Log Search

Logs are a type of stream supported in OpenObserve, logs search screen offers users of application with various functionalities like filtering logs based on specified criteria and/or time window , one can additionally leverage query functions to deduce data during query time.

Log search offer two modes :

- 1. intellisense mode where user can select and/or deduce fields(using query functions), specify where clauses for filtering
- 2. full sql mode where user can write sql to get data from specific logs stream

To navigate to logs in OpenObserve, select preferred organization using organization selection control, then click on screen. Logs screen lists all log streams for selected organization.

menu , which will take user to logs

Q Logs

🔲 Query 📹 Fields 📹 Histogram 🍞 SQL Mo	1 lode 🖉 Syntax Guide 1	Off ▾ Q
3		
Default 4	5 Showing 1000 out of 38,997 hits in 421 ms. (Scan Size: 60MB)	
Q Search for a field	600 400	
_p		lumit.
_timestamp kubernetes.annotations.kubernetes.io/psp	15:59:50 16:00:55 16:02:00 16:03:05 16:04:10 16:05:15 16:06:20 16:07:25 16:08:30 16:09:35 16:10:40 16:11:45 16:12:50 16:12:50	3:55
kubernetes.container_hash	timestamp Source 7	
	Jan 25, 2023 16:14:52.547 +05:30 {"_p":"F","_timestamp":1674643492547000,"kubernetes":{"annotations":("kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.container_image kubernetes.container_name	Jan 25, 2023 16:14:52:545 +05:30 {"_p":"F","_timestamp":1674643492545000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.container_name	Jan 25, 2023 16:14:52.545 +05:30 {"_p":"F","_timestamp":1674643492545000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.bocker_la	Jan 25, 2023 16:14:52.536 +05:30 {"_p":"F","_timestamp":1674643492536000,"code":200,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/zin	1c-cp@sha256:2cb
	Jan 25, 2023 16:14:52.503 +05:30 {"_p":"F","_timestamp":1674643492503000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.app.kubernetes.io/component	Jan 25, 2023 16:14:52.502 +05:30 {"_p":"F","_timestamp":1674643492502000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.app.kubernetes.io/instance	Jan 25, 2023 16:14:52.502 +05:30 {"_p":"F","_timestamp":1674643492502000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.app.kubernetes.io/name	Jan 25, 2023 16:14:52.502 +05:30 {"_p":"F","_timestamp":1674643492502000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"registry.k8s.io/ingress-nginx/controller@sha256:4ba73c6977706	64c1e00e9f968de
kubernetes.labels.pod-template-hash	Jan 25, 2023 16:14:51.992 +05:30 {"_p":"F","_timestamp":1674643491992000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"registry.k8s.io/ingress-nginx/controller@sha256:4ba73c6977706	64c1e00e9f968de
kubernetes.namespace_name	Jan 25, 2023 16:14:51.992 +05:30 {"_p":"F","_timestamp":1674643491992000,"code":200,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/zin	nc-cp@sha256:2cb
kubernetes.pod_id	Jan 25, 2023 16:14:51.961 +05:30 {"_p":"F","_timestamp":1674643491961000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.pod_name	Jan 25, 2023 16:14:51.961 +05:30 {"_p":"F","_timestamp":1674643491961000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
log	Jan 25, 2023 16:14:51.961 +05:30 {"_p":"F","_timestamp":1674643491961000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
stream	Jan 25, 2023 16:14:51.854 +05:30 {"_p":"F","_timestamp":1674643491854000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"registry.k8s.io/ingress-nginx/controller@sha256:4ba73c6977706	64c1e00e9f968de
time	Jan 25, 2023 16:14:51.853 +05:30 {"_p":"F","_timestamp":1674643491853000,"code":200,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/zin	nc-cp@sha256:2cb
kubernetes.annotations.checksum/config	Jan 25, 2023 16:14:51.849 +05:30 {"_p":"F","_timestamp":1674643491849000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"registry.k8s.io/ingress-nginx/controller@sha256:4ba73c6977706	64c1e00e9f968de
kubernetes.annotations.checksum/luascripts	Jan 25, 2023 16:14:51.848 +05:30 {"_p":"F","_timestamp":1674643491848000,"code":200,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/zin	nc-cp@sha256:2cb
kubernetes.labels.controller-revision-hash	Jan 25, 2023 16:14:51.819 +05:30 {"_p":"F","_timestamp":1674643491819000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.pod-template-generation	Jan 25, 2023 16:14:51.817 +05:30 {"_p":"F","_timestamp":1674643491817000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.app	Jan 25, 2023 16:14:51.814 +05:30 {"_p":"F","_timestamp":1674643491814000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.name	Jan 25, 2023 16:14:51.814 +05:30 {"_p":"F","_timestamp":1674643491814000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d
kubernetes.labels.role	Jan 25, 2023 16:14:51.812 +05:30 {"_p":"F","_timestamp":1674643491812000,"kubernetes":{"annotations":{"kubernetes":{"io/psp":"eks.privileged"}},"container_hash":"058694856476.dkr.ecr.us-west-2.amazonaws.com/ziox@sha256:	:3dbbb0dc1eab2d

Logs screen details :

- 1. Controls to toggle visibility or query mode for search, query, fields & histogram control toggle visibility of Query editor(3), Fields(6) & Histogram(5) respectively. SQL mode toggle query mode to intellisense mode or full sql mode, based on SQL mode Syntax guide is shown to user.
- 2. Controls for absolute & relative date-time selection , refresh options for screen & initiating search
- 3. Query editor, the behavior which is affected by sql mode, one can use inbuilt functions like match_all, match_all_raw and match_all_raw_ignore_case or can write complete sql

for search

4. Name of stream belonging to organization which will be target for search, one can change the target stream by selecting one from list

5. Histogram depicting details like how many records are being shown out of total number of records & total scanned volume(size in mb) eligible for search criteria provided

6. List of all fields belonging to stream, one can choose to add the field to add to query(3) or to search results table(7)

7. Search results pane, displaying all matching records