

04 - Kibana

Dokumenty mohou být zobrazeny v Kibaně aniž by bylo třeba psát Elasticsearch query.

Nejprve si zobrazíme všechny dostupné indexy v Elasticsearch:

Elasticsearch

Discover

Dashboards

Playground

Machine Learning

Index Management

Index Lifecycle Policies

Snapshot and Restore

Transforms

Rollup Jobs

Ingest

Ingest Pipelines

Logstash Pipelines

Relevance

Synonyms

Query rules

</>

Navigation feedback

Index Management

Index Management docs

IndicesData StreamsIndex TemplatesComponent TemplatesEnrich Policies

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

Search

Lifecycle status

Lifecycle phase

Reload indices

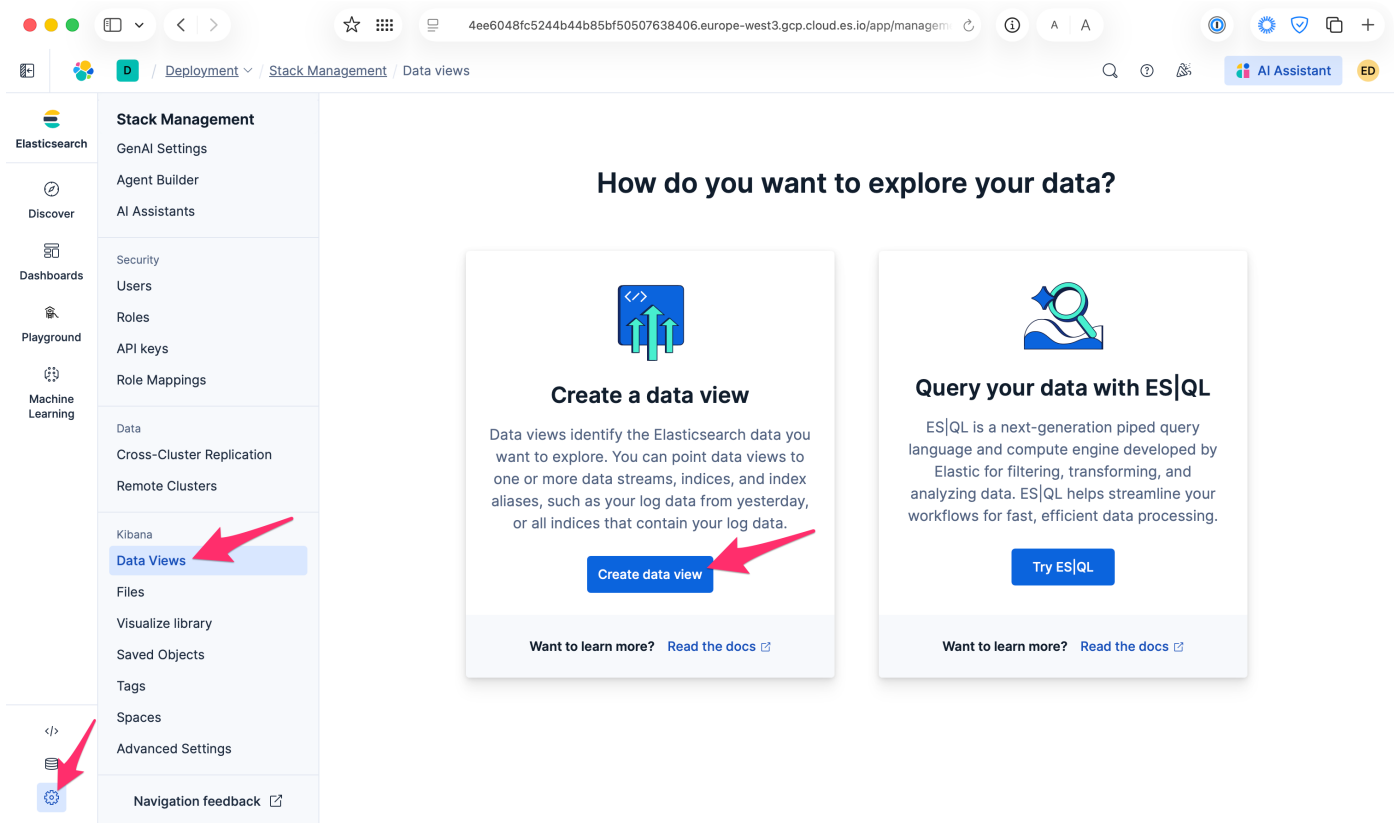
Create index

<input type="checkbox"/>	Name	Health	Status	Primaries	Replicas	Documents...	Storage size	Data stream
<input type="checkbox"/>	.apm-agent-configuration	green	open	1	1	0	499b	
<input type="checkbox"/>	.apm-custom-link	green	open	1	1	0	499b	
<input type="checkbox"/>	.apm-source-map	green	open	1	1	0	499b	
<input type="checkbox"/>	.async-search	green	open	1	1	0	494b	
<input type="checkbox"/>	.ds-.edr-workflow-insights-default-2025.11.08-000001	green	open	1	1	0	499b	.edr-workflow-insights-default
<input type="checkbox"/>	.ds-.kibana-event-log-ds-2025.11.08-000001	green	open	1	1	2	24.95kb	.kibana-event-log-ds
<input type="checkbox"/>	.ds-.logs-elasticsearch.deprecation-default-2025.11.08-000001	green	open	1	1	23	326.68kb	.logs-elasticsearch.deprecation-default

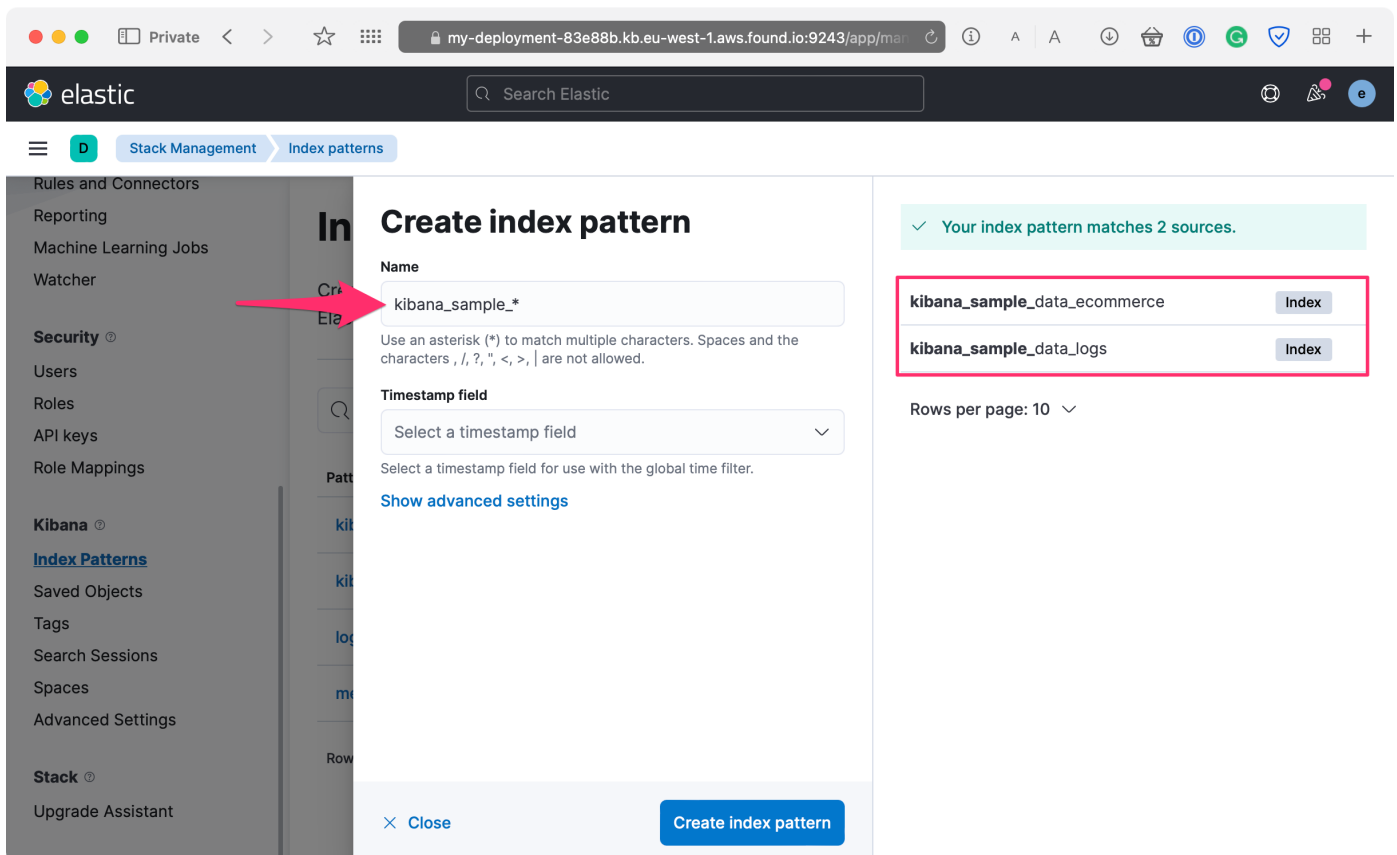
Console

Notebooks

Abychom mohli zobrazit samotné dokumenty, je třeba nejprve vytvořit **Data view** (dříve označovaný jako "index pattern"):



Při definici data view lze využít znak hvězdičky (*). Ten umožní označení více indexů zároveň a jejich současné použití v rámci jednoho data view:



Volitelně lze zvolit pole obsahující datum vytvoření záznamu.

Dokumenty mohou být zobrazeny v tabulce v sekci **Analytics > Discover**:

The screenshot shows the Elastic Discover interface. In the left sidebar, the 'Discover' menu item is highlighted with a red arrow. The main view displays a bar chart with 1,026 hits and a list of document snippets below it.

Document Snippets:

```

> Feb 5, 2022 @ 01:05:46.000 category: Men's Clothing currency: EUR customer_first_name: Jackson
customer_full_name: Jackson Fletcher customer_gender: MALE customer_id: 13
customer_last_name: Fletcher customer_phone: (empty) day_of_week: Saturday
day_of_week_i: 5 email: jackson@fletcher-family.zzz
event.dataset: sample_ecommerce geoip.city_name: Los Angeles

> Feb 5, 2022 @ 01:00:00.000 category: Women's Shoes, Women's Clothing currency: EUR
customer_first_name: Diane customer_full_name: Diane Elliott
customer_gender: FEMALE customer_id: 22 customer_last_name: Elliott
customer_phone: (empty) day_of_week: Saturday day_of_week_i: 5
email: diane@elliott-family.zzz event.dataset: sample_ecommerce

```

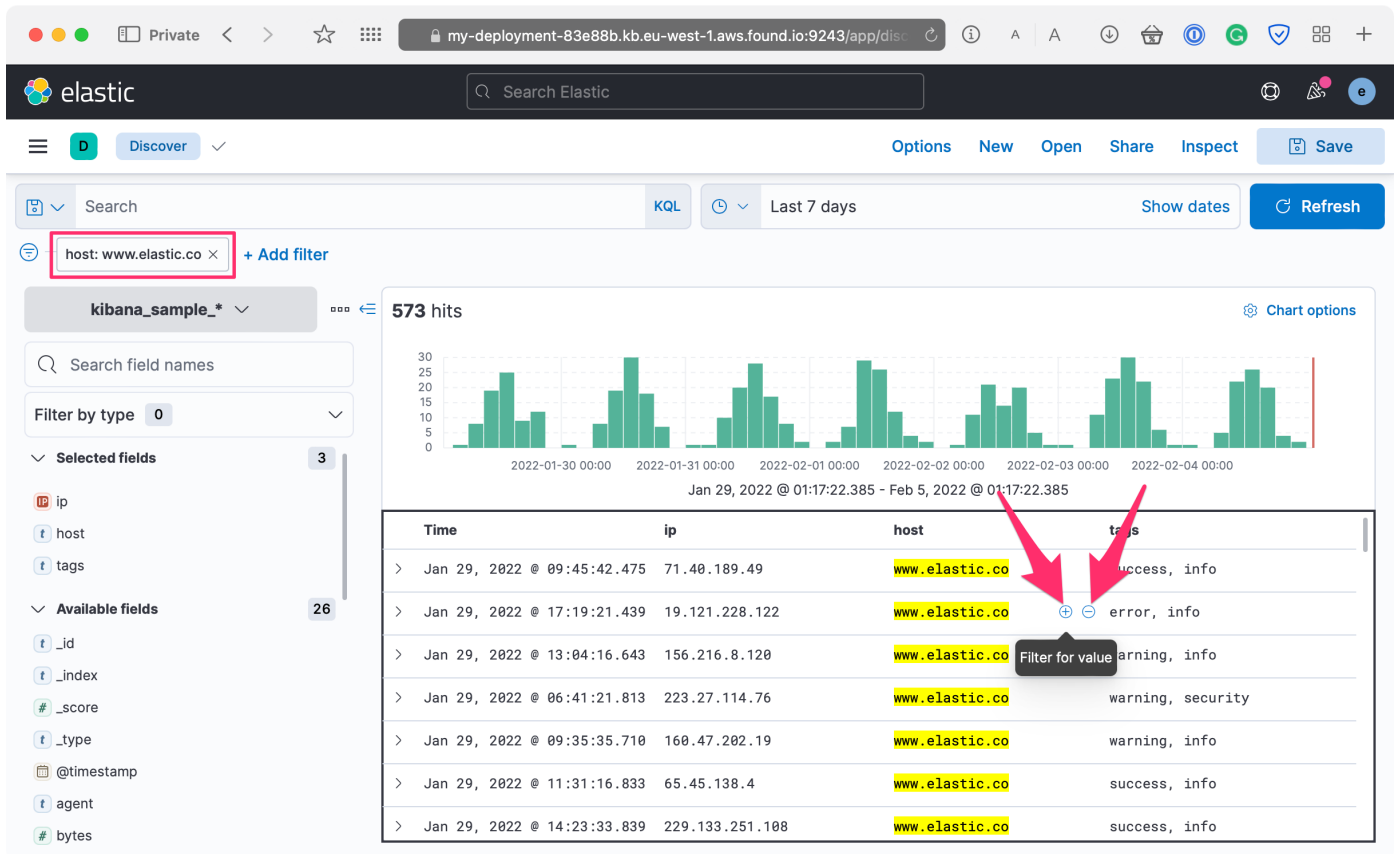
Tabulku lze vytvářet výběrem sloupců kliknutím na tlačítko plus vedle názvu sloupce:

The screenshot shows the Elastic Discover interface with the 'Add filter' section expanded. The 'Selected fields' list includes 'ip', 'host', and 'tags'. The 'Available fields' list includes '_id', '_index', '_score', '_type', '@timestamp', 'agent', and 'bytes'. A red arrow points to the plus icon next to the 'ip' field in the 'Selected fields' list.

Table Data:

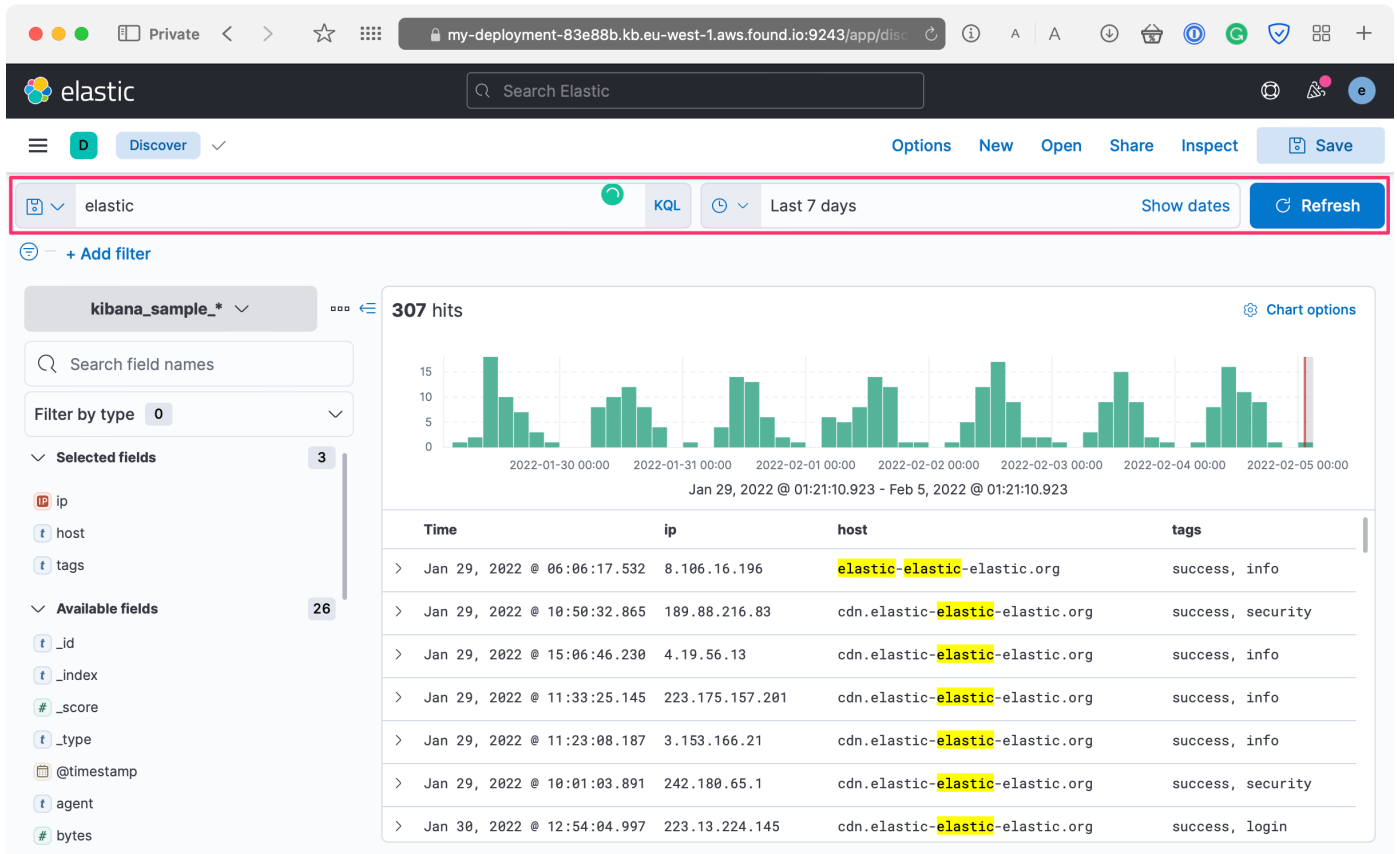
Time	ip	host	tags
> Jan 29, 2022 @ 08:52:19.729	74.171.40.87	artifacts.elastic.co	success, info
> Jan 29, 2022 @ 09:45:42.475	71.40.189.49	www.elastic.co	success, info
> Jan 29, 2022 @ 17:19:21.439	19.121.228.122	www.elastic.co	error, info
> Jan 29, 2022 @ 18:50:53.556	139.85.198.193	artifacts.elastic.co	success, info
> Jan 29, 2022 @ 11:39:38.178	84.145.10.104	artifacts.elastic.co	success, info
> Jan 29, 2022 @ 13:04:16.643	156.216.8.120	www.elastic.co	warning, info
> Jan 29, 2022 @ 06:41:21.813	223.27.114.76	www.elastic.co	warning, security

Data lze filtrovat kliknutím na znaménko plus nebo mínus vedle filtrované hodnoty:



Pokud jste definovali, které pole nese datum vzniku záznamu, bude také k dispozici výběr data a času.

V neposlední řadě lze v dokumentech fulltextově vyhledávat:



Globální nastavení zobrazení (například jiný formát datumu) lze nastavit v **Stack Management** > **Advanced Settings**:

D

Stack Management / Advanced Settings

Bytes format

Default numeral format for the "bytes" format

format:bytes:defaultPattern

0,0.[0]b

Currency format

Default numeral format for the "currency" format

format:currency:defaultPattern

(\$0,0.[00])

Field type format name

Map of the format name to use by default for each field type.
"_default_" is used if the field type is not mentioned explicitly

format:defaultTypeMap

```
{
  "ip": { "id": "ip", "params": {} },
  "date": { "id": "date", "params": {} },
  "date_nanos": { "id": "date_nanos", "params": {}, "es": true },
  "number": { "id": "number", "params": {} },
  "boolean": { "id": "boolean", "params": {} },
  "_source": { "id": "_source", "params": {} },
  "_default_": { "id": "string", "params": {} }
}
```

Formatting locale

Numeral language locale
Default: en

format:number:defaultLocale

Czech

Reset to default

Number format

Default numeral format for the "number" format

format:number:defaultPattern

0,0.[000]

Případně je možné formát zobrazení nastavit pro konkrétní pole kliknutím na ikonu tužky v detailu data view:

D

Stack Management / Index patterns / order

Ingest

Ingest Node Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Alerts and Actions

Reporting

Kibana

Index Patterns

Saved Objects

Spaces

Advanced Settings

Stack

License Management

8.0 Upgrade Assistant

order

★ ↺ 🗑

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

Fields (42)

Scripted fields (0)

Source filters (0)

🔍 Search

All field types ▾

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	✎
._id	string		●	●	✎
._index	string		●	●	✎
._score	number				✎
._source	_source				✎
._type	string		●	●	✎
channel	string		●	●	✎
createdDate	date		●	●	✎
customerEmail	string		●	●	✎
customerId	number		●	●	✎

Rows per page: 10 ▾

< 1 2 3 4 5 >

Například použití vlastního formátování data lze nastavit pomocí uvedení odpovídajícího patternu. Dostupné parametry pro formátování data naleznete v [dokumentaci](#). Pod polem je vidět náhled pro několik vzorových hodnot:

Stack Management / Index patterns / order / createdDate

Ingest ⓘ

Ingest Node Pipelines

Data ⓘ

Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters

Alerts and Insights ⓘ

Alerts and Actions
Reporting

Kibana ⓘ

[Index Patterns](#)
Saved Objects
Spaces
Advanced Settings

Stack ⓘ

License Management
8.0 Upgrade Assistant

order

Edit createdDate

Type
date

Format (Default: Date)
Date

Formatting allows you to control the way that specific values are displayed. It can also cause values to be completely changed and prevent highlighting in Discover from working.

Moment.js format pattern (Default: MMM D, YYYY @ HH:mm:ss.SSS)
YYYY-MM-DD HH:mm:ss

[Documentation](#)

Samples

Input	Output
1608068067478	2020-12-15 22:34:27
1577833200000	2020-01-01 00:00:00
1609455599999	2020-12-31 23:59:59

Popularity
2

[Save field](#) [Cancel](#)

Dále je možné nastavit vlastní formátování pro číselné hodnoty. Stačí uvést vhodný pattern, kde:

- `,` je oddělovač řádů
- `.` je oddělovač desetinné části
- `$` je znak měny

Ingest ②

Ingest Node Pipelines

Data ②

Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters

Alerts and Insights ②

Alerts and Actions
Reporting

Kibana ②

[Index Patterns](#)

Saved Objects
Spaces
Advanced Settings

Stack ②

License Management
8.0 Upgrade Assistant

order

Edit **totalPrice**

Type

number

Format (Default: Number)

Number

Formatting allows you to control the way that specific values are displayed. It can also cause values to be completely changed and prevent highlighting in Discover from working.

Numeral.js format pattern (Default: 0,0.[000])

0,0.00 \$

[Documentation](#)

Samples

Input	Output
10000	10 000,00 Kč
12.345678	12,35 Kč
-1	-1,00 Kč
-999	-999,00 Kč
0.52	0,52 Kč

Popularity

3

Save field

Cancel

Úkol: Kibana

1. Vytvořte následující dokumenty v Kibaně

```
POST europe_countries/_doc
{
  "country": "Germany",
  "subregion": "Western Europe",
  "population": 145934462,
  "area": 357386,
  "isEuMember": true,
  "euAccessionDate": "1958-01-01"
}
```

```
POST europe_countries/_doc
{
  "country": "United Kingdom",
  "subregion": "Northern Europe",
  "population": 67886011,
  "area": 242495,
  "isEuMember": false
}
```

```
POST europe_countries/_doc
{
  "country": "France",
  "subregion": "Western Europe",
  "population": 65273511,
  "area": 551695,
  "isEuMember": true,
  "euAccessionDate": "1958-01-01"
}
```

```
POST europe_countries/_doc
{
  "country": "Italy",
  "subregion": "Southern Europe",
  "population": 60461826,
  "area": 301338,
  "isEuMember": true,
  "euAccessionDate": "1958-01-01"
}
```

```
POST europe_countries/_doc
{
  "country": "Spain",
  "subregion": "Southern Europe",
  "population": 46754778,
  "area": 498511,
  "isEuMember": true,
  "euAccessionDate": "1986-01-01"
}
```

2. Vytvořte **data view** pro index `europe_countries`
 3. V Kibaně jděte do sekce **Discover**, zvolte data view z předchozího kroku a vytvořte tabulku, která:
 1. Obsahuje sloupce: `country`, `subregion`, `area`, `population`, `isEuMember`, `euAccessionDate`
 2. Řádky jsou řazeny podle sloupce `area` v sestupném pořadí
 3. Dokumenty jsou vyfiltrovány na `population` menší než `100,000,000`
 4. Dokumenty jsou vyfiltrovány na `isEuMember` rovno `true`
 5. Nastavte vlastní formátování pro sloupec `euAccessionDate` - zobrazte pouze datum, bez času
- Výsledná tabulka by měla vypadat následovně:

KQL

Refresh

+ Add filter

⇒ 3 hits

country	subregion	area ↓	population	isEuMember	euAccessionDate
> France	Western Europe	551,695	65,273,511	true	Jan 1, 1958
> Spain	Southern Europe	498,511	46,754,778	true	Jan 1, 1986
> Italy	Southern Europe	301,338	60,461,826	true	Jan 1, 1958