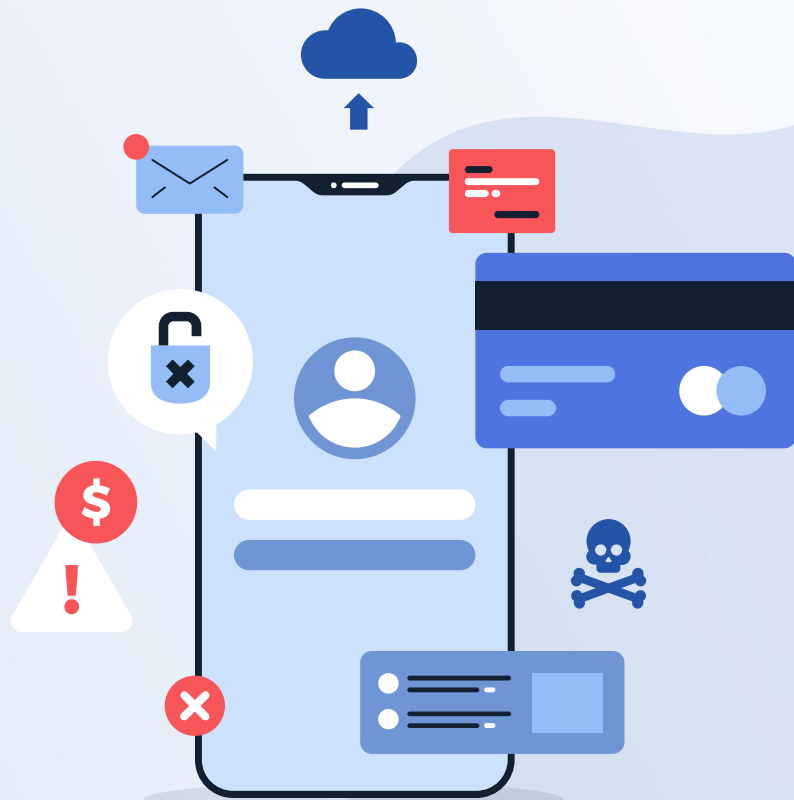


Lab 06

The First Foray Into OpenSearch



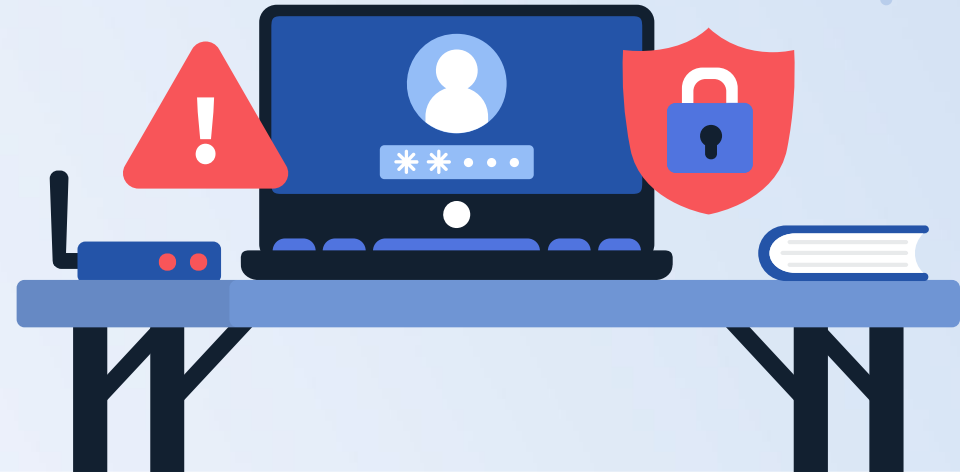
Lab Objectives

- Learn to Navigate around Opensearch
- Learn the basics of DQL
- Learn how to create a searchable index
- Find the Dev Tools Page



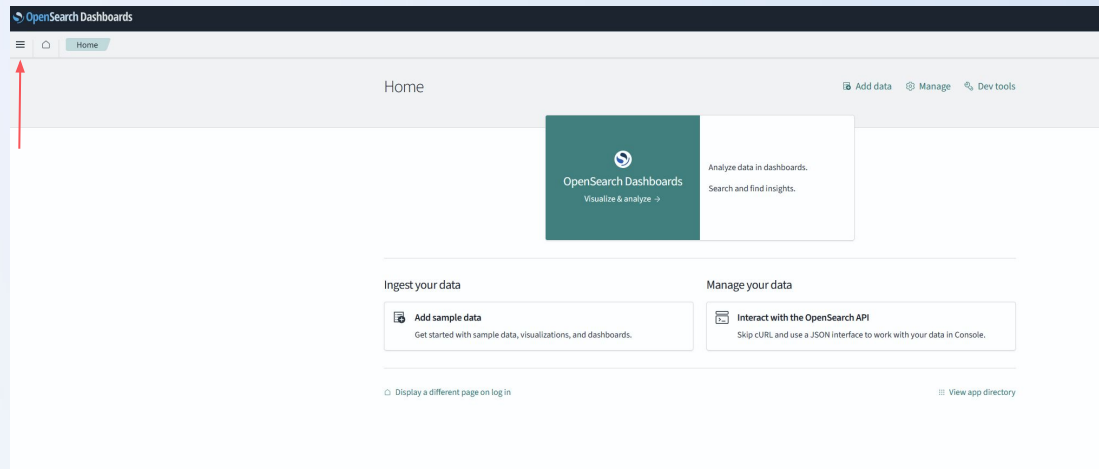
Lab Credentials

- Username: admin
- Password: Thoh8aeXuoyuuy



Log into OpenSearch

- Log into OpenSearch with the credentials that were distributed to you in class
 - <https://20.106.177.39.c.hossted.app/>
- From here, the three main options are to open OpenSearch Dashboards, add sample data, or interact with the API. For now, we will click on the menu bar on the left to expand it.



Navigation Pane

Opensearch has a variety of default options and pages. For now, let's start with the default “Discover” page. This is the page where you would search through your logs as a normal analyst.

Recently viewed

OpenSearch Dashboards

- Overview
- Discover
- Dashboards
- Visualize

Observability

- Applications
- Logs
- Metrics
- Traces
- Notebooks
- Dashboards

OpenSearch Plugins

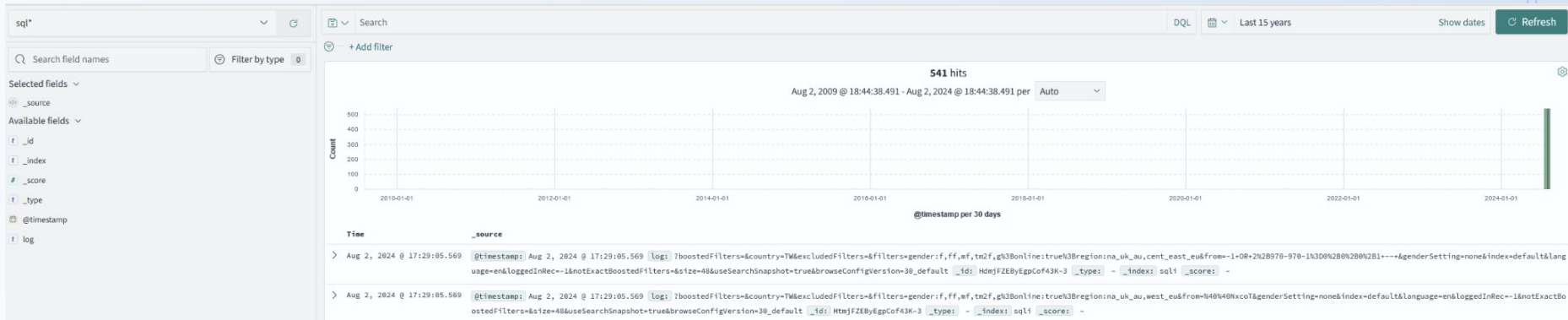
- Query Workbench
- Reporting
- Alerting
- Anomaly Detection
- Maps
- Security Analytics
- Search Relevance
- Machine Learning

Management

- Overview
- Index Management
- Snapshot Management
- Integrations
- Dashboards Management
- Data sources
- Security
- Notifications
- Dev Tools

Discover Page

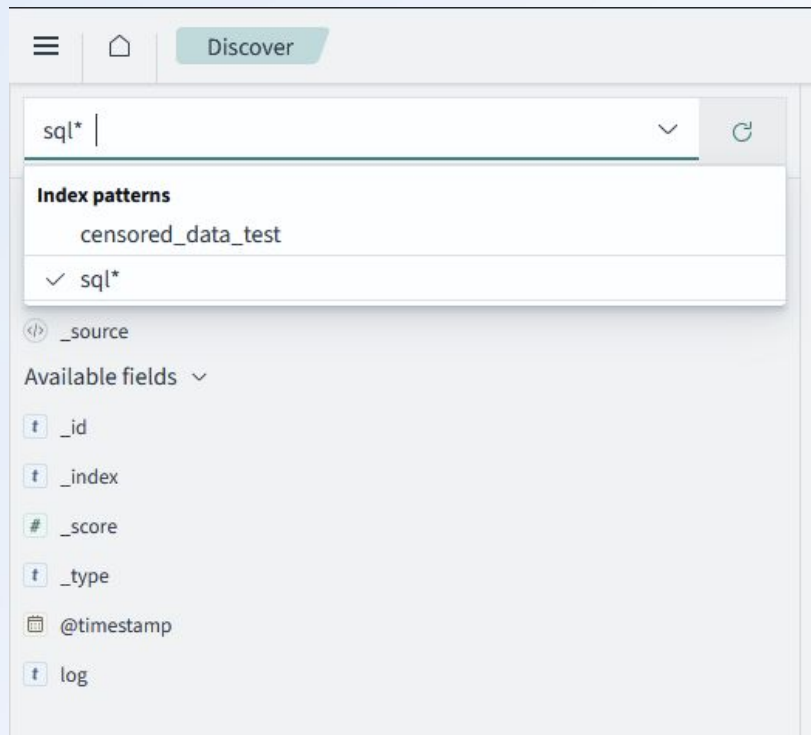
The Discover Page lets you search through logs using the Dashboard Query Language, or DQL. You also have the option to use Lucene by clicking on the “DQL” button in the search bar and disabling it. When you first open discover, you may not see any logs. Make sure the time filter is set to “Last 15 Years” in order to ensure you capture every log.



Index Patterns

In order to switch which index we are searching through, you must adjust the index pattern to match the index. We have set up this environment such that every index pattern corresponds to a single index.

Below the pattern selector, you can also see which fields have been parsed out from the logs in this index.



Example DQL

DQL is fairly easy to use. An example query you can use to filter the logs in the SQLi index is:

```
log:*na_uk*
```

This will filter the logs down to events that have the `na_uk` tag in them. Try to find two other fields in the “`log`” field to filter down on.



Index Management

In the Navigation pane on the left, click on Index Management on the bottom. From here, click on “**Indexes**”. This is the page where you can manage indexes. From here, you can see both internal/default indexes, as well as ones that have been created by the user. Let’s create an index by clicking on the Green “Create Index” button in the top right.

The screenshot displays the 'Index Management' interface. On the left, the navigation pane shows 'Index Management' expanded, with 'Indexes' selected. The main area is titled 'Indexes (39)' and features a search bar, a 'Refresh' button, an 'Actions' dropdown, and a 'Create Index' button. A table lists 39 indexes with columns for Index, Health, Managed by policy, Status, Total size, Size of primaries, Total documents, Deleted documents, Primaries, and Replicas. The table includes various internal indexes like 'test_population_data', 'tail', 'sql', and 'security-auditlog-2024.08.03', as well as user-created indexes like 'opensearch_dashboards_sample_data_logs', 'opensearch_con', 'my_test_data', and 'my_rag_test_data'. At the bottom, it shows 'Rows per page: 20' and a pagination control.

Index	Health	Managed by policy	Status	Total size	Size of primaries	Total documents	Deleted documents	Primaries	Replicas
test_population_data	Green	No	Open	416b	208b	0	0	1	1
tail	Green	No	Open	416b	208b	0	0	1	1
sql	Green	No	Open	153.1kb	76.5kb	541	0	1	1
security-auditlog-2024.08.03	Green	No	Open	4.4mb	2.1mb	1281	0	1	1
security-auditlog-2024.08.02	Green	No	Open	4.6mb	2.3mb	1310	0	1	1
security-auditlog-2024.08.01	Green	No	Open	4.8mb	2.3mb	2365	0	1	1
security-auditlog-2024.07.30	Green	No	Open	1.5mb	827.9kb	402	0	1	1
security-auditlog-2024.07.27	Green	No	Open	2.4mb	1.2mb	636	0	1	1
security-auditlog-2024.07.25	Green	No	Open	5mb	2.4mb	3227	0	1	1
security-auditlog-2024.07.24	Green	No	Open	4.9mb	2.5mb	2302	0	1	1
security-auditlog-2024.07.15	Green	No	Open	487.3kb	242.8kb	190	0	1	1
security-auditlog-2024.07.14	Green	No	Open	348.8kb	112kb	56	0	1	1
security-auditlog-2024.06.19	Green	No	Open	2mb	1016.4kb	593	0	1	1
security-auditlog-2024.06.17	Green	No	Open	1mb	560.5kb	742	0	1	1
security-auditlog-2024.06.16	Green	No	Open	4.6mb	2.2mb	2287	0	1	1
security-auditlog-2024.06.15	Green	No	Open	5.2mb	3.1mb	3055	0	1	1
opensearch_dashboards_sample_data_logs	Green	No	Open	18.8mb	9.4mb	14074	0	1	1
opensearch_con	Green	No	Open	59.1kb	29.5kb	2	0	1	1
my_test_data	Green	No	Open	91.7kb	45.8kb	6	0	1	1
my_rag_test_data	Green	No	Open	51.6kb	25.8kb	1	0	1	1

Index Creation

From this page, you can create your index. For now, let's just name the index after either your name or handle. Read through the rest of the options. We won't adjust anything here since this is just an exercise in creating the index. Once done, hit "Create" in the bottom right. You may have to scroll down for this to be visible.

index name

ksingh

Must be in lowercase letters. Cannot begin with underscores or hyphens. Spaces, commas, and characters like " " < > & " are not allowed.

index alias - optional

Allow this index to be referenced by existing aliases or specify a new alias.

Select aliases or specify new aliases.

Index settings

Number of primary shards

Specify the number of primary shards for the index. Default is 1. The number of primary shards cannot be changed after the index is created.

1

Number of replicas

Specify the number of replicas each primary shard should have. Default is 1.

1

Refresh interval

Specify how often the index should refresh, which publishes the most recent changes and make them available for search. Default is 1 second.

1s

> Advanced settings

Index mapping - optional

Define how documents and their fields are stored and indexed. [Learn more](#)

Mappings and field types cannot be changed after the index is created.

Visual Editor

JSON Editor

You have no field mappings.

Add new field

Add new object

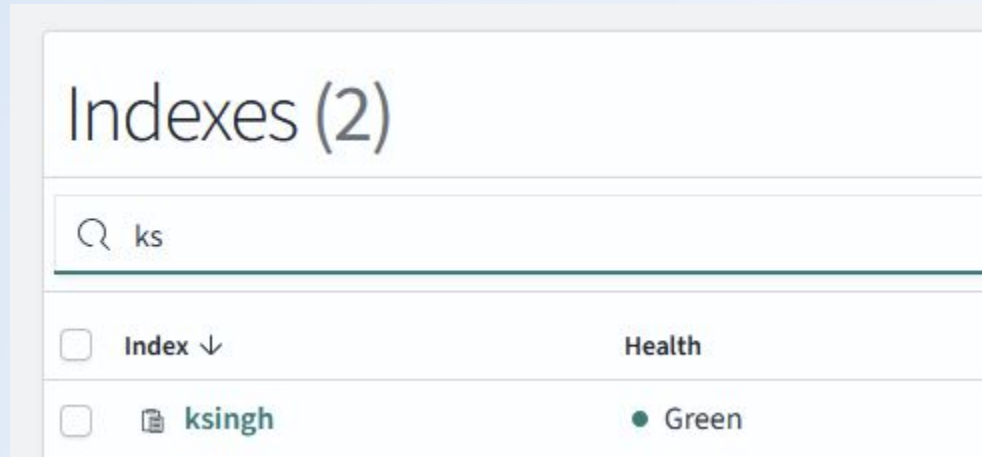
Cancel

Create

Indexes

You will be redirected back to the original Indexes page after hitting create. If you don't instantly see the index you made, you can search for it or browse through the pages to find it.

Go ahead and click on your index.



Personal Index

This page gives you a total overview of the index, including the size, the number of documents(or logs/events), allow you to make aliases and adjust how many replicas you need, and other statistics.

ksingh

Overview

Index name ksingh	Health ● Green	Status Open
Creation date 8/2/2024, 7:17:42 PM	Total size 416b	Size of primaries 208b
Total documents 0	Deleted documents 0	Primaries 1
Replicas 1	Index blocks -	Managed by policy -

Settings

Mappings

Alias

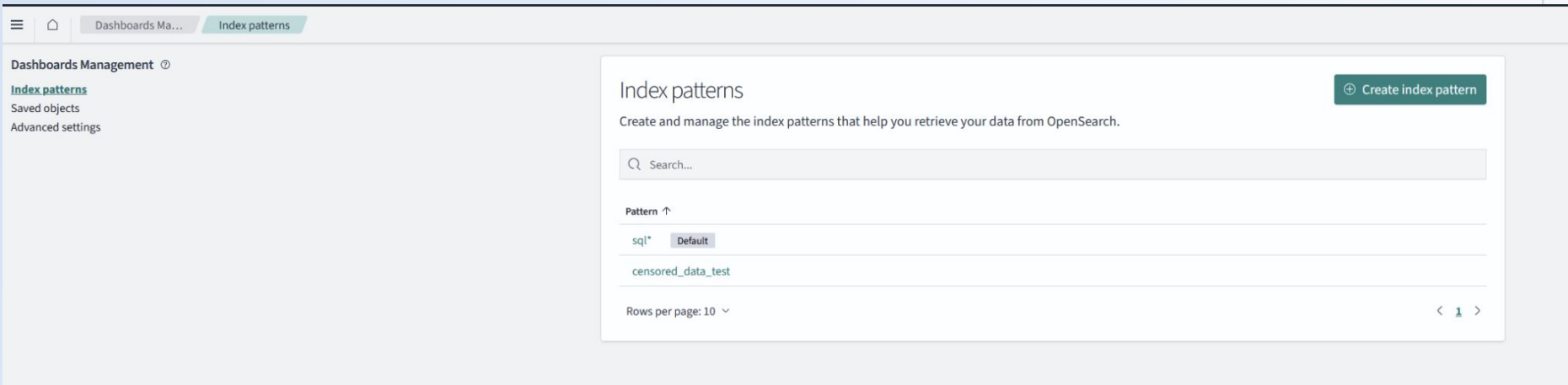
Index settings

Number of primary shards Specify the number of primary shards for the index. Default is 1. The number of primary shards cannot be changed after the index is created.	1
Number of replicas Specify the number of replicas each primary shard should have. Default is 1.	<input type="text" value="1"/>
Refresh interval Specify how often the index should refresh, which publishes the most recent changes and make them available for search. Default is 1 second.	<input type="text" value="1s"/>

> Advanced settings

Index Patterns

In order to actually search through indexes that have been created an **index pattern** must be created. Open up the Navigation Pane on the left, and go down to Dashboards Management. From here, click on Index Patterns. Hit the Green “Create Index Pattern” button.



Create Index Pattern

From here, we can type out a index pattern name to select one or multiple indexes. You can either type in the full name of an index, or use asterisks to select multiple. For instance, if you wanted to look through all of the security audit logs, typing in:

`security-auditlog*`

Would net you all of the logs into one index pattern for universal searching. For now, just typing in the name of the index you just created.

Click on “Next Step” when done.

Step 1 of 2: Define an index pattern

Index pattern name

ksingh

Use an asterisk (*) to match multiple indices. Spaces and the characters \

☐ Include system and hidden indices

✓ Your index pattern matches 1 source.

ksingh

Rows per page: 10

Index pattern name

security*

Use an asterisk (*) to match multiple indices. Spaces and the

☐ Include system and hidden indices

✓ Your index pattern matches 13 sources.

security-auditlog-2024.06.15
security-auditlog-2024.06.16
security-auditlog-2024.06.17
security-auditlog-2024.06.19
security-auditlog-2024.07.14
security-auditlog-2024.07.15
security-auditlog-2024.07.24
security-auditlog-2024.07.25
security-auditlog-2024.07.27
security-auditlog-2024.07.30

Rows per page: 10

Create Index Pattern

Since we do not have any logs in this index, and therefore any timestamp fields to pull from, this next page will be blank. Hitting Create Index Pattern will send you to the details page about the index pattern.

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.

[Read documentation](#)

Step 2 of 2: Configure settings

Specify settings for your **ksingh** index pattern.

The indices which match this index pattern don't contain any time fields.

> [Show advanced settings](#)

< Back

Create index pattern

Index Pattern Details

The Index Patterns page lets you see what fields are being parsed out. For this index, we only have the default fields, identified by the “_” at the beginning of the field name.

ksingh

★ ↺ 🗑

This page lists every field in the **ksingh** index and the field's associated core type as recorded by OpenSearch. To change a field type, use the OpenSearch [Mapping API](#) 📄

Fields (5)

Scripted fields (0)

Source filters (0)

🔍 Search

All field types ▾

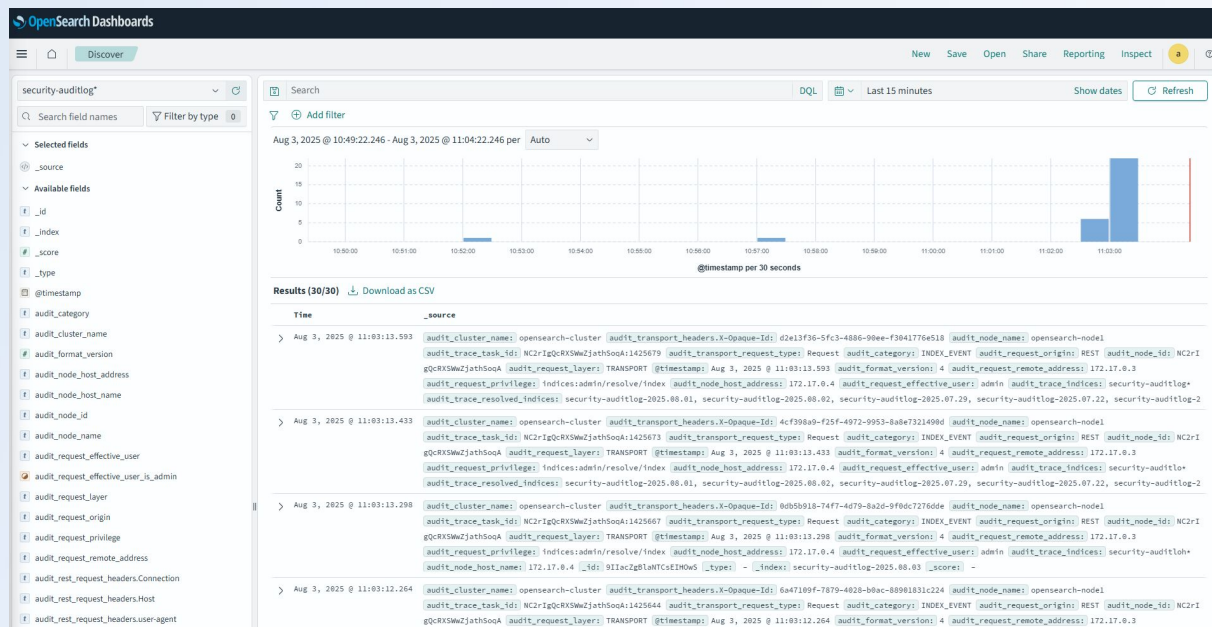
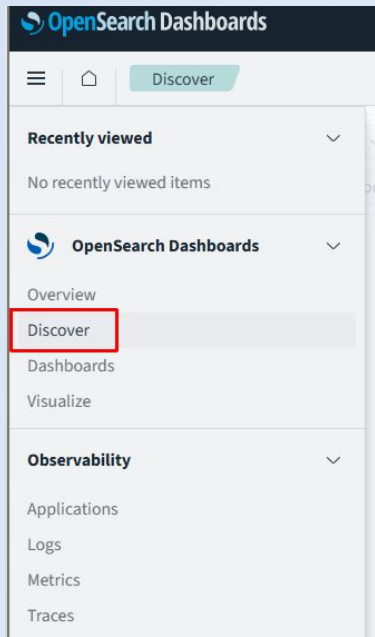
Name	Type	Format	Searchable	Aggregatable	Excluded
_id	string		•	•	✎
_index	string		•	•	✎
_score	number				✎
_source	_source				✎
_type	string				✎

Rows per page: 10 ▾

◀ 1 ▶

Search the Index Pattern

Navigate to **Discover** and select your index pattern in the top left, adjust the time (optional), and search.



Lab End

