ELK and Monasca Crossing: Logging as an OpenStack Service

Witold Bedyk, Roland Hochmuth, Martin Roderus

OpenStack Summit Tokyo, October 29, 2015

FUJITSU hp

INTRODUCTION

Logs in OpenStack

Component	Service	# log files
Ceilometer	Telemetry	8
Cinder	Block Storage	5
Glance	Images	2
Heat	Orchestration	3
Horizon	Dashboard	7
Keystone	Identity	1
Neutron	Networking	6
Nova	Compute	8
Swift	Object Storage	3
MongoDB, openvswitch, syslog	Supporting services / components	5
etc.	etc.	etc.

- >50 log files on a single node → hundreds of files in a (HA) production OpenStack system
- Need for centralized log management

FUJITSU hp

Logging as an OpenStack Service

- Multiple vendors offer logging solutions as add-ons
  - (Most of them based on Elasticsearch)
- Our mission: consolidate vendor-specific solutions into a standardized OpenStack project
- Analogy to Ironic: replaces multiple vendor-specific tools for bare metal deployment (Foreman, etc.)
- Logging-as-a-Service: provide same functionality to OpenStack users
  - API (RESTful)
  - Authentication
  - Multi-tenancy

FUJITSU hp

ELK and Monasca

ELK Stack

- **Elasticsearch**: search engine
- **Logstash**: collection, parsing and transformation
  - Alternatives: Beaver, Fluentd
- **Kibana**: graph dashboard
- Competitive to proprietary solutions, such as *Splunk*

Monasca

- Metrics Monitoring-as-a-Service
- Event processing coming soon
- Highly performant, scalable and fault-tolerant


ELK and Monasca Crossing

Why not start a separate project ``Logging‘‘?

- Related topics: both metrics and logs...
  - ... indicate the health status of your infrastructure and services
  - ... let you analyze the root cause of an error
- Functional (and nonfunctional) extension to ELK:
  - Multi-tenancy: Logging-as-a-Service
  - Performance/scalability
  - Alarms (future)
- Correlation of metrics and logs (and OpenStack notifications)

Metrics, Events and Logs

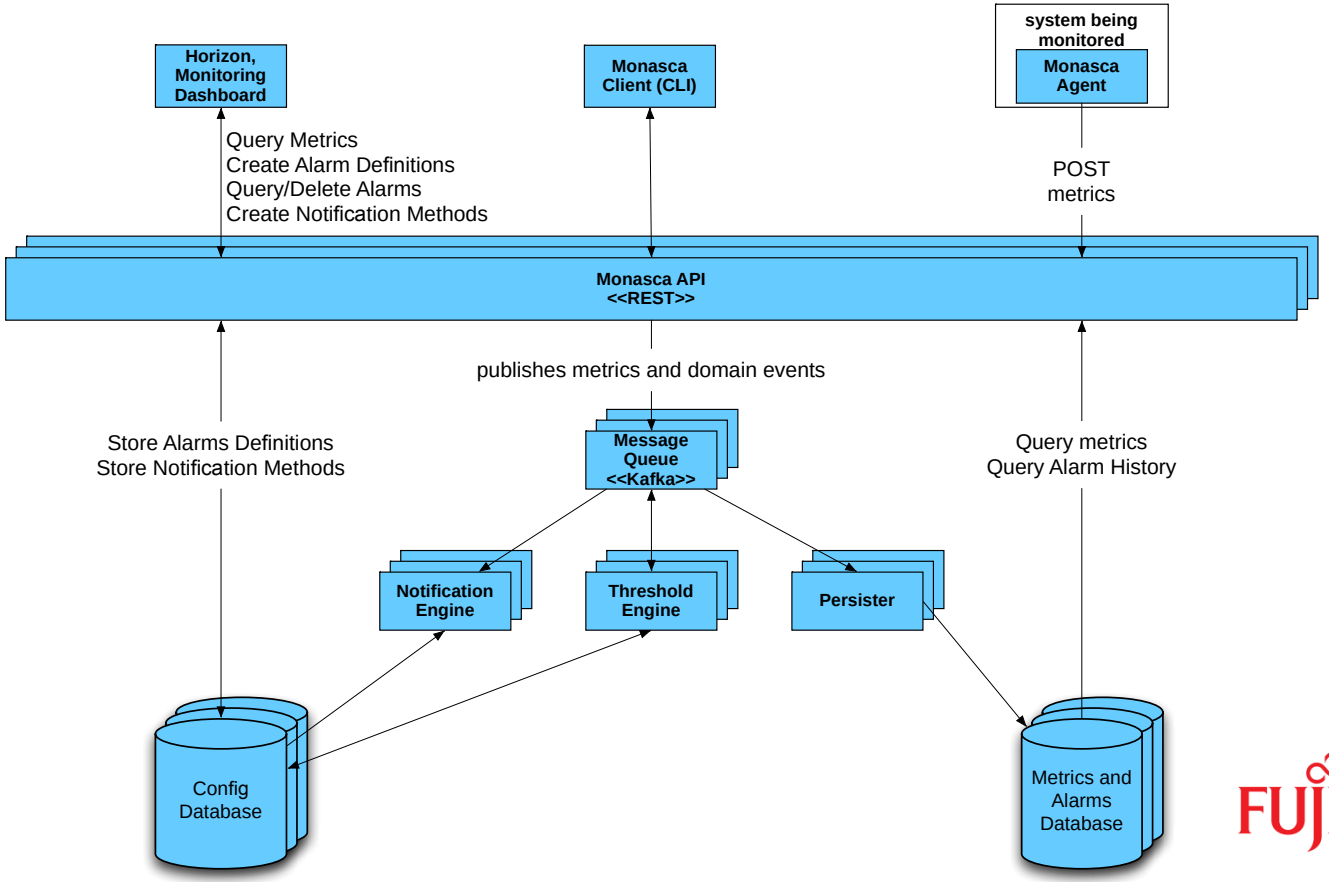
ARCHITECTURE

Metrics Monitoring Overview

- Monitoring-as-a-Service
  - First class RESTfull API for monitoring
  - Authentication and multi-tenancy
- Highly performant, scalable and fault-tolerant
- Micro-services message bus architecture provides flexibility, extensibility and load-balancing
- Built on Apache Kafka, Apache Storm, InfluxDB and the latest real-time streaming and big data infrastructure.
- Metrics storage, retrieval, thresholding and notifications
- Real-time streaming complex event processing in progress

FUJITSU hp

Metrics Architecture

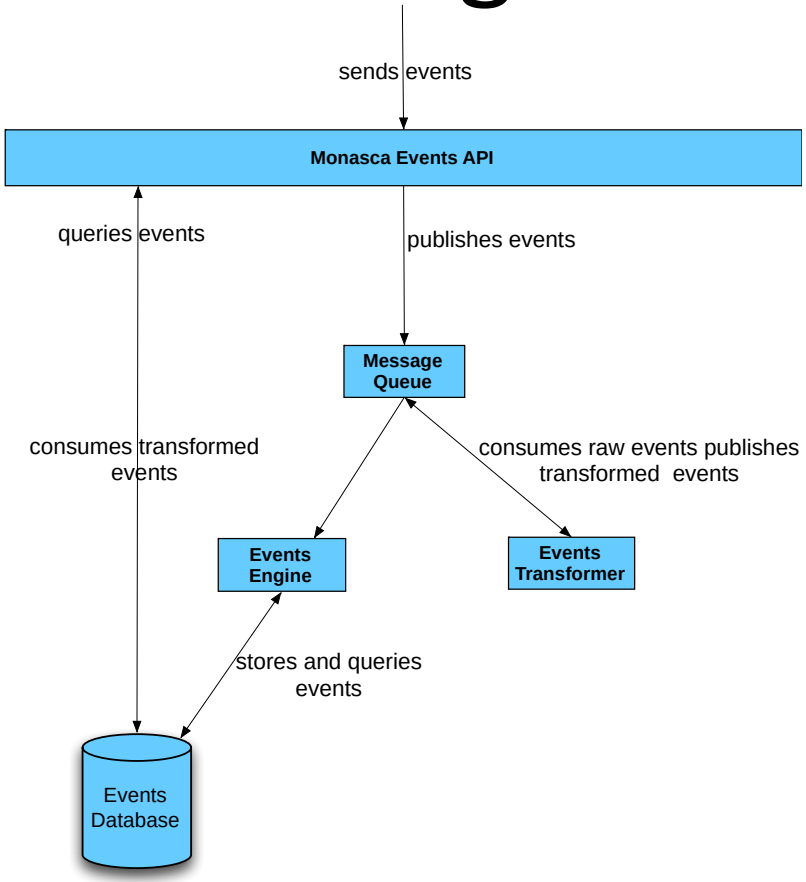


Complex Event Processing (in progress)

- Real-time event stream processing
- Events API
  - Store and query events. E.g. OpenStack Notifications
  - Specify event transforms
  - Define streams: Filter, group by and trigger on
    - Specific Events
    - Elapsed (expired)
  - Define stream/pipeline handlers
    - Code that runs when triggers occur. E.g. Evaluate the elapsed time between events.
- Transform Engine: Transforms events to normalize and reduce data
- Events Engine: Filters, groups, triggers and processes events

FUJITSU hp

Events Processing Architecture

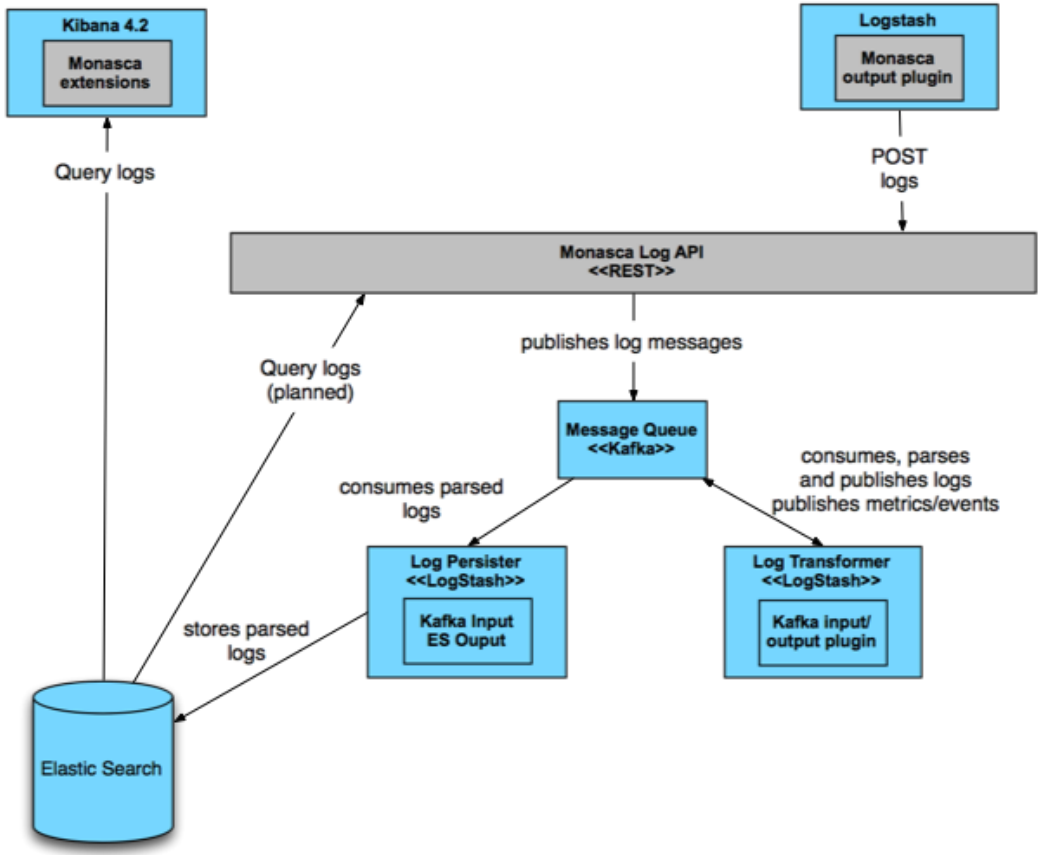


Logging Overview

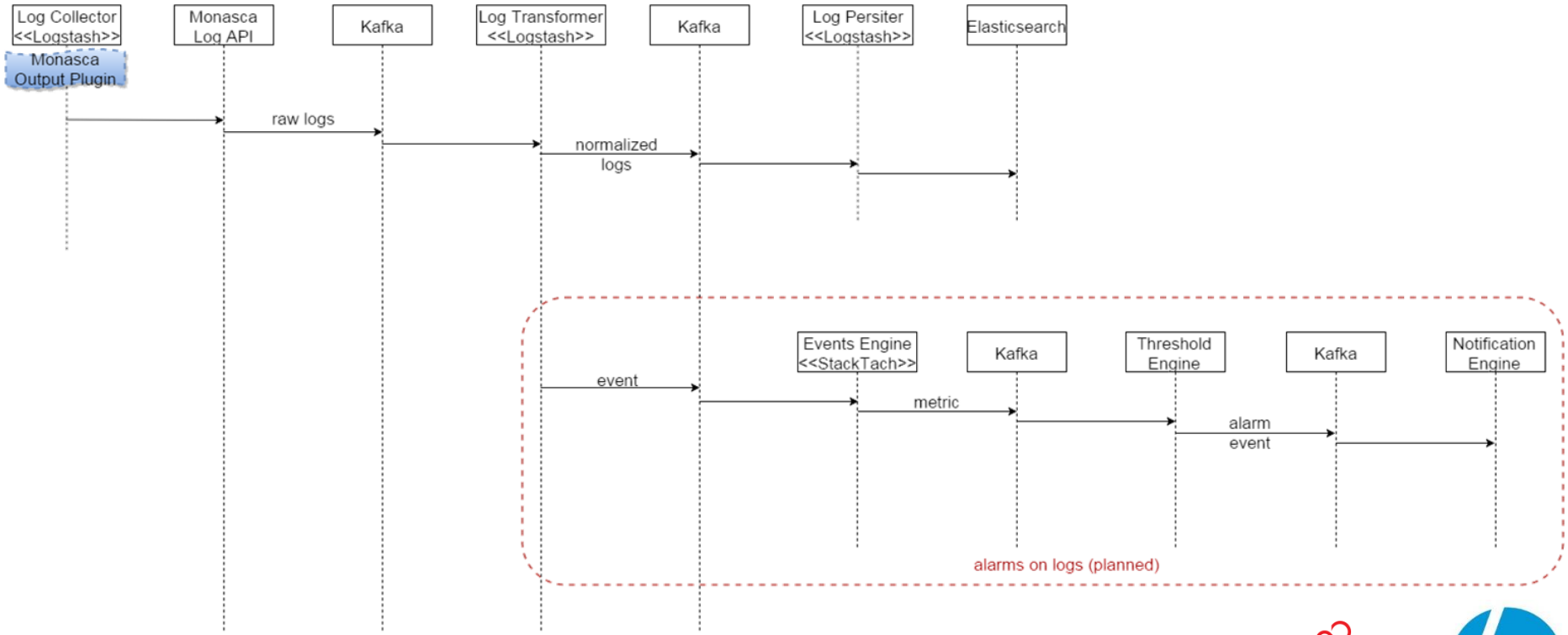
- Built on Elasticsearch, Logstash & Kibana (ELK)
- Added logging API + Logstash output plugin
- Leverage proven technologies, architecture & design patterns and code in Monasca
- Value-add to pure ELK:
  - Logging-as-a-Service
  - Greater scalability and performance
  - Alarms on logs (in progress)

FUJITSU hp

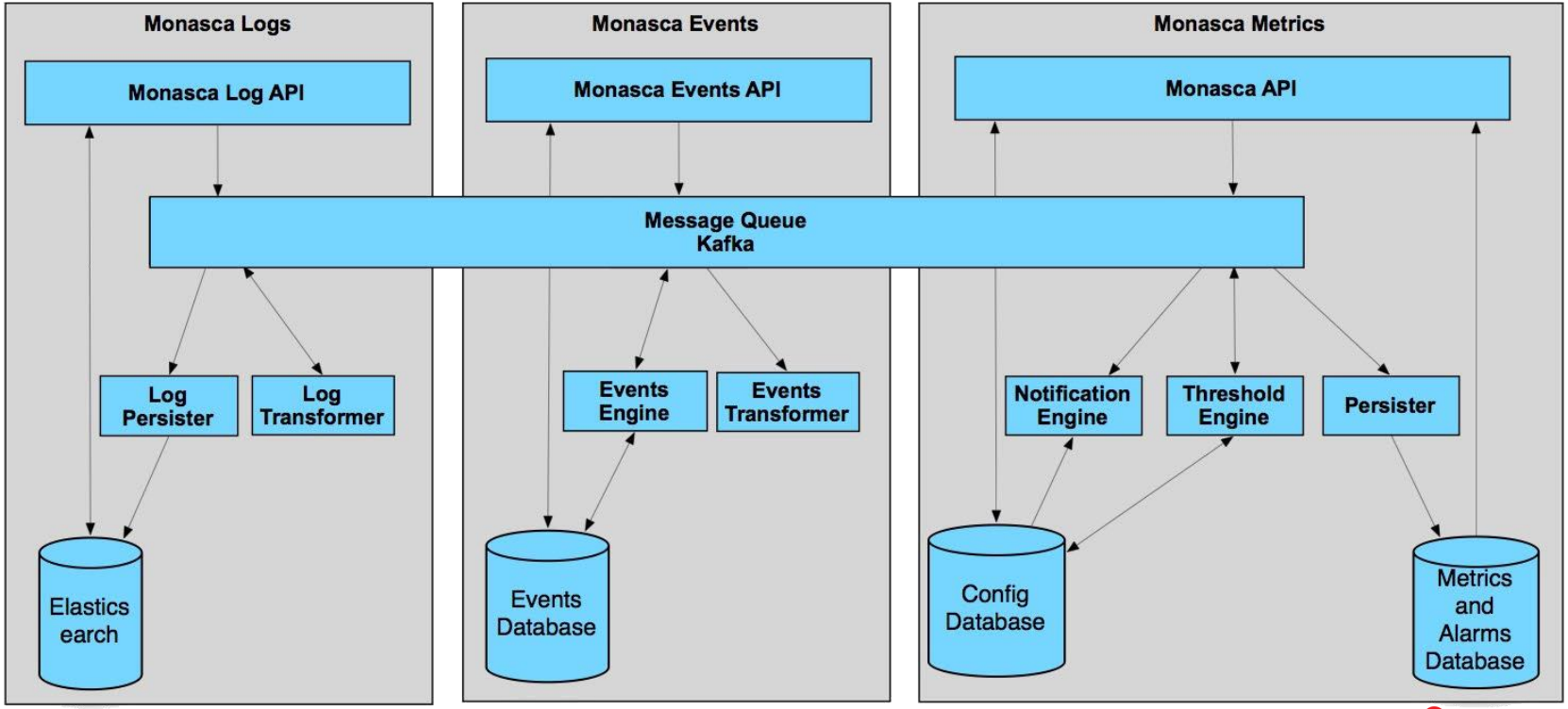
Logging Architecture



Logging Alarms Sequence



Combined Architecture



DEMO

Contact

martin.roderus@est.fujitsu.com
roland.hochmuth@hpe.com
witold.bedyk@est.fujitsu.com

Weekly meeting: Wednesdays at 15:00 UTC

IRC: #openstack-meeting-3 on freenode.net

wiki.openstack.org/wiki/Monasca

Introducing Using Monasca for Production OpenStack Monitoring

Roland Hochmuth, Dan Dyer

Aoba room

3:30pm - 4:10pm

Monasca Team Meeting

Sakura Tower, room S3.

4:40pm – 6:00pm

FUJITSU hp

Logging API

```
POST /v2.0/log/single HTTP/1.1
Content-Type: application/json
X-Auth-Token: 27feed73a0ce4138934e30d619b415b0
X-Application-Type: apache
X-Dimensions: applicationname:WebServer01,environment:production
{"message":"Hello World!", "from":"hoover"}
```

- POST methods: JSON. Single and bulk.
- Authentication -> scoped queries
- Future plan: allow direct Elasticsearch queries

FUJITSU hp