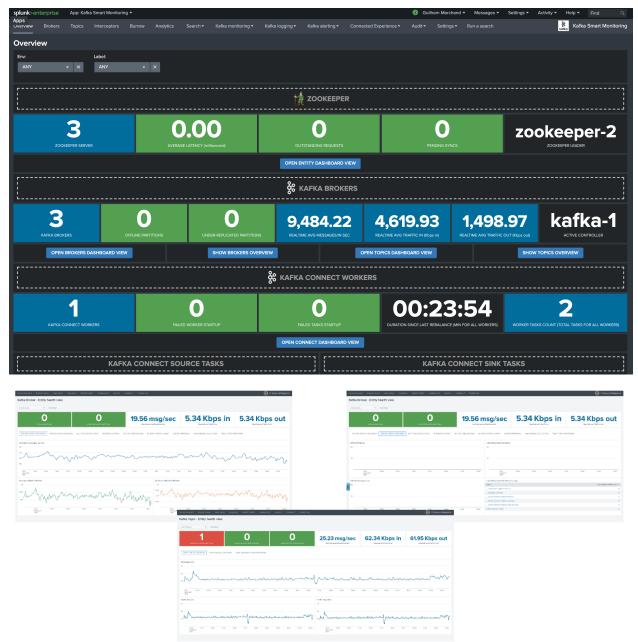
telegraf-kafka Documentation Release 1

Guilhem Marchand

Aug 29, 2021

Overview

1	Over	view:
	1.1	About
	1.2	Compatibility
	1.3	Known Issues
	1.4	Support & donate
	1.5	Download
2	Deplo	oyment and configuration:
	2.1	Deployment & Upgrades
	2.2	Implementation & data collection
	2.3	Docker testing templates
	2.4	Splunk dashboards (health views)
	2.5	Splunk Connected experience for Cloud Gateway
	2.6	Kafka infrastructure OOTB alerting 70
3	Trou	bleshoot: 10
	3.1	Troubleshoot & FAQ
4	Versi	oniong and build history: 10
	4.1	Release notes



The Splunk application for Kafka Smart Monitoring with provides performance management, reporting and alerting for Kafka components metrics ingested in the Splunk metric store:

Level 1997 g	Kife to set																	
	Life Yourky					Burrow												Cott Expert
						Time range:	e~		Low	lake-	Charlen Co.							
	ARY y signifiers						* #	89° K	ARYX	100	8	no los						
	🗞 kafka e	RPONERS											resp consumer	6				
	taled size/for the adarted insket)	Combined Horizon							programmer details)									
Ideal 1 Indea. Sector 1		add spatia add has t		ant Frein 6		And a		arresta Sarbar	N									
toring talkers		K.M. Schulder, Degewahrsteiner K.M. Schulder, Degewahrsteiner, Markeiner, Schulder, Degewahrsteiner, Schulder, Degewahrs			10.00 (0.00)			2011 1										
testing lafter2		1.4 Nyin at An		1.0 1.0	10.00	are 1		Lobe i p			racian rai				ge i kalfans i			marking_ris
terring tailor 1	ng Adarang Jaka na	deter monthel rac		0.04 0.00					consci faña consci sys			* hour	allandos (0.000			
-	Re-Enterprise Application International Marineses #				mought integet denies (due in)	Bolton , and	terra la		canned table connect tob			Sugar	und			The group of particle		
					P suite Dreat Monterrog	0.000.000	tering in	and the	allo nei ciorta			· ·		OK.	 0.04.08 	The group or particle		endied
	un Solnes base Gerver Metrice Soleiste Autoenendunger Rohelungerger Rohelungerge Ander Vieren	g* Research			Ruha Sma'l Muniurry							åt nore	w partitions					
		😨 Broker: kafka-1					w partitions (click o		er trechat legi									
						Sature		100										
S	Rat offerer					ANY a		494° 4										
			10.00	to access to	Martinia -	and the	and the second			1	6 Administration	Velage - Lellege	- ACM- 100-	Dec 1	caret.) specific i			mito description i
÷,	Red to press													Au brust Manhorn		hates *		The grade or partition 14, by
Surre		Contained metals	70.00 900		the Marke Search References to the signifi-	10000001 10110								PG 5121 9413011	The Innata	and a	0 10.04.04	The group or partition is in a
Den i		Res 1 Res 1	Topics														0 10.00 M	The group or pertition 14 in
		11 Presigns in Card					f.,										0 10.04.04	The group or partition is in
1.07	Artitian	14 Migrae in Aver					SC KV	AFKA TOPIC	ics.									
2.478		19.04 Marine and June			Antala for the anta-tand block												0 824.0	The grave or pertition to be
	Dearing	15.21 Bytes rejected care	Topos yaka an	The loss to stree bigs														
1.4.1	adjung .	11.17 Parine links report from Parine produce report /ex.	200 x		an Fatter Spinst													The price of pertition is in a
		Fallet protect report /arc	101				ince 1 day			Report Franklik I		Petiters North		able Brooking I				
		- Manapator - Manatana - Manatana	10.00		un	1765			2	15.17	1 Crain Hypern		19	1.00				The group or partition is in
			and on the local division of the local divis		senser offers					100.00			100					The proper or performents in the
		~ .		ter tra			*			140.00		× •		8.00				The price of pertition (a. in a
			B10.00	bed ing	Juffer connect reduct - dataset					100.00								
			And an unit	testing	Aufler coment reducts task confige					149.00			10	8.00				
	to to to to to to to	or he has his his his	maker, so		particular canada					100.00			-					
					orbeit kipt orbeit, taktes, tuoset, spis									1.00				
	Topia Datial pilek an the navia view logic skézik for the selected logic)		maker you		policies and the second s					140.00			#17					
teges i			Bobse and		urkunan Contragio urkunan Contra Contra Alfred Balletaria (martia) an					100.00			-	1.0	1			
	effanni sagant antras 2 k	1 1 1 10 10 10 10 10 10 10 10 10 10 10 1			Strate Art all and Oralis					140.00			-					
	naerafiata) a Nariamatingkakofhata 2 38	10 IIII II.LLARAMANANANANANANAN			ofference of a first start start of a					100.00								
	Aurometraliskutoriani () 3 Aurometraliskutoriani () 5	5 445 00.224	a.a.							100.00			30	1.00				
	An one of the second se	S LPS ROLLIN	maker you	hed ing	the sector during the strength of proceedings					100.00			~					
	functional (1 4 400 000	Andrew and		after moder shartler toge "Engrange by game mage to blan					149.00				1.00				
		1 8.86 (0)	maker year		after sealer sharts rise that samp integring					100.00								
to be	a weber hair. 1 K	8 MI 80 80.00	10.007.000		Parents parts to the segment title					140.00			.MD	4.00				
	a na se	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	maker year		ing ments					144.44			-					
	e matic cherte all serge chergelag 5	1 4.000 🖘	Bober and		ang filed nobel					140.00			*	1.00				
where	e waar viente wag play maat sharping 1 4	1 2.000 000	Bollow , was	Ded Dig	pile .					16.11				1.24				

The application provides builtin and native monitoring for Apache Kafka components, as well as the Confluent stack components:

- Zookeeper
- Apache Kafka Brokers
- Apache Kafka Connect
- Confluent schema-registry
- Confluent ksql-server
- · Confluent kafka-rest
- Kafka SLA and end to end monitoring with the LinkedIn Kafka monitor
- Confluent Interceptors monitoring for lag monitoring of consumers and producers
- Kafka Consumers lag monitoring with Burrow (Kafka Connect connectors, Kafka Streams...)

Fully multi-tenant compatible, the application can manage different environments, data-centers, etc specially using tags at metrics low level.

It is recommended to read the unified guide for Kafka and Confluent monitoring first:

https://splunk-guide-for-kafka-monitoring.readthedocs.io

CHAPTER 1

Overview:

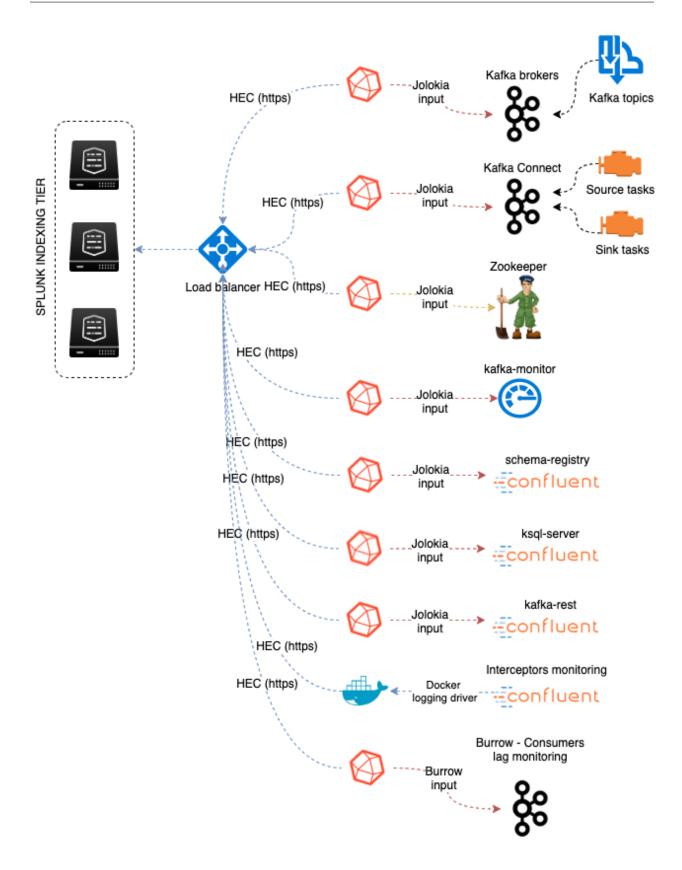
1.1 About

- Author: Guilhem Marchand
- First release published in October 2018
- Purposes:

The Splunk application for Kafka Smart Monitoring leverages the best components to provide a key layer monitoring for your Kafka infrastructure :

- Telegraf from Influxdata (https://github.com/influxdata/telegraf)
- Jolokia for the remote JMX collection over http (https://jolokia.org)
- Telegraf Jolokia2 input plugin (https://github.com/influxdata/telegraf/tree/master/plugins/inputs/jolokia2)
- Telegraf Zookeeper input plugin (https://github.com/influxdata/telegraf/tree/master/plugins/inputs/zookeeper)
- Optional: Xinfra Kafka monitor to provide end to end monitoring (https://github.com/linkedin/kafka-monitor)
- Optional: Confluent Interceptors Monitoring (https://docs.confluent.io/current/control-center/installation/ clients.html)
- Optional: Kafka Consumers lag monitoring with Burrow (https://github.com/linkedin/Burrow)

An ITSI module is also available: https://da-itsi-telegraf-kafka.readthedocs.io



1.2 Compatibility

1.2.1 Splunk compatibility

Splunk core version

- metrics are ingested into the high performance Splunk metric store, Splunk 7.0.x or later is required
- some queries are built using the latest syntax for metrics, Splunk 7.2.x or later is recommended

1.2.2 Telegraf compatibility

Telegraf supports various operating systems and process architectures including any version of Linux and Windows.

For more information:

• https://portal.influxdata.com/downloads

1.2.3 Containers compatibility

If you are running Kafka in containers, you are at the right place, all of the components can natively run in docker.

1.2.4 Kafka and Confluent compatibility

Apache Kafka and Confluent compatibility

• Qualification and certification is made against Kafka V2.x and Confluent V6.x, earlier versions might however work with no issues but are not being tested

1.2.5 Web Browser compatibility

The application can be used with any of the supported Web Browser by Splunk: https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements

1.3 Known Issues

There are no known issues at the moment.

1.4 Support & donate

I am supporting my applications for free, for the good of everyone and on my own private time. As you can guess, this is a huge amount of time and efforts.

If you enjoy it, and want to support and encourage me, buy me a coffee (or a Pizza) and you will make me very happy!

The Splunk application for Kafka monitoring with Telegraf is community supported. To get support, use of one the following options:

1.4.1 Splunk community

Open a question in Splunk Community:

• https://community.splunk.com

1.4.2 Splunk community Slack

Contact me on Splunk community slack, or even better, ask the community !

• https://splunk-usergroups.slack.com

1.4.3 Open a issue in Git

To report an issue, request a feature change or improvement, please open an issue in Github:

• https://github.com/guilhemmarchand/telegraf-kafka/issues

1.4.4 Email support

• guilhem.marchand@gmail.com

However, previous options are far betters, and will give you all the chances to get a quick support from the community of fellow Splunkers.

1.5 Download

1.5.1 Splunk Application for Kafka monitoring with Telegraf

The Splunk application can be downloaded from:

Splunk base

• https://splunkbase.splunk.com/app/4268

GitHub

• https://github.com/guilhemmarchand/telegraf-kafka

CHAPTER 2

Deployment and configuration:

2.1 Deployment & Upgrades

2.1.1 Deployment matrix

Splunk roles	required
Search head	yes
Indexer tiers	no

If Splunk search heads are running in Search Head Cluster (SHC), the Splunk application must be deployed by the SHC deployer.

2.1.2 Indexes creation

indexes

- Kafka SDM expects the creation of a metric index, by default telegraf_kafka which can be configured by customizing the macro telegraf_kafka_index
- If you use Confluent interceptors, the application expects the creation of a metric index confluent_interceptor_metrics which can be configured by customizing the macro confluent_interceptor_index

2.1.3 Dependencies

The application depends on:

• Horseshoe Meter - Custom Visualization, Splunk Base: https://splunkbase.splunk.com/app/3166

2.1.4 Initial deployment

The deployment of the Splunk application for Kafka monitoring with Telegraf is straight forward:

- Using the application manager in Splunk Web (Settings / Manages apps)
- Extracting the content of the tgz archive in the "apps" directory of Splunk
- For SHC configurations (Search Head Cluster), extract the tgz content in the SHC deployer and publish the SHC bundle

2.1.5 Upgrades

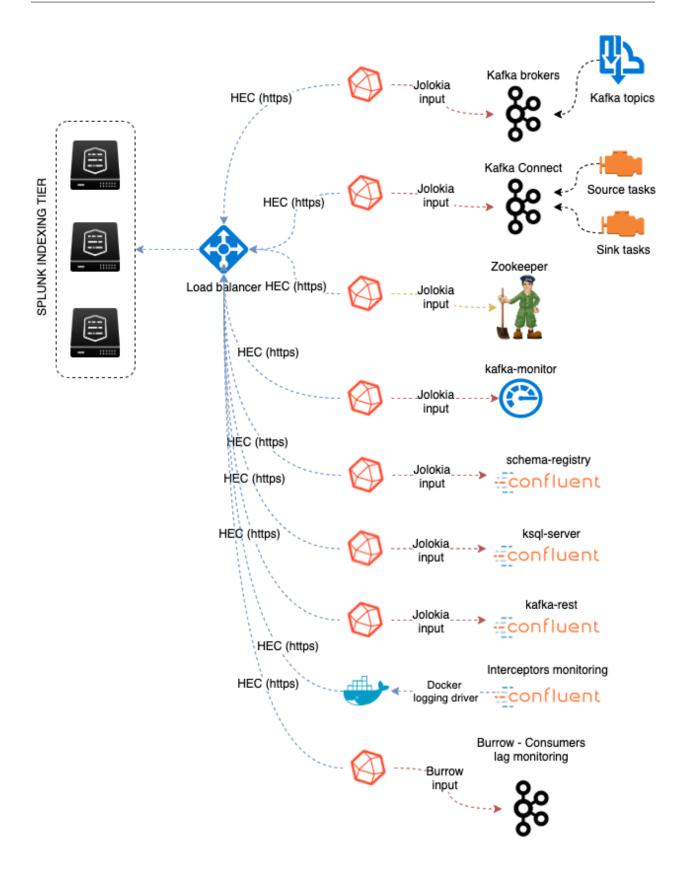
Upgrading the Splunk application is pretty much the same operation than the initial deployment.

2.1.6 Upgrades of the components

Upgrading the different components (Telegraf, Jolokia, etc.) rely on each of the technologies, please consult the deployment main pages.

2.2 Implementation & data collection

Data collection diagram overview:



2.2.1 Splunk configuration

Index definition

indexes

• Kafka SDM expects the creation of a metric index, by default telegraf_kafka which can be configured by customizing the macro telegraf_kafka_index

indexes.conf example with no Splunk volume::

```
[telegraf_kafka]
coldPath = $SPLUNK_DB/telegraf_kafka/colddb
datatype = metric
homePath = $SPLUNK_DB/telegraf_kafka/db
thawedPath = $SPLUNK_DB/telegraf_kafka/thaweddb
```

indexes.conf example with Splunk volumes::

```
[telegraf_kafka]
coldPath = volume:cold/telegraf_kafka/colddb
datatype = metric
homePath = volume:primary/telegraf_kafka/db
thawedPath = $SPLUNK_DB/telegraf_kafka/thaweddb
```

In a Splunk distributed configuration (cluster of indexers), this configuration stands on the cluster master node.

All Splunk searches included in the added refer to the utilisation of a macro called telegraf_kafka_index configured in:

• telegraf-kafka/default/macros.conf

If you wish to use a different index model, this macro shall be customized to override the default model.

Confluent Interceptors monitoring:

```
indexes
```

• If you use Confluent interceptors, the application expects the creation of a metric index confluent_interceptor_metrics which can be configured by customizing the macro confluent_interceptor_index

indexes.conf example with no Splunk volume::

```
[confluent_interceptor_index]
coldPath = $SPLUNK_DB/confluent_interceptor_index/colddb
datatype = metric
homePath = $SPLUNK_DB/confluent_interceptor_index/db
thawedPath = $SPLUNK_DB/confluent_interceptor_index/thaweddb
```

indexes.conf example with Splunk volumes::

```
[confluent_interceptor_index]
coldPath = volume:cold/confluent_interceptor_index/colddb
datatype = metric
homePath = volume:primary/confluent_interceptor_index/db
thawedPath = $SPLUNK_DB/confluent_interceptor_index/thaweddb
```

You can technically use the same index than for telegraf based metrics, or any index of your choice, if so update the macro called **confluent_interceptor_index** configured in:

telegraf-kafka/default/macros.conf

Role membership

The application creates a builtin Splunk role called "kafka_admin" that provides:

- · write permissions to the application name space
- write permissions to the various KVstore based lookups used for configuration purposes of the application
- can be used to automatically notify the Kafka administrators if you use Splunk Cloud Gateway and Splunk Mobile Connected Experience

We suggest that you configure the Kafka administrators to be member of this role. (by user configuration, role mapping or inheritance)

HEC input ingestion and definition

HTTP Event Collector

• The default recommended way of ingesting the Kafka metrics is using the HTTP Events Collector method which requires the creation of an HEC token

inputs.conf example:

```
[http://kafka_monitoring]
disabled = 0
index = telegraf_kafka
indexes = telegraf_kafka
token = 205d43f1-2a31-4e60-a8b3-327eda49944a
```

If you create the HEC input via Splunk Web interface, it is not required to select an explicit value for source and sourcetype.

If you plan to use Confluent Interceptors monitoring, you need to allow the target index too, for instance:

```
[http://kafka_monitoring]
disabled = 0
index = telegraf_kafka
indexes = telegraf_kafka,confluent_interceptor_index
token = 205d43f1-2a31-4e60-a8b3-327eda49944a
```

The HEC input will be ideally relying on a load balancer to provides resiliency and load balancing across your HEC input nodes.

Other ingesting methods

There are other methods possible to ingest the Kafka metrics in Splunk:

• TCP input (graphite format with tags support)

- KAFKA ingestion (Kafka destination from Telegraf in graphite format with tags support, and Splunk connect for Kafka)
- File monitoring with standard Splunk input monitors (file output plugin from Telegraf)

Notes: In the very specific context of monitoring Kafka, it is not a good design to use Kafka as the ingestion method since you will most likely never be able to know when an issue happens on Kafka.

These methods require the deployment of an additional Technology addon: https://splunkbase.splunk.com/app/ 4193

These methods are heavily described here: https://da-itsi-telegraf-os.readthedocs.io/en/latest/telegraf.html

These methods should however be considered as a second choice only if sending to HEC is not possible.

2.2.2 Telegraf installation and configuration

Telegraf installation, configuration and start

If you are running Telegraf as a regular process in machine, the standard installation of Telegraf is really straightforward, consult:

• https://github.com/influxdata/telegraf

If you have a Splunk Universal Forwarder deployment, you can deploy, run and maintain Telegraf and its configuration through a Splunk application (TA), consult:

• https://da-itsi-telegraf-os.readthedocs.io/en/latest/telegraf.html#telegraf-deployment-as-splunk-application-deployed-by-splunk-

An example of a ready to use TA application can be found here:

• https://github.com/guilhemmarchand/TA-telegraf-amd64

For Splunk customers, this solution has various advantages as you can deploy and maintain using your existing Splunk infrastructure.

Telegraf is extremely container friendly, a container approach is very convenient as you can easily run multiple Telegraf containers to monitor each of the Kafka infrastructure components:

https://hub.docker.com/r/_/telegraf/

Data collection environment design:

The most scalalable and highly available design in term of where placing the Telegraf instances is to deploy Telegraf locally on each server to be monitored (and collect locally the component) or running as a side car container for Kubernetes based environments.

It is to possible to collect multiple instances of multiple components via a unique Telegraf instance, however there will be a limit where issues can start, and this design will not provide high availability as the failure of this instance will impact the whole metric collection.

2.2.3 Telegraf configuration generator

The application provides a builtin user interface you can use to generate a telegraf.conf configuration file based on your parameters and for all the components to be monitored:

• Menu Settings / Telegraf Configuration Generator

splunk>enterprise App: K	afka Smart Monitoring 👻								6	Guilhem Marchand 🕶	Messages 🕶	Settings 🕶	Activity -	Help 🔻	Find Q
Overview Brokers Topics				Kafka logging 🔻					iettings -					🕺 Kafka	Smart Monitoring
Configuration helpe Use this configuration helper to cre	-	-	nple configuration	on											
					\bigcirc	tele	graf								
Define the value of the env t kafka_prod	ag: (used as the main i	dentifier for a g	given environment)				efine the value	of the label ta	ıg: (addition	al environment inform	ational selector)			
Enter the Splunk HEC URL in https://hec.mydomain.com:808		ress of your HE	C endpoint>: <port>/sen</port>	vices/collector			nter the Splunk 205d43f1-2a31-4e		Ja49944a						
Select the component you w Component: Kafka Broker • X Generate sample configurat	Running on:	or: •	Port number: 8778			Int	lain Telegraf op terval: 10s	ions: •	Linux OS r Yes	netrics:					
	_														
splunk >enterprise App: K Overview Brokers Topics	afka Smart Monitoring - Burrow Metrics	Telegraf c	onfig helper						6) Guilhem Marchand 💌	Messages *	Settings 👻	Activity *	Help •	Find Q Smart Monitoring
Configuration helpe	er - generate te	Generated tel Use the follow	legraf.conf: ving content as the definitio	n for your telegraf.c	conf to monitor and c	collect the metr	rics of the compor	ient.							
Use this configuration helper to cr Define the value of the envit kafka, prod Enter the Splunk HEC URL in http://hec.mydomain.com.800 Select the component you w Component: Kafka Broker + X Generate sample configurat	ag: (used as the main the form: https://cadic @/services/collector	<pre>[plobal_tag # the env env = "kad # the labo label = " [agent] interval = flumb_int hostname # outputs [[outputs.h] clata_form # Provid splumhmet # # Additic # Additic</pre>	a] tag is used by the applic FRA_prod" an additional to my_datacenter' "10s" erval = "10s "10s"	ation for multi-en g used by the appl #/services/collect	vironments manageme ication to identify or"	ent		lerit.		Download of	nfiguration				

2.2.4 Telegraf output configuration

Whether you will be running Telegraf in various containers, or installed as a regular software within the different servers composing your Kafka infrastructure, a minimal configuration is required to teach Telegraf how to forward the metrics to your Splunk deployment.

Telegraf is able to send to data to Splunk in different ways:

- Splunk HTTP Events Collector (HEC) Since Telegraf v1.8
- Splunk TCP inputs in Graphite format with tags support and the TA for Telegraf
- Apache Kafka topic in Graphite format with tags support and the TA for Telegraf and Splunk connect for Kafka

Who watches for the watcher?

As you are running a Kafka deployment, it would seem very logical to produce metrics to a Kafka topic and consume these metrics from the topic. However, this is not an ideal monitoring architecture design due to potential lack of visibility in case of an outage or issues.

If you use this same system for monitoring Kafka itself, it is very likely that you will never know when Kafka is broken because the data flow for your monitoring system will be broken as well.

The recommendation is to rely either on Splunk HEC or TCP inputs to forward Telegraf metrics data for the Kafka monitoring.

A minimal configuration for telegraf.conf, running in container or as a regular process in machine and forwarding to HEC:

```
[global_tags]
 # the env tag is used by the application for multi-environments management
 env = "my_env"
 # the label tag is an optional tag used by the application that you can use as_
↔additional label for the services or infrastructure
 label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# Regular OS monitoring for Linux OS
# Read metrics about cpu usage
[[inputs.cpu]]
 ## Whether to report per-cpu stats or not
 percpu = true
 ## Whether to report total system cpu stats or not
 totalcpu = true
 ## If true, collect raw CPU time metrics.
 collect_cpu_time = false
 ## If true, compute and report the sum of all non-idle CPU states.
 report_active = false
# Read metrics about disk usage by mount point
[[inputs.disk]]
  ## Ignore mount points by filesystem type.
 ignore_fs = ["tmpfs", "devtmpfs", "devfs"]
# Read metrics about disk IO by device
[[inputs.diskio]]
# Get kernel statistics from /proc/stat
[[inputs.kernel]]
# Read metrics about memory usage
[[inputs.mem]]
# Get the number of processes and group them by status
[[inputs.processes]]
# Read metrics about swap memory usage
[[inputs.swap]]
# Read metrics about system load & uptime
[[inputs.system]]
# # Read metrics about network interface usage
[[inputs.net]]
# # Read TCP metrics such as established, time wait and sockets counts.
[[inputs.netstat]]
```

(continues on next page)

(continued from previous page)

```
# # Monitor process cpu and memory usage
[[inputs.procstat]]
  pattern = ".*"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
```

If for some reasons, you have to use either of the 2 other solutions, please consult:

• https://da-itsi-telegraf-os.readthedocs.io/en/latest/telegraf.html

Notes: The configuration above provides out of the box OS monitoring for the hosts, which can be used by the Operating System monitoring application for Splunk:

https://splunkbase.splunk.com/app/4271/

2.2.5 Jolokia JVM monitoring



The following Kafka components require Jolokia to be deployed and started, as the modern and efficient interface to JMX that is collected by Telegraf:

- Zookeeper
- · Apache Kafka Brokers
- Apache Kafka Connect
- · Confluent schema-registry
- · Confluent ksql-server
- · Confluent kafka-rest

For the complete documentation of Jolokia, see:

https://jolokia.org

Jolokia JVM agent can be started in 2 ways, either as using the -javaagent argument during the start of the JVM, or on the fly by attaching Jolokia to the PID ot the JVM:

• https://jolokia.org/reference/html/agents.html#agents-jvm

2.2.6 Starting Jolokia with the JVM

To start Jolokia agent using the -javaagent argument, use such option at the start of the JVM:

-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0

Note: This method is the method used in the docker example within this documentation by using the environment variables of the container.

When running on dedicated servers or virtual machines, update the relevant systemd configuration file to start Jolokia automatically:

For Zookeeper

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-zookeeper.service
- Add -javaagent argument:

```
[Unit]
Description=Apache Kafka - ZooKeeper
Documentation=http://docs.confluent.io/
After=network.target
[Service]
Type=simple
User=cp-kafka
Group=confluent
ExecStart=/usr/bin/zookeeper-server-start /etc/kafka/zookeeper.properties
Environment="KAFKA_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
Environment="LOG_DIR=/var/log/zookeeper"
TimeoutStopSec=180
Restart=no
[Install]
WantedBy=multi-user.target
```

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-zookeeper
```

For container based environments:

Define the following environment variable when starting the containers:

KAFKA_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"

For Kafka brokers

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-kafka.service
- Add -javaagent argument:

```
[Unit]
Description=Apache Kafka - broker
Documentation=http://docs.confluent.io/
After=network.target confluent-zookeeper.target
[Service]
Type=simple
User=cp-kafka
Group=confluent
ExecStart=/usr/bin/kafka-server-start /etc/kafka/server.properties
Environment="KAFKA_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
TimeoutStopSec=180
Restart=no
[Install]
```

WantedBy=multi-user.target

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-kafka
```

For container based environments:

Define the following environment variable when starting the containers:

KAFKA_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"

For Kafka Connect

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-kafka-connect.service
- Add -javaagent argument:

```
[Unit]
Description=Apache Kafka Connect - distributed
Documentation=http://docs.confluent.io/
After=network.target confluent-kafka.target
[Service]
Type=simple
User=cp-kafka-connect
Group=confluent
ExecStart=/usr/bin/connect-distributed /etc/kafka/connect-distributed.properties
Environment="KAFKA_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
Environment="LOG_DIR=/var/log/connect"
TimeoutStopSec=180
Restart=no
[Install]
WantedBy=multi-user.target
```

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-kafka-connect
```

For container based environments:

Define the following environment variable when starting the containers:

```
KAFKA_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
```

For Confluent schema-registry

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-schema-registry.service
- Add -javaagent argument:

```
[Unit]
Description=RESTful Avro schema registry for Apache Kafka
Documentation=http://docs.confluent.io/
After=network.target confluent-kafka.target
[Service]
Type=simple
User=cp-schema-registry
Group=confluent
Environment="LOG_DIR=/var/log/confluent/schema-registry"
Environment="SCHEMA_REGISTRY_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,
→host=0.0.0.0"
ExecStart=/usr/bin/schema-registry-start /etc/schema-registry/schema-registry.
→properties
TimeoutStopSec=180
Restart=no
[Install]
WantedBy=multi-user.target
```

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-schema-registry
```

For container based environments:

Define the following environment variable when starting the containers:

SCHEMA_REGISTRY_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"

For Confluent ksql-server

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-ksqldb.service
- Add -javaagent argument:

```
Description=Streaming SQL engine for Apache Kafka
Documentation=http://docs.confluent.io/
After=network.target confluent-kafka.target confluent-schema-registry.target
[Service]
Type=simple
User=cp-ksql
Group=confluent
Environment="LOG_DIR=/var/log/confluent/ksql"
Environment="KSQL_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
ExecStart=/usr/bin/ksql-server-start /etc/ksqldb/ksql-server.properties
TimeoutStopSec=180
Restart=no
[Install]
WantedBy=multi-user.target
```

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-ksqldb
```

For container based environments:

Define the following environment variable when starting the containers:

KSQL_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"

For Confluent kafka-rest

For bare-metals and dedicated VMs:

- Edit: /lib/systemd/system/confluent-kafka-rest.service
- Add -javaagent argument:

```
[Unit]
Description=A REST proxy for Apache Kafka
Documentation=http://docs.confluent.io/
After=network.target confluent-kafka.target
[Service]
Type=simple
User=cp-kafka-rest
Group=confluent
Environment="LOG_DIR=/var/log/confluent/kafka-rest"
Environment="KAFKAREST_OPTS=-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0
\hookrightarrow "
ExecStart=/usr/bin/kafka-rest-start /etc/kafka-rest/kafka-rest.properties
TimeoutStopSec=180
Restart=no
[Install]
WantedBy=multi-user.target
```

• Reload systemd and restart:

```
sudo systemctl daemon-restart
sudo systemctl restart confluent-kafka-rest
```

For container based environments:

Define the following environment variable when starting the containers:

```
KAFKAREST_OPTS: "-javaagent:/opt/jolokia/jolokia.jar=port=8778,host=0.0.0.0"
```

Notes: "KAFKAREST_OPTS" is not a typo, this is the real name of the environment variable for some reason.

2.2.7 Starting Jolokia on the fly

To attach Jolokia agent to an existing JVM, identify its process ID (PID), simplistic example:

```
ps -ef | grep 'kafka.properties' | grep -v grep | awk '{print $1}'
```

Then:

java -jar /opt/jolokia/jolokia.jar --host 0.0.0.0 --port 8778 start <PID>

Add this operation to any custom init scripts you use to start the Kafka components.

2.2.8 Zookeeper monitoring

Since the v1.1.31, Zookeeper metrics are now collected via JMX and Jolokia rather than the Telegraf Zookeeper plugin.

Collecting with Telegraf

Depending on how you run Kafka and your architecture preferences, you may prefer to collect all the brokers metrics from one Telegraf collector, or installed locally on the Kafka brocker machine.

Connecting to multiple remote Jolokia instances:

```
[[inputs.jolokia2_agent]]
name_prefix = "zk_"
urls = ["http://zookeeper-1:8778/jolokia","http://zookeeper-2:8778/jolokia","http://
>zookeeper-3:8778/jolokia"]
```

Connecting to the local Jolokia instance:

```
# Zookeeper JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "zk_"
urls = ["http://$HOSTNAME:8778/jolokia"]
```

Full telegraf.conf example

The following telegraf.conf collects a cluster of 3 Zookeeper nodes:

```
[global_tags]
 # the env tag is used by the application for multi-environments management
 env = "my_env"
  # the label tag is an optional tag used by the application that you can use as_
↔additional label for the services or infrastructure
 label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
  ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# Zookeeper JMX collection
[[inputs.jolokia2_agent]]
 name_prefix = "zk_"
 urls = ["http://zookeeper-1:8778/jolokia", "http://zookeeper-2:8778/jolokia", "http://
→zookeeper-3:8778/jolokia"]
[[inputs.jolokia2_agent.metric]]
 name = "quorum"
 mbean = "org.apache.ZooKeeperService:name0=*"
 tag_keys = ["name0"]
[[inputs.jolokia2_agent.metric]]
 name = "leader"
 mbean = "org.apache.ZooKeeperService:name0=*,name1=*,name2=Leader"
 tag_keys = ["name1"]
[[inputs.jolokia2_agent.metric]]
 name = "follower"
 mbean = "org.apache.ZooKeeperService:name0=*,name1=*,name2=Follower"
 tag_keys = ["name1"]
```

Visualization of metrics within the Splunk metrics workspace application:

ink >enterprise App: Searc														
														> Search & Rep
«	🕤 🛈 Last 6 hours 🔻	-C Split all by N	ione 🔻 🖏 Refre	sh 👻								🗟 Clear all	: =	Analysis
ics Datasets Alerts	zookeeper.max_latency													zookeeper.max_latency
eeper X	400												= Avg	AGGREGATIONS
keeper	300													Select one or more aggregations display in the chart.
proximate_data_size	200													Avg Max Mi
g_latency	100													Std dev Sum
phemerals_count	54.00 Wed, 17 Oct	14.30	15.00	15:30	10.00	10:30	17.00	17:30	13.00	12:30	19.00	19:30		Percentiles
lowers	2018													90 × 75 × 50 × 25 ×
st_proposal_size	zookeeper.approximate_dat	a_size												TIME COMPARISON
ax_file_descriptor_count														Overlay previous time period on
nax_latency	25.08												Arg	Compare to None
ax_proposal_size	15.04													Compare to Rene
in_latency	10.DK													SPLIT BY
in_proposal_size	5.0k													Split this metric by a dimension.
im_alive_connections	14.00	14.30	13.00	15:30	10.00	10:30	17.00	17:30	13.00	18:30	19.00	18:30		Split by None
itstanding_requests	Wed, 17 Oct 2018													FILTERS
ickets_received														Include or exclude metrics from s
ckets_sent														categories.
ending_syncs														host
rnced_followers														port
rced_tollowers														server
vatch_count														

Using mcatalog search command to verify data availability:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=zk_*

2.2.9 Kafka brokers monitoring with Jolokia

Collecting with Telegraf

Depending on how you run Kafka and your architecture preferences, you may prefer to collect all the brokers metrics from one Telegraf collector, or installed locally on the Kafka brocker machine.

Connecting to multiple remote Jolokia instances:

```
# Kafka JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "kafka_"
urls = ["http://kafka-1:18778/jolokia","http://kafka-2:28778/jolokia","http://kafka-
$\implies3:38778/jolokia"]
```

Connecting to the local Jolokia instance:

```
# Kafka JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "kafka_"
urls = ["http://$HOSTNAME:8778/jolokia"]
```

Full telegraf.conf example

The following telegraf.conf collects a cluster of 3 Kafka brokers:

```
[global_tags]
  # the env tag is used by the application for multi-environments management
  env = "my_env"
  # the label tag is an optional tag used by the application that you can use as_
   additional label for the services or infrastructure
   label = "my_env_label"
[agent]
```

(continues on next page)

```
(continued from previous page)
```

```
interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
  ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# Kafka JVM monitoring
[[inputs.jolokia2_agent]]
 name_prefix = "kafka_"
 urls = ["http://kafka-1:18778/jolokia","http://kafka-2:28778/jolokia","http://kafka-
→3:38778/jolokia"]
[[inputs.jolokia2_agent.metric]]
        = "controller"
 name
              = "kafka.controller:name=*,type=*"
 mbean
 field_prefix = "$1."
[[inputs.jolokia2_agent.metric]]
        = "replica_manager"
 name
              = "kafka.server:name=*,type=ReplicaManager"
 mbean
 field_prefix = "$1."
[[inputs.jolokia2_agent.metric]]
 name = "purgatory"
 mbean
             = "kafka.server:delayedOperation=*,name=*,
→type=DelayedOperationPurgatory"
field_prefix = "$1."
 field name = "$2"
[[inputs.jolokia2_agent.metric]]
         = "client"
 name
         = "kafka.server:client-id=*,type=*"
 mbean
 tag_keys = ["client-id", "type"]
[[inputs.jolokia2_agent.metric]]
       = "network"
 name
              = "kafka.network:name=*,request=*,type=RequestMetrics"
 mbean
 field_prefix = "$1."
 tag_keys = ["request"]
[[inputs.jolokia2_agent.metric]]
            = "network"
 name
              = "kafka.network:name=ResponseQueueSize,type=RequestChannel"
 mbean
 field_prefix = "ResponseQueueSize"
```

(continues on next page)

(continued from previous page)

```
= ["name"]
 taq_keys
[[inputs.jolokia2_agent.metric]]
         = "network"
 name
             = "kafka.network:name=NetworkProcessorAvgIdlePercent,type=SocketServer"
 mbean
 field_prefix = "NetworkProcessorAvgIdlePercent"
             = ["name"]
 tag_keys
[[inputs.jolokia2_agent.metric]]
 name = "topics"
 mbean
            = "kafka.server:name=*,type=BrokerTopicMetrics"
 field_prefix = "$1."
[[inputs.jolokia2_agent.metric]]
 name = "topic"
mbean = "kafka.server:name=*,topic=*,type=BrokerTopicMetrics"
 field_prefix = "$1."
 tag_keys = ["topic"]
[[inputs.jolokia2_agent.metric]]
       = "partition"
 name
 mbean
           = "kafka.log:name=*,partition=*,topic=*,type=Log"
 field_name = "$1"
 tag_keys = ["topic", "partition"]
[[inputs.jolokia2_agent.metric]]
 name = "log"
           = "kafka.log:name=LogFlushRateAndTimeMs,type=LogFlushStats"
 mbean
 field_name = "LogFlushRateAndTimeMs"
          = ["name"]
 tag_keys
[[inputs.jolokia2_agent.metric]]
 name
        = "partition"
          = "kafka.cluster:name=UnderReplicated,partition=*,topic=*,type=Partition"
 mbean
 field_name = "UnderReplicatedPartitions"
 tag_keys = ["topic", "partition"]
[[inputs.jolokia2_agent.metric]]
 name
      = "request_handlers"
 mbean
          = "kafka.server:name=RequestHandlerAvgIdlePercent,
→type=KafkaRequestHandlerPool"
 taq_keys = ["name"]
# JVM garbage collector monitoring
[[inputs.jolokia2_agent.metric]]
        = "jvm_garbage_collector"
 name
          = "java.lang:name=*,type=GarbageCollector"
 mbean
         = ["CollectionTime", "CollectionCount", "LastGcInfo"]
 paths
 tag_keys = ["name"]
```

Visualization of metrics within the Splunk metrics workspace application:

splunk>enterprise App: Searc	n & Reporting + 🕜 Administrator = Messages = Settings = J	Activity • Help • Find Q
Search Metrics Datasets		Search & Reporting
Data «	⊙ OLast 6 hours • < Spital by None • Q Refersh •	Analysis »
Metrics Datasets Alerts	Lufta, Juffa morter condu delay no ang	kafka_kafka-monitor.records-delay- ms-avg
kafka-monitor X	multiment and	AGGREGATIONS Select one or more aggregations to display in the chart.
bytes-consumed-rate consume-availability-avg		Avg Max Min
consume-error-rate consume-error-total produce-availability-avg	18,38 N.M. N.M. 17.01 17.01 17.01 18,00 18,00 18,00 18,00 26	Percentiles
produce-delay-ms-99th produce-delay-ms-999th	kalka, kalko morito produce-delay-mo-org	TIME COMPARISON
 produce-delay-ms-avg produce-delay-ms-max 	- marken Mar	Overlay previous time period on the selected chart. Compare to None •
 produce-error-rate produce-error-rate-partition-0 produce-error-rate-partition-1 		SPLIT BY Split this metric by a dimension.
 produce-error-rate-partition-2 produce-error-rate-partition-3 	438 449 433 178 178 478 478 478 938 938 348 358 358 378 ### 178 ## ##	Split by None •
 produce-error-rate-partition-4 produce-error-rate-partition-5 produce-error-total 		Include or exclude metrics from specific categories.
producerentification producerentification proceedings records-consumed-total		lolokia_agent_url
records-delay-ms-99th records-delay-ms-99th		
records-delay-ms-avg records-delay-ms-max		
records-delayed-rate records-delayed-total		
records-duplicated-rate records-duplicated-total records-lost-rate		
 		Send feedback

Using mcatalog search command to verify data availability:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=kafka_*.*

2.2.10 Kafka connect monitoring

Collecting with Telegraf

Connecting to multiple remote Jolokia instances:

```
# Kafka-connect JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "kafka_connect."
urls = ["http://kafka-connect-1:18779/jolokia","http://kafka-connect-2:28779/jolokia
]
```

Connecting to local Jolokia instance:

```
# Kafka-connect JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "kafka_connect."
urls = ["http://$HOSTNAME:8778/jolokia"]
```

Full telegraf.conf example

bellow a full telegraf.conf example:

(continues on next page)

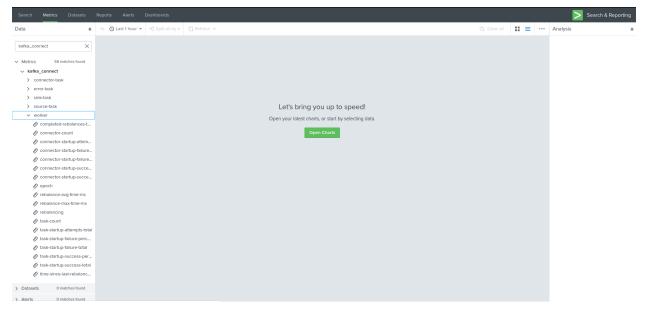
(continued from previous page)

```
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
  ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# Kafka-connect JVM monitoring
[[inputs.jolokia2_agent]]
 name_prefix = "kafka_connect."
 urls = ["http://kafka-connect-1:18779/jolokia", "http://kafka-connect-2:28779/jolokia
→", "http://kafka-connect-3:38779/jolokia"]
[[inputs.jolokia2_agent.metric]]
              = "worker"
 name
              = "kafka.connect:type=connect-worker-metrics"
 mbean
[[inputs.jolokia2_agent.metric]]
 name
         = "worker"
 mbean
              = "kafka.connect:type=connect-worker-rebalance-metrics"
[[inputs.jolokia2_agent.metric]]
 name = "connector-task"
 mbean
              = "kafka.connect:type=connector-task-metrics,connector=*,task=*"
 tag_keys = ["connector", "task"]
[[inputs.jolokia2_agent.metric]]
             = "sink-task"
 name
          = "kafka.connect:type=sink-task-metrics,connector=*,task=*"
 mbean
 tag_keys = ["connector", "task"]
[[inputs.jolokia2_agent.metric]]
           = "source-task"
 name
 mbean
              = "kafka.connect:type=source-task-metrics,connector=*,task=*"
 tag_keys = ["connector", "task"]
[[inputs.jolokia2_agent.metric]]
 name = "error-task"
 mbean
              = "kafka.connect:type=task-error-metrics,connector=*,task=*"
 tag_keys = ["connector", "task"]
# Kafka connect return a status value which is non numerical
# Using the enum processor with the following configuration replaces the string value.
                                                                        (continues on next page)
→by our mapping
```

(continued from previous page)

```
[[processors.enum]]
[[processors.enum.mapping]]
## Name of the field to map
field = "status"
## Table of mappings
[processors.enum.mapping.value_mappings]
    paused = 0
    running = 1
    unassigned = 2
    failed = 3
    destroyed = 4
```

Visualization of metrics within the Splunk metrics workspace application:



Using mcatalog search command to verify data availability:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=kafka_connect.*

2.2.11 Kafka Xinfra monitor - end to end monitoring

Installing and starting the Kafka monitor

LinkedIn provides an extremely powerful open source end to end monitoring solution for Kafka, please consult:

· https://github.com/linkedin/kafka-monitor

As a builtin configuration, the kafka-monitor implements a jolokia agent, so collecting the metrics with Telegraf cannot be more easy !

It is very straightforward to run the kafka-monitor in a docker container, first you need to create your own image:

https://github.com/linkedin/kafka-monitor/tree/master/docker

In a nutshell, you would:

```
git clone https://github.com/linkedin/kafka-monitor.git
cd kafka-monitor
./gradlew jar
cd docker
```

Edit the Makefile to match your needs

make container make push

Then start your container, example with docker-compose:

Once your Kafka monitor is running, you need a Telegraf instance that will be collecting the JMX beans, example:

```
[global_tags]
 # the env tag is used by the application for multi-environments management
 env = "my_env"
 # the label tag is an optional tag used by the application that you can use as,
↔additional label for the services or infrastructure
 label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# Kafka JVM monitoring
[[inputs.jolokia2_agent]]
 name_prefix = "kafka_"
 urls = ["http://kafka-monitor:8778/jolokia"]
[[inputs.jolokia2_agent.metric]]
              = "kafka-monitor"
 name
              = "kmf.services:name=*,type=*"
 mbean
```

unk>enterprise App: Sear			
			Search & Repo
a «	O Last 6 hours • < Split all by None • O Refresh •	:: ≡ ·	Analysis
trics Datasets Alerts	lada, Jaña erontorr ecede delay era ang		kafka_kafka-monitor.records- ms-avg
ka-monitor X		■ Avg	AGGREGATIONS Select one or more aggregations display in the chart.
consume-availability-avg consume-error-rate consume-error-total			Avg Max Min Std dav Sum Percentiles
roduce-availability-avg roduce-delay-ms-99th roduce-delay-ms-999th	Natural Sector produce delay one way		90 × 75 × 50 × 25 × TIME COMPARISON
roduce-delay-ms-avg roduce-delay-ms-max roduce-error-rate		 Arg 	Overlay previous time period on selected chart. Compare to None
roduce-error-rate-partition-0			SPLIT BY Split this metric by a dimension.
roduce-error-rate-partition-2 roduce-error-rate-partition-3	" (43) 400 493 (70) (73) 400 433 (940 93) 200 239 200 215 215		Split by None
roduce-error-rate-partition-4 roduce-error-rate-partition-5 roduce-error-total			FILTERS Include or exclude metrics from categories.
cords-consumed-rate			jolokia_agent_url
cords-delay-ms-99th			
cords-delay-ms-avg			
cords-delayed-rate			
cords-delayed-total cords-duplicated-rate cords-duplicated-total			
ecords-lost-rate			
records-produced-rate +			Send

Visualization of metrics within the Splunk metrics workspace application:

Using meatalog search command to verify data availability:

```
| mcatalog values(metric_name) values(_dims) where index=* metric_name=kafka_kafka-

->monitor.*
```

2.2.12 Confluent schema-registry

Collecting with Telegraf

Connecting to multiple remote Jolokia instances:

```
[[inputs.jolokia2_agent]]
name_prefix = "kafka_schema-registry."
urls = ["http://schema-registry:18783/jolokia"]
```

Connecting to local Jolokia instance:

```
# Kafka-connect JVM monitoring
[[inputs.jolokia2_agent]]
name_prefix = "kafka_schema-registry."
urls = ["http://$HOSTNAME:8778/jolokia"]
```

Full telegraf.conf example

bellow a full telegraf.conf example:

```
[global_tags]
# the env tag is used by the application for multi-environments management
env = "my_env"
# the label tag is an optional tag used by the application that you can use as_
additional label for the services or infrastructure
```

(continues on next page)

(continued from previous page)

```
label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
   # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# schema-registry JVM monitoring
[[inputs.jolokia2_agent]]
 name_prefix = "kafka_schema-registry."
 urls = ["http://schema-registry:18783/jolokia"]
[[inputs.jolokia2_agent.metric]]
              = "jetty-metrics"
 name
              = "kafka.schema.registry:type=jetty-metrics"
 mbean
 paths = ["connections-active", "connections-opened-rate", "connections-closed-rate"]
[[inputs.jolokia2_agent.metric]]
         = "master-slave-role"
 name
 mbean
              = "kafka.schema.registry:type=master-slave-role"
[[inputs.jolokia2_agent.metric]]
             = "jersey-metrics"
 name
 mbean
              = "kafka.schema.registry:type=jersey-metrics"
```

Visualization of metrics within the Splunk metrics workspace application:

splunk>enterprise App: Search	n & Reporting 🔻									Adminis	trator 💌	Messages 🔻	Settings	• Ad	tivity • Help • Find Q		
Search Metrics Datasets I	Search Metrica Datasets Reports Alerts Dashbeards 🔀 Search & Reporting														Search & Reporting		
Data «	🕤 🛈 Last 1 hour 🔹	-C Split all by -	Auto-refresh 🕶	(7s to refresh)								🕞 Clear all	:: =		Analysis »		
schema-registry X															kafka_schema-registry.jetty- metrics.connections-opened-rate		
 Metrics 77 matches found Kafica_schema-registy jersey-metrics compatibility subjects ven request-byte-rate request-byte-rate 	1 0.75 0.5 0.25 0 16. Fri 207	9 Nov	16:25	16.30	16.35	16:40	18.45	16:50	18.55	17:00	17.05	17:10	■ Avg	o	AGGREGATIONS Select one or more aggregations to display in the chart.		
request-latency-avg request-latency-avg request-latency-max request-latency-avg request-latency-avg request-latenx-avg response-tyte-nate response-tyte-nate response-laten-max response-laten-max	1 0.75 0.5 0.25 0 160		16.25	18-30	16.35	16-40	16.45	16.50	18.55	17.00	17.05	17:10	■ <i>log</i>	0	90 × 75 × 80 × 25 × 10 × TIME COMPARISON Overlap previous time period on the selected chart. Selected chart. Selected chart. • Split Tim W Split this method by admension. Split the selected chart. • •		
 ⊘ request-error-rate ⊘ response-rate ⊘ subjects ✓ delete-subject 	guest-rate kulkactema registry.inty interior. connections active sponse-rate											Mag and Ang			FILTERS Include or exclude metrics from specific categories. host jolokia_agent_urt		
 ✓ response-rate ✓ get-schema 	0 10: Fil, 20'		16:25	10:30	10:35	16:40	10:45	18:50	10.55	17:00	17:05	17:10					

Using meatalog search command to verify data availability:

2.2.13 Confluent ksql-server

Collecting with Telegraf

Connecting to multiple remote Jolokia instances:

```
[[inputs.jolokia2_agent]]
name_prefix = "kafka_"
urls = ["http://ksql-server-1:18784/jolokia"]
```

Connecting to local Jolokia instance:

```
[[inputs.jolokia2_agent]]
name_prefix = "kafka_"
urls = ["http://$HOSTNAME:18784/jolokia"]
```

Full telegraf.conf example

bellow a full telegraf.conf example:

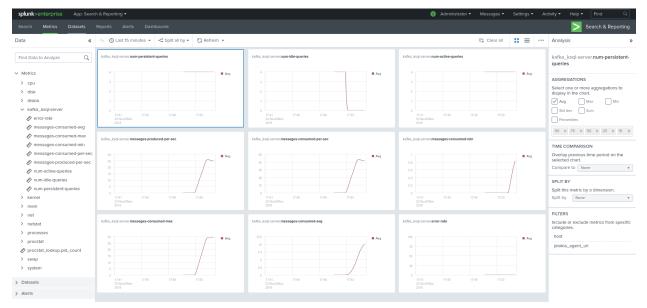
```
[global_tags]
# the env tag is used by the application for multi-environments management
env = "my_env"
# the label tag is an optional tag used by the application that you can use as_
additional label for the services or infrastructure
label = "my_env_label"
[agent]
interval = "10s"
```

(continues on next page)

(continued from previous page)

```
flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# ksql-server JVM monitoring
[[inputs.jolokia2_agent]]
  name_prefix = "kafka_"
  urls = ["http://ksql-server:18784/jolokia"]
[[inputs.jolokia2_agent.metric]]
  name
               = "ksql-server"
               = "io.confluent.ksql.metrics:type=*"
  mbean
```

Visualization of metrics within the Splunk metrics workspace application:



Using meatalog search command to verify data availability:

2.2.14 Confluent kafka-rest

Collecting with Telegraf

```
Connecting to multiple remote Jolokia instances:
```

```
[[inputs.jolokia2_agent]]
name_prefix = "kafka_kafka-rest."
urls = ["http://kafka-rest:8778/jolokia"]
```

Connecting to local Jolokia instance:

```
[[inputs.jolokia2_agent]]
name_prefix = "kafka_kafka-rest."
urls = ["http://$HOSTNAME:18785/jolokia"]
```

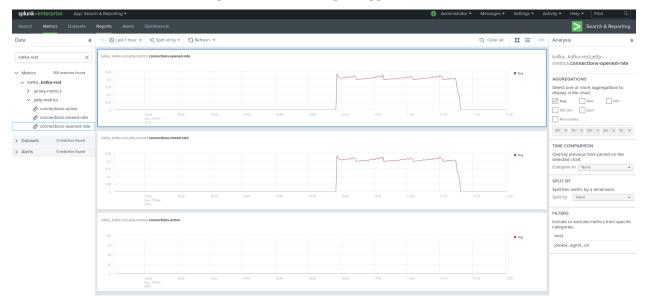
Full telegraf.conf example

bellow a full telegraf.conf example:

```
[global_tags]
 # the env tag is used by the application for multi-environments management
 env = "my_env"
 # the label tag is an optional tag used by the application that you can use as,
→additional label for the services or infrastructure
 label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# kafka-rest JVM monitoring
[[inputs.jolokia2_agent]]
  name_prefix = "kafka_kafka-rest."
  urls = ["http://kafka-rest:18785/jolokia"]
[[inputs.jolokia2_agent.metric]]
               = "jetty-metrics"
  name
               = "kafka.rest:type=jetty-metrics"
  mbean
  paths = ["connections-active", "connections-opened-rate", "connections-closed-rate"
 "
```

```
[[inputs.jolokia2_agent.metric]]
name = "jersey-metrics"
mbean = "kafka.rest:type=jersey-metrics"
```

Visualization of metrics within the Splunk metrics workspace application:



Using meatalog search command to verify data availability:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=kafka_kafka_ \$\dotskafka-rest.*

2.2.15 Confluent Interceptor Monitoring

Implement Confluent Interceptor integration to Splunk

Confluent Interceptor allows monitoring latency from producers and consumers in any kind of ways and is a very performing and rich way to monitor your Kafka components for Confluent customers:

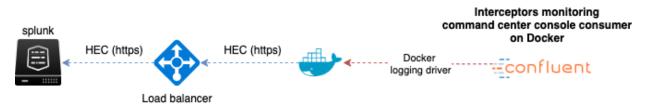
• https://docs.confluent.io/current/control-center/installation/clients.html

To collect Confluent Interceptors metrics in Splunk, we use the following method:

- We use a Docker container to run the command center console consumer from the interceptor topic, by default "_confluent-monitoring"
- You cannot consume this topic directly in Splunk without the command center console consumer as it contains binary data that would not be readable without the command center
- Once started, the Docker container consumes the topic and outputs the data in the stdout
- The Docker container uses the Splunk Docker logging driver to forward this data to a Splunk HTTP Event Collector endpoint
- Finally, we use the Splunk logs to metrics capabilities to transform the metric events into metrics stored in the Splunk metric store

For more information about Splunk logs to metrics capabilities, consult:

• https://docs.splunk.com/Documentation/Splunk/latest/Metrics/L2MOverview



Make sure you enabled Interceptors in your products as explained in the Confluent documentation, for instance for Kafka Connect you will add the following configuration in your worker properties:

```
producer.interceptor.classes=io.confluent.monitoring.clients.interceptor.

→MonitoringProducerInterceptor

consumer.interceptor.classes=io.confluent.monitoring.clients.interceptor.

→MonitoringConsumerInterceptor
```

Note: adding this config would require a restart of Kafka Connect to be applied

Once you decided where to run the Docker container, which could be the same machine hosting the command center for example, you will:

Create a new metric (not a event index!) index to store the Confluent interceptor metrics, by default the application excepts:

confluent_interceptor_metrics

Create an HEC token dedicated for it, or allow an existing token to forward to the metric index, example:

```
[http://confluent_interceptor_metrics]
disabled = 0
index = confluent_interceptor_metrics
indexes = confluent_interceptor_metrics
token = xxxxxx-xxxx-xxxx-xxxxx-xxxx
```

The following props.conf and transforms.conf configuration need to be deployed to the indexers or intermediate forwarders, these are not need on the search heads:

Define the following sourcetype in a props.conf configuration file in Splunk:

```
[confluent_interceptor]
SHOULD_LINEMERGE=false
LINE_BREAKER=([\r\n]+)
CHARSET=UTF-8
# Add the env, label and host inside the JSON, remove anything before the json start

→ "label":"\2", "host":"\3",/g

# Be strict and performer
TIME_FORMAT=%s%3N
TIME_PREFIX=\"timestamp\":\"
MAX_TIMESTAMP_LOOKAHEAD=35
# Handle the host Meta
TRANSFORMS-confluent-interceptor-host = confluent_interceptor_host
# Only keep the metrics, send any other events from the container to the null queue
TRANSFORMS-setnull = confluent_interceptor_setnull
# Logs to metrics
```

```
TRANSFORMS-fieldvalue=confluent_interceptor_fields_extraction
TRANSFORMS-metricslog=confluent_interceptor_eval_pipeline
METRIC-SCHEMA-TRANSFORMS=metric-schema:extract_metrics
```

Define the following transforms in a transforms.conf configuration file in Splunk:

```
[confluent_interceptor_setnull]
REGEX = ^confluentinc/cp-enterprise-control-center
DEST_KEY = queue
FORMAT = nullQueue
[confluent_interceptor_fields_extraction]
FORMAT = $1::$2
REGEX = \ ([a-zA-Z0-9], ]+) \ ([a-zA-Z0-9], -]+)
REPEAT_MATCH = true
SOURCE_KEY = _raw
WRITE_META = true
[confluent_interceptor_host]
DEST_KEY = MetaData:Host
FORMAT = host::$1
[confluent_interceptor_eval_pipeline]
INGEST_EVAL = metric_name="confluent_interceptor"
[metric-schema:extract_metrics]
METRIC-SCHEMA-MEASURES-confluent_interceptor=_ALLNUMS_
METRIC-SCHEMA-MEASURES-confluent_interceptor=count,aggregateBytes,aggregateCrc,
→totalLatency,minLatency,maxLatency,arrivalTime
METRIC-SCHEMA-BLACKLIST-DIMS-confluent_interceptor=host, session, sequence, window,
→minWindow, maxWindow
```

Define a new Docker container, you can use docker-compose for an easier deployment and maintenance:

• On the machine hosting the Docker container, create a new directory:

mkdir /opt/confluent-interceptor
cd /opt/confluent-interceptor

• In this directory, copy the command center properties file that you use for command center, at the minimal you need to define the kafka broker and zookeeper connection string:

properties

- We use the properties file to bootrap the command center console consumer, not an instance of the command center
- You can remove most of the configuration from the properties, what is required is providing the connectivity settings to your Kafka brokers and Zookeeper ensemble
- If you SSL and any mechanism use of authentication, make sure to include the settings accordingly
- Do not update the setting confluent.controlcenter.data.dir from your Command center configuration, if the directory cannot be used by the container, the console consumer will not start

control-center.properties

Finally, create a new docker-compose.yml file as follows, edit the Splunk index, the HEC target and the HEC token to match your deployment:

docker-compose version

- Make sure to download the very last version of docker-compose from https://docs.docker.com/compose/install
- If you cannot use a recent version of docker-compose and/or the Docker engine, lower the version on top of the yaml file

```
version: '3.8'
services:
 confluent-interceptor:
   image: confluentinc/cp-enterprise-control-center
   restart: always
   hostname: confluent-interceptor
   logging:
     driver: splunk
     options:
       splunk-token: "xxxxxxx-xxxx-xxxx-xxxx-xxxx"
       splunk-url: "https://mysplunk.domain.com:8088"
       splunk-insecureskipverify: "true"
       splunk-verify-connection: "false"
       splunk-index: "confluent_interceptor_metrics"
       splunk-sourcetype: "confluent_interceptor"
       splunk-format: "raw"
       tag: "{{.ImageName}}/{{.ID}}"
       env: "env, label, host"
   mem limit: 600m
   extra_hosts:
      - "kafka-1 kafka-1.acme.com:xxx.xxx.xxx"
      - "kafka-2 kafka-2.acme.com:xxx.xxx.xxx.xxx"
      - "kafka-3 kafka-3.acme.com:xxx.xxx.xxx.xxx"
   volumes:
      - ../confluent/control-center.properties:/etc/confluent-control-center/control-
⇔center.properties
   environment:
     env: "docker_env"
     label: "testing"
     host: "confluent-consumer-interceptor"
   command: "/usr/bin/control-center-console-consumer /etc/confluent-control-center/
→control-center.properties --topic _confluent-monitoring"
```

Tip:

 You can include an hosts mapping in the docker-compose file to populate the /etc/hosts on the container, depending on your Kafka brokers configuration, it might be required that the container knows how to communicate with the brokers using their FQDN / host name for instance

• DNS resolution from the container is a potential root cause of failure so it is important you handle this configuration properly

```
version: '3.8'
services:

confluent-interceptor:
    image: confluentinc/cp-enterprise-control-center
    restart: always
    hostname: confluent-interceptor
    mem_limit: 600m
    extra_hosts:
        - "kafka-1 kafka-1.acme.com:xxx.xxx.xxx"
        - "kafka-2 kafka-2.acme.com:xxx.xxx.xxx"
        - "kafka-3 kafka-3.acme.com:xxx.xxx.xxx"
```

Start the container:

docker-compose up -d

Shall the system be restarted, or the container be failing, Docker will automatically restart a new container.

After the image has been downloaded, the container automatically starts and metrics start to be forwarded to Splunk:

Overview Brokers Topics Burrow Analytics Search - Kafka monit	oring 👻 Kafka logging 👻 Kafka alerting 👻 Connected	Experience 🕶 Audit 🕶 Settings 🕶 Run a search	Kafka Smart Monitoring
New Search			Save As 🔻 Close
mcatalog values(metric_name) values(_dims) where index=* metric_name=confluent_	interceptor.* by index		Last 24 hours 🔻 🔍
✓ 10 events (17/10/2020 14:00:00.000 to 18/10/2020 14:46:25.000) No Event Sampling ▼		Job 🔻 🗉 📄 🏕 📥 Standard (search default) • • Smart Mode •
Events Patterns Statistics (1) Visualization			
100 Per Page ▼ ✓ Format Preview ▼			
index ‡	values(metric_name) \$	✓ values(_dims) ≎	/
confluent_interceptor_metrics	confluent_interceptor.aggregateBytes confluent_interceptor.agregateCrc confluent_interceptor.arrivalTime confluent_interceptor.count confluent_interceptor.minLatency confluent_interceptor.iniLatency confluent_interceptor.totalLatency	clientId clientType clusterId group monitoringTopicPartition partition samplePeriod shutdown topic type	

You can use the following search to verify that metrics are being ingested:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=confluent_ interceptor.* by index

You can as well use the msearch command:

msearch index=* filter="metric_name="confluent_interceptor.*""

Overview Brokers Topics B	Burrow Analytics	Search Kafka monitoring	Kafka logging 👻 Kafka alerting 🔻	Connected Experience •	Audit - Settings	👻 Run a search	Kafka Smart Monitoring
New Search							Save As 🔻 Close
msearch index=* filter="metric_na	ame="confluent_interce	ptor.*""					Last 15 minutes 🔻 🔍
✓ 180 events (18/10/2020 14:36:19.000 to	18/10/2020 14:51:19.000) No Event Sampling 🔻			Job 🔻		Standard (search default) • • Smart Mode •
Events (180) Patterns Statistics	Visualization						
Format Timeline - Zoom Out	+ Zoom to Selection	× Deselect					1 minute per column
	List 🔻 🖌 Forma	t 20 Per Page 🔻				< Prev 1	2 3 4 5 6 7 8 9 Next >
< Hide Fields :≡ All Fields	i Time	Event					
SELECTED FIELDS a host 1 a source 1 a source 1 a source 1 a source/spo 1 NTERESTNG FIELDS a client(3 a cli	> 18/02/22 14:51:05:000	<pre>([-]</pre>	bviUwA demo3 ceptor.aggregateGrc: 0 ceptor.arivalTime: 0 ceptor.carivalTime: 0 ceptor.maxLatency: 0 ceptor.maxLatency: 0	etype = confluent_interceptor			
<pre>minLatency 1 # metric_name:confluent_interceptor. otalLatency 1 # monitoringTopicPartition 1 # partition 1 # samplePeriod 1</pre>	> 18/10/2020 14:51:15.000	<pre>([-] clientId: connector-consumer clientType: CONSUMER clusterId: nBMrPOaRbyE-2Mp0 group: connect=sink=splunk-d metric_name.confluent_interce</pre>	aviDwA demo1				

Troubleshoot Confluent Interceptor consumer

If you do not receive the metrics in Splunk, there can be different root causes:

- The Docker container started and stopped almost immediately, which is most certainly linked to the properties configuration
- The command-center console consumer cannot access to Kafka due to configuration issues, network connectivity, DNS resolution, etc
- The connectivity between the Docker container and Splunk HTTP Event Collector is not valid

A first verification that can be done easily consists in disabling the Splunk logging driver to review the standard and error output of the container and command-center:

Stop the container if it is running, then edit the configuration, remove, create and start the container:

```
docker-compose stop confluent-interceptor
docker-compose rm -f confluent-interceptor
```

docker-compose.yml

```
version: '3.8'
services:

confluent-interceptor:
    image: confluentinc/cp-enterprise-control-center
    restart: always
    hostname: confluent-interceptor
    #logging:
    # driver: splunk
    # options:
    # splunk-token: "xxxxxx-xxxx-xxxx-xxxxxxxxxxx"
    # splunk-token: "https://mysplunk.domain.com:8088"
    # splunk-insecureskipverify: "true"
```

```
splunk-verify-connection: "false"
        splunk-index: "confluent_interceptor_metrics"
   #
        splunk-sourcetype: "confluent_interceptor"
   #
        splunk-format: "raw"
   #
        tag: "{{.ImageName}}/{{.Name}}/{{.ID}}"
        env: "env, label, host"
   mem_limit: 600m
   volumes:
     - ../confluent/control-center.properties:/etc/confluent-control-center/control-
⇔center.properties
   environment:
     env: "docker_env"
     label: "testing"
     host: "confluent-consumer-interceptor"
   command: "/usr/bin/control-center-console-consumer /etc/confluent-control-center/
⇔control-center.properties --topic _confluent-monitoring"
```

Then run the container in attached mode: (as opposed to daemon mode with the -d option)

docker-compose up confluent-interceptor

The container will output to stdout, any failure to start the console consumer due to a properties issues would appear clearly:

Press Ctrl+C to stop the container

```
Creating template_docker_splunk_localhost_confluent-interceptor_1 ... done
Attaching to template_docker_splunk_localhost_confluent-interceptor_1
confluent-interceptor_1
                            | OpenJDK 64-Bit Server VM warning: Option_
-UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a_
\hookrightarrowfuture release.
                           | SLF4J: Class path contains multiple SLF4J bindings.
confluent-interceptor_1
confluent-interceptor_1
                            | SLF4J: Found binding in [jar:file:/usr/share/java/acl/
⇔acl-6.0.0.jar!/org/slf4j/impl/StaticLoggerBinder.class]
confluent-interceptor_1
                            | SLF4J: Found binding in [jar:file:/usr/share/java/
→confluent-control-center/slf4j-log4j12-1.7.30.jar!/org/slf4j/impl/
→StaticLoggerBinder.class]
                            | SLF4J: See http://www.slf4j.org/codes.html#multiple_
confluent-interceptor_1
→ bindings for an explanation.
confluent-interceptor_1
                           | SLF4J: Actual binding is of type [org.slf4j.impl.
→Log4jLoggerFactory]
confluent-interceptor_1
                           | WARNING: An illegal reflective access operation has_
⇔occurred
confluent-interceptor_1
                           | WARNING: Illegal reflective access by com.google.
-to method java.lang.ClassLoader.defineClass(java.lang.String,byte[],int,int,java.
→security.ProtectionDomain)
confluent-interceptor_1
                            | WARNING: Please consider reporting this to the
→maintainers of com.google.inject.internal.cglib.core.$ReflectUtils$1
confluent-interceptor_1 | WARNING: Use --illegal-access=warn to enable warnings_
\hookrightarrow of further illegal reflective access operations
confluent-interceptor_1 | WARNING: All illegal access operations will be denied.
\rightarrow in a future release
confluent-interceptor_1
                            | _confluent-monitoring 0
                                                           2020-10-18T14:05:57.
                   {"clientType":"CONSUMER","clientId":"connector-consumer-sink-
-7717
             null
→splunk-demo2-0", "group": "connect-sink-splunk-demo2", "session": "f0538df4-a9bd-458b-
→94f6-5d2lc94f8l2d", "sequence":"4", "window":"0", "timestamp":"1603029957771", "topic":
→ "kafka_demo", "partition":0, "count":"0", "aggregateBytes":"0", "aggregateQcontinues on next page)
-- "totalLatency":"0", "minLatency":"0", "maxLatency":"0", "samplePeriod":"15000", "type":
40"monitoringTopicPartition":0, "clusterId": "nBWbrfChapter-2WpDeploymentland configuration:
→"arrivalTime":"0"}
```

```
2020-10-18T14:06:00.
confluent-interceptor_1
                        | _confluent-monitoring 0
→033Z
                {"clientType":"CONSUMER", "clientId":"connector-consumer-sink-
          null
→splunk-demo1-0", "group": "connect-sink-splunk-demo1", "session": "d18293d8-7f25-4b6c-
→bbfc-07a08efab9af", "sequence": "7", "window": "0", "timestamp": "1603029960033", "topic":
→ "kafka_demo", "partition":0, "count":"0", "aggregateBytes":"0", "aggregateCrc":0,
→ "totalLatency":"0", "minLatency":"0", "maxLatency":"0", "samplePeriod":"15000", "type":
→ "HEARTBEAT", "shutdown":false, "minWindow":"-1", "maxWindow":"-1",
→"arrivalTime":"0"}
confluent-interceptor_1
                       | _confluent-monitoring 0
                                                 2020-10-18T14:06:04.
↔652Z
       null {"clientType":"CONSUMER","clientId":"connector-consumer-sink-
→splunk-demo3-0", "group": "connect-sink-splunk-demo3", "session": "f0c0222c-a466-4b60-
→8497-7cb1d0ebfafc", "sequence": "22", "window": "0", "timestamp": "1603029964652", "topic":
→ "kafka_demo_headers", "partition":0, "count":"0", "aggregateBytes":"0", "aggregateCrc
→"arrivalTime":"0"}
^CGracefully stopping... (press Ctrl+C again to force)
Stopping template_docker_splunk_localhost_confluent-interceptor_1 ... done
```

In the output, raw metrics are:

If you can see metrics here, then the command center console consumer is able to bootstrap, access Kafka and Zookeeper, and there are activity in the topic.

Note that if you have no consumers or producers with the Confluent interceptors enabled, there will be no metrics generated here.

Disable command-center startup, keep the container running and exec into the container:

The next troubleshooting steps will allow you to enter the container and manually troubleshoot the startup of command center.

To achieve this, we disable the command replaced by a tail which allows keeping the container ready for operations:

```
version: '3.8'
services:

confluent-interceptor:
    image: confluentinc/cp-enterprise-control-center
    restart: always
    hostname: confluent-interceptor
    #logging:
    # driver: splunk
    # options:
    # splunk-token: "xxxxxx-xxxx-xxxx-xxxxxxxxxxxx"
    # splunk-token: "https://mysplunk.domain.com:8088"
    # splunk-insecureskipverify: "true"
```

```
splunk-verify-connection: "false"
        splunk-index: "confluent_interceptor_metrics"
   #
        splunk-sourcetype: "confluent_interceptor"
   #
        splunk-format: "raw"
        tag: "{{.ImageName}}/{{.Name}}/{{.ID}}"
        env: "env, label, host"
   mem_limit: 600m
   volumes:
     - ../confluent/control-center.properties:/etc/confluent-control-center/control-
⇔center.properties
   environment:
     env: "docker_env"
     label: "testing"
     host: "confluent-consumer-interceptor"
   #command: "/usr/bin/control-center-console-consumer /etc/confluent-control-center/
⇔control-center.properties --topic _confluent-monitoring"
   command: "tail -f /dev/null"
```

If the container is started, stop the container, then remove and create the container:

docker-compose stop confluent-interceptor
docker-compose rm -f confluent-interceptor

Start the container in daemon mode:

docker-compose up -d confluent-interceptor

Exec into the container:

docker-compose exec confluent-interceptor /bin/bash

Once you are in container, you can review the properties file as it seen by the container, make sure it contains the proper required configuration:

cat /etc/confluent-control-center/control-center.properties

You can attempt to manually run command-center console consumer and review step by step any failure:

Review carefully any failure.

Tip:

- By default, the exec command will make you enter the container as the relevant user "appuser"
- If you wish to access as root user instead, use the -user root argument in the exec command

docker-compose exec confluent-interceptor /bin/bash

For anymore troubleshooting related to command-center itself, consult:

• https://docs.confluent.io/current/control-center/installation/troubleshooting.html

If these steps are fine but you do not receive metrics in Splunk, there might a connectivity issue or misconfiguration on between the Docker container and Splunk, you can force the Docker logging driver to verify the connectivity when starting up:

```
splunk-verify-connection: "true"
```

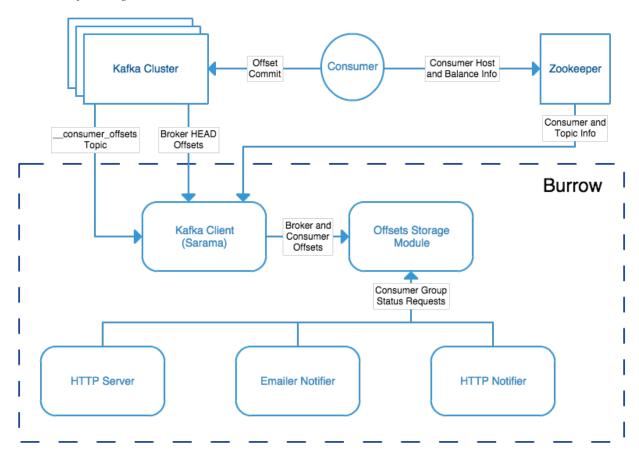
If the connectivty is not working, Docker will refuse to start the container.

2.2.16 Burrow Lag Consumers

As from their authors, Burrow is a monitoring companion for Apache Kafka that provides consumer lag checking as a service without the need for specifying thresholds.

See: https://github.com/linkedin/Burrow

Burrow workflow diagram:



Burrow is a very powerful application that monitors all consumers (Kafka Connect connectors, Kafka Streams...) to report an advanced state of the service automatically, and various useful lagging metrics.

Telegraf has a native input for Burrow which polls consumers, topics and partitions lag metrics and statuses over http, use the following telegraf minimal configuration:

See: https://github.com/influxdata/telegraf/tree/master/plugins/inputs/burrow

```
[global_tags]
# the env tag is used by the application for multi-environments management
```

```
env = "my_env"
 # the label tag is an optional tag used by the application that you can use as_
→additional label for the services or infrastructure
 label = "my_env_label"
[agent]
 interval = "10s"
 flush_interval = "10s"
 hostname = "$HOSTNAME"
# outputs
[[outputs.http]]
  url = "https://splunk:8088/services/collector"
  insecure_skip_verify = true
  data_format = "splunkmetric"
   ## Provides time, index, source overrides for the HEC
  splunkmetric_hec_routing = true
   ## Additional HTTP headers
   [outputs.http.headers]
  # Should be set manually to "application/json" for json data_format
     Content-Type = "application/json"
     Authorization = "Splunk 205d43f1-2a31-4e60-a8b3-327eda49944a"
     X-Splunk-Request-Channel = "205d43f1-2a31-4e60-a8b3-327eda49944a"
# Burrow
[[inputs.burrow]]
 ## Burrow API endpoints in format "schema://host:port".
 ## Default is "http://localhost:8000".
 servers = ["http://dockerhost:9001"]
 ## Override Burrow API prefix.
 ## Useful when Burrow is behind reverse-proxy.
 # api_prefix = "/v3/kafka"
 ## Maximum time to receive response.
 # response_timeout = "5s"
 ## Limit per-server concurrent connections.
 ## Useful in case of large number of topics or consumer groups.
 # concurrent connections = 20
 ## Filter clusters, default is no filtering.
 ## Values can be specified as glob patterns.
 # clusters_include = []
 # clusters_exclude = []
 ## Filter consumer groups, default is no filtering.
 ## Values can be specified as glob patterns.
 # groups_include = []
 # groups_exclude = []
 ## Filter topics, default is no filtering.
 ## Values can be specified as glob patterns.
 # topics_include = []
 # topics_exclude = []
```

```
## Credentials for basic HTTP authentication.
# username = ""
# password = ""
## Optional SSL config
# ssl_ca = "/etc/telegraf/ca.pem"
# ssl_cert = "/etc/telegraf/cert.pem"
# ssl_key = "/etc/telegraf/key.pem"
# insecure_skip_verify = false
```

Visualization of metrics within the Splunk metrics workspace application:

splunk>enterprise App: Sea	h & Reporting • () Administrator • Messages •	Settings 🔻	Act		Find C
Search Metrics Datasets				> s	earch & Reportir
Data «	🕤 💿 Last 6 hours 🔹 🔩 Split all by 🔹 🖏 Refresh 👻 (Im ago)	:: ≡		Analysis	
burrow X	burrow_group ling by group			burrow_group.la	g
Metrics Transformed and burrow_group or ling or stratus_code transformed and and and and and and and and and an	prop V Vita	e kafka-music		AGGREGATIONS Select one or more display in the chart // Avg M 	Min m 0 × 25 × 10 N me period on the
timestamp burrow_topic.offset				SPLIT BY Split this metric by Split by group	a dimension.
Datasets 0 matches found Alerts 0 matches found					* 5
				FILTERS Include or exclude categories.	metrics from speci
				cluster env group host	Ż

Using meatalog search command to verify data availability:

| mcatalog values(metric_name) values(_dims) where index=* metric_name=burrow_*

2.3 Docker testing templates

Docker compose templates are provided in the following repository:

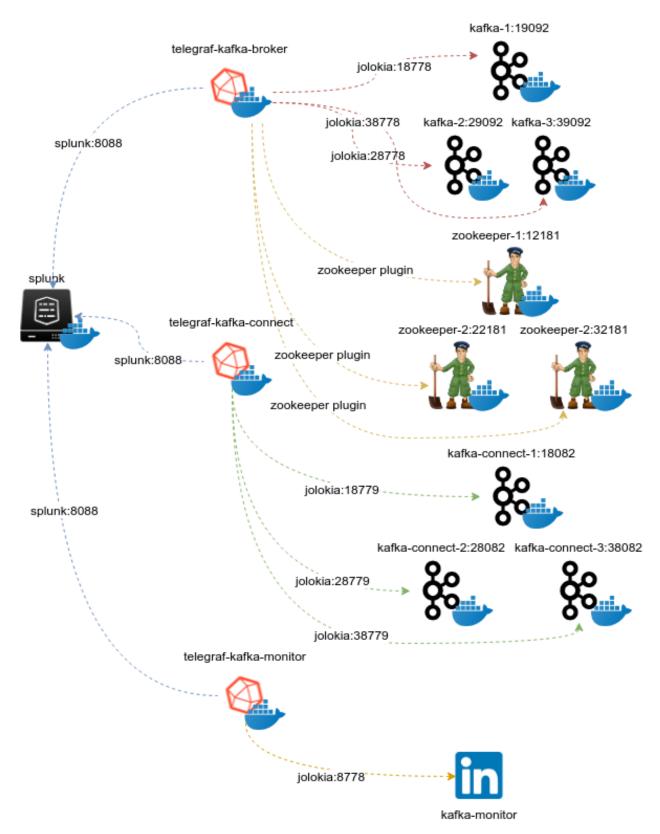
https://github.com/guilhemmarchand/kafka-docker-splunk

Using the docker templates allows you to create a full pre-configured Kafka environment with docker, just in 30 seconds.

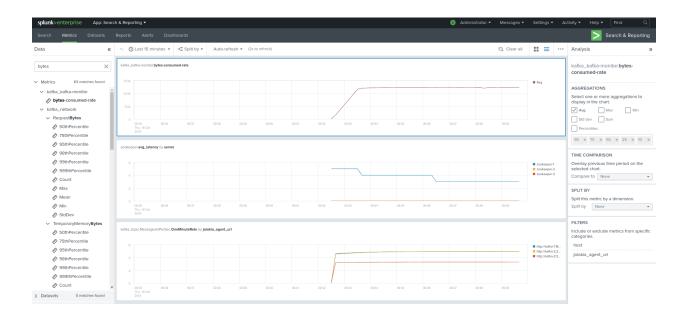
Example:

- Zookeeper cluster (3 nodes)
- Kafka broker cluster (3 nodes)
- Kafka connect cluster (1 node, can be extended up to 3 or more with additional config)
- · Confluent schema-registry
- · Confluent kafka-rest
- · Confluent ksql-server

- Kafka Xinfra SLA monitor container
- Telegraf container polling and sending to your Splunk metric store
- Yahoo Kafka Manager
- Confluent Interceptor console collector
- Kafka Burrow Consumer lag Monitoring

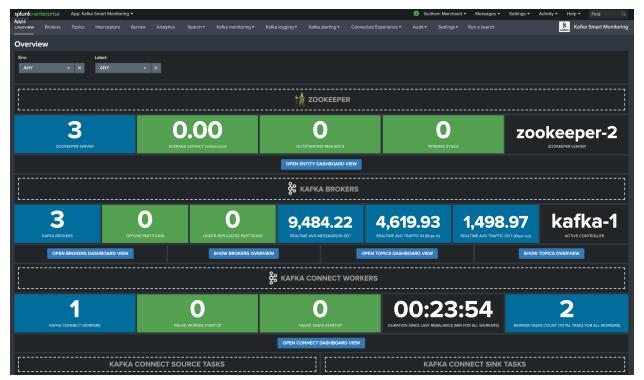


Start the template, have a very short coffee (approx. 30 sec), open Splunk, install the Metrics workspace app and observe the magic happening !



2.4 Splunk dashboards (health views)

2.4.1 Overview (landing page)



The Splunk application home page provides an overview of the Kafka infrastructure:

By default, all Kafka components including Confluent components are shown in the Overview page.

Shall a component be not detected, an informational panel replaces the metric related panel.

A configuration user interface is available in the app menu bar:

• Settings / Management of enable components

Use this user interface to enable or disable any of the components depending on your needs:

Overview Brokens Topics Burrow Metrics Search Kafka monitoring Kafka logging Kafka alerting Settings Run a search		Kafka Smart Monitoring
Kafka Smart Monitoring - Application configuration Use this interface to manage the main configuration items of the application		
Smart Components enablement		
Depending on the products in use, you can enable or disable a component, which will automatically configure the component of the second	ponent to be visible or hidden from the Overview dashboard	
Enable all components Disable all components		
label \$	state range range range	Ø
	enabled	0
	enabled	0
	enabled	0
narka_burrow Confluent_Kafka_Rest	enabled	0
	enabled	0
		-
Confluent_Schema_Registry	enabled	0

2.4.2 Overview Brokers

splunk >en	erprise	App: Kafka Si	mart Monitoring								0	Guilhem Marchand 🖣	Messages	🔹 Settings 🕶	Activity 🔻	Help 🔻 🛛 Fi	
	Brokers				Analytics		Kafka monito	ring 👻 Kafka logging 🔻	Kafka alertin	g 👻 Connected					åg kati	Kafka Sm	art Monitoring
Brokers																	
Env:		Lab	pel:		Kafka b	roker(s):											
$ANY \times$		A	$NY \times$		ANY :	×											
[& KAF	KA BROKE]
					or the selected							Combined Metr					<i>i</i>
		kafka_brok					KBytes out		offline	under-replicated		Rate \$		Mean 4	¢ 1 min ≑	5 min ¢	15 min \$
env \$	label \$			\$ sp	arkline_in \$		÷	sparkline_out \$				Messages in /sec		1029.32	2 1906.41	432.34	314.32
			3253.	95	_		1213.01	^			S	KBytes in /sec		773.72	2 1088.23	245.77	206.78
				36 🧹			5.36		0		9	KBytes out /sec		179.17	7 407.91	92.00	64.46
				37			5.37		0		e	Bytes rejected /	sec	0.06	ə ə.ee	0.00	0.00
												Failed fetch req	uest /sec	0.00	ə 0.00	0.00	0.00
												Failed produce r	equest /sec	0.00	9.00	0.00	0.00
:																	
·																	

The Brokers overview page inspired from Yahoo Kafka manager exposes the Kafka brokers and main metrics:

Broker drilldown page:

	App: Kafka S	mart Monitorir	ig *								6	Guilhem Marchand 🔻	Messages 🕶	Settings 🔻	Activity 🕶 Help 🕯	Find Q.
Brokers Overview Brokers															katka Ka	fka Smart Monitoring
Broker View																
								& Brol	ker: kafka-1							
Stoker entity view																
Heck to brokers																
Summary									Combined metrics							
Data 🕈								Rate 🗢	Rate 🗢			Mea	n ÷	1 min ≑	5 min ≑	15 min ≎
♥ of Topics									Messages in /sec			3261.		39263.17	12251.47	4882.56
# of Partitions									KBytes in /sec			2489.		18883.82	6803.73	2518.96
% of Messages								98.84	KBytes out /sec			561.	89	6161.20	2849.62	837.39
% of Incoming								99.55	Bytes rejected /see				.80	0.00	0.00	0.00
% of Outgoing								98.45	Failed fetch reque:				.80	0.00	0.00	0.00
									Failed produce requ	Jest /sec			.00	0.00	8.00	8.88
								Messages/sec — KE	ytesin/sec — KBytesOut	/sec						
32,000															J	16,000 (Bytes per sec
22:12 2 Wed Oct 21 2020	215	22:18	22:21	22:24	22:27	22:30 22:33	22:36	22:39 ;	2:42 22:45	22:48	22:51 22:5	4 22:57	23.00	23.03	23:06 23:09	23:12
Per Topic Detail (click	on the row t	to view topic	details for	he selected	topic)											
topic ¢		R	eplication 🕈	Total Parti	tions 🕈	Partitions on broker 🕈	Size MB 🕈	Partitions 🕈								
						50	0.019									
					25	25	0.080									
					25 5	25 5										
							0.086									

2.4.3 Overview Topics

The Topics overview page inspired from Yahoo Kafka manager exposes the Kafka topics and main metrics:

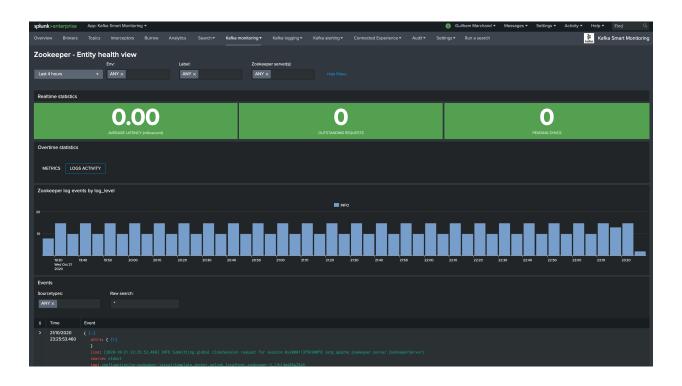
splunk>ent	terprise	App: Kaf	ka Smart Monitorii	ng 🕶							🚯 Gu	ilhem Marchand 🔻 🛛 🕴	Messages 🔻	Settings -	Activity 🔻	Help 🔻 Fin	d Q,
Overview		Topics			Analytics		Kafka monito		Kafka logging v	Kafka alerting 🕶						Kafka Sma	art Monitoring
Topics																	
									& KAF	KA TOPICS							
Topics (cli	ck on the r	ow to viev	v topic details fo	or the selec	ted topic)												
Env:			Label:		Kafk	a topic(s):											
$ANY \times$			$ANY \times$		AN	IY ×											
env \$	label :	≎ top	ic ¢				#	Partitions 🗢	# Brokers ≎	# Replicas ≎	Brokers spread % ≎	# UnderReplica	itedPartitions 4	• •	Size MB ¢	Producer Me	essage/sec ¢
								50	3					0 📀	0.062		0.00
														ə 🥑	0.000		
														ə 🧭	0.018		0.00
														ə 📀	0.007		0.00
													,	ə 🤣	0.000		
														9 📀	0.000		
														ə 🧭	0.251		0.10
														ə 🥝 _	0.001		0.00
														ə 🥝	29903.601		1982.69
													,	ə 🥝	262.054		19.72
														8 🕗	11583.261		
[

Topic drilldown page:

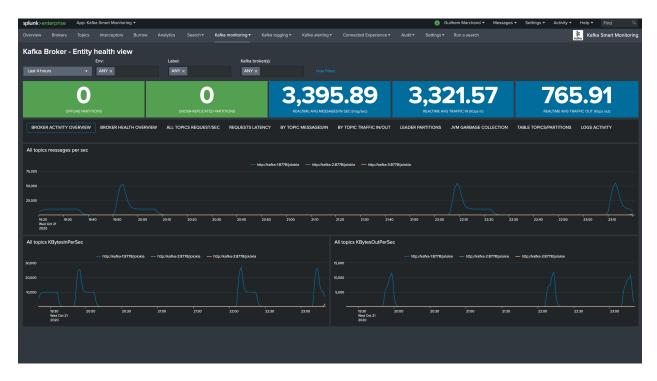
splunk>enterprise App: Kafka Smart Monitoring -		🚯 Gullt	nem Marchand 🔻 Messages 👻 Settings	▼ Activity ▼ Help ▼ Find Q
Overview Brokers Topics Interceptors Burrow Analytics	Search 👻 Kafka monitoring 👻 Kafka loggin	ng ▼ Kafka alerting ▼ Connected Experience ▼		Kafka Smart Monitoring
Topic View				
	٠ يك و	TOPIC: c3test		
L				i
Topic entity view				
Back to topics				
Summary	Operations			
summary ¢	Broker ¢		# of Partitions Partitions	
Numbers of Partitions: 12	kafka-2		3 (3,6,9)	
Total Number of Brokers: 3	kafka-3		4 (1,4,7,18)	
Under-replicated %: 0.00	kafka-1		5 (0,2,5,8,11)	
Size (MB): 32591.192				
Metrics				
Rate sparkline		Mean ¢	1 min \$	5 min ¢ 15 min ¢
Messages in /sec		2427.97	2292.87	2337.09 2483.34
KBytes in /sec		2405.31	2270.79	2314.98 2459.87
Partition Information				
Partition \$	Latest Offset ¢		Under Replicated? \$	
8	33691611	32591.192	false	
1	0	0.000	false	

2.4.4 Zookeeper dashboard view

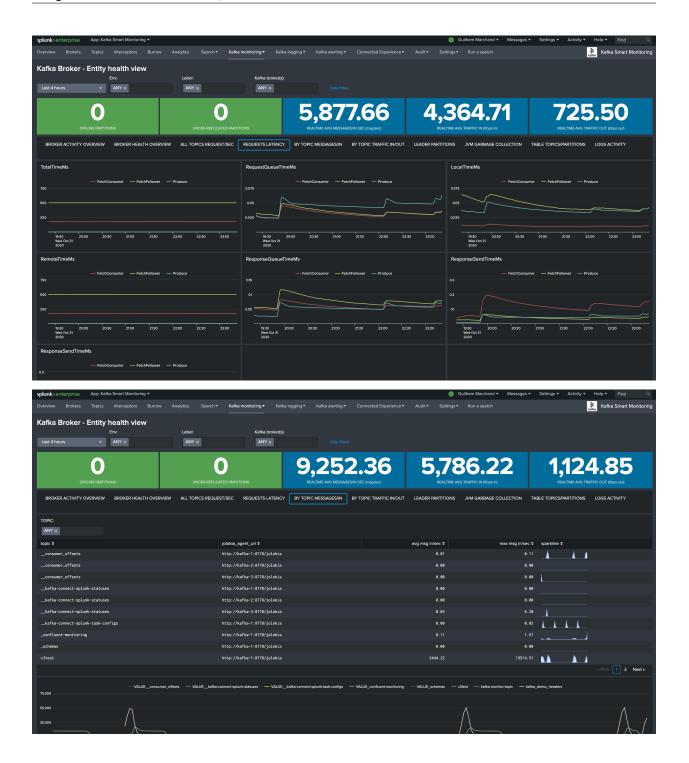
splunk>enterprise App: Kafka Smart Monitoring * Brokers		Guilhem Marchand ▼ Messages ▼ Settings ▼ Activity ▼ Help ▼ Find Q
	monitoring • Kafka logging • Kafka alerting • Connected Experience • Audit • Set	tings * Run a search Kafka Smart Monitoring
Zookeeper - Entity health view	Zookeeper server(s):	
Last 4 hours ANY X ANY X ANY X	ANY X Hide Fitters	
Realtime statistics		
0.00	0	0
AVERAGE LATENCY (milisecond)	OUTSTANDING REQUESTS	PENDING SYNCS
Overtime statistics		
METRICS LOGS ACTIVITY		
Average latency (millisecond)	Outstanding requests	Pending Sync
http://zookeeper-187780jolokia — http://zookeeper-2:87780jolokia — http://zookeeper-387780jolokia	http://zookeeper-18778ijolokia — http://zookeeper-2.8778ijolokia http://zookeeper-38778ijolokia	— http://zookeeper-1.87784jolokia — http://zookeeper-2:87784jolokia — http://zookeeper-3:87784jolokia
— пцрл/докеерег-з.а/ладоока 100	0.3	
		50
50	03	
1930 2000 2030 2100 2130 2200 2230 2300	19:30 20:00 20:30 21:00 21:30 22:00 22:30 23:00	1930 2000 2030 2100 2130 2200 2230 2300
9330 2000 2030 2000 2130 2200 2230 2300 Wed Oct 21 2020	1930 2000 2030 2000 2030 2000 2230 2200 2230 2300 Wed On 21 2020	1950 01:21 Weed 01:21 2020
Number Alive Connections	Packets received	Packets sent
 http://zookeeper-18778/jolokia http://zookeeper-2:8778/jolokia 	 http://zookeeper-1:9778/jolokia http://zookeeper-2:9778/jolokia 	— http://zookeeper-1.8778i/olokia — http://zookeeper-2:8778i/olokia — http://zookeeper-3.8778i/olokia
03	150	
02		100
at	50	50
930 2000 2030 2100 2130 2200 2230 2300	1930 2000 2030 2100 2130 2200 2230	1930 2000 2030 2100 2130 2200 2230
19:30 20:00 20:30 21:00 21:30 22:00 22:30 23:00 Wed Oct 21 20:20	19:30 20:00 20:30 21:00 21:30 22:00 22:30 23:00 Wed Oct 21 20:20	1930 20:00 20:30 21:00 21:30 22:00 22:30 23:00 Wed Oct 21 20:00



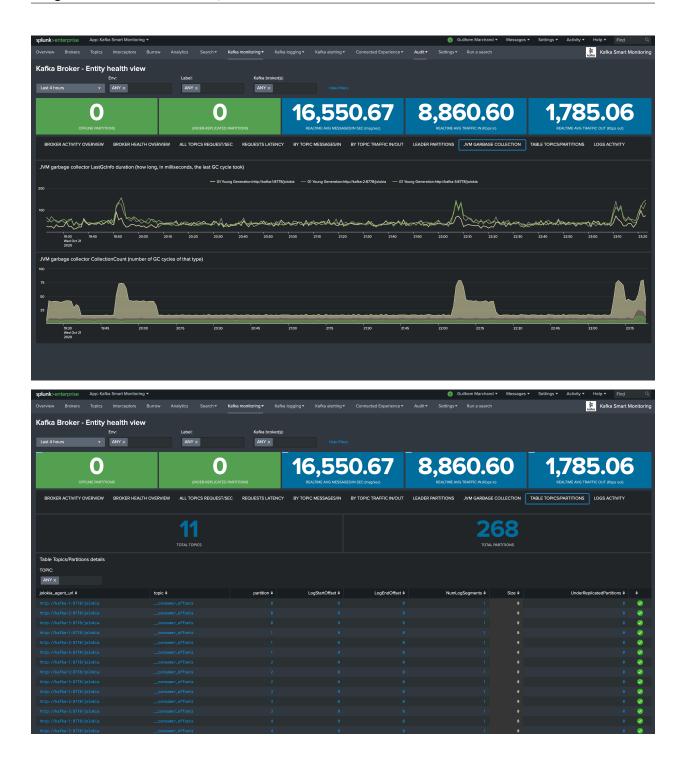
2.4.5 Kafka broker dashboard view



splunk>enterprise Overview Brokers	App: Kafi Topics	Ra Smart Monitoring • Interceptors Burrow		Kafka monitoring v Kafka	logging • Kafka alerting			m Marchand • Messages • un a search	Settings • Activity • Help •	Find Q
Kafka Broker		health view	Label:	Kafka broker(s):						
Last 4 hours	÷	ANY X	ANY X	ANY X						
c		NONS		PARTITIONS	3,86	57.10 AGES/IN SEC (msg/sec)	3,515		531.0	
BROKER ACTIVITY	OVERVIEW	BROKER HEALTH OVER	ALL TOPICS REQUEST/S	EC REQUESTS LATENCY	BY TOPIC MESSAGES/IN	BY TOPIC TRAFFIC IN/OUT	LEADER PARTITIONS JVN	A GARBAGE COLLECTION TAB	LE TOPICS/PARTITIONS LOGS A	стіліту
OfflinePartitions						UnderReplicatedPartitions				
100		http://kafka-1:8778.jolokia	— http://kefka-2:8778/jolokia — h	nttp://kafka-3:8778/jolokia			— http://kafka-1:8778/jolokia	- http://kafka-2:8778/jolokia - ht	tp://kafka-3:8778/jolokia	
50										
19:30 Wed Oct 21 2020	20:00	20:30	21:00 21:30	22.00 22.30	23:00	19:30 20 Wed Oct 21 2020	20:30	21,00 21:30	22:00 22:30	23:00
ISR Shrinking per s	iec					UnderReplicatedPartitions	by topic	jolokia_agent_url ≎	# Partitions ≎ # UnderR	eplicatedPartitions \$
100		— http://kafka-1:8778/jolokia	— http://kafka-2:8778/jolokia — h	nttp://kafka-3:8778/jolokia		consumer_offsets		http://kafka-1:8778/jolokia http://kafka-2:8778/jolokia http://kafka-3:8778/jolokia	50	epircatedPartitions •
50										
19:30 Wed Oct 21 2020	20:00	20:30	21:30 21:30	22:00 22:30	23:00					
						confluent-ksql-confluent _confluent-monitorin	standalone_1command_topic	http://kafka-2:8778/jolokia http://kafka-1:8778/jolokia	1	0
splunk>enterprise	App: Kafi	Ra Smart Monitoring 🕶					 Guilher 	m Marchand 🔻 Messages 🔻	Settings Activity Help	Find Q
Overview Brokers			n Analytics Search v	Kafka monitoring ▼ Kafka 	logging ▼ Kafka alerting	Connected Experience		m Marchand 👻 Messages 👻 un a search		Find Q
	Topics	Interceptors Burrow	Analytics Search • Label:	Kafka monitoring • Kafka Kafka broker(s): ANY ×	logging • Kafka alerting Hide Fil					
Overview Brokers Kafka Broker	Topics - Entity	Interceptors Burrow health view Env: ANY x	Label:	Kafka broker(s): ANY x		57.10		un a search		ka Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours	Topics - Entity - Control	Interceptors Burrow health view Env: ANY x	Label: ANY X UNDER REPUCATED	Kafka broker(s): ANY X	Hede Fi 3,86 Realtime avg mess	ors 577.10 ACESIN SEC (mgusc)	Audre Settingse R 3,519 REALTIME AND TRA	un a search 5.655 FRC N (RDays H)	5 31. 0	ka Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours	Topics - Entity	Interceptors Burrow health view Env: ANY X nows	Labee ANY X UNDER REPLICATED VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY	Hede Fi 3,86 Realtime avg mess	ors 577.10 ACESIN SEC (mgusc)	Aude Settings R 3,554 REALTRE RUG TRAF LEADER PARTITIONS AV	un a soarch 5.655 FIC N HORM M A GARBAGE COLLECTION TAB	E TOPICS/PARTITIONS	ka Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY	Topics - Entity	Interceptors Burrow health view Env: ANY X nows	Labee ANY X UNDER REPLICATED VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X	Hede Fi 3,86 Realtime avg mess	NY 577.10 RESM SEC Implex BY TOPIC TRAFFIC INOUT	Aude Settings R 3,554 REALTRE RUG TRAF LEADER PARTITIONS AV	un a search 5.655 FRC N (RDays H)	E TOPICS/PARTITIONS	ka Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/	Topics - Entity	Interceptors Burrow health view En: ANY X BROKER HEALTH OVER	Labee ANY X UNDER REPLICATED VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY	Hede Fi 3,86 Realtime avg mess	ors 577.100 MCD.Wr SIC program BY TOPIC TRAFFIC NVOLT Fetch requests/sec	Aude Settings R 3,554 REALTRE RUG TRAF LEADER PARTITIONS AV	un a soarch 5.655 FIC N HORM M A GARBAGE COLLECTION TAB	E TOPICS/PARTITIONS	ka Smart Monitoring
Overview Bookers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/ 200	Topics - Entity	Interceptors Burrow health view En: ANY X BROKER HEALTH OVER	Labee ANY X UNDER REPLICATED VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY	Hede Fi 3,86 Realtime avg mess	ns 577.10 RESIN SC propose BY TOPIC TRAFFIC INOUT Fetch requests/sec 10	Aude Settings R 3,554 REALTRE RUG TRAF LEADER PARTITIONS AV	un a soarch 5.655 FIC N HORM M A GARBAGE COLLECTION TAB	E TOPICS/PARTITIONS	ka Smart Monitoring
Overview Bookers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/ 200	Topics - Entity	Interceptors Burrow health view En: ANY X BROKER HEALTH OVER	Labee ANY X UNDER REPLICATED VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY	Hede Fi 3,86 Realtime avg mess	ns 577.10 RESIN SC propose BY TOPIC TRAFFIC INOUT Fetch requests/sec 10	Audt* Settings* R Audt* Settings* R RELINE AND TAK LEADER PARTITIONS AM - rep://a/ke-18778/pooks	un a soarch 5.655 FIC N HORM M A GARBAGE COLLECTION TAB	E TOPICS/PARTITIONS	ka Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/r 200 100 100 100 100 100 100 100 100 100	Topics - Entity FFELNE PARTITI OVERVIEW sec	Interceptor Burrow health view En: Inter En: Inter En: Inter En:	Labe: ANY X UNDER REPLICATE VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY ttp://wifka-3.8778jokekia		NT 577.10 MCSIN SEC (Imples) MCSIN SEC (Imples) Fetch requests/sec 0 0 0 0	Audt* Settings* R Audt* Settings* R RELINE AND TAK IEADER PARTITIONS AM - http://kafka-18778/power	un a search 5.655 16 CH 1050 H - http://wkike-2/8776000000 - 14		ta Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/r 200 0 10 10 10 10 10 10 10 10 10 10 10 10	Topics - Entity FFELNE PARTITI OVERVIEW sec	Interceptor Burrow health view En: Inter En: Inter En: Inter En:	Labe: ANY X UNDER REPLICATE VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY ttp://wifka-3.8778jokekia		NTS	Audt* Settings* R Audt* Settings* R RELINE AND TAK IEADER PARTITIONS AM - http://kafka-18778/power	un a search 5.655 16 CH 1050 H - http://wkike-2/8776000000 - 14		ta Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/r 200 0 10 10 10 10 10 10 10 10 10 10 10 10	Topics - Entity FFELNE PARTITI OVERVIEW sec	Interceptor Burrow health view En: Inter En: Inter En: Inter En:	Labe: ANY X UNDER REPLICATE VIEW ALL TOPICS REQUESTS	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY ttp://wifka-3.8778jokekia		NTS	Audt* Settings* R Audt* Settings* R RELINE AND TAK IEADER PARTITIONS AM - http://kafka-18778/power	un a search 5.655 16 CH 1050 H - http://wkike-2/8776000000 - 14		ta Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/r 200 0 10 10 10 10 10 10 10 10 10 10 10 10	Topics - Entity FFELNE PARTITI OVERVIEW sec	Interceptor Burrow health view En: Inter En: Inter En: Inter En:	Labe: ANY X UNCER REPUZATED VIEW ALL TOPICS REQUESTS 	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY ttp://wifka-3.8778jokekia		NTS	Audt* Settings* R Audt* Settings* R RELINE AND TAK IEADER PARTITIONS AM - http://kafka-18778/power	ил в search 5.655 FIC N (Карина) 4 GARBAGE COLLECTION ТАВ — http://киби-2.87776/рокиа — на 2100 2199		ta Smart Monitoring
Overview Brokers Kafka Broker Last 4 hours BROKER ACTIVITY Produce requests/r 200 0 10 10 10 10 10 10 10 10 10 10 10 10	Topics - Entity FFELNE PARTITI OVERVIEW sec	Interceptor Burrow health view En: Inter En: Inter En: Inter En:	Labe: ANY X UNCER REPUZATED VIEW ALL TOPICS REQUESTS 	Kafka broker(s): ANY X PARTITIONS EC REQUESTS LATENCY ttp://wifka-3.8778jokekia		NTS	Audt* Settings* R Audt* Settings* R RELINE AND TAK IEADER PARTITIONS AM - http://kafka-18778/power	ил в search 5.655 FIC N (Карина) 4 GARBAGE COLLECTION ТАВ — http://киби-2.87776/рокиа — на 2100 2199		ta Smart Monitoring

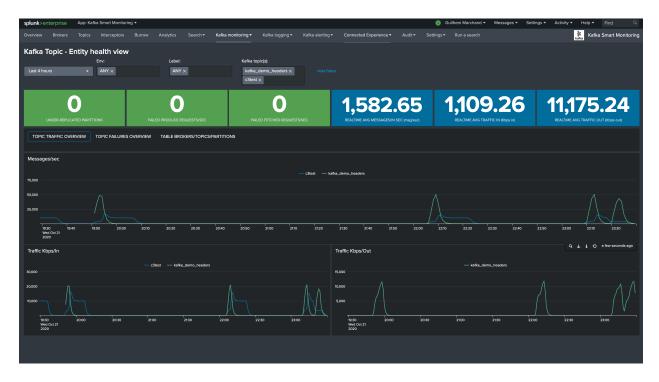


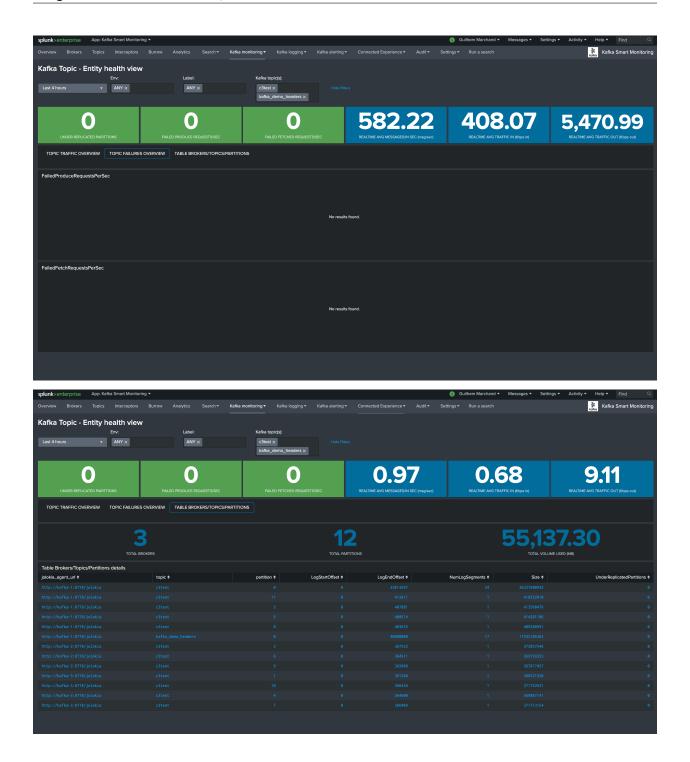
unk>enterprise App: Kafka Smar						
		tics Search ▼ Kafka	nonitoring • Kafka logging			👫 Kafka Smart Mo
afka Broker - Entity heal	lth view					
Env:		Label:	Kafka broker(s):			
ast 4 hours - ANY	'×	ANY X	ANY ×			
0		0		2 500 00	7404 76	4 4 4 0 26
U		U		2,589.09	7,191.76	1,449.26
OFFLINE PARTITIONS		UNDER-REPLICATED PARTITI	ONS			
BROKER ACTIVITY OVERVIEW BRC	DKER HEALTH OVERVIEW	ILL TOPICS REQUEST/SEC	REQUESTS LATENCY BY T	TOPIC MESSAGES/IN BY TOPIC TRAFFIC IN/OUT	LEADER PARTITIONS JVM GARBAGE COLLECTION	ON TABLE TOPICS/PARTITIONS LOGS ACTIVITY
PIC:				TOPIC:		
4Y ×				ANY X		
c≑ onsumer_offsets	jolokia_agent_url ¢	avg Kbps in/sec ¢ kia 0.08	max Kbps in/sec \$ sparklii 0.02		jolokia_agent_url ¢ avg k http://kafka-1:8778/jolokia	Kbps out/sec max Kbps out/sec sparkline 0.00 0.03
nsumer_offsets	http://kafka-2:8778/jold		8.08		http://kafka-2:8778/jolokia	8.00 0.00
nsumer_offsets	http://kafka-3:8778/jolc		6.68		http://kafka-3:8778/jolokia	8.99 9.80
fka-connect-splunk-statuses	http://kafka-1:8778/jolc		6.00			8.00 0.00
fka-connect-splunk-statuses	http://kafka-2:8778/jolo		8.98	kafka-connect-splunk-offse		8.99 0.99
fka-connect-splunk-statuses	http://kafka-3:8778/jolo		1.14	kafka-connect-splunk-offse		8.00 0.00
fka-connect-splunk-task-configs	http://kafka-1:8778/jolc		0.00			8.00 0.00
fluent-monitoring	http://kafka-1:8778/jolc		0.08	kafka-connect-splunk-statu		8.00 0.00
enas	http://kafka-1:8778/jolc	kia 0.09	0.08	kafka-connect-splunk-statu	ses http://kafka-3:8778/jolokia	0.00 0.08
st	http://kafka-1:8778/jolc	kia 2410.43	19301.34	kafka-connect-splunk-task-	configs http://kafka-1:8778/jolokia	8.88 8.89
				1 2 Next »		« Prev 1 2 1
fic Kbps/In				Traffic Kbps/Out		
				15,000		
,				15,000		
						٨
			Λ_{-}	15.000 10.000 5.000		\bigwedge
•		the Courts Kofen		10000		ages * Settings * Activity * Help * Find
o ■ Mc⊃enterprise App: KaRus Smar New Brokers Topics Inter		tics Search* Kafka	monitoring • Kafka logging:	10000	Guilhem Marchand • Mess Audit • Settings • Run a search	
o ■ Ns-enterprise App: Kafka Smar New Brokers Topics Inter	rceptors Burrow Analy Ith view	tics Search* <mark>Kafka</mark> Labet	nonitoring • Kafka logging : Kafka broker(s);	10000		
App: Kafka Smar App: Kafka Smar A	rceptors Burrow Analy			10000		ages * Settings * Activity * Help * Find States Kafka Smart Mc
k-enterprise App: Kafka Sinar New Brokers Topics Inter Ka Broker - Entity heal En: Ka hours Arv	rceptors Burrow Analy	Label: ANY X	Kafka broker(s): ANY X	Kafka alerting Connected Experience Hose Filters		🧩 Kafka Smart Mc
k:enterprise App: KaRia Smar ew Brokers Topics Inter ka Broker - Entity heal Enc	rceptors Burrow Analy	Label:	Kafka broker(s): ANY X	Kafka alerting Connected Experience Hose Filters		🧩 Kafka Smart Mc
k-enterprise App-Kafka Smar ew Brokers Topics Inter ka Broker - Entity heal en: 4 hours ANY	rceptors Burrow Analy	Label: ANY X	Kafka broker(s): ANY x	Kafka alerting Connected Experience Hose Filters		🧩 Kafka Smart Mc
k-enterprise App Kolko Smar www.Brokers Topics Inter ta Broker - Entity heal Annu Karting Karting Annu Karting Karting Annu Karting Karting Annu Karting Karting Annu Karting Karting Annu Karting Karting Annu Karting Kar	rceptors Burrow Analy Ith view		Kafka broker(s): ANY ×	 Kafka alerting* Connected Experience* Hole Fitter Fitter Source Establishing 	Audi* Settings* Run search 8,2122.688 REALTIME AND TRAVIEC NI (Robers ref	Kofka Smart Mc
k-enterprise App: Kafka Smar w Broker Topics Inter ka Broker - Entity heal Env: 4 hours Any OPELNE MATTICAS	rceptors Burrow Analy Ith view		Kafka broker(s): ANY ×	Kafka alerting Connected Experience Hose Filters	Audi* Settings* Run search 8,2122.688 REALTIME AND TRAVIEC NI (Robers ref	кана Smart M
k-enterprise App Kefke Smar ew Brokers Topics Inter ta Broker - Entity heal Env: 4 hours Env: ANY OFFLINE NATITIONS	rceptors Burrow Analy Ith view		Kafka broker(s): ANY ×	 Kafka alerting* Connected Experience* Hole Fitter Fitter Source Establishing 	Audi* Settings* Run search 8,2122.688 REALTIME AND TRAVIEC NI (Robers ref	Kofka Smart Mc
k-enterprise App Kefke Smar ew Brokers Topics Inter ta Broker - Entity heal Env: 4 hours Env: ANY OFFLINE NATITIONS	rceptors Burrow Analy Ith view		Katka broker(s): ANY X ANY X A	 value and management <	Audr * Settings * Run search 8,212,688 Relative and Trader on Rose at LEADER PARTITIONS	Kofka Smart Mc
k-enterprise App Kefke Smar ew Brokers Topics Inter ta Broker - Entity heal Env: 4 hours Env: ANY OFFLINE NATITIONS	rceptors Burrow Analy Ith view		Katka broker(s): ANY X ANY X A	 Kafka alerting* Connected Experience* Hole Fitter Fitter Source Establishing 	Audr * Settings * Run search 8,212,688 Relative and Trader on Rose at LEADER PARTITIONS	Kofka Smart Mc
k-enterprise App Kefke Smar ew Brokers Topics Inter ta Broker - Entity heal Env: 4 hours Env: ANY OFFLINE NATITIONS	rceptors Burrow Analy Ith view		Katka broker(s): ANY X ANY X A	 value and management <	Audr * Settings * Run search 8,212,688 Relative and Trader on Rose at LEADER PARTITIONS	Karke Smart Md 1,655.700 REALTME AND TRAFFC OUT (RODE OND
ktenterprise App Kafka Smar ew Brokers Topics Inter ca Broker - Entity heal Er: Anours Any Openee Partmone Corenee Partmone	rceptors Burrow Analy Ith view		Katka broker(s): ANY X ANY X A	 value and management <	Audr * Settings * Run search 8,212,688 Relative and Trader on Rose at LEADER PARTITIONS	Kofka Smart Mc
k: enterprise App Kafka Smar ew Brokers Topics Inter ka Broker - Entity heal Er: A hours Any orelae partitions	rceptors Burrow Analy Ith view		Katka broker(s): ANY X ANY X A	 value and management <	Audr * Settings * Run search 8,212,688 Relative and Tradier on Rose at LEADER PARTITIONS	Kofka Smart Mc
ksenterprise App KaRa Smar ew Bokers Topics Inter ca Broker - Entity heal Erv: Ahours Armonic Any Operation American construct overview Bro to leader %.	rceptors Burrow Analy Ith view	Labet: ANY X UNDER REPUCATED PARTITI	Katka broker(s): ANY X ANY X A	 value and management <	Audt* Settings* Run search Restructer and Tradier in Roya ed LEADER PARTITIONS Mod GARBAGE COLLECTIC Reporter	Karke Smart Md 1,655.700 REALTME AND TRAFFC OUT (RODE OND
ksenterprise App KaRa Smar ew Bokers Topics Inter ca Broker - Entity heal Er: Anur Operuse harmous Noker Activity overview Bro D leader %	reeptors Burrow Analy Ith view X X X X X X X X X X X X X X X X X X	Labet: ANY X UNDER REPUCATED PARTITI	Katka broker(s): ANY X NRS REQUESTS LATENCY BY T 	 Kafka aerting * Connected Experience * Kafka aerting * Connected Experience * Hote Fare Kafka aerting * Connected Experience * Hote Fare Kafka aerting * Optic Fare Optic Fare Optic Kafka aerting * 	Audt* Settings* Run search Restructer and Tradier in Roya ed LEADER PARTITIONS Mod GARBAGE COLLECTIC Reporter	Kafra Smart Ko
k-enterprise App: Kaßa Smar enterprise Topics Inter ka Broker - Entity heal enterprise App: Kaßa Smar ka Broker - Entity heal enterprise App: Kaßa Smar enter ka Broker - Entity enterprise App: Kaßa Smar enter enterprise App: Kaßa Smar enterprise App: App: Kaßa Smar enterprise App: App: App: App: App: App: App: App	reeptors Burrow Analy Ith view X X X X X X X X X X X X X X X X X X	Labet: ANY X UNDER REPUCATED PARTITI	Katka broker(s): ANY X NRS REQUESTS LATENCY BY T 	 Kafka aerting * Connected Experience * Kafka aerting * Connected Experience * Hote Fare Kafka aerting * Connected Experience * Hote Fare Kafka aerting * Optic Fare Optic Fare Optic Kafka aerting * 	Audt* Settings* Run search Restructer and Tradier in Roya ed LEADER PARTITIONS Mod GARBAGE COLLECTIC Reporter	Kafra Smart Ko
k-enterprise App: Kaßa Smar wei Broker - Entity Heal Anours Filter Anours Filter Corrue partmones Roker Activity OVERVIEW BRC o leader % 10-10-20-20-20-20-20-20-20-20-20-20-20-20-20	reeptors Burrow Analy Ith view X X X X X X X X X X X X X X X X X X		Kafka broker(p): ANY × ANS REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000	1000 1000 1000 </td <td>Audt* Settings* Run search Restructer and Tradier in Roya ed LEADER PARTITIONS Mod GARBAGE COLLECTIC Reporter</td> <td>Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230</td>	Audt* Settings* Run search Restructer and Tradier in Roya ed LEADER PARTITIONS Mod GARBAGE COLLECTIC Reporter	Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230
k-enterprise App: Kaßa Smar wei Broker - Entity Heal Anours Filter Anours Filter Corrue partmones Roker Activity OVERVIEW BRC o leader % 10-10-20-20-20-20-20-20-20-20-20-20-20-20-20	Burow Anay Ith view		Kafka broker(p): ANY × ANS REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000	1000 1000 1000 1000	Audit* Settings* Run s search B3,2212.688 Reactive aver Traverer Nir Kope viz REACTIVE AVE TRAVER IN INCOME JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION 2150 2200 2230 2	Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230
k-enterprise App: Kaßa Smar wei Broker - Entity Heal Anours Filter Anours Filter Corrue partmones Roker Activity OVERVIEW BRC o leader % 10-10-20-20-20-20-20-20-20-20-20-20-20-20-20	Burow Anay Ith view		Kafka broker(p): ANY × ANS REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000	1000 1000 1000 </td <td>Audit* Settings* Run s search B3,2212.688 Reactive aver Traverer Nir Kope viz REACTIVE AVE TRAVER IN INCOME JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION 2150 2200 2230 2</td> <td>Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230</td>	Audit* Settings* Run s search B3,2212.688 Reactive aver Traverer Nir Kope viz REACTIVE AVE TRAVER IN INCOME JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION 2150 2200 2230 2	Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230
Ac-enterprise App: Kalka Smar inve Broker - Entity heal Ka Broker - Entity heal Enter Corrige Control Control Corrige Control Corrige Control Corrige Control Corrige Control Con	Burow Anay Ith view		Kafka broker(p): ANY × ANS REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000	1000 1000 1000 1000	Audit* Settings* Run s search B3,2212.688 Reactive aver Traverer Nir Kope viz REACTIVE AVE TRAVER IN INCOME JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION 2150 2200 2230 2	Karka Smart K 1,6555.700 RELINE AND TRAFFIC OUT ROOP OUT N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 250 230
	Burow Anay Ith view		Kafka broker(p): ANY × ANS × REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000 ke3.8778jotobia -	• Kafka aerting • Connected Expensesce • • Kafka aerting • Expensesce • • Tatio Tatio	Audit* Settings* Run search B3,2212.688 Run search RATINE AVE TRAFFE C N ROPE PE ILEDER PARTITIONS JVM GARRAGE COLLECTOR B000068 220 220 2 1 100// Multi- 1877800000 — M2// Multi- 2877800000 — M2// Multi- 2877800000	Katka Smart Ki Line State Line State N Table TOPICS/PARTITIONS LOGS ACTIVITY
	Burow Anay Ith view		Kafka broker(p): ANY × ANS REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000	• Kafka aerting • Connected Expensesce • • Kafka aerting • Expensesce • • Tatio Tatio	Audit* Settings* Run s search B3,2212.688 Reactive aver Traverer Nir Kope viz REACTIVE AVE TRAVER IN INCOME JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION REQUIRE JAMI GARBAGE COLLECTION 2150 2200 2230 2	Kafka Smart K Landschutz Landschutz N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 2250 2300 2310
	Burow Anay Ith view		Kafka broker(p): ANY × ANS × REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000 ke3.8778jotobia -	• Kafka aerting.• Connected Expensesce* • Kafka aerting.• Expensesce* • Kafka aerting.• Expensesce* • Top:/ks/ke-287785pakka — http:/ks/ke-3877 • 12.22 21.30 24.40 • 12.22 21.30 24.40 • 12.22 21.30 24.40	Audit* Settings* Run search B3,2212.688 Run search RATINE AVE TRAFFE C N ROPE PE ILEDER PARTITIONS JVM GARRAGE COLLECTOR B000068 220 220 2 1 100// Multi- 1877800000 — M2// Multi- 2877800000 — M2// Multi- 2877800000	Kafka Smart K Landschutz Landschutz N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 2250 2300 2310
	Burow Anay Ith view		Kafka broker(p): ANY × ANS × REQUESTS LATENCY BY T - http://kafka-1877619 D44 2050 2000 ke3.8778jotobia -	• Kafka aerting • Connected Expensesce • • Kafka aerting • Expensesce • • Tatio Tatio	Audit* Settings* Run search B3,2212.688 Run search RATINE AVE TRAFFE C N ROPE PE ILEDER PARTITIONS JVM GARRAGE COLLECTOR B000068 220 220 2 1 100// Multi- 1877800000 — M2// Multi- 2877800000 — M2// Multi- 2877800000	Kafka Smart K Landschutz Landschutz N TABLE TOPICS/PARTITIONS LOGS ACTIVITY 230 2240 2250 2300 2310

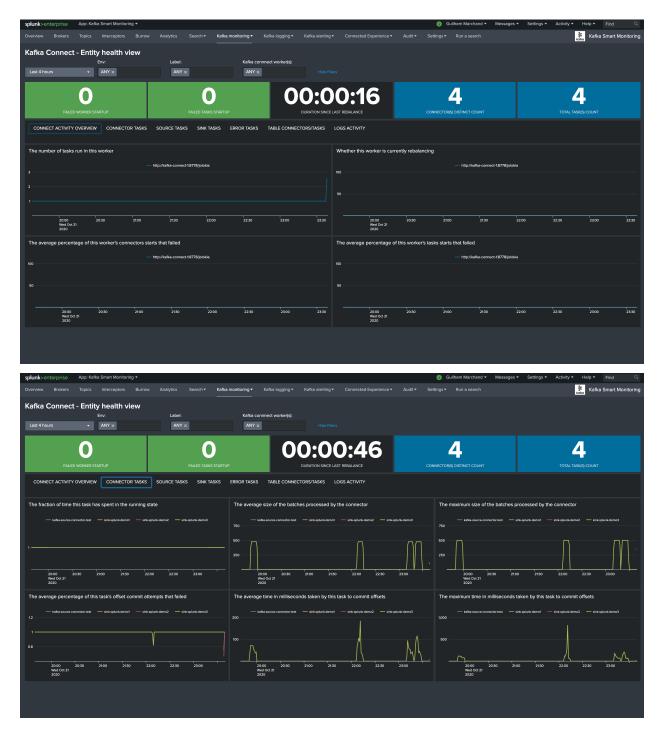


splun	enterprise	App: Kafk	a Smart Monito	oring v											🚯 Guil	lhem Marchand	 Messages 	 Settings 	 Activity 	▪ Help ▪	Find Q
Overvie							Kafka n	nonitoring •												💏 Kafk	a Smart Monitoring
Kafk	a Broker	- Entity	health vi	ew																	
			Env:		Lab	el:		Kafka k	oroker(s):												
Last	4 hours	•	$ANY \times$		At	łY×		ANY	×												
						UNDER-REPLICA				17,7 realtime av	82 messages/in		7			9.4			,9		
BR	OKER ACTIVITY	OVERVIEW	BROKER HE	ALTH OVERVI	EW ALL	TOPICS REQUE	ST/SEC	REQUESTS L	ATENCY E	BY TOPIC MESSA	ges/in by	Y TOPIC TRAFFI	C IN/OUT	LEADER PAR	TITIONS .	JVM GARBAGE	COLLECTION	TABLE TOPIC	CS/PARTITION	S LOGS A	СТІVІТҮ
Kafk	a broker log ev	ents by log	_level																		
										DEBU	g 📕 INFO	TRACE									
150																					
100																					
50																					
		,						·													ℯ┻╻┫┍╸╽
w	20 19:30 ed Oct 21 20	19:40	19:50	20:00	20:10	20:20	20:30	20:40	20.50 21	100 21:10		2130	2140	2150	22:00	22:10 22:2	0 22:30	22:40	22:50	23:00	23:10 23:20
Ever	its																				
Sour	etypes:		Raw search:																		
AN	Υ×																				
i	Time	Event																			
>	21/10/2020 23:24:14.053	([-] attrs: {																			
		host = kafka		http://docker_k	ogs source	type = dockerd	kafka:brokei														
>	21/10/2020 23:24:14.053	([-] attrs: (
		}																			

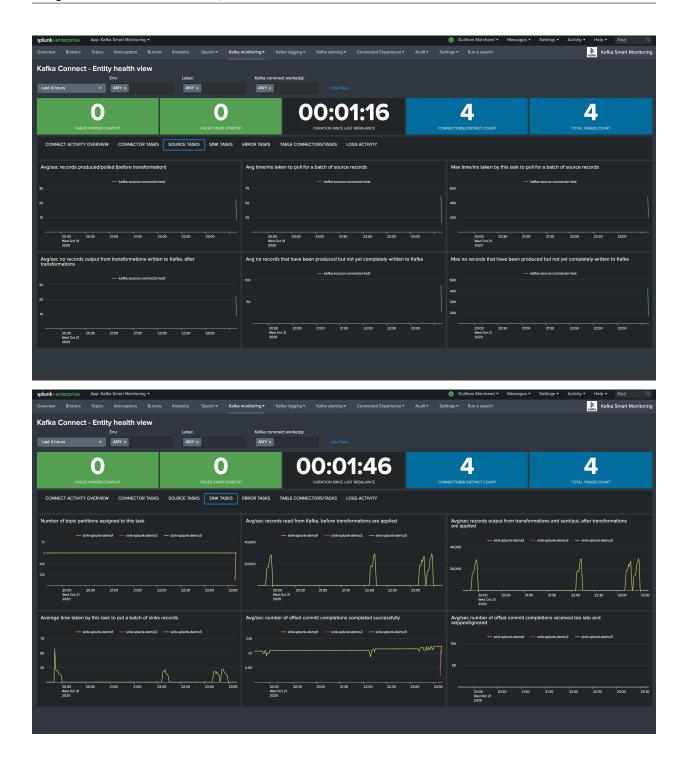
2.4.6 Kafka topic dashboard view

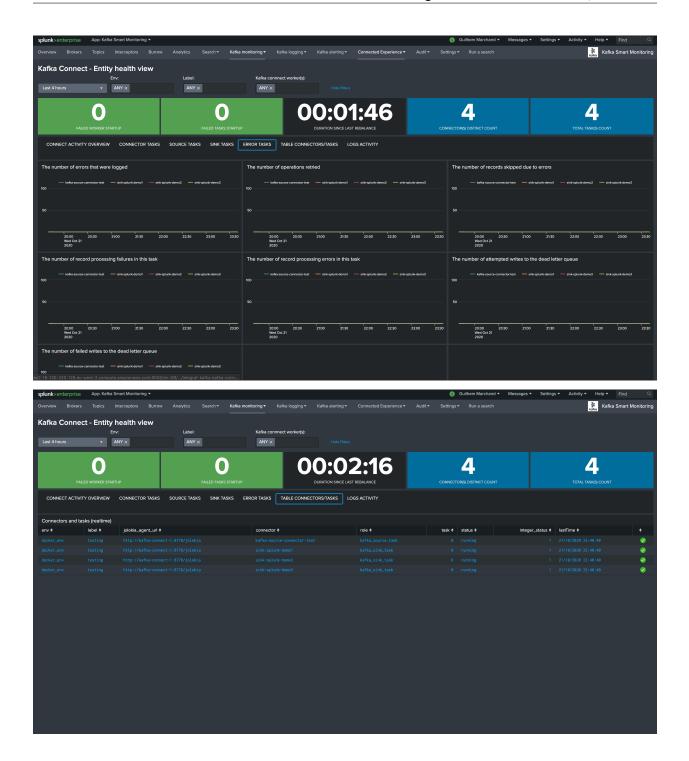


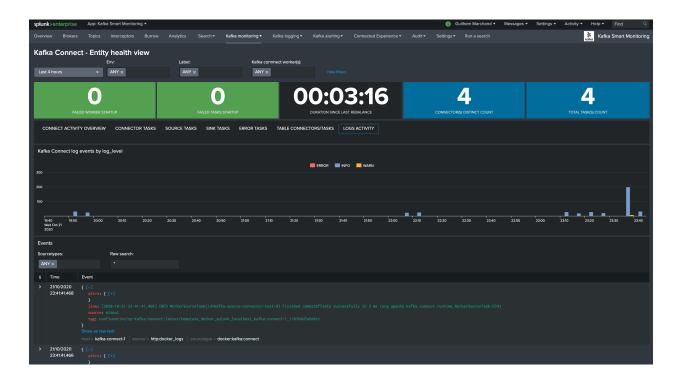




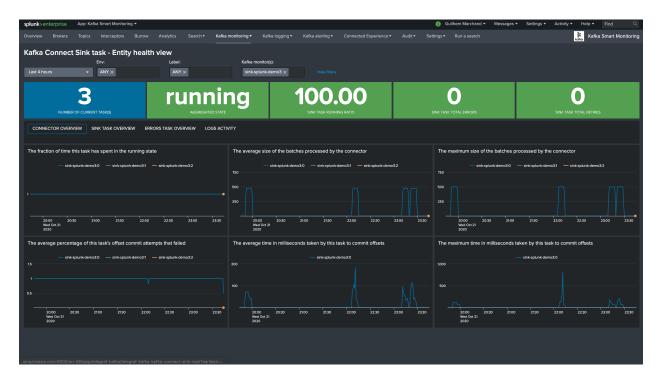
2.4.7 Kafka connect dashboard view

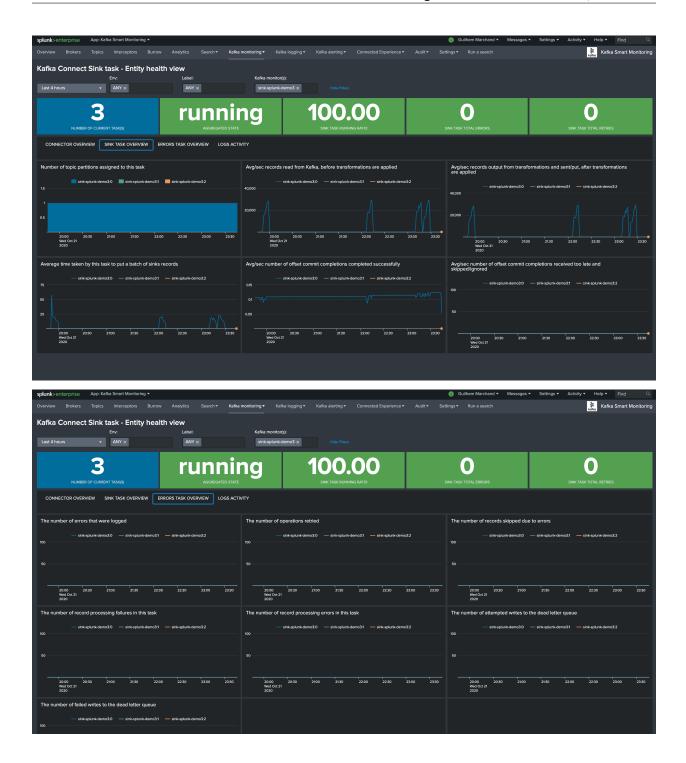






2.4.8 Kafka connect sink task dashboard view





splunk>enterprise App: Kafk	a Smart Monitoring 🕶				🚯 Guilhem Marchand 👻 Messages	Settings Activity Help Find				
Overview Brokers Topics Interceptors Burrow Analytics Search* Kalka monitoring* Kalka logging* Kalka eletting* Connected Experience* Audit* Settings* Run a search										
Kafka Connect Sink task - Entity health view										
Last 4 hours 👻	ANY X	ANY X	sink-splunk-demo3 \times							
	r TASK(S)	runnin Aggregated state	ng 1	00.00 SINK TASK RUNNING RATIO	SINK TASK TOTAL ERRORS	O SINK TASK TOTAL RETRIES				
CONNECTOR OVERVIEW SI	NK TASK OVERVIEW ERRORS	S TASK OVERVIEW LOGS ACTIVIT								
Kafka Connect log events by lo	g_level									
40			•	ERROR 📕 INFO 🔜 WARN						
40						_				
20						<u>lılı</u> .				
19:50 20:00 2 Wed Oct 21 2020	0:10 20:20 20:30	20:40 20:50 21:00	2110 2120 2130	21:40 21:50 22:00 23	210 22:20 22:30 22:40 22:50 2	300 2310 2320 2330 2340				
Events										
Raw search:										
i Time Event										
source: tag: cor) Show as ray host = kafka		WorkerSinkTask(id=sink-splunk-de atest/template_docker_splunk_loca er_logs source = stdout { sourcety								
> 21/10/2020 { [-] 23:43:52.771 attrs: { }	([+]									

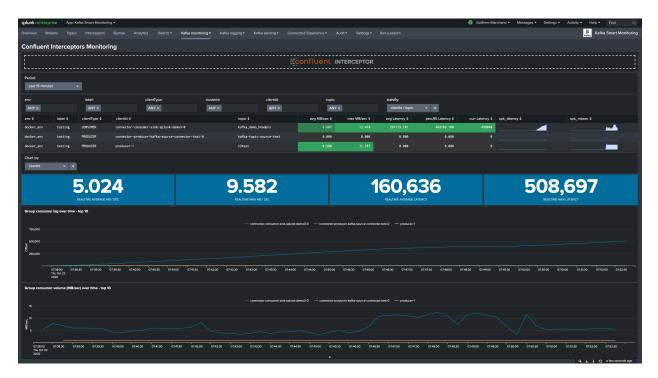
2.4.9 Kafka connect source task dashboard view

splunk>enterprise App: Kafka Smart Monitoring *		6 Guilhem Marchand ▼ Messages ▼ Settings ▼ Activity ▼ Help ▼ Find Q					
Overview Brokers Topics Interceptors Burrow Analytics Search • Kafka	monitoring Kafka logging Kafka alerting Connected Experience Audit S	sttings • Run a search Kafka Smart Monitoring					
Kafka Connector Source task - Entity health view Env: Labet: Labet: ANY x ANY x ANY x	Kafka monitor(s) kafka source-connector X Hude Filters						
Austree OF CURRENT TASKEP CONNECTOR OVERVIEW SOURCE TASK OVERVIEW ERRORS TASK OVERVIEW LOGS.		O O SINK TASK TOTAL ERRORS SINK TASK TOTAL RETIRES					
CONNECTOR OVERVIEW SOURCE TASK OVERVIEW ENRORS TASK OVERVIEW LOGS							
The fraction of time this task has spent in the running state	The average size of the batches processed by the connector	The maximum size of the batches processed by the connector					
- kafka-source-connector-test.0	- kafka-source-connector-test0	kafka-source-connector-test.0					
22.50 23.00 23.10 23.20 23.30 23.40 Wed out 21 2070	22:50 23:00 23:10 23:20 23:30 23:40 Wed Oct 21 20:20	2250 2330 2330 2330 2330 2330 2330 2340 Web 05121 2010					
The average percentage of this task's offset commit attempts that failed	The average time in milliseconds taken by this task to commit offsets	The maximum time in milliseconds taken by this task to commit offsets					
- kafka-source-connector-test.0	- kafka-source-connector-test:0	kafka-source-connector-test.0					
1 09 08 	5	20 10 					
wadda21 2020	WiciGo 21	wa/da 27 2020					

splunk>enterprise App: Kafka Smart Monitoring •			👔 Guilhem Marchand 👻 Messag	
				Kafka Smart Monitoring
Kafka Connector Source task - Entity he	alth view Label: Kafka monitu	or(s):		
Last 60 minutes + ANY ×	ANY × kafka-sour	ce-connector X Hide Fitters		
		400.00		
1	running	100.00	0	0
NUMBER OF CURRENT TASK(S)	AGGREGATED STATE	SINK TASK RUNNING RATIO	SINK TASK TOTAL ERRORS	SINK TASK TOTAL RETRIES
CONNECTOR OVERVIEW SOURCE TASK OVERVIEW ER	RORS TASK OVERVIEW LOGS ACTIVITY			
Avg/sec records produced/polled (before transformation)	Avg time/ms ta	ken to poll for a batch of source records	Max time/ms taken by this task t	o poll for a batch of source records
- kafka-source-connector-test.0		kafka-source-connector-test:0		kafka-source-connector-test.0
20				
10				
22:50 23:00 23:10 23:20 Wed Oct 21 20:20	2330 2340 2250 Wed Oct 21 2020	23:00 23:10 23:20 23:30	23:40 22:50 23:00 Wed Oct 21 2020	23:10 23:20 23:30 23:40
		s that have been produced but not yet completely written		produced but not yet completely written to Kafka
Avg/sec no records output from transformations written to H transformations		kafka-source-connector-test:0		kafka-source-connector-test.0
kafka-source-connector-test:0				
20			500	
10				
22:50 23:00 23:10 23:20 Wed Oct 21 20:20	22:50 23:30 23:40 20:20 20:20	23:00 23:10 23:20 23:30 1	23:40 22:50 23:00 Wed Oct 21 2020	2310 2320 2330 2340
splunk>enterprise App: Kafka Smart Monitoring •	Analvtics Search▼ Kafka monitorino▼ K	afka logging ▼ Kafka alerting ▼ Connected Experience ▼		es * Settings * Activity * Help * Find Q
Overview Brokers Topics Interceptors Burrow		afka logging • Kafka alerting • Connected Experience •		as * Settings * Activity * Help * Find Q & Kafka Smart Monitoring
Overview Brokers Topics Interceptors Burrow Kafka Connector Source task - Entity he Env.	alth view Label: Kafka monite	orfs):		
Overview Brokers Topics Interceptors Burrow	alth view Label: Kafka monite			
Overview Brokers Topics Interceptors Burrow Kafka Connector Source task - Entity he Env.	alth view Labet Kafka monito ANY X kafka-sour	or(s): ce-connector	Audt + Settings + Run a search	Kafka Smart Monitoring
Overview Brokers Topics Interceptors Burrow Kafka Connector Source task - Entity he Env Last 60 minutes ANY ×	alth view Label: Kafka monite	orfs):	Audt+ Settings+ Run a search	Kafka Smart Monitoring
Overview Brokers Topics Interceptors Burrow Kafka Connector Source task - Entity he Env.	alth view Labe: Kafka none MYX kafka-sou running Addreamed state	or(s): ce-connector	Audt + Settings + Run a search	Kafka Smart Monitoring
Overview Brokers Topics Interception Burrow Kafka Connector Source task - Entity he Env: Env: Last 60 minutes ANY × Number of Clurrent Tasks Number of Clurrent Tasks Convector overview Source task overview	alth view Labe: Kafka nonit ANY X kafka sour Running Addrease State Rors Task overview Logs Activity	ordy: ce-connector x Hear Flams 1000.000 Saw: Track Ruiveling BATTO	Audt • Settings • Run a search	Kafka Smart Monitoring
Overview Brokers Topics Interception Burrow Last 60 minutes Env Env Env Last 60 minutes ANY × Interception Interception NUMBER OF CUEREENT TAKES CONNECTOR OVERVIEW SOURCE TASK OVERVIEW Env The number of errors that were logged	alth view Labe: Kafka nonit ANY X kafka sour Running Addrease State Rors Task overview Logs Activity	ord: ce-connectorum X trais filter: 1000.000 serv: Tack Ruseines BATTO Poperations retried	Audt+ Settings+ Run a search	Kafka Smart Monitoring
Overview Brokers Topics Interception Burrow Kafka Connector Source task - Entity he Env: Env: Last 60 minutes ANY × Number of Clurrent Tasks Number of Clurrent Tasks Convector overview Source task overview	alth view Labe: Kafka nonit ANY X kafka sour Running Addrease State Rors Task overview Logs Activity	ordy: ce-connector x Hear Flams 1000.000 Saw: Track Ruiveling BATTO	Audt • Settings • Run a search	Kafka Smart Monitoring
Yourwan Bokes Yopics Burecoptor Burecoptor Kafka Connector Source task - Entity he Enc Last 60 minutes ANY X Number of errors that were logged	alth view Labe: Kafka nonik ANY × Kafka nonik Franciska view Roman State Nones TASK overview Loos Activity The number of	ord: ce-connectorum X trais filter: 1000.000 serv: Tack Ruseines BATTO Poperations retried	Audt * Settings * Run a search	Kafka Smart Monitoring
Yourwan Bokes Yopics Burecoptor Burecoptor Kafka Connector Source task - Entity he Enc Last 60 minutes ANY X Number of errors that were logged	alth view Labe: Kafka nonik ANY × Kafka nonik Franciska view Roman State Nones TASK overview Loos Activity The number of	ord: ce-connectorum X trais filter: 1000.000 serv: Tack Ruseines BATTO Poperations retried	Audt * Settings * Run a search	Kafka Smart Monitoring
Yourwan Bokes Yopics Burecoptor Burecoptor Kafka Connector Source task - Entity he Enc Last 60 minutes ANY X Number of errors that were logged	alth view Labe: Kafka nonik ANY × Kafka nonik Franciska view Roman State Nones TASK overview Loos Activity The number of	ord: ce-connectorum X trais filter: 1000.000 serv: Tack Ruseines BATTO Poperations retried	Audt * Settings * Run a search	Kafka Smart Monitoring
Overview Bokers Topics Interception Burrow Env: Env: Env: Env: Env: Last 60 minutes ANY × Interception Env: NUMERER OF CLUERENT TAGE(S) Env: Env: Env: CONNECTOR OVERVIEW SOURCE TASK OVERVIEW Env: The number of errors that were logged Interception Env:	alth view Libei: Kafka nonik ANY × Kafka nonik safka sozi safka sozi Ladiesozi Ladiesozi Lods ACTWITY The number of 5230 2340 505 10 2340 20 2350 20 2550	ord: ce.connectorx Hear Filters 1000.000 Siter: Tack Ruseinies Barto reperations retried = kafka source connector frast.	Audit* Settings* Run a search	Exercises connector tests 0 2310 2320 2320 2320
Overview Bokers Topics Burrow Connector Source task - Entity he Env Last 60 minutes ANY X NUMBER OF CLIEBENT TASKS CONNECTOR OVERVIEW Env CONNECTOR OVERVIEW CONNECTOR OVERVIEW Source Task overview The number of errors that were logged 00 00	alth view Libei: Kafka nonik ANY × Kafka nonik safka sozi safka sozi Ladiesozi Ladiesozi Lods ACTWITY The number of 5230 2340 505 10 2340 20 2350 20 2550	srd: ce-connectorx Her Films 1000.000 Sinc: Tack Rubeine BATC Poperations retried 2330 230 2320 2320 2320	Audit* Settings* Run a search	Exercises connector tests 0 2310 2320 2320 2320
Overview Bokes Topics Burrow Env Env Env Env ANY x Image: Communities ANY x Connector Overview Source Task overview The number of errors that were logged The number of errors that were logged Image: Communities 2100 2200 Image: Communities 2200 2200 The number of record processing failures in this task.	alth view Labe: Kafka novnk kafka sounk kafka sounk	seconectorx Hee Files the Files the Files the Files seconectorx Hee Files the Files trace runnels are seconector texts 23.00 23.00 23.00 23.00 record processing errors in this task	Audt* Settings* Run a search	Katika Smart Monitoring
Overview Bokes Topics Burrow Env Env Last 60 minutes Instance of colspan="2">Connector Source task - Entity here Instance of colspan="2">Instance of colspan="2" Instance of record processing follows in this task Instance of record processing follows in this task Instance of record processing follows in this task	alth view Labe: Kofka nonik ANY × Kofka nonik Subcassor Subcas	seconectorx Hee Files the Files the Files the Files seconectorx Hee Files the Files trace runnels are seconector texts 23.00 23.00 23.00 23.00 record processing errors in this task	Audit* Settings* Run a search Image: settings in the search Image: setting	Katika Smart Monitoring
Overview Bokes Topics Burrow Env Env Last 60 minutes Instance of colspan="2">Connector Source task - Entity here Instance of colspan="2">Instance of colspan="2" Instance of record processing follows in this task Instance of record processing follows in this task Instance of record processing follows in this task	alth view Labe: Kofka nonik ANY × Kofka nonik Subcassor Subcas	seconectorx Hee Files the Files the Files the Files seconectorx Hee Files the Files trace runnels are seconector texts 23.00 23.00 23.00 23.00 record processing errors in this task	Audit* Settings* Run a search Image: settings in the search Image: settings in the search Image: settings in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: search Image: search Image: search Image: search Imag	Katika Smart Monitoring
Overview Bokers Topics Burrow Env Env Last 60 minutes Instance of colspan="2">Convector Source task - Entity her Instance of colspan="2">Instance of colspan="2" Instance of colspan="2" Instance of errors that were logged Instance of ercord processing failures in this task Instance of ercord processing failures in this task	alth view Labe: Kafka nonik ANY × Kafka nonik Extressour COUNTRY COUNT	srd: reconnectorx Her fiture 1000.000 	Audit* Settings* Run a search Image: settings in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: setting in the search Image: search Ima	karka Smart Monitoring Serve Tack TotAL RETRIES due to enrors serve tack TotAL RETRIES 22.00 23.00

splunk>enterprise App: Kafka Smart Monitoring •			🚯 Guilhem Marchand 👻 Messages	
Overview Brokers Topics Interceptors Burro	w Analytics Search • Kafka monitoring •	Kafka logging • Kafka alerting • Connected Experience		Kafka Smart Monitoring
Kafka Connector Source task - Entity Env Last 60 minutes • ANY ×	Label: Kafka mon	itor(s); urce-connector X Hide Filters		
NUMBER OF CURRENT TASK(S)	running	100.00 SINK TASK RUNNING RATIO	D SINK TASK TOTAL ERFORS	SNK TASK TOTAL RETRIES
CONNECTOR OVERVIEW SOURCE TASK OVERVIEW	ERRORS TASK OVERVIEW LOGS ACTIVITY			
Kafka Connect log events by log_level				
20		NFO		
20 20248 2258 2254 2257	2250 2203 2206 2209	2212 2215 2318 2221	, 2124 2127 2120 2133 2125	
Wed Oct 21 2020				
Events Raw search:				
i Time Event				
source: stdout tag: confluentinc/cp-kafka-cor) Show as raw text	7) 1090 WorkerSourceTask(Id=KafKa=source-connector-toss wnet:latest/template_docker_splumk_localhost_kafka-co tpudocker_logs source = sidout source+poe = dockerkafk			
> 21/10/2020 ([-] 23/48/41.674 attrs: ([+]				

2.4.10 Confluent Interceptors Monitoring



splunk >enterprise App: IT Service Intelligence ▼ Service Analyzer▼ Episode Review Glass Tables Deep Dives Multi-Kl	Pi Alerts Dashboards* Search* Configure* Product Tour	0 #	dministrator • Messages • Settings • Activity • Help • Find Q
Kafka schema-registry - Entity health view			
Last 4 hours			
master Matteria Role	0.00 req/sec	0.11 req/sec	0.11 req/sec
GLOBAL METRICS AGGREGATED ENDPOINTS SUBJECTS GET-SCHEMA	SUBJECTS LIST SUBJECTS DELETE SUBJECTS VERSIONS SCHEM	MA IDS-GET-SHEMAS COMPATIBILITY SUBJECTS VERSIONS	
Total number of active Jetty TCP connections (connections-active)		Average rate per second of opened Jetty TCP connections (connections	ctions-opened-rate)
100		1	
50		0.5	
		0.25	
14:30 15:00 15:30 16:00 Fin Nov 9 2018	16.30 17.00 17.30 18.00	M-30 15:00 15:30 16:00 Fri Nov Ø 2018	16:30 17:00 17:30 18:00
Average rate per second of closed Jetty TCP connections (connections-clo	sed-rate)	Historical master/slave state (master-slave-role, 0=slave / 1=master)
1			
0.5		1	
0.25			
14:30 15:00 15:30 16:00 Fri Nov 9 2018	16:30 17:30 18:00	14/30 15:00 15:30 16:00 Fit Nov 9 2018	16:30 17:00 17:30 18:00
2018		2018	
splunk>enterprise App: IT Service Intelligence +		0 #	dministrator • Messages • Settings • Activity • Help • Find Q
Service Analyzer Episode Review Glass Tables Deep Dives Multi-Ki	Pi Alerts Dashboards▼ Search▼ Configure▼ Product Tour		IT Service Intelligence
Kafka schema-registry - Entity health view			
Last 4 hours Hide Filters			
master	0.00 req/sec	0.17 req/sec	0.17 req/sec
GLOBAL METRICS AGGREGATED ENDPOINTS SUBJECTS GET-SCHEMA	SUBJECTS LIST SUBJECTS DELETE SUBJECTS VERSIONS SCHEP	MA IDS-GET-SHEMAS COMPATIBILITY SUBJECTS VERSIONS	
Average number of HTTP requests per second (request-rate)	Average request latency in ms (request-latency	y-avg) Average no of n	equests/sec HTTP error responses (request-error-rate)
1	0.75	· · · · · · · · · · · · · · · · · · ·	
0.75	0.5	0.75	
0.25	0.25		
M-30 15:00 15:30 16:00 16:30 17:00 17	730 18:00 14:30 15:00 15:30 16:00 Fillow 9	16:30 17:00 17:30 18:00 Fil Nov 9	15.00 15.30 16:00 16:30 17:00 17:30 18:00
3040		2018	
Average number of HTTP requests per second (response-rate)	Average response size in bytes (response-size	-avg) Bytes/second or	outgoing responses (response-byte-rate)
2018 Average number of HTTP requests per second (response-rate) 1	Average response size in bytes (response-size	-avg) Bytes/second o	outgoing responses (response-byte-rate)
2018 - Average number of HTTP requests per second (response-rate) 1 075	Average response size in bytes (response-size	-avg) Bytes/second o	outgoing responses (response-byte-rate)
2018 - Average number of HTTP requests per second (response-rate) 1 0.75 0.5 0.5	Average response size in bytes (response-size	Bytes/second o	outgoing responses (response-byte-rate)
1 075 05 0.23	Average response size in bytes (response-size	Bytes/second o	outgoing responses (response-byte-rate)

2.4.11 Confluent schema-registry dashboard view

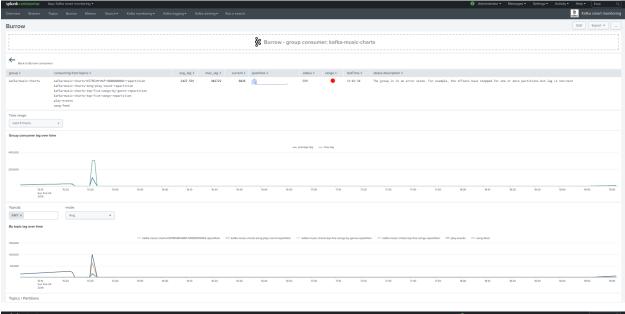
2.4.12 Xinfra Kafka monitor view

Service Analyzer • Epi	sode Review	Glass Tables	Deep Dives	Multi-KPI Alerts	Dashboard	is ▼ Searci	h▼ Config	ure 🔻 🛛 Produ	uct Tour									IT Serv	ice Intelligence				
Kafka LinkedIn	monitor -	End to En	d monitori	ng with ka	afka-moni	tor																	
Between Date-times																							
100.00										100.00													
			PRODU		ATE									CONSUME AV	ALABILITY RATE								
END TO END HEALTH	END TO END HEALTH OVERVIEW END TO END PRODUCE PERFORMANCE END TO END CONSUME PERFORMANCE																						
produce-availability-rate	,					consume-	avallability-rate	•					records-	lost-rate									
50						50							50										
12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00		12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00		12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00				
produce-error-rate						consume-	error-rate							duplicated-rate									
100						100							100										
50						50							50										
12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00		12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00		12:00 Wed Oct 17 2018	14:00	16:00	18:00	20:00	22:00				
2010							2018							2018									
																		~					
Service Analyzer • Epi		Glass Tables		Multi-KPI Alerts			h▼ Config	ure • Produ	uct Tour									IT Serv	ice Intelligence				
Kafka LinkedIn			d monitori	ng with ka	atka-moni	tor																	
Between Date-times	▼ Hide	Filters																					
			10	0.0	0									100).0(
			PRODU	CE AVAILABILITY R	ATE					CONSUME AVALABILITY RATE													
END TO END HEALTH	OVERVIEW	END TO END PRO	DDUCE PERFORM	ANCE END	TO END CONSU!	ME PERFORMA	NCE																
produce-delay-ms-avg										produce-delay-ms	99th												
7.5										100													
5																							
25 worth they	www.ww	when and the way	mahan	monum	where the second	Mum not	human	-	multim									يعليان العر					
and the second the part definition of the second								WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW															
11:00 12:00 Wed Oct 17 2018						10.00				1100 1200 1300 1400 1500 1500 1500 1800 1900 2000 2100 2200 Www.or.fr 2018													
produce-delay-ms-max																							
750																							
500																							
	ulnum				manner	mmu																	
11:00 12:00 Wed Oct 17 2018	13:00	14:00	15:00 16:00	17:00	18:00	19:00	20:00	21:00 2	12:00														

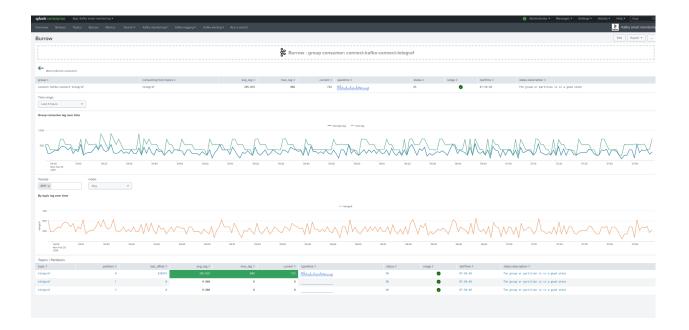
Service Analyzer Episode Review Glass Tables Deep Dives Multi-KPI Alerts Dashboards Search Configure Product Tour	IT Service Intelligence
Kafka LinkedIn monitor - End to End monitoring with kafka-monitor	
Between Date-times Hole Filers	
100.00 Procee and later ly part	100.00 CONTRE AND ADDRESS
END TO END HEALTH OVERNEW END TO END PRODUCE PERFORMANCE END TO END CONSUME PERFORMANCE	
records-delay-ms-avg	records-delay-ms-99th
75	100
2 22 ml May war a burn a burn and a flore a flore a burn and a flore a burn a second a flore a burn	~~
11000 12.00 13.00 14.00 15.00 16.00 17.00 18.00 19.00 20.00 21.00 22.00 19.00 17.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00 20.00	1000 1200 1100 1400 1500 1600 1700 1800 2000 2100 2200 Web 04:17 2018
records-delay-ms-max	records-consumed-rate
200 200 200 200 200 200 200 200	60 ⁵⁰ Wen / M. M. Man Mar

2.4.13 Burrow Kafka Consumers lagging view

splunk>e	nterprise Ac	op: Kafka sma	rt monitoring •	_	_	_			_	_	_	_			_		I Administrator ▼ Messages ▼ Settings ▼ Activity ▼ Help ▼ Find Q.
																	Kafka smart monitoring
Burrow	,		_														Edit Export •
Time range		Env:			Label:		Kafka cluster((5):									
Last 4 ho	urs	* AN1	r×		$ANY \times$		$ANY \times$		Hide Filt	ers							
[oup consume	rs			
Burrow	onsumer groups	s (click on ro	ow to open grou	consume	r details)												
Status:		Cor	sumer group(s):														
$ANY \times$		A	NY×														
env ≎	label 0	clus	iter ¢ group	•		avg_lag 0	max_lag 0	current 0	sparkline 0		status 0	range ©	lastTime ≎	status description	0		
my_env	my_env_label	100	al kafka	music-char	ts	2422.589	302722	5727	1		ERR	•	19:03:10	The group is in	an error st	ate. For examp	le, the offsets have stopped for one or more partitions but lag is non-zero
											<u></u>	Burrow	: partitions				
Burrow	consumer partitic																
	Burrow consumer partitions (click on a row to open timechart lag)																
Status:	onsumer purere		i a row to open t ic(s):	nechart la	g)												
Status: ANY ×	onsumer parate	Тор		mechart la	g)												
	label 0	Top	(c(s):		g) topic ©				partition 0	avg_lag ≎	max_lag 0	current 0	sparkline 0	status 0	range 0	lastTime 0	Mutu description 3
ANY X		Top	ic(s): NY X	1	topic 0	rts-KSTREAM-HAP		artition	partition 0	avg_lag 0 79.752	max_lag 0 57404	current 0	sparkine ≎	status e STOP	range 0	lastTime 0 19:02:40	Suburdemorphics 1 The partition has stopped, for example, the offsets have not been committed in a long period of time
ANY × env 0	label 0	Top Al cluster 0	ic(s): NY X group 0	arts k	topic 0 cafka-music-char					79.752		current 0 1 1	sparkline © 		range 0		
ANY × env 0 my_env	label 0 my_env_label	Top Al cluster 0 local	ic(s): NY X group 0 kafka-music-c	arts k	topic 0 cafka-music-char cafka-music-char	rts-KSTREAM-MAP		artition	٥	79.752	57404	1	sparkline 0 	STOP	•	19:02:40	The partition has stopped. For example, the offsets have not been committed in a long period of time
ANY X env 0 my_env my_env	iabel 0 my_env_label my_env_label	Top Al cluster 0 local local	ic(s): NY X group 0 kafka-music-c kafka-music-c	arts k arts k arts k	topic 0 cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAM-MAP rts-KSTREAM-MAP	-8080808084-repa	artition	0 1	79.752 260.282	57404	1	sparkline 0 l l	STOP	•	19:02:40 19:02:40	The partition has stopped. For example, the offsets have not been committed in a long period of time The partition has stopped. For example, the offsets have not been committed in a long period of time
ANY × env 0 my_env my_env my_env	label 0 my_env_label my_env_label my_env_label	Top At cluster 0 local local local	ic(s): NY X group 0 kafka-music-c kafka-music-c	arts k arts k arts k arts k	lopic 0 cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAM-MAP rts-KSTREAM-MAP rts-song-play-c	-80808088884-repa	artition artition	0 1 2	79.752 260.282 80.103	57404 187634 57686	1 1 0	sparkline 0	STOP STOP OK	•	19:02:40 19:02:40 19:02:40	The partition has stopped, for example, the offsets have not been committed in a long period of time. The partition has stopped. For example, the offsets have not been committed in a long period of time. The group or partition is in a good state.
ANY × emv 0 my_env my_env my_env my_env	iabel 0 ny_env_label ny_env_label ny_env_label ny_env_label	Top Al cluster 0 local local local	kt(s): group 9 kafka-nusic-c kafka-nusic-c kafka-nusic-c kafka-nusic-c	taarts k aarts k aarts k aarts k aarts k	lopic 0 cafka-music-char cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAH-HAP rts-KSTREAH-HAP rts-song-play-o rts-song-play-o	-0000000004-repa	artition artition	0 1 2	79.752 260.282 80.103 0.000	57404 187634 57686 0	1 1 0	sparkline 0	STOP STOP OK OK	•	19:02:40 19:02:40 19:02:40 19:02:40	The partition has stanged. For example, the offsets have not have committed in a long period of time. The partition has stanged. For example, the offsets have not been committed in a long period of time. The groups or partition is in a good state.
ANY × emv 0 my_env my_env my_env my_env	label 0 ny_env_label ny_env_label ny_env_label ny_env_label	Top Al cluster 0 local local local local local	ec(s): group 0 kafka-nusic-c kafka-nusic-c kafka-nusic-c kafka-nusic-c	tarts k karts k karts k karts k karts k karts k	topic 0 cafka-music-char cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAH-MAP rts-KSTREAH-MAP rts-song-play-o rts-song-play-o	-0000000004-repa -0000000004-repa count-repartition	artition artition 1	0 1 2 0 1	79.752 260.282 80.103 0.000 59.727	57404 187634 57686 0 43063	1 1 0	sparkline :	STOP STOP ОК ОК	•	19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not have committed in a long period of time. The partition has stopped. For example, the offsets have not been committed in a long period of time. The group or partition is in a good state. The group or partition is in a good state.
ANY × env 0 my_env my_env my_env my_env my_env	label 0 ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Top A cluster 0 local local local local local local	etis: group 9 kafka-nusie-o kafka-nusie-o kafka-nusie-o kafka-nusie-o kafka-nusie-o	tarts k karts k karts k karts k karts k karts k karts k	lopic 0 cafka-music-char cafka-music-char cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAH-HAP rts-KSTREAH-HAP rts-song-play-o rts-song-play-o rts-song-play-o rts-top-five-so	-0000000004-repa -0000000004-repa count-repartition count-repartition	artition artition a a a a artition	0 1 2 0 1 2	79.752 260.282 80.103 0.080 59.727 19.931	57404 187634 57686 0 43063 14341	1 1 0	sparkline : _/ _/ _/ _/	STOP STOP OK OK OK STOP		19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not been committed is a long period of time. The partition has stopped. For example, the offsets have not been committed is a long period of time. The group or partition is in a good state. The group or partition is in a good state. The group or partition is in a good state.
ANY X emv 0 my_env my_env my_env my_env my_env my_env my_env	label 0 ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Top Al cluster 0 local local local local local local local	ktij: group 8 kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e	tarts k karts k karts k karts k karts k karts k karts k karts k	lopic 8 cafka-music-char cafka-music-char cafka-music-char cafka-music-char cafka-music-char cafka-music-char	rts-KSTREAH-HAP rts-KSTREAH-HAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so	-0000000004-repa -0000000004-repa count-repartition count-repartition count-repartition ngs-by-genre-rep	artition artition 1 3 assertition asartition	0 1 2 0 1 2 0	79.752 260.282 80.103 0.000 59.727 19.931 18.584	57404 187634 57686 0 43063 14341 13262	1 9 8 1 9	sparkline 0	STOP STOP OK OK OK STOP OK		19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not been committed in a long period of time The partition has stopped. For example, the offsets have not been committed in a long period of time The groups or partition is in a good state The groups or partition is in a good state The partition has staped. For example, the offsets have not been committed in a long period of time The groups or partition is in a good state
ANY X emv 0 my_env my_env my_env my_env my_env my_env my_env	label 0 ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Top Al cluster 0 local local local local local local local local	ets): group 8 kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e kafka-nusie-e	arts karts	opic 9 arfia-music-char arfia-music-char arfia-music-char arfia-music-char arfia-music-char arfia-music-char arfia-music-char arfia-music-char	rts-KSTREAH-HAP rts-KSTREAH-HAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so	-000000004-repa -000000004-repa count-repartition count-repartition count-repartition ngs-by-genre-rep ngs-by-genre-rep	artition artition 1 3 assertition asartition	e 1 2 6 1 2 6 1	79.752 260.282 80.103 0.000 59.727 19.931 18.584 0.000	57404 187634 57686 0 43063 14341 13262 0	1 9 9 1 9	ъранкіте : 	STOP STOP OK OK OK STOP OK OK		19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not been committed in a long period of time. The partition has stopped. For example, the offsets have not been committed in a long period of time. The groups arguittime is in a good state. The groups or partitime is in a good state. The groups arguittime has stopped. For example, the offsets have not been committed in a long period of time. The groups or partitime is in a good state. The groups or partitime is in a good state. The groups or partitime is in a good state. The groups or partitime is in a good state.
ANY × env 0 sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env	label 0 ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Top A cluster 0 local local local local local local local local	kcjs: NY X group 3 kafka-nusio-o kafka-nusio-o kafka-nusio-o kafka-nusio-o kafka-nusio-o kafka-nusio-o kafka-nusio-o kafka-nusio-o	arts b arts b	opic 8 afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar	rts-KSTREAM-RAP rts-KSTREAM-RAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so	-000000004-repa -00000004-repa ount-repartition ount-repartition ngs-by-genre-rep ngs-by-genre-rep ngs-by-genre-rep	artition artition a artition cartition cartition	0 1 2 0 1 2 0 1 2	79.752 260.282 80.103 0.000 59.727 19.931 18.584 0.000 55.115	57404 187634 57686 0 43063 14341 13262 0 39738	1 9 9 1 9	sparkline 5 	510P 510P 0K 0K 0K 510P 0K 0K 0K		19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not have constituted is a long period of time. The partition has stopped. For example, the offsets have not have constituted is a long period of time. The groups or partition is in a paint halo. The groups or partition is in a paint halo.
ANY × env 0 sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env sy_env	Inbel 8 my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label	Top All cluster 0 local local local local local local local local local	kitik: NYYX Syrup 1 kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c kafka-nasie-c	i talarts i k karts i k	opic 8 afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar	rts-KSTREAM-RAP rts-KSTREAM-RAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so	-000000004-repa -000000004-repa ount-repartition ount-repartition ngs-by-genre-rep ngs-by-genre-rep ngs-repartition	artition artition a artition cartition cartition	0 1 2 0 1 2 0 1 2	79.752 260.282 80.103 0.000 59.727 19.931 18.584 0.000 55.115 73.696	57404 187634 57686 0 43063 14341 13262 0 39738 52998	1 9 9 1 9	spartine 0	510P 510P 0K 0K 0K 510P 0K 0K 0K		19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40 19:02:40	The partition has stopped. For example, the offsets have not have committed is a long period of time. The partition has stopped. For example, the offsets have not have committed is a long period of time. The group or partition is in a gend state. The group or partition is in a gend state. The partition has staped. For example, the offsets have not have committed is a long period of time. The group or partition is in a gend state. The group or partition is in a gend state.
ANY × errv 0 sy_errv sy_errv sy_errv sy_errv sy_errv sy_errv sy_errv sy_errv sy_errv sy_errv	الفعة 1 هر_سعر_الغاد هر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر_الغاد مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مر_سعر مررس مراس مررس مررس مراس مراس مراس مراس مراس مراس مراس مراس مراس م م مر م م م م م م م م م م م م م	Top All cluster 3 local local local local local local local local local	kitis MYX group 1 kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere kafta-masiere	in ants in ant	opic 8 afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar afka-maic-dar	rts-KSTREAM-RAP rts-KSTREAM-RAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so	-000000004-repa -000000004-repa ount-repartition ount-repartition ount-repartition ngs-by-genre-rep ngs-by-genre-rep ngs-repartition ngs-repartition	artition artition a artition cartition cartition	0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1	79,752 260,282 80,103 0,000 59,727 19,931 18,584 0,000 55,115 73,696 0,000	57404 187634 57686 0 43063 14341 13362 0 39738 52998 52998	1 9 9 1 9	sparkfire 0 	510P 510P 0K 0K 0K 510P 0K 0K 0K 0K		19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00	The partition has stapped. For example, the offsets have not been constitut is a long period of time. The partition has stapped. For example, the offsets have not been constitut is a long period of time. The group or partition is in a good state. The group or partition is in a good state.
ANY × emv 0	Intel 1 ay_aw_late1	Top A cluster 0 local local local local local local local local local local local local local local local local local local	ktyl: WYX group 1 kt/lamaster	arts b arts b ar	opic 8 arka-muic-char arka-muic-char arka-muic-char arka-muic-char arka-muic-char arka-muic-char arka-muic-char arka-muic-char arka-muic-char	rts-KSTREAM-RAP rts-KSTREAM-RAP rts-song-play-o rts-song-play-o rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so rts-top-five-so	-000000004-repa -000000004-repa ount-repartition ount-repartition ount-repartition ngs-by-genre-rep ngs-by-genre-rep ngs-repartition ngs-repartition	artition artition a artition cartition cartition	0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1	79.752 260.282 80.103 0.080 59.727 19.931 18.584 0.080 55.115 73.696 0.080 0.080	57444 187634 57685 0 43063 14341 13262 0 39738 52998 0 9 0	1 9 9 1 9	sparkline S	510P 0K 0K 0K 0K 0K 0K 0K 0K 0K 0K		19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00 19:02:00	The partition has stopped. For example, the offsets have not been constituted is a long period of time. The partition has stopped. For example, the offsets have not been constituted is a long period of time. The groups or partition is in a paint black. The group or partition is in a paint black. The groups or partition is in a good state. The groups or partition is in a good state. The group or partition is in a good state.



	iterprise App:	Kafka smart mo	onitoring •														0 4	dministrator •	Messages •	Settings •	Activity •	Help • Fi	nd
erview	Brokers Topic	s Burrow	Metrics Se	arch 🔻 Kafka m	onitoring • K	Kafka loggi	ing∙ Kaf	ka alerting v	Run a sear	ch												Kafka sm	iart moniti
Irrow																						Edit Exp	ort •
e range:		Env:		Label:		Ka	fka cluster(s):																
ast 4 hou	irs •	ANY ×		ANY ×		4	$ANY \times$		Hide	Filters													
										۶¢ ۱	Burrow: gr	oup consu	mers										
atus:	onsumer groups (c		o open group cons	sumer details)																			
ANY X		ANY X																					
nv ¢	label \$			group ¢				avg_k		max_lag ¢	current	¢ sparkline ≎			status ‡	range ¢	lastTime		status description	- 4			
w e	ny_env_label			group ∓ connect-kafka-conr	actatelerraf			avg_k 294.		max_lag =	current 18		A		status ÷	range ÷	07:58:00		status description The group or pa		and state		
_env	ny_env_label			connect-kafka-sink			-		.127	12		_			ok		07:58:00		The group or pa				
env	ny_env_label			kafka-music-charts					.000			·	NWW		ok		07:58:00		The group or pa				
											Burrow	: partition:	5										
rrow ci	onsumer partitions	(click on a ro Topic(s):		art lag)							Starrow	v: partition:	5										
rrow ci tus:				art lag)							Se Burrow	v: partition:	5										
tow ci us: VY X		Topic(s):		art lag)	topic ‡						Burrow partition \$	/: partition: avg_lag \$	5 max_lag ≑	current 0	sparkline \$		status ¢	range ¢	lastTime ¢	status descri	vien ÷		
tus: NY X	onsumer partitions	Topic(s): ANY ×	<		topic≎ telegra									current ¢ 180	sparkline \$	Vnuvy	status ¢ OK	range ≎ ♥	lastTime 0 07:58:10		xion≎ partition is	in a good st	ate
now cr tus: NY X env	onsumer partitions	Topic(s): ANY × cluster ©	< group ≎	onnect-telegraf		af						avg_lag \$	max_lag \$	_		Vnvy				The group o			
now cr tus: NY X env env	label ÷ ny_env_label	Topic(s): ANY × cluster ≎ local	group 0 connect-kafka-c	onnect-telegraf	telegra	of vf						avg_lag ≎ 294.912	max_lag ≎ 886	180		Vy	OK	٢	07:58:10	The group o	partition is	in a good st	ate
rrow cr tus: NY × env env env	label = ny_env_label ny_env_label	Topic(s): ANY × cluster ≎ local local	group 0 connect-kafka-c	onnect-telegraf onnect-telegraf	telegra	of of of						avg_lag \$ 294.912 0.000	max_lag ≎ 886 Ø	180			OK OK	0	07:58:10 07:58:10	The group o The group o The group o	partition is partition is	in a good st in a good st	ate ate
nrow cr tus: NY × env env env	label 2 ny_env_label ny_env_label ny_env_label	Topic(s): ANY × cluster ÷ local local local	connect-kafka-c connect-kafka-c	onnect-telegraf onnect-telegraf ink-task-syslog	telegra telegra telegra syslog	of of	-ts-KSTREAH+		<pre>4-repartitio</pre>		partition 0 0 1 2	avg_lag 0 294,912 0.000 0.000	max_lag ≎ 886 0 0	180	-		OK OK	0	07:58:10 07:58:10 07:58:10	The group o The group o The group o The group o	partition is partition is partition is	in a good st in a good st in a good st	ate ate ate
env env env	Iabel 2 ny_env_label ny_env_label ny_env_label ny_env_label	Topic(s): ANY × cluster ≎ local local local local	group 0 connect-kafka-c connect-kafka-c connect-kafka-c	onnect-telegraf onnect-telegraf onnect-telegraf ink-task-syslog rts	telegra telegra telegra syslog kafka-m	af af nusic-char		w-seccores		25.	partition 0 0 1 2	avg_lag ¢ 294.912 0.080 0.080 0.127	max_Jag ÷ .536 0 12	180	-		ok ok	0 0 0	07:58:10 07:58:10 07:58:10 07:58:10	The group of The group of The group of The group of The group of	partition is partition is partition is partition is	in a good st in a good st in a good st in a good st	ate ate ate ate
rrow ci tus: NY × env env env env env env	label : ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Topic(s): ANY × cluster ≎ local local local local local	group © connect-kafka-c connect-kafka-c connect-kafka-s kafka-music-cha	onnect-telegraf onnect-telegraf ink-task-syslog rts rts	telegra telegra telegra syslog kafka-m kafka-m	af af nusic-char nusic-char	ts-KSTREAM-1		4-repartitio	25	partition 0 0 1 2	avg_lag 0 294.912 0.000 0.000 0.127 0.000	max_liag © 886 0 0 12 0	180	-		ox ox ox	0	07:58:10 07:58:10 07:58:10 07:58:10 07:58:10	The group o The group o The group o The group o The group o The group o	partition is partition is partition is partition is partition is	in a good st in a good st in a good st in a good st in a good st	ate ate ate ate
rrow ci tus: NY × env env env env env env env	label : ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Topic(s): ANY × cluster ≎ local local local local local local	group 9 connect-kafka-c connect-kafka-c connect-kafka-c connect-kafka-s kafka-music-cha kafka-music-cha	onnect-telegraf onnect-telegraf ink-task-syslog rts rts rts rts	telegra telegra syslog kafka-m kafka-m	of of nusic-char nusic-char nusic-char	ts-KSTREAH-I	WP-2002002004	4-repartitio	25	partition 0 0 1 2	avg_lag © 294.912 0.000 0.127 0.000 0.800	max_lag ≎ 5556 0 0 12 0 0	180	-		0K 0K 0K 0K 0K		07:58:10 07:58:10 07:58:10 07:58:10 07:58:10 07:58:10	The group of The group of The group of The group of The group of The group of The group of	partition is partition is partition is partition is partition is partition is	in a good st in a good st	ate ate ate ate ate
irrow ci lus: invy × 0 .env .env .env .env .env .env	tabel = my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label my_env_label	Topicişi: ANY × cluster = local local local local local local	group * connect-kafka-c connect-kafka-c connect-kafka-c connect-kafka-s kafka-music-cha kafka-music-cha kafka-music-cha	onnect-telegraf onnect-telegraf ink-task-syslog rts rts rts rts rts	telegra telegra telegra syslog kafka-m kafka-m kafka-m	af af nusic-char nusic-char nusic-char	-ts-KSTREAM-1 -ts-KSTREAM-1 -ts-song-play	WP-2002002004	4-repartition	25	partition \$ 0 1 2 0 0 0 1 2 2	avg_lag 2 294,512 0.000 0.127 0.000 0.000 0.000	max_Jag = 886 0 0 12 0 0 0 0	180	-		ок ок ок ок		07:58:10 07:58:10 07:58:10 07:58:10 07:58:10 07:58:10 07:58:10	The group of The group of	partition is partition is partition is partition is partition is partition is	in a good st in a good st	ate ate ate ate ate ate ate ate
Lenv Lenv Lenv Lenv Lenv Lenv Lenv Lenv	label : ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label ny_env_label	Topiciji, ANY × cluster 0 local local local local local local local	c group 0 connect-kafka-c connect-kafka-c connect-kafka- connect-kafka- kafka-music-cha kafka-music-cha kafka-music-cha	onnect-telegraf onnect-telegraf onnect-telegraf ink-task-syslog rts rts rts rts rts rts rts	telegra telegra systog kafka-m kafka-m kafka-m	af af nusic-char nusic-char nusic-char nusic-char	ts-KSTREAM-M ts-KSTREAM-M ts-song-play	WP-8002002004 WP-8002002004 /-count-repart	4-repartition tition	25	partition \$ 0 1 2 0 0 0 1 2 2	avg_lag 2 294.512 0.000 0.127 0.000 0.000 0.000 0.000	mac_lag 0 835 0 0 12 0 8 0 0 0 0	180	-		0K 0K 0K 0K		07:58:10 07:58:10 07:58:10 07:58:10 07:58:10 07:58:10 07:58:10	The group of The group of	partition is partition is partition is partition is partition is partition is partition is	in a good st in a good st	ate ate ate ate ate ate ate ate



2.5 Splunk Connected experience for Cloud Gateway

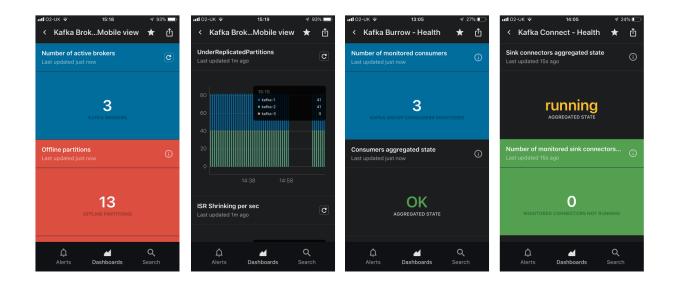


Connected experience dashboards are builtin dashboards optimised for visualization on Splunk Mobile and Splunk TV with Splunk Cloud gateway:

https://docs.splunk.com/Documentation/Mobile

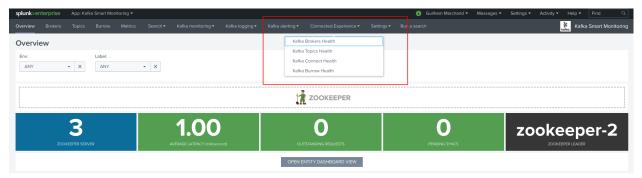
Using Splunk Cloud Gateway and the Connected Experience dashboards, you can easily send data to your mobile Apple TV and device users with compatible and optimized dashboards.

Screenshots from some of the Connected Experience dashboards in Apple Iphone devices:



2.5.1 Access the Connected Experience dashboards

The builtin Connected Experience dashboards are available from the "Connected Experience" menu in the Splunk application:



Although these dashboards are specially designed for the Splunk Connected experience, these are entirely compatible with Splunk Web:

splunk >enterprise App: Kafka Sma								Guilhem Marchand	Messages • Settings •	Activity + Help +	Find Q
Overview Brokers Topics Bun										👸 Kafka	Smart Monitoring
Kafka Brokers - Health										Edit	Export •
Number of active brokers				Offline partitions				Under-replicated partition			
	3 KAFKA BROKERS										
Average messages/in per sec				Average Kbps traffic/in per sec				Average Kbps traffic/out pe	sec		
58.5		/sec		18.4	18 Kb			17.7	75 Kbps	s ou	t
All topics messages per sec				OfflinePartitions				UnderReplicatedPartitions			
	afka-1 — kafka-2 — kafk			100	📕 kafka-1 📕 kafka-2 📕	kafka-3			📕 kafka-1 📕 kafka-2 📕 ka	ifka-3	
16:30 17:00 17:30 Sun Apr 21 2019	18:00 18:30	19:00 19:30	20:00	16:30 17:00 17: Sun Apr 21 2019	30 18:00 18:30	19:00 19:30	20:00	16:30 17:00 Sun Apr 21 2019	17:30 18:00 18:30	19:00 19:30	20:00
Combined Metrics				Brokers traffic statistics				Offline / Under-replicated p	artitions by broker		
Rate ©		5 min 0	15 min 🕈	Broker 0	Msg/sec ≎	KB/in ¢	KB/out ¢	Broker #	Offline •		Under rep. 🕈
Fail.prod /sec	0.00	0.00									

For these dashboards to be available from your Apple devices, the builtin permissions share the dashboards to the global level of the Splunk search instance(s). (See metadata/default.meta)

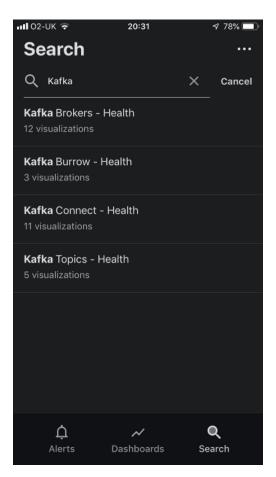
2.5.2 Deploy and configure Splunk Cloud Gateway

Download, install and configure the Splunk Cloud Gateway application in your environment:



https://splunkbase.splunk.com/app/4250/

Once you configured Splunk Cloud Gateway and registered a device, you can search for the Kafka Connected Experience dashboards:



Open any of the dashboards to start your amazing Splunk Connected journey!

2.5.3 Send to mobile alert action

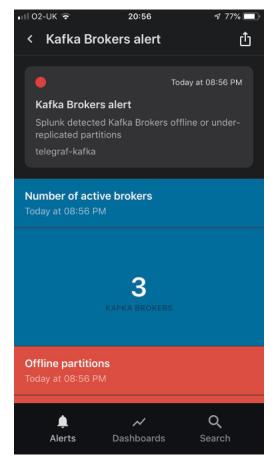
With Splunk Mobile and Splunk Cloud Gateway, you can configure a Kafka alert to send a notification to your apple device, and link with the dashboard of your choice:

https://docs.splunk.com/Documentation/Alerts/latest/Alerts/SendAlerts

The application provides a builtin **"kafka_admin"** role that we suggest you use for Kafka alerting, make sure the users that should receive the Kafka alert notifications are members of the role.

Overview Brokers Topics Burrow Metrics Search + Kafka n	Edit Alert				×		Kafka Smart Monitoring
Kafka monitoring - Kafka Brokers - Offline or Unde		* A6	ou Acuons *			^	
Under-replicated partitions : This measurement, provided on each broker in a cluster, give from a broker being down to resource exhaustion. Offline partitions: Along with the under	When triggered	>	Add to Trigg	gered Alerts	Remove		
number of partitions in the cluster that currently have no leader. Partitions without leader		~	> Send to mo	bile	Remove		
Enabled: No. Enable App: telegraf-kafka			То	kafka_admin 👻 🗙	Select the role that should receive this alert. All users with	J	
Permissions:			Severity	Critical 🔻	the selected role will receive this alert.	1	
Alert Type: Scheduled. Cron Schedule. Edit			,		Max 25 characters	1	
				Kafka Brokers alert		J	
This alert is disabled.			Description	Splunk detected Kafka Brokers offline or under- replicated partitions	Max 150 characters	I	
			Visualization	None Dashboard	Select a supported dashboard to display the events data.	l	
				Kafka Brokers 👻 🗙		Ш	
				Token Name	If your dashboard supports	Ш	
				optional	input tokens, you can specify a token name and a corresponding token value	Ш	
				Result Fieldname optional	using the result field name. Learn more 🗷	Ш	
						Ш	
			Action Label	Optional	Specify a label and URL to open when action label is tapped.	Ш	
			Action URL	Optional			
					Cancel Save		

Shall an alert trigger, a notification will be sent to the members of the kafka_admin role that have a registered device:



2.5.4 Create custom dashboards included in the menu

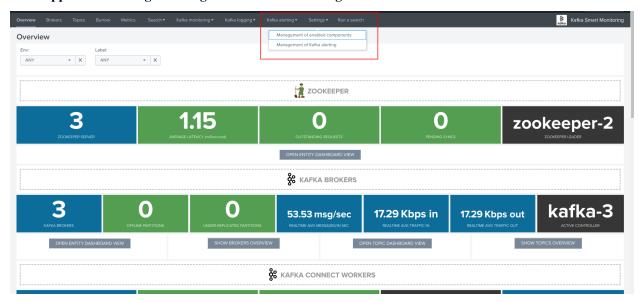
Because there are limitations in Connected Experience dashboards, you might need to create your own versions if for example you have to manage multiple environments.

If you need to create custom versions, achieve the following:

- Clone the dashboard you want to customize and make sure the id of the dashboard starts by "cloudgw_"
- Any dashboard starting by "cloudgw_" will automatically be included within the Connected Experience menu
- Modify the dashboard based on your requirements, to focus on a given environment replace any occurrence of env=* label=* according to the target
- Make sure to clone the existing permissions of the dashboard, or share the dashboard to all apps to allow it to be visible from the mobile app

2.6 Kafka infrastructure OOTB alerting

The application provides out of the box alerting for all the components of the Kafka and Confluent infrastructure.



Go to app menu / Settings / Management of Kafka alerting:

2.6.1 Management of Kafka alerting (user interface)

The OOTB alerting model relies on several KVstore collections being automatically populated, the user interface "Management of Kafka alerting" allows you to interact easily with different aspects of the monitoring:

	DIS	ABLED			
Enable maintenance mode	MAINTE	ANCE MODE STATUS	Disable maintenance mode		
ALERT CONFIGURATION SUMMARY STALE METRICS MONITORING PER COMPONENT STALE METRICS MONITORING I	PER NUMBER OF NODES KAFKA TOPICS MONITO	RING KAFKA CONNECT TASKS MONITORING KAFKA CONSUMER GRO	OUP MONITORING		
ka infrastructure monitoring help - Summary configuration of embedded alerts					
edded alerts: click on a table row to access object contextual actions					
	cron_schedule \$	schedule_window alert.suppress.fields alert	alert.suppress.period \$	disabled next_scheduled_time	ran
sfka components - active node numbers - stale metrics life test	*/5 * * * *	0 env, label, role	4h	0 2019-04-14 11:30:00 UTC	
monitoring - Burrow - group consumers state monitoring	*/5 * * * *	Ø env, label, cluster, group	45	0 2019-04-14 11:30:00 UTC	
monitoring - Confluent kafka-rest - stale metrics life test	*/5 * * * *	0 env, label, name	4	0 2819-04-14 11:38:08 UTC	
monitoring - Confluent ksql-server - stale metrics life test	*/5 * * * *	0 env, label, name	46	0 2819-04-14 11:38:08 UTC	
monitoring - Confluent schema-registry - stale metrics life test	*/5 * * * *	env, label, name	45	0 2819-04-14 11:30:00 UTC	
monitoring - Kafka Brokers - Abnormal number of Active Controllers (2 minutes grace period)	*/5 * * * *	env, label, kafka_broker	45	0 2819+04-14 11:38:08 UTC	
	*/5 * * * *	<pre>@ env, label, kafka_broker, metric_name</pre>	4h	0 2819-04-14 11:30:08 UTC	
monitoring - Kafka Brokers - Failed producer or consumer was detected				0 2819-04-14 11:38:08 UTC	
	*/5 * * * *	Ø env, label, kafka_broker	4h		
monitoring - Kafka Brokers - ISR Shrinking detection	*/5 * * * *	<pre>0 env, label, kafka_broker 0 env, label, kafka_broker, metric_name</pre>	4 4	0 2819-04-14 11:38:08 UTC	
monitoring - Kafka Brokers - 15R Shrinking detection monitoring - Kafka Brokers - Offline or Under-replicated partitions					
sonitoring - Kafka Brokers - 138 Skrinking detection monitoring - Kafka Brokers - Offlier or Odder-replicated partitions monitoring - Kafka Brokers - stale metrics life test	*/5 * * * *	<pre>0 env, label, kafka_broker, metric_name</pre>	45	0 2819-04-14 11:38:08 UTC	
monitoring - Kufika Brokers - 135 Stricklag detection monitoring - Gufika Brokers - Offician or Under-registration partitions monitoring - Kufika Goneet - Auto-entric Life test monitoring - Kufika Goneet - connector or task startup failure detected	*/5 * * * *	<pre>0 env, label, kafka_broker, metric_name 0 env, label, name</pre>	e e	0 2019-04-14 11:30:00 UTC 0 2019-04-14 11:30:00 UTC	
monitoring - Kafha Brokers - 138 Shrinking detection monitoring - Kafha Brokers - 010 Shrinking detection monitoring - Gafha Grokers - stale montions life test monitoring - Gafha Growe - anomater ar with saturby failure detected monitoring - Gafha Convect - stale montris life test	*/5 * * * * */5 * * * *	 env, label, kafka_broker, metric_name env, label, name env, label, connector 	4 4 4	 2019-04-14 11:30:00 UTC 2019-04-14 11:30:00 UTC 2019-04-14 11:30:00 UTC 	
amitoring - Gafta Brokers - 119 Shrinking detections amotoring - Gafta Brokers - 4011 Sing of Unit-registrated partitions construings - Gafta Goovert - analysis - Sing and - Si	*/5 * * * * */5 * * * * */5 * * * *	 ev, label, kafa,broker, metric,name ev, label, name ev, label, connector ev, label, name 	6 6 6 6	 2819-04-14 11:35:00 UTC 2819-04-14 11:35:00 UTC 2819-04-14 11:36:00 UTC 2819-04-14 11:36:00 UTC 	
a monitoring - Gafaa Brokens - Fillad producer ar commune was detected a monitoring - Gafaa Brokens - 100 Borinking detection monitoring - Gafaa Brokens - Officiane outer-monitored partitions a monitoring - Gafaa Brokens - stale motivis life feast monitoring - Gafaa Growet - stale motivis life feast a monitoring - Gafaa Growet - stale motivis life feast a monitoring - Gafaa Growet - stale motivis life feast a monitoring - Gafaa Growet - stale motioning monitoring - Gafaa Growet - tanka status monitoring a monitoring - Gafaa Growet - stale motioning a monitoring - Gafaa Growet - monitoring detected partitions attented on topic a monitoring - Gafaa Growet - monitoring detected partitions attented on topic	*/5 * * * * */5 * * * */5 * * * */5 * * *	em, lakel, kafla,broker, metric_rowe em, lakel, nowe em, lakel, connector em, lakel, connector em, lakel, connector	6 6 6 6 6	2015-04-14 11:30:00 UTC 2015-04-14 11:30:00 UTC	

KVstore collections and lookup definitions

The alerting framework relies on several KVstore collections and associated lookup definitions:

Purpose	KVstore collection	Lookup definition
Monitoring per component en-	kv_telegraf_kafka_inventory	kafka_infra_inventory
tity		
Monitoring per nodes number	kv_kafka_infra_nodes_inventory	kafka_infra_nodes_inventory
Monitoring of Kafka topics	kv_telegraf_kafka_topics_monitoring	kafka_topics_monitoring
Monitoring per component en-	kv_telegraf_kafka_connect_tasks_monitori	ngafka_connect_tasks_monitoring
tity		
Monitoring per Burrow con-	kv_kafka_burrow_consumers_monitoring	kafka_burrow_consumers_monitoring
sumers		
Maintenance mode manage-	kv_telegraf_kafka_alerting_maintenance	kafka_alerting_maintenance
ment		

Permissions and authorizations

Managing the alerting framework and its objects require KVstore collection and lookup definition write permissions.

You can rely on the builtin role kafka_admin and configure your Kafka administrators to be member of the role.

The role provides the level of permissions required to administrate the KVstore collections.

Shall an unauthorized user attempt to perform an operation, or access to an object that is no readable, the following type of error window will be showed:

Overview Brokers Topics Burrow Metrics Search	Oops! ×	a search	& Kafka Smart Monitoring
Kafka Smart Monitoring - Management of er Use this interface to manage kafka Infrastructure alerting for Kafka	Sorry but it looks like an error occurred while attempting to perform the KVstore collection update.		
	You might not have the permission to write to the collection, or an unexpected failure was encountered.		
Enable maintenance mode	The server returned the following error message:	Dischle melatorenen mede	
ALERT CONFIGURATION SUMMARY STALE METRICS MONITORING	Error in 'outputlookup' command: Lookup failed for collection 'kv_telegraf_kafka_alerting_maintenance' in app 'telegraf-kafka' for user 'test': User 'test' with roles { power, test, user } cannot write: /nobody/telegraf- kafka/collections/kv_telegraf_kafka_alerting_maintenance { read : [*], write : [admin] }, owner: admin, removable: no.	FRA TOPICS MONITORING	KAFKA CONNECT TASKS MONITORING
Kafka infrastructure monitoring help - Summary co	Close		
Embedded alerts: click on a table row to access object contextual a Refresh this table			
title 0			
All Kafka components - active node numbers - stale metrics life tes			0 2019-04-14 11:45:00
Kafka monitoring - Burrow - group consumers state monitoring			0 2019-04-14 11:45:00

Maintenance mode

All alerts are by default driven by the status of the maintenance mode stored in a KVstore collection.

Shall the maintenance be enabled by an administrator, Splunk will continue to run the schedule alerts but none of them will be able to trigger during the maintenance time window.

When the end of maintenance time window is reached, its state will be automatically disabled and alerts will be able to trigger again.

A maintenance time window can start immediately, or be automatically automatically scheduled according to your selection.

Enabling the maintenance mode

• Click on the enable maintenance mode button:

Overview Brokers Topics Burrow Metrics Search • Kafka monitoring • Ka	Enabling the maintenan	ce mode	×		& Kafka Smart Me	
Kafka Smart Monitoring - Management of embedded alerting Use this interface to manage kafka infrastructure alerting for Kafka	Enable maintenance mode to avo time window:	id alerts triggering during	your maintenance			
	Maintenance modes starts on:					
	15/06/2019					
Enable maintenance more	At:					
ALERT CONFIGURATION SUMMARY STALE METRICS MONITORING PER COMPONENT STALE	Maintenance modes ends on: 17/06/2019 At:					
Kafka Infrastructure monitoring help - Summary configuration of embed	07:00am • X					
Embedded alerts: click on a table row to access object contextual actions Refresh this table	Cancel	_	Ok			
Ille ¢						
All Kafka components - active node numbers - stale metrics life test						×
Kafka monitoring - Burrow - group consumers state monitoring						
Kafka monitoring - Confluent kafka-rest - stale metrics life test						
Kafka monitoring - Confluent ksql-server - stale metrics life test						
Kafka monitoring - Confluent schema-registry - stale metrics life test						
Kafka monitoring - Kafka Brokers - Abnormal number of Active Controllers (2 minutes grace pe						

• Within the modal configuration window, enter the date and hours of the end of the maintenance time window:

	a logging 👻 Kafka alerting 👻	Connected Experience Audit	Settings - Run a search		Kafka Smart Monitoring
Kafka Smart Monitoring - Management of embedded alerting for Use this interface to manage kafka infrastructure alerting for Kafka	ramework				
		ABLED			
	Ends on: ESTIMATED DATE FOR AUTO-F	17 Jun 07:00			
Enable maintenance mode			Disable maintenance	mode	
ALERT CONFIGURATION SUMMARY STALE METRICS MONITORING PER COMPONENT STALE N		OF NODES KAFKA TOPICS MONITO	RING KAFKA CONNECT TASKS MONITORIN	IG KAFKA CONSUMER GROUP	NONITORING
Embedded alerts: click on a table row to access object contextual actions					
Refresh this table					
	cron_schedule \$	schedule_window \$ alert.suppress	fields ¢ alert.suppress	s.period \$ disabled \$ next.	_scheduled_time \$
Refresh this table	cron_schedule \$ */5 * * *	schedule_window to alert.suppress 0 env, label,		s.period to disabled to next.	scheduled_time \$ \$
Refresh this table title 0			role 4h	1	
Refresh this Lable title S All Kafka components - active node numbers - stale metrics life test	*/5 * * * *	0 env, label,	role 4h cluster, group 4h	1 0 2019-	×

- When the date and hours of the maintenance time window are reached, the scheduled report "Verify Kafka alerting maintenance status" will automatically disable the maintenance mode.
- If a start date time different than the current time is selected (default), this action will automatically schedule the maintenance time window.

Disabling the maintenance mode

During any time of the maintenance time window, an administrator can decide to disable the maintenance mode:

Overview Brokers Topics Burrow Metrics Search •	Disabling the maintenance mode	×	1 search	🐰 Kafka Smart Monitoring
	o you want to confirm disabling the maintenance mode?			
	nce the maintenance mode will be disabled, all activated alerts v igger.	vill be able to		
	Cancel	Ok		
Kafka infrastructure monitoring help - Summary config	guration of embedded alerts			
				0 2019-04-14 11:30:00

Scheduling a maintenance window

You can configure the maintenance mode to be automatically enabled between a specific date time that you enter in the UI.

• When the end time is reached, the maintenance mode will automatically be disable, and the alerting will return to normal operations.

Conversion Defense Defense Defense Called memory and an expense Defense Conversion Conversion	Enabling the maintenance mode Enable maintenance mode to avoid alers triggering du time vindow: Maintenance modes starts on: 17/06/2019 At 12:00am • X Maintenance modes ends on: 17/06/2019 At 07:00am • X	X Ing your maintenance	Rut a leach Dealer and former and the Kapia connect tasks monitoring Ka	Kafka Smart Monito	ring
Refresh this table					
title ©					0
All Kafka components - active node numbers - stale metrics life test					×
					0
					0
					0
					0

• When a maintenance mode window has been scheduled, the UI shows a specific message with the starts / ends on dates:

Overview	Brokers	Topics	Burrow	Metrics	Search 🕶	Kafka monitoring 🕶	Kafka logging 🔻	Kafka alerting 🕶	Connected Experience	 Audit ▼ 	Settings 🕶 🛛	Run a search			Kafka Smart	Monitoring
	Kafka Smart Monitoring - Management of embedded alerting framework Use this Interface to manage kafka Intrastructure alerting for Kafka															
	SCHEDULED MATTEMAKE MODE STATUS															
	Starts on: 17 Jun 00:00 / Ends on: 17 Jun 07:00															
				E	Enable mainten	ance mode						Disabl	e maintenance mode			
ALERT	CONFIGURAT	ION SUMM	ARY STA	LE METRICS	MONITORING	PER COMPONENT	STALE METRICS MO	NITORING PER NUMB	ER OF NODES KAFKA	TOPICS MONIT	ORING KAFKA	A CONNECT TAS	SKS MONITORING KAFKA	CONSUMER G	ROUP MONITORING	
Kafka	Infrastruct	ture mo	nitoring h	nelp - Su	mmary coi	nfiguration of er	mbedded alerts									
_	led alerts: cli h this table	ck on a tal	ble row to a	ccess obje	ct contextual	actions										
title 0								cron_schedule \$	schedule_window \$	alert.suppres	s.fields ¢		alert.suppress.period \$	disabled \$	next_scheduled_time \$	0
All Kafk	a components	- active r	ode numbers	- stale me	etrics life to	st		*/5 * * * *	0	env, label,	role		4h	1		×
Kafka mo	nitoring - Bu	urrow - gro	up consumer	s state mor	nitoring			*/5 * * * *	0	env, label,	cluster, group		4h	0	2019-06-15 23:10:00 BS	st 🥑
Kafka mo	nitoring - Co	onfluent ka	fka-rest -	stale metri	ics life test			*/5 * * * *	0	env, label,	name		4h	0	2019-06-15 23:05:00 BS	st 🥑
Kafka mo	nitoring - Co	onfluent ks	ql-server -	stale metr	ics life test			*/5 * * * *	0	env, label,	name		4h	0	2019-06-15 23:05:00 85	st 🥑

The collection KVstore endpoint can be programmatically managed, as such it is easily possible to reproduce this behaviour from an external system.

(https://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTkvstore)

Monitoring state default definition

When new objects are automatically discovered such as Kafka components or topics, these objects are added to the different KVstore collection with a default enabled maintenance mode.

The default maintenance mode that is applied on a per type of object basis can be customised via the associated macros definitions:

Purpose	Macro definition
Type of component (nodes number monitoring)	zookeeper_default_monitoring_state
Zookeeper nodes	zookeeper_default_monitoring_state
Kafka Brokers	kafka_broker_default_monitoring_state
Kafka Topics	kafka_topics_default_monitoring_state
Kafka Connect workers	kafka_connect_default_monitoring_state
Kafka Connect connectors	kafka_connect_tasks_default_monitoring_state
Kafka Burrow group consumers	kafka_burrow_consumers_default_monitoring_state
Confluent Schema registry	schema_registry_default_monitoring_state
Confluent ksql-server	ksql_server_default_monitoring_state
Confluent kafka-rest	kafka_rest_default_monitoring_state
LinkedIn kafka-monitor	kafka_monitor_default_monitoring_state

The default macro definition does the following statement:

```
eval monitoring_state="enabled"
```

A typical customisation can be to disable by default the monitoring state for non Production environments:

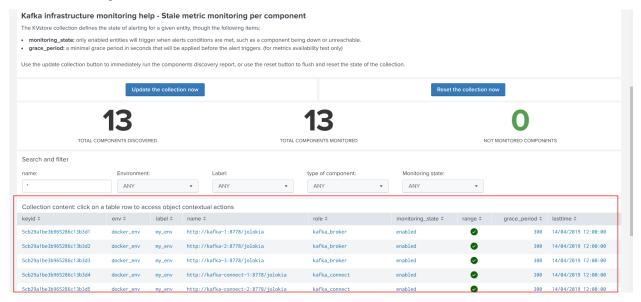
```
eval monitoring_state=if(match(env, "(?i)PROD"), "enabled", "disabled")
```

Such that if a new object is discovered for a development environment, this will not be monitored unless a manual update is performed via the user configuration interface.

Administrating collection entries

Each type of component can be administrated in a dedicated tab within the user management interface.

When objects have been discovered, the administrator can eventually search for an object, and click on the object definition, which opens the modal interaction window:



The modal interaction window provides information about this object, and different action buttons depending on this type of object:

		metric	monitoring per cr	mnonen	•				
		ntity, thoug	Actions for entity: http	p://kafka-1:87	778/jolokia		×		
 monitoring_state: only enable grace_period: a minimal grace 			Name: http://kafka-1:87	778/jolokia					
			Env: docker_env						
		ients disco	Label: my_env						
			Keyid: 5cb29a1be3b9	65286c13b3d	31				
		on now	Current monitoring st	ate: enabled			Reset		
	13 MPONENTS DISCOVE		Current grace period:	300 seconds		Disable	Delete		
		L							
		v		Ŧ					
								range ¢	
								0	
								0	

Enable/Disabling monitoring state

When an object has a disabled monitoring state, the button "enable monitoring" is automatically made available:

netric [,]	monitoring per component									
ity, thoug	Actions for entity: http://kafka-1:8778/jolokia									
s conditio pplied be	Name: http://kafka-1:8778/jolokia									
nto diago	Env: docker_env									
nts disco	Label: my_env									
	Keyid: 5cb29a1be3b965286c13b3d1									
now	Current monitoring state: disabled									
	Current grace period: 300 seconds									
	Close Modify Enable Disable Delete									

When an object has an enabled monitoring state, the button "disable monitoring" is automatically made available:

netric	monitoring per component									
ity, thoug	Actions for entity: http://kafka-2:8778/jolokia ×									
s conditio pplied be	Name: http://kafka-2:8778/jolokia									
nto dio co	Env: docker_env									
nts disco	Label: my_env									
_	Keyid: 5cb29a1be3b965286c13b3d2									
now	Current monitoring state: enabled									
	Current grace period: 300 seconds									
	Close Modify Enable Disable Delete									

Shall the action be requested and confirmed, the object state will be updated, and the table exposing the object definition be refreshed.

Deleting objects in the collection

An object that was discovered and added to the collection automatically can be deleted via the UI:

netric <mark>m</mark>	conitoring per component									
ity, thoug	Actions for entity: http://kafka-2:8778/jolokia									
s conditio pplied be	Name: http://kafka-2:8778/jolokia									
nto disco	Env: docker_env									
nts disco	Label: my_env									
	Keyid: 5cb29a1be3b965286c13b3d2									
now	Current monitoring state: enabled									
	Current grace period: 300 seconds									
	Close Modify Enable Disable Delete									

Shall the action be requested and confirmed, the object state will be entirely removed from the collection, and the table exposing the object definition be refreshed.

Important:

By default, objects are discovered every 4 hours looking at metrics available for the last 4 hours.

This means that if the object has been still generated metrics to Splunk, it will be re-created automatically by the workflow.

To avoid having to re-delete the same object again, you should wait 4 hours minimum before purging the object that was decommissioned.

Finally, note that if an object has not been generating metrics for a least 24 hours, its monitoring state will be disabled a special "disabled_autoforced" value.

This state can still be manually updated via the UI, to permanently re-enable or disable the monitoring state if the component is still an active component.

Modifying an object in the collection

Depending on the type of object, the modal interaction window can provide a modification button:

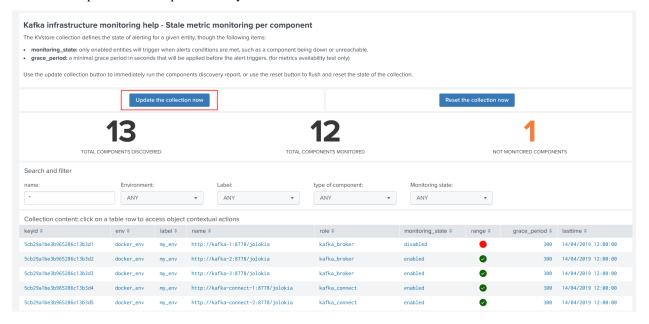
netric	monitoring per component									
ity, thoug	Actions for entity: http://kafka-1:8778/jolokia X									
s conditio pplied be	Name: http://kafka-1:8778/jolokia									
nts disco	Env: docker_env									
	Label: my_env									
	Keyid: 5cb29a1be3b965286c13b3d1									
1 now	Current monitoring state: disabled									
	Current grace period: 300 seconds									
	Close Modify Enable Disable Delete									

The type of modification that can be applied depends on type of component, example:

netric <mark>r</mark>	appitoring per component	_								
ity, thoug	Grace period update ×									
s conditio pplied be	Select a grace period value in seconds, and press Ok to update:									
nto dia an	grace period in seconds:									
nts disco	5 min (300 sec) 👻 🗙									
1 now	Cancel	Ok								
	12									
	TOTAL COMPONENTS MONITORED									

Manually request a collection update job

A collection update can be requested at any time within the UI:



Shall the action be requested and confirmed, the UI will automatically run the object discovery report, any new object that was not yet discovered since the last run of the report, will be added to the collection and made available within the UI.

Kafka infrastructure monitoring help - Stale metric monitoring per component The KVstore collection defines the state of alerting for a given entity, though the following items: • monitoring_state: only enabled entities will trigger when alerts conditions are met, such as a component being down or unreachable. • grace_period: a minimal grace period in seconds that will be applied before the alert triggers. (for metrics availability test only) Use the update collection button to immediately run the components discovery report, or use the reset button to flush and reset the state of the collection.										
13 TOTAL COMPONENTS DISCOVERED TOTAL COMPONENTS										
					~		ANY			
								0		
								0		
								0		
								0		

Once the job has run, click on the refresh button:

e metric "	popitoring por component									
entity, thoug	KVstore collection update	×								
lerts conditio pe applied be	The KVstore collection was updated successfully. All relevant searches were refreshed.									
oonents disco	onents disco It is recommended to reload the dashboard, using the button bellow.									
ction now	Close & refr	esh	Reset th							
	12									
	TOTAL COMPONENTS MONITORED									

Enable/Disabling monitoring state

When an object has a disabled monitoring state, the button "enable monitoring" is automatically made available:

netric <mark>m</mark>	onitoring per component								
ity, thoug	Actions for entity: http://kafka-1:8778/jolokia								
s conditio pplied be	Name: http://kafka-1:8778/jolokia								
nts disco	Env: docker_env								
	Label: my_env								
_	Keyid: 5cb29a1be3b965286c13b3d1								
n now	Current monitoring state: disabled								
	Current grace period: 300 seconds								
	Close Modify Enable Disable Delete								

When an object has an enabled monitoring state, the button "disable monitoring" is automatically made available:

netric	monitoring per component									
ity, thoug	Actions for entity: http://kafka-2:8778/jolokia X									
s conditio pplied be	Name: http://kafka-2:8778/jolokia									
nte disco	Env: docker_env									
nts disco	Label: my_env									
	Keyid: 5cb29a1be3b965286c13b3d2									
n now	Current monitoring state: enabled									
	Current grace period: 300 seconds									
	Close Modify Enable Disable Delete									

Shall the action be requested and confirmed, the object state will be updated, and the table exposing the object definition be refreshed.

Deleting objects in the collection

An object that was discovered and added to the collection automatically can be deleted via the UI:

netric	monitoring per component	
ity, thoug	Actions for entity: http://kafka-2:8778/jolokia	
s conditio pplied be	Name: http://kafka-2:8778/jolokia	
nto dio og	Env: docker_env	
nts disco	Label: my_env	
_	Keyid: 5cb29a1be3b965286c13b3d2	
n now	Current monitoring state: enabled	Rese
	Current grace period: 300 seconds	
	Close Modify Enable Disable Delete	

Shall the action be requested and confirmed, the object state will be entirely removed from the collection, and the table exposing the object definition be refreshed.

Important:

By default, objects are discovered every 4 hours looking at metrics available for the last 4 hours.

This means that is the object has been still generated metrics to Splunk, it will be re-created automatically by the workflow.

To avoid having to re-delete the same object again, you should wait 4 hours minimum before purging the object that was decommissioned.

Finally, note that if an object has not been generating metrics for a least 24 hours, its monitoring state will be disabled a special "disabled_autoforced" value.

This state can still be manually updated via the UI, to permanently re-enable or disable the monitoring state if the component is still an active component.

Modifying an object in the collection

Depending on the type of object, the modal interaction window can provide a modification button:

netric	monitoring per component											
ity, thoug	Actions for entity: http://kafka-1:8778/jolokia ×											
s conditio pplied be	lame: http://kafka-1:8778/jolokia											
nto diago	Env: docker_env											
nts disco	Label: my_env											
	Keyid: 5cb29a1be3b965286c13b3d1											
now	Current monitoring state: disabled	Rese										
	Current grace period: 300 seconds											
	Close Modify Enable Disable Delete											

The type of modification that can be applied depends on type of component, example:

netric <mark>'</mark>	monitoring per component	_	
ity, thoug	Grace period update	×	
s conditio pplied be	Select a grace period value in seconds, and press Ok to update:		
	grace period in seconds:		
nts disco	5 min (300 sec) 🔹 🗙		
n now	Cancel	Ok	
	12		
	TOTAL COMPONENTS MONITORED		

Manually request a collection update job

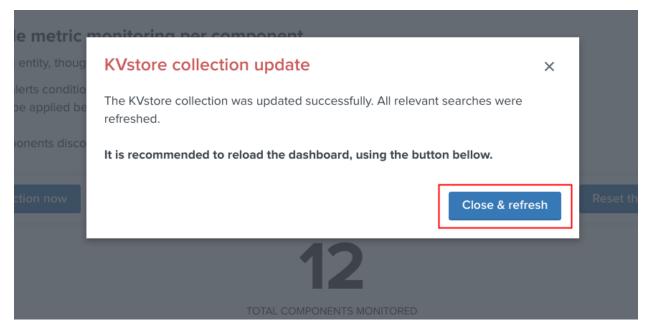
A collection update can be requested at any time within the UI:

Kafka infrastructure n	nonitoring he	lp - Stale	metric monitoring per	compone	nt					
The KVstore collection defines t	the state of alerting	, for a given er	ntity, though the following items:							
			ts conditions are met, such as a co applied before the alert triggers. (
Use the update collection butto	n to immediately ru	in the compon	ents discovery report, or use the	eset button to	o flush and reset the state of th	ne collectio	on.			
	Updat	te the collectic	on now				Reset	the collection r	now	
	13				12				1	
TOTAL CO	MPONENTS DISCOVE	:RED		TOTAL C	OMPONENTS MONITORED			NO	T MONITORED COMPONE	INTS
Search and filter										
name:	Environmen	t:	Label:		type of component:		Monitoring state:			
•	ANY		- ANY	•	ANY	•	ANY			
Collection content: click on	a table row to ac	cess object:	contextual actions							
keyid \$	env ‡	label \$	name \$		role \$	n	nonitoring_state ‡	range \$	grace_period ‡	lasttime ‡
5cb29a1be3b965286c13b3d1	docker_env	my_env	http://kafka-1:8778/jolokia		kafka_broker	d	isabled	•	300	14/04/2019 12:00:00
			http://kafka-2:8778/jolokia		kafka_broker	e	nabled	0	300	14/04/2019 12:00:00
5cb29a1be3b965286c13b3d2	docker_env	my_env								
	docker_env docker_env	my_env	http://kafka-3:8778/jolokia		kafka_broker	e	nabled	Ø	300	14/04/2019 12:00:00
5cb29a1be3b965286c13b3d2 5cb29a1be3b965286c13b3d3 5cb29a1be3b965286c13b3d4			http://kafka-3:8778/jolokia http://kafka-connect-1:8778,	jolokia	kafka_broker kafka_connect		nabled nabled	0	300	14/04/2019 12:00:00 14/04/2019 12:00:00

Shall the action be requested and confirmed, the UI will automatically run the object discovery report, any new object that was not yet discovered since the last run of the report, will be added to the collection and made available within the UI.

Kafka infrastructure n The KVstore collection defines t • monitoring_state: only enab • grace_period: a minimal grad Use the update collection butto	he state of alerting led entities will trig ce period in second		gh the following item ons are met, such as efore the alert trigge				
	13 MPONENTS DISCOVE		Up	odating th	n		
				Ţ	¥		
						•	
						0	
						0	
						Ø	
						0	

Once the job has run, click on the refresh button:



Shall the job fail for some reasons such as a lack of permissions, an error window with the Splunk error message would be exposed automatically.

Manually request a collection rebuild job

A collection reset can be requested at any time within the UI:

Kafka infrastructure n The KVstore collection defines t	5			51							
 monitoring_state: only enable grace_period: a minimal grade 											
Jse the update collection butto	n to immediately ru	n the compon	ents disco	very report, or use the reset b	utton to f	flush and reset the state o	f the collec	tion.			
	Updat	e the collectic	n now					Reset 1	the collection r	iow	
	13					12				1	
TOTAL CO	MPONENTS DISCOVE	RED		1	FOTAL CO	MPONENTS MONITORED			NO	T MONITORED COMPONE	INTS
Search and filter											
name:	Environmen	t:		Label:		type of component:		Monitoring state:			
*	ANY		•	ANY	•	ANY	•	ANY	•		
Collection content: click on	a table row to ac	cess object	contextua	al actions							
keyid \$	env ‡	label \$	name ‡			role ‡		monitoring_state ‡	range ‡	grace_period ‡	lasttime ‡
5cb29a1be3b965286c13b3d1	docker_env	my_env	http://k	kafka-1:8778/jolokia		kafka_broker		disabled	•	300	14/04/2019 12:00:00
5cb29a1be3b965286c13b3d2	docker_env	my_env	http://k	afka-2:8778/jolokia		kafka_broker		enabled	Ø	300	14/04/2019 12:00:00
5cb29a1be3b965286c13b3d3	docker_env	my_env	http://k	afka-3:8778/jolokia		kafka_broker		enabled	0	300	14/04/2019 12:00:00
5cb29a1be3b965286c13b3d4	docker_env	my_env	http://k	afka-connect-1:8778/jolok	ia	kafka_connect		enabled	Ø	300	14/04/2019 12:00:00

Important: When requesting a reset of the collection, all changes will be irremediably lost. All matching objects will be reset to their default discovered values.

Shall the action be requested and confirmed, the UI will automatically run the object discovery report, any new object that was not yet discovered since the last run of the report, will be added to the collection and made available within the UI.

Kafka infrastructuro n		In - Stale				nt				
	0			01						
 monitoring_state: only enable 										
	13			Flushing and u	ipdat	ting the KVstore	colle	ction		
	DMPONENTS DISCOVE									
			v		v		Ŧ		v	
									•	
									-	
									0	

Once the job has run, click on the refresh button:

e metric "	ionitoring per component	-	
entity, thoug	KVstore collection update	×	
lerts conditio be applied be	The KVstore collection was updated successfully. All relevant searches were refreshed.		
onents disco	It is recommended to reload the dashboard, using the button bellow.		
ction now	Close & refre	sh	eset th
	12		
	TOTAL COMPONENTS MONITORED		

Shall the job fail for some reasons such as a lack of permissions, an error window with the Splunk error message would be exposed automatically.

2.6.2 Enabling OOTB alerts

Important: By default, all alerts are disabled, you must enable the alerts within Splunk Web depending on your needs.

You need to decide which alert must be enabled depending on your needs and environments, and achieve any additional alert actions that would be required such as creating an incident in a ticketing system.

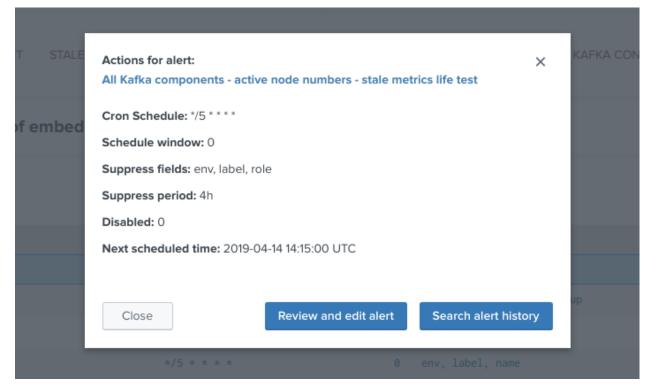
Splunk alerts can easily be extended by alert actions.

Alert configuration summary user interface

The summary alert tab exposes most valuable information about the alerts, and provides a shortcut access to the management of the alerts:

ALERT CONFIGURATION SUMMARY STALE METRICS MONITORING PER COMPONENT STALE METRICS	MONITORING PER NUM	BER OF NODES KAFKA TOPICS MONITORIN	G KAFKA CONNECT TASKS MONITORING	KAFKA CONSUME	R GROUP MONITORING	
Kafka infrastructure monitoring help - Summary configuration of embedded ale	rts					
Embedded alerts: click on a table row to access object contextual actions Refresh this table						
title ‡	cron_schedule \$	schedule_window alert.suppress.fields	alert.suppress.period \$	disabled \$	next_scheduled_time \$	range 🗘
All Kafka components - active node numbers - stale metrics life test	*/5 * * * *	0 env, label, role	4h	0	2019-04-14 14:15:00 UTC	0
Kafka monitoring - Burrow - group consumers state monitoring	*/5 * * * *	0 env, label, cluster	, group 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Confluent kafka-rest - stale metrics life test	*/5 * * * *	0 env, label, name	4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Confluent ksql-server - stale metrics life test	*/5 * * * *	0 env, label, name	4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Confluent schema-registry - stale metrics life test	*/5 * * * *	0 env, label, name	4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Brokers - Abnormal number of Active Controllers (2 minutes grace period)	*/5 * * * *	0 env, label, kafka_	proker 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Brokers - Failed producer or consumer was detected	*/5 * * * *	0 env, label, kafka_	proker, metric_name 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Brokers - ISR Shrinking detection	*/5 * * * *	0 env, label, kafka_	proker 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Brokers - Offline or Under-replicated partitions	*/5 * * * *	0 env, label, kafka_	proker, metric_name 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Brokers - stale metrics life test	*/5 * * * *	0 env, label, name	4h	9	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Connect - connector or task startup failure detected	*/5 * * * *	0 env, label, connect	tor 4h	9	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Connect - stale metrics life test	*/5 * * * *	0 env, label, name	4h	9	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Connect - tasks status monitoring	*/5 * * * *	0 env, label, connect	tor 4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Topics - Under-replicated partitions detected on topic	*/5 * * * *	0 env, label, topic	4h	0	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Kafka Topics - errors detected on a topic	*/5 * * * *	0 env, label, topic	4h	9	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Linkedin Kafka Monitor - stale metrics life test	*/5 * * * *	0 env, label, name	4h	9	2019-04-14 14:20:00 UTC	0
Kafka monitoring - Zookeeper - stale metrics life test	*/5 * * * *	0 env, label, name	4h	0	2019-04-14 14:20:00 UTC	0

Click on any alert to open the modal interaction window:



Click on the "Review and edit alert" button to open the Splunk alert configuration UI for this alert:

Overview Brokers Topics Burrow Metrics Sea		Kafka Smart Monitoring
All Kafka components - active node num This alert will trigger if the number of active nodes generating metrics	onents are down) The minimal number of nodes and monitoring state can be configured within the kv_kafe	Edit •
Enabled:Yes. Disable App:Shared in App. Owned by admin. Edit Modified: Apr 2019 21:34:16 Alert Type:Scheduled. Cron Schedule. Edit	er Condition: Number of Results is > 0. Edit ns: < 1 Action Edit & Add to Triggered Alerts	
There are no fired events for this allert.		

Click on the "Search alert history" button to automatically open a search against the triggering history for this alert

										Administrato				
												kafka	Kafka Smart N	lonitoring
New Search													Save As 🕶	Close
index=_audit action="	"alert_fired"	ss_app="	elegraf-kafk	a" ss_name="	All Kafka compone	nts – active node r	umbers - stale metr	ics life test"					Last 24 hours	Q
✓ 1 event (13/04/2019 17:0	00:00.000 to 1	4/04/2019	17:04:36.000)	No Event S	ampling 🔻						Job 🔻	 	• • Smar	Mode 💌
Events (1) Patterns	Statistics	Visualia	ation											
Format Timeline 🕶	- Zoom Out	+ Zoor		× Desele									1 hou	r per column
		List	 Forma 	t 20 Per	Dago #									
			Time	Event	Fage •									
< Hide Fields	:≡ All Fields	-												
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	14/04/2019 14:46:38.119	eradmin_c	GVsZWdyYWYta2Fma		i5eb7_at_1555253100		r="nobody", ss_app= actions="", severit					d="schedul

Stale metrics life test by component

Life test monitoring alerts perform a verification of the metric availability to alert on a potential downtime or issue with a component.

• Kafka monitoring - [component] - stale metrics life test

Once activated, stale metrics alert verify the grace period to be applied, and the monitoring state of the component from the KVstore collection.

Alerts can be controlled by changing values of the fields:

- grace_period: The grace value in seconds before assuming a severe status (difference in seconds between the last communication and time of the check)
- monitoring_state: A value of "enabled" activates verification, any other value disables it

Stale metrics life test by number of nodes per type of component

If you are running the Kafka components in a container based architecture, you can monitor your infrastructure availability by monitoring the number of active nodes per type of component.

As such, you will be monitoring how many nodes are active at a time, rather than specific nodes identities which will change with the life cycle of the containers.

• All Kafka components - active node numbers - stale metrics life test

Shall an upgrade of a statefullSet or deployment in Kubernetes fail and new containers fail to start, the OOTB alerting will report this bad condition on per type of component basis.

Kafka brokers monitoring

The following alerts are available to monitor the main and most important aspects of Kafka Broker clusters:

- Abnormal number of Active Controllers
- Offline or Under-replicated partitions
- Failed producer or consumer was detected
- ISR Shrinking detection

Kafka topics monitoring

The following alerts are available to monitor Kafka topics:

- Under-replicated partitions detected on topics
- Errors reported on topics (bytes rejected, failed fetch requests, failed produce requests)

Kafka Connect task monitoring

Alerts are available to monitor the state of connectors and tasks for Kafka Connect:

• Kafka monitoring - Kafka Connect - tasks status monitoring

Alerts can be controlled by changing values of the fields:

- grace_period: The grace value in seconds before assuming a severe status (difference in seconds between the last communication and time of the check)
- monitoring_state: A value of "enabled" activates verification, any other value disables it

Kafka Consumers monitoring with Burrow

Alerts are available to monitor and report the state of Kafka Consumers via Burrow:

· Kafka monitoring - Burrow - group consumers state monitoring

Alerts can be controlled by changing values of the fields:

• monitoring_state: A value of "enabled" activates verification, any other value disables it

Notes: Kafka Connect source and sink connectors depending on their type are as well consumers, Burrow will monitor the way the connectors behave by analysing their lagging metrics and type of activity, this is a different, complimentary and advanced type of monitoring than analysing the state of the tasks.

2.6.3 Programmatic access and interactions with external systems

Requirements and recommendations

- Create a Splunk service account user that is member of the builtin kafka_admin role
- The builtin kafka_admin role provides read and write permission to the different KVstore collections
- Make sure splunkd REST API is reachable from your external tool

References

- http://dev.splunk.com/view/webframework-developapps/SP-CAAAEZG
- https://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTprolog
- https://docs.splunk.com/Documentation/Splunk/latest/RESTTUT/RESTandCloud
- https://www.urlencoder.org/ (example online tool to URIencode / decode)

For convenience of the documentation bellow

export splunk_url="localhost:8089"

Authentication

For Splunk prior to 7.3.x

The recommended approach is authentication to Splunk API via a token, see:

Official documentation: Splunk docs API token.

Example authenticating with a user called svc_kafka that is member of the kafka_admin role:

```
curl -k https://$splunk_url/services/auth/login --data-urlencode username=svc_kafka --

→data-urlencode password=pass

<response>

    <sessionKey>DWGNbGpJgSj30w0GxTAxMj8t0dZKjvjxLYaP^yphdluFN_FGz4gz^

    →NhcgPCLDkjWH3BUQalVewt8FTF8KXyyfI09Hqj0icIthMuBIB70dVJA8Jg</sessionKey>

    <messages>

        <messages>

        </messages>

        </response>

export token="DWGNbGpJgSj30w0GxTAxMj8t0dZKjvjxLYaP^yphdluFN_FGz4gz^

        →NhcgPCLDkjWH3BUQalVewt8FTF8KXyyfI09Hqj0icIthMuBIB70dVJA8Jg"
```

A token remains valid for the time of a session, which is by default valid for 1 hour.

For Splunk 7.3.0 and later

Splunk 7.3.0 introduced the usage of proper authentication tokens, which is the recommended way to authenticate against splunkd API:

Official documentation: Splunk docs JSON authentication token.

Once you have created an authentication token for the user to be used as the service account, using curl specify the bearer token:

```
curl -k -H "Authorization: Bearer <token>"
```

Maintenance mode management

Get the current maintenance mode status

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    →telegraf_kafka_alerting_maintenance
```

Enabling the maintenance mode

Enabling the maintenance mode requires:

- a first operation that flushed any record of the KVstore collection
- a value for the end of the maintenance period in epochtime (field maintenance_mode_end)
- the current time in epochtime (field time_updated)

Example: Enable the maintenance mode till the 11 of May 2019 at 9.pm

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

Disabling the maintenance mode

Disabling the maintenance mode requires:

- a first operation that flushed any record of the KVstore collection
- the current time in epochtime (field time_updated)

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" -X DELETE \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    →telegraf_kafka_alerting_maintenance
```

(continues on next page)

(continued from previous page)

Kafka Connect task monitoring management

Retrieve all the records from the KVstore

```
For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"
```

Request tasks inventory update: automatically Add any new task to the collection

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" https://$splunk_url/servicesNS/nobody/

→telegraf-kafka/search/jobs -d search="| savedsearch \"Update Kafka Connect tasks_

→inventory\""
```

Create a new connector to be monitored

Create a new connector entry which enables monitoring for the connector, with recommended fields (env, label, connector, role):

Example:

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    delegraf_kafka_connect_tasks_monitoring \
    -H 'Content-Type: application/json' \
    -d '{"env": "docker_env", "label": "testing", "connector": "kafka-connect-my-
    connector", "role": "kafka_sink_task", "monitoring_state": "enabled", "grace_period
    d": "300"}'
```

Get the entries for a specific connector

example:

Encode the URL and use a query:

Notes: URI encode everything after the "query="

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    otelegraf_kafka_connect_tasks_monitoring?query=%7B%22connector%22%3A%20%22kafka-
    oconnect-my-connector%22%7D
```

Delete a Kafka connector

Delete the record with the key ID " 5410be5441ba15298e4624d1":

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" -X DELETE \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    →telegraf_kafka_connect_tasks_monitoring/5410be5441ba15298e4624d1
```

Deactivating the monitoring state of a connector

Using a search triggered via rest call: (a different method is possible by altering the record, see after)

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" https://$splunk_url/servicesNS/nobody/

→telegraf-kafka/search/jobs -d search="| inputlookup kafka_connect_tasks_monitoring_

→| search env=\"docker_env\" label=\"testing\" connector=\"kafka-connect-syslog\" |_

→eval monitoring_state=\"disabled\" | outputlookup kafka_connect_tasks_monitoring_

→append=t key_field=_key"
```

Or using a rest call (all wanted fields have to be mentioned):

• get the key ID, and if required get the current value of every field to be preserved

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    detelegraf_kafka_connect_tasks_monitoring/5cd5a890e3b965791163eb71 \
    -H 'Content-Type: application/json' \
    -d '{"env": "docker_env", "label": "testing", "connector": "kafka-connect-my-
    docker_env", "label": "testing", "connector": "disabled", "grace_period
    d": "300"}'
```

Activating the monitoring state of a connector

Using a search triggered via rest call: (a different method is possible by altering the record, see after)

For Splunk 7.3.0 and later, replace with -H "Authorization: Bearer <token>"

curl -k -H "Authorization: Splunk \$token" https://\$splunk_url/servicesNS/nobody/ →telegraf-kafka/search/jobs -d search="| inputlookup kafka_connect_tasks_monitoring_ →| search env=\"docker_env\" label=\"testing\" connector=\"kafka-connect-syslog\" |_ →eval monitoring_state=\"enabled\" | outputlookup kafka_connect_tasks_monitoring_ →append=t key_field=_key"

Or using a rest call (all wanted fields have to be mentioned):

• get the key ID, and if required get the current value of every field to be preserved

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    telegraf_kafka_connect_tasks_monitoring/5cd5a890e3b965791163eb71 \
    -H 'Content-Type: application/json' \
    -d '{"env": "docker_env", "label": "testing", "connector": "kafka-connect-my-
    connector", "role": "kafka_sink_task", "monitoring_state": "enabled", "grace_period
    s": "300"}'
```

Delete a connector

example:

Encode the URL and use a query:

Notes: URI encode everything after the "query="

For Splunk 7.3.0 and later, replace with -H "Authorization: Bearer <token>"

Delete the record using the key ID:

For Splunk 7.3.0 and later, replace with –H "Authorization: Bearer <token>"

```
curl -k -H "Authorization: Splunk $token" -X DELETE \
    https://$splunk_url/servicesNS/nobody/telegraf-kafka/storage/collections/data/kv_
    →telegraf_kafka_connect_tasks_monitoring/5410be5441ba15298e4624d1
```

CHAPTER $\mathbf{3}$

Troubleshoot:

3.1 Troubleshoot & FAQ

3.1.1 No metrics data could be found

Shall the application not be able to find any Kafka metrics in Splunk in respect with your configuration, the Overview landing page will show the following modal message:



Root causes can be:

- No metrics could be collected by Telegraf
- Telegraf cannot send the metrics to your Splunk HEC endpoint
- The index name differs from the default "telegraf_kafka" index and the macro "telegraf_kafka_index" was not customised

• Telegraf configuration does not provide a value for env and label tags

3.1.2 Unsupported configuration detected in tags

The value for env and label tags must not contain any white spaces or tabs to avoid token exchange issues in the dashboard navigation.

Shall this be the case, a modal error window will open automatically when opening the Overview page:

					is 🔻 Activity 👻 Help 👻 🛛 Find 🔍
Overview Brokers Topics Burrow	Oops! Unsupported configu	iration detected	×		Kafka Smart Monitoring
	Sorry but we detected an unsupported of	onfiguration in your installation.			
Env: Label:	The Telegraf tags for env and/or label Recommended characters are:	contain unsupported characters.			
	A to Z, in lower or upper case 0-9				
	Underscores, dots and hyphens				
	White spaces or tabs are not supported during token exchanges.	d, and will produce unexpected en	rors		_
J 3	Review your telegraf.conf configuration t	lle:	_		0
ZOOKEEPER SERVER	[global_tags] env = "my_env"		ESTS		PENDING SYNCS
	label = "my_env_label"				
	Visit telegraf-kafka.readthedocs.io				
		Clo	ose		
3	0	52 // mag	0 22		8.32 Kbps out
KAFKA BROKERS					REALTIME AVG TRAFFIC OUT
OPEN ENTITY DASHBOARD V					SHOW TOPICS OVERVIEW
	20 KAEKA 000				
	Se KAFKA COM				
2			00:13:	27	0
5			00:15:	3/	

If this happens, then your Telegraf tags are incorrect, fix your telegraf.conf configuration files, example:

```
[global_tags]
# the env tag is used by the application for multi-environments management
env = "docker_env"
# the label tag is an optional tag used by the application that you can use as_
additional label for the services or infrastructure
label = "testing_env"
```

Once the fix has been applied properly, the error message will disappear.

CHAPTER 4

Versioniong and build history:

4.1 Release notes

4.1.1 Version 1.1.41

• Change: JQuery simple XML dashboard update

4.1.2 Version 1.1.40

• Fix: OS MAIN KPIs file-system usage bar style missing in some builtin views

Version 1.1.39

- · Feature: Improvements on Confluent Interceptor UI and related Overview page subcomponents
- Feature: OS Main KPIs views in each component dashboard
- Change: navigation bar review

- Feature: Integration with Confluent Interceptor Monitoring for producers and consumers advanced lag monitoring with Confluent
- Change: Kafka Smart Monitoring goes Dark theme!
- Change: When no Kafka Connect source or sink connector have been detected, show the aggregated single form in black rather than yellow
- Fix: Issue #64 mMissing double quotes in the flush interval telegraf config UI generator #64
- Fix: Issue #66 Missing dot in telegraf config for Kafka Connect #66

• Fix: Issue #67 - Bad image file path in broker view #67

Version 1.1.37

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

- Fix: Show Kafka Connect tasks return empty results in home page
- Fix: The usage of unit makes single form content way too small in different views

Version 1.1.36

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

• Fix: Avoid mcatalog calls with metric_name as metric_name, some versions of Splunk will incorrectly complain about this, and this causes appinpsect failures in Splunk Base

Version 1.1.35

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

- change: Zookeeper metric collection switches from Telegraf plugin to JMX collection via Jolokia Telegraf input
- fix: Topic entity dashboard should break by topic rather than per broker, fix aggregation when any selected
- fix: Burrow does not show up in Overview page
- fix: Telegraf configuration helper UI is broken, and update for Zookeeper collection
- fix: appinspect warnings
- fix: Increase time range of searches in Overview page to better cover longer time between measures
- fix: Kafka Connect connectors discovery does not preserve a non default monitoring_state

Version 1.1.34

• unpublished

Version 1.1.33

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

- change: Zookeeper metric collection switches from Telegraf plugin to JMX collection via Jolokia Telegraf input
- fix: Topic entity dashboard should break by topic rather than per broker, fix aggregation when any selected
- fix: Burrow does not show up in Overview page
- fix: Telegraf configuration helper UI is broken, and update for Zookeeper collection
- fix: appinspect warnings
- fix: Increase time range of searches in Overview page to better cover longer time between measures

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

- change: Zookeeper metric collection switches from Telegraf plugin to JMX collection via Jolokia Telegraf input
- fix: Topic entity dashboard should break by topic rather than per broker, fix aggregation when any selected
- fix: Burrow does not show up in Overview page
- fix: Telegraf configuration helper UI is broken, and update for Zookeeper collection
- fix: appinspect warnings

Version 1.1.31

CAUTION: Zookeeper metric collection switches from Telegraf plugin to JMX for easier and more consistent metric collection across all the components. If you were using the application prior to this version, please update your configuration to collect metrics via JMX.

See: https://telegraf-kafka.readthedocs.io/en/latest/implementation.html

- change: Zookeeper metric collection switches from Telegraf plugin to JMX collection via Jolokia Telegraf input
- fix: Topic entity dashboard should break by topic rather than per broker, fix aggregation when any selected
- fix: Burrow does not show up in Overview page
- fix: Telegraf configuration helper UI is broken, and update for Zookeeper collection

Version 1.1.30

• fix: Realtime traffic In and Out refer to the same field in Overview for Kafka Brokers

Version 1.1.29

• fix: Realtime traffic In and Out refer to the same field in Kafka broker entity view

Version 1.1.28

• feature: Improvement of the maintenance mode with start date time selection capability and automatic scheduling

• fix: Drilldown link broken for Kafka Broker view from dynamic Brokers overview in main Overview dashboards, or Kafka Brokers dashboard (change introduced in 1.1.26)

Version 1.1.26

- fix: The total number of Kafka Connect connectors reported in Alerting management UI is incorrect if connectors have the same ID across multiple tenants
- fix: Cleaning / deletion of unused css and js objects
- feature: Improved table icons rendering with courtesy of Chrys Younger
- feature: Improved Broker overview panels in Overview and Brokers views

Version 1.1.25

- fix: Regression introduced in version 1.1.21 impacts the Kafka Connect tasks inventory if a task is inactive or removed for a long period
- fix: Incorrect number of connectors reported in Alerting managing interface if connectors have the same names across environments

Version 1.1.24

• feature: Introducing logs mapping macros used in entity views to provide customization capabilities for logs integration

Version 1.1.23

• fix: Missing env/label filters in entity views impact results if multiple env/label and ANY selected

Version 1.1.22

- fix: Improves searches for Connected experience dashboard for Kafka Connect (listing connectors in alert)
- fix: Improves Telegraf configuration generator modal window rendering and adds link button to documentation
- fix: Missing env / label filtering in show tasks in alert button from Overview
- feature: Add dynamic view inclusion in menu for Connected Experience custom dashboards

- feature: Introduction of the Telegraf configuration generator, a guided user interface that generates the telegraf.conf configuration files depending on your requirements
- feature: Adding new Audit menu with builtin Audit dashboard for scheduled performance and daily volume indexing analysis
- feature: Use bootstrap buttons in Overview rather than custom buttons design
- feature: Adding active button in Overview to show Kafka Connect tasks in alert (tasks not reporting)

- feature: Adding drilldown from single in Overview / Kafka Connect health views for failed connectors / failed tasks
- feature: Store the last operational time of Kafka Connect connectors in the KVstore, update at inventory / alert run time, return when an alert triggers
- fix: Lag field missing in table from Splunk Connected experience Burrow dashboard due to typo

• fix: Remove any console.log (even while these are commented) in javascript to avoid manual check from appinspect

Version 1.1.19

- fix: Static index reference in new Splunk Connected experience Kafka Connect dashboard
- fix: lag field name type in new Splunk Connected experience Burrow dashboard
- fix: Remove restart required after installation to allow installation in Splunk Cloud via Self-services (SSAI)
- feature: Adding Splunk Connected experience mobile dashboard for Zookeeper health

Version 1.1.18

- feature: Introduction of the builtin kafka_admin role
- feature: Provides default kafka_admin role member write access to the application name space and the KVstore based lookup collections
- feature: Introduction of the Connected Experience dashboards, Health overview dashboards designed to be used with Splunk Connected Experience and Splunk Cloud Gateway (Splunk Mobile, Splunk TV)
- fix: Static indexes references in Kafka Connect and Kafka Burrow dashboards

Version 1.1.17

- fix: Expose units for Zookeeper latency metrics in Overview and entity view
- feature: Introducing the smart component enablement, which allows enabling / disabling a Kafka component to be visible from the Overview, to be managed via the configuration user interface
- feature: Expose Zookeeper leader and Broker active controller in Overview dashboard when mono tenancy (environment) detected or selected
- feature: Configuration checker, detect incomplete installation (Kafka inventory not updated) when loading Overview, and provide modal update user interaction
- fix: Prevents multiple endpoint calls in Alerting User Interface management in Ajax

- feature: Spinner during update / rebuild of KVstore collections within the management of embedded alerting UI
- feature: Manage unprivileged user access to the UI, and proper error handling due to lack of permission against the KVstore collections

- fix: Improved handling of topics / connectors / consumers discovery reports
- feature: Kafka Brokers OOTB alerts and Kafka Connect connector or task startup failure detected are not linked to a monitoring_state that can be deactivated via the KVstore collections
- feature: Configuration error checker which verifies at overview loading page for unsupported tags in env/label such as white spaces.

- feature: Major improvements of the user experience with the management of embedded alerting via modal contextual user interactions
- feature: Maintenance mode is now time conditioned with an end of maintenance period requested via UI calendar during activation
- feature: Migration to native modal windows for user interactions in the alerting management user interface (removal of bootbox js plugin)
- feature: Default schedule change of the maintenance mode status verification report
- feature: Request Splunk restart by default in app.conf
- fix: Kafka Connect tasks that are paused do not properly affect the aggregated state single form in Overview
- fix: Burrow task single form in Overview page results in appendcols related error in Overview page within Splunk 7.0.x
- fix: Regression in Kafka Connect task listing for Splunk 7.0.x in PostProcess search due to append (introduced by Alerting Management UI)
- fix: Regression in dynamic table overview for Kafka Connect status per task in Overview (introduced by 1.1.14)

- feature: Major improvements of the user experience with the management of embedded alerting via modal contextual user interactions
- feature: Maintenance mode is now time conditioned with an end of maintenance period requested via UI calendar during activation
- feature: Migration to native modal windows for user interactions in the alerting management user interface (removal of bootbox js plugin)
- · feature: Default schedule change of the maintenance mode status verification report
- feature: Request Splunk restart by default in app.conf
- fix: Kafka Connect tasks that are paused do not properly affect the aggregated state single form in Overview
- fix: Add Kafka Connect tasks in the dynamic table tasks overview if the tasks are listed as monitored in the collection, and the tasks do not report metrics currently (collection stopped, tasks were removed but not from collection)
- fix: Burrow task single form in Overview page results in appendcols related error in Overview page within Splunk 7.0.x

- fix: Static span is defined in Burrow detailed view charts
- fix: Prevents removed Burrow consumers to appear as low range when latest metrics available are part of the selected time range
- fix: Missing group by statement for Burrow consumers monitoring in OOTB alert, generates unexpected output containing OK consumers, while alerts are correctly justified for ERR consumers

4.1.3 Version 1.1.12

- feature: Adding drilldown to single forms for Offline and Under-replicated partitions in Overview and Kafka Brokers entities views
- fix: ISR Shrinking missing env/label/broker filters in Kafka broker entity view
- feature: Better table rendering in Kafka broker entity view for Under-replicated partitions

4.1.4 Version 1.1.11

- feature: Improvement of the Alerting framework management interface with tabs categorization, capability to update and reset collections on demand, alert activation summary, UI experience greatly improved
- fix: Prevent low range state for Kafka Connect tasks that were recently deleted in tasks overview
- fix: Improve Kafka Connect tasks table in Kafka Connect entity view
- fix: Pastel red color for under-replicated partitions in topics views
- fix: Properly order per topic/partitions in broker entity table view
- fix: Prevents a failing component that was unreachable for a long period to be entirely removed from the infrastructure collection, replaced by a disabled_autoforced monitoring_state value if downtime>24 hours
- fix: Preserve _key_id of KVstore collections during updates for kafka_infra_inventory / kafka_infra_nodes_inventory lookups

4.1.5 Version 1.1.10

- fix: Static index references instead of macro usage in Kafka Connect entity view, Kafka Connect status report and drilldown links
- fix: Switch to dopdown selector for env/label in Overview to avoid multiselect issues with forwarding tokens to dashboards

4.1.6 Version 1.1.9

• fix: Static index reference instead of macro usage in Kafka Connect report

4.1.7 Version 1.1.8

- feature: Improvements of the Kafka Connect task status overview report
- feature: Add icon ranges and filters for Kafka Connect task status overview from Overview main dashboard, configure drilldown from table to entity views

4.1.8 Version 1.1.7

- feature: Add input text filter for Consumers in UI Monitoring management
- fix: Non working filters for Consumers / partitions in UI Burrow
- feature: Map monitoring_state in Consumers status preview in Overview

4.1.9 Version 1.1.6

- fix: incompatibility for ksql-server with latest Confluent release (5.1.x) due to metric name changes in JMX model
- feature: avoid no results returned by single in Overview page for Burrow when no consumers are yet added to the monitored collection

4.1.10 Version 1.1.5

Burrow integration: Kafka Consumer Lag monitoring

- feature: Integration of Burrow, new Burrow consumer lag monitoring UIs
- feature: Management of Kafka consumers state within the alerting framework
- feature: Integration of Burrow consumers state within the Overview UI
- feature: Schedule Kvstore collection update reports (infra, topics, tasks, consumers) on a per 4 hours basis
- fix: Prevents user from attempting to disable maintenance mode when already disabled, and vice-versa
- fix: Properly sort Connect tasks statuses on Overview page to show Unknown status when tasks are missing but monitored

The Burrow integration provides advanced threshold less lag monitoring for Kafka Consumers, such as Kafka Connect connectors and Kafka Streams.

4.1.11 Version 1.1.4

Burrow integration: Kafka Consumer Lag monitoring

- feature: Integration of Burrow, new Burrow consumer lag monitoring UIs
- · feature: Management of Kafka consumers state within the alerting framework
- feature: Integration of Burrow consumers state within the Overview UI
- feature: Schedule Kvstore collection update reports (infra, topics, tasks, consumers) on a per 4 hours basis
- fix: Prevents user from attempting to disable maintenance mode when already disabled, and vice-versa

The Burrow integration provides advanced threshold less lag monitoring for Kafka Consumers, such as Kafka Connect connectors and Kafka Streams.

4.1.12 Version 1.1.3

- fix: Properly order partitions in new Brokers detailed UI
- fix: Allows selection of special topics in entity topic view

4.1.13 Version 1.1.2

- feature: New Brokers/Brokers details, Topics/Topics details UIs inspired from Yahoo kafka-manager
- feature: Allows environment and label selection from Overview, propagates tokens across all UIs
- fix: Incorrect number of partitions reported within Brokers entity view when multiple Brokers are selected

4.1.14 Version 1.1.1

• fix: Static index called in report Kafka monitoring - tasks status report

4.1.15 Version 1.1.0

CAUTION: Breaking changes, telegraf modification is required to provide global tags for env and label dimensions!

https://da-itsi-telegraf-kafka.readthedocs.io/en/latest/kafka_monitoring.html#telegraf-output-configuration

Upgrade path:

- Upgrade telegraf configuration to provide the env and label tags
- Upgrade the application

Features/fixes:

- feature: Multi-environment / Multi-dc support via env and label tagging at Telegraf metric level, allows embedded management of any number of environment and/or additional sub-dividing notion (multi-env, multi-dc...)
- feature: New kvstore collection to allow monitoring of services in a container environment philosophy based on the number of active nodes per role rather than their identity
- feature: Update of the Alerting Management User Interface
- feature: New OOTB Alerting based on active nodes numbers per role
- · feature: Refreshed Overview page with layers icons, additional overview in page views
- · feature: New applications icons
- fix: Various fixes and improvements

4.1.16 Version 1.0.12

- fix: Improve detection of Kafka Connect tasks not successfully running on the Overview page
- fix: Drilldown on single forms for Kafka Connect tasks

4.1.17 Version 1.0.11

- fix: Management interface toggle panels not working (bad reference in js)
- fix: Management interface disable maintenance button not showing up properly in Splunk 7.0.x
- fix: Preset a default value for maintenance mode status
- fix: share lookups, transforms and macros at system level by default

4.1.18 Version 1.0.10

• Unpublished

4.1.19 Version 1.0.9

- feature: Added OOTB Alert for under-replicated partitions per topics
- feature: Management interface for embedded Kafka alerting
- · feature: Enabling / Deactivating maintenance mode through UI for alerting management

4.1.20 Version 1.0.8

- feature: Out of the box alerting templates for Kafka infrastructure
- fix: Kafka Connect aggregated states issues in Overview page

4.1.21 Version 1.0.7

- feature: Out of the box alerts for Kafka Infrastructure
- feature: Support for Confluent ksql-server
- feature: Support for Confluent kafka-rest
- feature: Overview home page improvements
- · feature: event logging integration with the TA-kafka-streaming-platform
- fix: minor fixes and improvements in views

4.1.22 Version 1.0.6

• fix: Typo in Overview

4.1.23 Version 1.0.5

• feature: Confluent schema-registry support

4.1.24 Version 1.0.4

- fix: inverted filters for source/task in Overview
- fix: dropdown replaced by multiselect and key per connector/task in source/sink views

4.1.25 Version 1.0.3

• fix: Overview page, link for topic management should be under brokers category

4.1.26 Version 1.0.2

• various: logo update

4.1.27 Version 1.0.1

• fix: missing link for Kafka topics reporting

4.1.28 Version 1.0.0

• initial and first public release