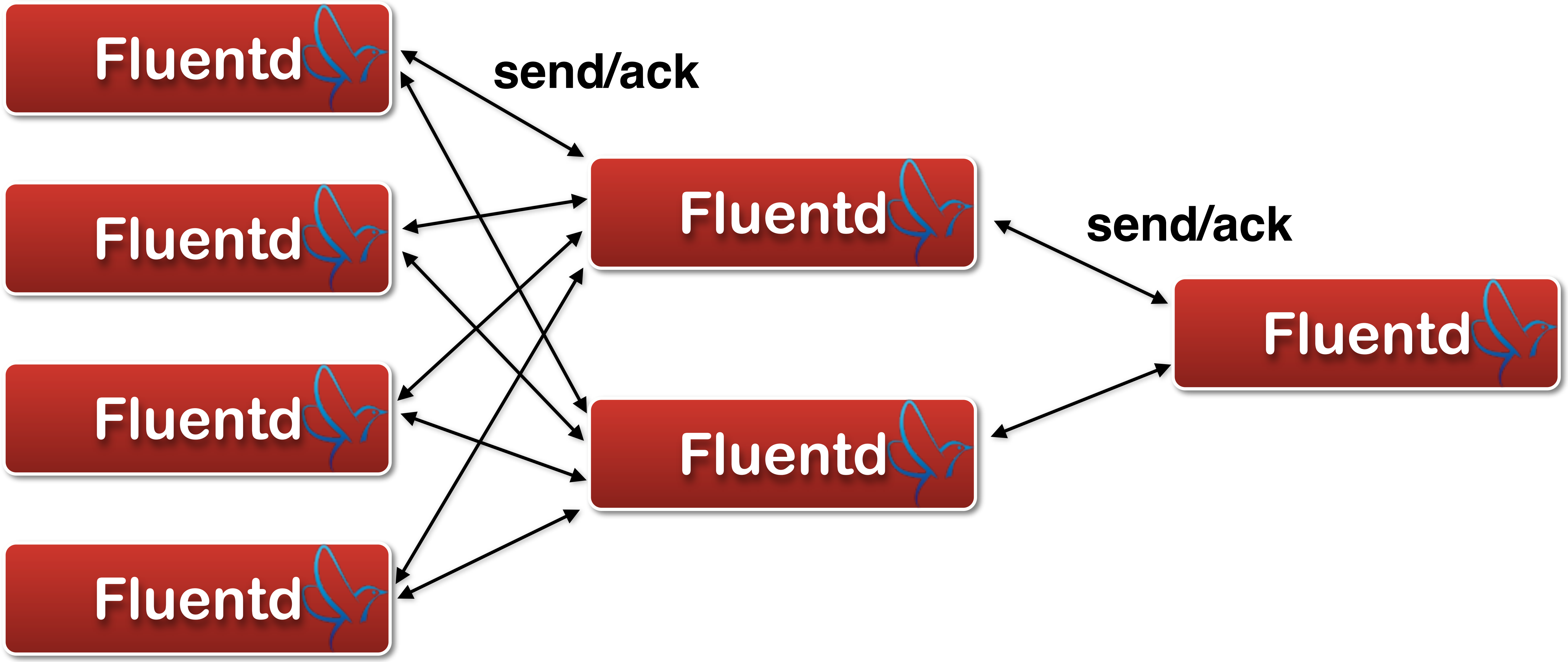
out_forward

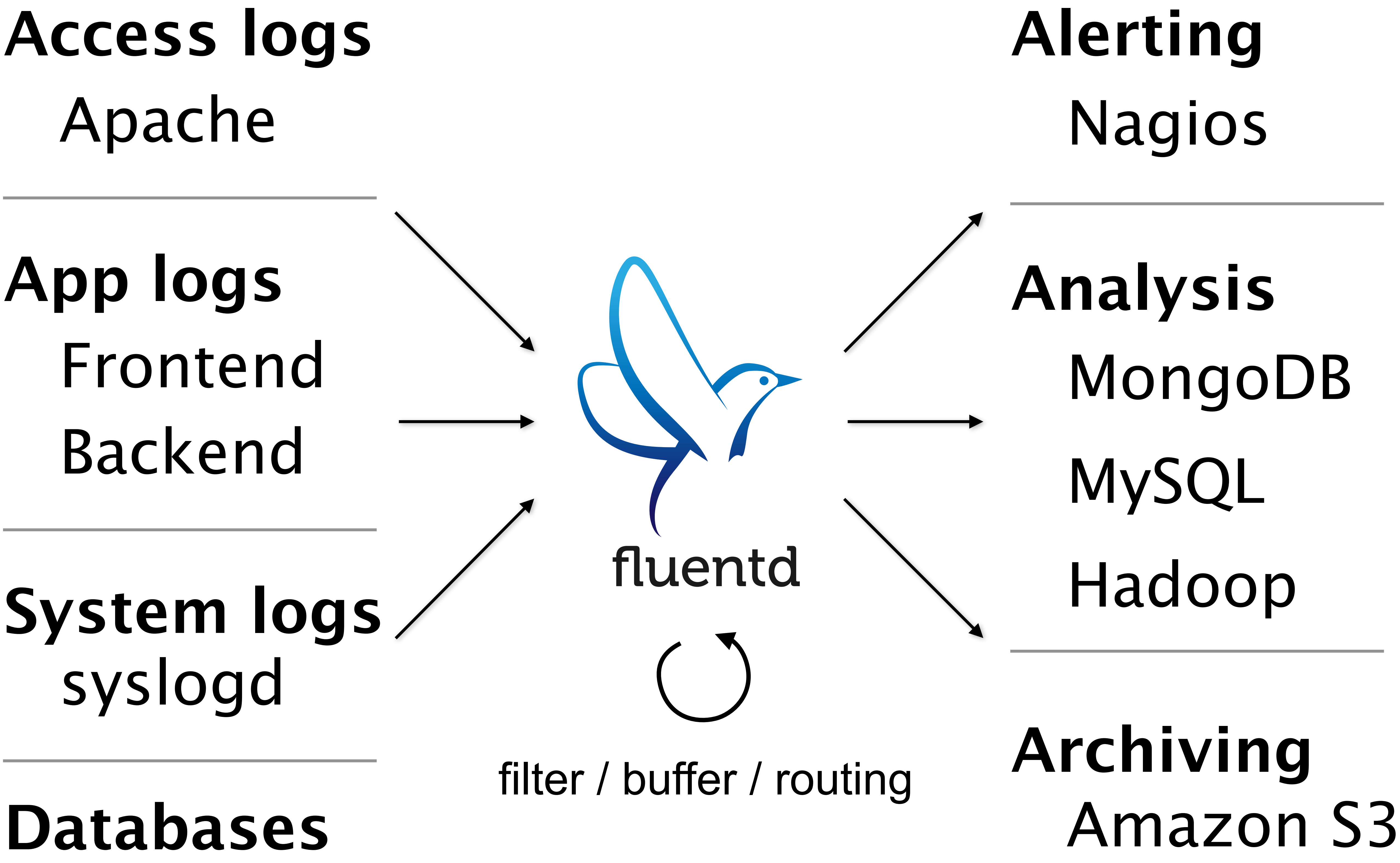
✓ automatic fail-over
✓ load balancing



✓ retry automatically
✓ exponential retry wait
✓ persistent on a file

Forward topology





Access logs

Apache

App logs

Frontend

Backend

System logs

syslogd

Databases

fluentd

filter / buffer / routing

Alerting

Nagios

Analysis

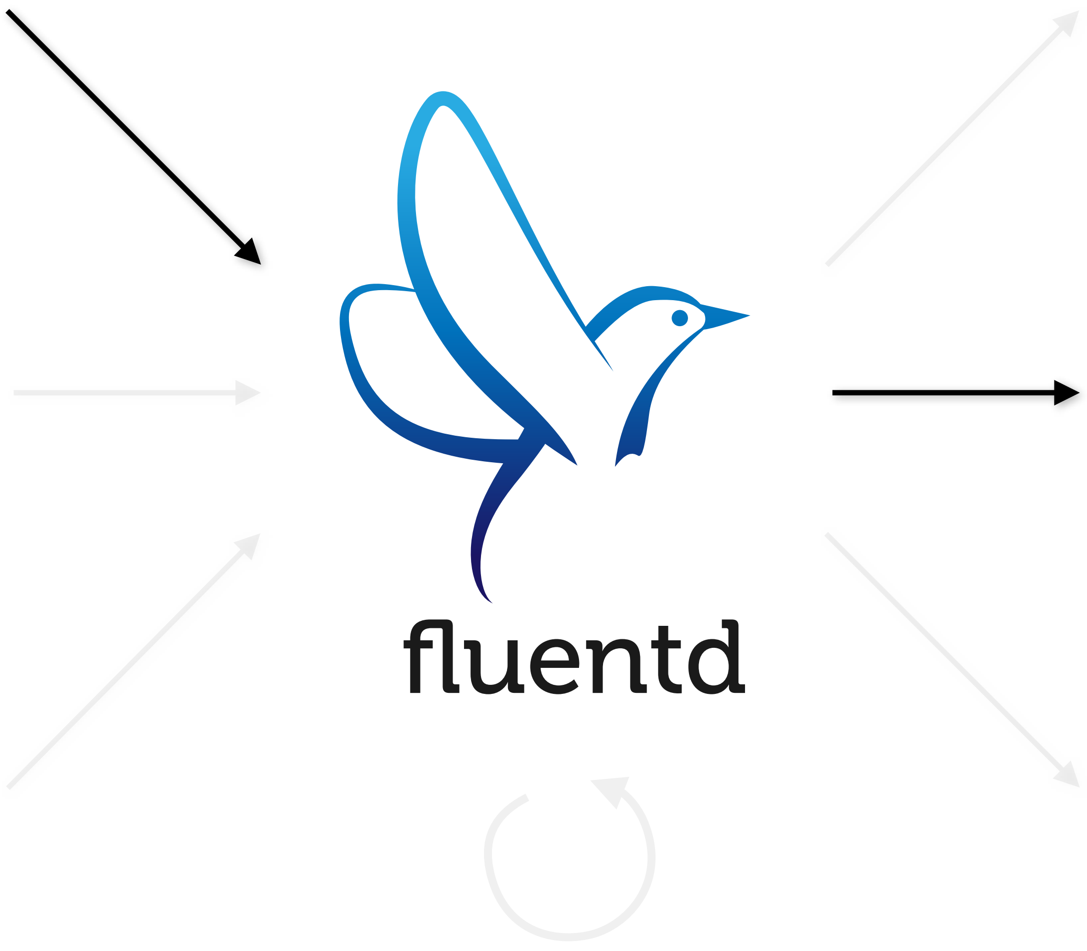
MongoDB

MySQL

Hadoop

Archiving

Amazon S3



Access logs

Apache

App logs

Frontend

Backend

System logs

syslogd

Databases

fluentd

filter / buffer / routing

Alerting

Nagios

Analysis

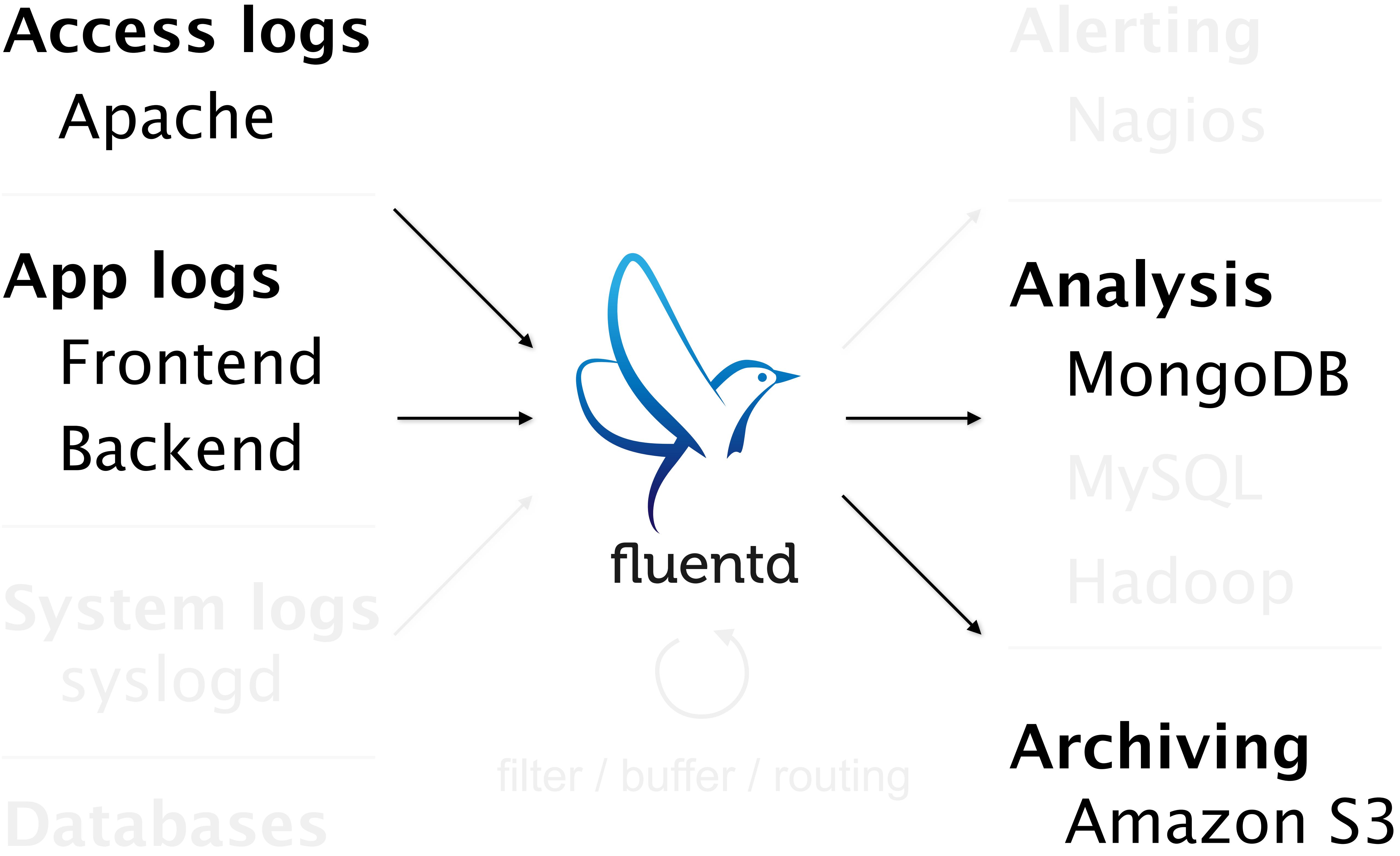
MongoDB

MySQL

Hadoop

Archiving

Amazon S3



Access logs

Apache

App logs

Frontend

Backend

System logs

syslogd

Databases

fluentd

filter / buffer / routing

Alerting

Nagios

Analysis

MongoDB

MySQL

Hadoop

Archiving

Amazon S3

td-agent

- Open sourced distribution package of fluentd
- ETL part of Treasure Data
- Including useful components
  - ruby, jemalloc, fluentd
  - 3rd party gems: td, mongo, webhdfs, etc...

    td plugin is for TD
- http://packages.treasure-data.com/

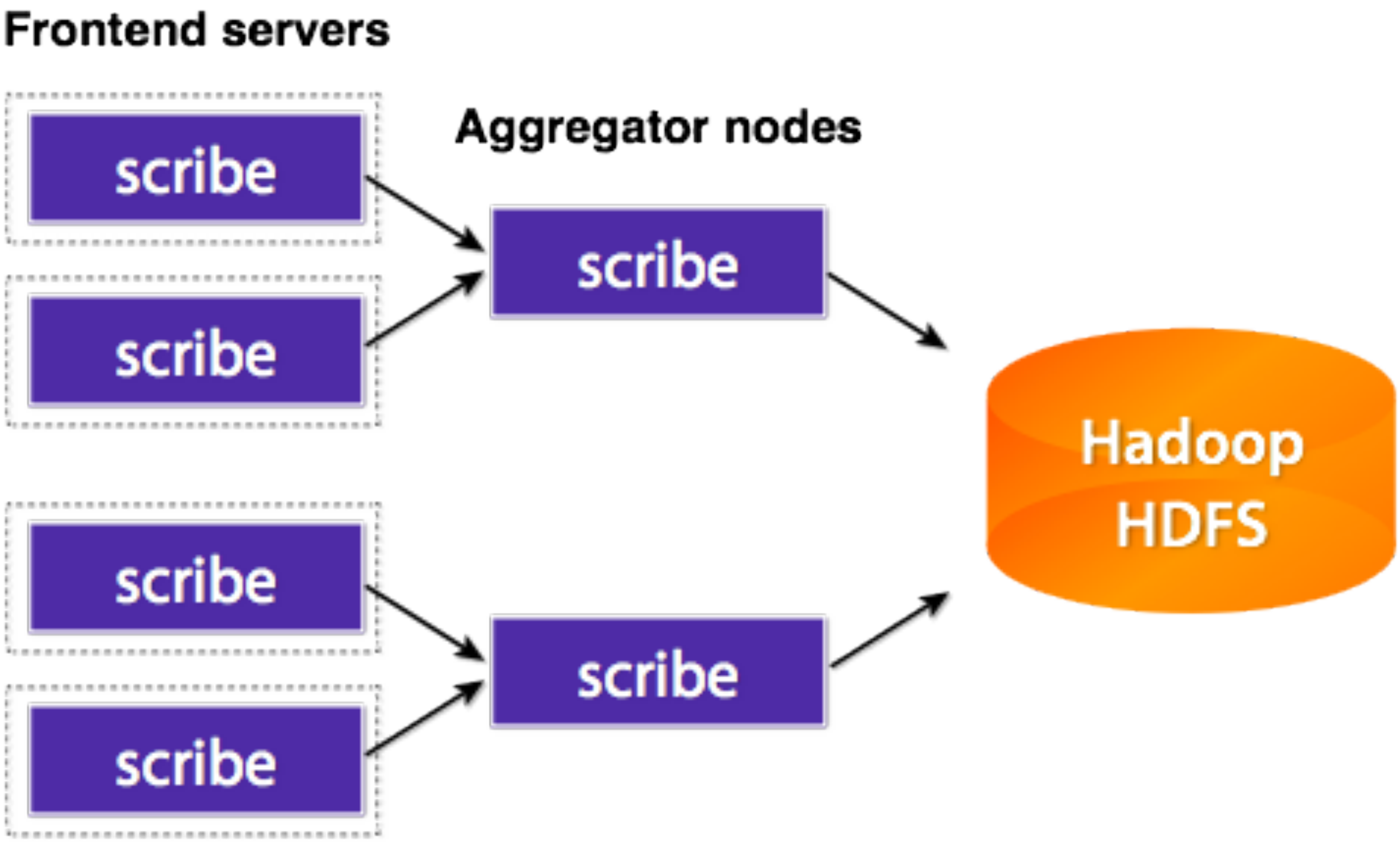
v11

- Breaking source code compatibility
  - Not protocol.
- Windows support
- Error handling enhancement
- Better DSL configuration
- etc: https://gist.github.com/frsyuki/2638703

Product Comparison

Scribe

Scribe: log collector by Facebook



Pros and Cons

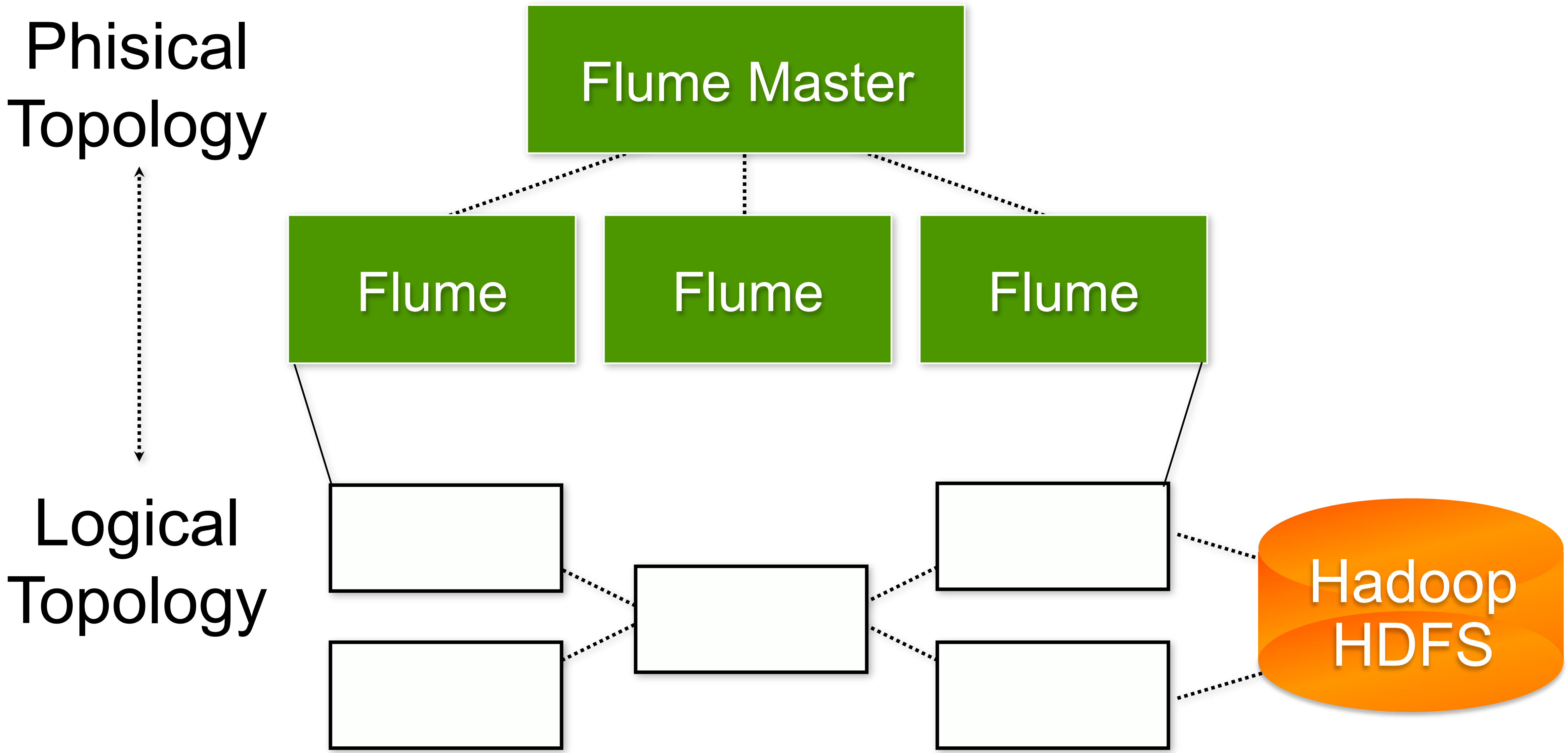
- Pros
  - Fast (written in C++)
- Cons
  - Hard to install and extend

    Are you a C++ magician?
  - Deal with unstructured logs
  - No longer maintained

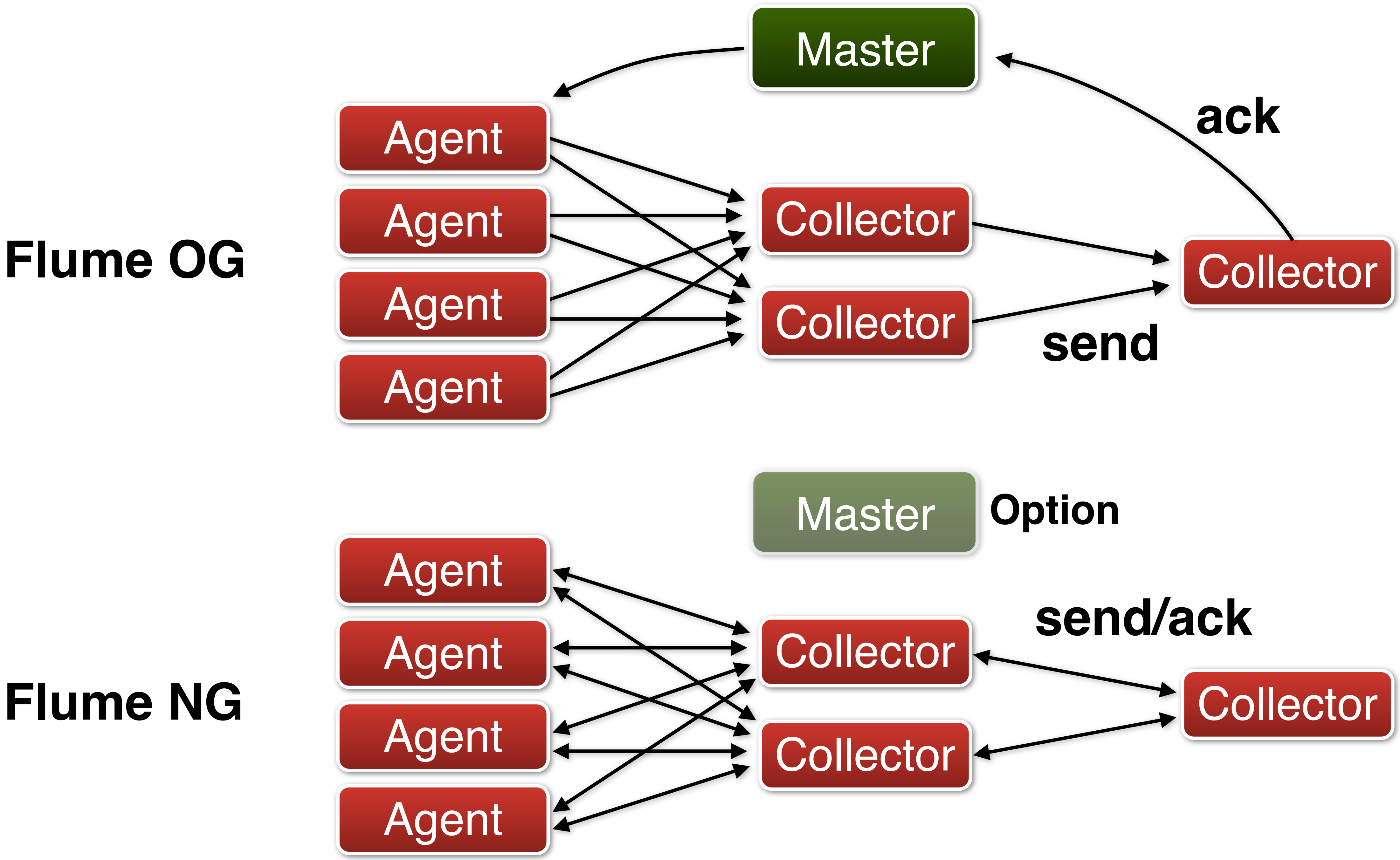
    Replaced with Calligraphus at Facebook

Flume

Flume: distributed log collector by Cloudera



Network topology



Pros and Cons

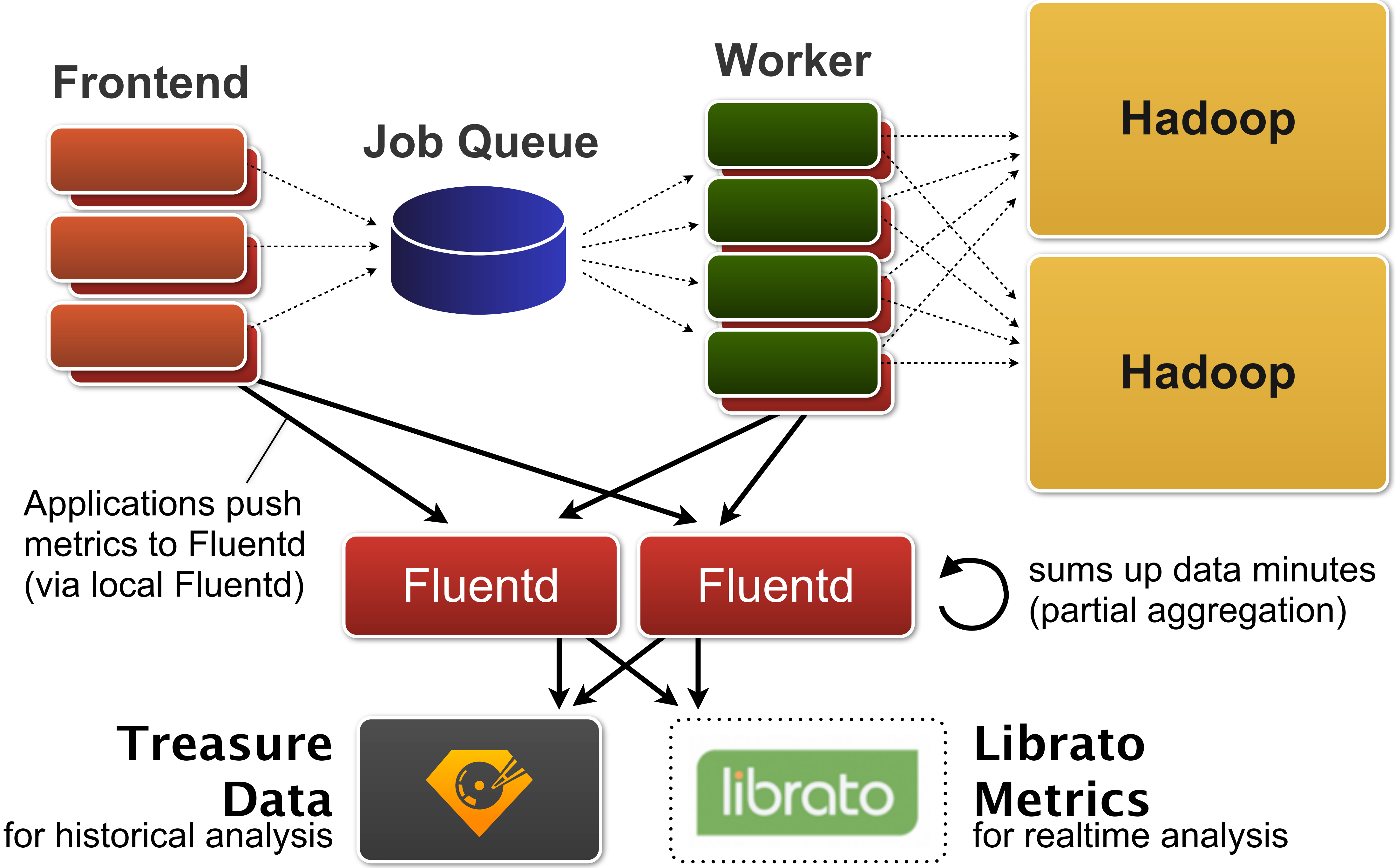
- Pros
  - Using central master to manage all nodes
- Cons
  - Java culture (Pros for Java-er?)

    Difficult configuration and setup
  - Difficult topology
  - Mainly for Hadoop

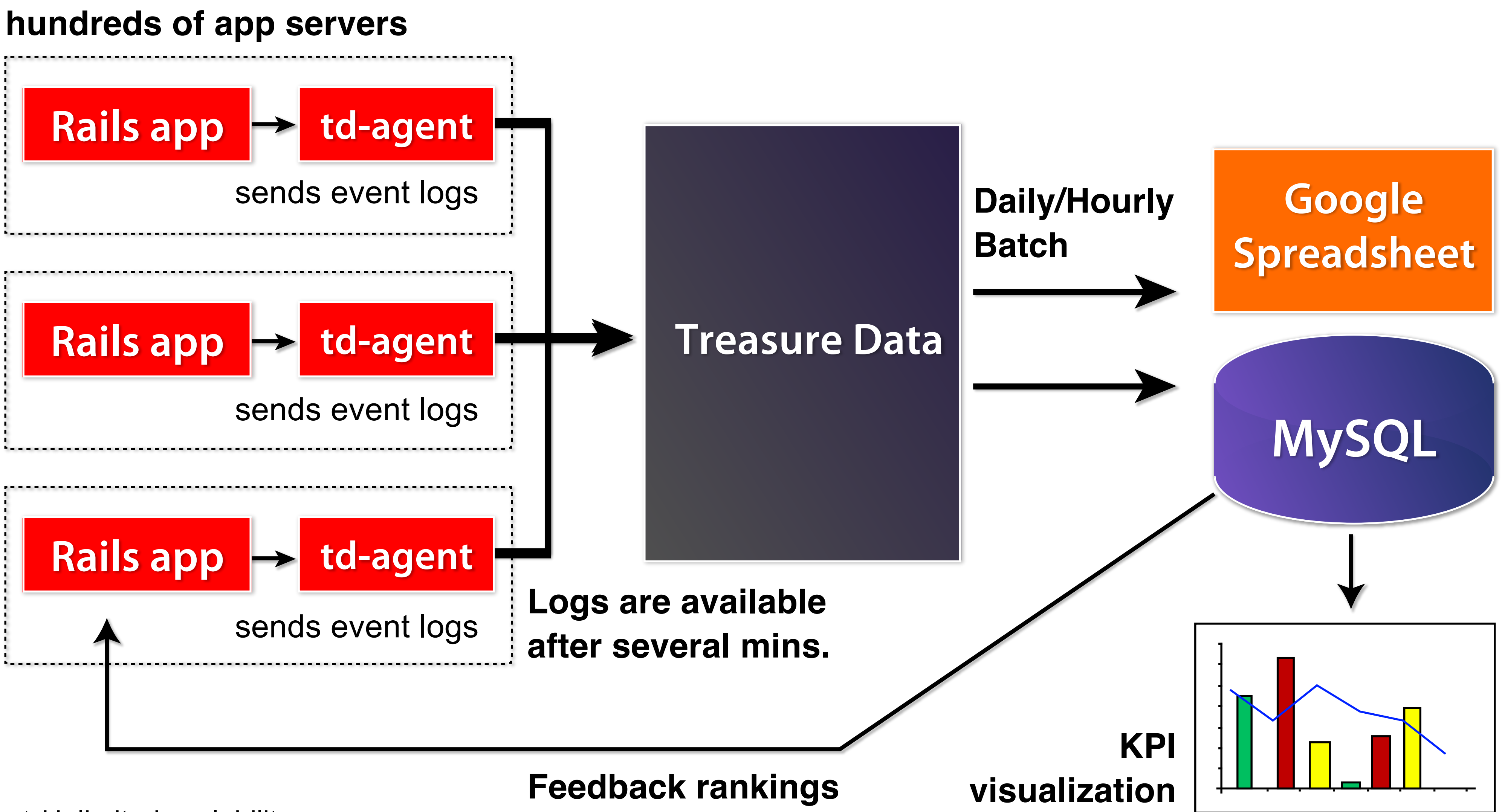
    less plugins?

Use cases

Treasure Data



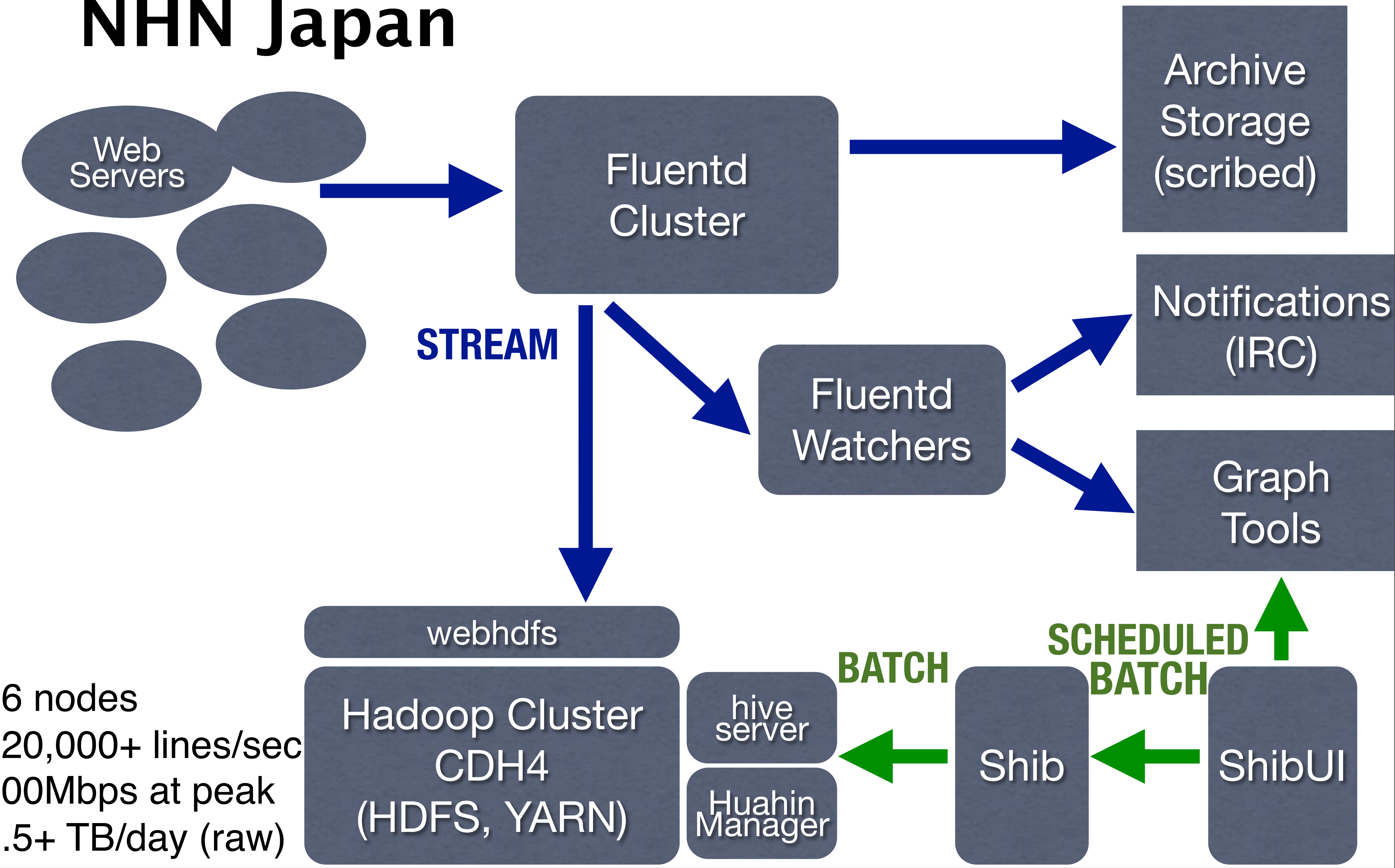
Cookpad



- ✓ Unlimited scalability
- ✓ Flexible schema
- ✓ Realtime
- ✓ Less performance impact

✓ Over 100 RoR servers (2012/2/4)

NHN Japan



- ✓ 16 nodes
- ✓ 120,000+ lines/sec
- ✓ 400Mbps at peak
- ✓ 1.5+ TB/day (raw)

http://www.slideshare.net/tagomoris/log-analysis-with-hadoop-in-livedoor-2013 by @tagomoris

Other companies

CyberAgent

BACKPLANE

slideshare
Present Yourself

ContextLogic

PPTV
每个人的网络电视

TREASURE DATA
BIG DATA AS A SERVICE

viki

GREE

Conclusion

- Fluentd is a widely-used log collector
  - There are many use cases
  - Many contributors and plugins
- Keep it simple
  - Easy to integrate your environment