

### **Splunk Open Telemetry Collector** for Kubernetes.

Step 1: Prepare the enviroment

Step 2: Install Kubectel, Kubernetes and HELM

#### Step 3: Install Otel Collector Helm Chart

- 1. Pull OTel helm repo locally, by running the following script
- 2. Open the values file
- 3. Check your pods for errors, Get running pods
- 4. View cluster-receiver pod logs with the following command
- 5. Check Splunk



### **OpenTelemetry Collector for Kubernetes.**

This Splunk validated architecture (SVA) applies to Splunk Cloud Platform and Splunk Enterprise products.



#### OpenTelemetry Collector incorporates many additional benefits, including:

- Built on OpenTelemetry open standards.
- Improved logging scale with OTel logging versus Fluentd. See https://github.com/ signalfx/splunk-otel-collector-chart/blob/main/docs/advanced-configuration. md#performance-of-native-opentelemetry-logs-collection
- Advanced metrics collection features.
- Advanced pipeline features including data manipulation.
- Support for trace collection.
- Support for Kubernetes annotations provides ability to route namespace and pod logs to certain indexes, set sourcetypes or even include or exclude logs from being monitored. See <u>https://github.com/signalfx/splunk-otel-collector-chart/</u> <u>blob/main/docs/advanced-configuration.md#managing-log-ingestion-by-using-annotations</u>
- Support for multiline logs via the filelog receiver's recombine operator. Users can
  define their line breaking rules in the collector to ensure multiline logs are properly
  rendered in Splunk. See : <u>https://github.com/signalfx/splunk-otel-collector-chart/
  blob/main/docs/advanced-configuration.md#processing-multi-line-logs</u>
- Access to OpenTelemetry components. See all components supported in the Splunk Helm chart at <u>https://github.com/signalfx/splunk-otel-collector/blob/main/ docs/components.md#components</u>

To deploy the OpenTelemetry Collector, some configuration is required by both Splunk admins and Kubernetes admins.

The following sections describe a simple process of getting started with the Splunk OpenTelemetry Collector for Kubernetes (without using the load balancer). Of course a high-level process can be configured depending on the customer's environment and aims in terms of the configuration and use

## **Step 1: Prepare the environment.**

1. First you are going to create 1 events index called otel\_events and 1 metrics index calles otel\_metrics

#### NOTE: YOU ARE BEING ASKED TO CREATE ONE EVENTS INDEX AND ONE METRICS INDEX! PLEASE CONFIGURE THE INDEX DATA TYPE ACCURATELY!!

See below the figures for more instructions on

eral Settings						
Index Name	otel_metrical		General Settings			
	Set Index name (e.g., INDEX_NAME). Search using index	-NDEX, WHE	Index Name	otel_events		
Index Deta Type	@Events	Ø Metrics		Set index neme (e.g., NOEX_NAME), Search using inde	INVERTING	
	The type of data to store jevent based or metrics)		Index Data Type	Eliverts .	Ø Metrics	
Home Path	optional		100000	The type of data to store (even-based or metrics).		
	Potiwern do peth. Leave blank for default (\$SPLIAN, D	BINDEX, NAVERAL	Home Path	optional		
Cold Pwth	optional			Holivern di petit. Leave blank for default (ESPUJNE, DEINDEX, NAREME		
	Cold do peth. Leeve blank for default (\$5PLUNC_DB/M	EX_NAMEAniatti,	Cold Peth	optional		
Thewed Path	optional		Thewed Path	Contract lines on the state of		
	Thered resurrected db peth. Leave blank for default (\$	PUNCOBINDEX,NWEItweedds		optional Nexedimentation of both Lazar bind to default (SDLINK DR/WDEX MARE/Parameters)		
Timestamp Resolution	Seconds	Miliseconds	Data Intentity Charle	Enable Disable		
	Specify the timestamp precision of the metrics in this intereduced search performance.	ios, indexes with militarcond timestang precision have		Enable this Eyou went Splank to compute heathes on every sites of your date for the purpose of data integ		
sx Size of Entire Index	500	68+	Max Size of Entire Index	500	60 -	
	Maximum target size of entire index.			Waximum target stor-of-entire index.		
Max Size of	8,00	68 *	Max Size of	euto	G8 =	
st/Warm/Cold Bucket	Maximum target size of buckets, Enter lauto_high_sclur	er for high-volume indexes.	Poerwarm/Cold Bucket	Maximum target size of buckets. Enter 'auto, high, velu	ine' for high-volume indexes.	
Frozen Path	optional		Frozen Path	optional Frozer bucket archive path. Set this if you want Splank to automatically archive hozen buckets.		
	Proper bucket erchive path. Set this if you want Spluris t	to automatically archive frozen buckets.	10.0			
A00	Search & R	eporting *	App	Search &	Reporting •	
			Storage Optimization			

2. To create the Http Event Collector, go to settings and Data Input, Select HEC Collector, then create a new HEC Token

## Step 2: Install Kubectl, Kubernetes and HELM

Along with this document, you have been provided with a series of scripts to make your life easier when it comes to deploying all of the technologies that are needed for the lab.

- **1.** Do the following steps locally:
  - Download and unzip the files in your local machine and desired directory.
  - Give execution permission to the following files: chmod +x microk8s-deploy1.sh microk8s-deploy2.sh otel-deploy.sh
  - Move the files to the VM where you will be deploying K8S, Kubernetes and HELM. (I do it with scp, but you will know better how to bring them in for your environment).

scp microk8s-values.yaml microk8s-deploy1.sh microk8s-deploy2.sh otel-deploy.sh<Insert User Here>@<insert IP here>:/home/splunker

- 2. Now, in the VM where you will be deploying the tools, (and counting that the scripts are already there): /microk8s-deploy1.sh
- 3. Then add microk8s to a new group: newgrp microk8s
- 4. Run the second deployment script: ./microk8s-deploy2.sh
- 5. Sourcing files: source ~/.bash\_aliases

### **Step 3: Install Otel Collector Helm Chart**

**1.** Pull OTelm helm repo locally by running the following script:

#### ./otel-deploy.sh

This script will run the following commands on your behalf: microk8s helm3 repo add splunk-otel-collector-chart https://signalfx. github.io/splunk-otel-collector-chart microk8s kubectl create ns otel microk8s helm3 -n otel install my-splunk-otel-collector -f microk8s-values.yaml splunk-otel-collector-chart/splunk-otel-collector

#### 2. Open the values file yaml: nano values.yaml

Take a minute to look through the different sections contained in the default values.yaml file.

Note that the yaml file is sensitive to indentation and may cause parsing issues when deploying the helm chart in the next step.

Find and Update the following values with the created HEC token in Step 1-2 :

clusterName: "<yourDesiredName>" endpoint: "https://<yourSplunkInstance>:8088/services/collector" token: "0000000-0000-0000-000000000000000" #Your HEC token goes here index: "otel\_events" metricsIndex: "otel\_metrics" insecureSkipVerify: true metricsEnabled: true logsEngine: otel containerRuntime: "containerd" excludeAgentLogs: false

When complete, save and quit.

# 3. Check your pods for errors, Get running pods kubectl -n otel get pods

Output should show that both your "agent" and "cluster-receiver" are both running. Be patient, it may take a minute.

/nome/spiunkei				
splunker@so1:~\$ kubectl -n otel get pods				
NAME	READY	STATUS	RESTARTS	AGE
mmodestino-tko-otel-splunk-otel-collector-k8s-cluster-rece9h94v	1/1	Running	1 (13h ago)	24h
mmodestino-tko-otel-splunk-otel-collector-agent-ptvmt	1/1	Running	1 (13h ago)	19h

You can also use the "watch flag" to keep an eye on the pods as they do their thing...

kubectl -n otel get pods -w

Press "ctrl + c" to stop the watch.

ctrl + c

Now, Check both your pods for errors.

kubectl -n otel logs -f <collector-agent-pod>

Replace <collector-agent-pod> with the agent pod name from previous command.

You should see startup logs showing the collector is running correctly. When running smoothly the pod will not log much info. It should look something like this:

1023-01-26720140:08.2062	2459	service/pipelines.gor% Process	or started. (*kind*	"processor", "name":	"batch", "pipeline": "ings"}		
1823-45-36728:48:88.2862	1nfa	service/pipelines_go:92 Process	or is starting	("kind": "processor",	"name": "filter/logs", "pipeline": "logs")		
2023-02-26720140100.2062	Lefte -	service/pipelines.got% Process	or started. ("kind"	"processor", "name")	"Filter/logs", "pipeline": "logs")		
2823-81-26728148188.2862	2459	service/pipelines.go:92 Process	or is starting	("kind": "processor",	"name": "Adsattributes", "pipeline": "logs")		
2023-01-26720140100-2062	1000	service/pipelines.gotvs Process	or started. C'kind'	"processor", "name")	"adsattributes", "pipeline": "ings")		
2023-02-20120140200-2002	1000	service/pipelines.gotv2 Process	or is starting	C.KTHL	"name": "wantey_limiter", "pipeline": "loge"?		
1822-45-20128148280.2002	1000	service-popelines.goove Process	or scenter, transfer	"processor", "lane";	Terrory_limiter, "pipeline": "Joge")		
1075-01-31730-08-08-305-	Lafe .	service/pipelines on the Process	or started Phinds	Antipartante Antipart	Pressure & Pringlings: Santriagth		
1073-01-34730-L8-08-3847	inter .	service/significes en/02 Process	or is startion	Chindly Services	Tennet: Transportation, Talaglingt: Tenteling	-	
1023-02-36730148108.2067	Laffa	service/plostines.oc/M Process	or started. Chind?	"DEDCASAGE", "Dame")	"resourcedetection", "significa"; "metrica")		
923-41-35728:48:88.2562	Lafe	service/pipelines.opc92 Process	or is starting	C"kind": "processor".	"name": "batch", "signalize": "matrics")		
1023-02-36720168108-2067	Laffa	service/sizetines_ports Process	or started. Chinds	"processor", "name";	"batch", "significa": "metrics")		
1023-02-36720140100.2062	Laffa	service/pipelines.go:92 Process	or is starting	C"kind": "processor".	"name": "memory limiter", "pipeline": "metrics")		
923-40-36720144108.2862	Left 1	service/pipelines.go:96 Process	or started. C'kind"	"processor", "name";	"momory_limiter", "pipeline"; "metrics")		
1823-45-36720148108.2042	Laffe	service/pipelines_go:92 Process	or is starting	C"kind": "processor",	"name": "resource", "pipeline": "metrics/agent")		
N23-45-26720:44:08.286Z	Sefe	service/pipelines.go:V& Process	or started. ("kind"	"processor", "name":	"resource", "pipeline": "metrics/agent")		
1823-45-36T20148108.386Z	Lafe .	service/pipelines.got#2 Process	or is starting	C"kind": "processor".	"name": "resourcedetection", "pipeline": "metrics	/agent/*)	
2023-01-20720140:00.2002	Sefe	service/pipelines.gor% Process	or started. (*kind*	"processor", "name":	"resourcedetection", "pipeline": "metrics/agent")		
2823-40-36T28148188.286Z	Lefte	service/pipelines.go:92 Process	or is starting	C"kind": "processor",	"name": "resource/add_agent_kds", "pipeline": "ne	tries/agent*)	
2823-45-26728148188.2842	Sette	service/pipelines_got% Process	or started. (*kind*	"processor", "name":	"resource/add_agent_kds", "pipeline": "metrics/ag	ent.)	
1923-40-36720:44:08.2862	Sefe	service/pipelines.go:92 Process	or is starting	("kind": "processor",	"name": "batch", "pipeline": "metrics/agent")		
2823-40-26720148/08.2862	14fe	service/pipelines.gor% Process	or started. (*kind*	"processor", "name":	"batch", "pipeline": "metrics/agent")		
2823-40-26728:48:88.2862	1nfo	service/pipelines_gor%2 Process	or is starting	C*kind*: "processor",	"name": "memory_limiter", "pipeline": "metrice/ag	ent*3	
2023-05-36720140100.2062	Sette .	service/pipelines.go:%6 Process	or started. C'kind"	"processor", "name":	"memory_limiter", "pipeline": "metrics/agent")		
2823-45-26720148:00.2062	Sette:	service/pipelines_poli00	Starting receivers				
M23-45-26728:44:08.2MZ	2450	service/pipelines.go:184	Receiver is starting	C"kind": "receiver",	"name": "hostmetrics", "pipeline": "wetrics")		
2823-05-26120(40)08.2872	1400	service/pipelines.go:108	Receiver started.	C"Kind": "receiver",	"name": "hostmetrics", "pipeline": "wetrics")		
2823-49-26728:44:388.2872	1000	service/pipelines_gol184	Receiver is starting	C.FOR.1 .Decement.	"name": "Aubeletatata", "pipeline": "Metrice")		
2823-49-26720144106-2872	1000	service/pipelines.goc100	Receiver started.	C'KING'I "Decelvez",	'name'i "Aubeletstate", "pipeline"i "metrice")		
1822-49-26128148188-2872	1966	internal Control on and I links at	Mecelver 18 starting	C-KIND-1 -December-,	"name"  "utip", "pipeline"  "wetrick")	f families assesses	Objects Recolumn Research Reduct Relations
to Respected Adaption and a contract	The second second	Internativersing operationing to	A sector of the test of the test	en trian server to ever	y necessary interrates, which may recall the percent of	- SHIVION BUCKS	Carbon L. Decensen, L. James L. Acth., Abbertose
1075.01.34710-10.00.0077	Calls.	at longering of the long of the second of th	Starting (000 server	Phindle Prevaluert	Present Aution Anighter Protection Andreset		
1025-01-26120-06-06-2072		Internal America and I. Dalas I	he & & & & address webber	as this server to ever	and a starface, which may facilitate Desial of	farries attacks	disingly researchest, house, build, felation
"I "metrics", "documentation")	Action 1	Ani thub .com/open-talemetry/openti	alemetry-collector/blob/	min/docs/enturity-bes	t-practices_admafesuards-assisst-decisi-of-servic	-attacks*3	( the content of the content of the content
1023-01-36720-48-08.2027	Laffa	at lange   werive, 47, 8/at la. as: 98	Startion HTTP server	C"kind": "receiver".	Some": "stla", "sigeline": "setrics", "endpoint":	10.0.0.01471013	
1823-40-36720148188.2872	Laffa	service/sizetimes_port#6	Receiver started.	C"kind": "receiver".	teamer: "etla", "elaeline": "estrica")		
1023-05-26720:40:00.2072	info	service/pipelines.goc184	Receiver is starting	C"kind": "receiver".	"name": "receiver.creator", "pipeline": "metrics")		
1923-05-36T20140-08.287Z	Setta .	service/pipelines.go:186	Receiver started.	C"kind": "receiver",	'name': 'receiver.creator', 'pipeline': 'metrics')		
1823-45-36T20148108.287Z	Seffe	service/pipelines.go:184	Receiver is starting	("kind": "receiver",	"name": "wignalfs", "pipeline": "metrics")		
1923-41-3sT20:48:08.297Z	##C1	internal/warming.gor51 Uwing th	he 0.0.0.0 address expose	es this server to ever	y network interface, which may facilitate Denial o	f Service attacks	("kind": "receives", "name": "signalfs", "pipe
line": "metrics", "documentatio	e*1. *868	ps://github.com/spen-telemetry/s	pentalemetry-collector/b	lok/waEn/does/security	-best-practices.mdFsafepuards-against-devial-of-se	rvice-attacks*)	
2823-01-26720:48:08.2872	Sefe	service/pipelines_go:100	Receiver started.	("kind": "receiver",	'name': "wignalfs", "pipeline": "metrics")		
2823-45-26720148:08.2872	SHEE	service/pipelines.go:184	Receiver is starting	C"kind": "receiver",	'name': 'prometheus/agent', 'pipeline': 'metrics')		
2823-40-26720148188.2872	1459	prometheusreceiver@v8.67.8/metr	ics_receiver.go:243	Scrape job added	("kind": "receiver", "name": "prometheus/agent"	. "pipeline": "metrice",	"jotRune": "otel-agent")
2823-45-26728148188.2872	2459	service/pipelines.go:100	Receiver started.	C"kind": "receiver",	"neme": "prometheus/epent", "pipeline": "metrics")		
2823-49-26728148188-2872	100	service/pipelines.gol104	Metelver is starting	Carlingal stepeiner.	"name"  "fllelog", "pipeline"  "loge")		
2023-03-20120340300.2072	1000	adapter/receiver.gotte startin	g stands receiver	("KING": "Debeliver",	"name": "Tileing", "pipeline": "loge")		and a distance of the second s
2023-00-26120140.00.2072	1489	Tibeconsumer/Tibe.gec312	Resurcing from previously	y known offsetial. 'st	surfar, setting as not emprovement c.erud.:	ver, "name": "Fileling",	"bibelive.1 .lobs." .comboueur.1 .Liteconomet
1075 AL 14778-14-08 1087	inter .	animation providential at Almeter	tes receiver en 205	Startion discourses	tanan (Palad): President, Sama's Personities	Const. Tolesticst: To	atrice?)
1023-01-34730148108.3082	Lafe	annetheusreceiverbel. 67.8/eetr	ics receiver.no.288	Startion scrate spoat	or ("alad") "receiver", "name"; "accentheus/apent"	"mineline": "metrics")	relate /
1023-01-35720140100.2907	Laffa	service/pipelines.occ108	Receiver started.	C"kind": "receiver".	teame": "fileloo", "pipeline": "loos")	paperson i mersone p	
023-03-26720:40:00.298Z	Lafe	service/pipelines.pcc184	Receiver is starting	C'kind': "receiver".	"name": "fluentferward", "ploaline": "loos")		
1823-40-26728168188.2942	Laffe	service/pipelines_port#8	Receiver started.	("kind": "receiver".	"name": "fluentferward", "pipeline": "loos")		
1823-45-26728:48:88.2997	Setto	service/pipelines.go:184	Receiver is starting	C"kind": "receiver".	'name": "utlo", "pipeline": "logs")		
1923-40-26720148108.2962	Laffe	service/pipelines.gor186	Receiver started.	Chind's "receiver",	'name": "etla", "pipeline": "logs")		
2823-40-26728:68:88.2992	<b>Sefe</b>	healthcheck/handler.go:129	Health Check state chang	pe ("kind": "ext	engion", "name": "health_check", "status": "greaty"	>	
2023-05-26T20:40:00.290Z	Lefe	service/service.got185 Everyth	ing is ready. Begin runn	ing and processing dat	h.		
1023-02-26720140:08.4912	Lafe	fileconsumer/file_goc159	Started watching file	C"kind": "receiver",	"name": "filelog", "pipeline": "logs", "component"	: "fileconsumer", "path":	: */wat/log/pods/kube-system_callos-kube-contro
Lers-566cb5780-4wet2_e9418cdb-		e-a5e3-151ece22e832/cel5co-kube-	controllers/#.log")				
1823-85-26728148189.288Z	Laffe	THERE's are reader of the state of the serve	chandler.gor84 starting	preceiver ("kin	0"1 "receiver", "ease": "receiver_creator", "pipel	ine": "eetrics", "name":	"smartagent/coredna", "endpoint": "38.1.62.139
", "endpoint_id": "kds_observer	/806/1025	A-febs-4242-a803-28f2aba44cc5*)					

Press "ctrl+c" to exit followtail view

4. View cluster-receiver pod logs with the following command

kubectl -n otel logs -f <collector-cluster-reciever-pod>

press "ctrl" + "c" to exit followtail view

If there is an issue with the configuration, you will see a constant stream of warnings or errors. You will need to go back and fix your configuration then use the following command to deploy your changes:

helm -n otel upgrade <yourDesiredName> -f values.yaml splunk-otelcollector-chart/splunk-otel-collector

Once you deploy your config updates, return to the previous step to check your pods are running and there are no errors in your pod logs.

### 5. Check Splunk

index=otel\_events

Navigate back to Splunk Web and the Search & Reporting app. Use the default search time range to ensure you are seeing events.

Search Analytics Datasets R	Reports Alerts	Dashboards	Search & Reporting
New Search			Save As • Create Table View Close
index=otel_events			Last 24 hours * Q
- 544 events (06/05/2024 11:00:00:000 1	6 07/05/2024 11:24	S4.000) No Event Samping • Jab •	1 = 🗈 🕹 🔟 🕈 Smart Mode •
Events (544) Patterns Statistics	Visualization		
Format Timeline • - Zoom Out			1 hour per column
			<b>—</b> —
	Lbt.• ZR	emet 20 Per Page + Chav 1 2	3 4 5 6 7 8 . Net >
CHide Fields III All Fields	i Time	Event	
SELECTED FELDS	> 07/05/202 11/26:43.0	4 2024-05-07 11:26:43.024 [DvF0][77] moniter-addresses/autodetection_methods.go 103: Using aut 15 02.10.31/21	edetected IPv4 address on interface ens5: 10.2
source		host = so1 source = Aastog/pods/kube-system_csiko-node-25/29_8c0cts24-825/-4419-99a8-ber/21.	sourcetype = kubecontainercalico-node
INTERESTING FIELDS	> 07/05/20	4 2824-85-87 11:28:32.688 [DWD][76] felix/summary.gn 180: Summarising 11 dataplane reconcilis () () host = sof   source = /wwrlog/pods/kube-system_calco-node-25/29_8cOct624-825f.4419-99w8.bef21.	tion loops over 1n2.8s: avg=6ns longest=22ss sourcetype = kubecontainercalico-node
ong container.kt container.image.name container.image.tag	> 07/05/20 11/25:43.0	2024-05-07 11:25:43.023 (DNF0)(77) noniter-addresses/autodetection_nethods.go 103: Using aut     02:10.31/21     02:10.31/21     02:00.01.01.01.01.01.01.01.01.01.01.01.01.0	adetected IPv4 address on interface ens5: 10.2
kills cluster name 1	> 07/05/20	nost = soi	ton loose over 181.5s: averTes longest=77m ()
klis.container.name	11:25:29.9	13 host = sol source = /vanlog/pods/kube-system_calico-node-25/29_8c0ct624-825/-4419-99a8-ber/21.	sourcetype = kube:container:calico-node
kills namespace name 2 kills node.name 1 kills node.name 1	> 07/05/20 11/24/43.0	14 2024-05-07 11:24:43.012 [INF0][77] monitor-addresses/autodetection_methods.go 103: Using aut 3 02:10.01/21 	adetected IPv4 address on interface ens5: 10.2
klis.pod.name	> 0205/20	nos son source - vanaggooskupesystem_caktoroce_stray_aturtare sarente vana oraz.	tion loose over 102 in: eventer loosestation /r
kills pod uki linecount	11:24:26.3	9 esync-nat-v4) hot = so1 source = Awrlooloodukube-svitem calco-note-25/29 Bc0cts24 B25/4419-998 ber/21.	sourcetupe = kubecontainencalico-node
logteg 1 longest 26 lostype 1	> 07/05/20 11:23:43.0	N4 2024-05-07 11:23:43.012 [INF0][77] monitor-addresses/autodetection_methods.go 103: Using aut 5 02.10.01/21	odetected IPv4 address on interface ens5: 10.2
punct		host = solsource = /vanlog/pods/kube-system_calico-node-25/29_8c0cts/24-825/-4419-99a8-ber/21.	sourcetype = kube:containencalico-node
23 more fields	> 07/05/20/ 11:23:23:5	<ol> <li>2024-05-07 11:23:23.521 (1070)[76] feltx/summary.gn 100: Summarising 13 dataplane reconcilia</li> <li>host = sof</li></ol>	tion loops over In3s: avg=6ns longest=22ns () sourcetype = kubercontainencalico-node
+ Extract New Fields	> 07/05/20	<ol> <li>2004-05-07 11:22:43.001 [INF0][77] monitor-addresses/autodetection_methods.go 103: Using aut 91 02:10.01/21</li> </ol>	odetected IPv4 address on interface ens5: 10.2

### If you click on more fields, you'll see:

Ser	Select Fields								
N	2	elect All \	Within Filter Deselect All	Coverage: 1% or more +	Filter			+1	street New Fields
		1.	Field #				# of Values +	Event Coverage #	Type #
P	>	×	host				1	100%	String
1		R	source				6	100%	String
Det		R	sourcetype				4	100%	String
6			adminUp				2	156	String
			avg					21.69%	String
			chainName				6	3.3%	String
			container.id				6	100%	String
125			container.image.name				3	100%	String
1			container image teg				2	100%	String
			failed				1	155	String
			id				- 4	4.78%	String
			ifindex				2	1.9%	Number
and a			ifaceName				2	2.76%	String
			index				1	100%	String
			igWersiton				1	4.6%	String
			kBs.cluster.name				1	100%	String
			kBs.container.name				4	100%	String
			kBs.container/estart_count				1	100%	Number
			kBs.namespace.name				2	100%	String
			k8s.node.name				1	100%	String
			kBs.pod.labels.app				1	32.9%	String
- 1			k8s.pod.neme				5	100%	String
			kBs.pod.uid				5	100%	String
			known				2	135	String
			linecount				1	100%	Number
			log.iostream				2	100%	String
+1			logtag				1	100%	String
			longest				26	2169%	String
			mıg				5	5.7%	String
			name				1	0.92%	String
			node				1	0.92%	String
		-	operUp				2	135	String
			orchestrator				1	0.92%	String
		-	ostype				1	100%	String
			punct				96	100%	String

The sourcetypes are:

sourcetype				×
4 Values, 100% of eve	nts	Sel	ected Yes	No
Reports Top values	Top values by time	Rai	re values	
Events with this field				
Values		Count	%	
kube:container:cali	co-node	201	52.618%	
kube:container:otel	-collector	178	46.597%	
kube:container:cali	co-kube-controllers	2	0.524%	
kube:container:migr	ate-checkpoint	1	0.262%	

The type of metrics that can be displayed using the query: mcatalog values(metric\_name) WHERE index=otel\_metrics

system.paging.faults system.paging.operations system.processes.count system.processes.created up

protation       Note:         Protein       Note:         Volume       Volume    Volume <pv< th=""><th colspan="7">New Search</th></pv<>	New Search						
Processor       Processor       Valuation         To be regar       Forma       Processor         Container-council       Container-council       Container-council         Container-councol       Container-council	mcatalog values(	metric_name;	) WHERE index≕	otel_metrics			
Teters         Years         Years           Interpreter         Image: Teters         Teters	✓ 5,494 events (06/0	05/2024 09:0	0:00.000 to 07/	05/2024 09:31:04.00	00) No Event Sampling -		
100 Per Page 1         Verwat           volues(metric_num)            container, cpu, utilization            container, filesystem. available            container, filesystem. available            container, filesystem. available            container, filesystem. available            container, memory, varge            container, memory, varge            container, memory, varge            container, memory, request            coredrs, dns, requests, total            k8s. container, nemory, request            k8s. container, ready            k8s. conta	Events Patterns	Statistics	s (1) Visualiz	ation			
volues(metric_name) f container.cpu.time container.cpu.time container.flexystem.available container.flexystem.available container.memory.major_page_faults container.epu_limi kas.container.rest container.epu_limi kas.container.rest container.epu_limi kas.container.rest container.epu_limi kas.container.rest container.epu_limi kas.container.epu_limi kas.container.epu_limi kas.container.epu_limi kas.container.rest container.epu_limi kas.container.epu_limi kas.co	100 Per Page 🔻	<ul> <li>Format</li> </ul>	Preview 🔻				
container.cpu.tile container.cpu.tile container.flesystem.available container.filesystem.available container.memory.available container.cpu.lisi coredms.dms.request.site.bytes coredms.dms.r	values(metric_name)	÷					
kas pod memory rss	container.cpu.time container.cpu.utiliz container.filesyste container.filesyste container.memory.me container.memory.me container.memory.me container.memory.me container.memory.me container.memory.we coredns_cache_entriz coredns_dns_request coredns_dns_request coredns_dns_respons k8s.container.cpu_2 k8s.container.cpu_2 k8s.container.ready k8s.container.ready k8s.container.ready k8s.container.ready k8s.container.ready k8s.daemonset.desit k8s.daemonset.misse k8s.daemonset.ready k8s.daemonset.ready k8s.node.condition_ k8s.node.cpu.utiliz k8s.node.filesystem k8s.node.filesystem k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.memory.ma k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.filesystem k8s.node.memory.majo k8s.pod.cpu.time	ization em.available em.capacity em.usage vailable ajor_page_faults ss sage orking_set ies t_size_bytes ts_total ses_total limit request ry_limit ry_request y arts ent_schedule cheduled_nod y_nodes ilable ired e _ready zation m.available incapacity m.usage ailable jor_page_fau ge_faults s age rking_set ation .available icapacity .usage ilable icapacity .usage ilable capacity .usage ilable	ults d_nodes d_nodes les				

```
k8s.pod.network.errors
k8s.replicaset.available
otelcol_exporter_send_failed_log_records
otelcol_exporter_send_failed_metric_points
otelcol_exporter_sent_log_records
otelcol_otelsvc_k8s_ip_lookup_miss
otelcol_otelsvc_k8s_pod_added
otelcol_otelsvc_k8s_pod_deleted
otelcol_otelsvc_k8s_pod_table_size
otelcol_otelsvc_k8s_pod_updated
otelcol_process_cpu_seconds
otelcol_process_memory_rss
otelcol_process_runtime_heap_alloc_bytes
otelcol_process_runtime_total_alloc_bytes
otelcol_process_runtime_total_sys_memory_bytes
otelcol_processor_accepted_log_records
otelcol_processor_accepted_metric_points
otelcol_processor_dropped_log_records
otelcol_processor_dropped_metric_points
otelcol_processor_filter_logs_filtered
otelcol_processor_refused_log_records
otelcol_processor_refused_metric_points
otelcol_receiver_accepted_log_records
otelcol_receiver_accepted_metric_points
otelcol_receiver_refused_log_records
otelcol_receiver_refused_metric_points
otelcol_scraper_errored_metric_points
otelcol_scraper_scraped_metric_points
scrape_duration_seconds
scrape_samples_post_metric_relabeling
scrape_samples_scraped
scrape_series_added
system.cpu.load_average.15m
system.cpu.load_average.1m
system.cpu.load_average.5m
```

Navigate to the Analytics tab and confirm you see metrics, you can check there the different dashboards, set analysis filters, and find the data that you want to analyze



