

# SOC Workshop

David Crooks

UKRI STFC

EGI CSIRT/IRIS Security team

[david.crooks@stfc.ac.uk](mailto:david.crooks@stfc.ac.uk)



# Goals

- *Gain experience with Portainer container orchestration*
  - *Used by sandbox*
- Gain experience in a sandbox SOC environment
- Generate traffic and examine the logs created as a result
  - Connection
  - File
- Create a MISP event based on these findings

# Preamble

- One issue when deploying network monitoring as we have discussed: Volume of information
- Very easy when presented with 10's of Gbs of data to be overwhelmed
  - My experience!
  - Wait, I didn't know that happened, is that normal!? (Probably!)
- Intention of the environment we will use is to create a quiet SOC sandbox based on the principles we have discussed

# Environment design

- Everything is on a private network
- Small amount of traffic: lets us focus on things that we trigger
- Start with an “internal” client connected to an “external” webserver

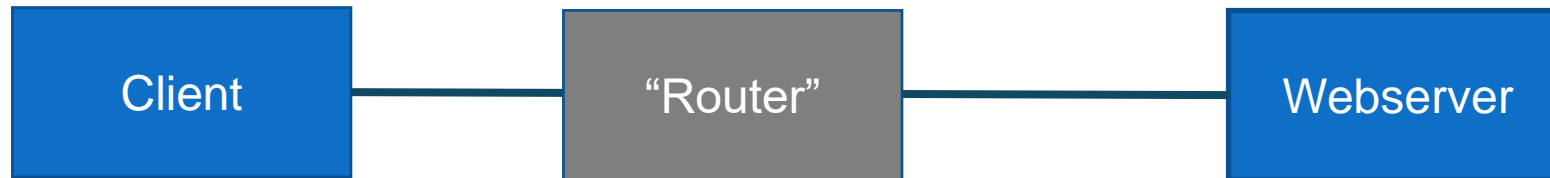
# Environment logical design

- Start with an “internal” client connected to an “external” webserver



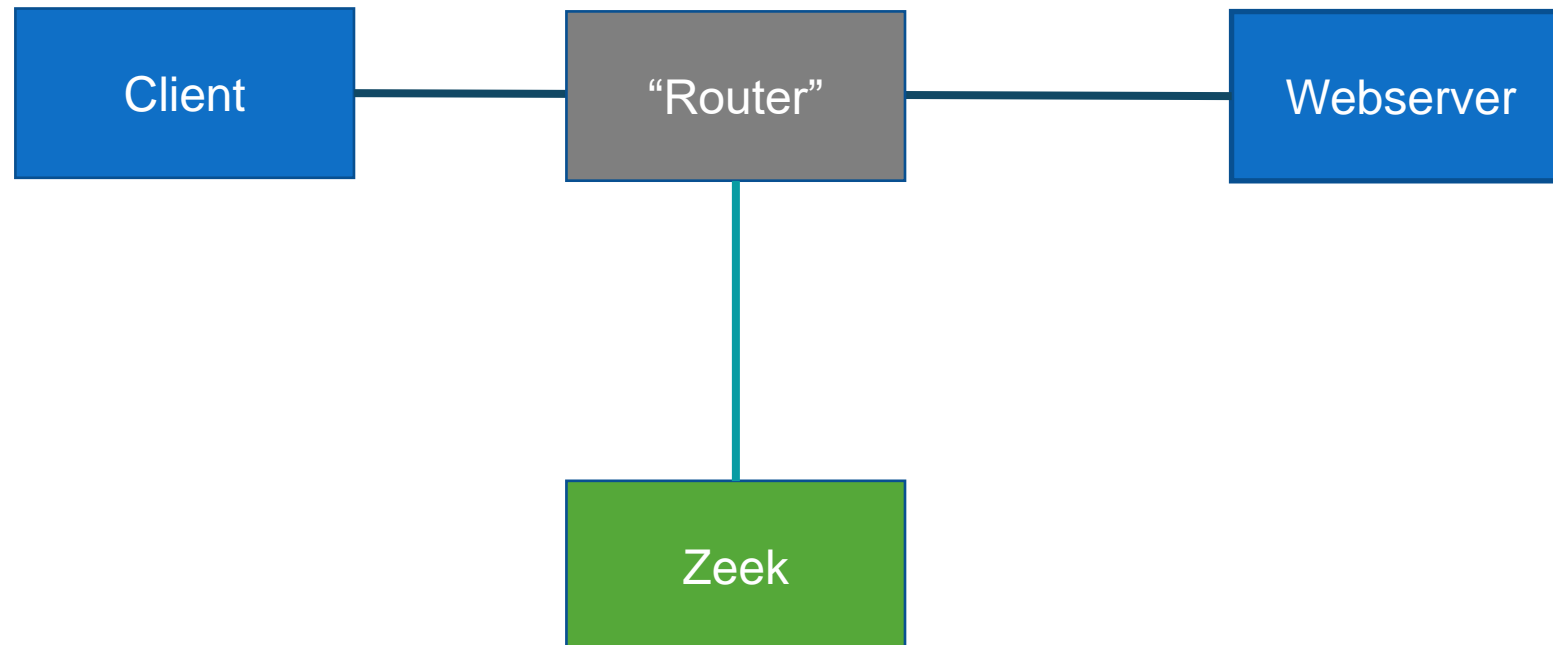
# Environment design

- Implement a router between them: the “edge router”



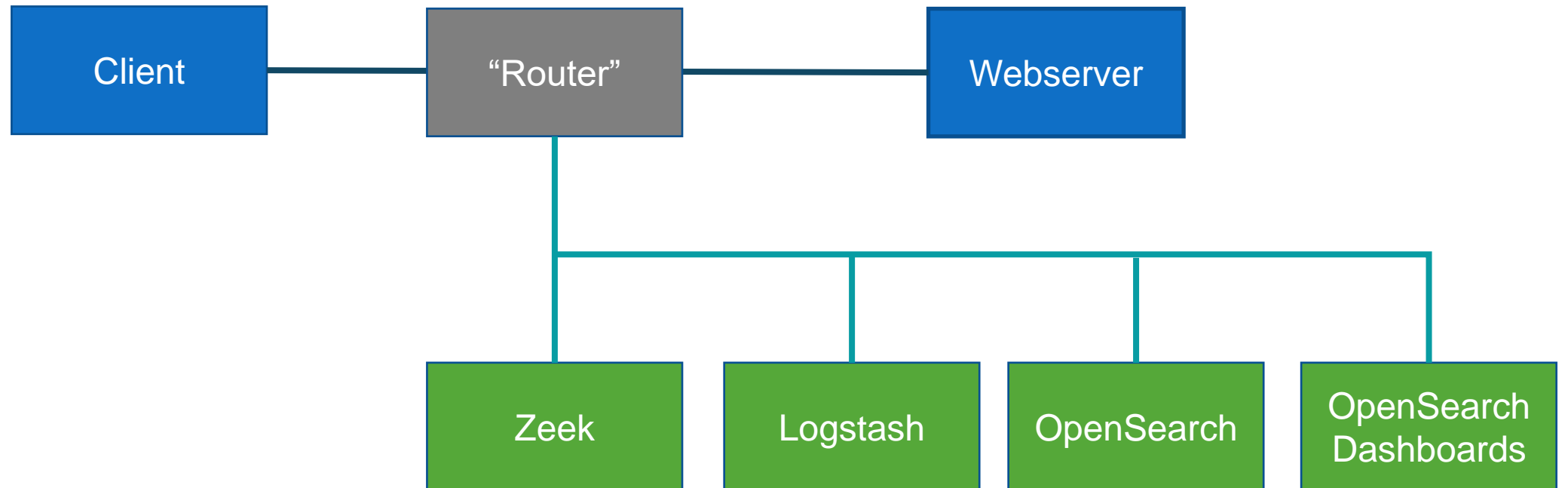
# Environment design

- Tap traffic crossing router with zeek



# Environment design

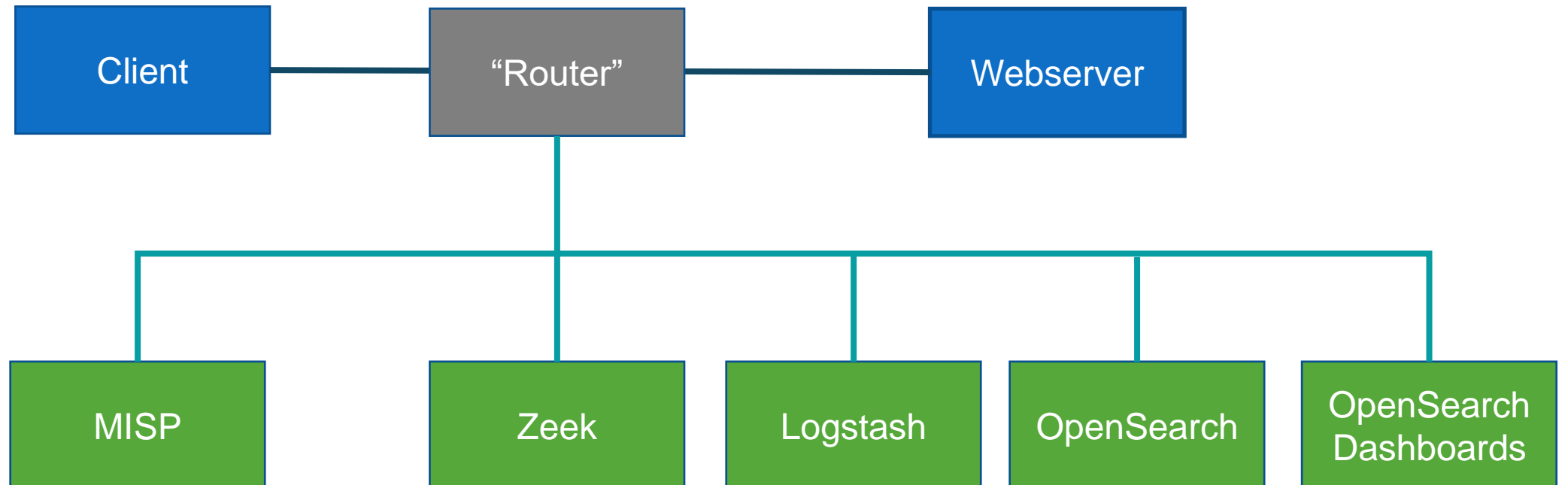
- Deploy logstash, Opensearch and Opensearch Dashboards





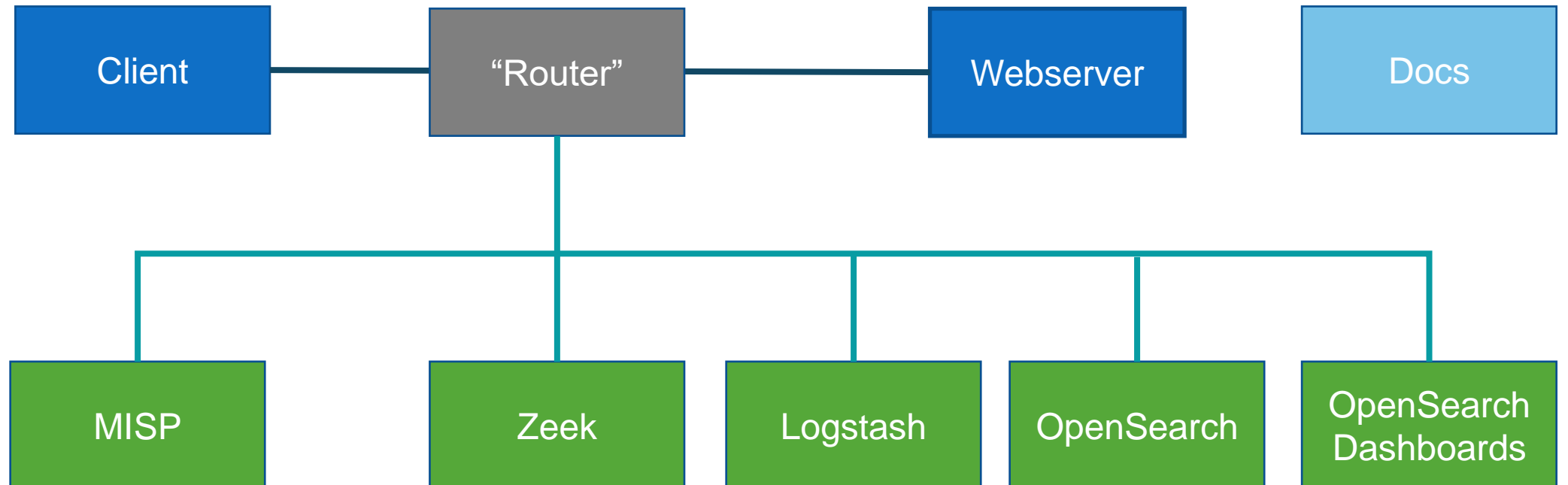
# Environment design

- Add MISP instance



# Environment design

- Documentation server for exercise details



# Before we start

- Talking to a couple of people over lunch, I forgot to mention:
- Zeek runs very well on a Raspberry Pi to monitor a 1Gb/s connection
  - If you wanted to monitor your home network
- I also commend to you the Corelight@Home program
  - <https://corelight.com/blog/corelight-at-home>

# Setup [1]

- We have enough instances for you to work in pairs

`csc-2023-07.cern.ch`

`csc-2023-08.cern.ch`

...

`csc-2023-19.cern.ch`

- (with some spares)

# Setup [2]

- **Note**
- These instances are **not** available publicly: we'll use proxying through `lxplus`
  - Hence need for one CERN person per pair

# Setup [3]

- Please visit <https://cern.ch/scsc-soc> and select an environment
- We'll pause to make sure that everyone has one



# Setup [4] (Exercise Zero)

- Once you have your machine, need to configure SSH tunnel and web browser
- Tunnel (can be a port other than 50000 but pick a high number)
  - `ssh -D 50000 -q -C -N lxpplus`
- Then in your web browser, find the proxy settings, and set a manual proxy to `localhost:50000`

# Setup [5]

- Visit <https://csc-2023-XY>
- Contains links and credentials to the relevant web interfaces
- The contents of the documentation (without the links or credentials) can be found:
  - [www.github.com/drmcrooks/pocketsoc-ng-docs](https://www.github.com/drmcrooks/pocketsoc-ng-docs)



# Portainer

- Portainer is used as the orchestrator for this environment



Log in to your account

Welcome back! Please enter your details

Username

Password



Login

# Portainer

- Main interface

🌿 Environments

! Click on an environment to manage

🔄 Refresh

🔍 Search by name, group, tag, status, URL...

Platform



Status



Tags



Groups



Clear all





local up 2022-06-15 09:52:06

☰ 2 stacks 🌐 15 containers - 🟢 15 🔴 0 / 🟢 2 🟡 0 🗄️ 12 volumes 📄 20 images

📊 0.2 GB

# Portainer

Environment	local  4  8.2 GB - Standalone 20.10.17
URL	/var/run/docker.sock
Tags	-



2

Stacks



15

Containers

 2 healthy  15 running  
 0 unhealthy  0 stopped



20

Images

 13.4 GB



12


Volumes






6

Networks

# Portainer

 Stacks

 Remove  + Add stack

 Search...

Name ↓  
Filter ▼







































































**pocketsoc-ng**

pocketsoc-ng-portainer

# Portainer

▶ Start ■ Stop 🛑 Kill ↺ Restart || Pause ▶ Resume 🗑️ Remove

🔍 Search...

<input type="checkbox"/>	Name	State Filter ▼	Quick Actions	Stack	Image	Created	IP Address	Published Ports
<input type="checkbox"/>	misp	healthy	    	pocketsoc-ng	pocketsoc-ng_misp	2022-06-13 16:49:58	172.20.0.13	<a href="#">50000:50000</a> <a href="#">8080:8080</a>
<input type="checkbox"/>	misp-modules	healthy	    	pocketsoc-ng	ghcr.io/nukib/misp-modules:latest	2022-06-13 16:49:51	172.20.0.2	-
<input type="checkbox"/>	logstash-zeek	running	    	pocketsoc-ng	pocketsoc-ng_logstash-zeek	2022-06-13 16:49:51	172.20.0.4	<a href="#">5044:5044</a>
<input type="checkbox"/>	misp-mysql	running	    	pocketsoc-ng	maxmind/mysql	2022-06-13 16:49:51	172.20.0.10	-
<input type="checkbox"/>	misp-redis	running	    	pocketsoc-ng	redis	2022-06-13 16:49:51	172.20.0.9	-
<input type="checkbox"/>	sshserver	running	    	pocketsoc-ng	pocketsoc-ng_sshserver	2022-06-13 16:49:51	172.18.0.4	-
<input type="checkbox"/>	client	running	    	pocketsoc-ng	pocketsoc-ng_client	2022-06-13 16:49:51	172.18.0.5	-
<input type="checkbox"/>	opensearch-node1	running	    	pocketsoc-ng	pocketsoc-ng_opensearch-node1	2022-06-13 16:49:51	172.20.0.3	<a href="#">9200:9200</a> <a href="#">9600:9600</a>
<input type="checkbox"/>	opensearch-dashboards	running	    	pocketsoc-ng	pocketsoc-ng_opensearch-dashboards	2022-06-13 16:49:51	172.20.0.7	<a href="#">5601:5601</a>
<input type="checkbox"/>	reverse-proxy	running	    	pocketsoc-ng	pocketsoc-ng_reverse-proxy	2022-06-13 16:49:51	172.20.0.6	<a href="#">443:443</a> <a href="#">8443:8443</a>
<input type="checkbox"/>	opensearch-node2	running	    	pocketsoc-ng	pocketsoc-ng_opensearch-node2	2022-06-13 16:49:51	172.20.0.12	-
<input type="checkbox"/>	zeek	running	    	pocketsoc-ng	pocketsoc-ng_zeek	2022-06-13 16:49:51	172.20.0.5	-
<input type="checkbox"/>	router	running	    	pocketsoc-ng	pocketsoc-ng_router	2022-06-13 16:49:51	172.18.0.3	-
<input type="checkbox"/>	webserver	running	    	pocketsoc-ng	pocketsoc-ng_webserver	2022-06-13 16:49:51	172.18.0.2	-


# Portainer

>\_ Execute

Command  /bin/bash

Use custom command



User  root

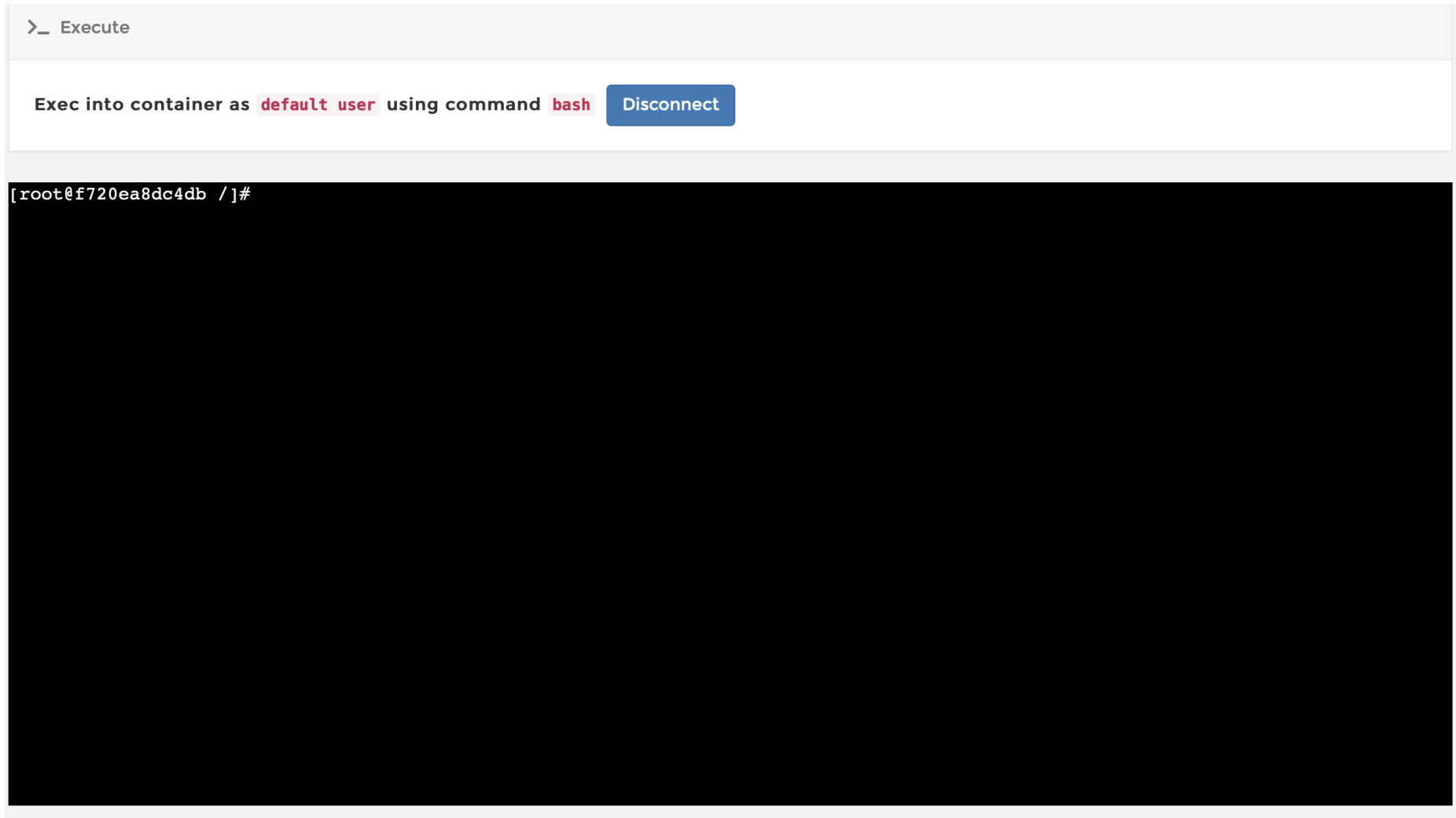
Connect

# Portainer

>\_ Execute

Exec into container as `default user` using command `bash` [Disconnect](#)

```
[root@f720ea8dc4db /]#
```

The image shows a screenshot of the Portainer web interface. At the top, there is a header bar with the text ">\_ Execute". Below this, there is a white box containing the text "Exec into container as default user using command bash" and a blue button labeled "Disconnect". The main area of the screenshot is a black terminal window with the text "[root@f720ea8dc4db /]#" at the top left, indicating the user is root in a container with ID f720ea8dc4db.

# OpenSearch Dashboards

- Log into Dashboards with the credentials provided



Log in to OpenSearch Dashboards

If you have forgotten your username or password,  
contact your system administrator.



Username



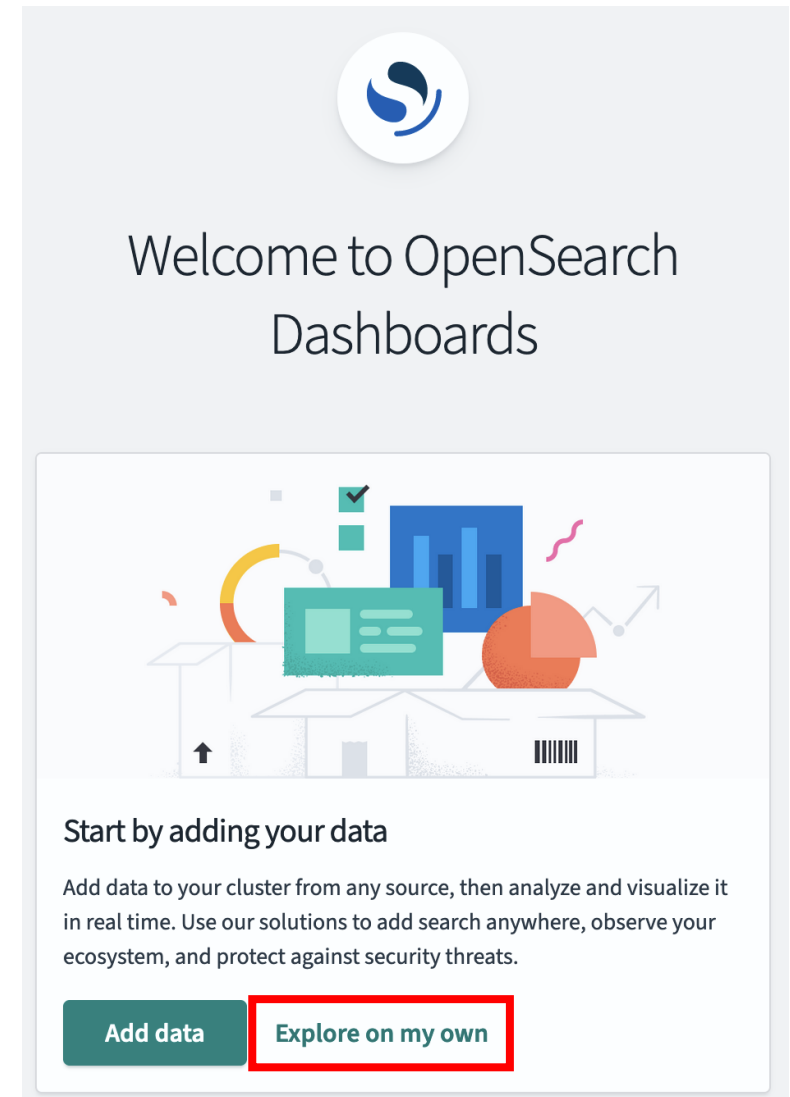
Password

Log in



# OpenSearch Dashboards

- Select “Explore on my own”



The image shows the OpenSearch Dashboards welcome screen. At the top center is the OpenSearch logo, a blue stylized 'S' inside a white circle. Below the logo, the text "Welcome to OpenSearch Dashboards" is displayed in a dark grey font. Underneath this is a large, colorful illustration featuring various data visualization elements: a bar chart, a pie chart, a line graph, a checkmark, and a document icon, all set against a light grey background with a subtle grid. Below the illustration, the text "Start by adding your data" is followed by a paragraph: "Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats." At the bottom of the screen, there are two buttons: "Add data" and "Explore on my own". The "Explore on my own" button is highlighted with a red rectangular border.

Welcome to OpenSearch Dashboards

Start by adding your data

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

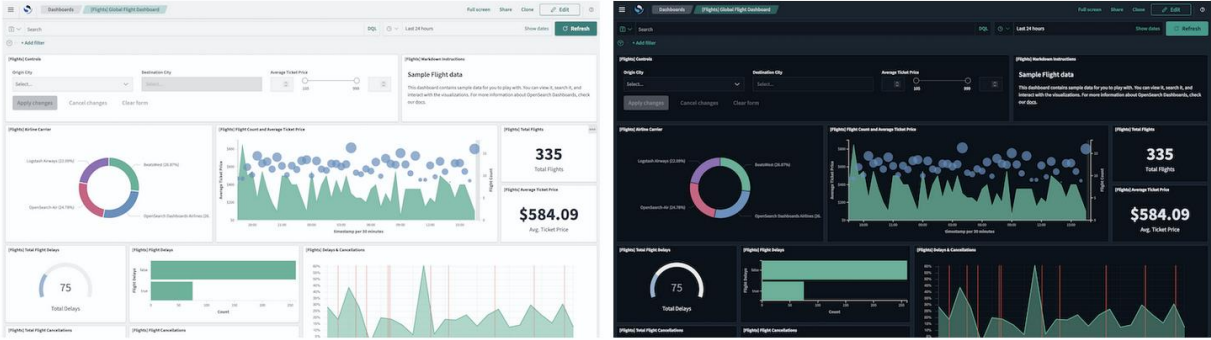
[Add data](#) [Explore on my own](#)

# OpenSearch Dashboards

- Dismiss the “new look and feel” window

Introducing new OpenSearch Dashboards look & feel

You are now previewing the newest OpenSearch Dashboards theme with improved light and dark modes. You or your administrator can change to the previous theme by visiting [Advanced Settings](#).



Dismiss

# OpenSearch Dashboards

- Confirm “private tenant”

✕

## Select your tenant

Tenants are useful for safely sharing your work with other OpenSearch Dashboards users. You can switch your tenant anytime by clicking the user avatar on top right.

Global  
The global tenant is shared between every OpenSearch Dashboards user.

Private  
The private tenant is exclusive to each user and can't be shared. You might use the private tenant for exploratory work.

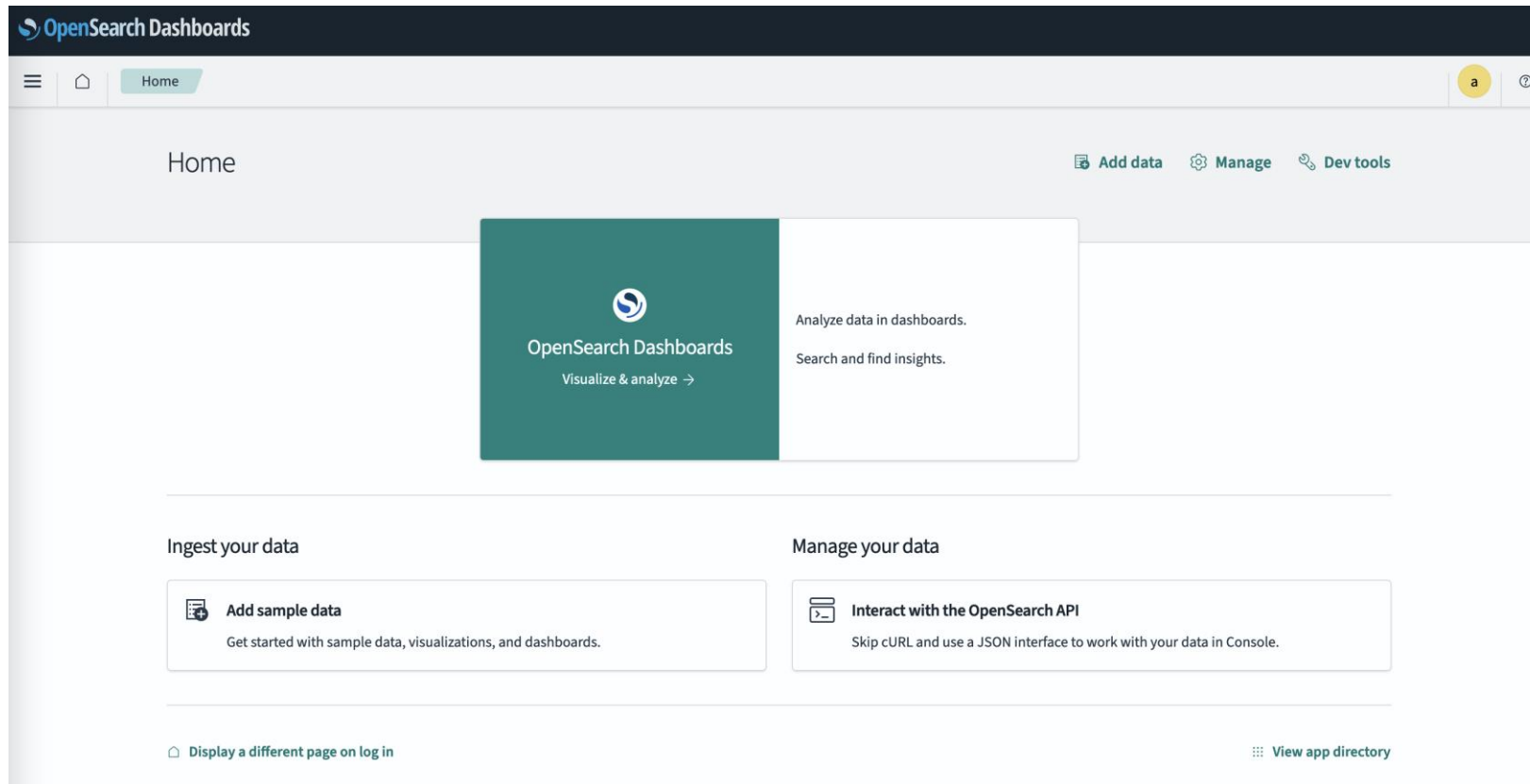
Choose from custom

Cancel

Confirm

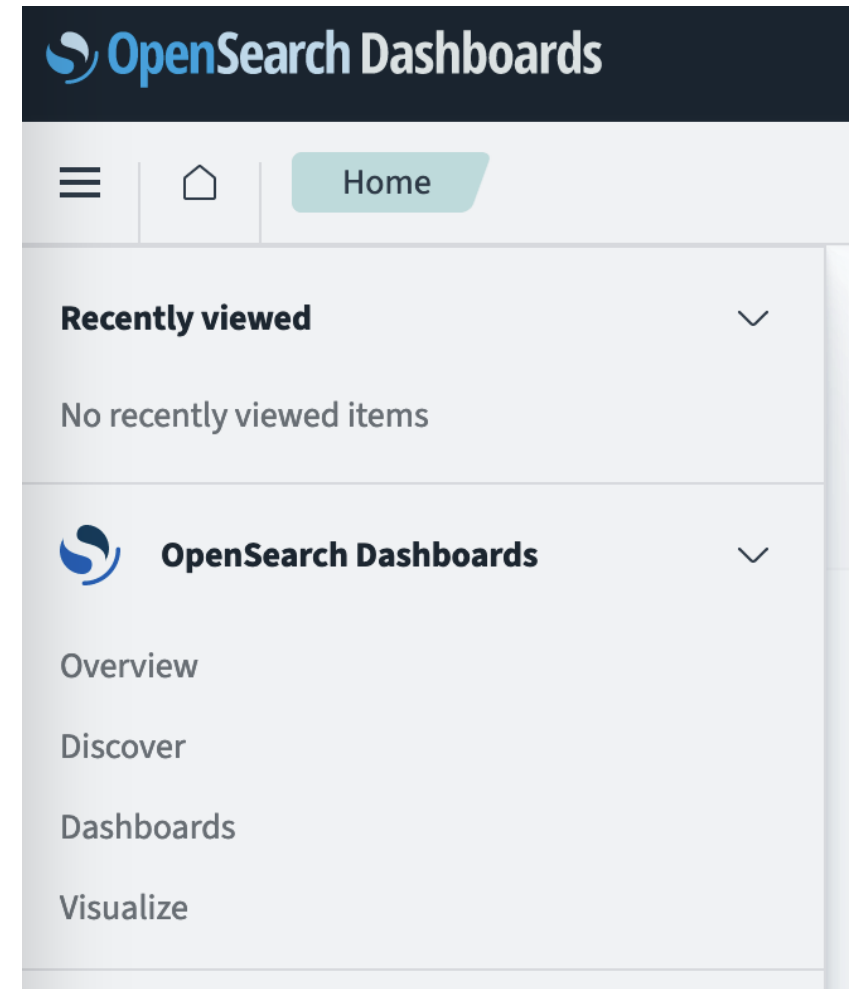
# OpenSearch Dashboards

- You should see this view



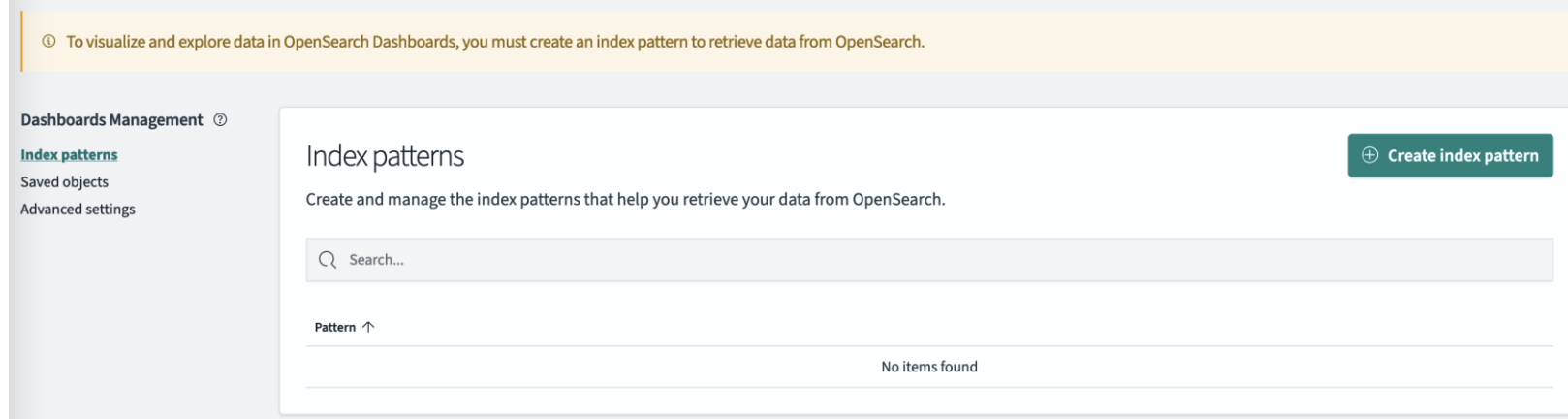
# OpenSearch Dashboards

- Click the three bar menu in the top left and select “Discover”



# OpenSearch Dashboards

- Now we need to create an *index pattern* to select which records to display. Click on “Create index pattern”



# OpenSearch Dashboards

- You should see something like the following, with `opensearch-logstash-zeek-2023.10.12`

## 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 1 of 2: Define an index pattern

**Index pattern name**

Next step >

Use an asterisk (\*) to match multiple indices. Spaces and the characters `\, /, ?, ", <, >, |` are not allowed.

Include system and hidden indices

Your index pattern can match any of your 2 sources.

<code>opensearch-logstash-zeek-2023.10.12</code>	Index
<code>security-auditlog-2023.10.12</code>	Index

Rows per page: 10 ▾

# OpenSearch Dashboards

- Enter `opensearch-logstash-zeek-*` (this will match multiple days): Next step.

## 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 1 of 2: Define an index pattern

Index pattern name

[Next step >](#)

Use an asterisk (\*) to match multiple indices. Spaces and the characters `\, /, ?, ", <, >, |` are not allowed.

Include system and hidden indices

✓ Your index pattern matches 1 source.

---

<code>opensearch-logstash-zeek-2023.10.12</code>	Index
--	-------

---

Rows per page: 10 ▾



# OpenSearch Dashboards

- Select `@timestamp` in the Time field

## 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 **opensearch-logstash-zeek-\*** index pattern.

Select a primary time field for use with the global time filter.

Time field Refresh

`@timestamp` ▼

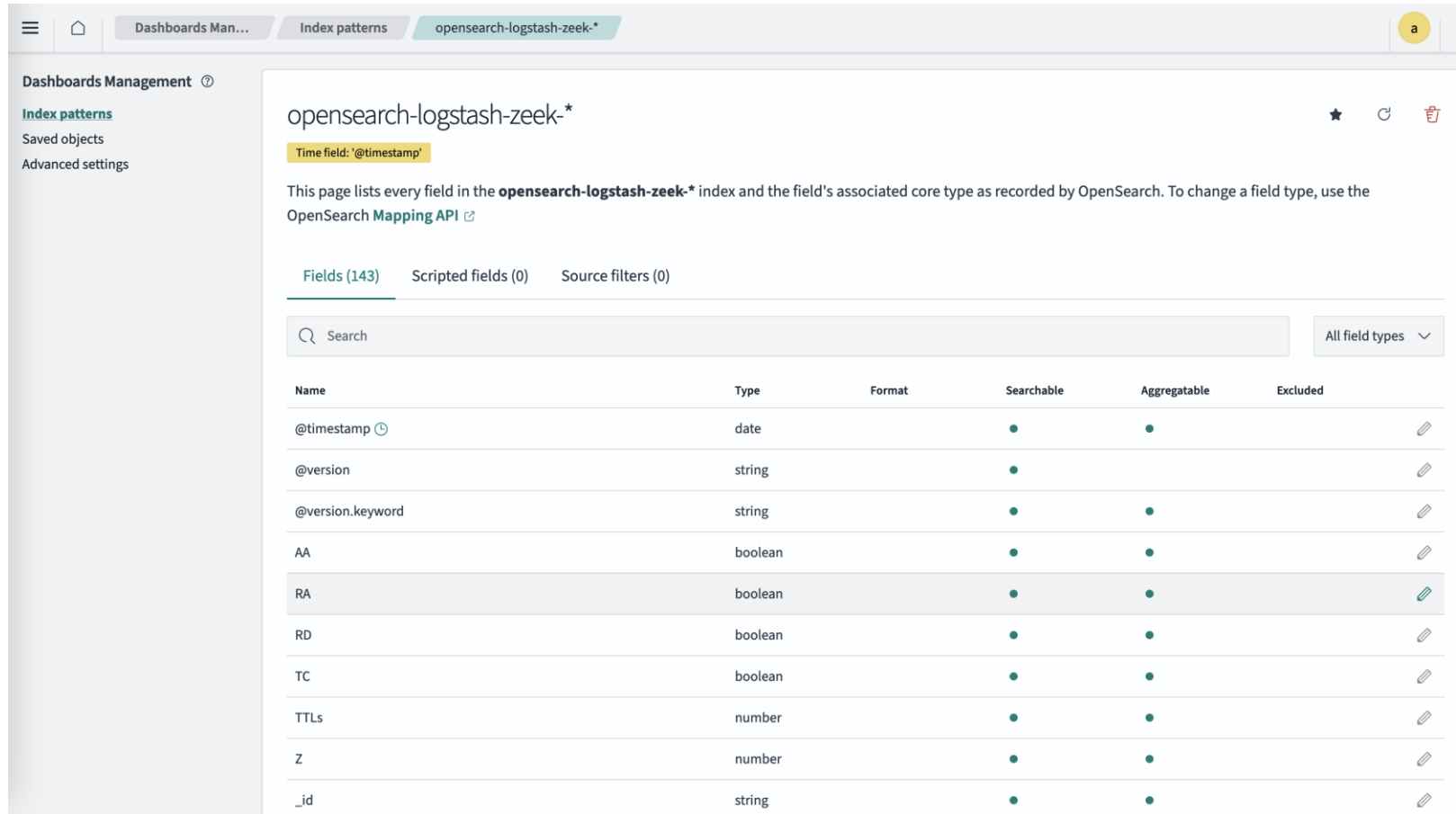
---

[> Show advanced settings](#)

[< Back](#) [Create index pattern](#)

# OpenSearch Dashboards

- You should see something like this

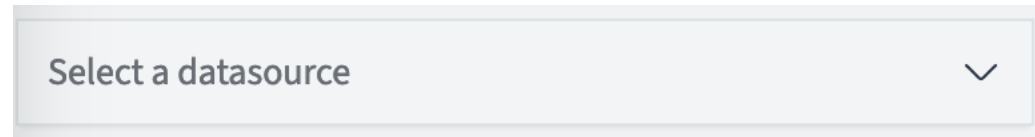


The screenshot displays the OpenSearch Dashboards interface for the 'opensearch-logstash-zeek-\*' index. The left sidebar shows 'Dashboards Management' with options for 'Index patterns', 'Saved objects', and 'Advanced settings'. The main content area is titled 'opensearch-logstash-zeek-\*' and includes a 'Time field: '@timestamp'' indicator. Below this, a text block explains that the page lists fields and their core types. A navigation bar shows 'Fields (143)', 'Scripted fields (0)', and 'Source filters (0)'. A search bar and a dropdown menu for 'All field types' are present. The main part of the interface is a table listing fields with columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. The 'RA' field is highlighted.

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	string		●		
@version.keyword	string		●	●	
AA	boolean		●	●	
RA	boolean		●	●	
RD	boolean		●	●	
TC	boolean		●	●	
TTLs	number		●	●	
Z	number		●	●	
_id	string		●	●	

# OpenSearch Dashboards

- From the menu select Discover again: at the top left of the window you'll see "Select a datasource" : choose the index pattern you just created



Select a datasource

# OpenSearch Dashboards

- You should see some data: time to explore!

The screenshot displays the OpenSearch Dashboards interface. At the top, there's a navigation bar with 'Discover' selected. Below it, a search bar contains 'opensearch-logstash-zeek\*'. The interface is divided into several sections:

- Left Panel:** Contains 'Selected fields' (currently showing '\_source') and 'Available fields' (listing fields like '\_id', '\_index', '\_score', '\_type', '@timestamp', '@version', 'acks', 'active\_dns\_requests', 'active\_files', 'active\_icmp\_conns', and 'active\_tcp\_conns').
- Top Right:** Includes a search bar, 'DQL' button, a date range selector set to 'Last 15 minutes', 'Show dates' button, and a 'Refresh' button.
- Center:** A bar chart titled '21 hits' showing the distribution of data over time. The x-axis is '@timestamp per 30 seconds' and the y-axis is 'Count'. A notification banner above the chart states: 'You're viewing Discover 2.0. The old Discover app will be retired in OpenSearch version 2.11. To switch back to the old version, turn off the New Discover toggle. To provide feedback, open an issue.'
- Bottom:** A table with columns 'Time (@timestamp)' and 'Source'. It shows two log entries with detailed message content.

Time (@timestamp)	Source
Oct 12, 2023 @ 09:15:37.069	<code>{ "missed_bytes": 0, "message": { "ts": "1697094924.43476", "uid": "C2wVGK1YHsvyrxOo", "id.orig_h": "172.19.0.16", "id.orig_p": "39064", "id.resp_h": "172.19.0.11", "id.resp_p": "5044", "proto": "tcp", "duration": 0.025580883026123047, "orig_bytes": 528, "resp_bytes": 0, "conn_state": "SO", "local_orig": true, "local_resp": true, "missed_bytes": 0, "history": { "ScAD": { "orig_pkts": 4, "orig_ip_bytes": 744, "resp_pkts": 0, "resp_ip_bytes": 0 } }, "history": { "ScAD": { "resp_ip_bytes": 0, "orig_pkts": 4, "id.orig_p": 39064, "log.offset": 641, "log.file.path": "/opt/zeek/logs/current/weird.log", "@version": 1, "id.resp_h": "172.19.0.11", "id.resp_p": "5044", "notice": false, "ecs.version": "8.0.0" } }</code>
Oct 12, 2023 @ 09:15:34.011	<code>{ "name": "data_before_established", "message": { "ts": "1697094924.437308", "uid": "C2wVGK1YHsvyrxOo", "id.orig_h": "172.19.0.16", "id.orig_p": "39064", "id.resp_h": "172.19.0.11", "id.resp_p": "5044", "name": "data_before_established", "notice": false, "peer": "zeek", "source": "TCP" }   ts 1,697,094,924.437 source TCP id.orig_p 39,064 log.offset 641 log.file.path /opt/zeek/logs/current/weird.log @version 1 id.resp_h 172.19.0.11 id.resp_p 5,044 notice false ecs.version 8.0.0 }</code>