


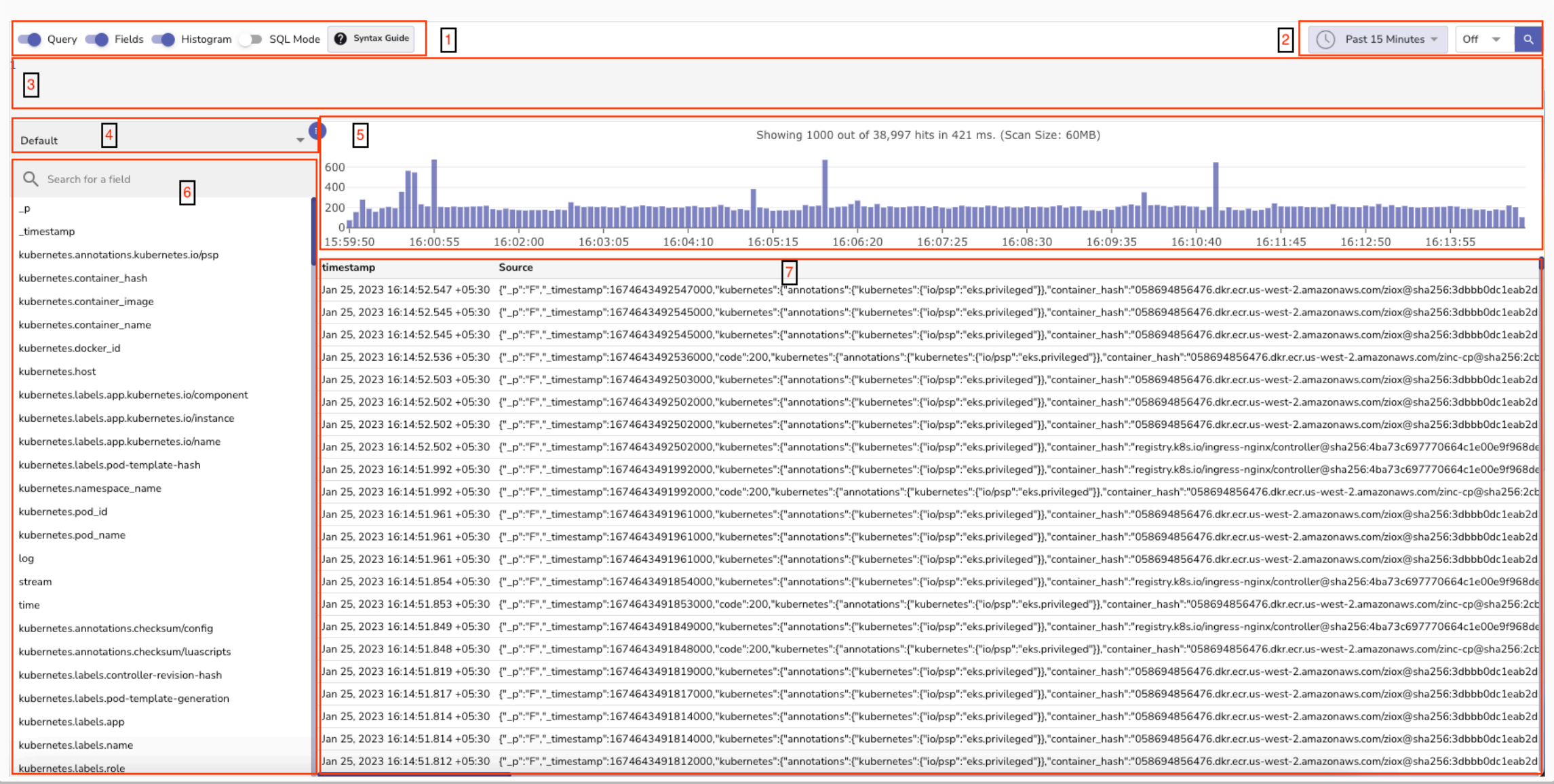
Log Search

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  menu , which will take user to logs screen. Logs screen lists all log streams for selected organization.



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

