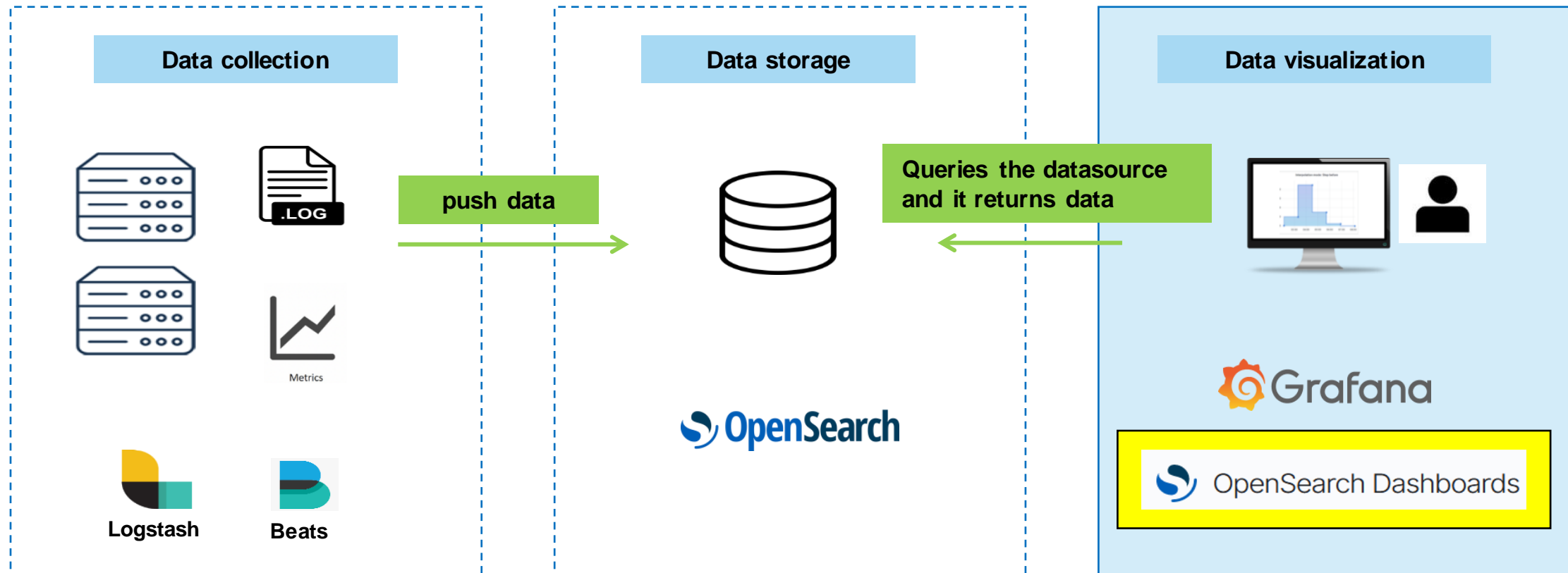




# Components of monitoring architecture

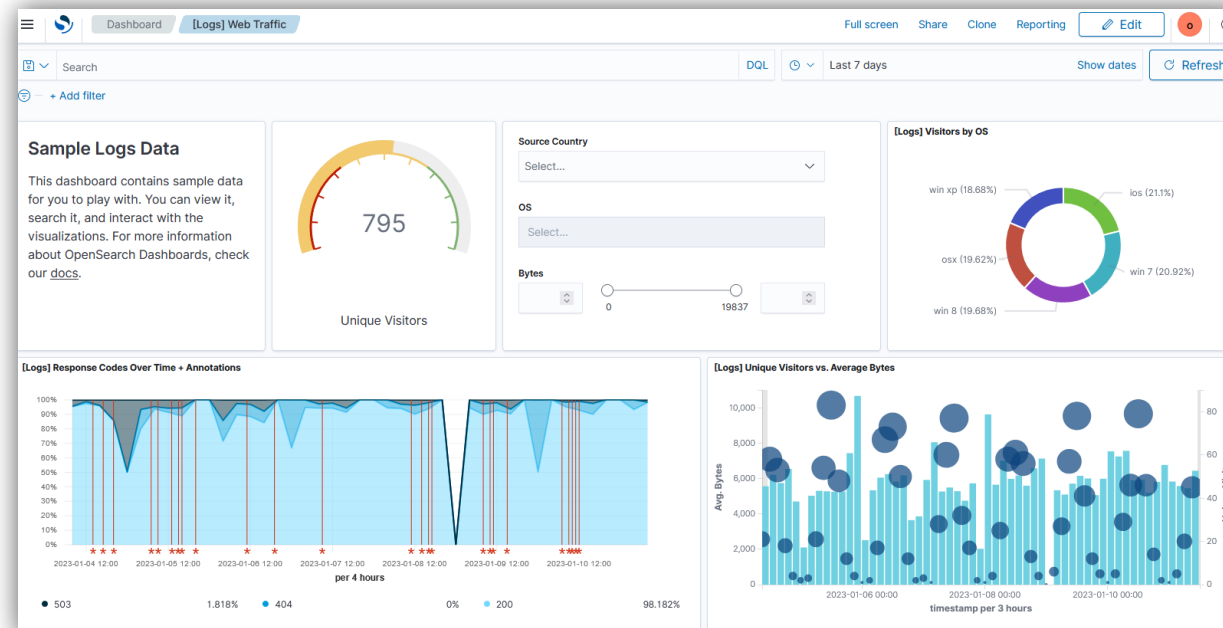


# Agenda

- What is the OpenSearch Dashboards?
- Features
  - Discover
  - Visualize
  - Dashboard
  - Other features (Query Workbench, Reporting, Notebooks)

# What is the OpenSearch Dashboards?

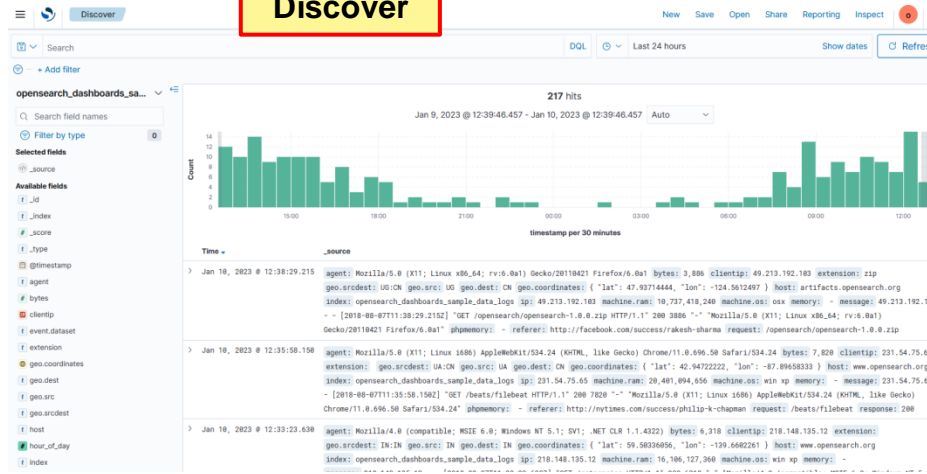
The **OpenSearch Dashboards** is an open-source, integrated visualization tool that makes it easy for users to explore their data in **OpenSearch**.



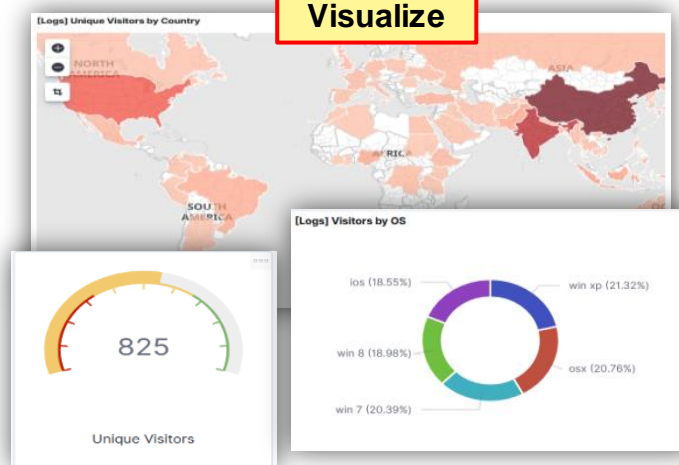
# Features

Open the menu on the left

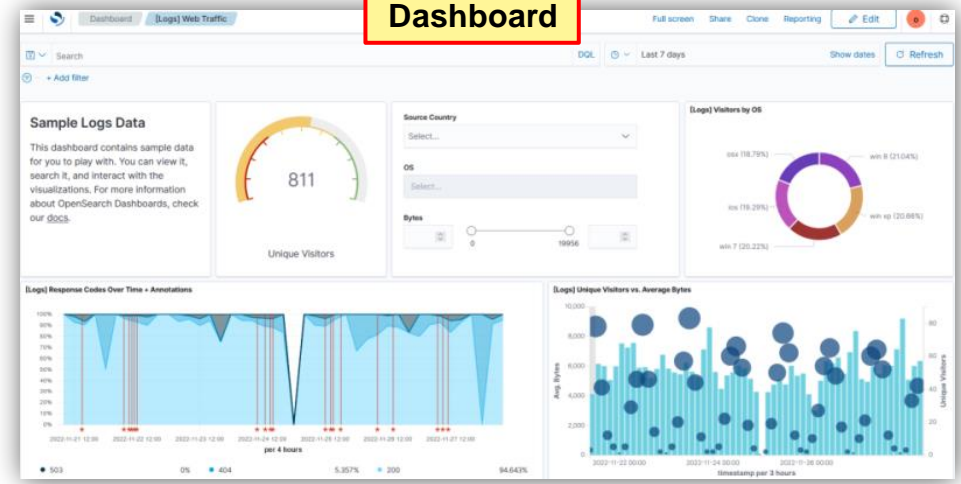
Discover



Visualize



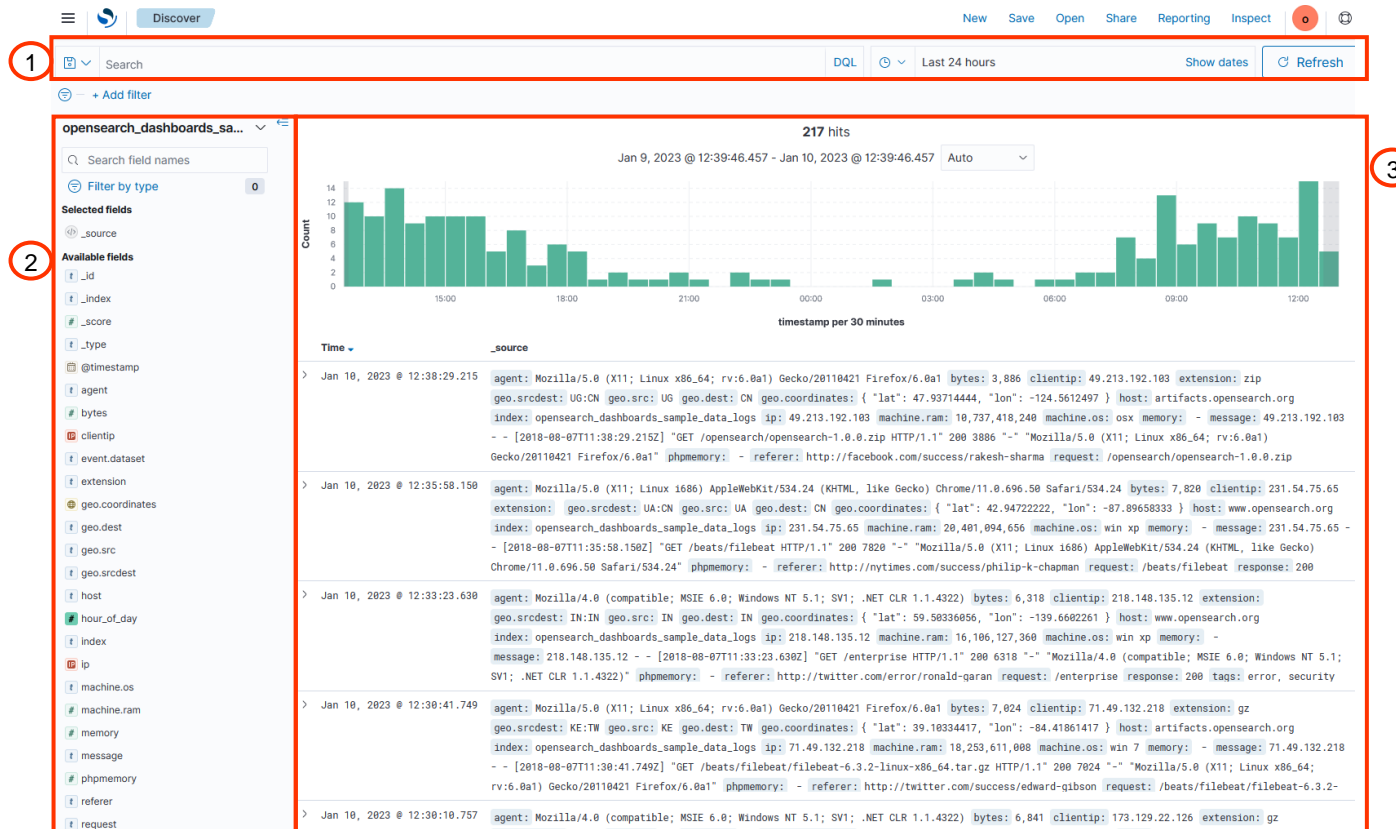
Dashboard



# Discover

■ The Discover screen is divided into three major sections:

1. Top of screen: Query bar --> Enter an expression to filter the data
2. Left: Switch index and display field list
3. Right: Time-series display of search results and individual logs. Fields can also be specified and displayed in table format



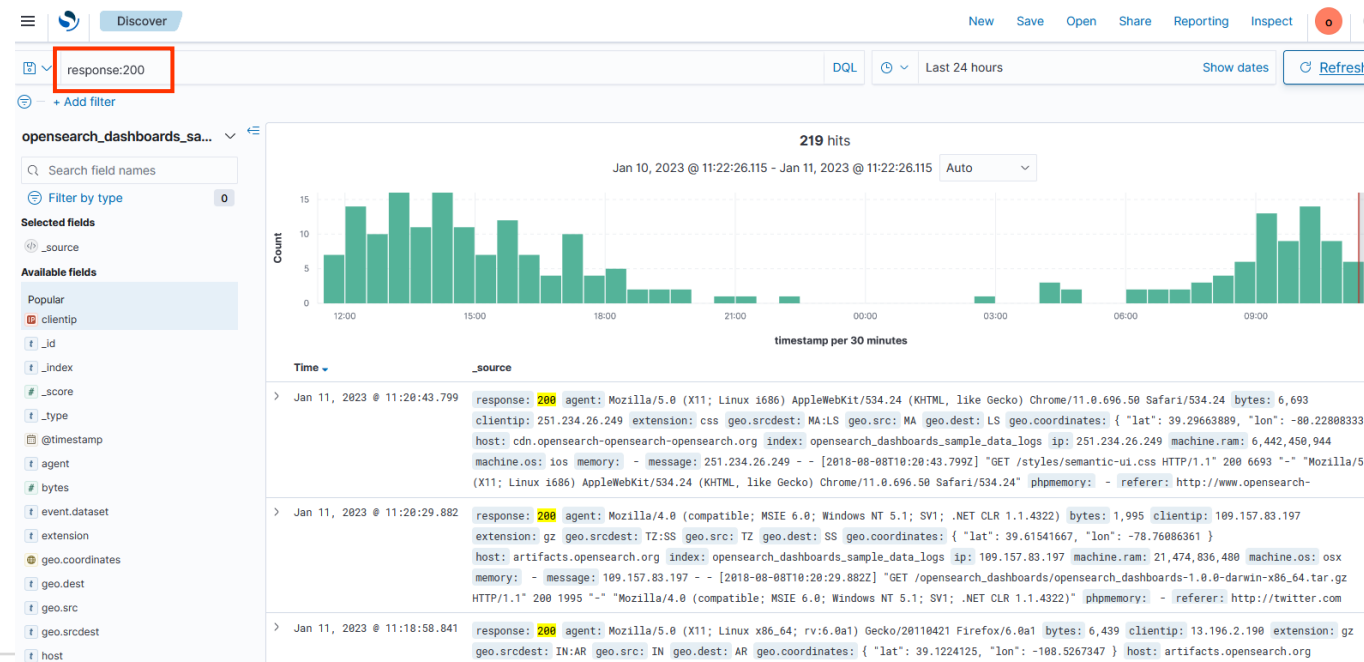
The screenshot shows the OpenSearch Discover interface. At the top, there is a search bar (1) with a search input, a 'DQL' button, and filters for 'Last 24 hours', 'Show dates', and 'Refresh'. On the left, there is a sidebar (2) with 'Filter by type' and a list of 'Available fields' including \_source, \_id, \_index, \_score, \_type, @timestamp, agent, bytes, clientip, event.dataset, extension, geo.coordinates, geo.dest, geo.src, geo.srcdest, host, hour\_of\_day, index, ip, machine.os, machine.ram, memory, message, phpmemory, referer, and request. The main area (3) displays a time-series bar chart showing 'Count' vs 'timestamp per 30 minutes' with 217 hits. Below the chart is a table of individual log entries with columns for Time, \_source, and log details.

Try it !

Go to <https://opensearch-dashboards.scc.kit.edu>  
and use the sample web logs dataset

# Dashboards Query Language

- You can use the Dashboards Query Language (DQL) in OpenSearch Dashboards to search for data and visualizations.
  - **Terms query.** To query using exact search terms, enter the field name followed by : and then the values separated by spaces. Example: `response:200`
  - **Boolean queries (or, and, and not).** Example: `response:(200 or 404)`
  - **Range queries (>, >=, <, and <=** on numeric and date types.)
  - **Exist queries:** matches documents that contain any value for a field, for example `response:*`
  - **Wildcards queries** can be used to search by a term prefix or to search multiple fields. Example: to match documents where `machine.os` starts with `win` (such as "windows 7" and "windows 10") use: `machine.os:win*`























# Visualize

- **Visualize** enables you to create visualizations of the data from your indices.

## New Visualization

Q Filter

 Area	 <b>E</b> Controls	 Coordinate Map	 Data Table
 Gantt Chart	 Gauge	 Goal	 Heat Map
 Horizontal Bar	 Line	 Markdown	 Metric
 Pie	 Region Map	 TSVB	 Tag Cloud
 Timeline	 Vega	 Vertical Bar	 <b>E</b> VisBuilder

## Select a visualization type

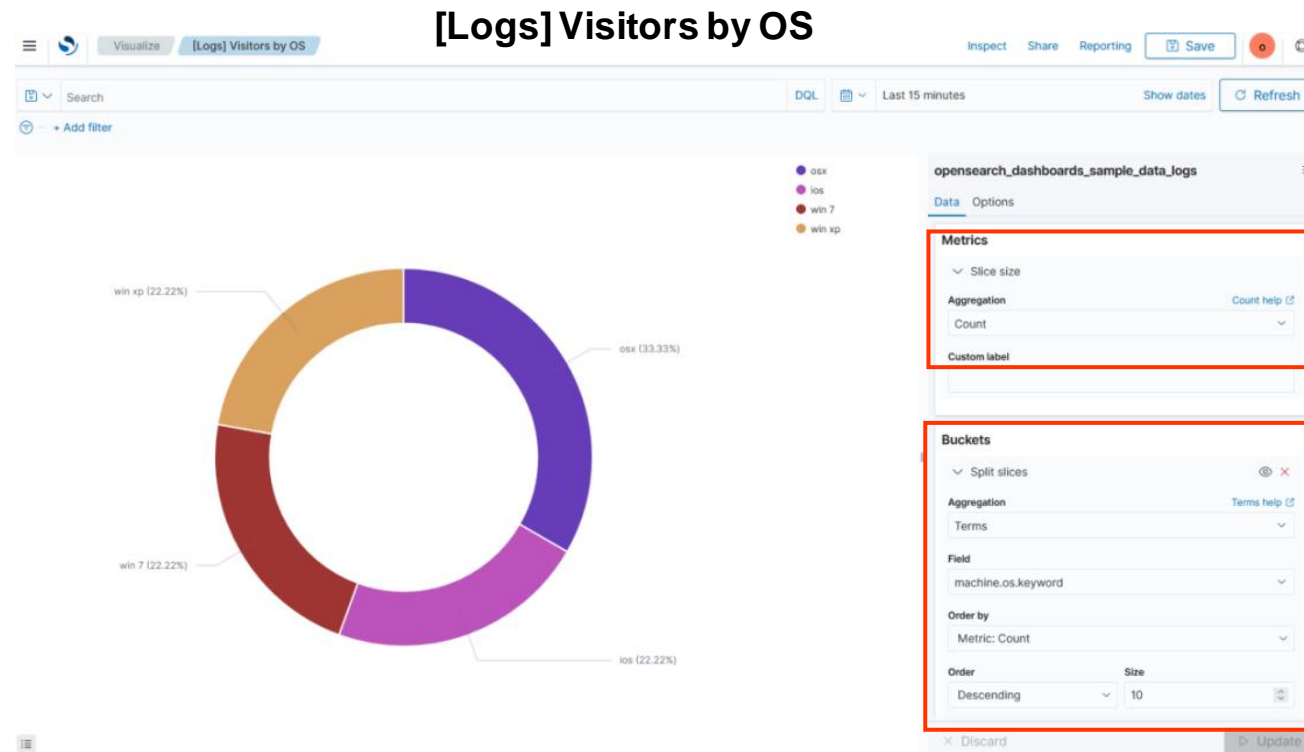
Start creating your visualization by selecting a type for that visualization.





# Aggregations

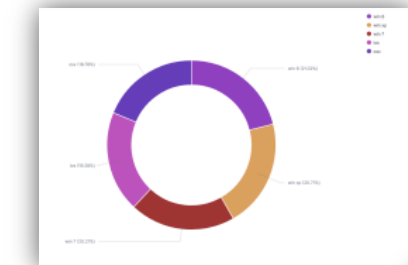
- **Aggregation** refers to the collection of documents or a set of documents obtained from a particular search query or filter.
  - **Metric Aggregation** that calculate metrics, such as a sum or average, from field values
  - **Bucket Aggregation** that group documents into buckets, also called bins, based on field values, ranges, or other criteria



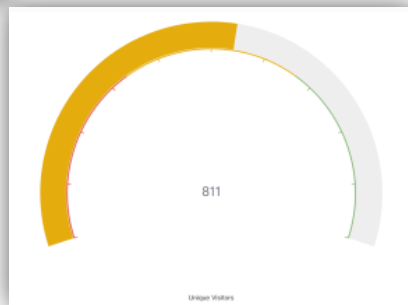
# Dashboard

- A **dashboard** is a collection of visualizations, searches and maps.
- You can create your personal dashboard based on saved visualizations to get an overview of your data.
- Generally data put on a dashboard is typically related but it is possible to add visualizations from different index patterns

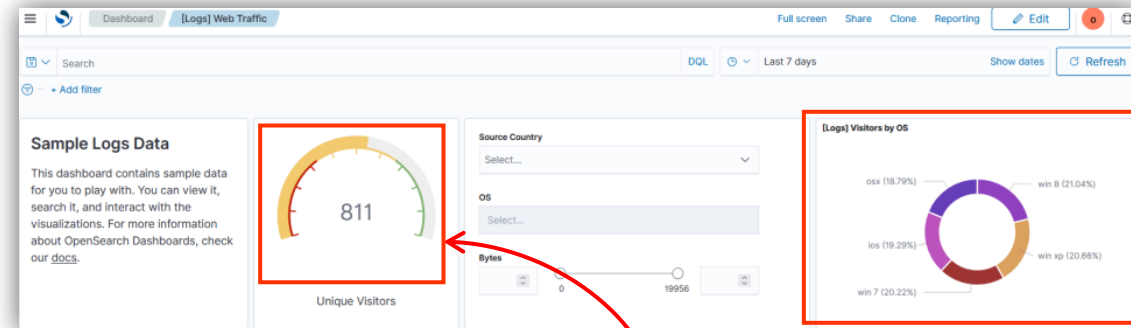
## Dashboard [Logs] Web traffic



[Logs] Visitors by OS



[Logs] Unique count of clientip

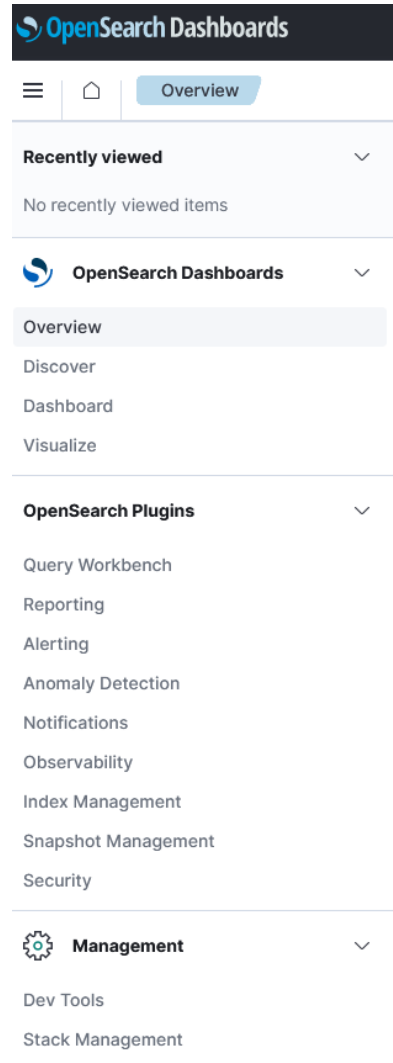


Easy Drag & Drop

Try it !

Go to <https://opensearch-dashboards.scc.kit.edu>  
and explore the [Logs] Web Traffic Dashboard

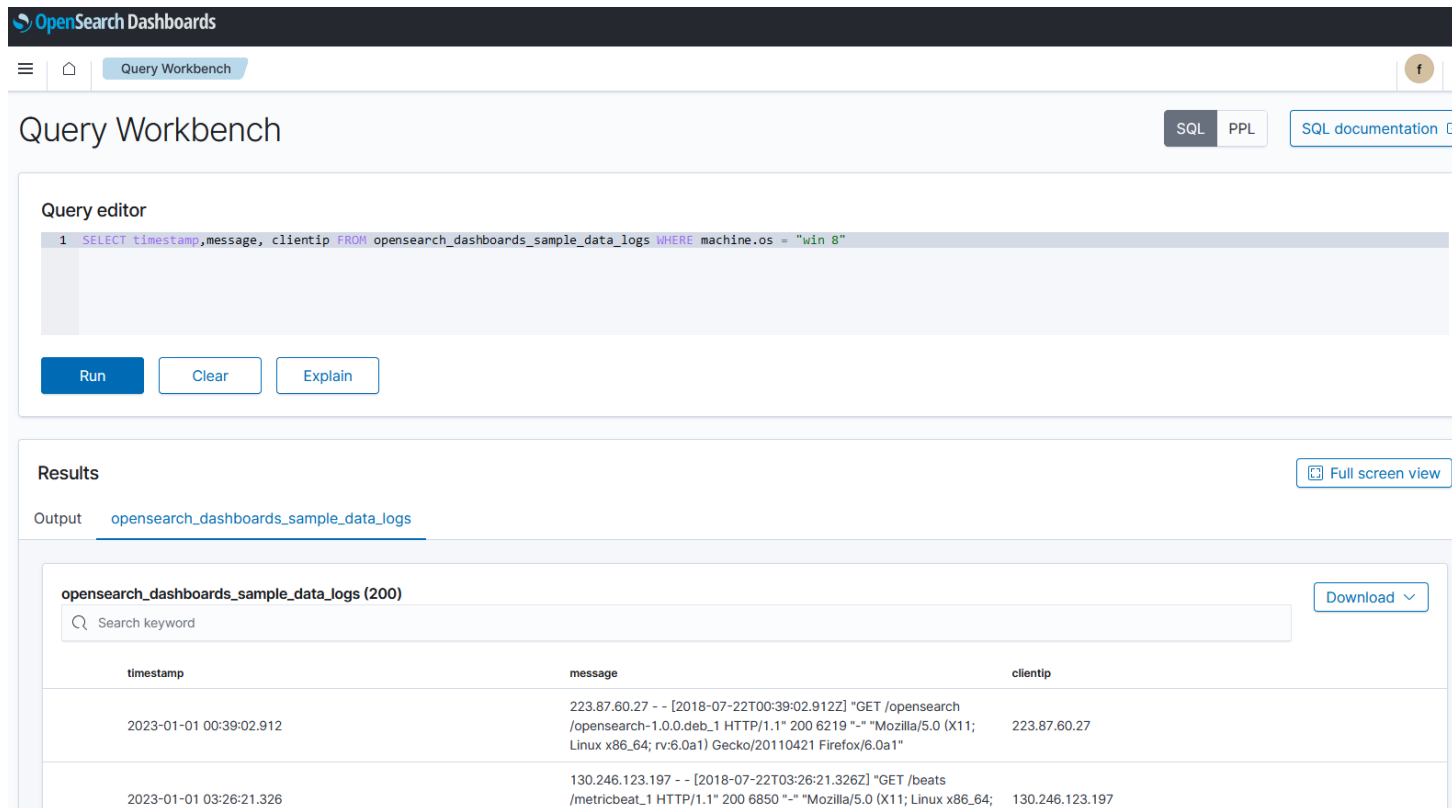
# Other features



- Query Workbench
- Reporting
- Observability: es. create Notebooks
- Admin tasks:
  - Stack Management: settings, create index patterns
  - Index Management: periodically perform certain operations (e.s. delete older indexes after a set period of days or index rollover after a certain amount of time)
  - Snapshots Management: create daily backups
  - Security: manage authentication and access control

# Query Workbench

- Use the Query Workbench to easily run on-demand SQL queries and translate SQL into its REST equivalent.



The screenshot displays the OpenSearch Dashboards Query Workbench interface. At the top, the title bar reads "OpenSearch Dashboards" and "Query Workbench". Below the title bar, there are navigation icons and a search bar. The main content area is divided into two sections: "Query editor" and "Results".

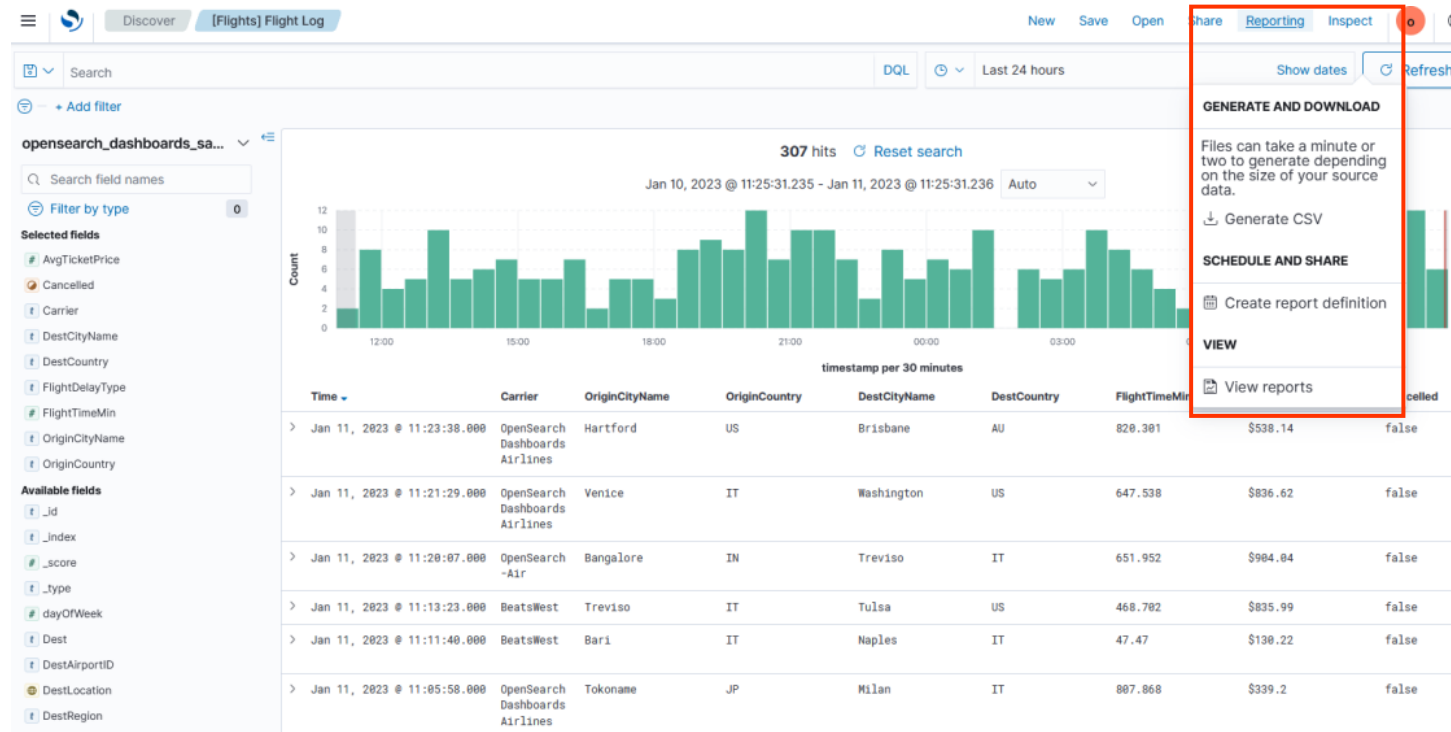
**Query editor:** Contains a SQL query: `1 SELECT timestamp,message, clientip FROM opensearch_dashboards_sample_data_logs WHERE machine.os = "win 8"`. Below the query editor are three buttons: "Run", "Clear", and "Explain".

**Results:** Shows the output of the query. The output is labeled "opensearch\_dashboards\_sample\_data\_logs". Below this, there is a search bar and a "Download" button. The results are displayed in a table with three columns: "timestamp", "message", and "clientip".

timestamp	message	clientip
2023-01-01 00:39:02.912	223.87.60.27 - - [2018-07-22T00:39:02.912Z] "GET /opensearch/opensearch-1.0.0.deb_1 HTTP/1.1" 200 6219 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"	223.87.60.27
2023-01-01 03:26:21.326	130.246.123.197 - - [2018-07-22T03:26:21.326Z] "GET /beats/metricbeat_1 HTTP/1.1" 200 6850 "-" "Mozilla/5.0 (X11; Linux x86_64;	130.246.123.197

# Reporting

- Es. Create a CSV report from your search from the Discover page:
  - Choose **Generate CSV** (save your Search first).

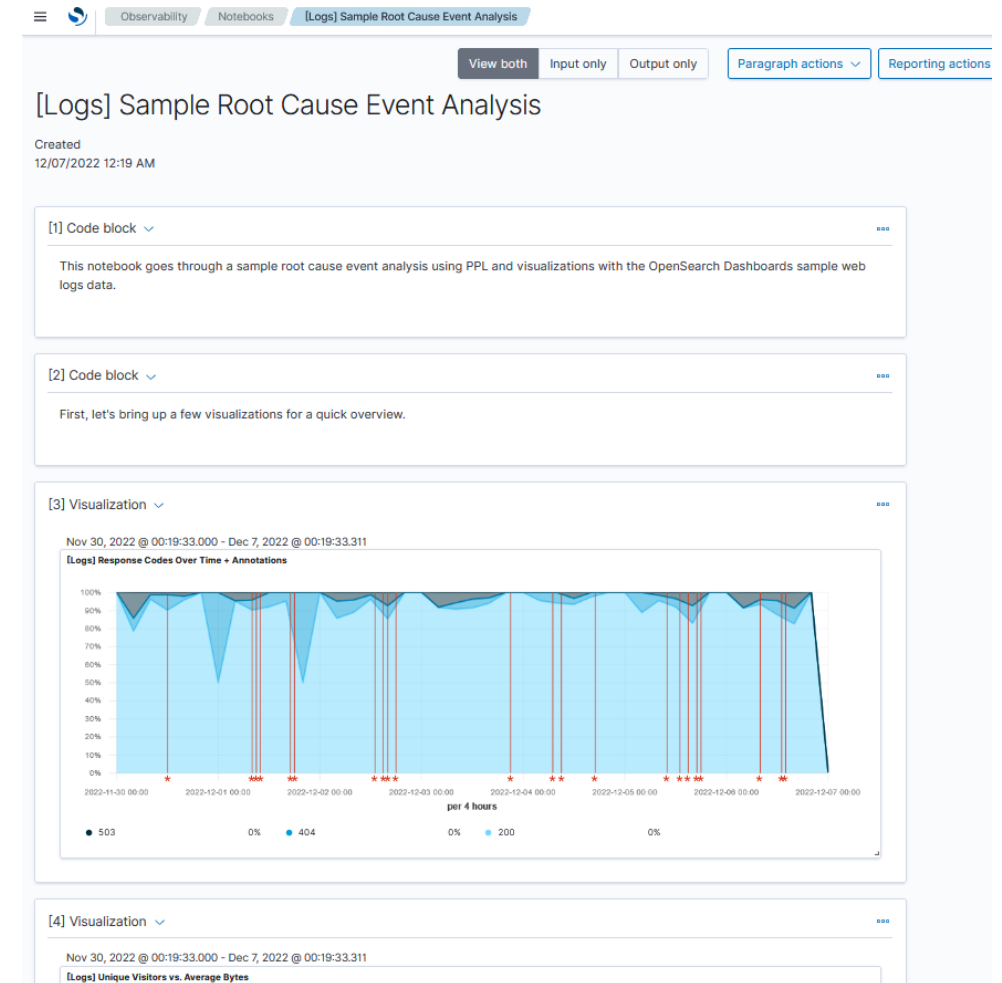


The screenshot shows the OpenSearch Discover interface for a search titled "[Flights] Flight Log". The search results are displayed as a bar chart showing the count of flights over time, with a table view below it. The table has columns for Time, Carrier, OriginCityName, OriginCountry, DestCityName, DestCountry, FlightTimeMin, and a cancelled status. A red box highlights the "Reporting" menu, which contains the following options:

- GENERATE AND DOWNLOAD**
  - Files can take a minute or two to generate depending on the size of your source data.
  - Generate CSV
- SCHEDULE AND SHARE**
  - Create report definition
- VIEW**
  - View reports

# Notebooks

- An OpenSearch Dashboards Notebook is an interface that lets you easily combine code snippets, live visualizations, and narrative text in a single interface.
- A notebook is a document composed of two elements: code blocks (Markdown/SQL/[Piped Processing Language](#) or [PPL](#)) and visualizations



The screenshot shows a notebook interface with the following components:

- Navigation:** A top bar with a hamburger menu, a search icon, and tabs for 'Observability', 'Notebooks', and the active notebook '[Logs] Sample Root Cause Event Analysis'. On the right, there are buttons for 'View both', 'Input only', 'Output only', 'Paragraph actions', and 'Reporting actions'.
- Title and Metadata:** The notebook title is '[Logs] Sample Root Cause Event Analysis'. Below it, it says 'Created 12/07/2022 12:19 AM'.
- Code Block [1]:** Contains the text: 'This notebook goes through a sample root cause event analysis using PPL and visualizations with the OpenSearch Dashboards sample web logs data.'
- Code Block [2]:** Contains the text: 'First, let's bring up a few visualizations for a quick overview.'
- Visualization [3]:** Titled '[Logs] Response Codes Over Time + Annotations'. It shows a stacked area chart from Nov 30, 2022 @ 00:19:33.000 to Dec 7, 2022 @ 00:19:33.311. The y-axis represents percentages from 0% to 100%. The x-axis is labeled 'per 4 hours'. The legend includes 503 (dark blue), 404 (light blue), and 200 (grey). Vertical red lines with asterisks indicate specific time points.
- Visualization [4]:** Titled '[Logs] Unique Visitors vs. Average Bytes'. It shows the same time range and data series as visualization [3].

# Useful links

- OpenSearch Dashboards at SDM:  
<https://opensearch-dashboards.scc.kit.edu>
- Project Documentation:  
<https://opensearch.org/docs/latest/dashboards/>