

IT2240 - Red Hat OpenShift and Splunk - Better Together!



Mattia Mascia | Red Hat

Matthew Modestino | Splunk



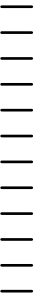
Mattia

Principal Consultant | Red Hat



Matt

IT Practitioner | Splunk



Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Agenda

Timestamps

1. Intro & Overview 2 min
2. OpenShift Container Platform 5 min
3. Red Hat Universal Base Image 5 min
4. Splunk 2min
5. Splunk Operator 3 min
6. Splunk Connect for Kubernetes, App for Infrastructure & Business Flow 10min
7. Use Cases 5 min
8. Q&A 5 min

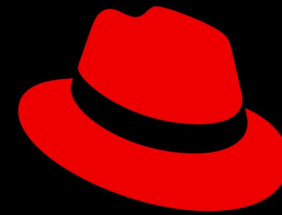
“Last Page First!”

A great guiding principal for us Techies 😊

Red Hat & Splunk

Red Hat + Splunk partnership delivers key outcomes for our customers!

- Enterprise Platforms
- Simple, Secure & Scalable
- Hybrid - Any Data Center. Any Data.
- Opensource & Community



Red Hat

splunk 

Metrics Analysis | Splunk App | x +

← → ↻ Not Secure | i-02782275744fca325.ec2.splunkit.io:8000/en-US/app/splunk_app_infrastructure/metrics_analysis?group=19e3209c-bdd1-4494-8df7-b6835929bf80

splunk>enterprise App: Splunk App for Infrastructure Administrator Messages Settings Activity Help Find

Investigate Alerts Add Data Settings Dashboards Splunk App for Infrastructure

microk8s-splunk (6) cluster_name: microk8s pod_namespace: splunk

Data Last 3 hours Split by Refresh (1h ago) Clear all Analysis

Find Data to Analyze

Metrics

- kube
 - container
 - cpu
 - usage
 - usage_rate
 - logs
 - memory
 - available_bytes
 - major_page_faults
 - page_faults
 - rss_bytes
 - usage_bytes
 - working_set_bytes
 - rootfs
 - uptime
 - pod
 - cpu
 - usage
 - usage_rate
 - ephemeral-storage
 - memory

Events

kube.pod.cpu.usage_rate by pod-name

kube.pod.memory.usage_bytes by pod-name

kube:container:splunk-fluentd-k8s-metrics-aggr

AGGREGATIONS

Select one or more aggregations to display in the chart.

Avg Max Min

Std dev Sum

Percentiles

90 x 75 x 50 x 25 x 10 x

TIME COMPARISON

Overlay previous time period on the selected chart.

Compare to None

SPLIT BY

Split this metric by a dimension.

Split by pod-name

Display Highest 5

Stack Series

FILTERS

Include or exclude metrics from specific categories.

cluster_name

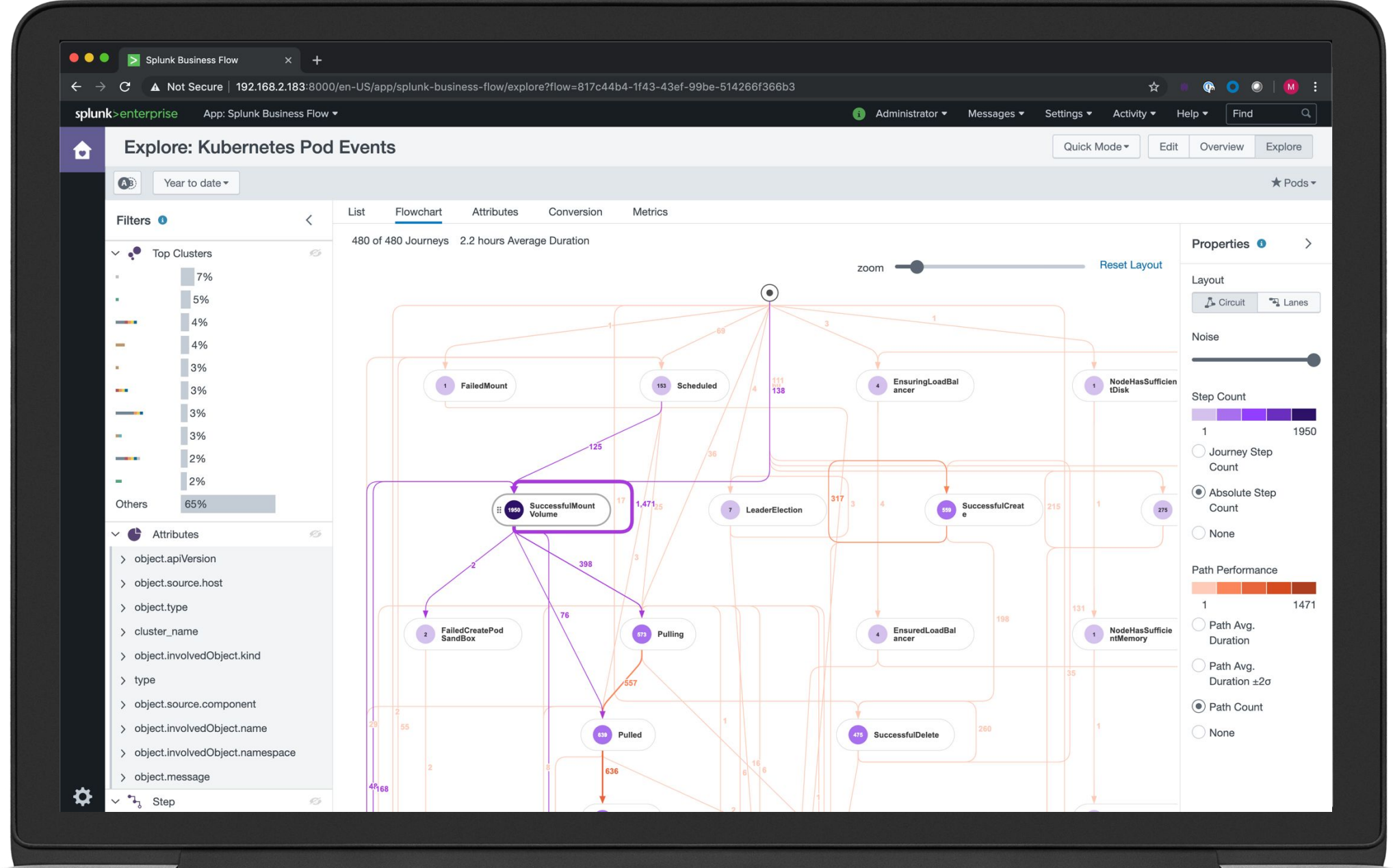
entity_type

extracted_source

host

index

node





OpenShift Container Platform

What is it?

“OpenShift is an Integrated Platform”

It's not Just Kubernetes Certified!

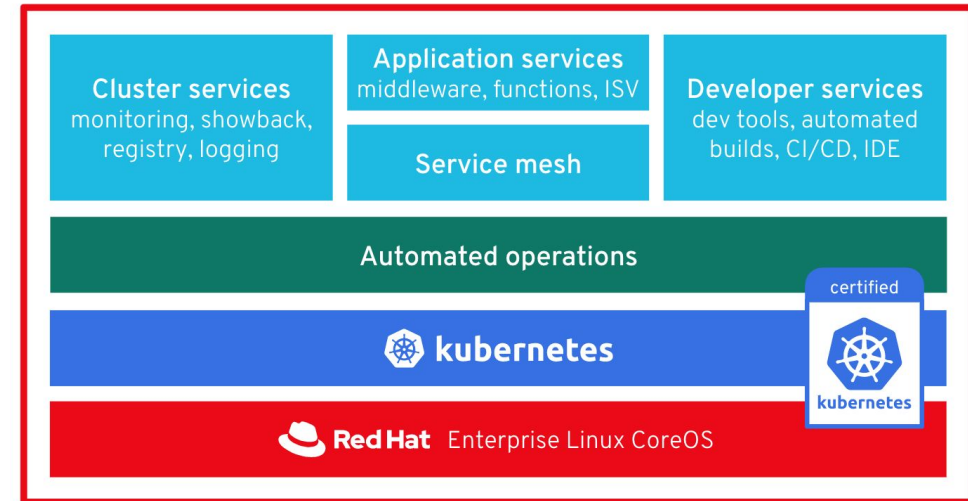
OpenShift Container Platform

Everything you need, out of the box

- Fully integrated and automated architecture
- Seamless Kubernetes deployment on any cloud or on-premises environment



Best IT ops experience — CaaS ↔ PaaS | FaaS — Best developer experience



Physical



Virtual



Private



Public

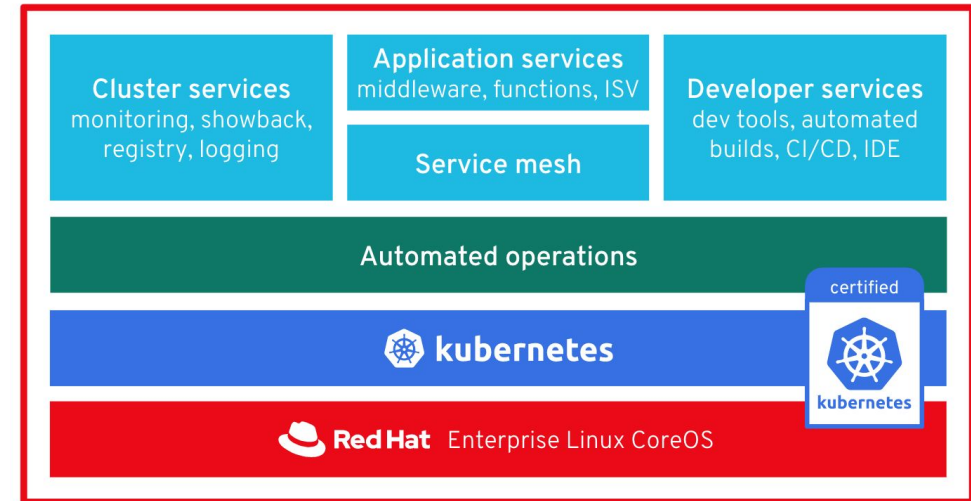
OpenShift Container Platform

Everything you need, out of the box

- Fully automated installation, from cloud infrastructure to OS to application services
- One click platform and application updates
- Auto-scaling of cloud resources



Best IT ops experience | CaaS ↔ PaaS | FaaS | Best developer experience



Physical



Virtual



Private



Public



Red Hat Universal Base Image

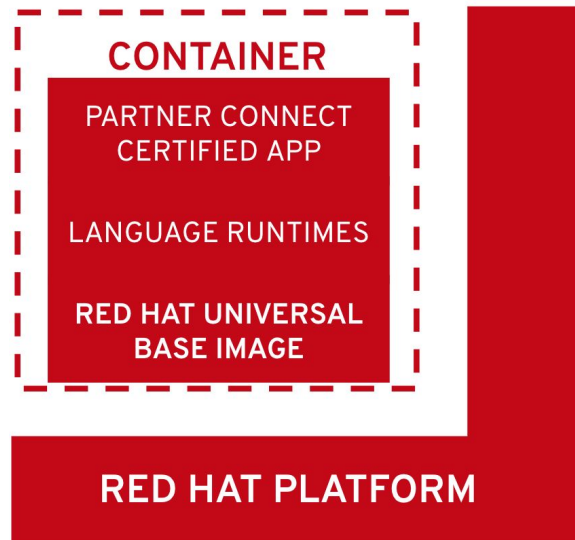
A bold change that will help us expand the ecosystem

“Red Hat Universal Base Image”

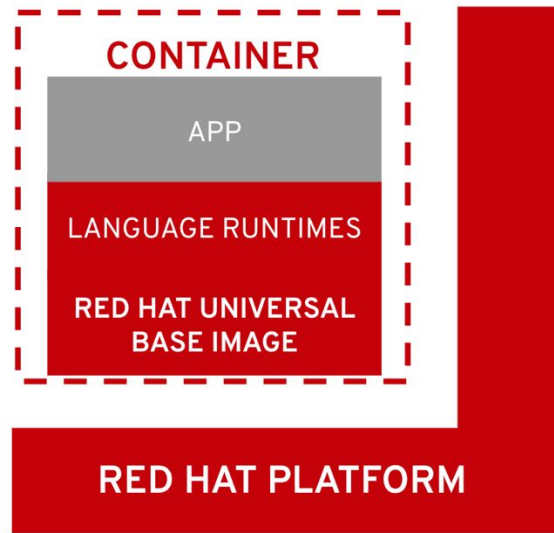
The aim is to be the highest quality and most flexible base container image available

Can Be Build & Deployed Anywhere

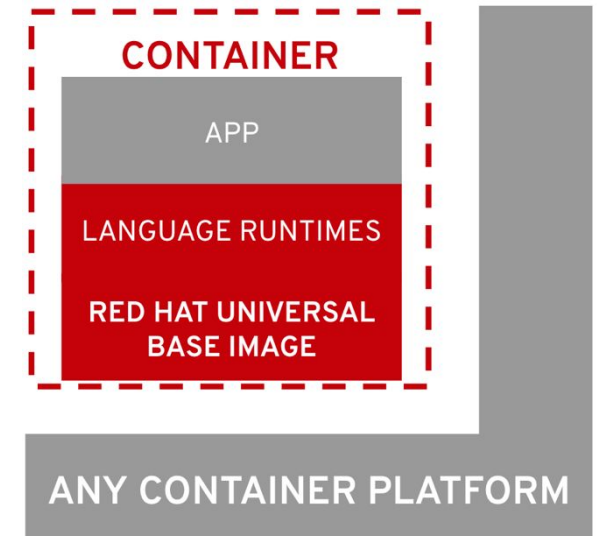
Building on UBI is the first step



“Certification provides the highest level of support.”



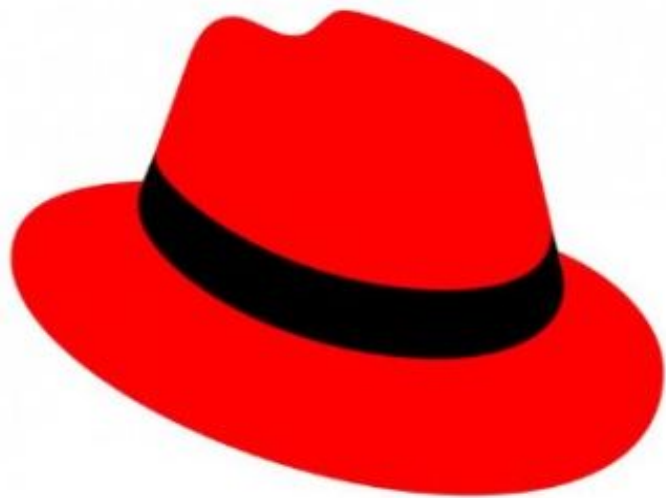
“Enterprise support when run on Red Hat platforms”



“Trusted base for any environment”

“On The Shoulders of Giants!”

Leaving the the OS & Infra to the Pros so we
can Splunk!



splunk[®]>



Splunk

Any Question. Any Data. One Splunk.

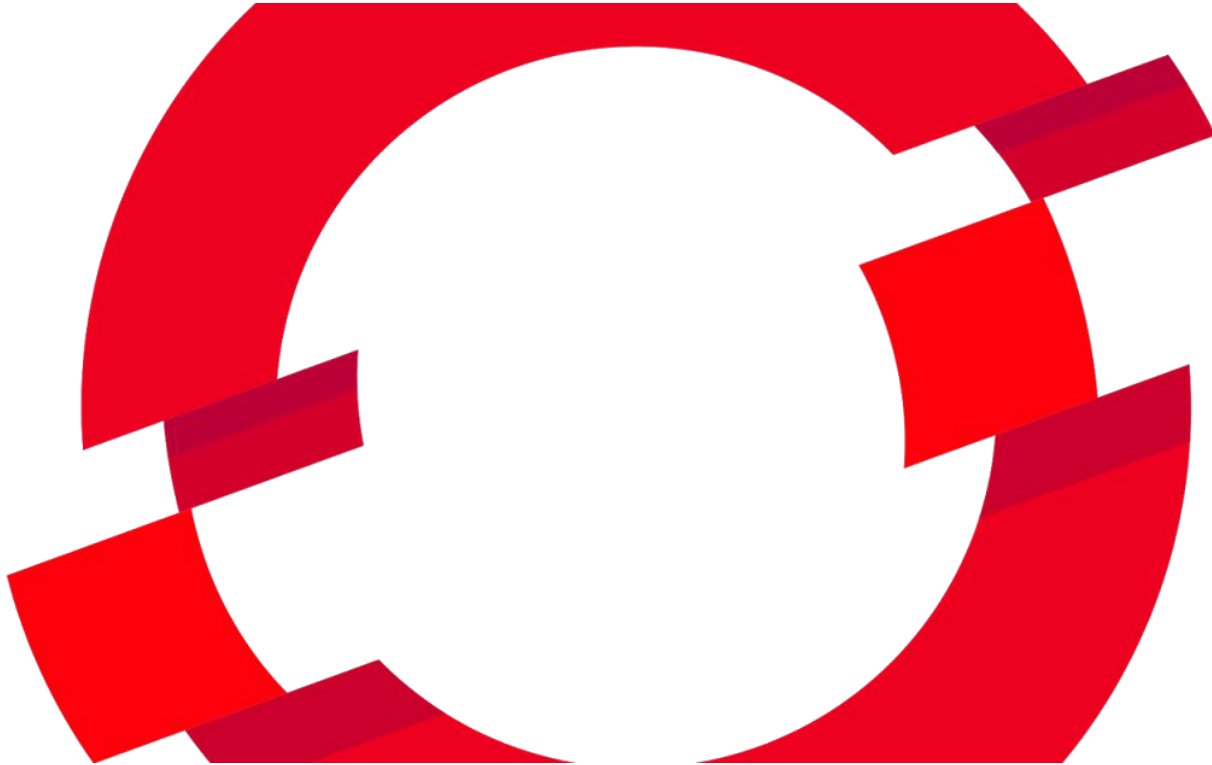


Splunk Operator

Deploying the Splunk Platform on Openshift
with Red Hat Universal Base Image

Splunk Operator

Encoding Operational Knowledge



```
apiVersion: enterprise.splunk.com/v1alpha1
kind: SplunkEnterprise
metadata:
  name: cluster
  finalizers:
  - enterprise.splunk.com/delete-pvc
spec:
  splunkVolumes:
  - name: licenses
    configMap:
      name: splunk-licenses
  licenseUrl: /mnt/licenses/enterprise.lic
  resources:
    splunkVarStorage: 10Gi
    splunkIndexerStorage: 50Gi
  topology:
    indexers: 3
    searchHeads: 3
```



Splunk App for Infrastructure

The easy button for OpenShift Integration

Add Data | Splunk App for Infra x +

Not Secure | i-02782275744fca325.ec2.splunkit.io:8000/en-US/app/splunk_app_infrastructure/configure

splunk>enterprise App: Splunk App for Infrastructure Administrator Messages Settings Activity Help Find

Investigate Alerts Add Data Settings Dashboards Splunk App for Infrastructure

Configure Integrations

- Linux/Unix
- AWS
- Windows
- OSX
- Kubernetes
- OpenShift

To monitor your OpenShift deployment, follow the instructions below.

- 1 Prepare for deployment**

Install the [Helm client](#) and [OpenShift Container Platform CLI](#) on a local machine you'll use to set up data collection.

The script runs the `helm template` command to render manifests locally. The script does not attempt to install Tiller on your cluster to deploy manifests.

Download Config Only This option generates manifests but does not deploy them. If you enable this option, you have to manually deploy the manifests.
- 2 Specify configuration options**

Data to be collected 2 Objects [Customize Objects](#)

Monitoring machine
Specify the FQDN or IP address of the system you want to send data to. Do not enter a hostname.

HEC token
Enter the HEC token you configured to send data to the app. The HEC token's sourcetype must be `em_metrics`. [Global HEC settings must have tokens enabled.](#)

HEC port
Enter the HEC port of the system you want to send metrics data to. The recommended port is 8088.

Cluster name
Specify a name for the cluster. Use a unique name. This creates a cluster name dimension to track entities from the cluster.

OpenShift project

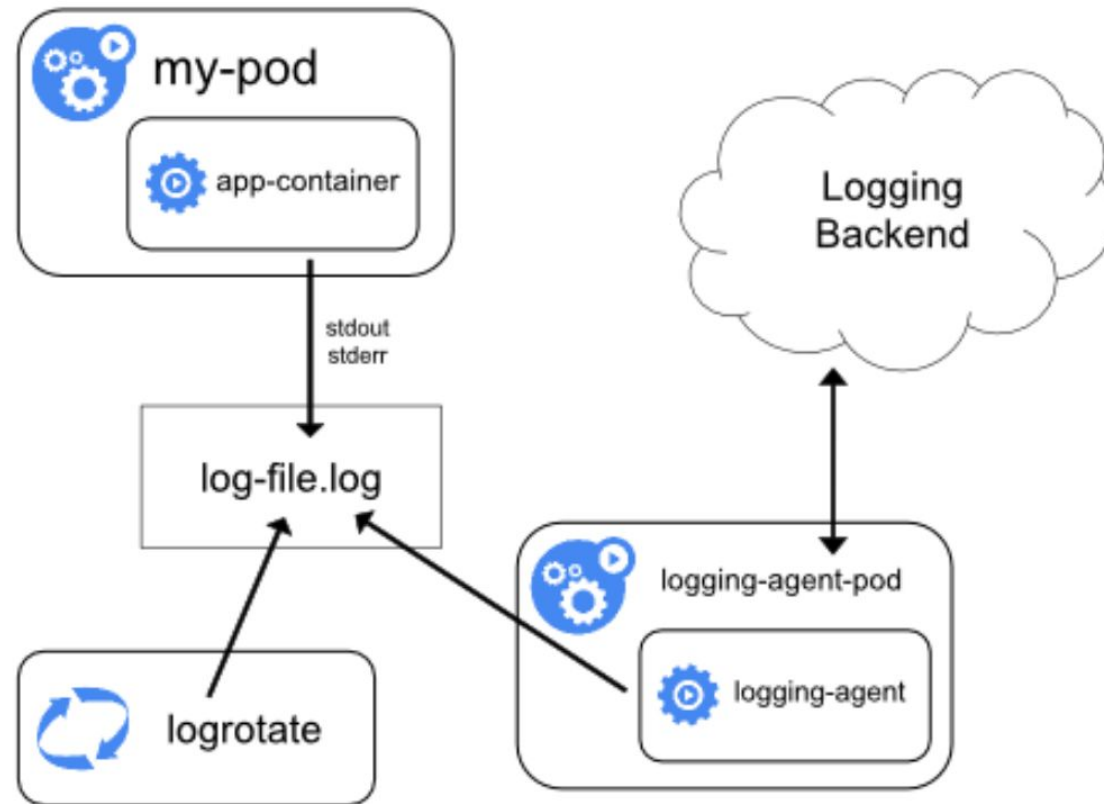


Splunk Connect for Kubernetes

Kubernetes Data Collection by Splunk & the
open source Community!

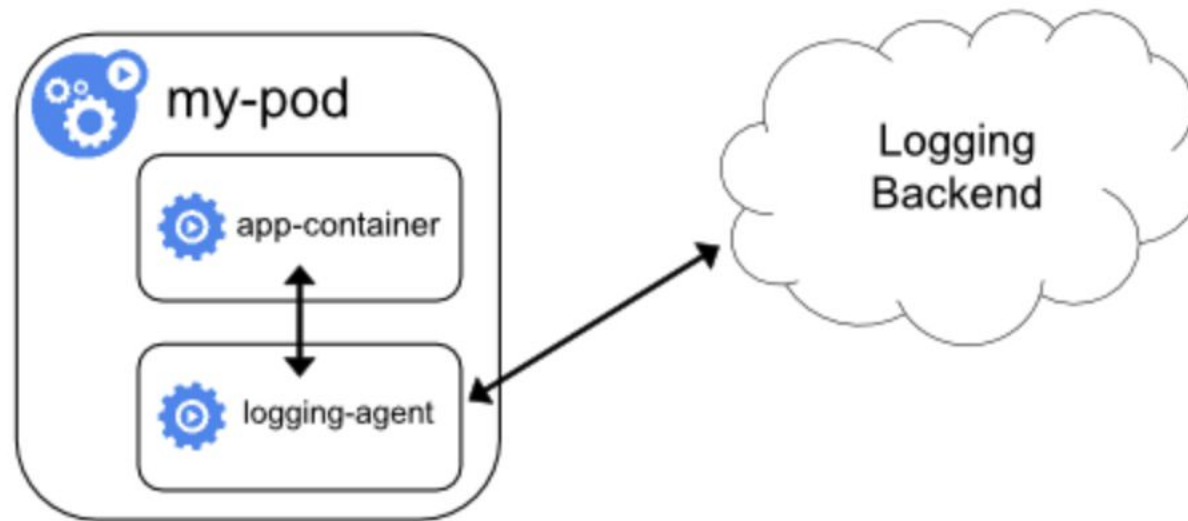
Kubernetes Logging Architecture

Node Agent



Kubernetes Logging Architecture

Sidecar Agent



Splunk Connect for Kubernetes

Kubernetes Data Sources



Splunk Kubernetes
Logging



Splunk Kubernetes
Metrics

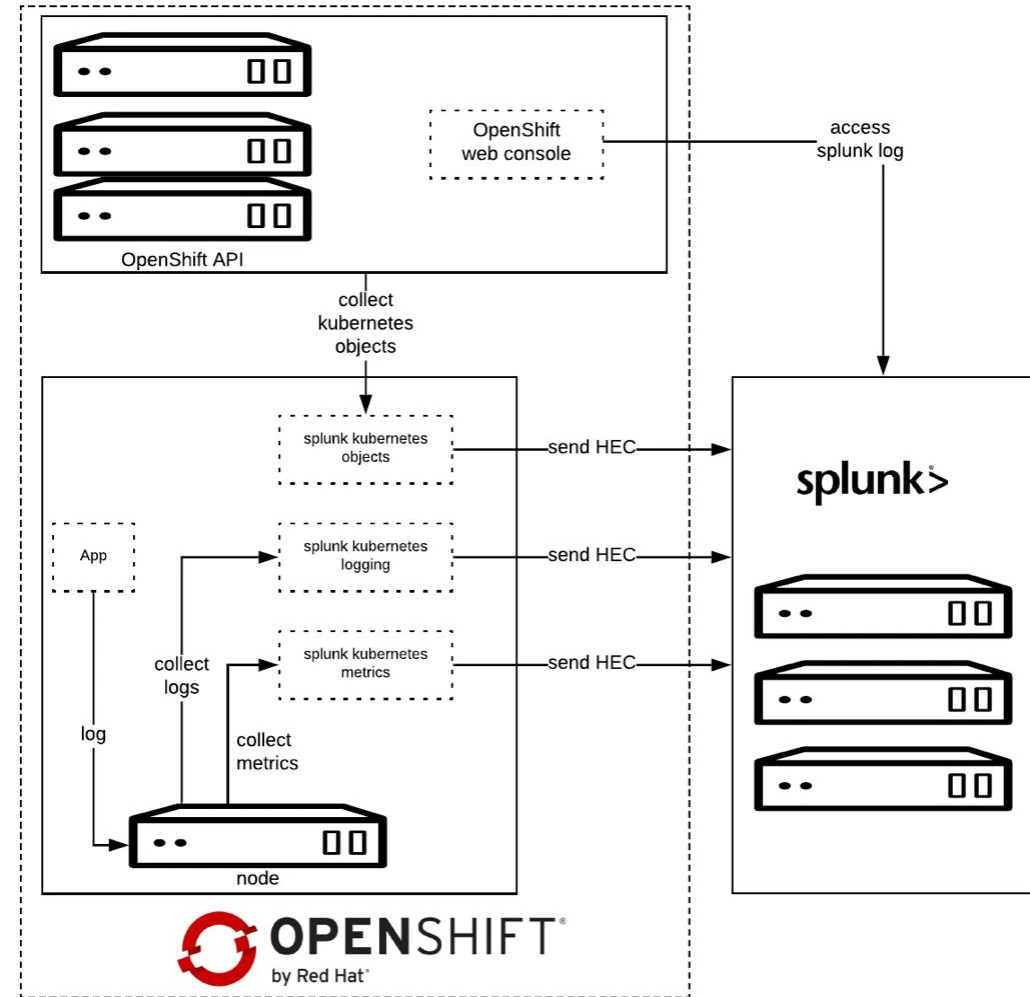


Splunk Kubernetes
Objects

Architecture

Logging, Metrics, Objects

- Logging DaemonSet
- Metrics DaemonSet
- Metrics-Agg Deployment
- Objects Deployment
- OpenShift Web Console



Splunk Kubernetes Logging

Application & OpenShift Cluster Logging



Splunk Kubernetes Objects

OpenShift Metadata Collection



Splunk Kubernetes Metrics

OpenShift Platform Metrics



OpenShift Web Console

Extending OpenShift Console

The screenshot displays the OpenShift Container Platform web console interface. The top navigation bar includes the 'OPENSIFT CONTAINER PLATFORM' logo, a user profile for 'Mascia Mattia', and a search bar labeled 'Search Catalog'. The left sidebar contains navigation options: Overview, Applications, Builds, Resources, and Storage. The main content area shows the details for a pod named 'strimzi-cluster-operator-67cc499c74-q98hk', which was created 16 days ago. The 'Logs' tab is selected, showing a log entry from the container 'strimzi-cluster-operator' running on April 16, 2019, at 4:52:11 PM. The log message is: '2019-04-25 17:20:13 INFO ClusterOperator:118 - Triggering periodic reconciliation for namespace kafka-devl...'. A pink rectangular overlay is positioned over the 'splunk>' button and the 'Follow' button in the log viewer interface.

“Make the Data Dance!”

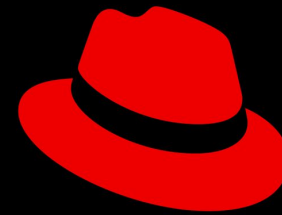
OpenShift Use Case Demos

Demo

Red Hat & Splunk

Red Hat + Splunk partnership delivers key outcomes for our customers!

- Enterprise Platforms
- Simple, Secure & Scalable
- Hybrid – Any Data Center. Any Data.
- Open source & Community



Red Hat

splunk 



Q&A

Mattia Mascia | Red Hat
Matthew Modestino | Splunk

<https://www.openshift.com>

<https://docs.splunk.com/Documentation/InfraApp/latest/Admin/AddDataOpenShift>

<https://github.com/splunk/splunk-connect-for-kubernetes>

<https://github.com/splunk/docker-splunk>

<https://github.com/splunk/splunk-operator>



splunk>

Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

