Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing 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. © 2022 Splunk Inc. All rights reserved.

© 2022 SPLUNK INC.

Scalability and Efficiency with the Splunk® OpenTelemetry Collector for Kubernetes®

OBS1668C

Jodee Varney
Product Manager | Splunk

Aunsh Chaudhari
Product Manager | Splunk

splunk> .conf22

© 2022 SPLUNK INC.

Jodee Varney

Product Manager
Getting Data In, Splunk® Enterprise

Aunsh Chaudhari

Product Manager
Getting Data In, Splunk® Observability Cloud

splunk> .conf22

© 2022 SPLUNK INC.

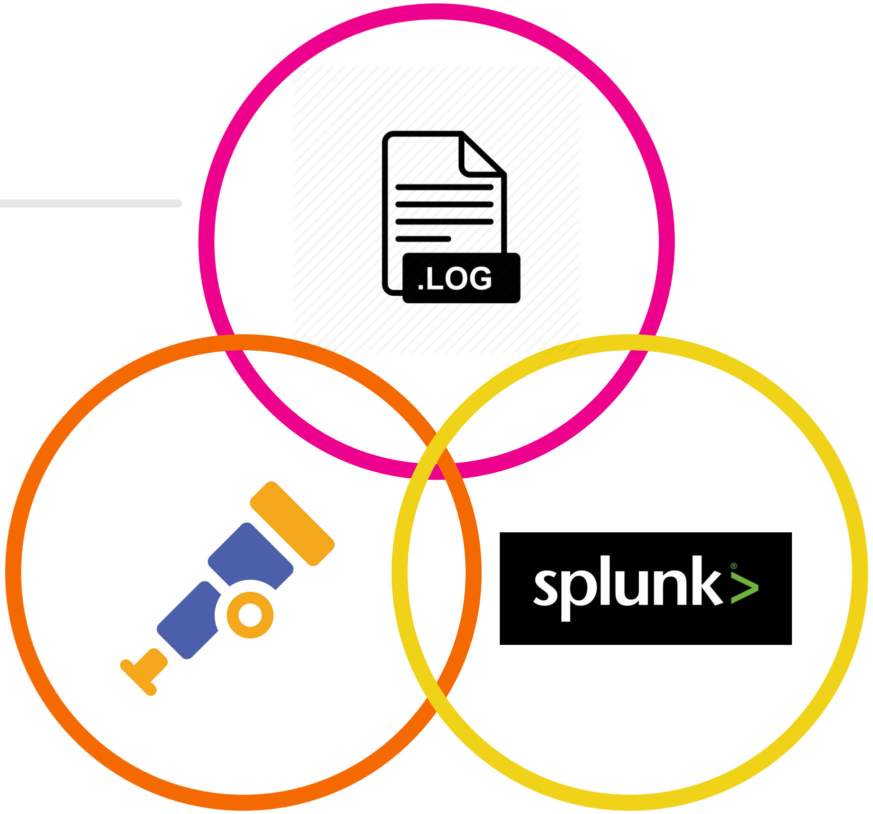
Agenda

- Use the Splunk® OpenTelemetry Collector for Kubernetes to send data to Splunk® Enterprise and Observability Cloud
- Why use Splunk® OpenTelemetry Collector for Kubernetes ?
- Useful background on the OpenTelemetry Collector
- DEMO
- Explore some cool stuff that you can do
- Closing

© 2022 SPLUNK INC.

Splunk OpenTelemetry Collector for K8s

A single agent for both Splunk® Enterprise and Observability Cloud: Traces, Metrics & Logs!



OTel logs data model is now stable

OTel native logs has ↑↑↑ performance over fluentd

Splunk OTel Collector for K8s supports sending logs to Splunk® Enterprise and/or o11y

© 2022 SPLUNK INC.

Performance, performance, performance

Native OTel logging offers significant benefits over Fluentd

	EPS	Volume (GB/Day)	Mem Max (MiB)	CPU Usage (core)
SCK/fluentd	2,303	32	252	1
SOCK/fluentd	3,143	44	219	1
SOCK/otel	**9,971**	**135**	**978**	**1**

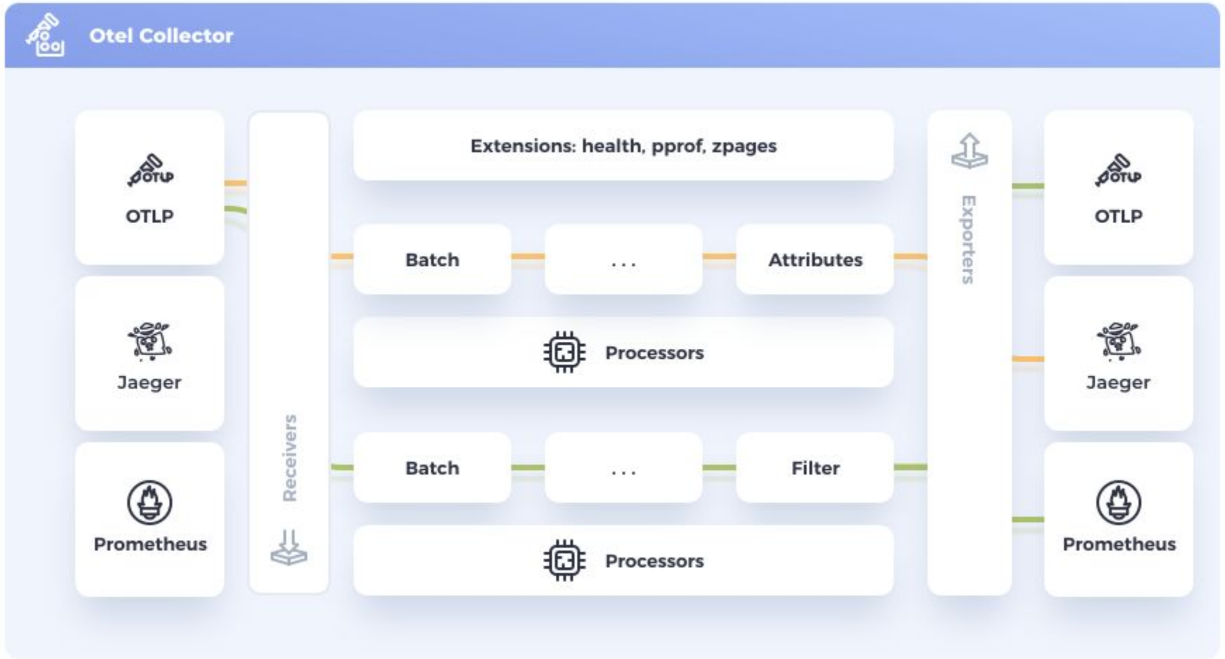
Significant events per second throughput improvement

Much greater flexibility: can use multiple cores, which is not possible with fluentd

© 2022 SPLUNK INC.

OpenTelemetry Collector

- **Architecture view**



- Components
  - **Receivers:** how you get data in (can be push or pull-based)
  - **Processors:** what you to do the data (e.g. batching, metadata, etc.)
  - **Exporters:** how you get data out (can be push or pull-based)
  - **Extensions:** things you do in the collector typically outside processing data (e.g. health check)
- Configuration is done in YAML and consists of two steps:
  - Define component configuration
  - Enable the component

© 2022 SPLUNK INC.

Configuration

- Configure SOCK to send data to your desired destination(s):
  - Splunk® Enterprise:

    ```
    splunkPlatform:
        token: xxxxxx
        endpoint: http://localhost:8088/services/collector
    ```

  - Splunk® Observability Cloud:

    ```
    splunkObservability:
         accessToken: xxxxxx
         realm: <realm>
    ```

  - Splunk® Enterprise or Observability Cloud:

    ```
    clusterName: <clusterName>
    ```

- And, to use OpenTelemetry logs collection instead of fluentd:
  - Splunk® Enterprise or Observability Cloud:

    ```
    logsEngine: otel
    ```

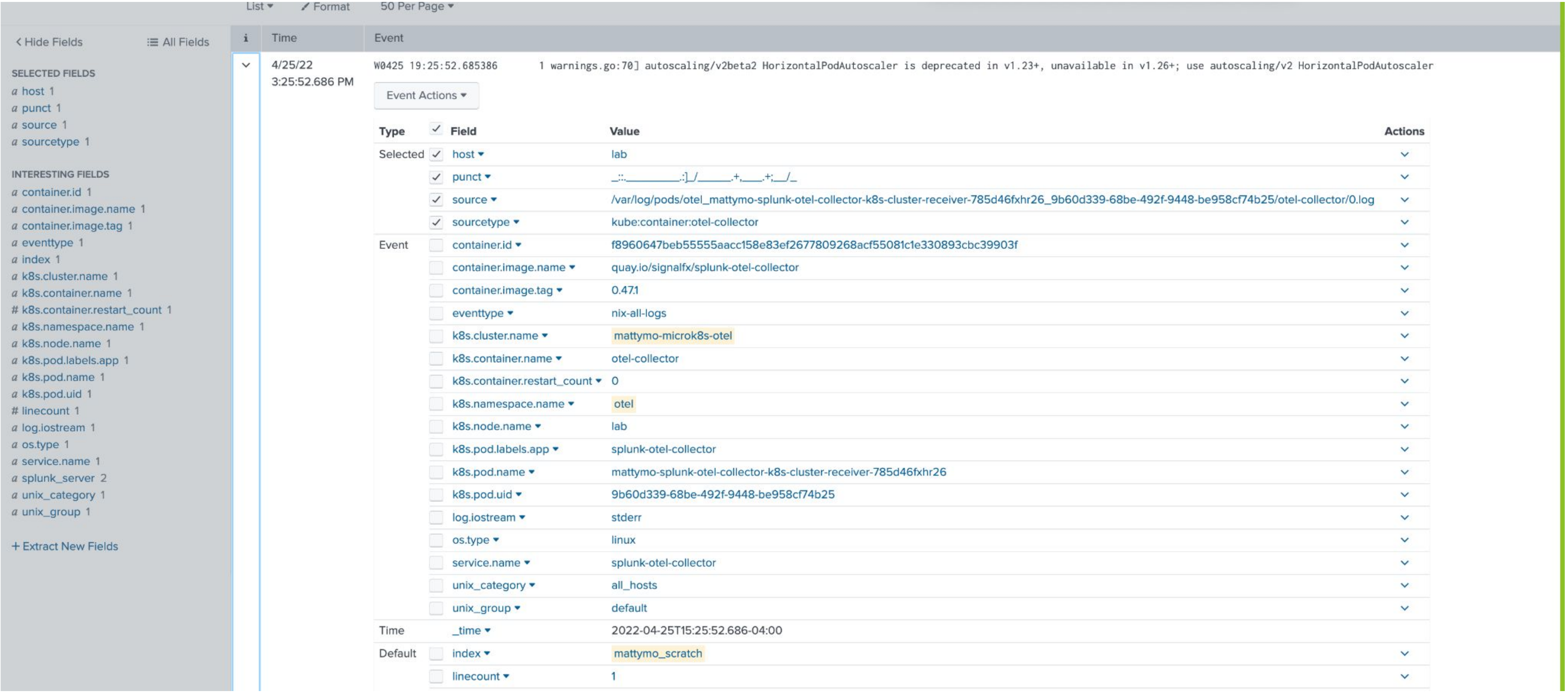
© 2022 SPLUNK INC.

What does a payload look like?

Under the covers

```
{
  "timestamp": "2022-04-25T19:25:52.685386",
  "body":  "2022-04-25 19:25:52.685 1 warnings.go:70 autoscaling/v2beta2 HorizontalPodAutoscaler is deprecated in v1.23+,
unavailable in v1.26+; use autoscaling/v2”,
  "attributes": {
    "log.iostream": "stdout"
  },
  "resource": {
    "com.splunk.source":
"/var/log/pods/otel_mattymo-splunk-otel-collector-k8s-cluster-receiver-785d46fxhr26_9b60d339-68be-492f-9448-be958cf74b25/otel-coll
ector/0.log",
    "com.splunk.sourcetype": "kube:container:otel-collector",
    “k8s.cluster.name”: “mattymo-microk8s-otel”
    "k8s.container.name": "otel-collector",
    "k8s.container.restart_count": "0",
    "k8s.namespace.name": "otel",
    “k8s.pod.labels.app”: “splunk-otel-collector”
    "k8s.pod.name": "mattymo-splunk-otel-collector-k8s-cluster-receiver-785d46fxhr26",
    "k8s.pod.uid": "c273b74e-2f9b-4c21-8912-20f6681ea6b3"
  }
}
```

© 2022 SPLUNK INC.



SELECTED FIELDS

a host 1
a punct 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a container.id 1
a container.image.name 1
a container.image.tag 1
a eventtype 1
a index 1
a k8s.cluster.name 1
a k8s.container.name 1
# k8s.container.restart_count 1
a k8s.namespace.name 1
a k8s.node.name 1
a k8s.pod.labels.app 1
a k8s.pod.name 1
a k8s.pod.uid 1
# linecount 1
a log.iostream 1
a os.type 1
a service.name 1
a splunk_server 2
a unix_category 1
a unix_group 1

+ Extract New Fields

4/25/22
3:25:52.686 PM

```
W0425 19:25:52.685386       1 warnings.go:70] autoscaling/v2beta2 HorizontalPodAutoscaler is deprecated in v1.23+, unavailable in v1.26+; use autoscaling/v2 HorizontalPodAutoscaler
```

Type	✓	Field	Value	Actions
Selected	✓	host ▾	lab	⌄
	✓	punct ▾	_::__________:]_/______.+,____.+;__/_	⌄
	✓	source ▾	/var/log/pods/otel_mattymo-splunk-otel-collector-k8s-cluster-receiver-785d46fxhr26_9b60d339-68be-492f-9448-be958cf74b25/otel-collector/0.log	⌄
	✓	sourcetype ▾	kube:container:otel-collector	⌄
Event	☐	container.id ▾	f8960647beb55555aacc158e83ef2677809268acf55081c1e330893cbc39903f	⌄
	☐	container.image.name ▾	quay.io/signalfx/splunk-otel-collector	⌄
	☐	container.image.tag ▾	0.47.1	⌄
	☐	eventtype ▾	nix-all-logs	⌄
	☐	k8s.cluster.name ▾	mattymo-microk8s-otel	⌄
	☐	k8s.container.name ▾	otel-collector	⌄
	☐	k8s.container.restart_count ▾	0	⌄
	☐	k8s.namespace.name ▾	otel	⌄
	☐	k8s.node.name ▾	lab	⌄
	☐	k8s.pod.labels.app ▾	splunk-otel-collector	⌄
	☐	k8s.pod.name ▾	mattymo-splunk-otel-collector-k8s-cluster-receiver-785d46fxhr26	⌄
	☐	k8s.pod.uid ▾	9b60d339-68be-492f-9448-be958cf74b25	⌄
	☐	log.iostream ▾	stderr	⌄
	☐	os.type ▾	linux	⌄
	☐	service.name ▾	splunk-otel-collector	⌄
	☐	unix_category ▾	all_hosts	⌄
	☐	unix_group ▾	default	⌄
Time		_time ▾	2022-04-25T15:25:52.686-04:00	
Default	☐	index ▾	mattymo_scratch	⌄
	☐	linecount ▾	1	⌄

© 2022 SPLUNK INC.

Advanced configuration

Cool stuff you can do

- Enable or disable particular types of telemetry
- Process or parse multi-line logs to help understand and trouble shoot them
- Use annotations to route or filter logs from a particular namespace or pod
- Transform events - more powerful than fluentd or Universal Forwarders
- Route logs dynamically based on their content with operators
- Add labels that can be used to enrich the log data collected

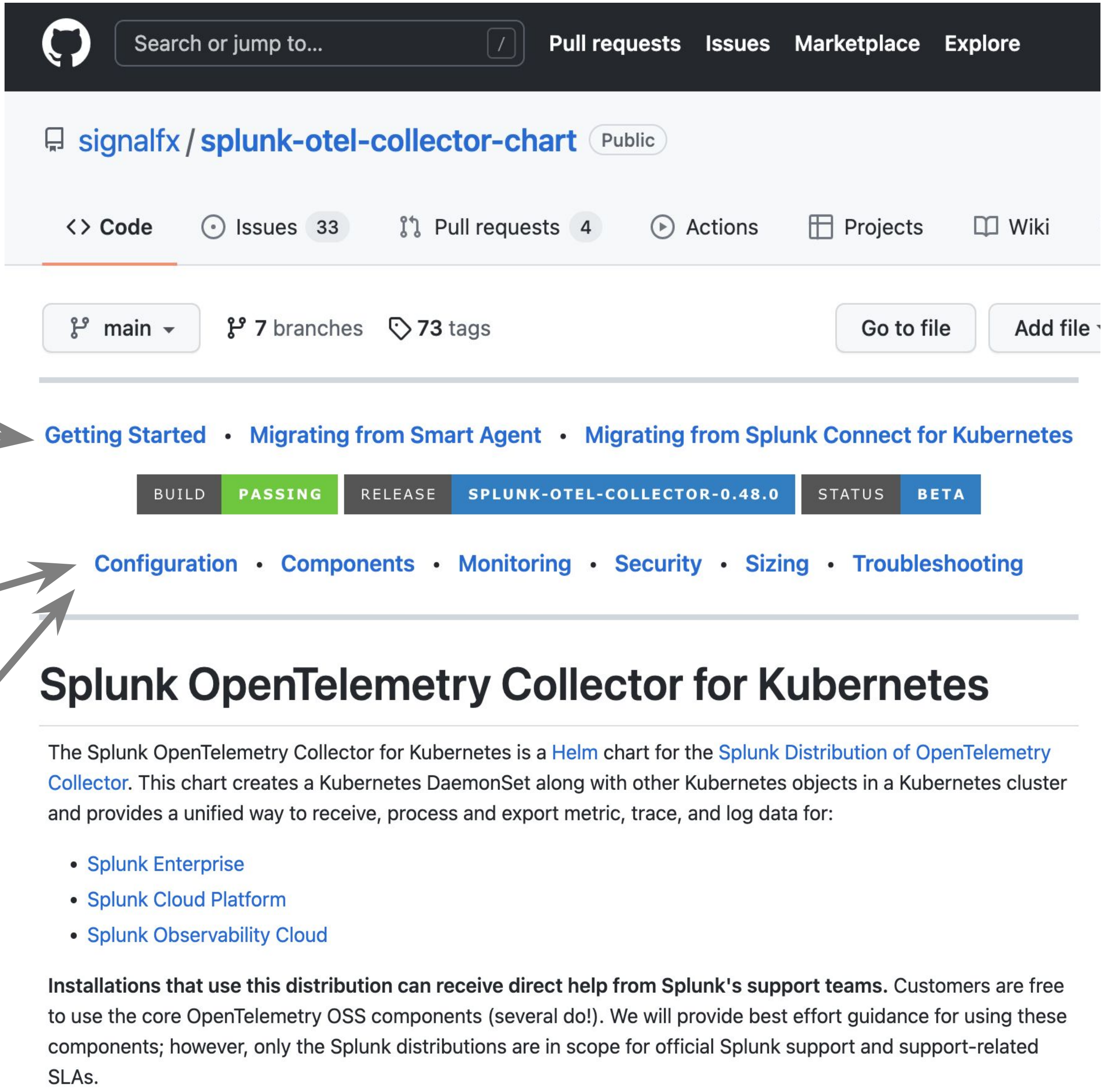
Powerful! Use at your discretion: processing costs resources at the edge.

© 2022 SPLUNK INC.

Where to go from here

It's easy to get started!

1. Get it running.
   - Go to https://github.com/signalfx/splunk-otel-collector-chart and deploy the Helm chart
2. Play around with routing & annotations - basic tools to shape your data.
3. Explore other operators & exporters - there are many levers available.
4. Use GitHub - ask questions, open issues, contribute!


Search or jump to...
Pull requests
Issues
Marketplace
Explore
signalfx / splunk-otel-collector-chart
Public
Code
Issues 33
Pull requests 4
Actions
Projects
Wiki
main
7 branches
73 tags
Go to file
Add file
Getting Started • Migrating from Smart Agent • Migrating from Splunk Connect for Kubernetes
BUILD PASSING
RELEASE SPLUNK-OTEL-COLLECTOR-0.48.0
STATUS BETA
Configuration • Components • Monitoring • Security • Sizing • Troubleshooting

Splunk OpenTelemetry Collector for Kubernetes

The Splunk OpenTelemetry Collector for Kubernetes is a Helm chart for the Splunk Distribution of OpenTelemetry Collector. This chart creates a Kubernetes DaemonSet along with other Kubernetes objects in a Kubernetes cluster and provides a unified way to receive, process and export metric, trace, and log data for:

- Splunk Enterprise
- Splunk Cloud Platform
- Splunk Observability Cloud

Installations that use this distribution can receive direct help from Splunk's support teams. Customers are free to use the core OpenTelemetry OSS components (several do!). We will provide best effort guidance for using these components; however, only the Splunk distributions are in scope for official Splunk support and support-related SLAs.

© 2022 SPLUNK INC.

Thank You

splunk> .conf22