OpenSearchCon EUROPE

Upcoming Changes for the OpenSearch Index Authorization Mechanisms

Nils Bandener

eliatra

The OpenSearch Experts

Nils Bandener

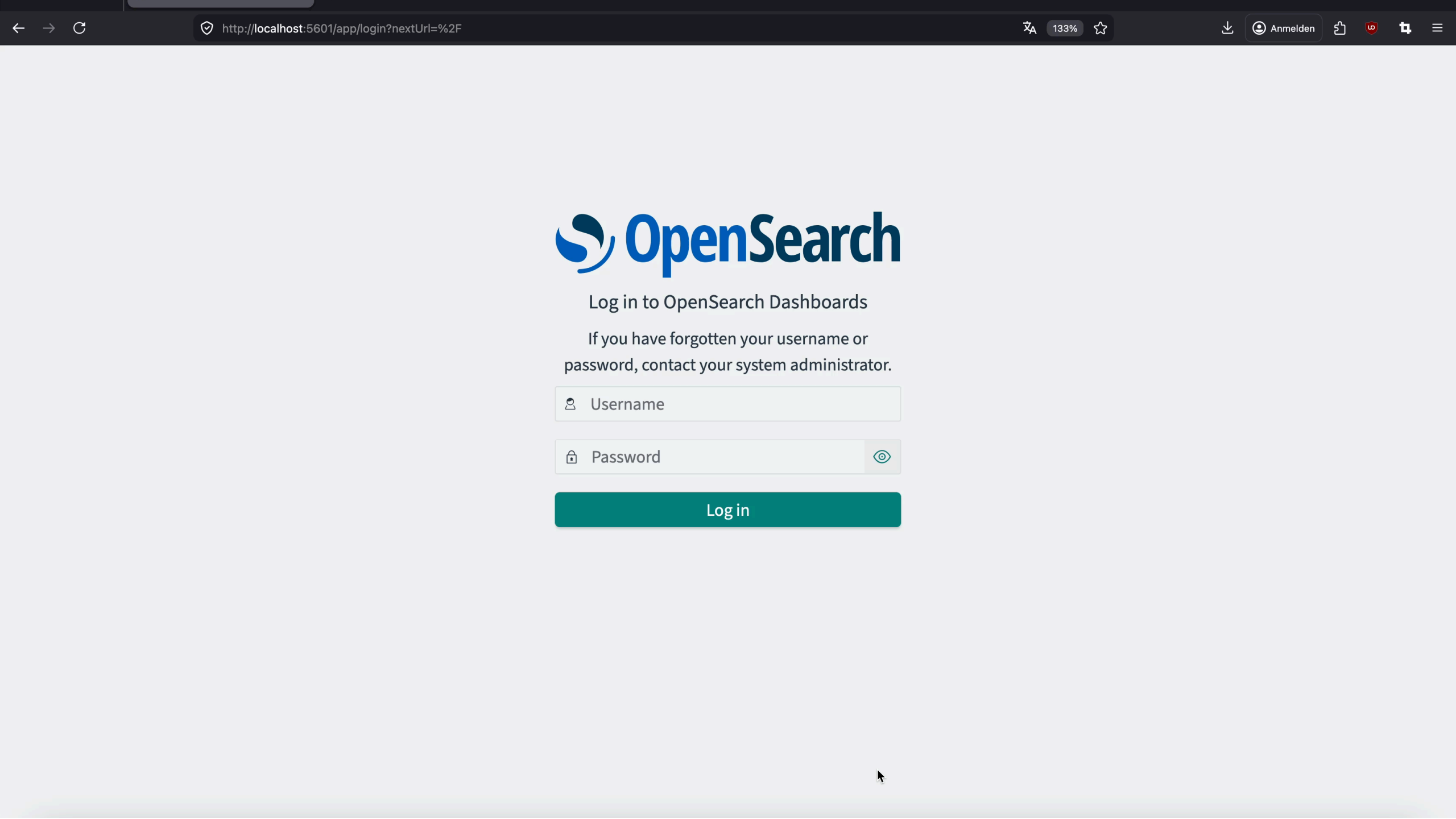
Freelance Software Architect and Consultant

Co-Maintainer of the OpenSearch Security Plugin

The OpenSearch Experts

Overview

- What's the problem?
- The path to a solution
- Index resolution semantics
- Alias privilege semantics


http://localhost:5601/app/login?nextUrl=%2F
133%
Anmelden
OpenSearch
Log in to OpenSearch Dashboards
If you have forgotten your username or password, contact your system administrator.
Username
Password
Log in

[Flights] Controls

Origin City

Select...

Destination City

Select...

Average Ticket Price

192 1191

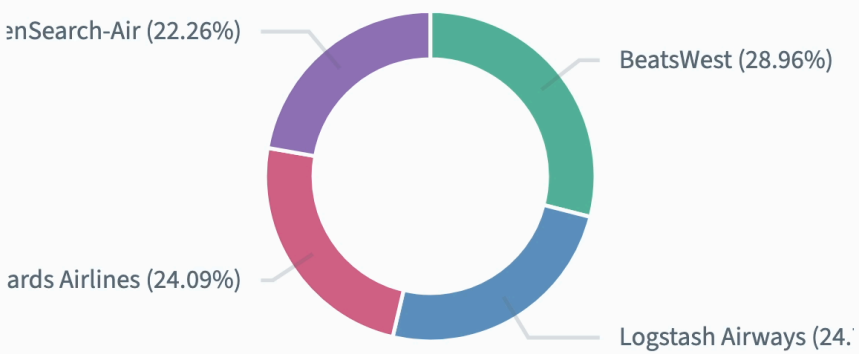
Apply changes Cancel changes Clear form

[Flights] Markdown Instructions

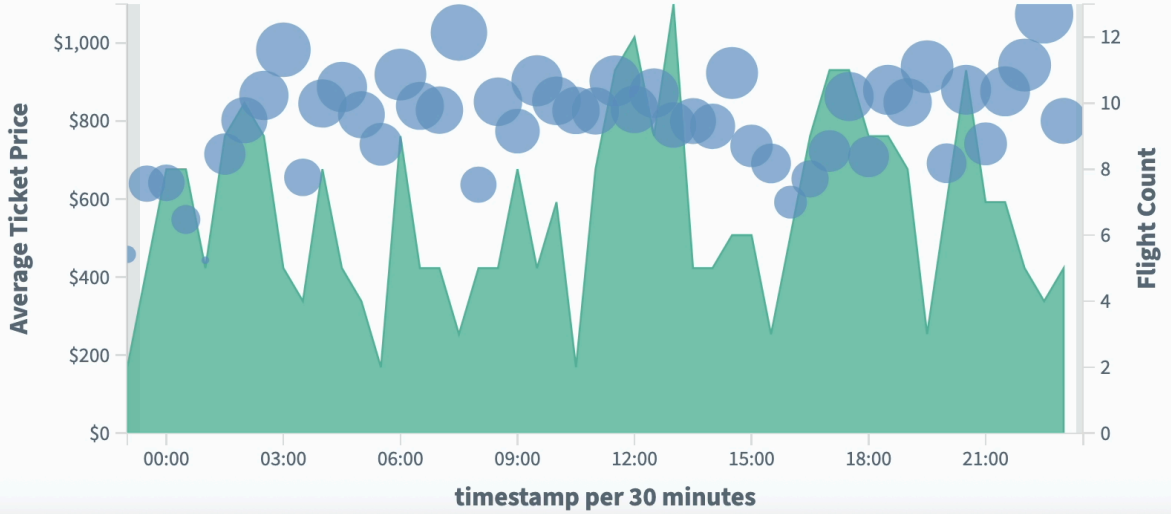
Sample Flight data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about OpenSearch Dashboards, check our docs.

[Flights] Airline Carrier



[Flights] Flight Count and Average Ticket Price



[Flights] Total Flights

328

Total Flights

[Flights] Average Ticket Pr...

$796...

Avg. Ticket Price

Index Management

- State management policies
- Policy managed indexes
- **Indexes**
- Data streams
- Templates
- Aliases
- Rollup jobs
- Transform jobs
- Notification settings

Snapshot Management

- Snapshot policies
- Snapshots
- Repositories

Indexes (10)

Refresh | Actions | + Create Index

Search | Show data stream indexes

Index	Health	Manage...	Status	Total size	Size of p...	Total do...	Deleted ...	Primaries	Replicas
top_queries-2026.04.11-55134	Green	No	Open	347.4kb	175.2kb	132	2	1	1
security-auditlog-2026.04.11	Green	No	Open	4.1mb	2mb	832	0	1	1
opensearch_dashboards_sample_data_flights	Green	No	Open	11.1mb	5.5mb	13059	0	1	1
opensearch_dashboards_sample_data_ecommerce	Green	No	Open	8.2mb	4mb	4675	0	1	1
.ql-datasources	Green	No	Open	416b	208b	0	0	1	1
.plugins-ml-config	Green	No	Open	9kb	4.5kb	1	0	1	1
.opendistro_security	Green	No	Open	469.9kb	234.9kb	9	5	1	1

opensearch_dashboards_sample_data_flights

Remove

Index

opensearch_dashboards_sample_data_flights ×

Specify index pattern using *

Index permissions

You can specify permissions using both action groups or single permissions. A permission group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.

read × indices_monitor ×

Create new permission group

Document level security - *optional*

You can restrict a role to a subset of documents in an index. **Learn more**

```
{
  "bool": {
    "must": {
```

Field level security - *optional*

You can restrict what document fields a user can see. If you use field-level security in conjunction with document-level security, make sure you don't restrict access to the field that document-level security uses.

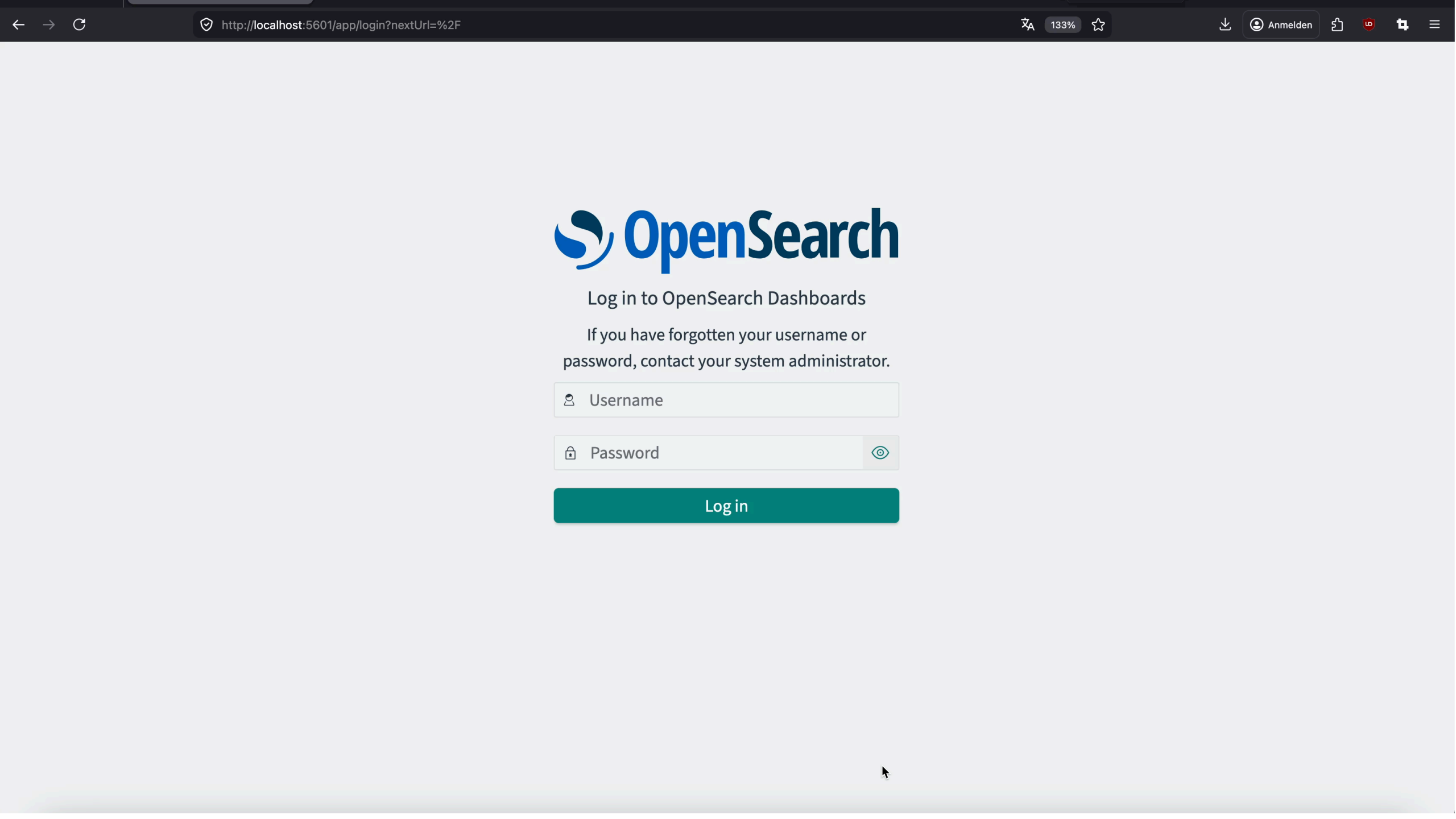
Exclude

Type in field name

Anonymization - *optional*

Masks any sensitive fields with a random value to protect your data security.

Type in field name


http://localhost:5601/app/login?nextUrl=%2F
133%
Anmelden
OpenSearch
Log in to OpenSearch Dashboards
If you have forgotten your username or password, contact your system administrator.
Username
Password
Log in

http://localhost:5601/app/dashboards#/view/7adfa750-4c81-11e8-b3d7-01146121b73d?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(133% Anmelden

OpenSearch Dashboards

Dashboards / [Flights] Global Flight Dashboard

Full screen | Share | Clone | Reporting | Edit | I

Search | DQL | Last 24 hours | Show dates | Refresh

Add filter

[Flights] Controls

Origin City: Select...

Destination City: Select...

Average Ticket Price: 128 1191

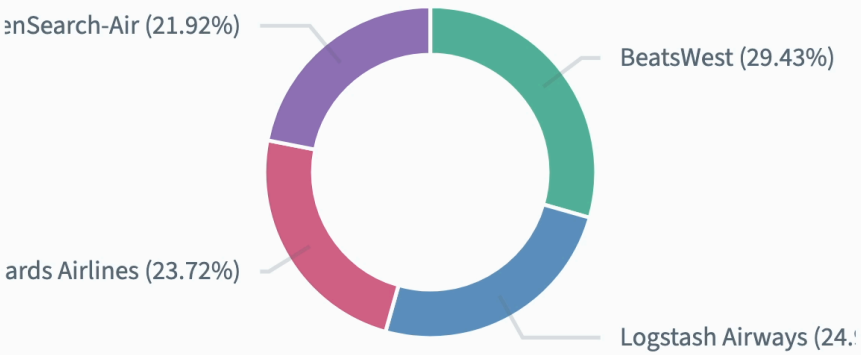
Apply changes | Cancel changes | Clear form

[Flights] Markdown Instructions

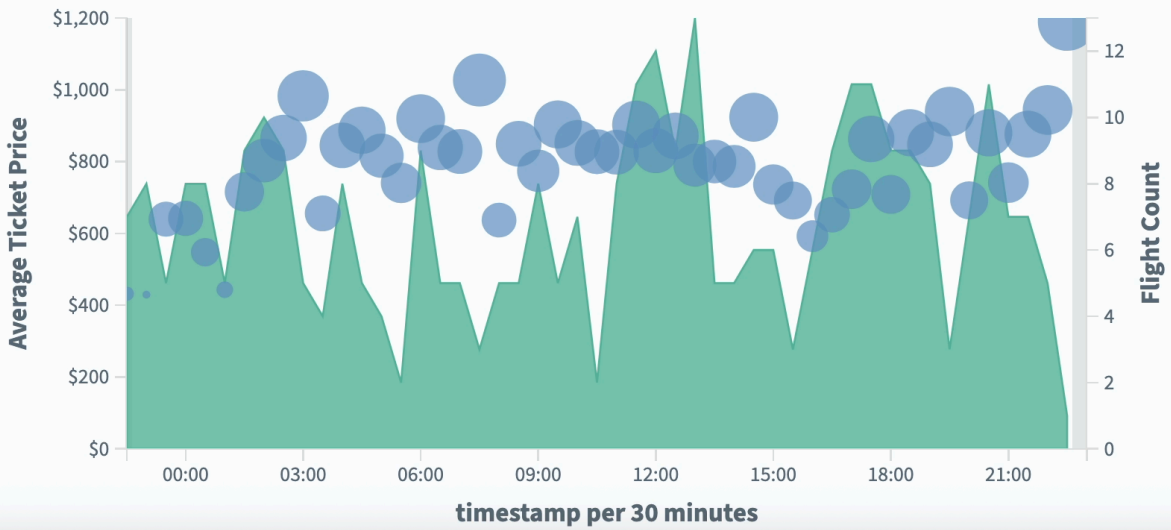
Sample Flight data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about OpenSearch Dashboards, check our docs.

[Flights] Airline Carrier



[Flights] Flight Count and Average Ticket Price



[Flights] Total Flights

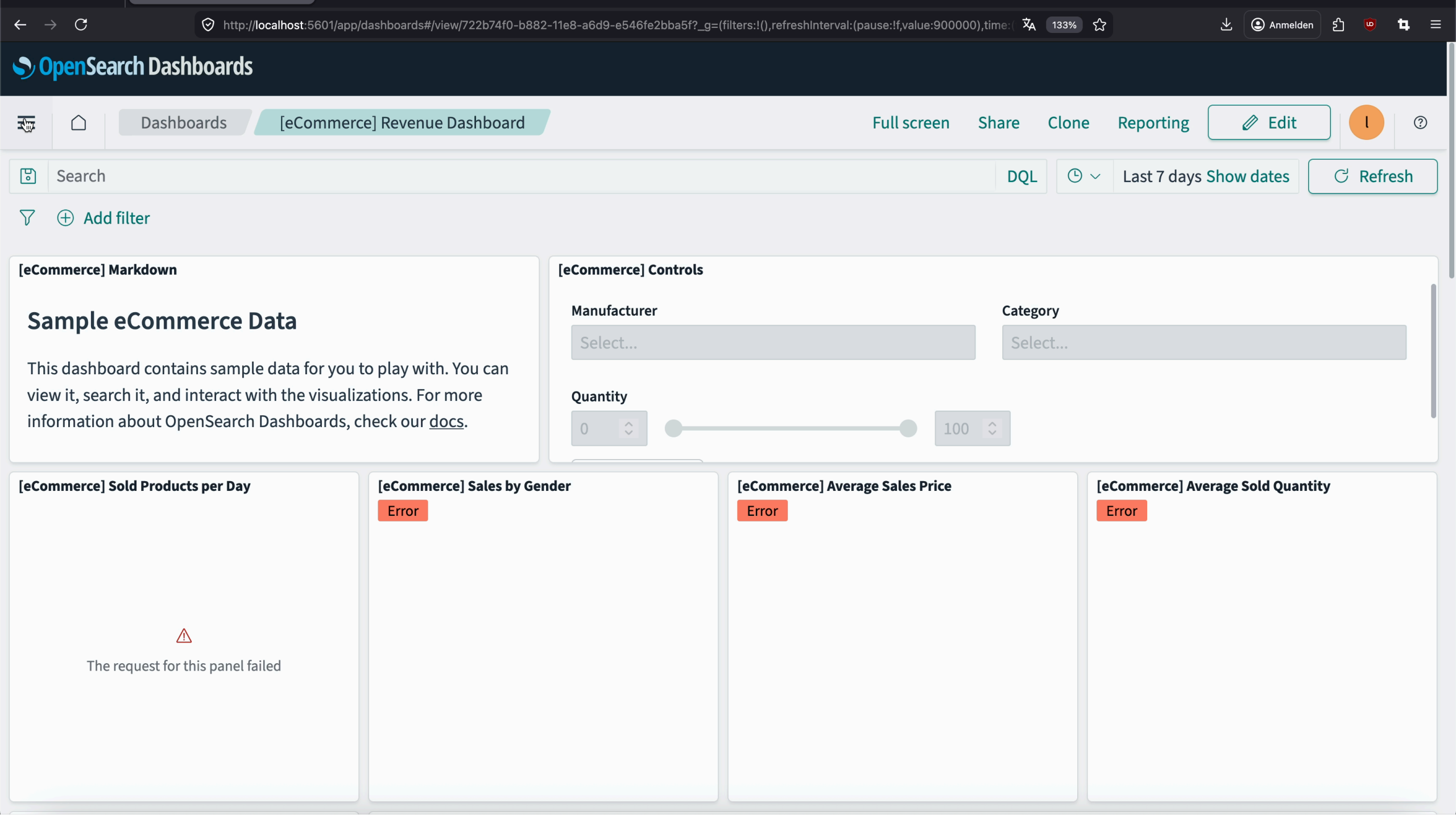
333

Total Flights

[Flights] Average Ticket Pr...

$779...

Avg. Ticket Price


http://localhost:5601/app/dashboards#/view/722b74f0-b882-11e8-a6d9-e546fe2bba5f?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(
133%
Anmelden
OpenSearch Dashboards
Dashboards
[eCommerce] Revenue Dashboard
Full screen
Share
Clone
Reporting
Edit
I
Search
DQL
Last 7 days
Show dates
Refresh
Add filter
[eCommerce] Markdown
Sample eCommerce Data
This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about OpenSearch Dashboards, check our docs.
[eCommerce] Controls
Manufacturer
Select...
Category
Select...
Quantity
0
100
[eCommerce] Sold Products per Day
The request for this panel failed
[eCommerce] Sales by Gender
Error
[eCommerce] Average Sales Price
Error
[eCommerce] Average Sold Quantity
Error

OpenSearch Dashboards

Dashboards Management

Index patterns
Data sources
Saved objects
Advanced settings

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

The index pattern you've entered doesn't match any indices. You can match any of your **0 indices**, below.

Rows per page: 10

opensearch-node1

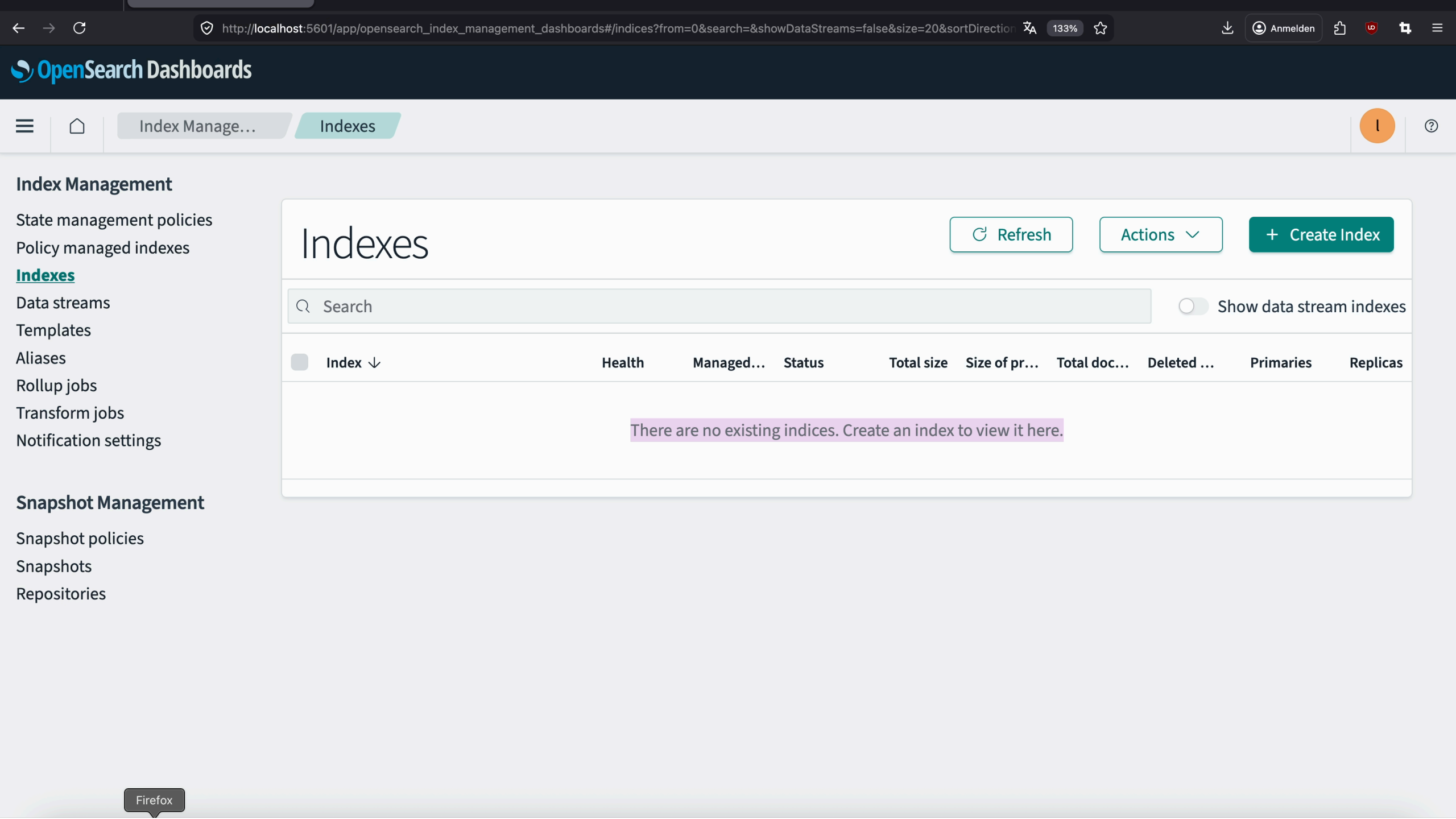
3028bd2f177c opensearchproject/opensearch:latest
9200:9200 9600:9600

STATUS
Running (40 minutes ago)

Logs Inspect Bind mounts Exec Files Stats Debug

Docker Debug brings the tools you need to debug your container with one click.
Requires a paid Docker subscription. Learn more.

```
drwxr-xr-x 3 opensearch opensearch 4096 Apr  4 06:55 ..
-rwxr-x--- 1 opensearch opensearch 3875 Apr  4 06:55 SECURITY_ADMIN_TESTS.md
-rwxr-x--- 1 opensearch opensearch  418 Apr  4 06:55 audit_config_migrater.bat
-rwxr-x--- 1 opensearch opensearch 1059 Apr  4 06:55 audit_config_migrater.sh
-rwxr-x--- 1 opensearch opensearch  421 Apr  4 06:55 hash.bat
-rwxr-x--- 1 opensearch opensearch 1047 Apr  4 06:55 hash.sh
-rwxr-x--- 1 opensearch opensearch  859 Apr  4 06:55 install_demo_configuration.bat
-rwxr-x--- 1 opensearch opensearch 1951 Apr  4 06:55 install_demo_configuration.sh
-rwxr-x--- 1 opensearch opensearch  491 Apr  4 06:55 securityadmin.bat
-rwxr-x--- 1 opensearch opensearch 1088 Apr  4 06:55 securityadmin.sh
sh-5.2$ ls -la ../../../config/securityadmin_demo.sh
-r-x--x--x 1 opensearch opensearch 304 Apr 11 19:53 ../../../config/securityadmin_demo.sh
sh-5.2$ ls -la ../../../config/
esnode-key.pem               jvm.options.d/              opensearch-notifications/      opensearch-security/          root-ca.pem
esnode.pem                   kirk-key.pem                opensearch-notifications-core/ opensearch-security-analytics/ securityadmin_demo.sh
fips_java.security           kirk.pem                    opensearch-observability/      opensearch.keystore
jvm.options                  log4j2.properties           opensearch-reports-scheduler/  opensearch.yml
sh-5.2$ ls -la ../../../config/opensearch-security
total 92
drwxr-x--- 1 opensearch opensearch  4096 Apr 11 20:33 .
drwxr-xr-x 1 opensearch opensearch  4096 Apr 11 19:53 ..
-rw-rw---- 1 opensearch opensearch    50 Apr  4 06:55 action_groups.yml
-rw-rw---- 1 opensearch opensearch  1973 Apr  4 06:55 allowlist.yml
-rw-rw---- 1 opensearch opensearch  2541 Apr  4 06:55 audit.yml
-rw-r--r-- 1 root       root       10378 Apr 11 20:33 config.yml
-rw-rw---- 1 opensearch opensearch  1513 Apr 11 19:53 internal_users.yml
-rw-rw---- 1 opensearch opensearch   154 Apr  4 06:55 nodes_dn.yml
-rw-rw---- 1 opensearch opensearch 12381 Apr  4 06:55 opensearch.yml.example
-rw-rw---- 1 opensearch opensearch 19867 Apr  4 06:55 roles.yml
-rw-rw---- 1 opensearch opensearch   844 Apr  4 06:55 roles_mapping.yml
-rw-rw---- 1 opensearch opensearch   170 Apr  4 06:55 tenants.yml
sh-5.2$
```


http://localhost:5601/app/opensearch_index_management_dashboards#/indices?from=0&search=&showDataStreams=false&size=20&sortDirection
133%
Anmelden
OpenSearch Dashboards
Index Manage...
Indexes
Index Management
State management policies
Policy managed indexes
Indexes
Data streams
Templates
Aliases
Rollup jobs
Transform jobs
Notification settings
Snapshot Management
Snapshot policies
Snapshots
Repositories
Indexes
Refresh
Actions
Create Index
Search
Show data stream indexes
Index
Health
Managed...
Status
Total size
Size of pr...
Total doc...
Deleted ...
Primaries
Replicas
There are no existing indices. Create an index to view it here.
Firefox

OpenSearch Dashboards

Index Manage... Indexes

Index Management

- State management policies
- Policy managed indexes
- **Indexes**
- Data streams
- Templates
- Aliases
- Rollup jobs
- Transform jobs
- Notification settings

Snapshot Management

- Snapshot policies
- Snapshots
- Repositories

Indexes (3)

Refresh | Actions | + Create Index

Search

Show data stream indexes

Index	Health	Managed...	Status	Total size	Size of pr...	Total doc...	Deleted ...	Primaries	Replicas
opensearch_dashboards_sample_data_flights	Green	Yes	Open	11.1mb	5.5mb	13059	0	1	1
.kibana_176117146_limited_1	Green	Yes	Open	11.5kb	5.7kb	1	0	1	1
.kibana_1	Green	Yes	Open	169.6kb	86.9kb	101	0	1	1

Rows per page: 20

1

do_not_fail_on_forbidden

- must be explicitly enabled, globally
- drops any unauthorized index from index expressions
  - can be wanted but also unwanted

do_not_fail_on_forbidden: pro

- Enables use of GET /_search and GET /_cat/indices
- A user does not have to think about indices they do not have access to
- Makes OpenSearch Dashboards work
- Robust against appearance of new, unauthorized indices

do_not_fail_on_forbidden: contra

- fail-fast mechanism can be useful for verifying privileges
- just getting empty result set when not having authorization can be counter-intuitive
- under certain conditions: silently drops indices with typos from request
- not all APIs supported

Goals for Replacement

- enabled by default
- gives user control over behavior
- support all APIs
- simplified and hardened implementation

[RFC] Refined index authorization (replacement for do_not_fail_on_forbidden) #3905

Open

nibix opened on Jan 2, 2024 Member

Background

The `do_not_fail_on_forbidden` setting switches globally between two different modes how OpenSearch reacts to cases when users have no privileges for indices.

By default, OpenSearch will resolve any patterns specified in action requests against all indices on the cluster. If then the current user does not have access privileges for any of these indices, OpenSearch will yield a 403 error.

If `do_not_fail_on_forbidden` is enabled, the behavior is changed: The resolution is limited to indices to which the user has access. Thus, the operation will succeed.

A very common example for the difference is a `_search` request to all indices (`GET /_search` , or `GET /*/_search`). For users which have not complete read-access to all indices on the cluster, this request will always fail with a 403 error if `do_not_fail_on_forbidden` disabled. If `do_not_fail_on_forbidden` is enabled, these users will get the search result limited to

[RFC] Revised index action authorization scheme #5814

Open

nibix opened on Nov 25, 2025 Member

Introduction

This is a follow-up and extension of the RFC on Refined index authorization from #3905 and #5367.

Based on that, we already worked on an implementation, which current state can be found in #5399.

During implementation we found quite a few issues and oddities with the current index action authorization implementation. Many of these are documented inside the integration tests at https://github.com/opensearch-project/security/tree/main/src/integrationTest/java/org/opensearch/security/privileges/int_tests

The changes in #5399 have the goal to fix these. However, this sometimes requires quite fundamental, breaking changes.

This RFC shall document these changes and open a forum to discuss the approaches.

Feature flag

Improved index resolution and revised index authorization #5827

Merged cwperks merged 8 commits into opensearch-project:main from nibix:improved-index-resolution-2 4 days ago

Conversation 27 Commits 8 Checks 63 Files changed 80

nibix commented on Dec 2, 2025 Member

Description

This introduces all the necessary changes for the improved index resolution and revised index authorization described in #5814.

This has several advantages:

- The old index authorization and index resolution system had many inconsistencies and oddities. These are fixed by the new approach.
- The responsibility for index resolution is moved from the security plugin to the individual transport actions. This makes the whole authorization process much more robust and the code less messy and fragile.
- As each transport action knows its indices it is operating on very well, it can do the resolution in a more efficient manner (often actually no resolution takes place at all, as all indices are already determined as constant values). This reduces the performance overhead induced by the security plugin.

Release

OpenSearch 3.7.0

Gated by feature flag privileges_evaluation_type=v4 in config.yml.

OpenSearch 4.0.0

New default

Index Resolution Semantics

Existing index options

```
GET /index_a,index_b/_search?ignore_unavailable=true&allow_no_indices=false
```

ignore_unavailable

Specifies whether to include missing or closed indexes in the response. Default is false.

Existing index options

```
GET /index_a,index_b/_search?ignore_unavailable=true&allow_no_indices=false
```

allow_no_indices

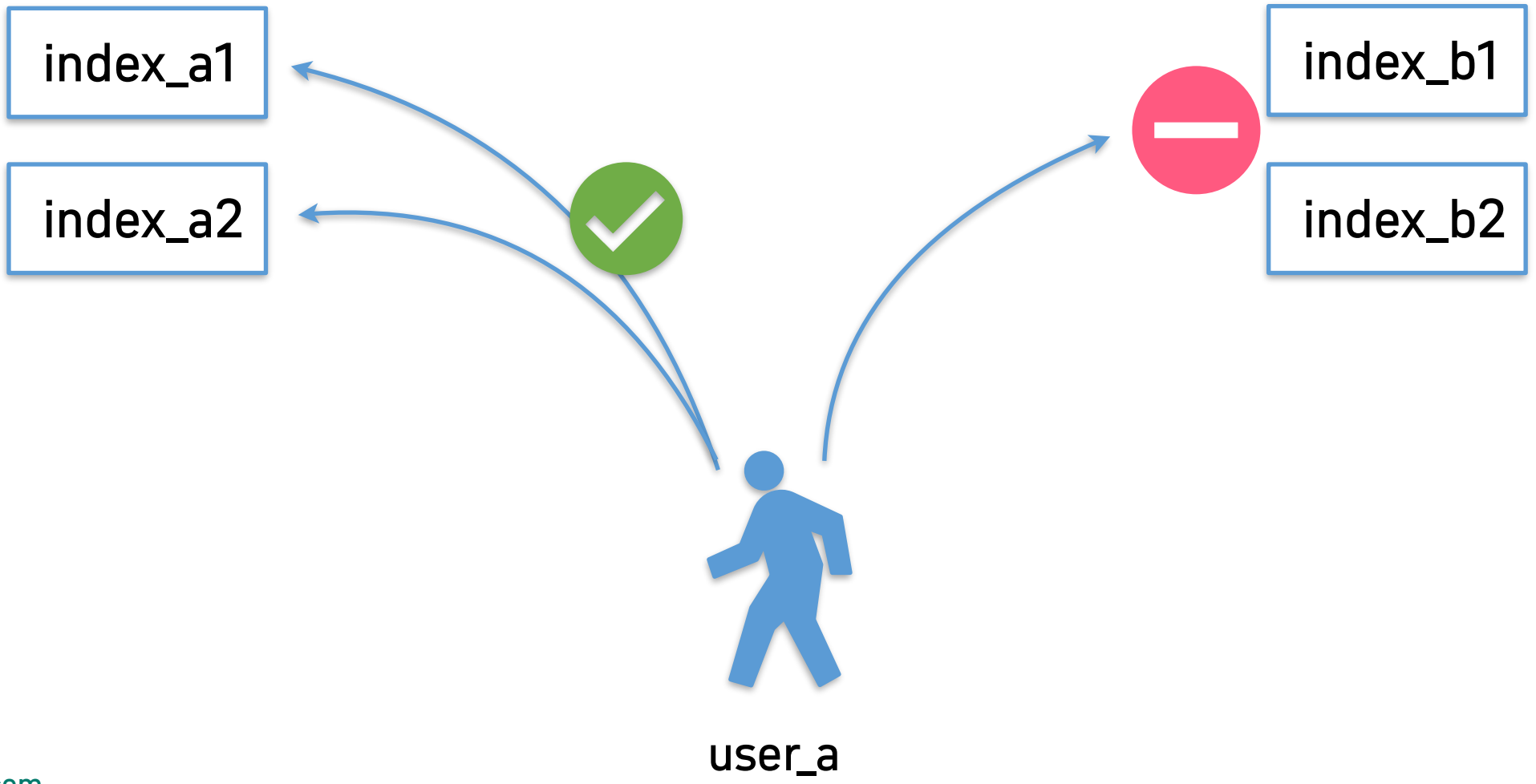
If set to true, wildcard expressions that do not match any index will yield an empty result. If false, this will lead to an error message.

Default is true.

Extended Semantics

- We just build upon these existing options and extend their semantics for security privileges

Extended Semantics: Example



Extended Semantics: Example

```
GET /_search
```

```
GET /_all/_search
```

```
GET /*/_search
```

Search result will include index_a1 and index_a2

Extended Semantics: Example

```
GET /index_a*,index_b*/_search
```

Search result will include index_a1 and index_a2

Extended Semantics: Example

```
GET /index_a1,index_b1/_search
```

Operation will fail with error 403 Forbidden

Extended Semantics: Example

```
GET /index_a1,index_b1/_search?ignore_unavailable=true
```

Result will contain documents from index_a1

Extended Semantics: Example

```
GET /index_b1/_search?ignore_unavailable=true
```

Result will be empty result set

Extended Semantics: Example

```
GET /index_b1/_search?ignore_unavailable=true&allow_no_indices=false
```

Operation will fail with error 403 Forbidden

Extended Semantics

Unauthorized indices will be automatically removed from index expression if:

- ignore_unauthorized=true
- A wildcard is used

Supported APIs

- All APIs are automatically supported as soon as request class implements IndicesRequest.Replaceable

```
67
68 > /** A request to execute search against one or more indices (or all). Best created using ...*/
82   @PublicApi(since = "1.0.0")
83   public class SearchRequest extends ActionRequest implements IndicesRequest.Replaceable {
84
```

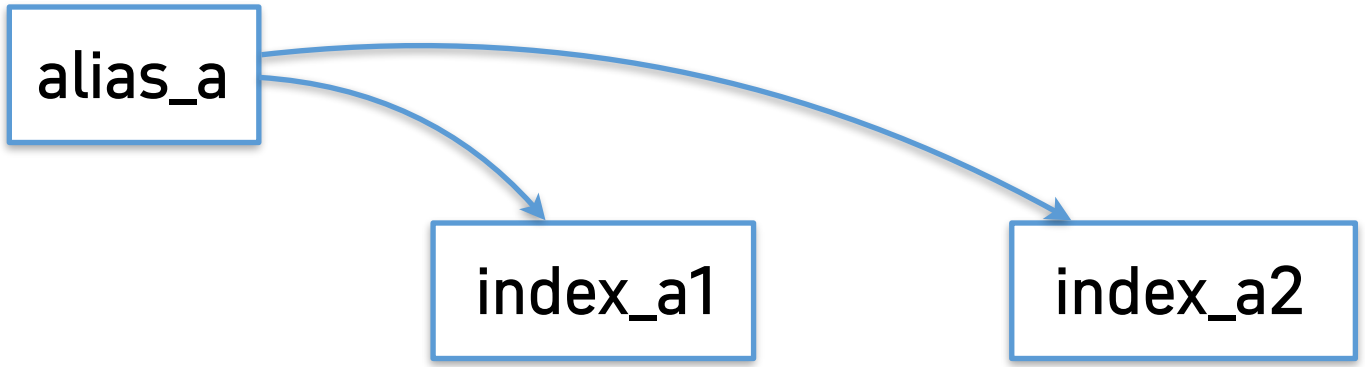

Supported APIs

- Actions with non-standard index resolution logic should also implement TransportIndicesResolvingAction

```
14  /**
15   * An additional interface that should be implemented by TransportAction implementations which need to resolve
16   * IndicesRequests or other action requests which specify indices. This interface allows other components to retrieve
17   * precise information about the indices an action is going to operate on. This is particularly useful for access
18   * control implementations, but can be also used for other purposes, such as monitoring, audit logging, etc.
19   * <p>
20   * Classes implementing this interface should make sure that the reported indices are also actually the indices
21   * the action will operate on. The best way to achieve this, is to move the index extraction code from the execute
22   * methods into reusable methods and to depend on these both for execution and reporting.
23   */
24  public interface TransportIndicesResolvingAction<Request extends ActionRequest> {
25
26      /**
27       * Returns the actual indices the action will operate on, given the specified request and cluster state.
28       */
29      OptionallyResolvedIndices resolveIndices(Request request);
30  }
```

Alias semantic changes

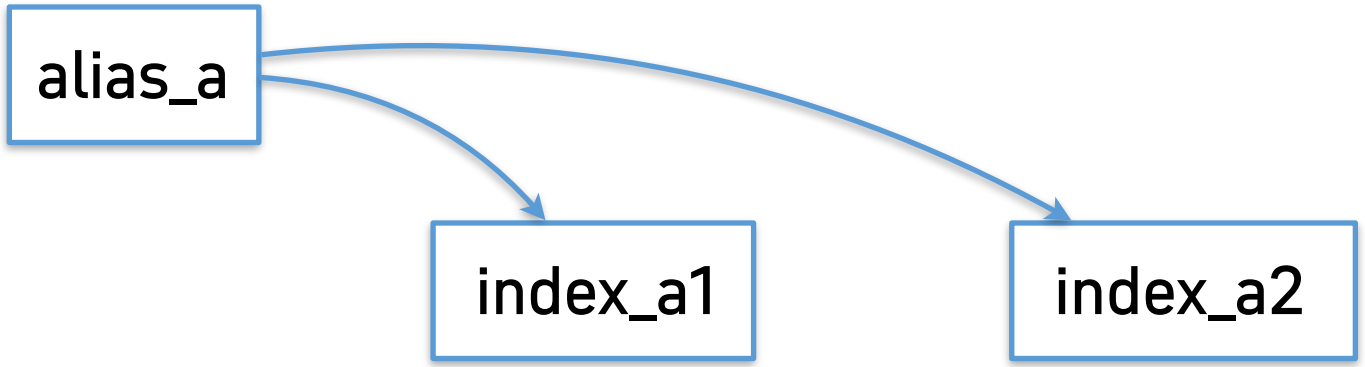
Alias Privilege Semantics: Example



Alias Privilege Semantics: Example

```
1  privileges_on_indices:
2    index_permissions:
3      - index_patterns:
4          - index_a*
5        allowed_actions:
6          - READ
```


Old Semantics

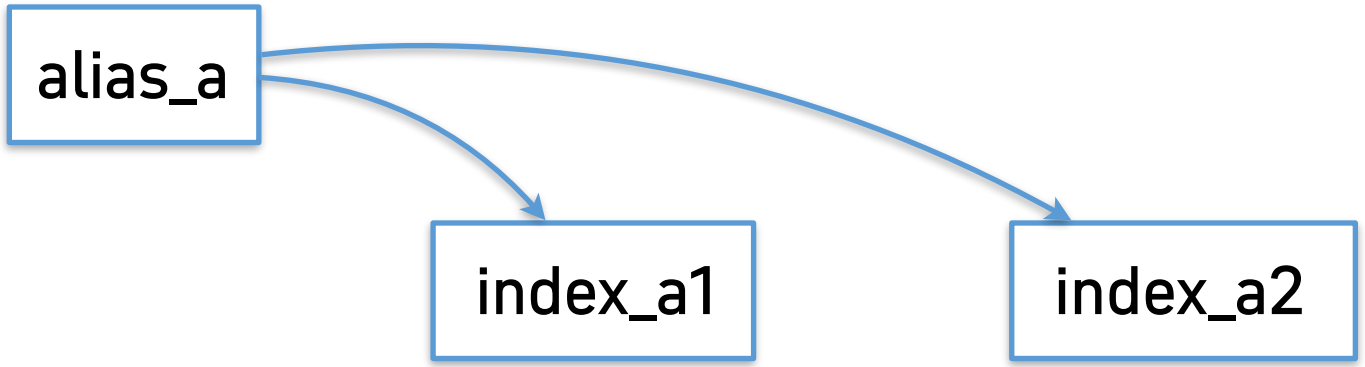



```
GET /alias_a/_search
```

Alias Privilege Semantics: Example

```
privileges_on_just_one_index:
  index_permissions:
    - index_patterns:
        - index_a1
      allowed_actions:
        - READ
```

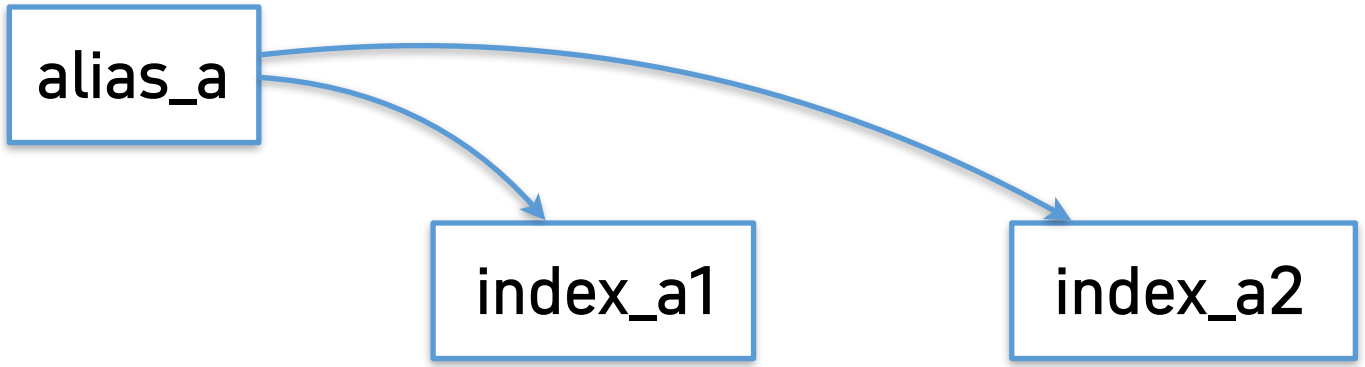
Old Semantics




```
GET /alias_a/_search
```

Result set will only contain documents from index_a1

New Semantics




```
GET /alias_a/_search
```

Privileges must be given directly on alias in order to access it

Alias Privilege Semantics: Example

```
privileges_on_alias:
  index_permissions:
    - index_patterns:
        - alias_a
      allowed_actions:
        - READ
```


New Semantics

- Privileges must be given directly on alias in order to access it
- Aliases will be never broken into individual indices, no matter which index options are specified
- Fixes behavior for filtered aliases, which could lose filter before
- Similar behavior for data streams and backing indices

New Semantics

- If you use aliases, it is necessary to review role privilege configuration before switching to new mode.
- You need to make sure that privileges are granted directly on the aliases.

More semantic changes

More semantic changes

- Alias management APIs require privileges on alias names
- Analyze action without index needs indices:admin/analyze on arbitrary index
- Point in time actions with _all mode need special cluster privileges

More changes

- All system index protection features will be enabled
- All the changes allow us to drop 10 security plugin settings, which simplifies configuration and code
- Improved index resolution code yields performance gains

Outlook

Outlook

- New role configuration structure
- Improved security configuration tooling and API
- Improved validation of configuration

Questions?

Get in touch ...

Nils Bandener

https://www.linkedin.com/in/nils-bandener


OpenSearchCon
EUROPE