A Container Adventure: Scaling and Monitoring Kubernetes Logging Infrastructure

Gimi Liang | Sr. Software Engineer
Matthew Modestino | IT Practitioner
David Baldwin | Product Manager

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- The container landscape
- Choose your Adventure
  - Splunk Connect for Docker
  - Splunk Universal Forwarder
  - Splunk Connect for Kubernetes
    - Amazon EKS
    - Openshift
- Wrap-up
- Q&A

Container Landscape

Cloud Native Landscape

v20180525

See the interactive landscape at l.cncf.io

Greyed logos are not open source

App Definition and Development

Database and Data Warehouse

Vitess (CNCF Incubating)

Streaming

NATS (CNCF Incubating), cloudevents (CNCF Sandbox)

Source Code Management

GitHub, GitLab

Application Definition and Image Build

CNCF Sandbox

Continuous Integration / Continuous Delivery (CI/CD)

Orchestration & Management

Scheduling & Orchestration

kubernetes (CNCF Graduated)

Coordination & Service Discovery

CoreDNS (CNCF Incubating)

Service Management

gRPC (CNCF Incubating), envoy (CNCF Incubating), LINKERD (CNCF Incubating), Open Policy Agent (CNCF Sandbox)

Runtime

Cloud-Native Storage

ROOK (CNCF Sandbox)

Container Runtime

CNCF Incubating, CNCF Incubating

Cloud-Native Network

CNI (CNCF Incubating)

Provisioning

Host Management / Tooling

Infrastructure Automation

Container Registries

Secure Images

CNCF Incubating, CNCF Incubating

Key Management

spiffe (CNCF Sandbox), SPIRE (CNCF Sandbox)

Cloud

Public

Private

Platforms

Certified Kubernetes - Distribution

Certified Kubernetes - Hosted

Certified Kubernetes - Installer

Non-Certified Kubernetes

PaaS/Container Service

Observability & Analysis

Monitoring

Prometheus (CNCF Incubating)

Logging

fluentd (CNCF Incubating)

Tracing

JAEGER (CNCF Incubating), OPENTRACING (CNCF Incubating)

Serverless

Special

Kubernetes Certified Service Provider

Kubernetes Training Partner

l.cncf.io

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION

Redpoint Amplify

Select the tools to deploy and maintain your apps...

Host on the public,private, or hybrid cloud...

Select the tools to deploy and maintain your container cluster...

“ Gartner predicts that, by 2020, more than 50% of global organizations will be running containerized applications in production, up from less than 20% today”.

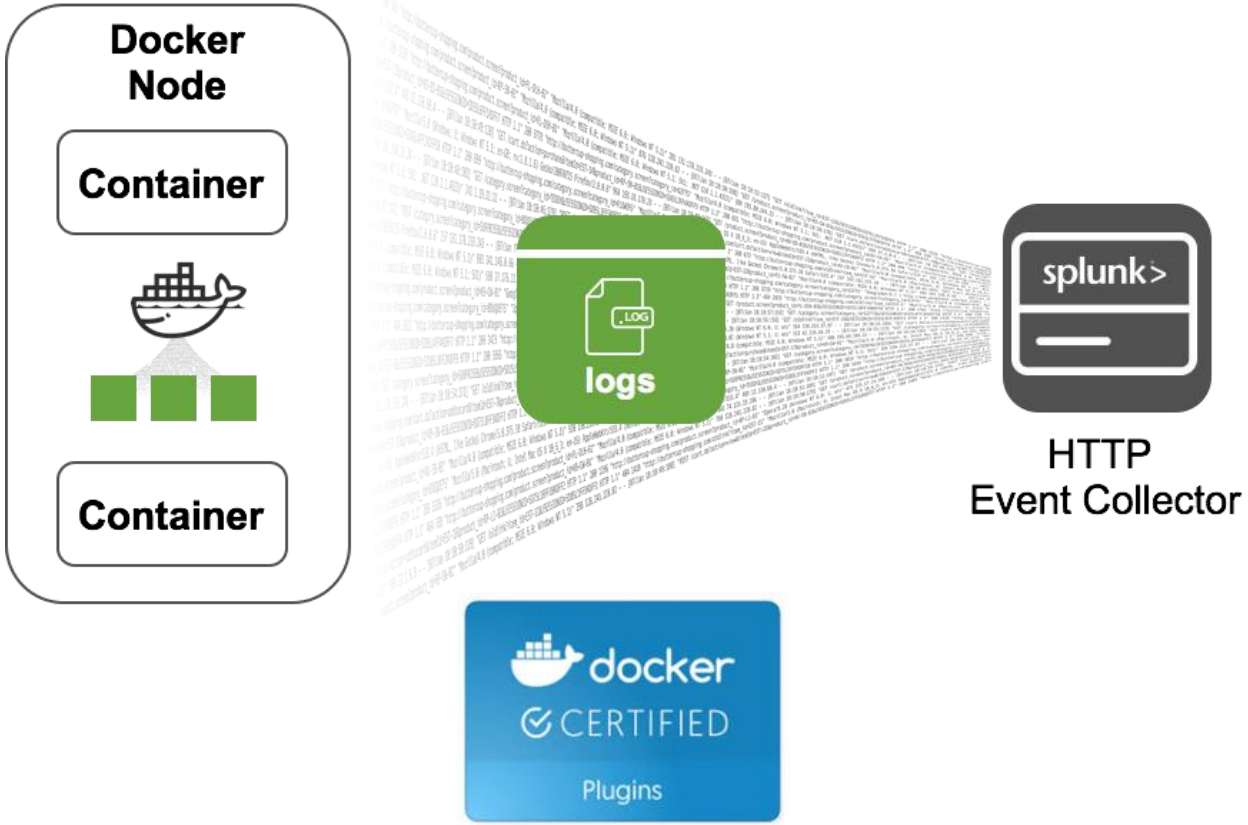
Market Guide for Public Cloud Container Services August 2017 ID: G00317096

splunk> .conf18

Choose Your Adventure

Splunk Connect for Docker

- 2015:
  - Introduced Docker Logging Driver
- 2018:
  - Certified Docker Logging Plug-in
  - Replacement for Docker Logging Driver
  - Supported Open Source*
  - Optimize consumption into Splunk through HEC



Search | Splunk 7.2.0 | Splunk Connect for Docker - D | splunk/docker-logging-plugin: | David

Secure https://store.docker.com/plugins/splunk-connect-for-docker

Bookmarks | Splunk Inc. | Cont | Git-Fingals | DA Kanban | FDSE Kanban | DA Current Progress | TA 3rd Party | DA Priorities | DA Landing | Other Bookmarks

docker store

Explore Publish Feedback Log In

splunk>

Splunk Connect for Docker

By Splunk

Splunk Connect for Docker is a Splunk supported Docker Logging Plug-in

Plugin | Docker Certified | Linux | x86-64 | Logging

docker CERTIFIED

Free Plan

$0.00

Splunk Connect for Docker is an open source plug-in available for users of Splunk Enterprise, Splunk Light, and Splunk Cloud.

Terms of Service

Setup Instructions

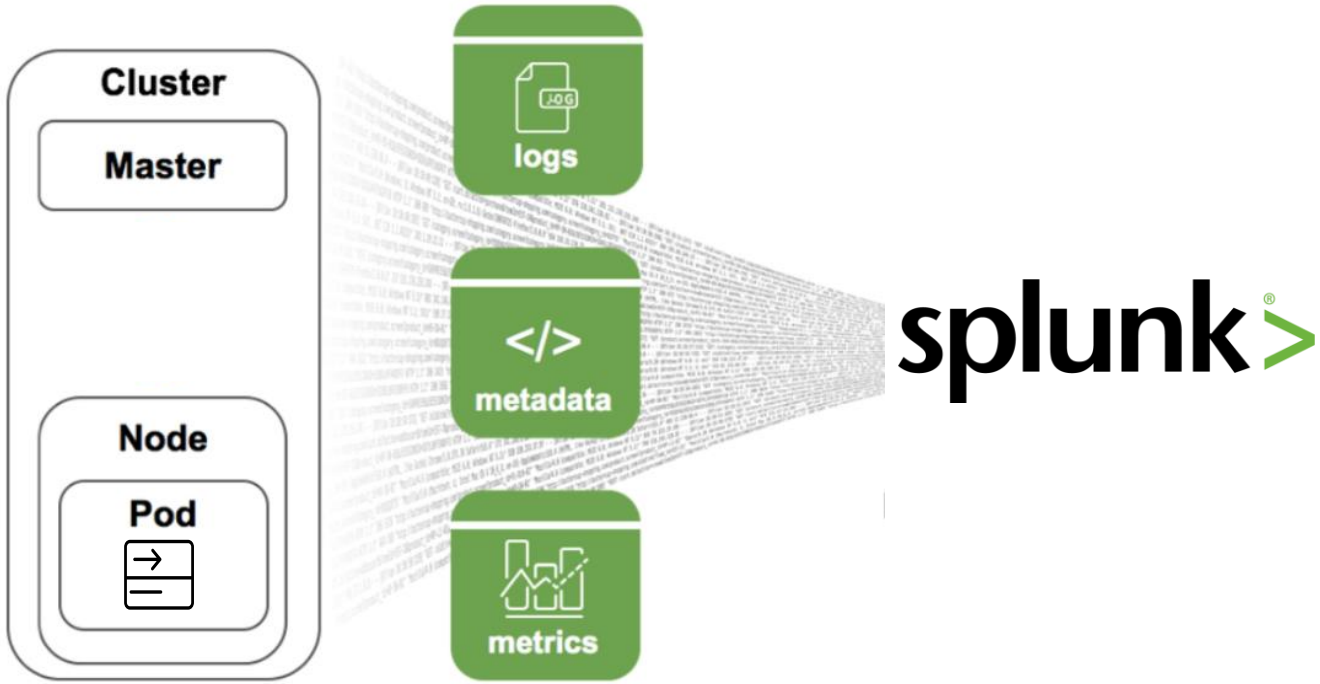
DESCRIPTION REVIEWS RESOURCES

Online Chart Maker ....htm

Show All

Universal Forwarder

- Run directly on Kubernetes nodes or as a daemonset using docker image
- Easy way for Splunk teams to get started with container logs
- Can move a lot of data, reliably and securely using existing Splunk process
- Needs modifications to make integration easier with json driver and journald



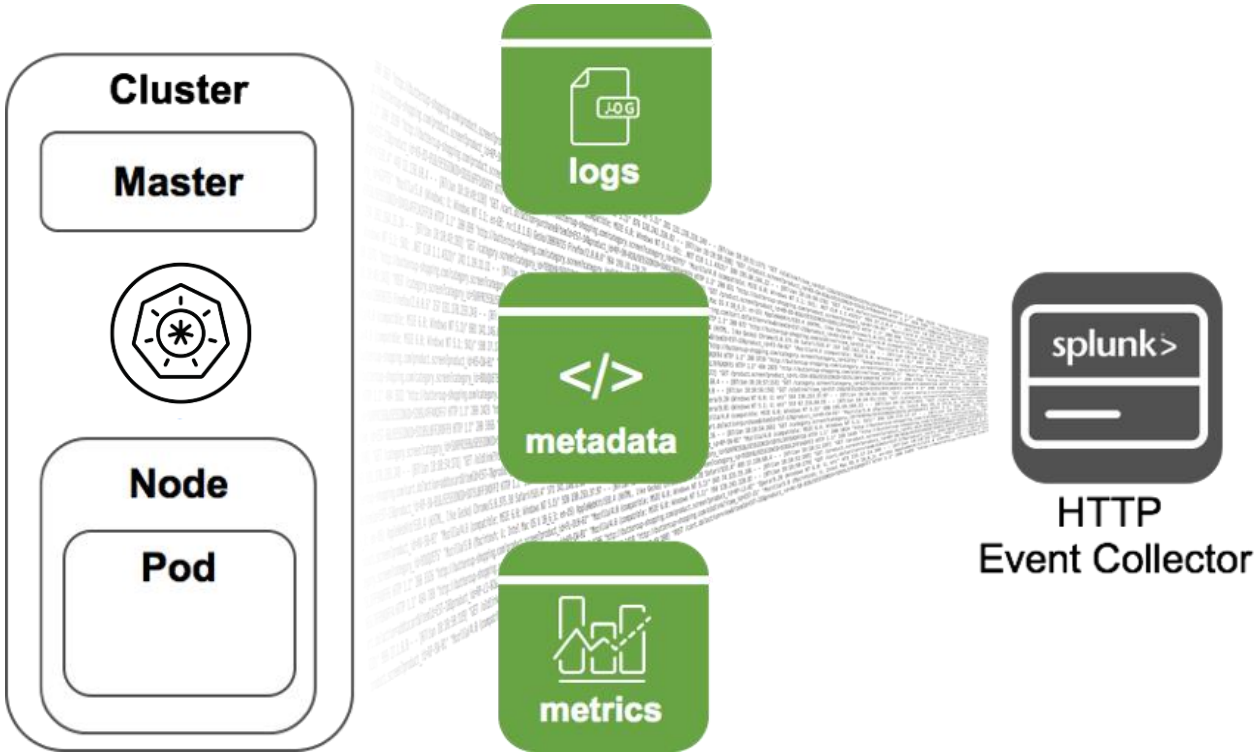
Terminal Shell Edit View Window Help

kubernetes — -bash — 203×60

```
mmodestino-mbp:kubernetes mmodestino$
mmodestino-mbp:kubernetes mmodestino$
mmodestino-mbp:kubernetes mmodestino$
mmodestino-mbp:kubernetes mmodestino$
mmodestino-mbp:kubernetes mmodestino$
```

Splunk Connect for Kubernetes

- Secure, Simple, Scale, Configurable
- 3 Components
  - **Logging**
  - **Metadata/Objects**
  - **Metrics**
- Leveraged CNCF sponsored projects
- Managed through Helm
- Supported Open Source*
- Optimize consumption into Splunk through HEC



REFERENCE DEPLOYMENT

Red Hat OpenShift on AWS

Container application platform with Kubernetes orchestration on the AWS Cloud

View deployment guide

This Quick Start sets up a cloud architecture and deploys Red Hat OpenShift Container Platform on AWS.

Red Hat OpenShift Container Platform is based on Docker-formatted Linux containers, Google Kubernetes orchestration, and Red Hat Enterprise Linux (RHEL).

The Quick Start includes AWS CloudFormation templates that build the AWS infrastructure using AWS best practices, and then pass that environment to Ansible playbooks to build out the OpenShift environment. The deployment provisions OpenShift master instances, etcd instances, and node instances in a highly available configuration.

This deployment also includes AWS Service Broker, which provides direct access to AWS services on the Red Hat OpenShift Container Platform.

RED HAT OPENSHIFT

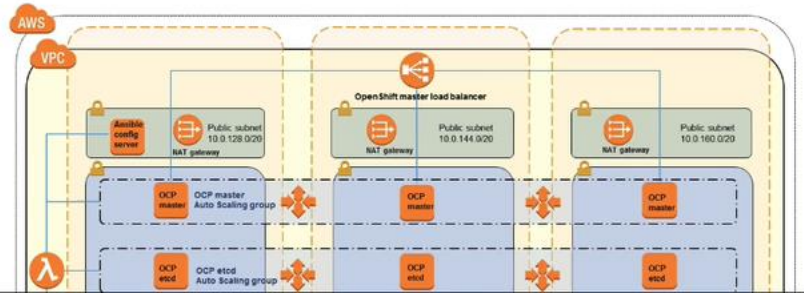
This Quick Start was developed by AWS solutions architects.

Request AWS credits for this deployment

What you'll build | How to deploy | Cost and licenses

Use this Quick Start to automatically set up the following Red Hat OpenShift environment on AWS:

- A virtual private cloud (VPC) that spans three Availability Zones, with one private and one public subnet in each Availability Zone.*
- An internet gateway to provide internet access to each subnet.*
- In one of the public subnets, an Ansible config server instance.
- In the private subnets:
  - Three OpenShift master instances in an Auto Scaling group



Testing

Benchmarking Guidelines

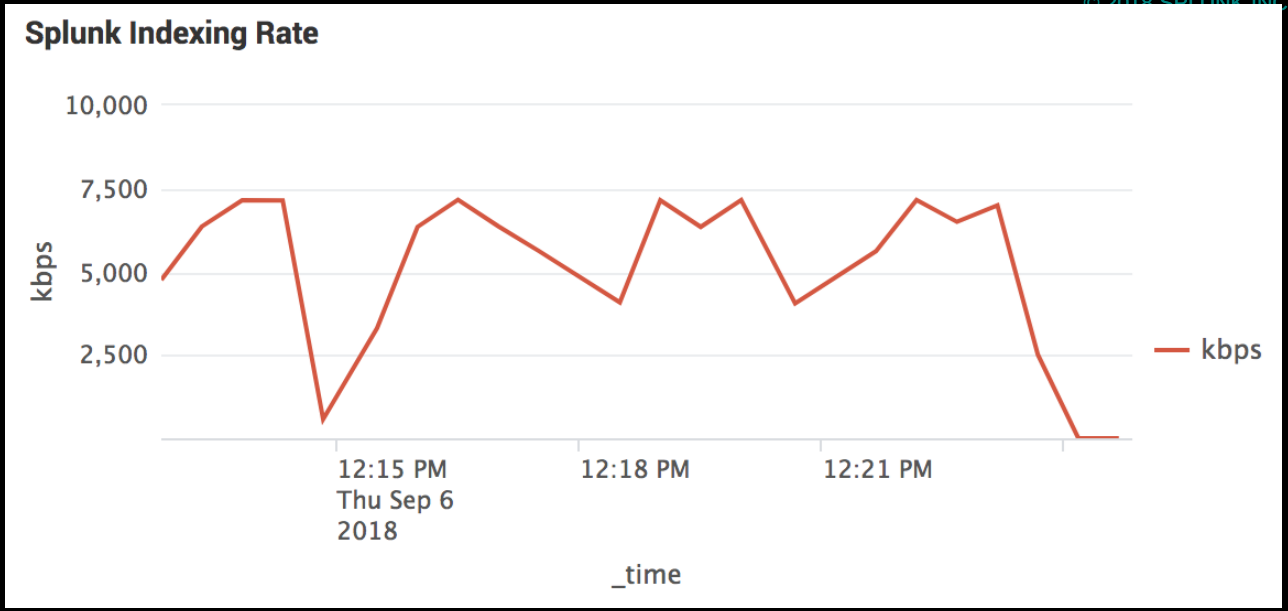
Environment and Setup

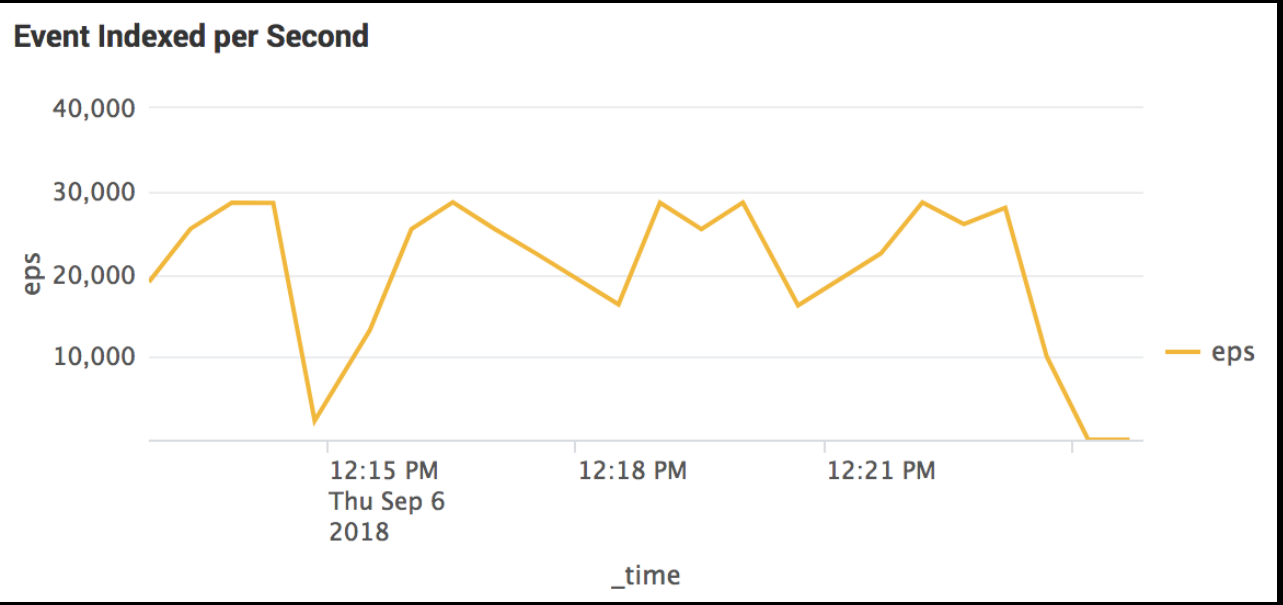
- 3 Node Kubernetes Cluster
  - Master - m4.large
  - Nodes - m4.16xlarge
- Splunk Deployment
  - Focus is on a single node indexer performance
- Tested with different message sizes
  - 256 Byte
  - 1 KiB
- 30 containers generating 1000 messages/sec each
  - 30K messages/sec/node

Benchmarking Results

256 byte Message Size

- **Consistent ~7.5 Mbps and ~30K EPS through indexer**
- Results repeatable with different buffer size
- Executed 4X with 60 sec pause in between

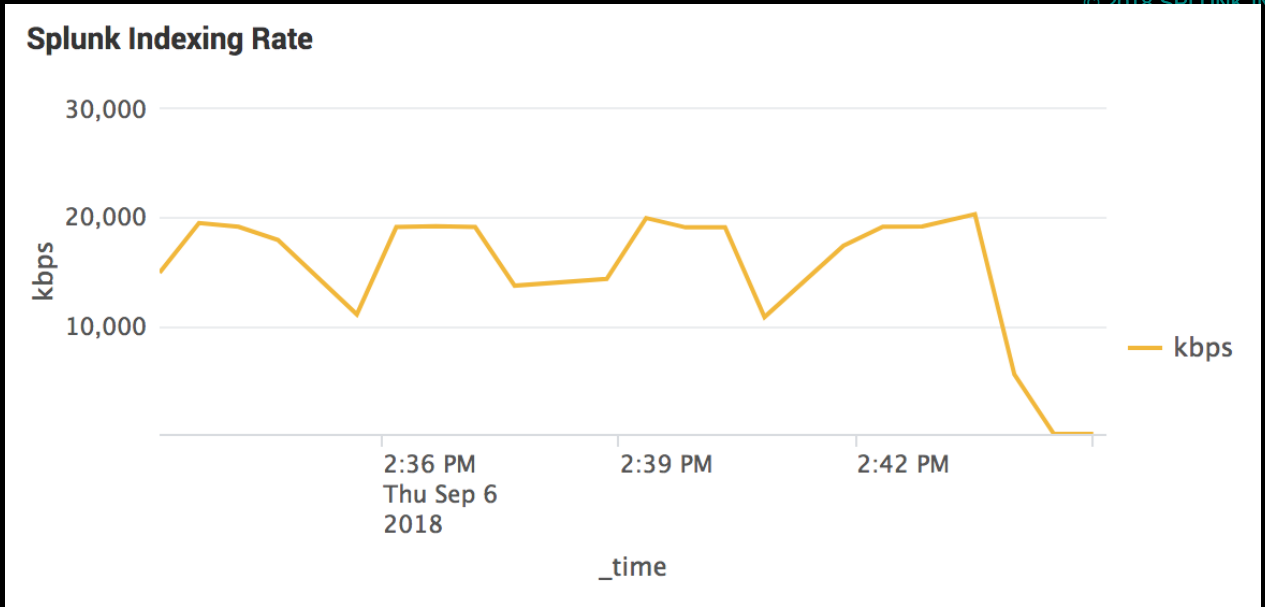


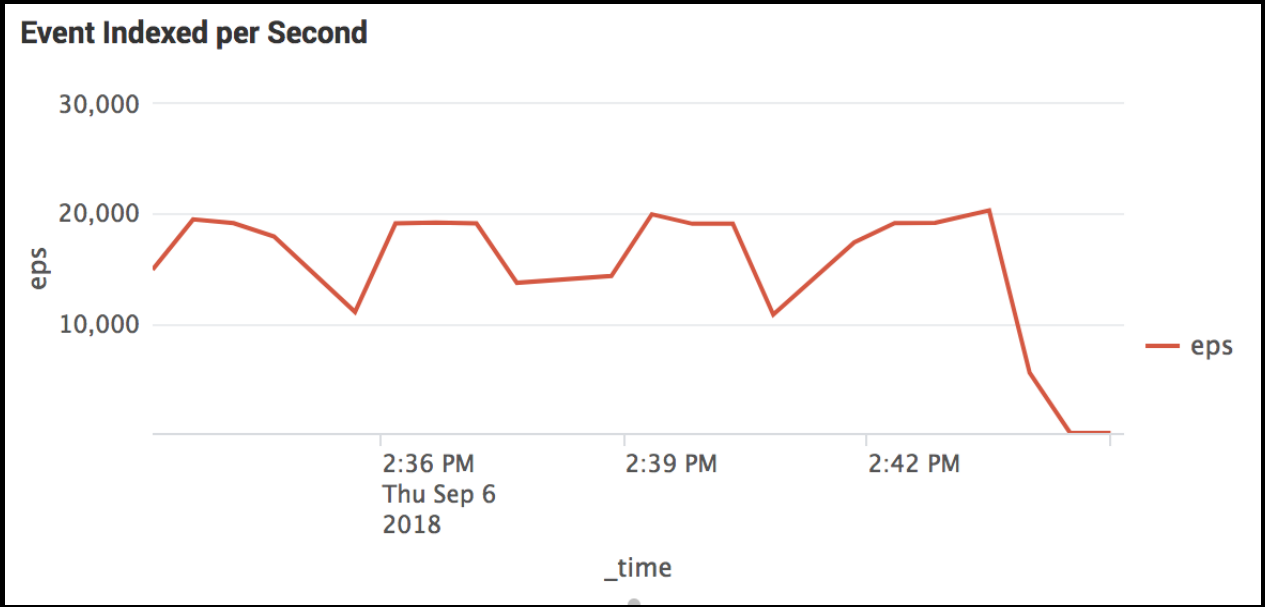


Benchmarking Results

1KiB Message Size

- **Consistent ~20 Mbps and ~20K EPS through indexer**
- Results repeatable with different buffer size
- Executed 4X with 60 sec pause in between





Testing in the Wild

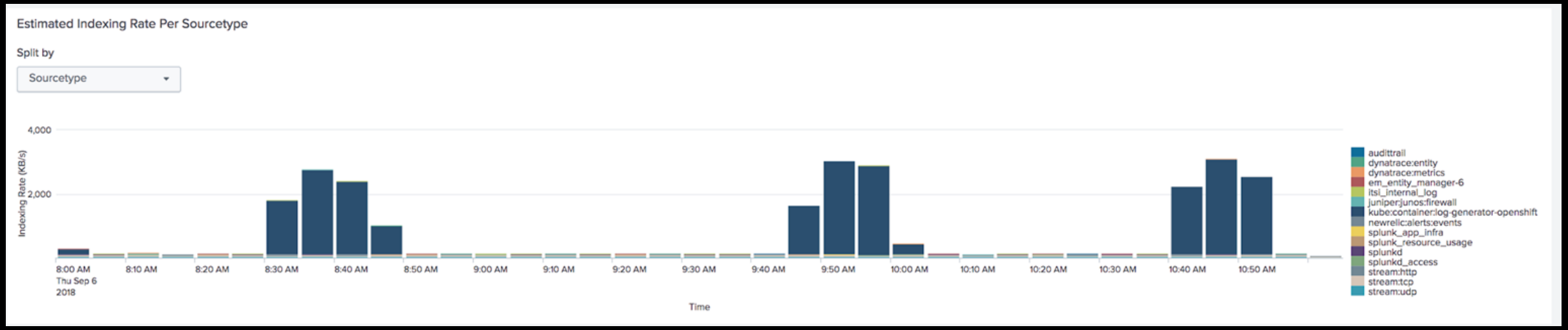
Results in a less controlled environment

- AWS Openshift Quickstart Cluster (Oregon)
  - 3x Master - m4.xlarge
  - 3x Nodes - m4.xlarge
- Splunk Deployment
  - Standalone Splunk with 2 indexing pipes
  - 12 Cores 96GB ram, bare metal with 20% CPU utilization
  - Consumer ISP internet (60Mbps down/ 10Mbps up)
- Message sizes
  - 256 bytes, 1000 bytes, 256KB
- 30 containers generating 1000 messages/sec each
- ~9 Million messages generated in 5 mins

Testing in the Wild

Results in a less controlled environment

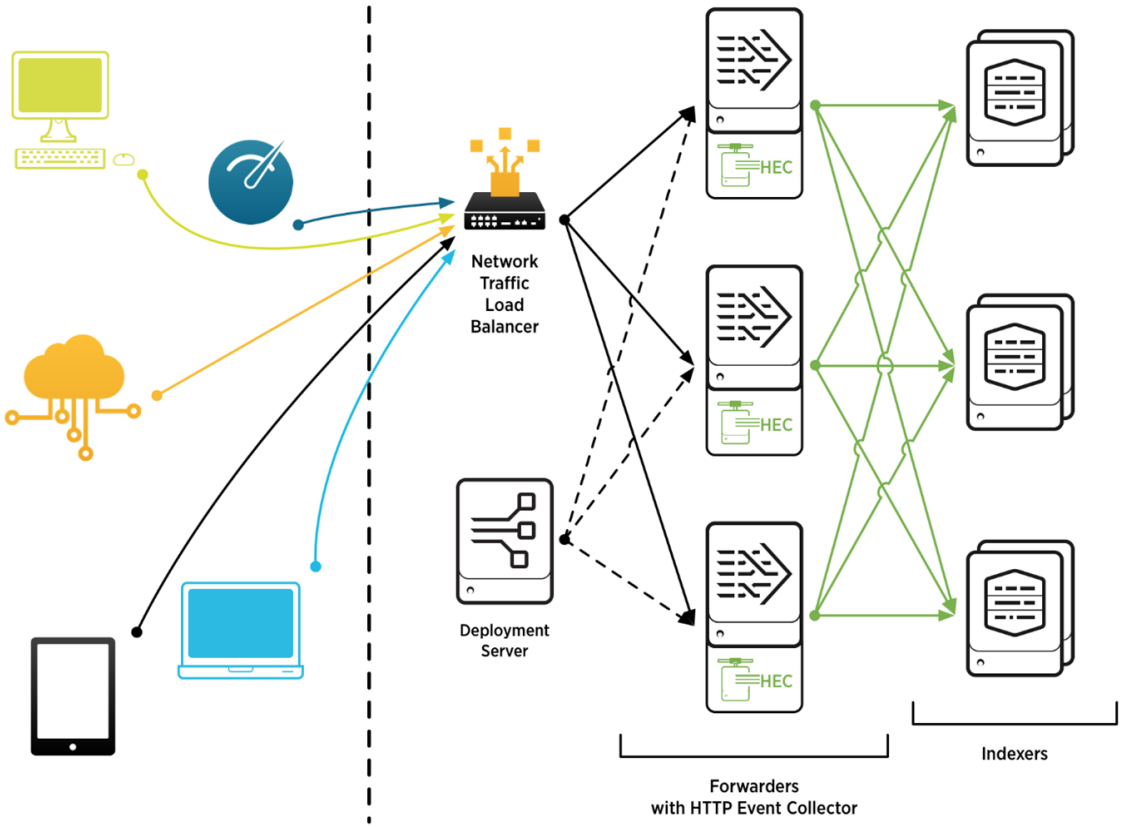
- Indexing throughput
  - Maxed ~3MB/s - Not bad for public internet!
- Indexing Latency
  - Saw up to ~7 mins indexing delay, but no message loss



Benchmarking Guidelines

Load Balancing

- HEC Architecture
- Single Connection (HF)
  - Each logging pod has 1 connection to HEC
  - HF or LB can be used to spread logs across indexer tier
  - HEC Deploy
    - http://dev.splunk.com/view/event-collector/SP-CAAAE73
  - NGINX
    - http://dev.splunk.com/view/event-collector/SP-CAAAE9Q



Key Takeaways

- Container orchestration is the foundation for current and future applications
- Splunk is the go to solution for container insights for every container deployment
- Extremely scalable and flexible

Q&A

Gimi Liang | Engineering
Matthew Modestino | Practitioner & Evangelist
David Baldwin | Product Management

splunk> .conf18

Looking for More?

Check out these sessions here at .conf18!

All Skill Levels | IT Operations

IT1501 - Deep Dive into Boss of the NOC 2018 with a Splunk IT Specialist

SCHEDULE

Thursday, Oct 04, 11:00 a.m. - 11:45 a.m.

Advanced | Foundations/Platform

FN1089 - Dockerizing Splunk at Scale 2: The Container Strikes Back

SCHEDULE

Thursday, Oct 04, 2:45 p.m. - 3:30 p.m.

Join us in the Innovation Lab for more on Splunk and containers!

splunk> .conf18

Resources

Resources Discussed During Session

- Splunk Connect for Kubernetes
  - Repo: https://github.com/splunk/splunk-connect-for-kubernetes
  - Gems:
    - https://rubygems.org/gems/fluent-plugin-kubernetes-objects
    - https://rubygems.org/gems/fluent-plugin-splunk-hec
  - Docker Hub:
    - https://hub.docker.com/r/splunk/fluentd-hec/
    - https://hub.docker.com/r/splunk/kube-objects/
- Splunk Connect for Docker
  - Repo: https://github.com/splunk/docker-logging-plugin
  - Docker Store: https://store.docker.com/plugins/splunk-connect-for-docker
- Universal Forwarder:
  - https://store.docker.com/community/images/splunk/universalforwarder

Resources

Resources Discussed During Session

- Splunk Connect for Kubernetes with Amazon EKS
  - Amazon EKS Blog: https://www.splunk.com/blog/2018/07/19/splunk-connect-for-kubernetes-on-eks.html
  - Demo: https://www.youtube.com/watch?v=_3QrIfBXpq0&list=PLhr1KZpdzukdc-jfSvpQYOO9nsOiCbVtX&index=4

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>