大数据监控告警系统

__author__: 汤英康
__company__: 优亿科技

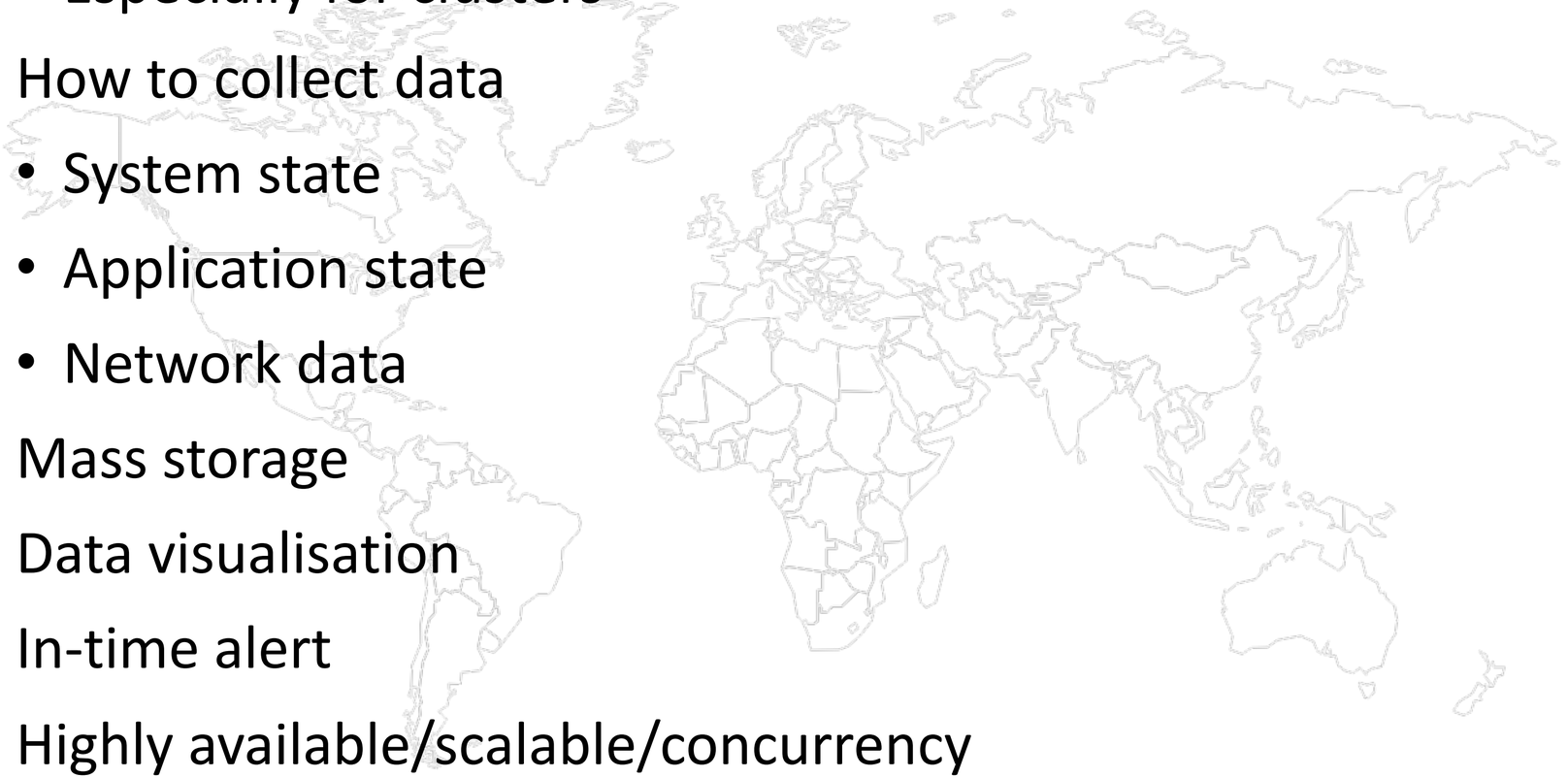
Agenda

- Background
- Architecture Road
  - Storage
  - Collector
  - Task Queue
  - API Server
  - Visualization
  - Alert
- Technology Selection

Background

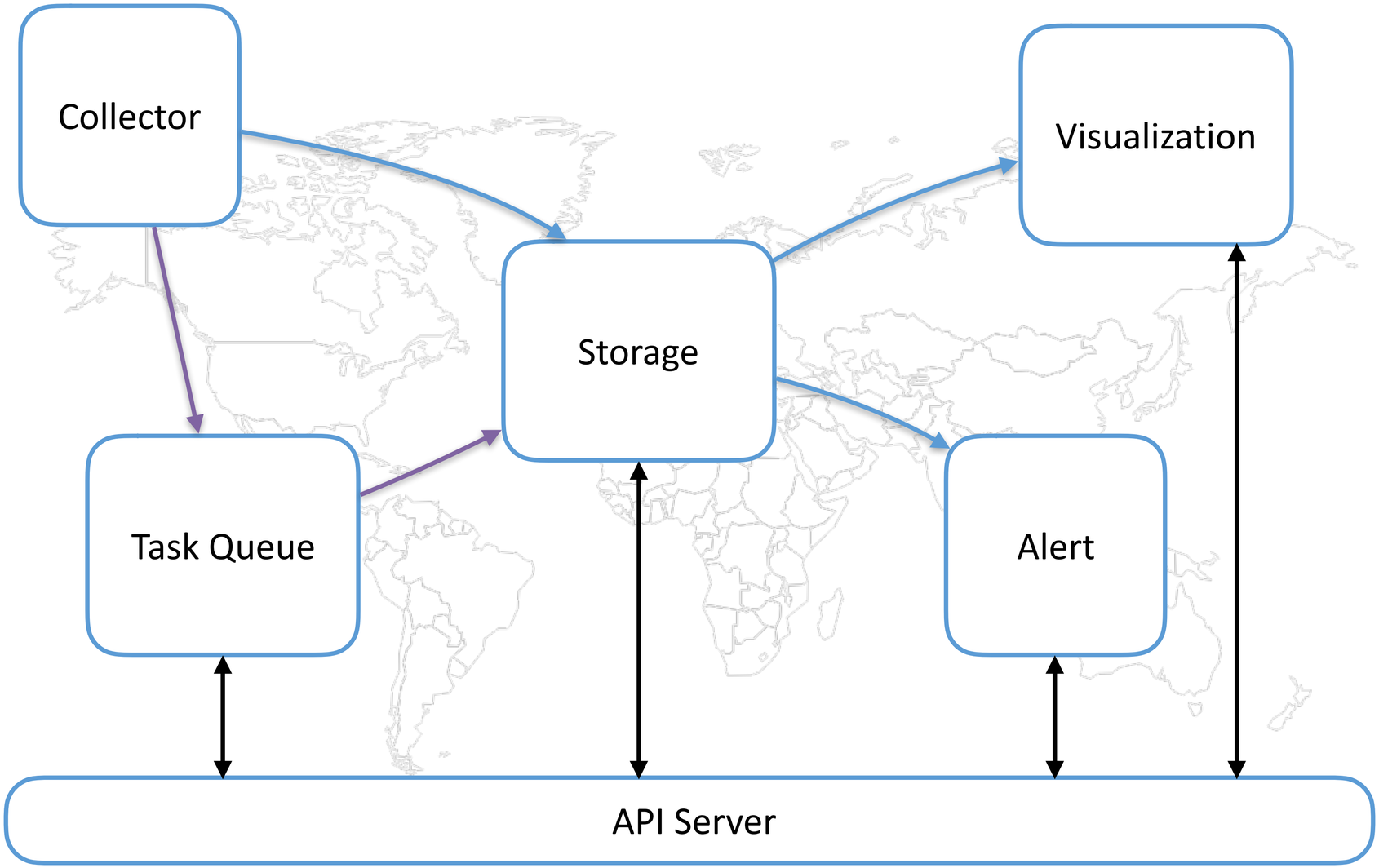
PyCon 2016 CHINA

- Significance of monitor
  - Especially for clusters
- How to collect data
  - System state
  - Application state
  - Network data
- Mass storage
- Data visualisation
- In-time alert
- Highly available/scalable/concurrency



So…

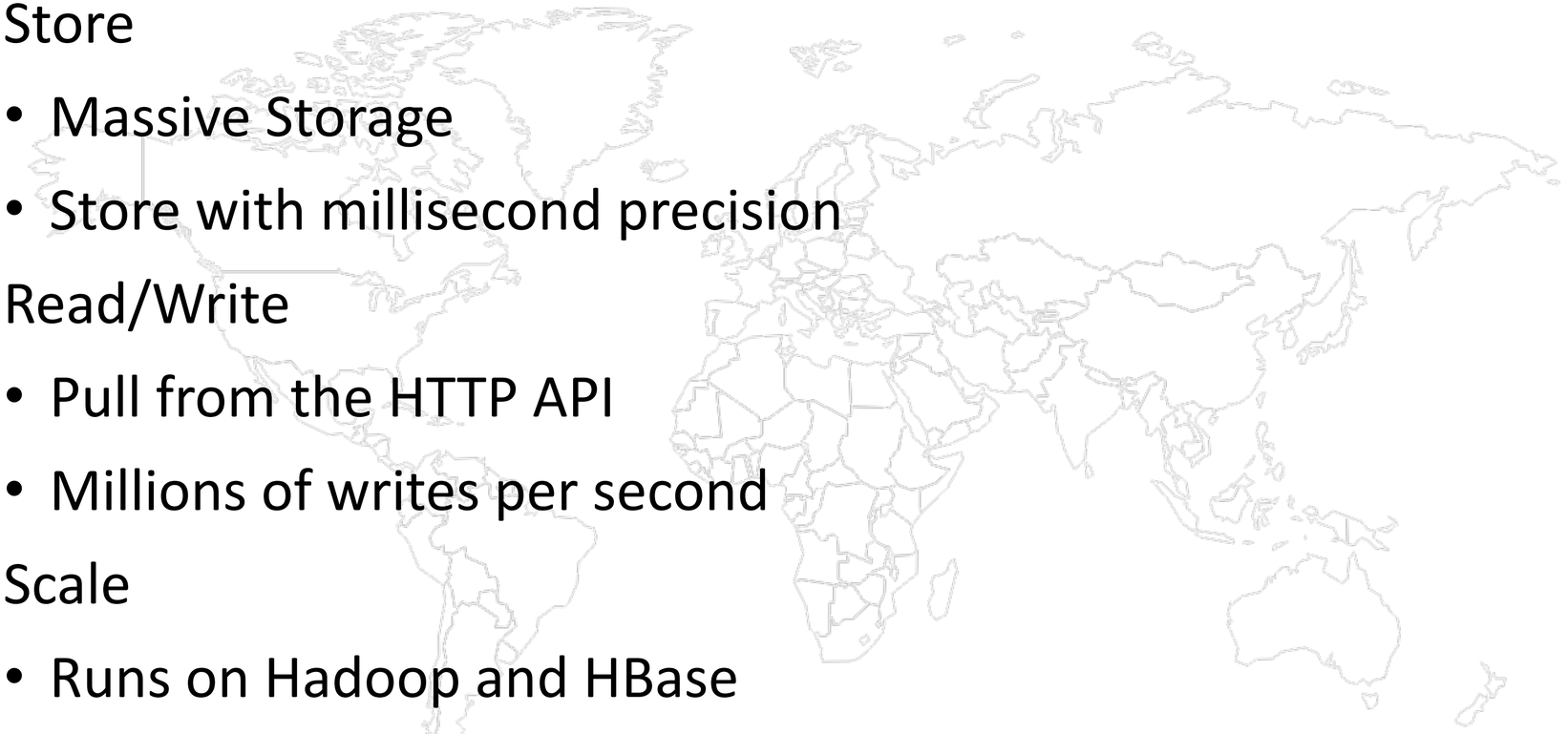
Architecture



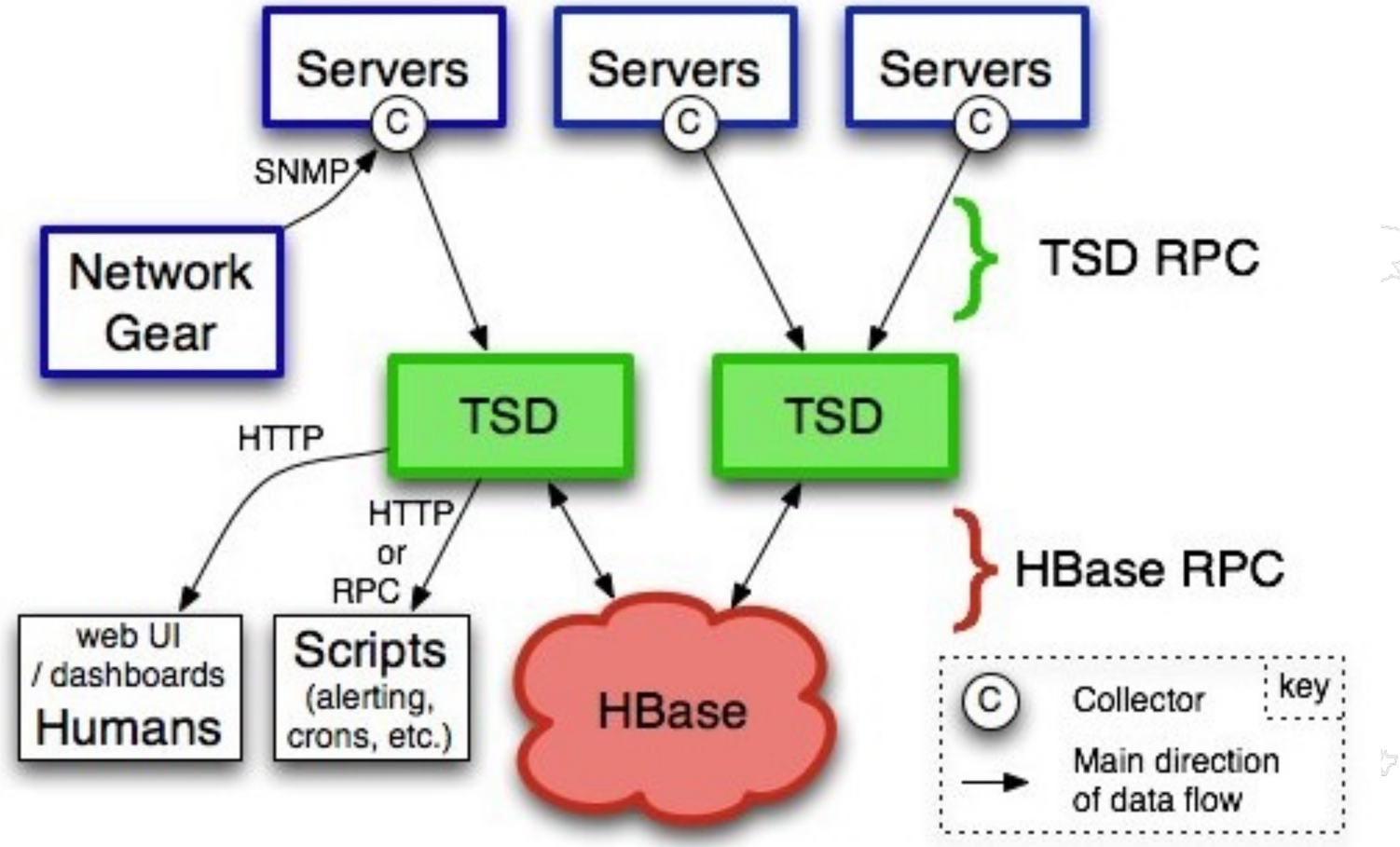
Storage - OpenTSDB

OpenTSDB

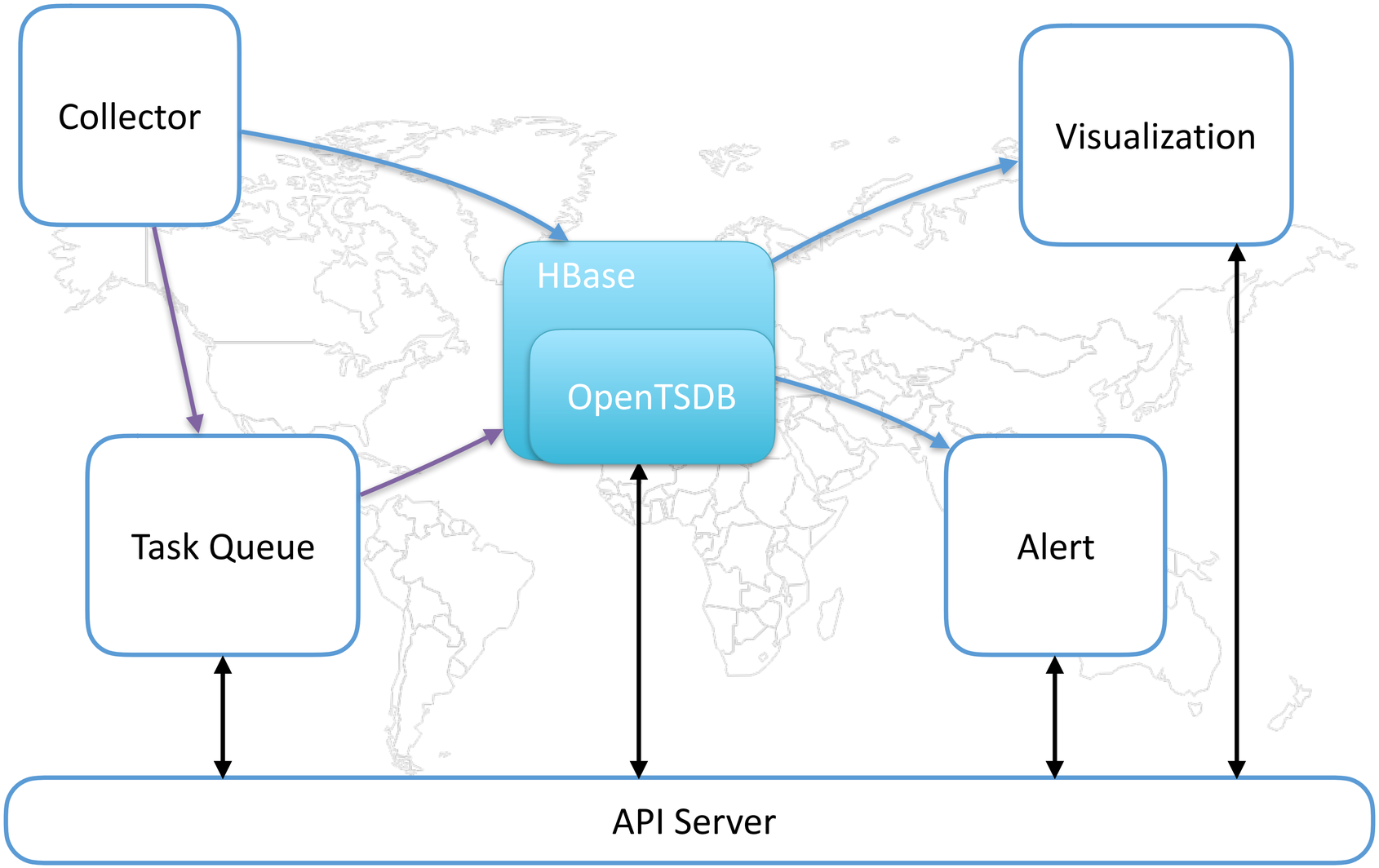
- Distributed, scalable Time Series Database (TSDB) written on top of HBase
- Store
  - Massive Storage
  - Store with millisecond precision
- Read/Write
  - Pull from the HTTP API
  - Millions of writes per second
- Scale
  - Runs on Hadoop and HBase
  - Add capacity by adding nodes



- OpenTSDB


Servers
C
Servers
C
Servers
C
SNMP
Network Gear
TSD RPC
TSD
TSD
HTTP
HTTP or RPC
HBase RPC
web UI / dashboards
Humans
Scripts (alerting, crons, etc.)
HBase
C
Collector
key
Main direction of data flow

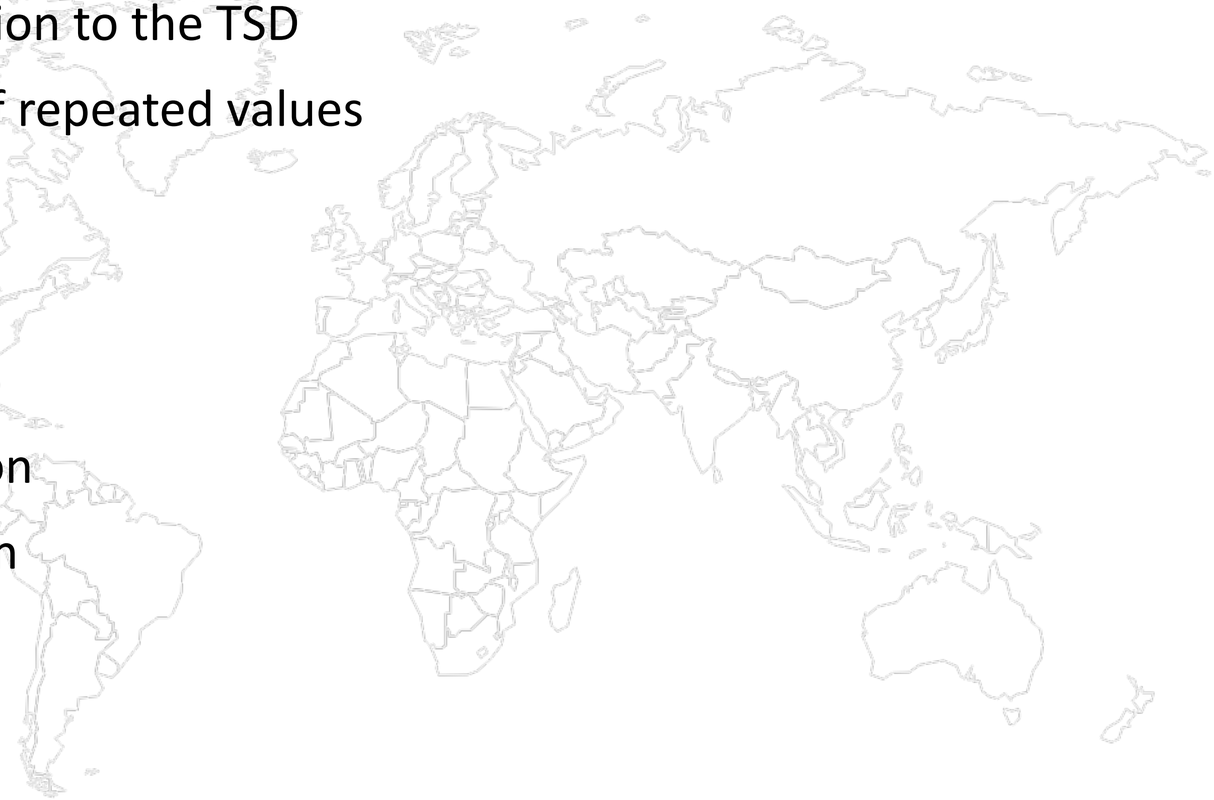
Architecture



Collector - TCollector

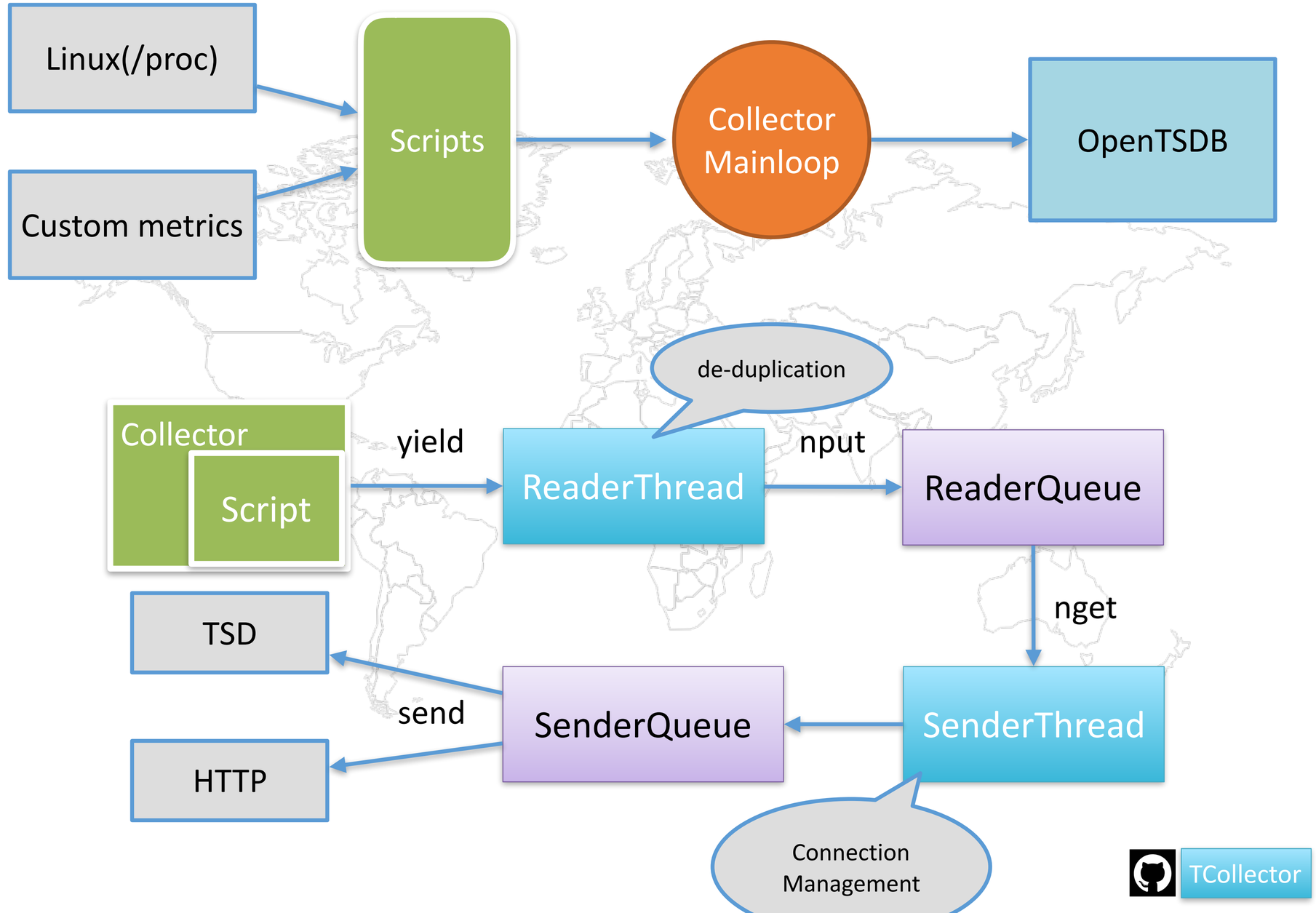
Collector

- TCollector(python)
  - Run collector scripts and gather their data
  - Manage connection to the TSD
  - De-duplication of repeated values
- What we do…
  - Reconstruction
  - Proxy support
  - User authorization
  - Celery Integration

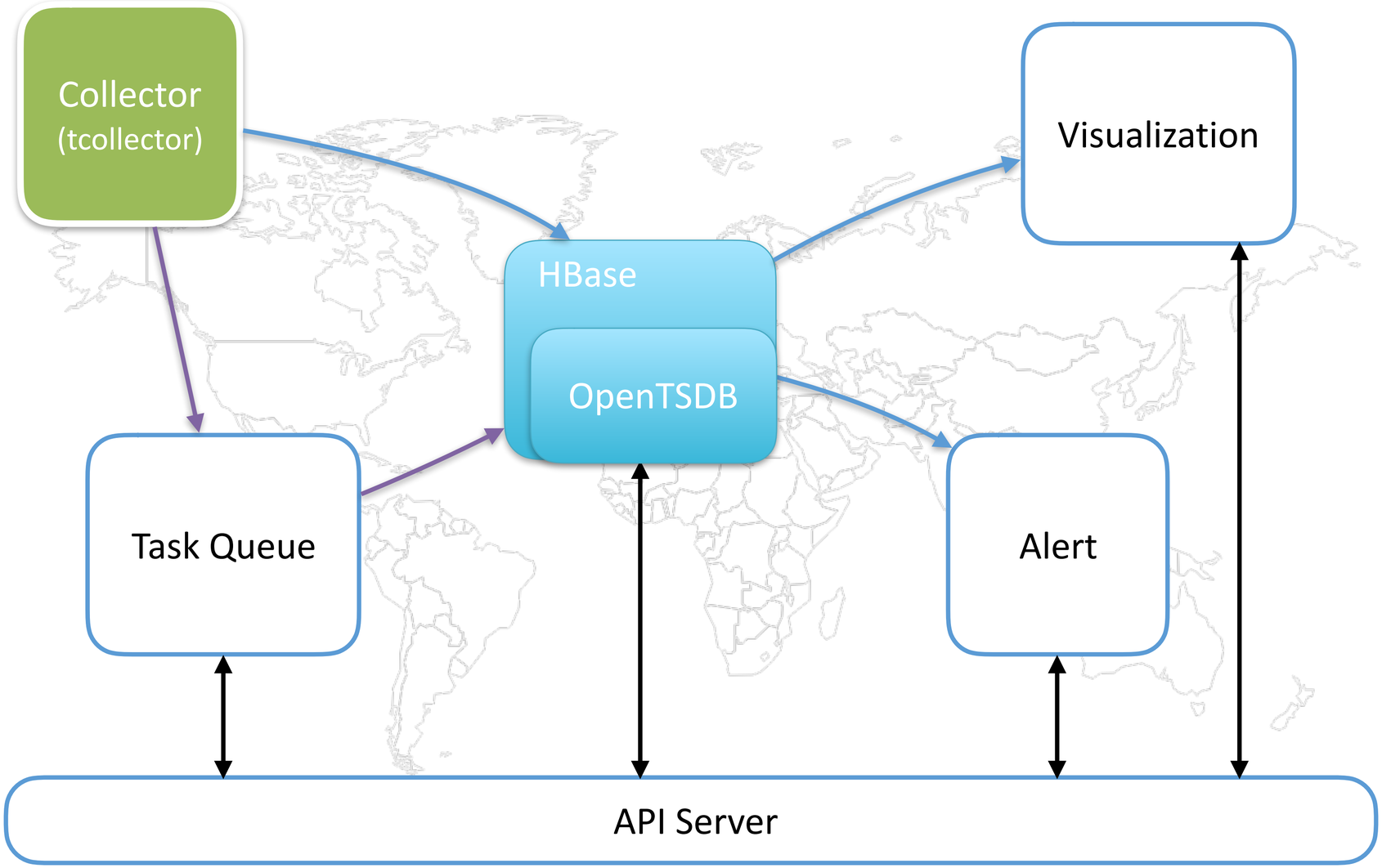


TCollector

Collector


Linux(/proc)
Custom metrics
Scripts
Collector Mainloop
OpenTSDB
de-duplication
Collector
Script
yield
ReaderThread
nput
ReaderQueue
nget
TSD
send
SenderQueue
SenderThread
HTTP
Connection Management
TCollector

Architecture

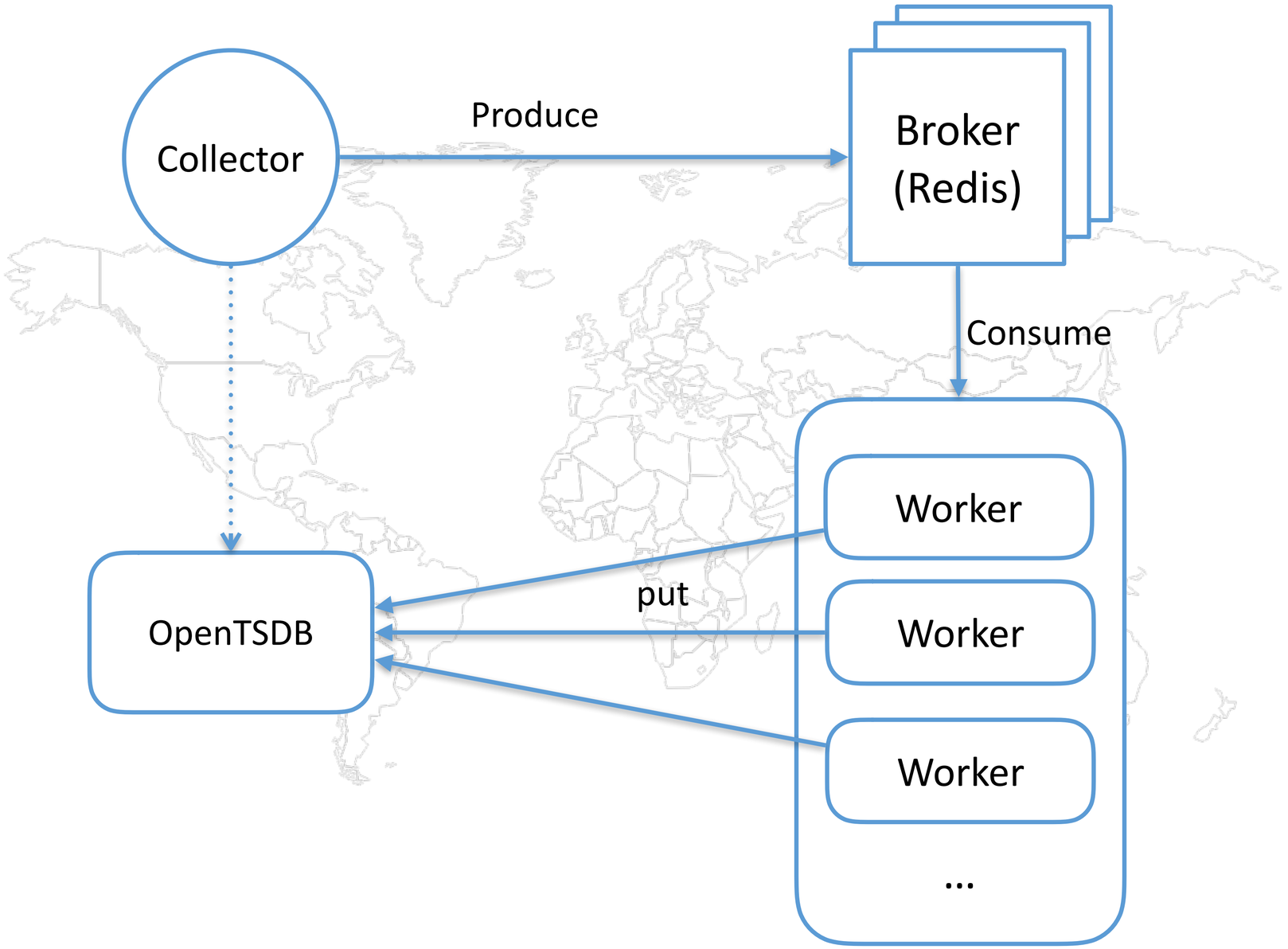


Task Queue - Celery

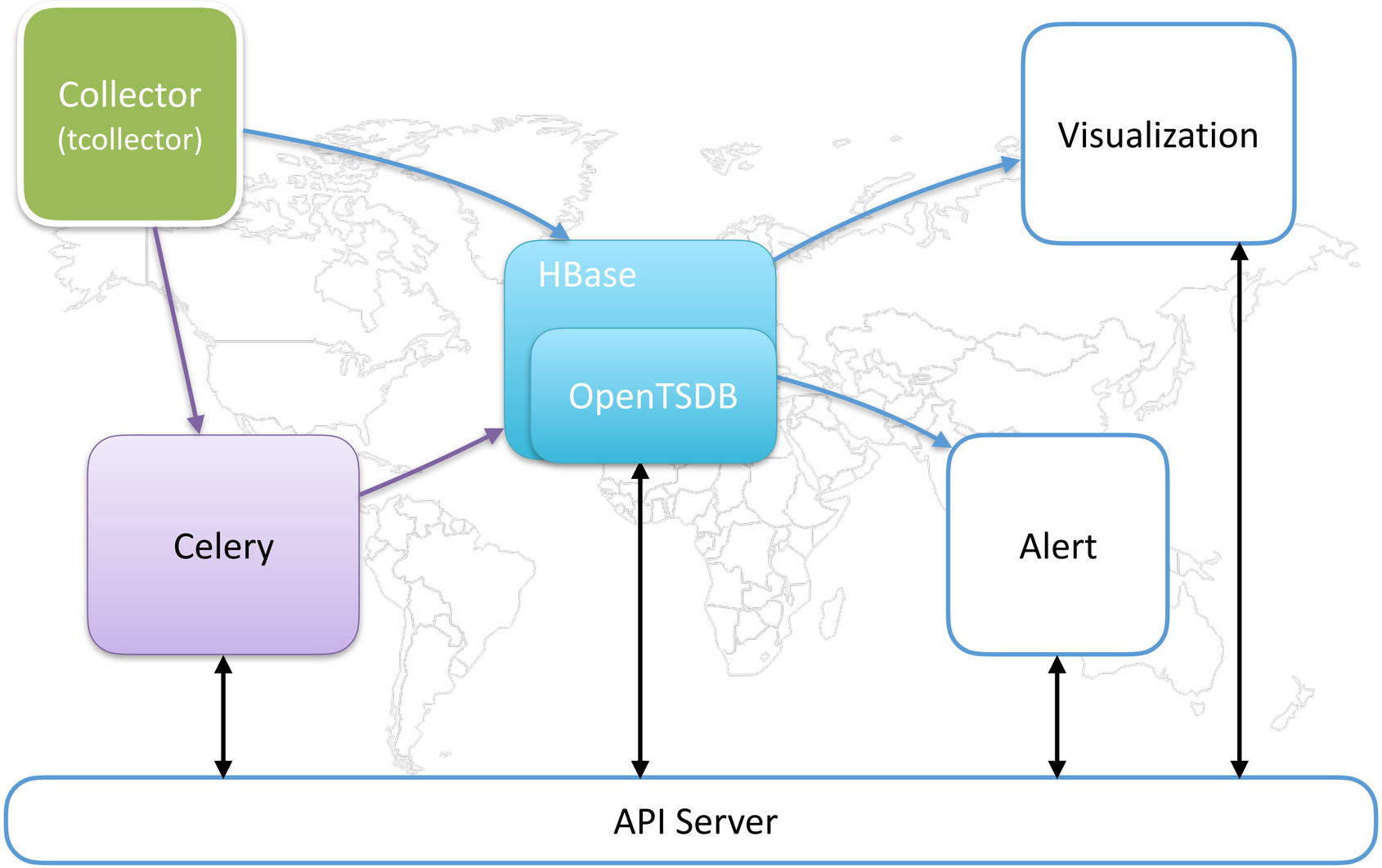
Celery

- Distributed asynchronous Task Queue
- Highly Available & Fast & Flexible
- Focus on real-time processing
- Time & Rate Limits
- Task scheduling
- User Components
- Message Broker
  - Redis
    - Use both RDB and AOF for redis persistence
      - RDB allows us to have snapshots of the datastore.
      - AOF allows us persistence across restarts of redis.

Celery


Collector
Produce
Broker
(Redis)
Consume
Worker
Worker
Worker
...
put
OpenTSDB

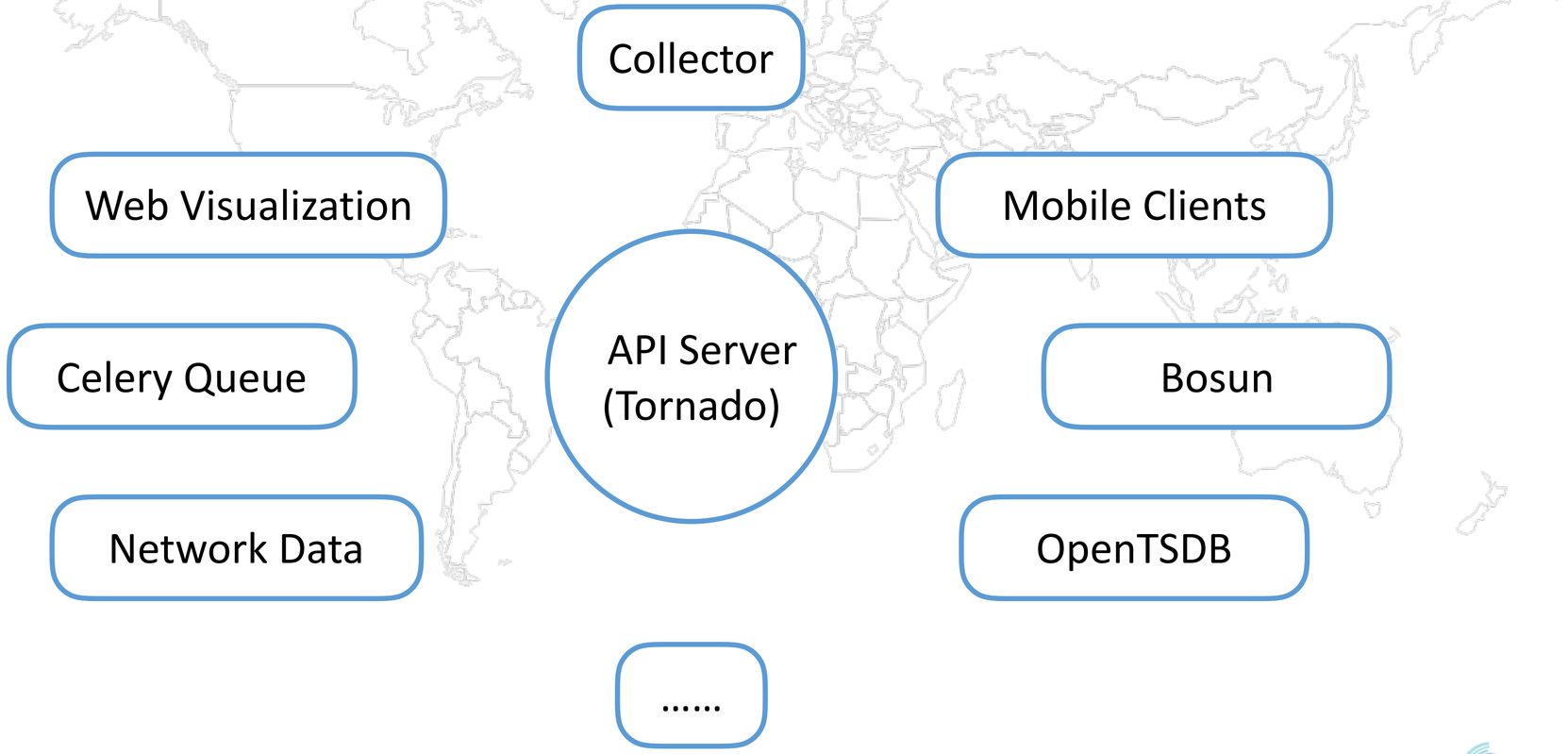
Architecture



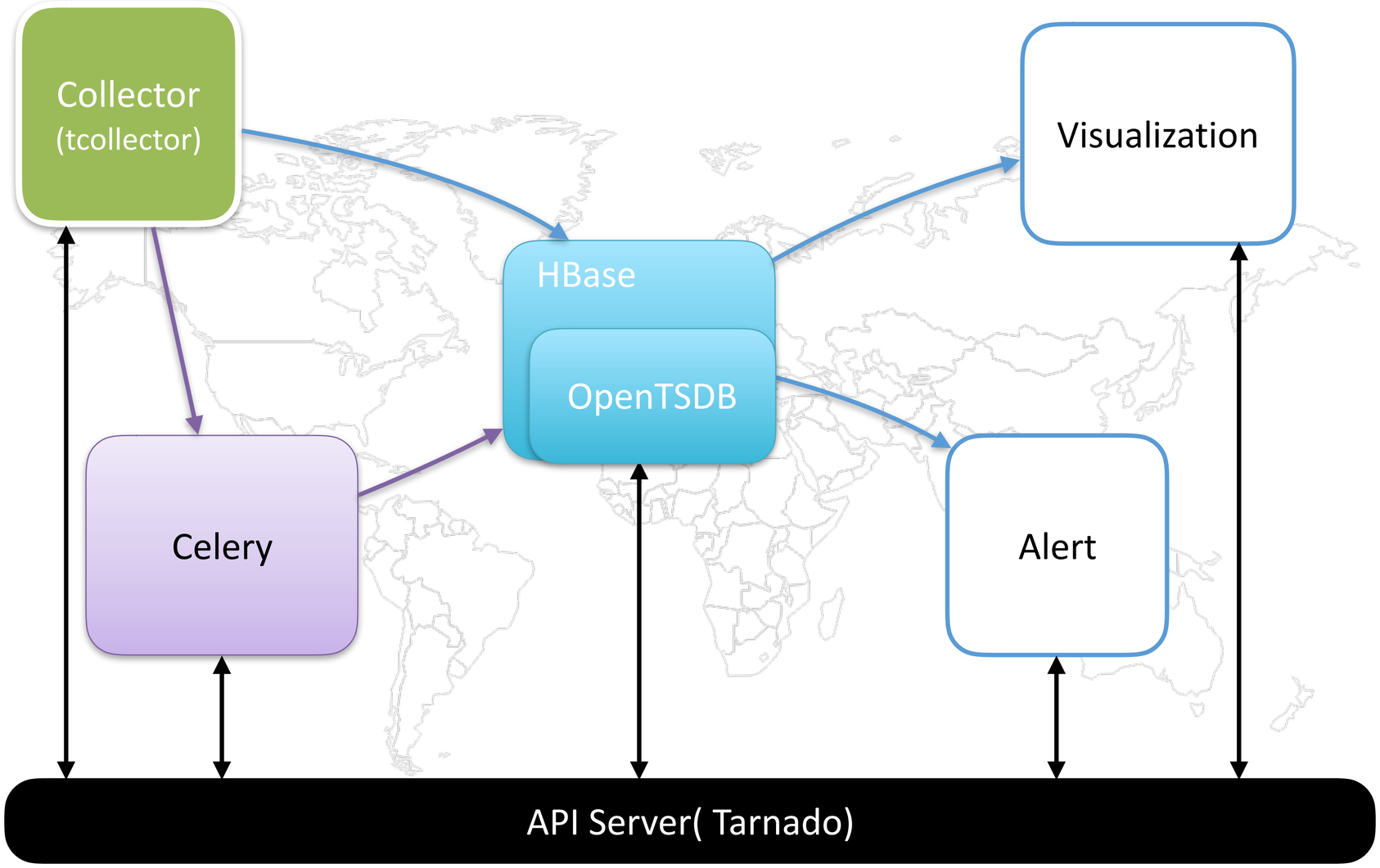
API Server - Tornado

Tornado

- High concurrent restful api server
- Graceful integration with celery
- API Encapsulation



Architecture

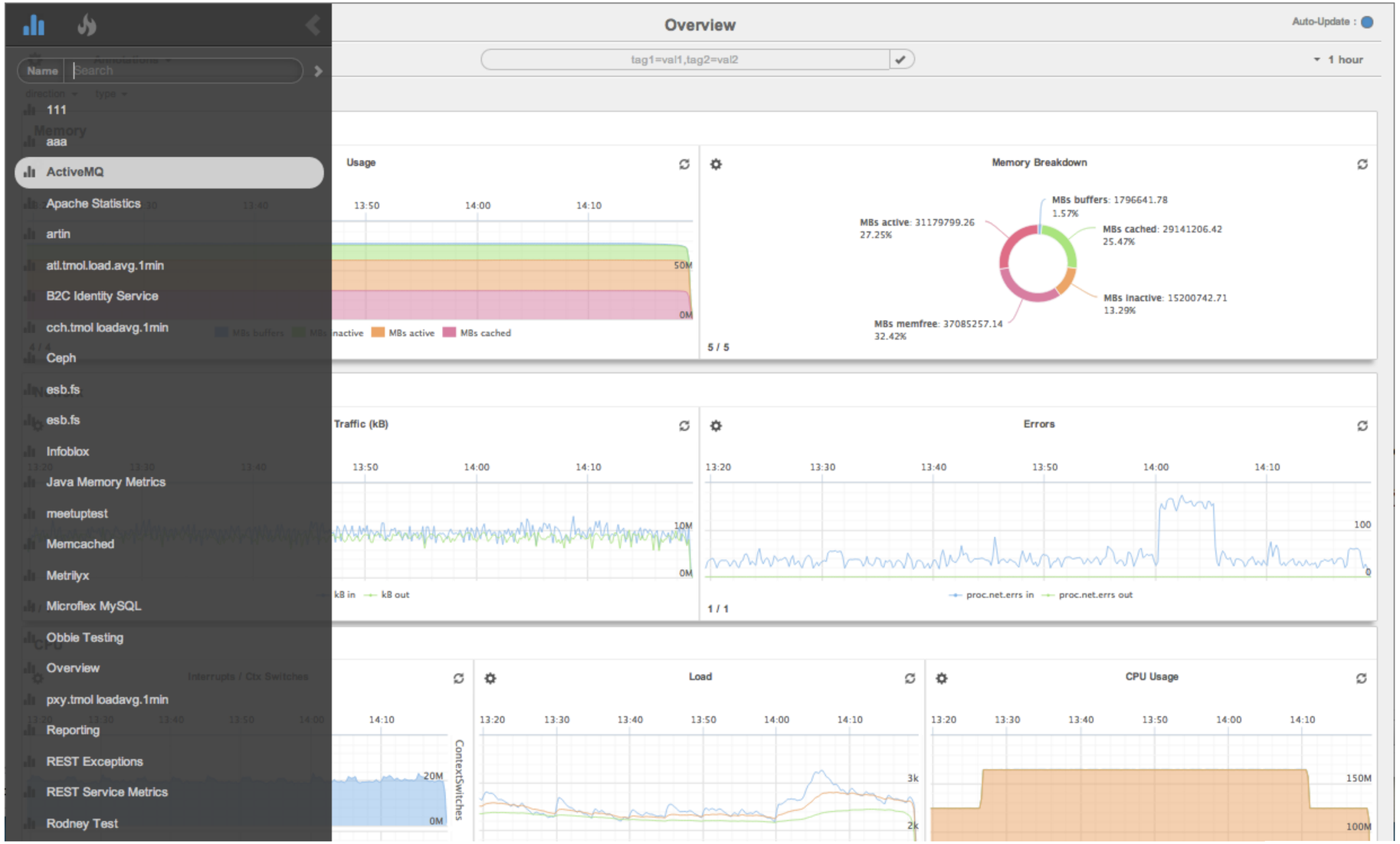


Visualization - Metrilyx

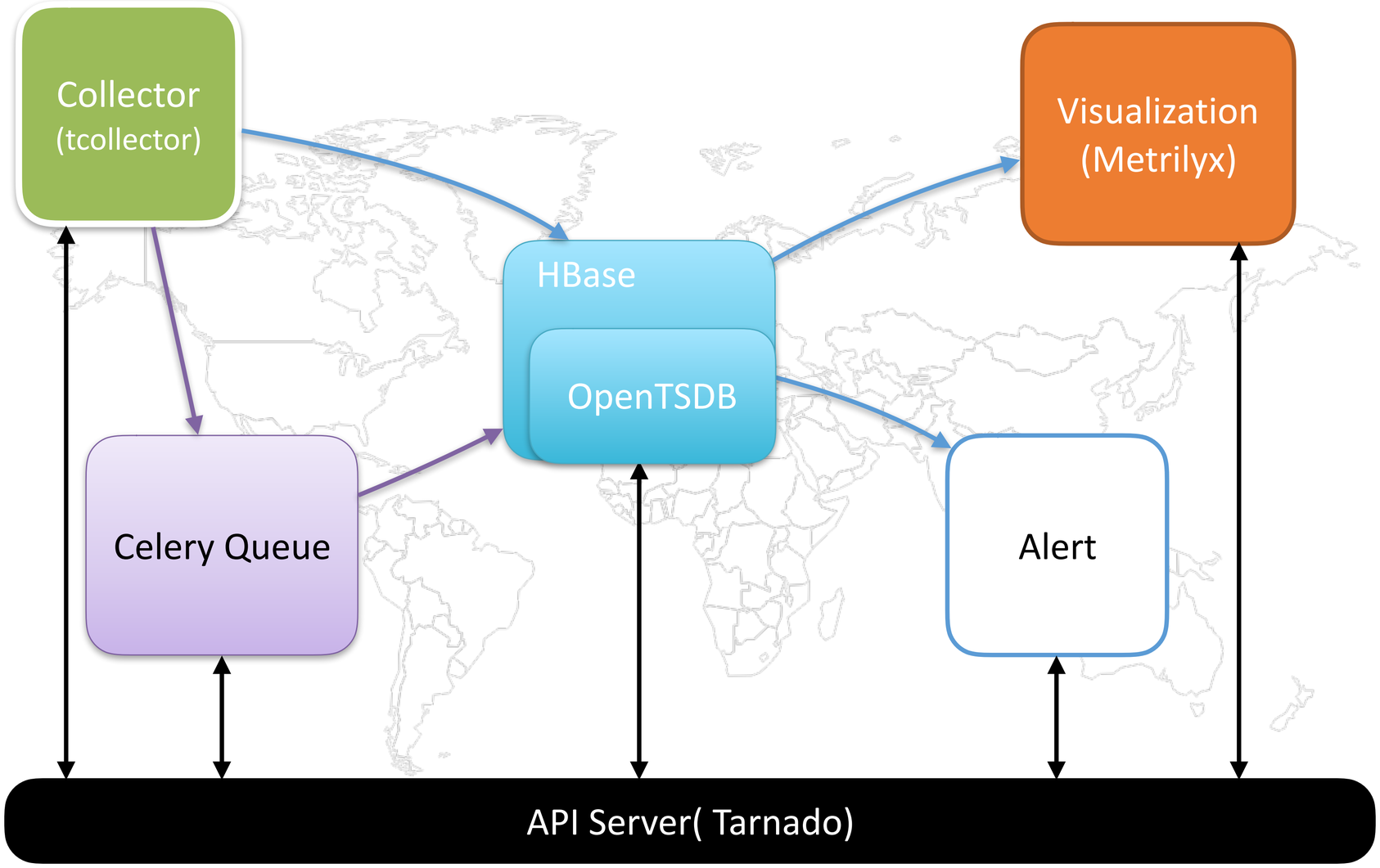
Architecture

- Metrilyx
  - Based on django
  - Easy Dashboards
  - Data Analysis / Metric Operations
  - WebSocket Data Delivery
  - Richer Metric Search
  - Distributed, Highly-Available, Redundant

Metrilyx-Dashboard



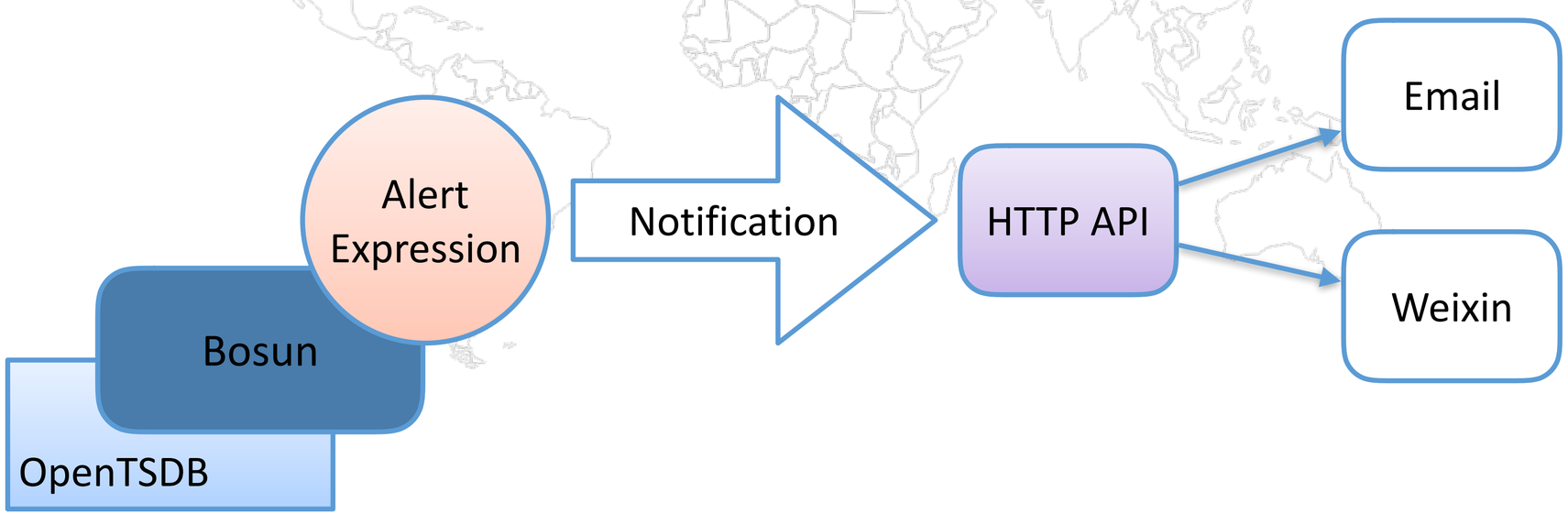
Architecture



Alert - Bosun

Bosun

- Used in monitoring infrastructure at Stack Overflow
- Written in Go and AngularJS
- Based on OpenTSDB
- Define alert with powerful expression language
- Useful notification template
- HTTP API alert

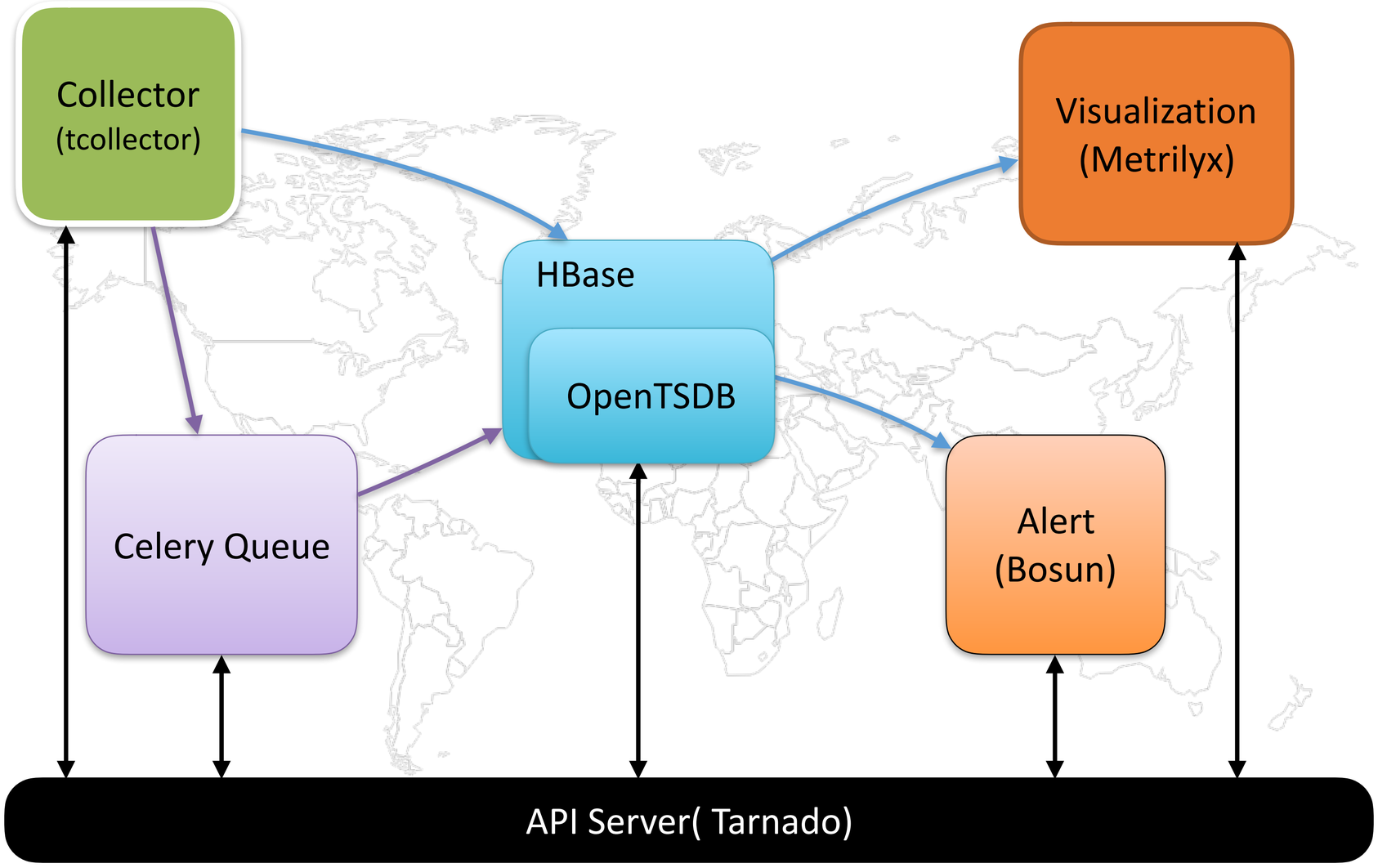


Bosun - Expression

- Take various time series and reduce them them a single number
- True or false indicates whether the alert should trigger or not

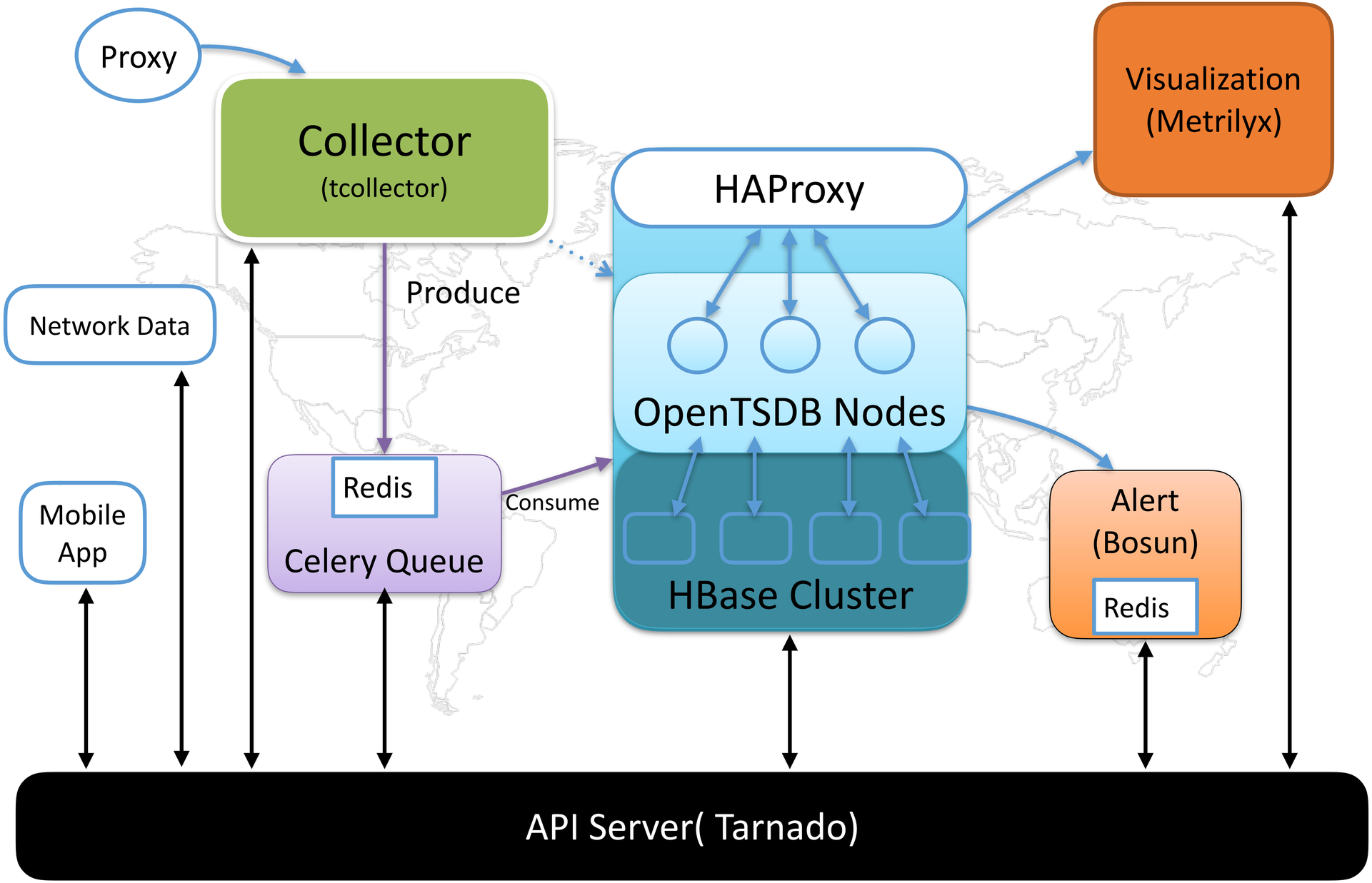
```
1  tsdbHost = tsdb01.stackoverflow.com:4242
2  smtpHost = mail.stackoverflow.com:25
3
4  template cpu {
5      body = `Alert definition:
6      Name: {{.Alert.Name}}
7      Crit: {{.Alert.Crit}}
8
9      Tags:{{range $k, $v := .Group}}
10     {{$k}}: {{$v}}{{end}}
11     `
12     subject = cpu idle at {{.Alert.Vars.q | .E}} on {{.Group.host}}
13 }
14
15 notification default {
16     email = someone@domain.com
17     next = default
18     timeout = 1h
19 }
20
21 alert cpu {
22     template = cpu
23     $q = avg(q("sum:rate:linux.cpu{host=*,type=idle}", "1m"))
24     crit = $q < 40
25     notification = default
26 }
```

Architecture



A Little More…

Architecture



redis

django

Metrilyx

python

Bosun

Tornado

OpenTSDB

APACHE HBASE

TCollector

297279664

tyingk@163.com

知 Eacon