Induction training of Dev Team

Just log

PuGong

Agenda

- What’s Log
- What should be logged
- How to use the log
- Examples of Log System
- Q&A

What’s Log

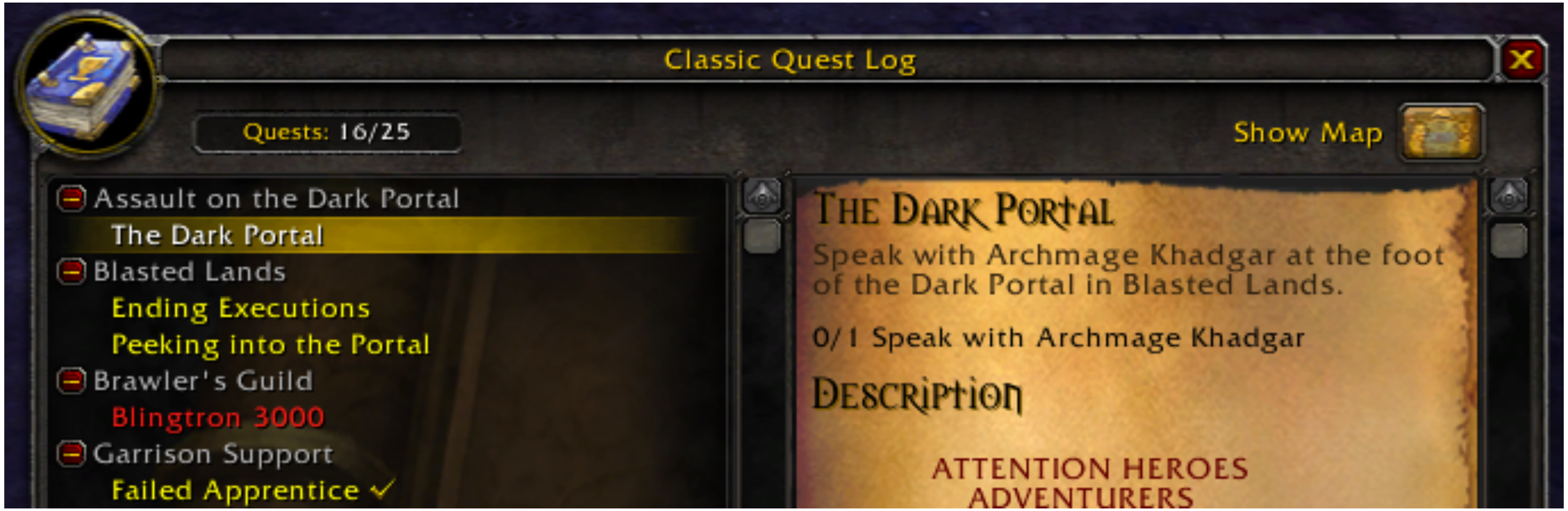
- a record of a journey made by a ship or aircraft, detailing all events, or the book in which it is kept
- (Computers) Any of various chronological records made concerning the use of a computer system, the changes made to data, etc.

- The logs are often met
  - Transaction Log／Binlog
  - Operation Log
  - Application Log

Are they log

- 编年史：（元年）夏，五月，郑伯克段于鄢。

- Black-box



Assault on the Dark Portal
The Dark Portal
Blasted Lands
Ending Executions
Peeking into the Portal
Brawler's Guild
Blingtron 3000
Garrison Support
Failed Apprentice ✓

THE DARK PORTAL

Speak with Archmage Khadgar at the foot of the Dark Portal in Blasted Lands.

0/1 Speak with Archmage Khadgar

DESCRIPTION

ATTENTION HEROES
ADVENTURERS

Key point of log

- Timestamp
- Sequence
- Meaningful
  - Format of records
  - Contents
- Immutable
- Structured vs Unstructured

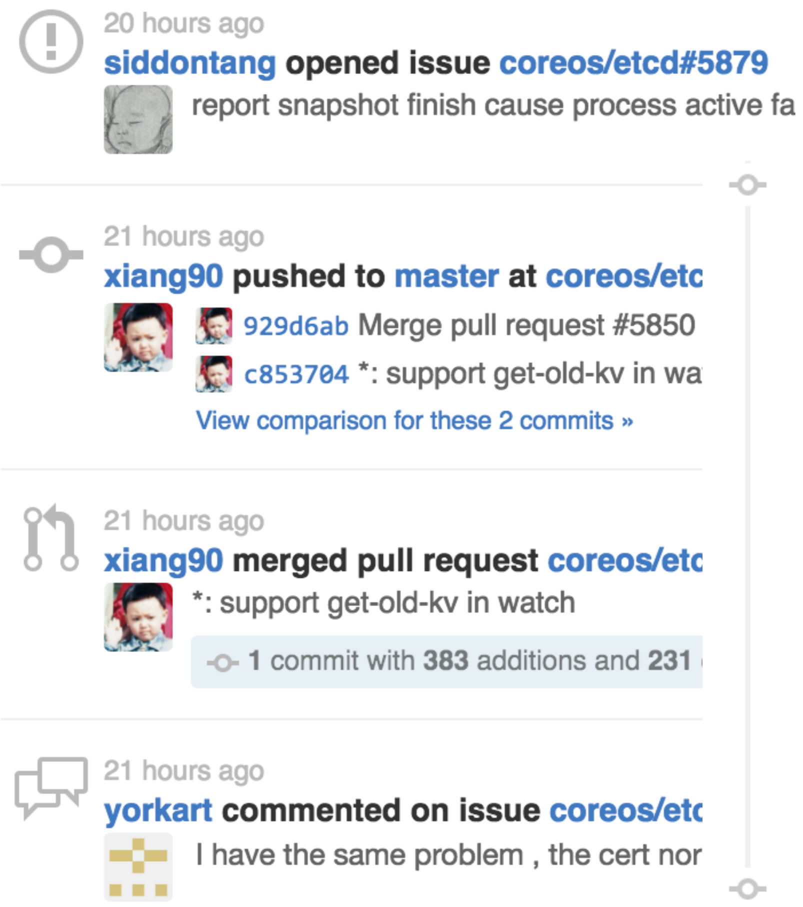
Why Log are important

- Compliance and regulations: Provide an audit trail of who, what, where, when and why
- Situational awareness
- Incident reponse
- Real time alerts

Operation log

- Purpose
  - Keep the track of what user had done
  - For AUDIT
  - For Track of record change
- Key elements
  - When - Timestamp
  - Who - User
  - What - what was did
  - Where - IP/Host
  - Identifier - Table(moudle) Name, record_id

Sample of Op

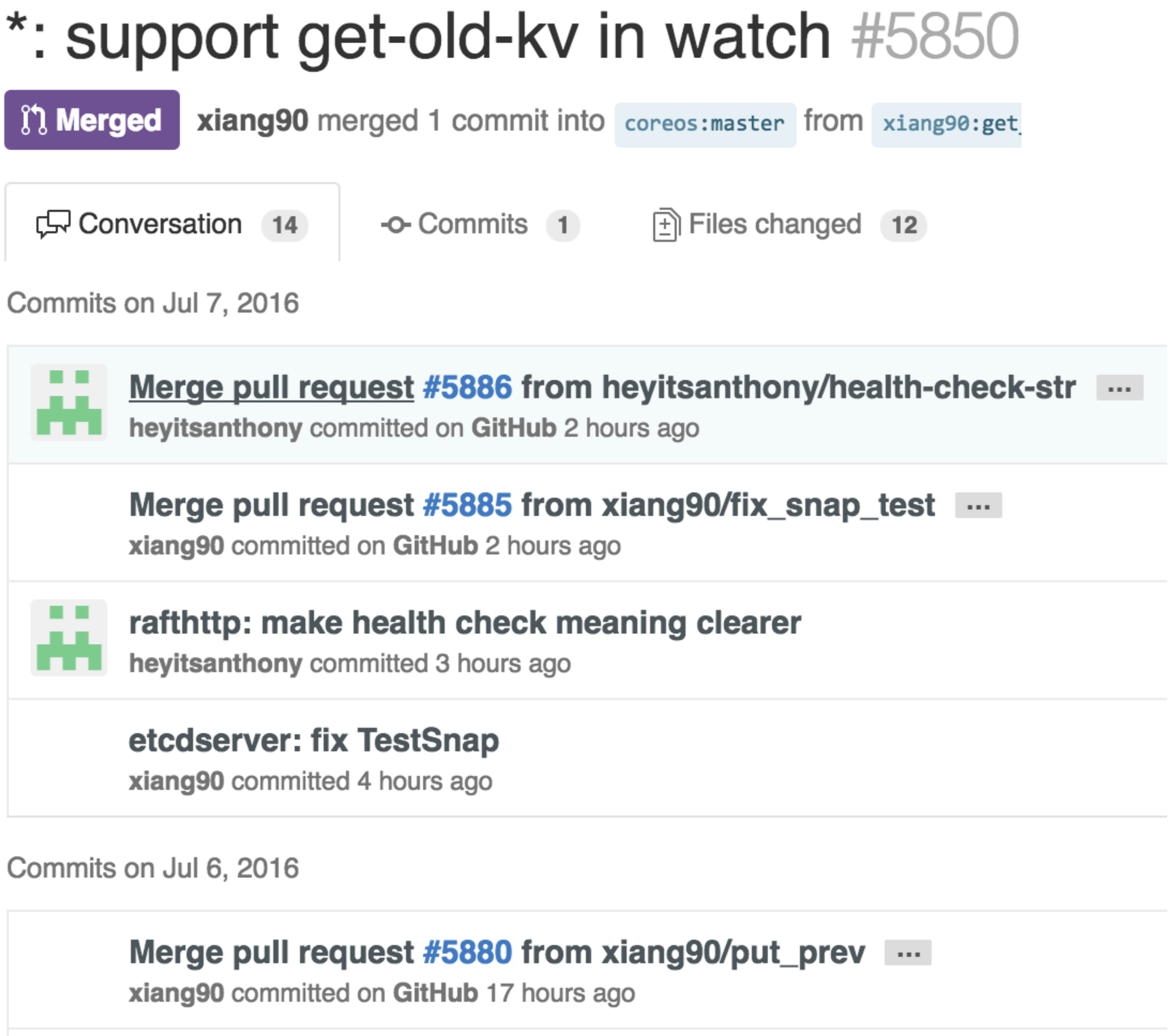


20 hours ago
siddontang opened issue coreos/etcd#5879
report snapshot finish cause process active fa

21 hours ago
xiang90 pushed to master at coreos/etc
929d6ab Merge pull request #5850
c853704 *: support get-old-kv in wa
View comparison for these 2 commits »

21 hours ago
xiang90 merged pull request coreos/etc
*: support get-old-kv in watch
1 commit with 383 additions and 231

21 hours ago
yorkart commented on issue coreos/etc
I have the same problem , the cert nor



*: support get-old-kv in watch #5850

Merged xiang90 merged 1 commit into coreos:master from xiang90:get

Commits on Jul 7, 2016

Merge pull request #5886 from heyitsanthony/health-check-str ...
heyitsanthony committed on GitHub 2 hours ago

Merge pull request #5885 from xiang90/fix_snap_test ...
xiang90 committed on GitHub 2 hours ago

rafthttp: make health check meaning clearer
heyitsanthony committed 3 hours ago

etcdserver: fix TestSnap
xiang90 committed 4 hours ago

Commits on Jul 6, 2016

Merge pull request #5880 from xiang90/put_prev ...
xiang90 committed on GitHub 17 hours ago

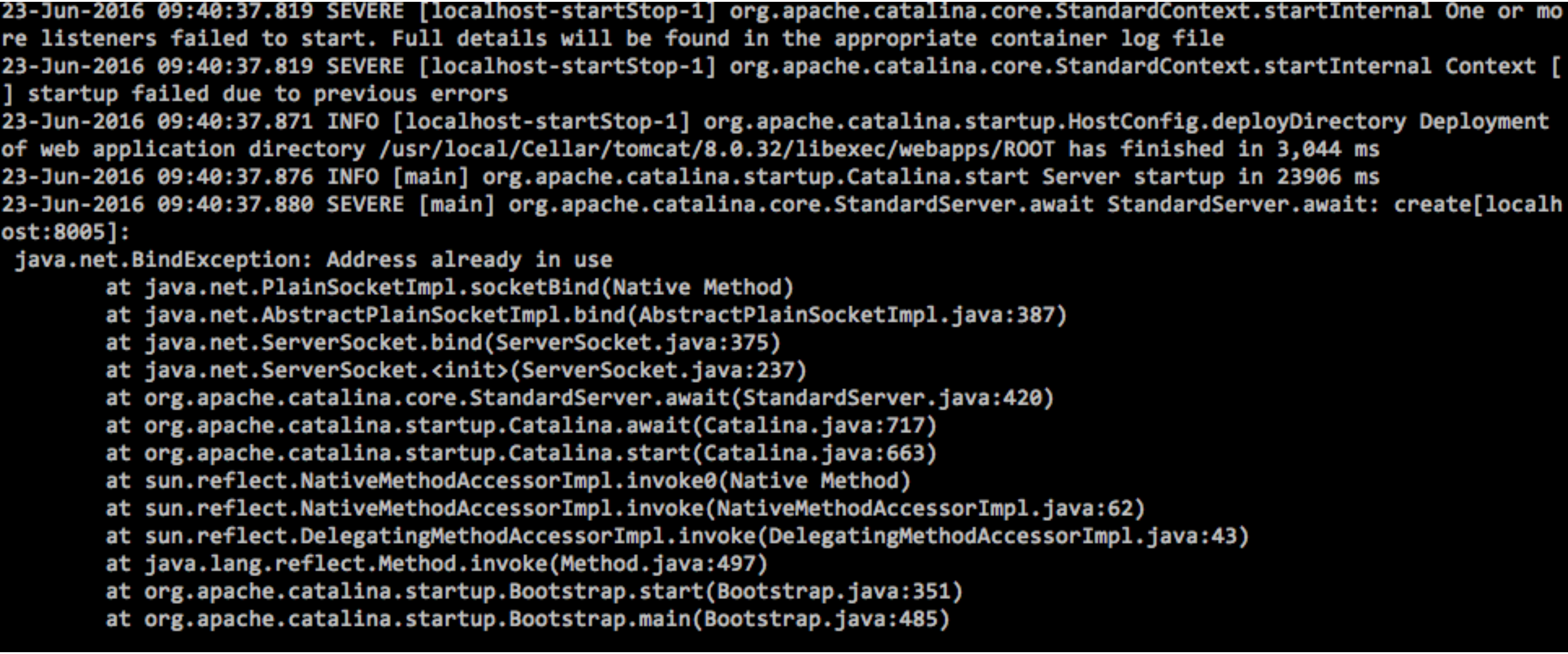
Application log

- Purpose
  - Keep necessary application running information
  - For online problem analysis
  - For debug
- Key elements
  - When - Timestamp
  - What
    - Log Level
    - (Error) Message
    - Stacktrace
  - Where – Host/IP
  - Secure – remove sensitive information
  - Centralize

Log Level

- Debug: Used only for development and testing. Temporary open on production to find more information. (Caution with the log size)
- Information: Used to keep the information that is useful for system running and management. The entry and exit points of key functions should be kept in this level.
- Warning: Used to keep the handled exceptions or other important log events.
- Error: Used to keep the unhandled exceptions
- Fatal: Reserved for special exceptions/conditions that need to be taken care of.

Sample of Application Log

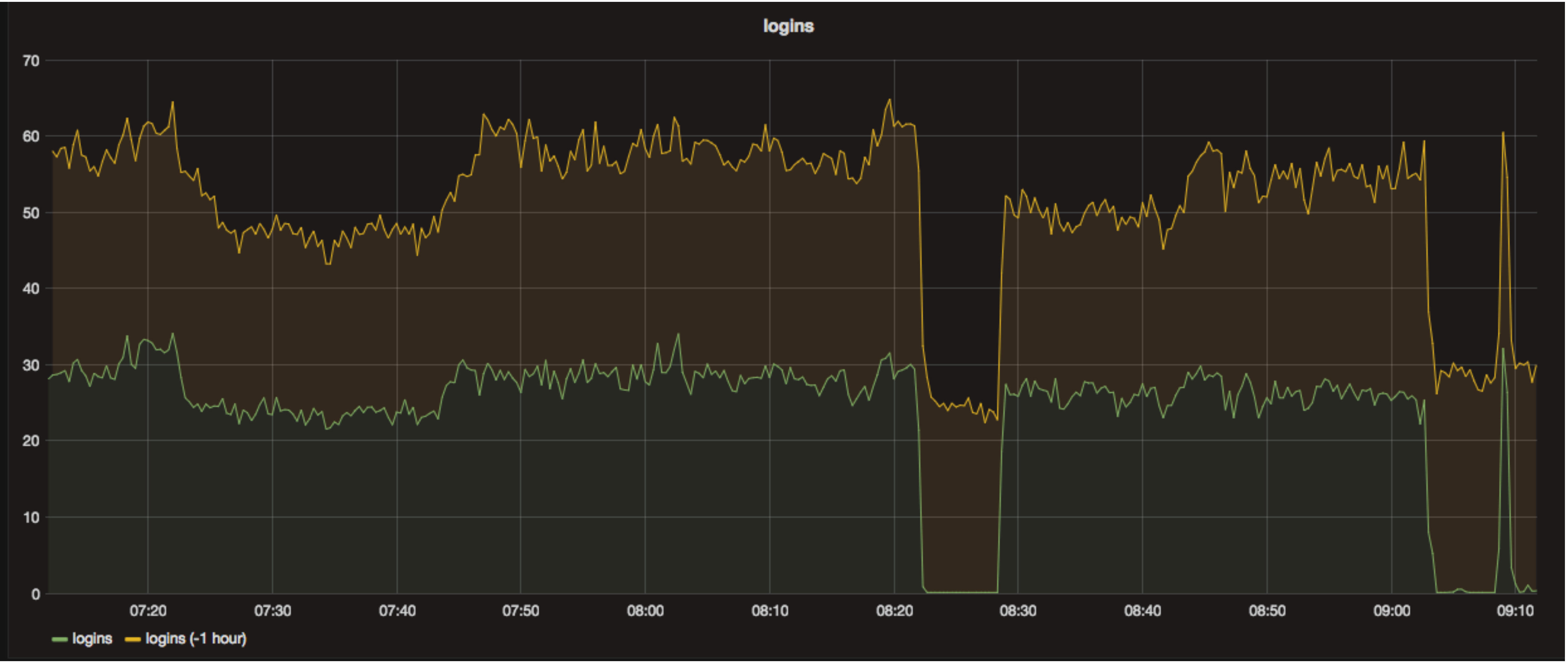


```
23-Jun-2016 09:40:37.819 SEVERE [localhost-startStop-1] org.apache.catalina.core.StandardContext.startInternal One or mo
re listeners failed to start. Full details will be found in the appropriate container log file
23-Jun-2016 09:40:37.819 SEVERE [localhost-startStop-1] org.apache.catalina.core.StandardContext.startInternal Context [
] startup failed due to previous errors
23-Jun-2016 09:40:37.871 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDirectory Deployment
of web application directory /usr/local/Cellar/tomcat/8.0.32/libexec/webapps/ROOT has finished in 3,044 ms
23-Jun-2016 09:40:37.876 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in 23906 ms
23-Jun-2016 09:40:37.880 SEVERE [main] org.apache.catalina.core.StandardServer.await StandardServer.await: create[localh
ost:8005]:
 java.net.BindException: Address already in use
	at java.net.PlainSocketImpl.socketBind(Native Method)
	at java.net.AbstractPlainSocketImpl.bind(AbstractPlainSocketImpl.java:387)
	at java.net.ServerSocket.bind(ServerSocket.java:375)
	at java.net.ServerSocket.<init>(ServerSocket.java:237)
	at org.apache.catalina.core.StandardServer.await(StandardServer.java:420)
	at org.apache.catalina.startup.Catalina.await(Catalina.java:717)
	at org.apache.catalina.startup.Catalina.start(Catalina.java:663)
	at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
	at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
	at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
	at java.lang.reflect.Method.invoke(Method.java:497)
	at org.apache.catalina.startup.Bootstrap.start(Bootstrap.java:351)
	at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:485)
```

How to log - Metric log

- Purpose
  - Keep Application running stat, mainly numbers about business
  - Monitor
  - Alert
- Key element
  - When – Timestamp
  - Who – App Identifier
  - Where – Host/IP/Tags
  - What - Metrics

Sample of Metric Log



How to log - Trace Log

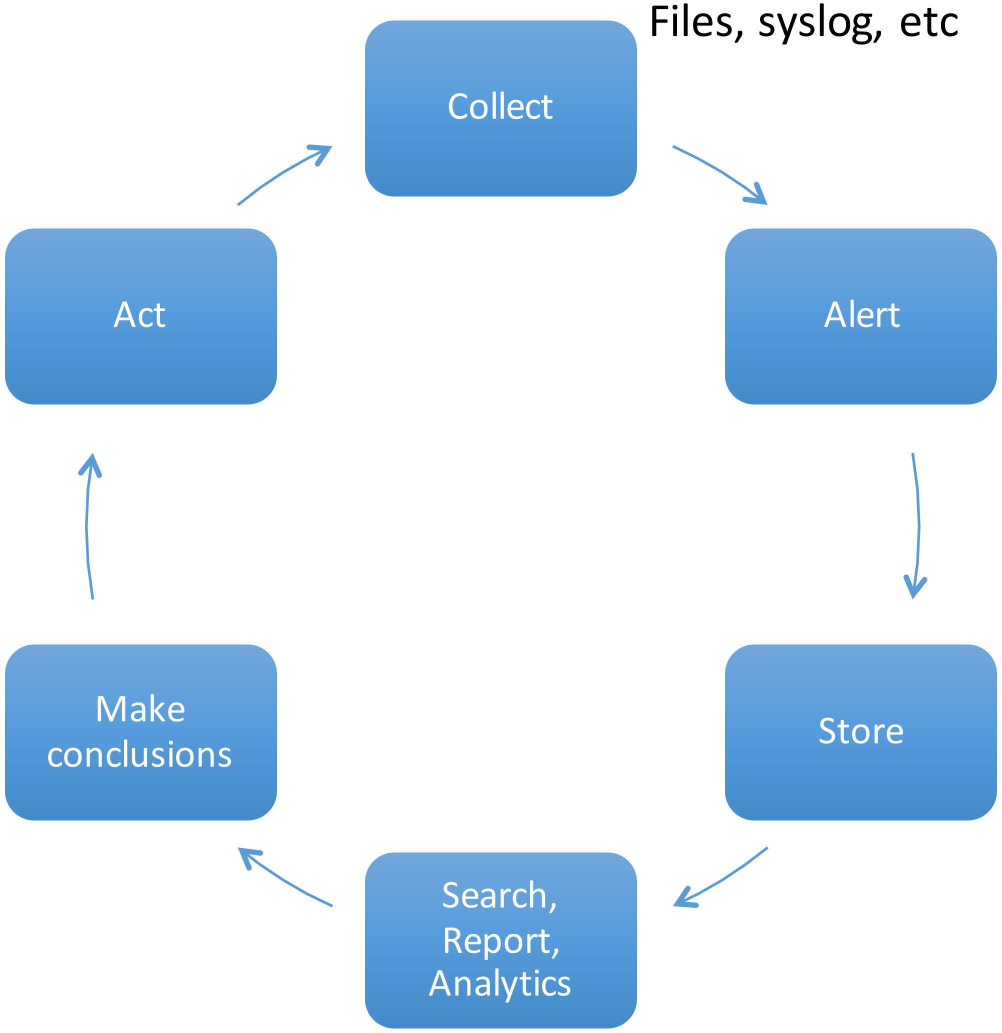
- Purpose
  - An unique Id to link the logs in different application
    - Generated at the very beginning at the request
    - Save in every logs as a field or a tag
  - Online problem analysis
  - User behavior tracking
- Key Elements
  - What – unique tracke Id in other log
  - Others – almost the same as

How to use the logs

- Metrics for monitor and alert
- Where alerts rings, go to application log for detail information
- Use trace to find association logs in other app is necessary

- Prediction

How to use logs



Files, syslog, etc

SMS, E-mail, etc

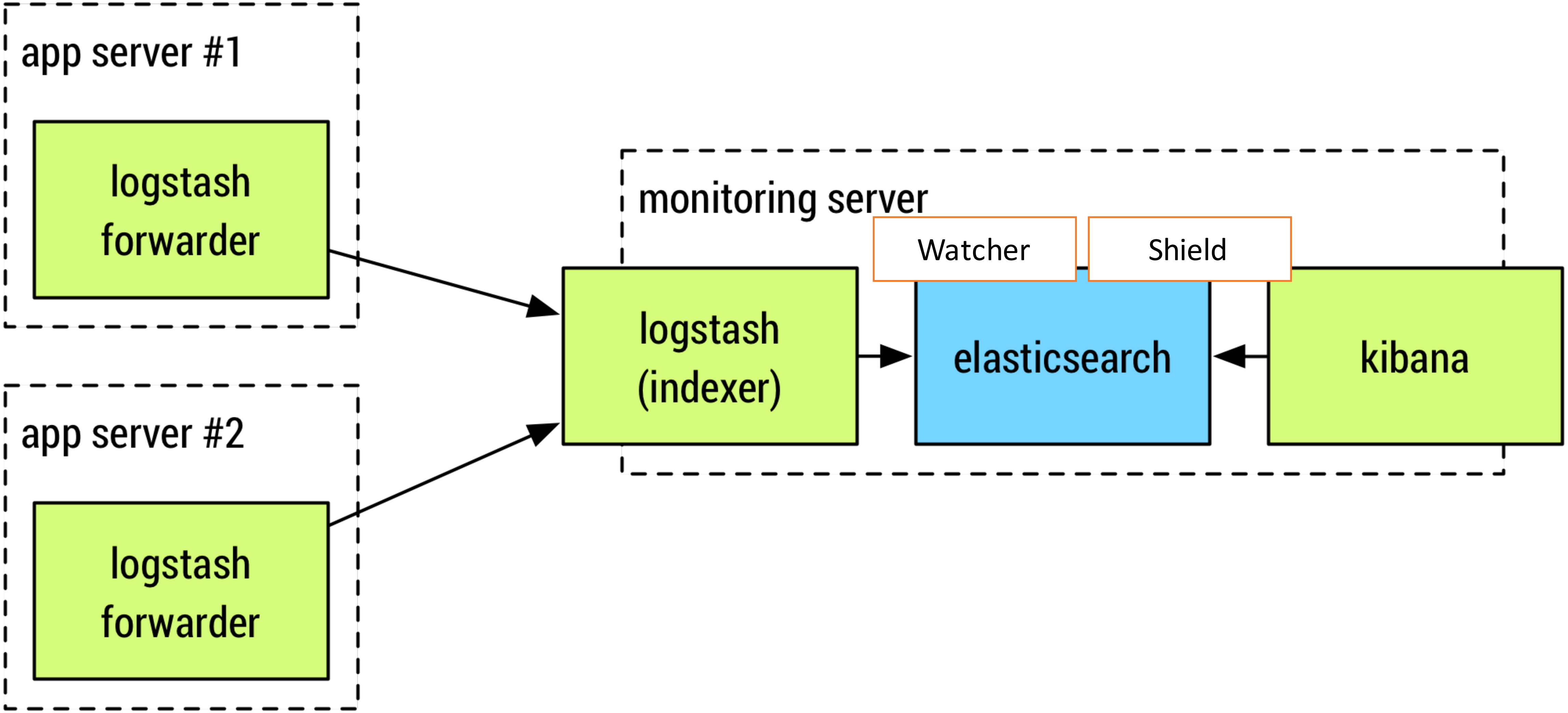
Immutable logs

Humans needed!

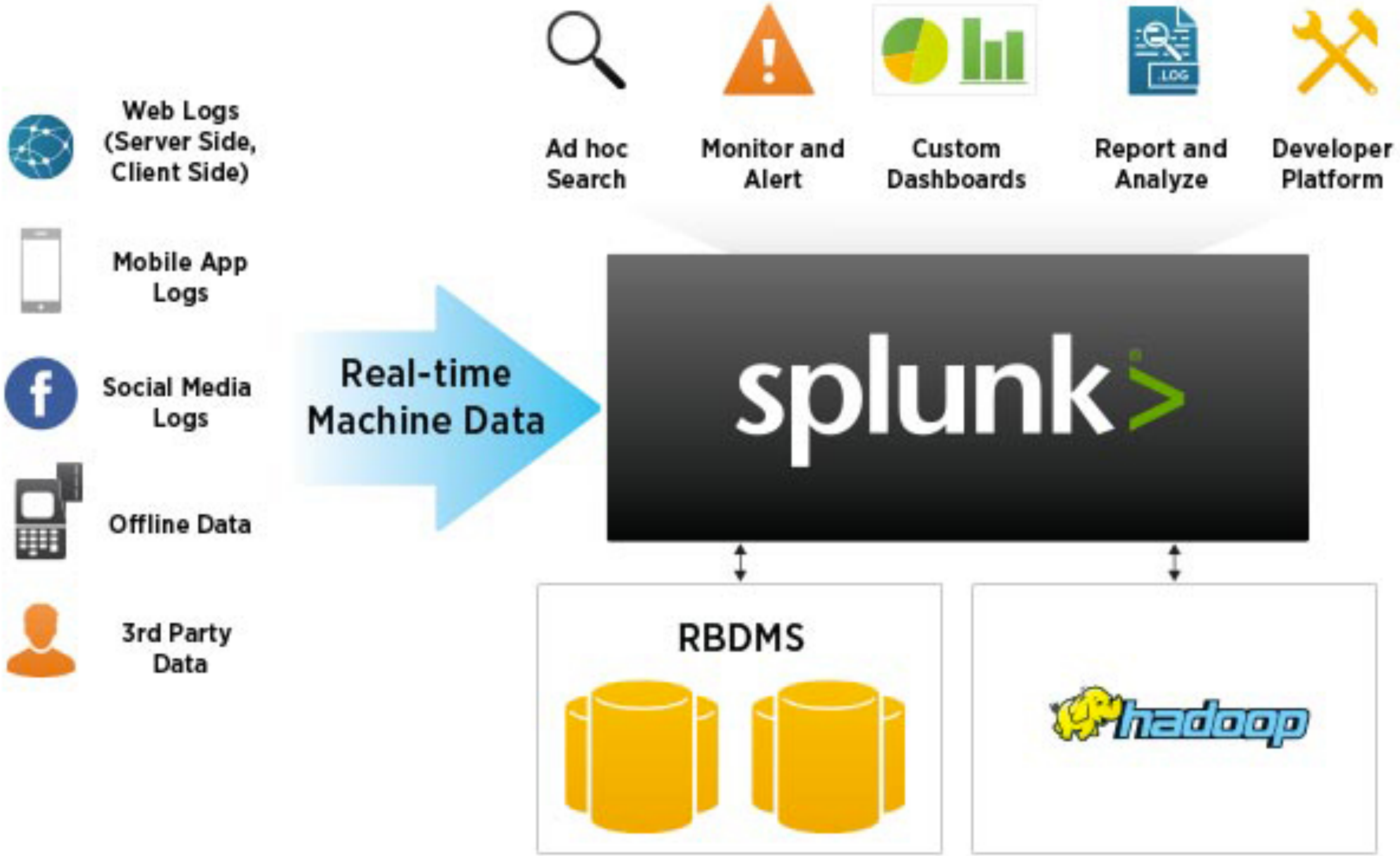
Log System

- ELK – Metrics, application log etc
- Statsd+Grafana / statsd + graphite – Metrics
- Splunk – commercial
- Customized

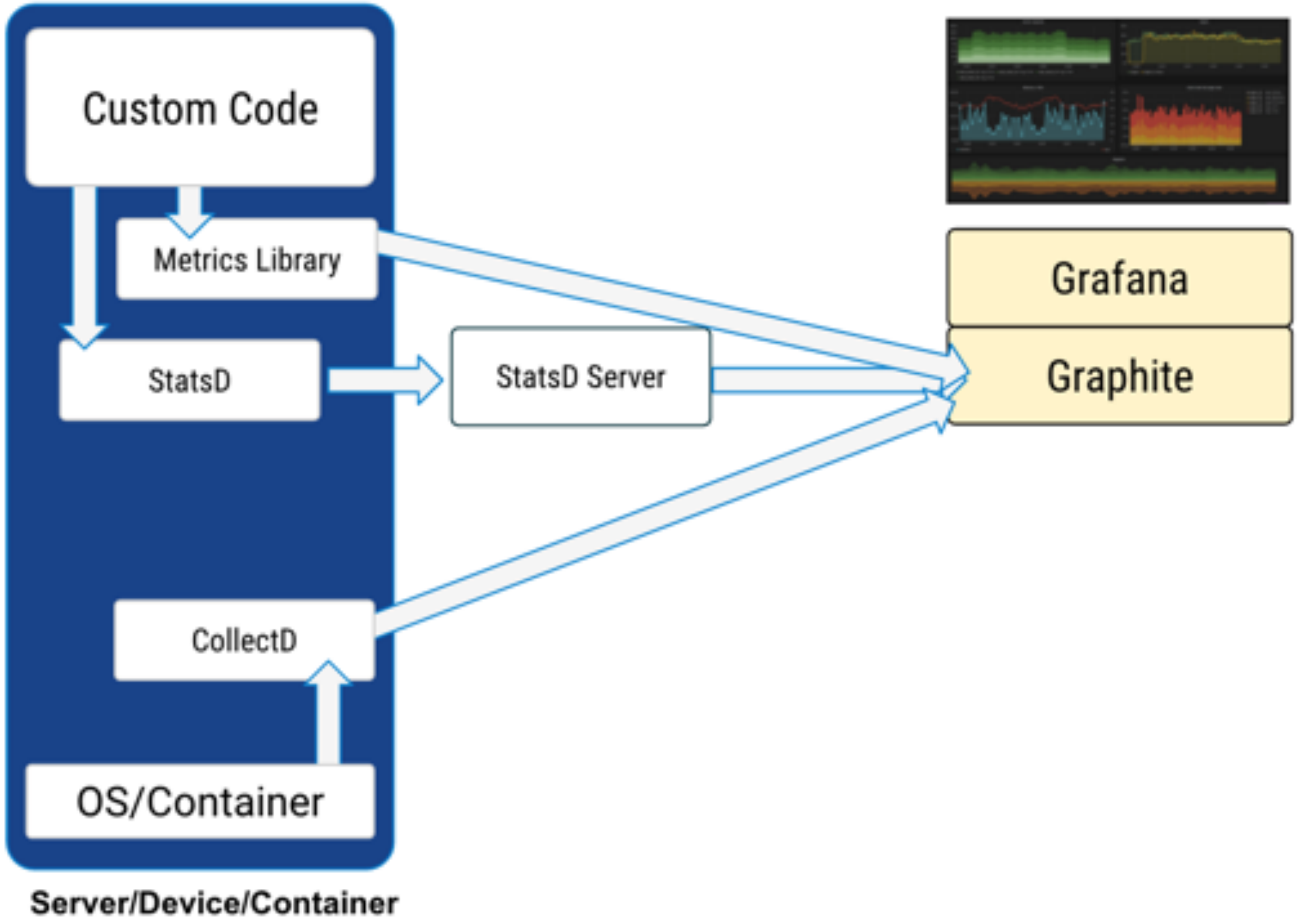
ELK


app server #1
logstash forwarder
app server #2
logstash forwarder
monitoring server
Watcher
Shield
logstash (indexer)
elasticsearch
kibana

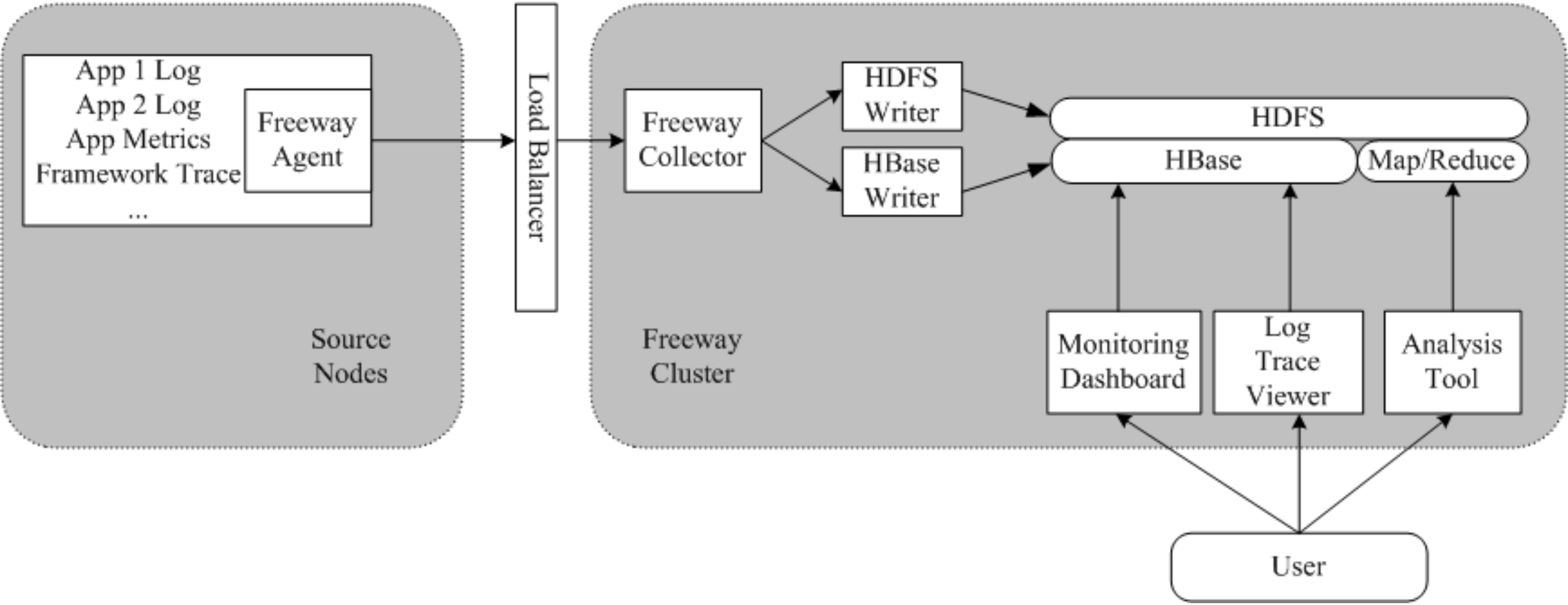
Splunk


Web Logs (Server Side, Client Side)
Mobile App Logs
Social Media Logs
Offline Data
3rd Party Data
Real-time Machine Data
Ad hoc Search
Monitor and Alert
Custom Dashboards
Report and Analyze
Developer Platform
splunk>
RBDMS
hadoop

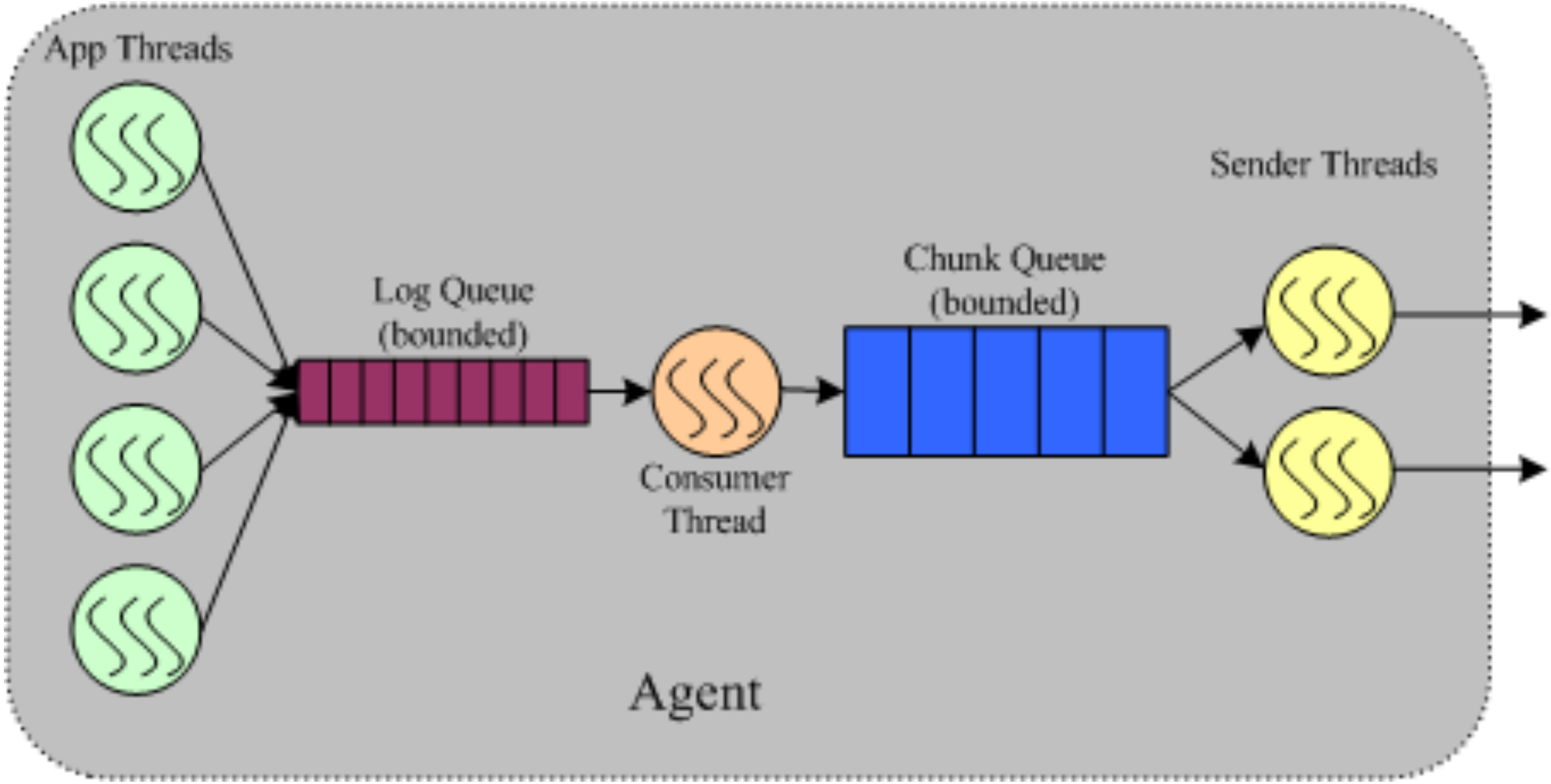
StatSD + Grafana



A Custimized Log system architecture



Log agent



App Threads
Log Queue (bounded)
Consumer Thread
Chunk Queue (bounded)
Sender Threads
Agent

Sum Up

- Careful choose log level
- Centralize the logs
- Secure the logs

- Do Log
- Do Use the log:
  - Monitor & Alert
  - Analysis the logs

Reference

- The Log: What every software engineer should know about real-time data's unifying abstraction
- 日志：每个软件工程师都应该知道的有关实时数据的统一概念
- Log Everything All The Time
- http://play.grafana.org/
- Elastic Search, Logstash & Kibana
- Splunk: http://www.splunk.com/
- Zabbix: https://www.zabbix.com/
- Cacti: http://cacti.net/
- nagios: https://www.nagios.org/