Lab 06

The First Foray Into OpenSearch

Lab Objectives

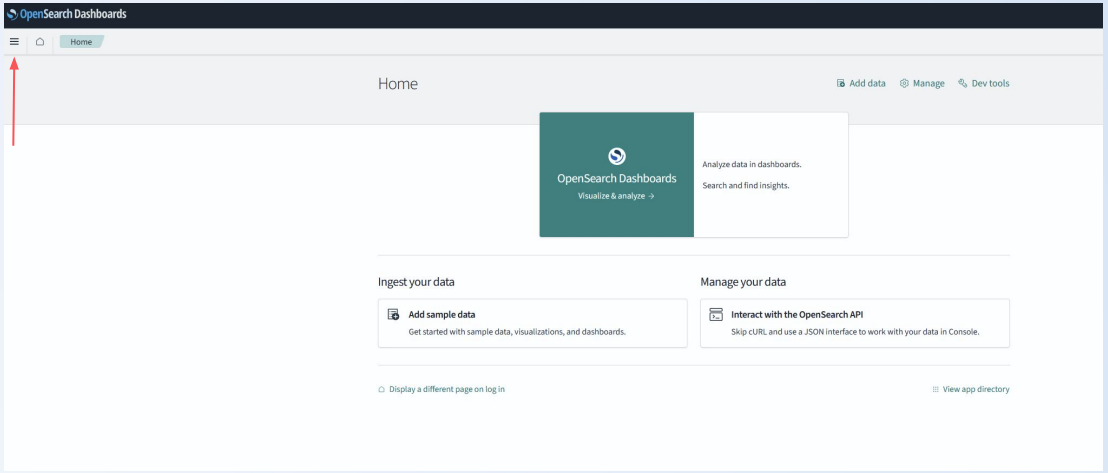
- Learn to Navigate around Opensearch
- Learn the basics of DQL
- Learn how to create a searchable index
- Find the Dev Tools Page

Lab Credentials

- Username: admin
- Password: Thoh8aeXuoyuuy

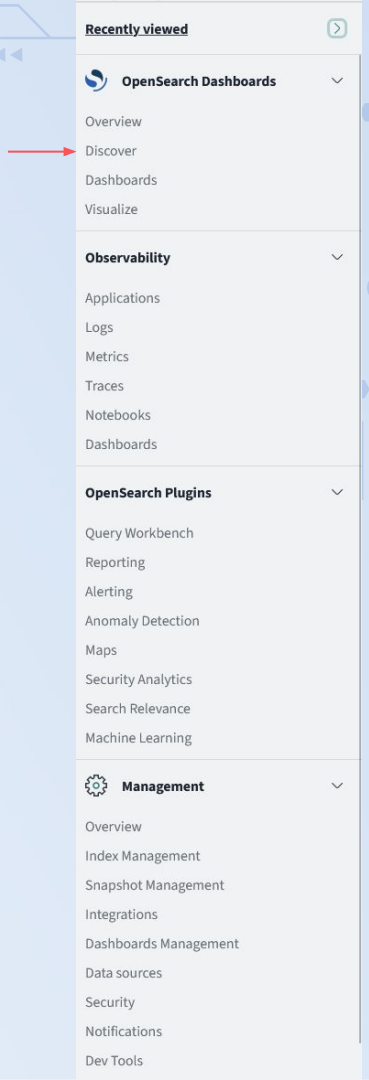
Log into OpenSearch

- 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.



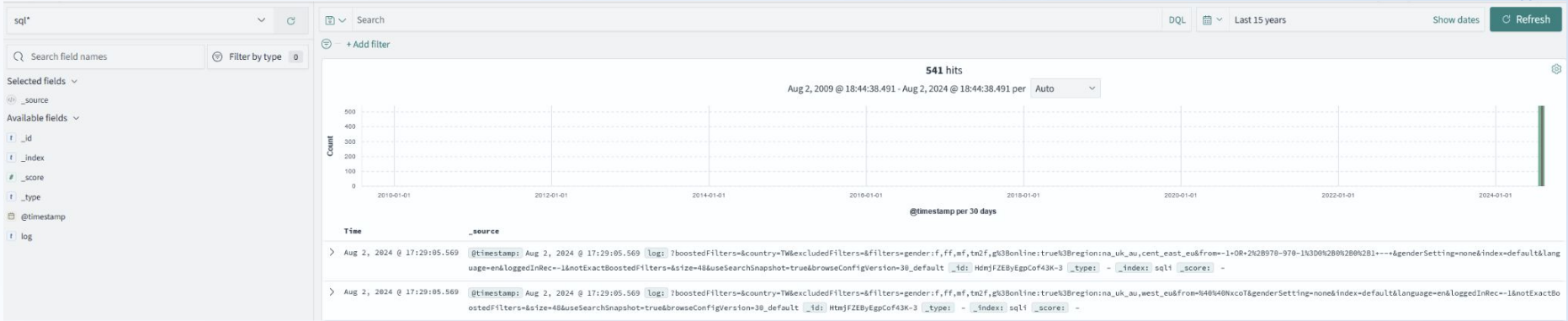
Navigation Pane

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.



Discover Page

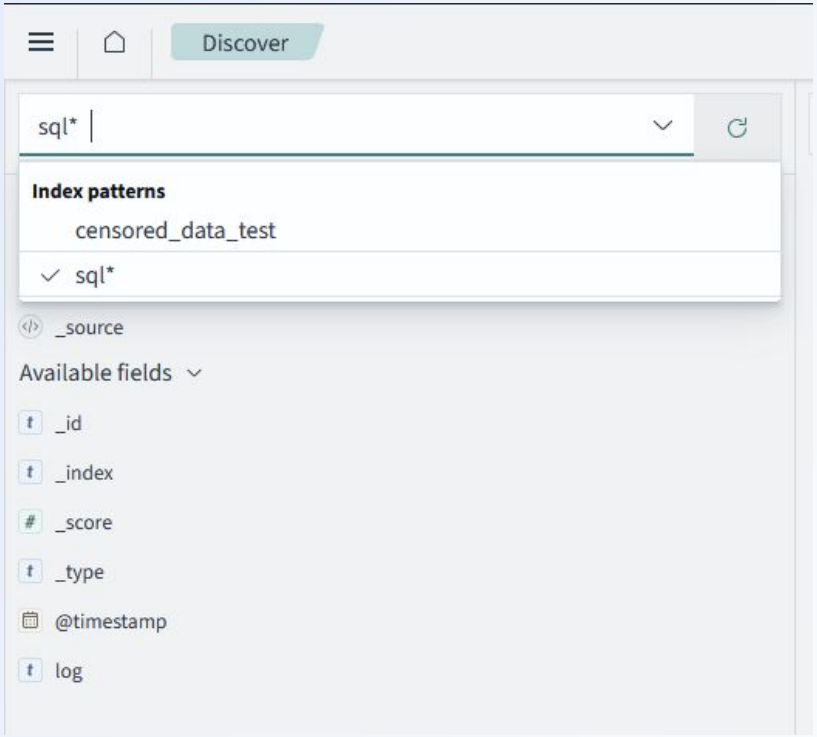
The Discover Page lets you search through logs using the Dashboard Query Language, or DQL. You also have the option to use Lucene by clicking on the “DQL” button in the search bar and disabling it. When you first open discover, you may not see any logs. Make sure the time filter is set to “Last 15 Years”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

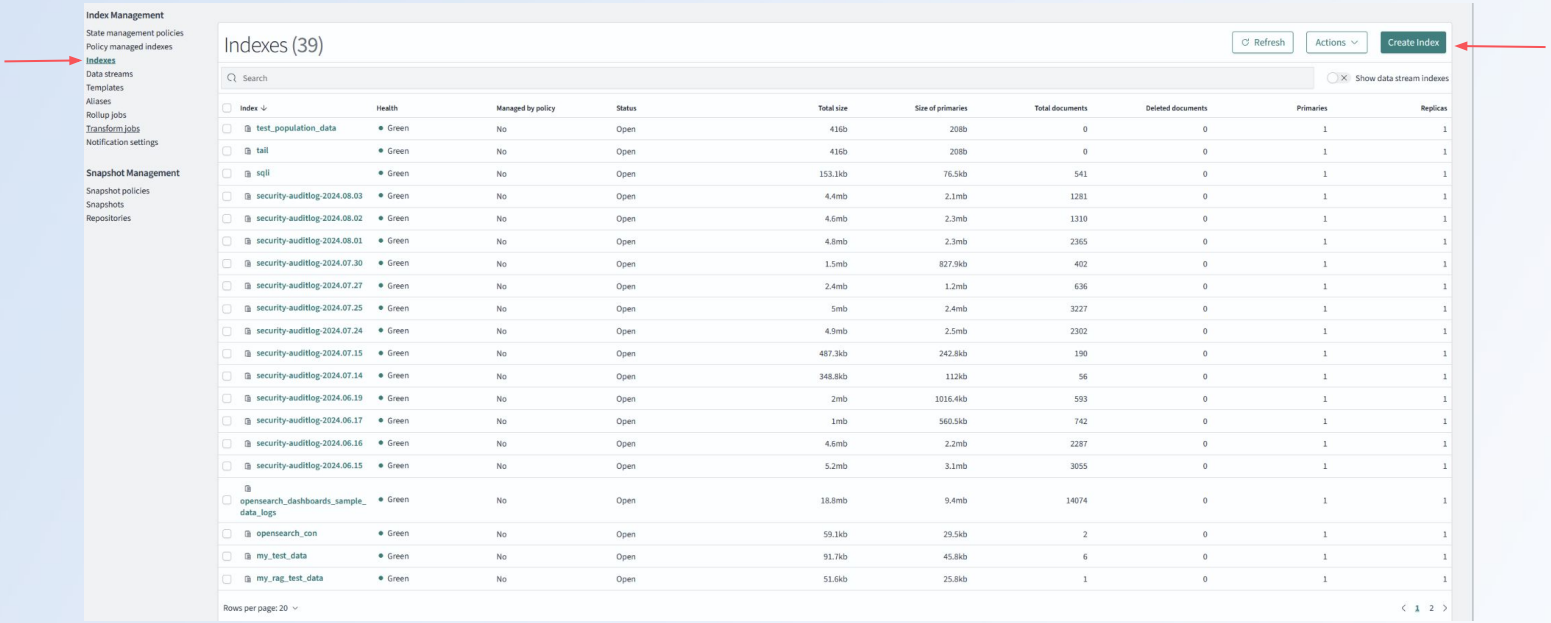
DQL is fairly easy to use. An example query you can use to filter the logs in the SQLi index is:

```
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.

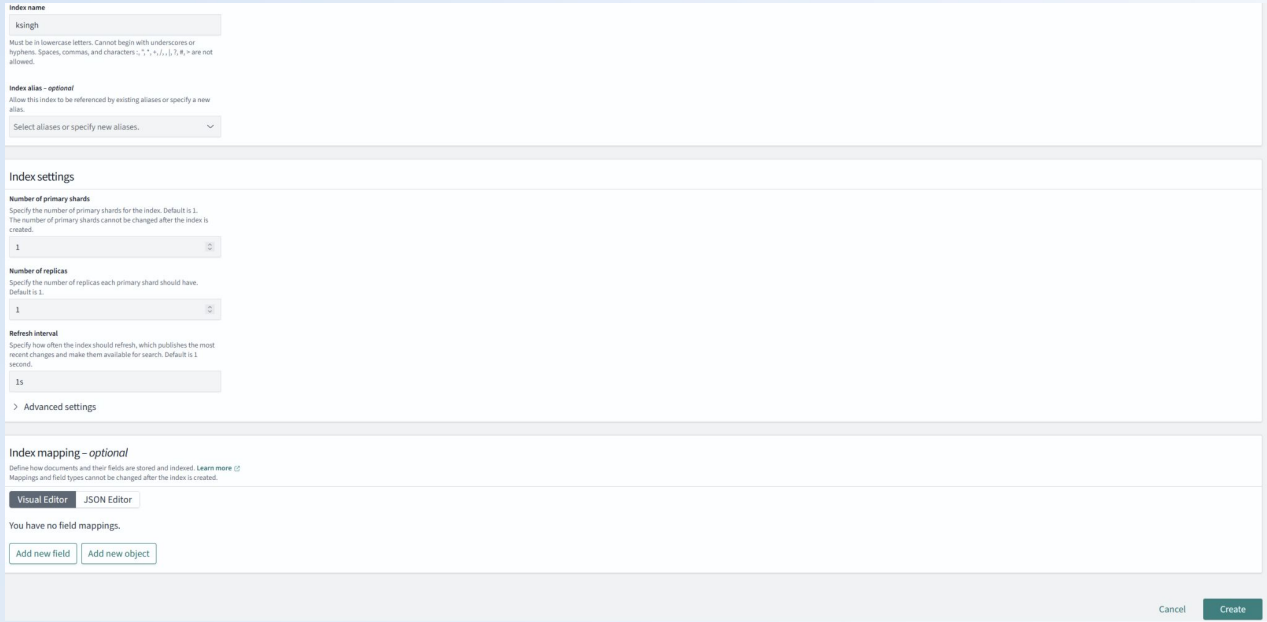
Index Management

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.



Index Creation

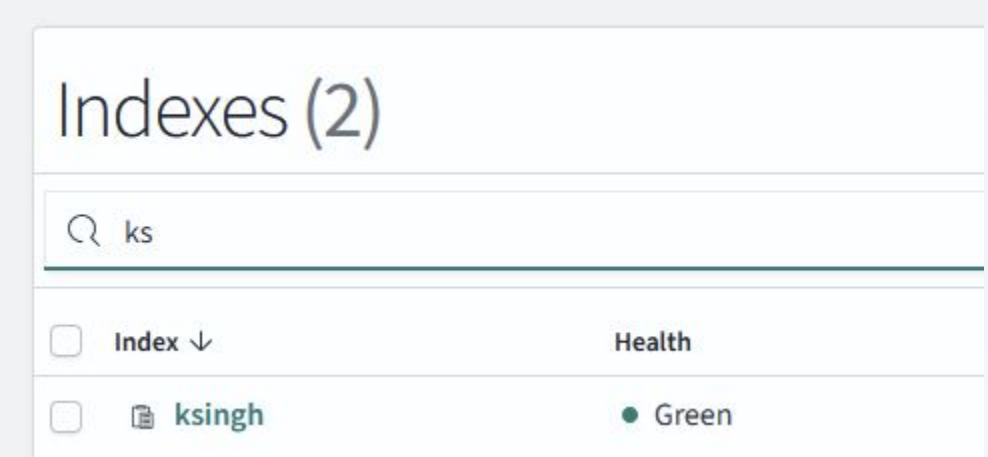
From this page, you can create your index. For now, let's just name the index after either your name or handle. Read through the rest of the options. We won't adjust anything here since this is just an exercise in creating the index. Once done, hit "Create" in the bottom right. You may have to scroll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



Indexes

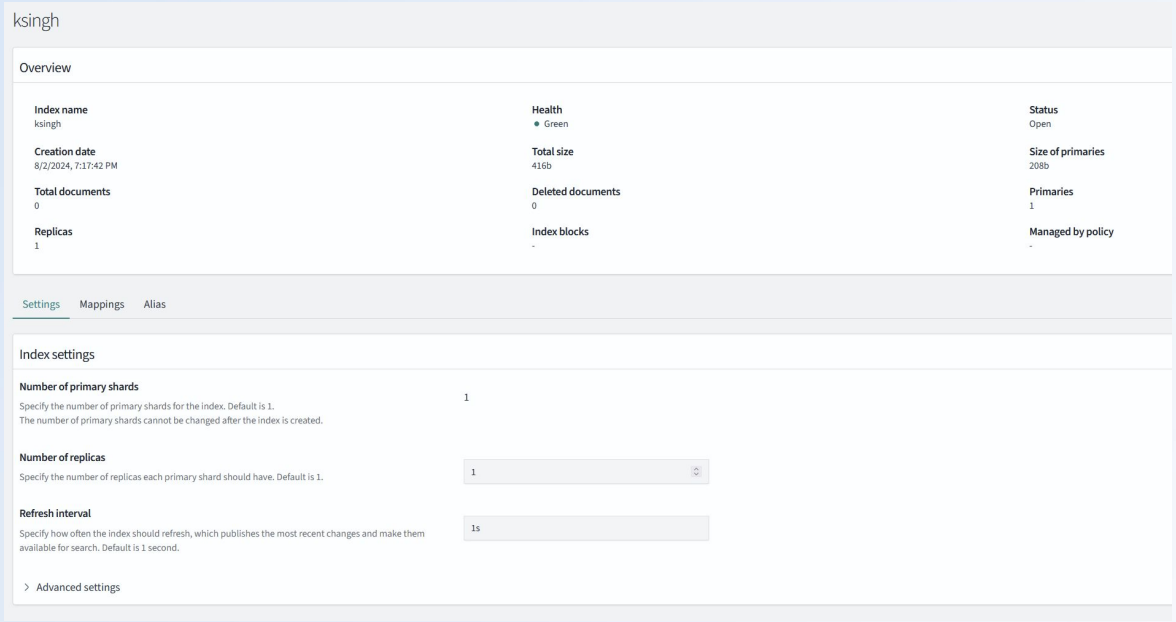
You will be redirected back to the original Indexes page after hitting create. If you don't instantly see the index you made, you can search for it or browse through the pages to find it.

Go ahead and click on your index.



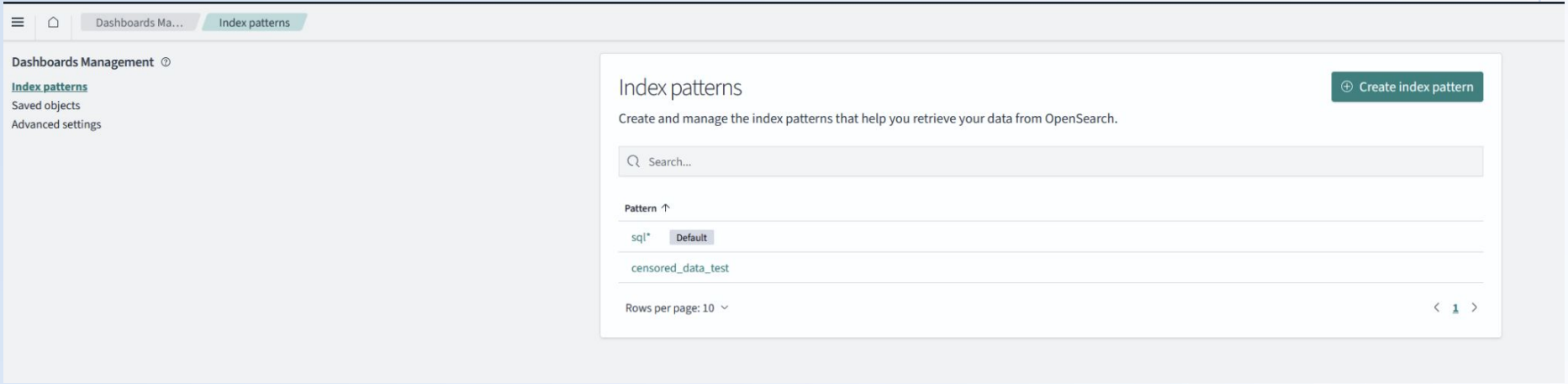
Personal Index

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.



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.



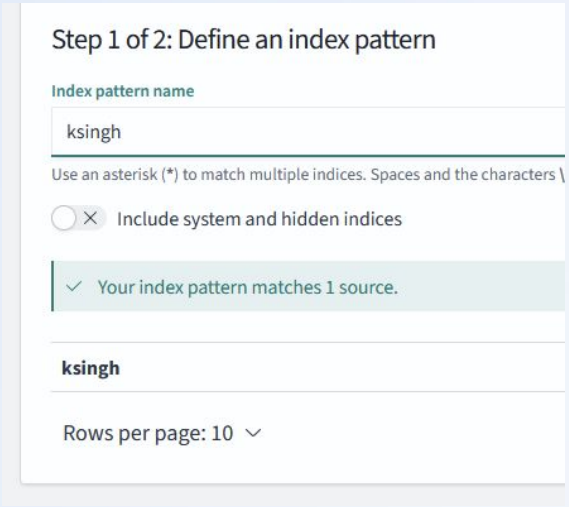
Create Index Pattern

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.

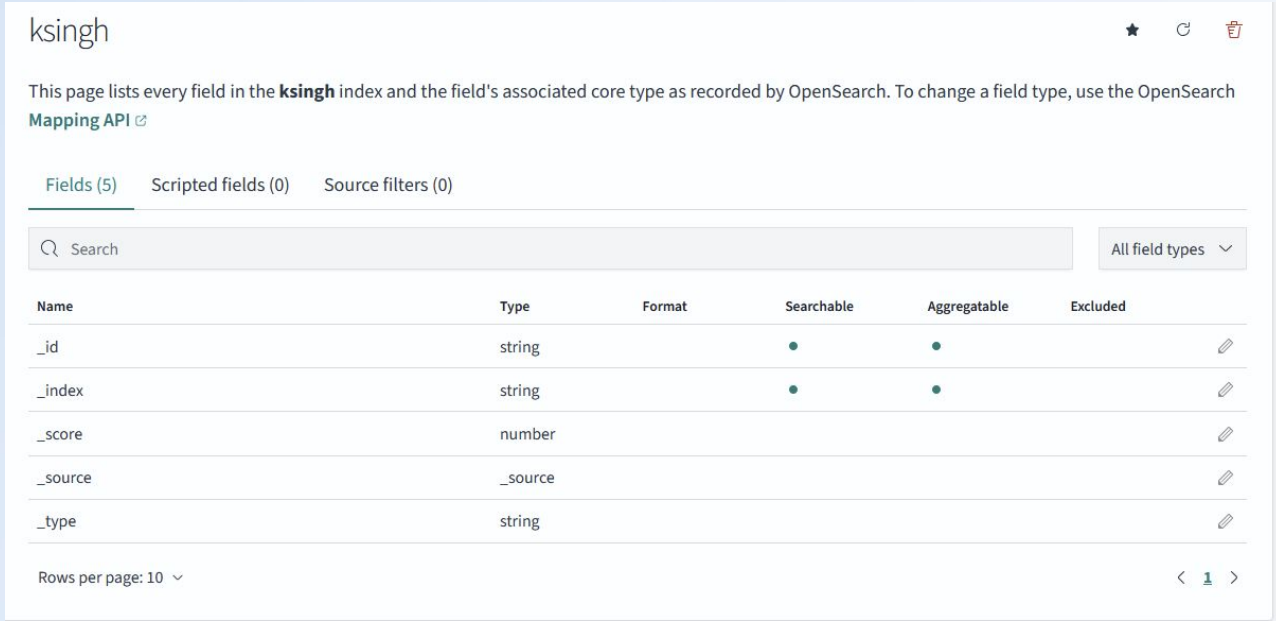


Create Index Pattern

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.

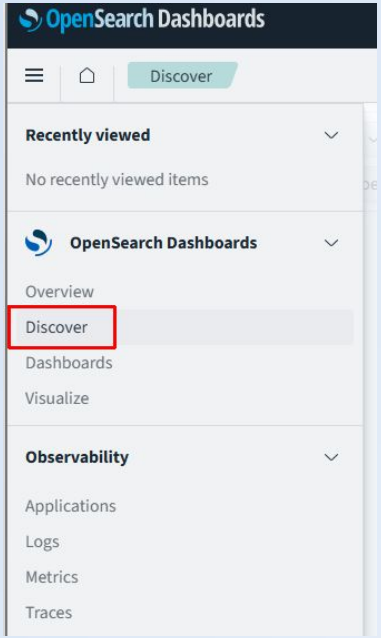
Index Pattern Details

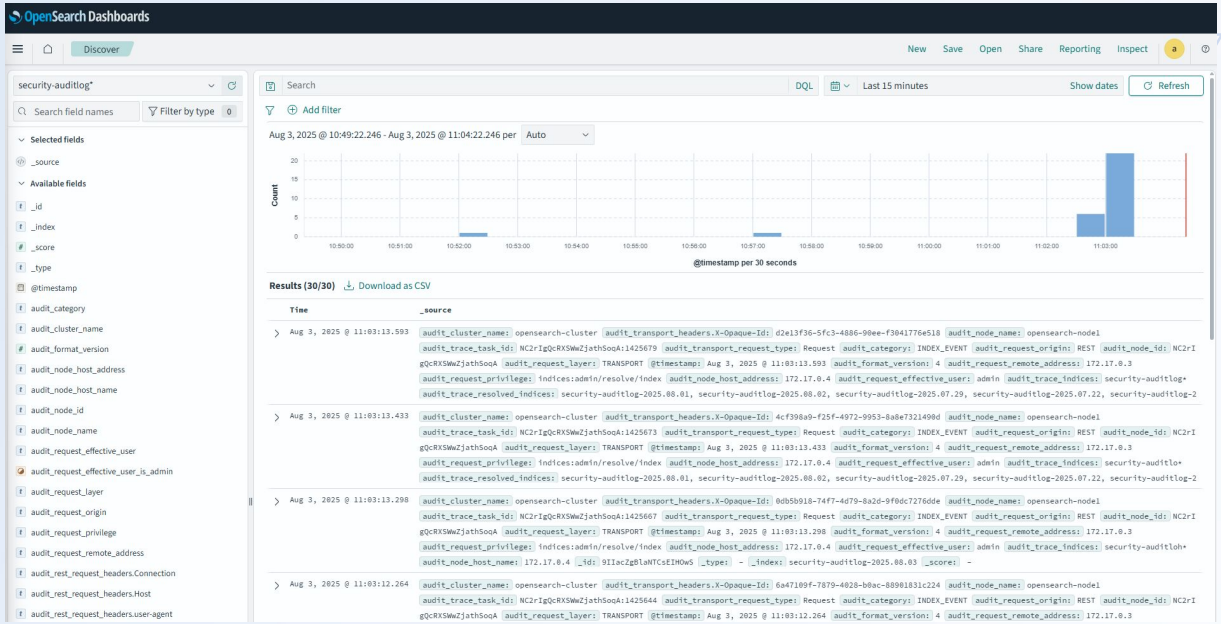
The Index Patterns page lets you see what fields are being parsed out. For this index, we only have the default fields, identified by the "_" at the beginning of the field name.



Search the Index Pattern

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





Lab End