Hadoop For OpenStack Log Analysis

Grizzly Summit, April 16th, 2013,

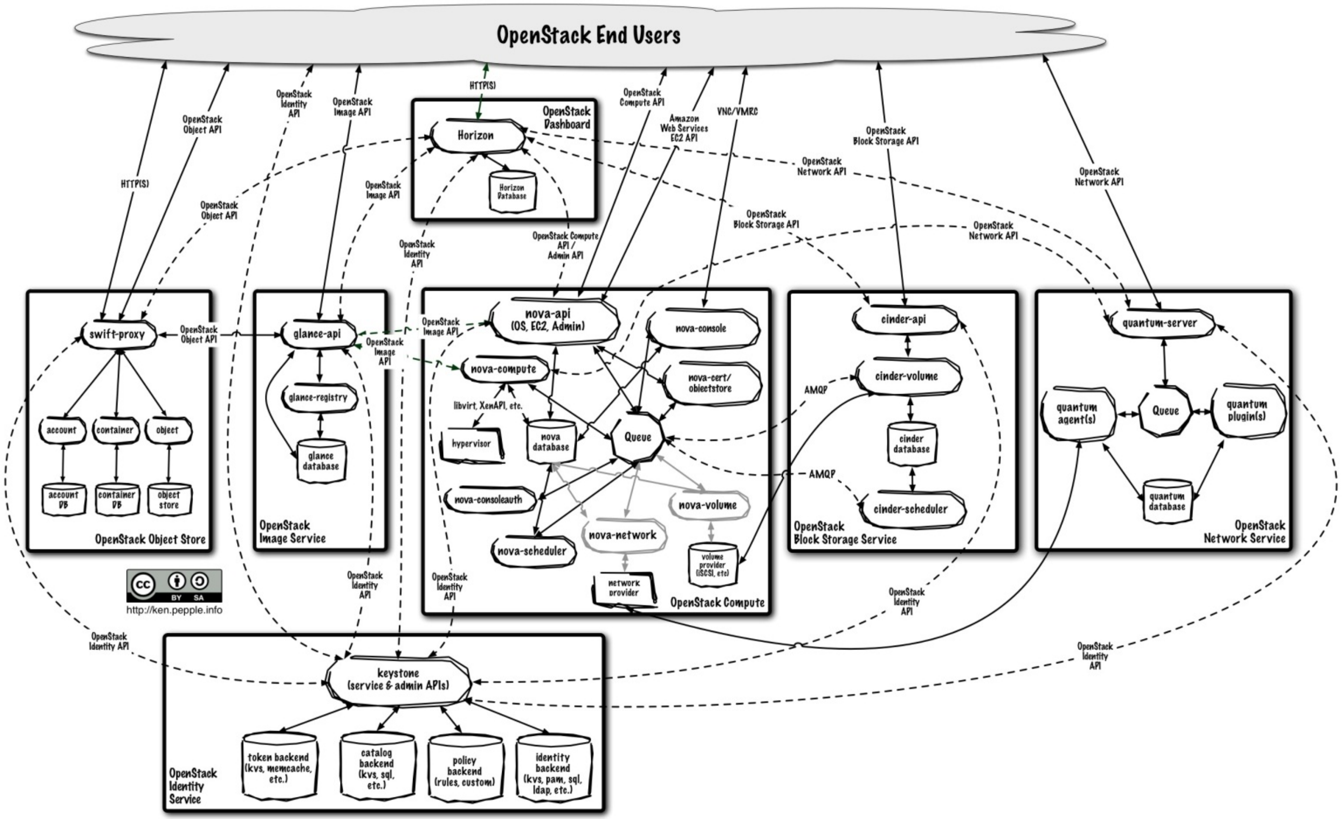
Mike Pittaro

Principal Architect, Big Data Solutions

@pmikeyp   Freenode: mikeyp

michael_pittaro@dell.com

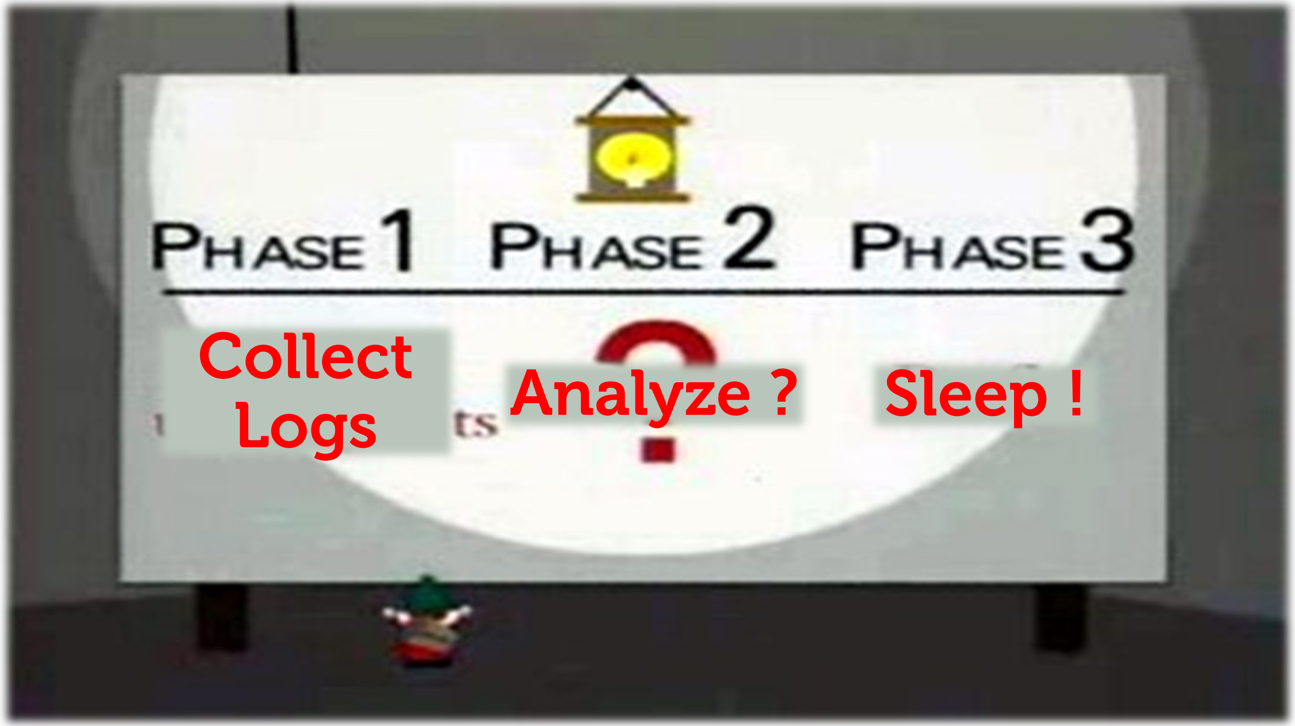
The Problem : Operating OpenStack at Scale



The Search for the Holy Grail of OpenStack Operations

- Imagine if we could follow a request …
  - Through the entire system …
  - Across compute, storage, network …
  - Independent of physical nodes …
  - With timestamps …
  - Correlated with events outside OpenStack …

It's Easy !



OpenStack Log Analysis is a Big Data Problem

Big Data is when the data itself is part of the problem.

Volume

A large amount of data, growing at large rates

Velocity

The speed at which the data must be processed

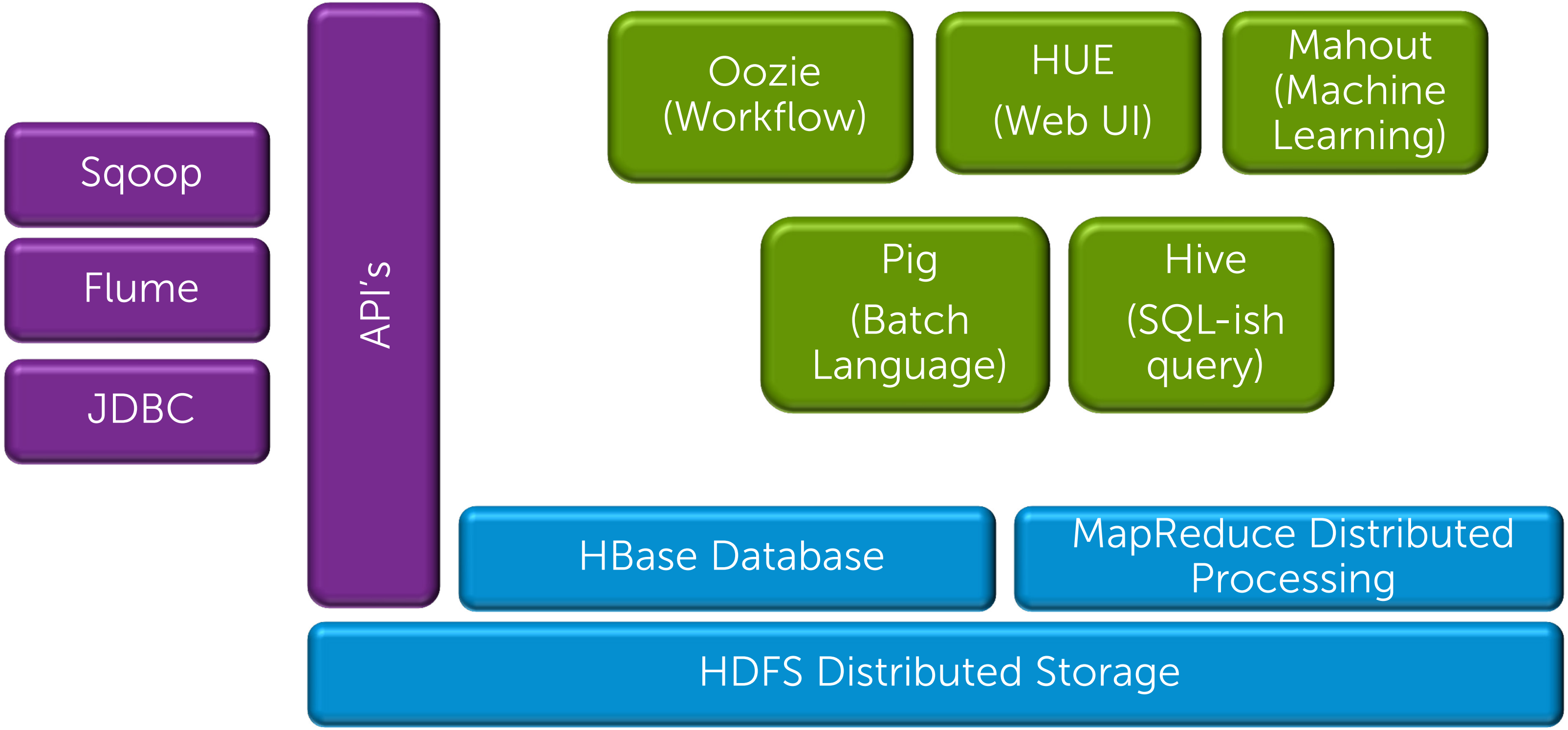
Variety

The range of data types and data structure

Initial Focus and Scope of Our Efforts

- The Operators
  - Assist in running OpenStack
  - Not for tenants
- The Data
  - Load all detail into Hadoop
  - Extract and index significant fields
  - Enable future analysis
- The Patterns
  - What works
  - What is repeatable across installs
  - How can we collaborate

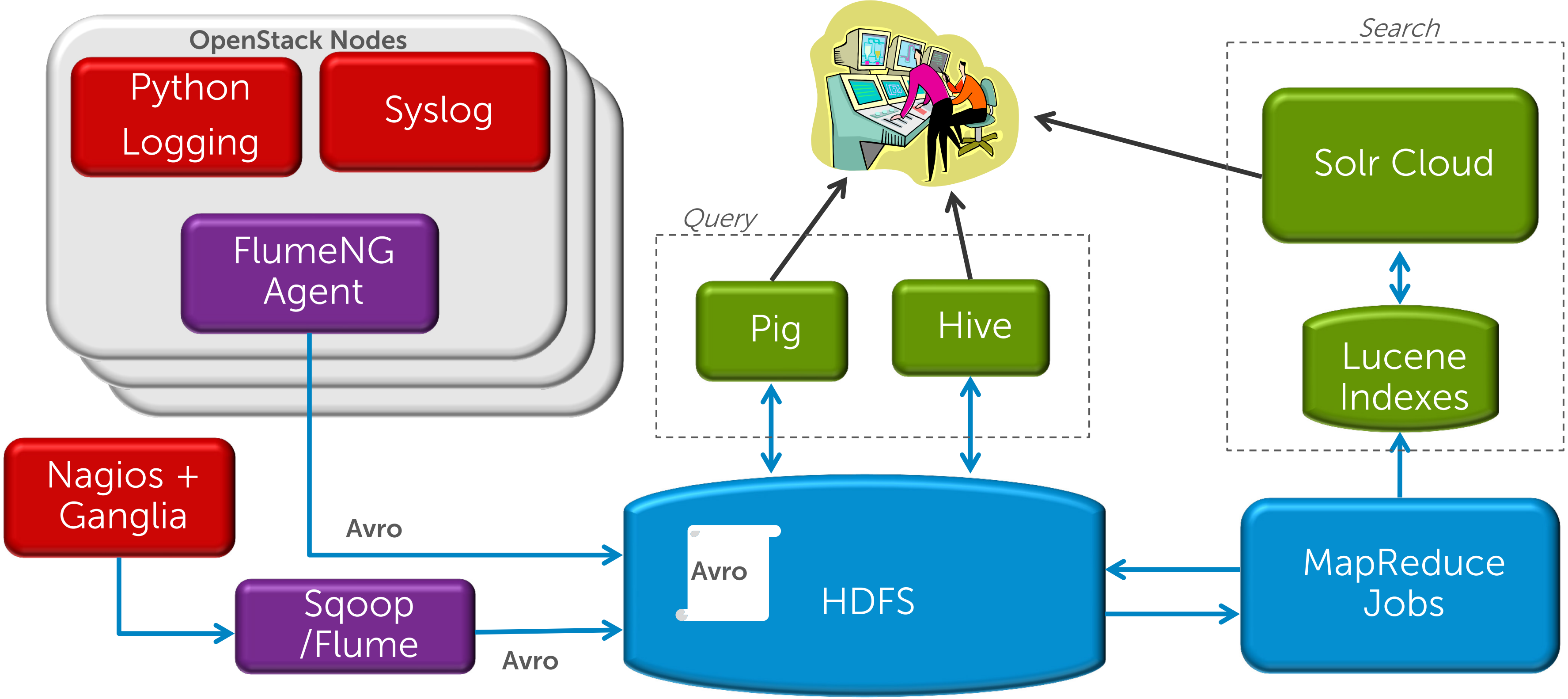
Hadoop 101 – Simplified Block Diagram



The Big Pieces

- Log Collection
  - Continuous streaming of log data into Hadoop from OpenStack
- Intelligent Log parsing, Indexing and Search
  - Should ‘know’ about OpenStack
- Well Defined Storage Organization
  - Defined schema for the data
  - Predefined queries for high level status - dashboard
- Straightforward implementation pattern
  - Add as little complexity as possible
- Ability to perform deeper analysis
  - Hadoop enables this

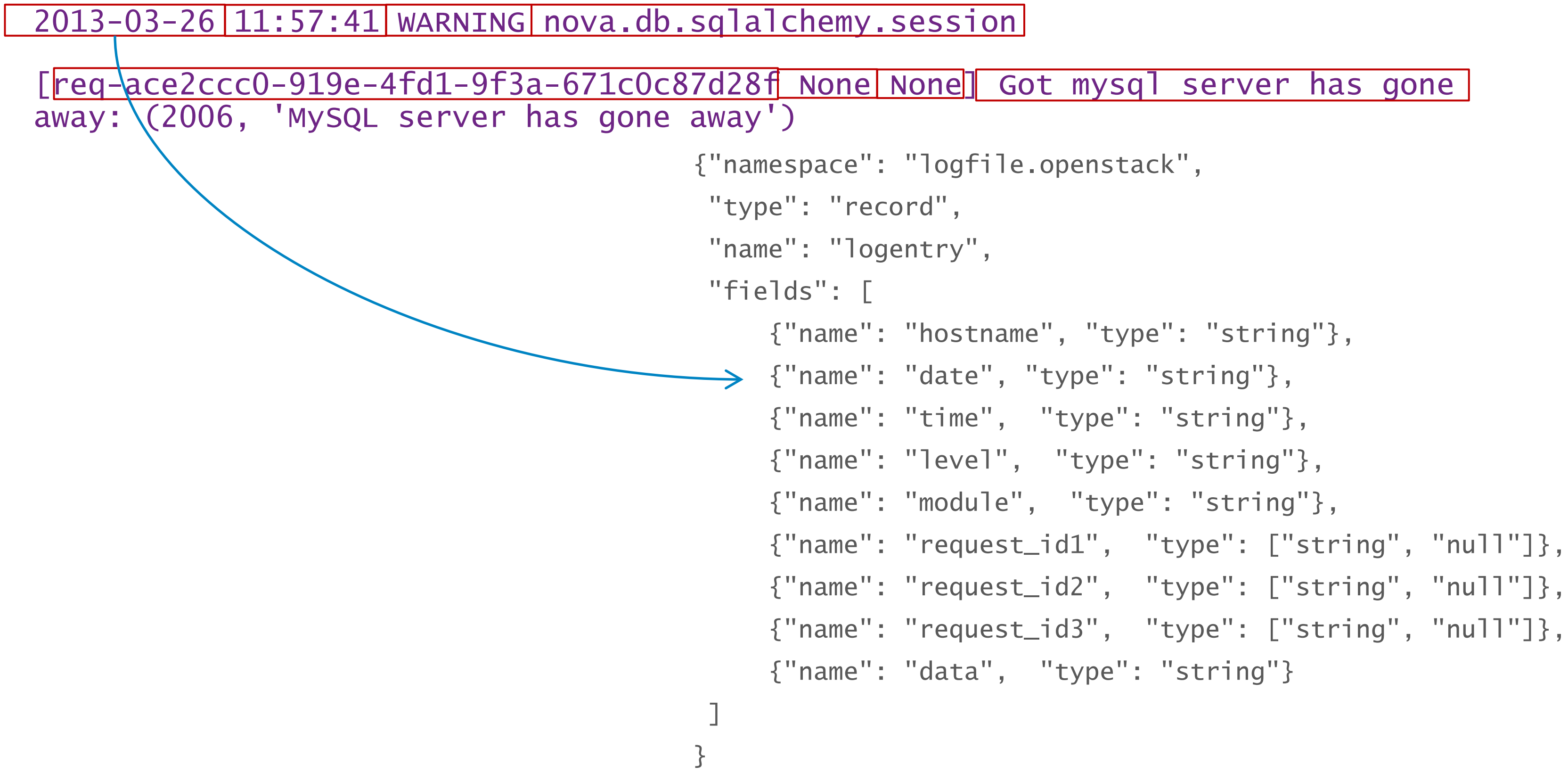
OpenStack Log Analysis Block Diagram



Current Development Status

- Batch Only, no Flume Collection
- Converting logs to AVRO format
- First cut of schema in place
- Loading into Hadoop
- Processing into SOLR indexes
- Starting to look at data
  - Solr Searches
  - Pig scripts

Schema Thoughts



```
2013-03-26 11:57:41 WARNING nova.db.sqlalchemy.session

[req-ace2ccc0-919e-4fd1-9f3a-671c0c87d28f None None] Got mysql server has gone
away: (2006, 'MySQL server has gone away')
```

```
{"namespace": "logfile.openstack",
 "type": "record",
 "name": "logentry",
 "fields": [
     {"name": "hostname", "type": "string"},
     {"name": "date", "type": "string"},
     {"name": "time",  "type": "string"},
     {"name": "level",  "type": "string"},
     {"name": "module",  "type": "string"},
     {"name": "request_id1",  "type": ["string", "null"]},
     {"name": "request_id2",  "type": ["string", "null"]},
     {"name": "request_id3",  "type": ["string", "null"]},
     {"name": "data",  "type": "string"}
 ]
}
```

Demo: Where we are today

- Solr Indexing and Search
  - Example of indexed fields and searching.
- Pig for batch analysis
  - Reconstruct a sequence of messages related to an API request

Data Collection Thoughts

- Sources
  - OpenStack subsystems
  - Syslog files
  - Nagios and Ganglia
  - General Infrastructure Data
    - Network Switches / Routers
- Input Formats
  - Mostly Semi-structured text
  - Subsystem, timestamp, hostname, severity and error level are important
- Output Formats
  - Avro
  - Thrift
  - Protocol Buffers

Log Collection Thoughts

- Well understood patterns
  - Evolving best practices
- Commonly Used Tools
  - Kafka
  - Scribe
  - Flume and FlumeNG
- Key Requirements
  - Distributed
  - Reliable
  - Aggregators – consolidate streams
  - Store and Forward – when links are down

Storage Organization Thoughts

- File Organization within Hadoop
  - Naming Convention
  - Directory Organization

- Data Lifecycle
  - Input and Staging
  - 'Hot' and 'Cold' Data
  - Tiered Indexes
  - Compression
  - Archival and Deletion

What should we do next ?

- Document the basic patterns so far ?
- Are there any related efforts ?
- Begin deeper discussions
  - Lots of decisions to make
  - Need community input and suggestions
- Collaborate on Schema Design
- What upstream OpenStack changes are needed ?
- Get sample logs in hands of Hadoopians
  - Cleansed reference log sets would be useful

References

- The unified logging infrastructure for data analytics at Twitter
- Building LinkedIn's Real-time Activity Data Pipeline
- Advances and challenges in log analysis
- BP: Ceilometer HBase Storage Backend
- BP: Cross Service Request ID
- Log Everything All the Time

- Holy Grail, Gangam Style