

비정형 빅데이터 분석의 응용과 실습

Week-07. Elastic Stack

서중원 2020.11.07

Elasticsearch Mapping

Mapping이란?

- 관계형 데이터의 스키마와 동일
- Mapping 없이 데이터를 엘라스틱서치에 삽입?
 - 가능
 - 하지만, Mapping을 없이 데이터를 넣는 것은 데이터의 사용성이 떨어질 수 있음
 - 예를들어 2020-11-07이라는 값을 Mapping없이 넣는다면?
 - String으로 인지할 수 있음
 - 날짜별 정렬, 월별 정렬/필터링과 같은 연산을 사용할 수 없음
 - 숫자를 입력했지만, 문자열로 인식했다?
 - Min, max, mean, median과 같은 연산을 사용할 수 X
- 가능하다면! 항상 Mapping을 먼저 지정해 놓고 데이터를 삽입!
 - 데이터 먼저 넣고, Mapping을 후에 지정해줄 수도 있음

Elasticsearch Search

Search 방식

- request_body에 json 형식으로 조건을 작성!

```
body = {  
    "query": {  
        "term": {  
            "points":30  
        }  
    }  
}  
  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Elasticsearch Aggregation

Aggregation 이란?

- Search Query 사용시 수치적 값들의 다양한 값을 얻어 낼 수 있다.

```
body = {  
    "size" : 0,  
    "aggs" : {  
        "avg_score" : {  
            "avg" : {  
                "field" : "points"  
            }  
        }  
    }  
}  
  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Elasticsearch Bucket Aggregation

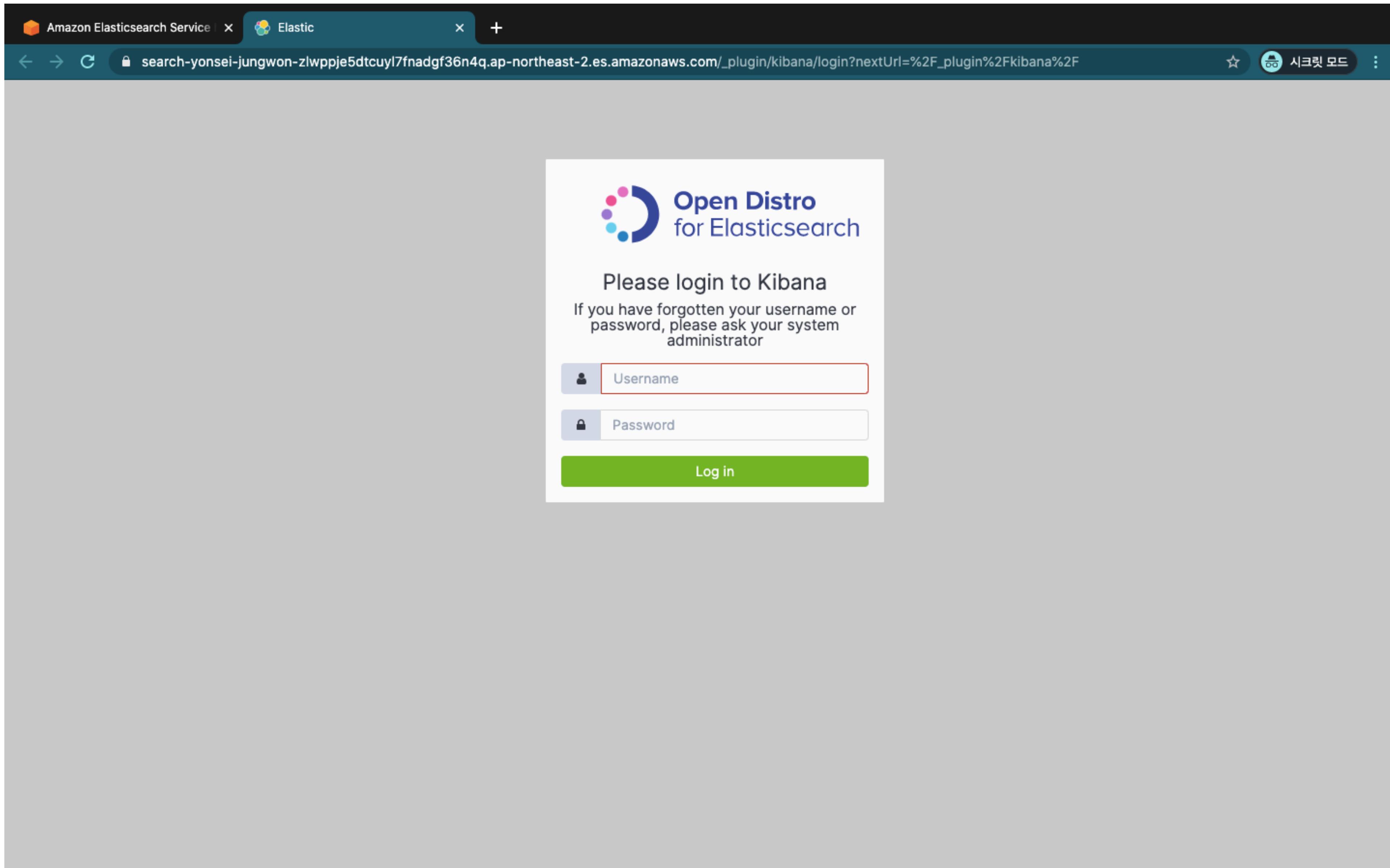
Bucket Aggregation 이란?

- RDB의 group by와 유사한 기능
- “document의 bucket을 만든다”

```
body = {  
    "size" : 0,  
    "aggs" : {  
        "team_stats" : {  
            "terms" : {  
                "field" : "team"  
            },  
            "aggs" : {  
                "stats_score" : {  
                    "stats" : {  
                        "field" : "points"  
                    }  
                }  
            }  
        }  
    }  
}  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Kibana

AWS 엘라스틱 서치 콘솔로 이동후 Kibana 부분의 링크 클릭!



좌측의 메뉴화면에서 Index Management 클릭후, 그동안 생성한 인덱스들이 잘 들어갔는지 확인

The screenshot shows the Kibana home page with the URL https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/home. The left sidebar has a 'Management' section with 'Index Management' selected. The main content area displays sections for 'Manage and Administer the Elastic Stack' and 'Discover'.

Recently viewed
No recently viewed items

Kibana

- Anomaly Detection
- SQL Workbench
- Alerting
- Discover
- Dashboard
- Visualize

Management

- Index Management** (selected)
- Dev Tools
- Stack Management

Security

Tenants

Account

Dock navigation

Discover
Interactively explore your data by querying and filtering raw documents.

Visualize
Create visualizations and aggregate data stores in your Elasticsearch indices.

Console
Skip cURL and use this JSON interface to work with your data directly.

Saved Objects
Import, export, and manage your saved searches, visualizations, and dashboards.

Security Configuration
Configure users, roles and permissions for Open Distro Security.

Didnt find what you were looking for?
[View full directory of Kibana plugins](#)

https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/opendistro_index_management_kibana

잘들어갔네요!

Amazon Elasticsearch Service | x Elastic x +

search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/opendistro_index_management_kibana#/indices?from=...

시크릿 모드 : admin

Index Management / Indices

Index Management

Index Policies

Managed Indices

Indices

Indices

Apply policy

Search

Off

<input type="checkbox"/> Index ↓	Health	Managed by Policy	Status	Total size	Primaries si...	Total docu...	Deleted do...	Primaries	Replicas
<input type="checkbox"/> toy_index	● yellow	No	open	25.7kb	25.7kb	5	2	5	1
<input type="checkbox"/> movie_index	● yellow	No	open	736.7kb	736.7kb	403	0	5	1
<input type="checkbox"/> classes	● yellow	No	open	26.1kb	26.1kb	24	0	5	1
<input type="checkbox"/> basketball	● yellow	No	open	25.7kb	25.7kb	16	0	5	1
<input type="checkbox"/> .opendistro_security	● green	No	open	50.1kb	50.1kb	9	4	1	0
<input type="checkbox"/> .kibana_92668751_admin	● yellow	No	open	3.8kb	3.8kb	1	0	1	1
<input type="checkbox"/> .kibana_1	● green	No	open	208b	208b	0	0	1	0

Rows per page: 20 < 1 >

https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/opendistro_index_management_kibana#/indices

Kibana Discover

가장 기본이 되는 View



기존에 Elasticsearch에 등록된 Index를 Kibana에 등록, Stack Management 클릭

The screenshot shows the Amazon Elasticsearch Service console interface. The top navigation bar includes tabs for 'Amazon Elasticsearch Service' and 'Elastic'. The URL in the address bar is https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/opendistro_index_management_kibana#/indices?from=.... The top right corner shows a user icon and the word 'admin'.

The left sidebar has a tree view with the following sections and items:

- Kibana**:
 - Anomaly Detection
 - SQL Workbench
 - Alerting
 - Discover** (selected)
 - Dashboard
 - Visualize
- Management**:
 - Index Management (selected)
 - Dev Tools
 - Stack Management
- Security
- Tenants
- Account
- Dock navigation

The main content area displays a table of indices:

	Health	Managed by Policy	Status	Total size	Primaries si...	Total docu...	Deleted do...	Primaries	Replicas
...	● yellow	No	open	25.7kb	25.7kb	5	2	5	1
...	● yellow	No	open	736.7kb	736.7kb	403	0	5	1
...	● yellow	No	open	26.1kb	26.1kb	24	0	5	1
...	● yellow	No	open	25.7kb	25.7kb	16	0	5	1
...	● green	No	open	50.1kb	50.1kb	9	4	1	0
2668751_admin	● yellow	No	open	3.8kb	3.8kb	1	0	1	1
...	● green	No	open	208b	208b	0	0	1	0

At the bottom of the main content area, there is a URL: https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/discover.

The screenshot shows the Kibana interface for creating an index pattern. The top navigation bar includes tabs for 'Amazon Elasticsearch Service' and 'Elastic', and a search bar with the URL 'search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_pattern?_g=()'. The user is logged in as 'admin'. The left sidebar has links for 'Kibana', 'Index Patterns' (which is selected), 'Saved Objects', and 'Advanced Settings'. The main content area is titled 'Create index pattern' and explains that Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations. A checkbox 'Include system indices' is present. The 'Step 1 of 2: Define index pattern' section contains a text input field with 'basketball*' and a note explaining the use of wildcards. Below the input field, a success message states 'Success! Your index pattern matches 1 index.' with an example 'basketball'. At the bottom, there is a dropdown for 'Rows per page: 10'.

In order to visualize and explore data in Kibana, you'll need to create an index pattern to retrieve data from Elasticsearch.

Kibana

[Index Patterns](#)

Saved Objects

Advanced Settings

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

Step 1 of 2: Define index pattern

Index pattern

basketball*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ Success! Your index pattern matches 1 index.

basketball

Rows per page: 10

submit_date 선택

The screenshot shows the 'Create index pattern' interface in Kibana. The top navigation bar includes tabs for 'Amazon Elasticsearch Service' and 'Elastic'. The URL in the address bar is `search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_pattern?_g=()`. The user is logged in as 'admin'. The left sidebar has 'Index Patterns' selected under 'Kibana'.

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

[Include system indices](#)

Step 2 of 2: Configure settings

You've defined **basketball*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

submit_date

The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

[Show advanced options](#)

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

각각의 field가 잘 들어갔는지 확인

Amazon Elasticsearch Service | X basketball* - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns/aae2c510-... ☆ 시크릿 모드 :

Stack Management / Index patterns / basketball*

admin

Kibana

Index Patterns

Saved Objects

Advanced Settings

basketball*

Time Filter field name: 'submit_date' Default

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

Fields (14) 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		●	●	✎
assist	number		●	●	✎
assists	number		●	●	✎
blocks	number		●	●	✎
name	string		●	●	✎
points	number		●	●	✎

우상단에서 날짜 조정후 Basketball 데이터 확인

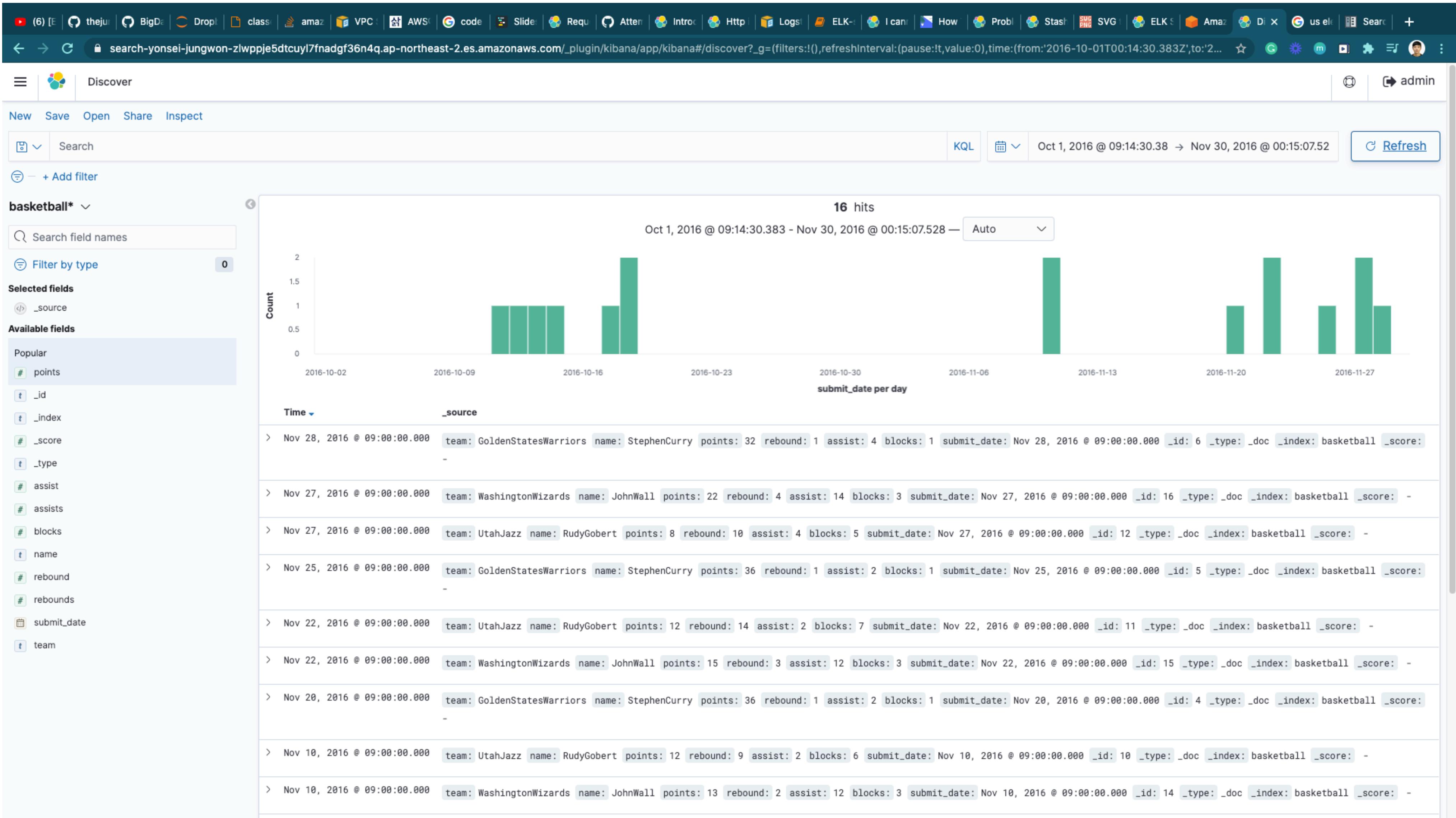
The screenshot shows the Kibana Discover interface. At the top, there is a browser-style header with various tabs and icons. Below it is the main navigation bar with options like 'Discover', 'New', 'Save', 'Open', 'Share', and 'Inspect'. A search bar is present, followed by a 'KQL' button and a date range selector set to 'Last 15 hours'. On the left, a sidebar displays a search term 'basketball*' with a dropdown menu, a 'Search field names' input, and a 'Filter by type' section showing 0 results. Below this are sections for 'Selected fields' (including '_source') and 'Available fields'. The main content area shows a message: 'No results match your search criteria'. Below this message is a section titled 'Expand your time range' with a explanatory text about date fields and time ranges.

No results match your search criteria

Expand your time range

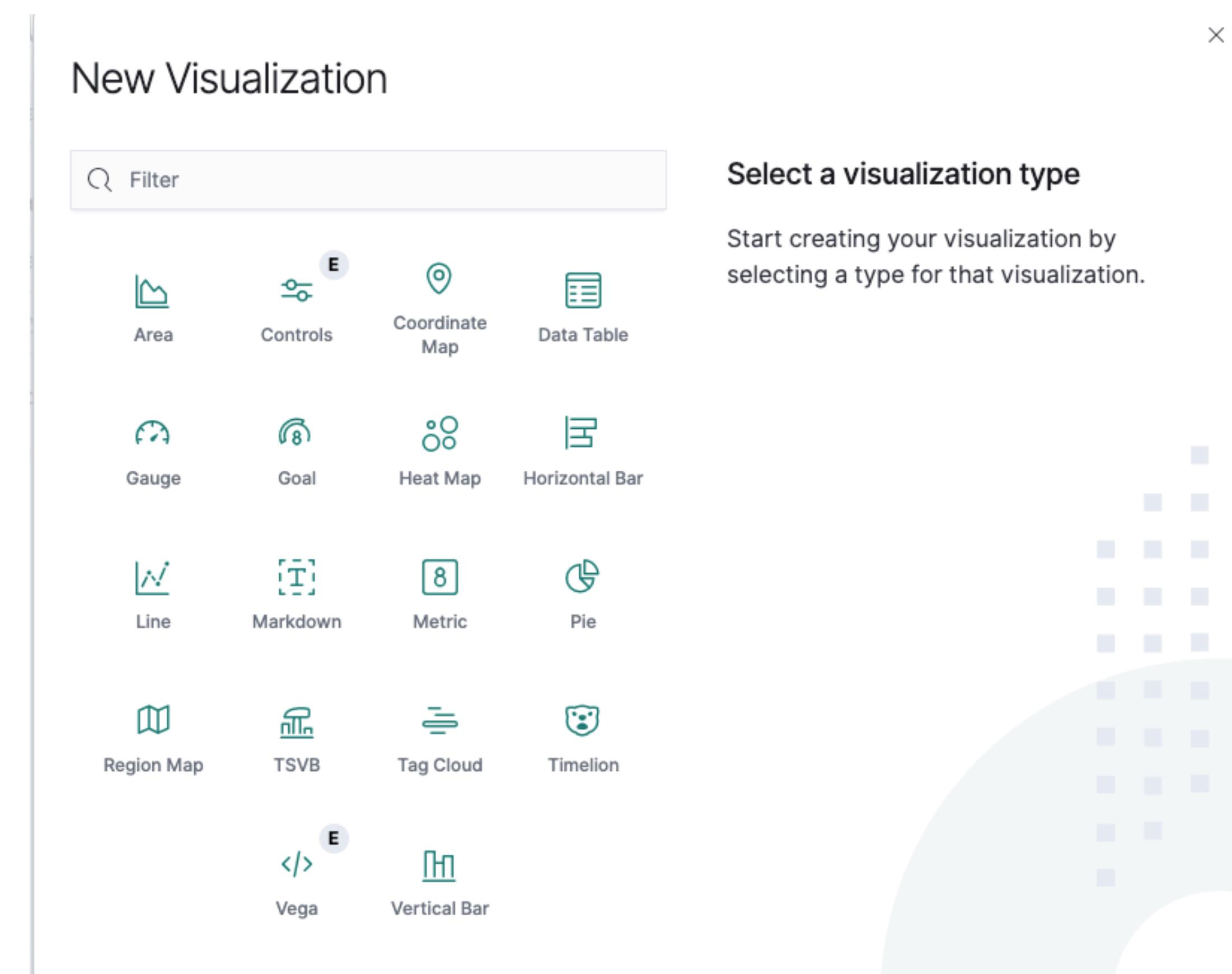
One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try changing the time range to one which contains data.

2016년 10월 1일 부터 11월 30일까지로 설정



Kibana Visualize

Bar Chart, Pie Chart



메뉴에서 Visualize 클릭

Amazon Elasticsearch Service | x Discover - Elastic x +

← → C search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!,value:0),time:(from:'2016-10-01T12:19:57.679Z',to:'2016-12-01T12:20:06.855Z'))&_sourceType=discover

Discover admin Refresh

Home

Recently viewed

No recently viewed items

Kibana

Anomaly Detection

SQL Workbench

Alerting

Discover

Dashboard

Visualize

Management

Index Management

Dev Tools

Stack Management

Security

Tenants

Account

Dock navigation

close KQL Oct 1, 2016 @ 21:19:57.679 → Dec 1, 2016 @ 21:20:06.855 Auto

16 hits Oct 1, 2016 @ 21:19:57.679 - Dec 1, 2016 @ 21:20:06.855 submit_date per day

Date	points
2016-10-11	30
2016-10-12	3
2016-10-13	32
2016-10-14	4
2016-10-17	28
2016-10-18	8
2016-10-19	8
2016-10-20	12
2016-10-21	13
2016-10-22	36
2016-10-23	0
2016-10-24	0
2016-10-25	0
2016-10-26	0
2016-10-27	0
2016-10-28	0
2016-10-29	0
2016-10-30	0
2016-10-31	0
2016-11-01	0
2016-11-02	0
2016-11-03	0
2016-11-04	0
2016-11-05	0
2016-11-06	0
2016-11-07	0
2016-11-08	0
2016-11-09	0
2016-11-10	0
2016-11-11	0
2016-11-12	0
2016-11-13	0
2016-11-14	0
2016-11-15	0
2016-11-16	0
2016-11-17	0
2016-11-18	0
2016-11-19	0
2016-11-20	0
2016-11-21	0
2016-11-22	0
2016-11-23	0
2016-11-24	0
2016-11-25	0
2016-11-26	0
2016-11-27	0
2016-11-28	0
2016-11-29	0
2016-11-30	0
2016-12-01	0

https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,value:0),time:(from:'2016-10-01T12:19:57.679Z',to:'2016-12-01T12:20:06.855Z'))&_sourceType=discover

첫 시각화 만들기!

Amazon Elasticsearch Service | X Discover - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:1m),time:(from:now-1h,until:now))&_indexPattern=

시크릿 모드

☰ Visualize admin



Create your first visualization

You can create different visualizations, based on your data.

+ Create new visualization

Vertical Bar 고르기

Amazon Elasticsearch Service | X Discover - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:1m))&_indexPattern=&_sourceType=discover

Visualize admin

New Visualization

Filter

Area Controls Coordinate Map Data Table

Gauge Goal Heat Map Horizontal Bar

Line Markdown Metric Pie

Region Map TSVB Tag Cloud Timelion

Vega Vertical Bar

Vertical Bar
Assign a continuous variable to each axis

The screenshot shows the Kibana interface with a modal window titled 'New Visualization'. The modal contains a grid of visualization icons. The 'Vertical Bar' icon, which is a bar chart with a vertical axis, is highlighted with a light blue border. To its right, the text 'Vertical Bar' and 'Assign a continuous variable to each axis' is displayed. The other visualization types shown include Area, Controls, Coordinate Map, Data Table, Gauge, Goal, Heat Map, Horizontal Bar, Line, Markdown, Metric, Pie, Region Map, TSVB, Tag Cloud, Timelion, Vega, and another Vertical Bar icon.

Basketball 인덱스 고르기

Amazon Elasticsearch Service | X Discover - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:1m),time:(from:now-1h,until:now))&_index=basketball*&_source_type=Vertical Bar

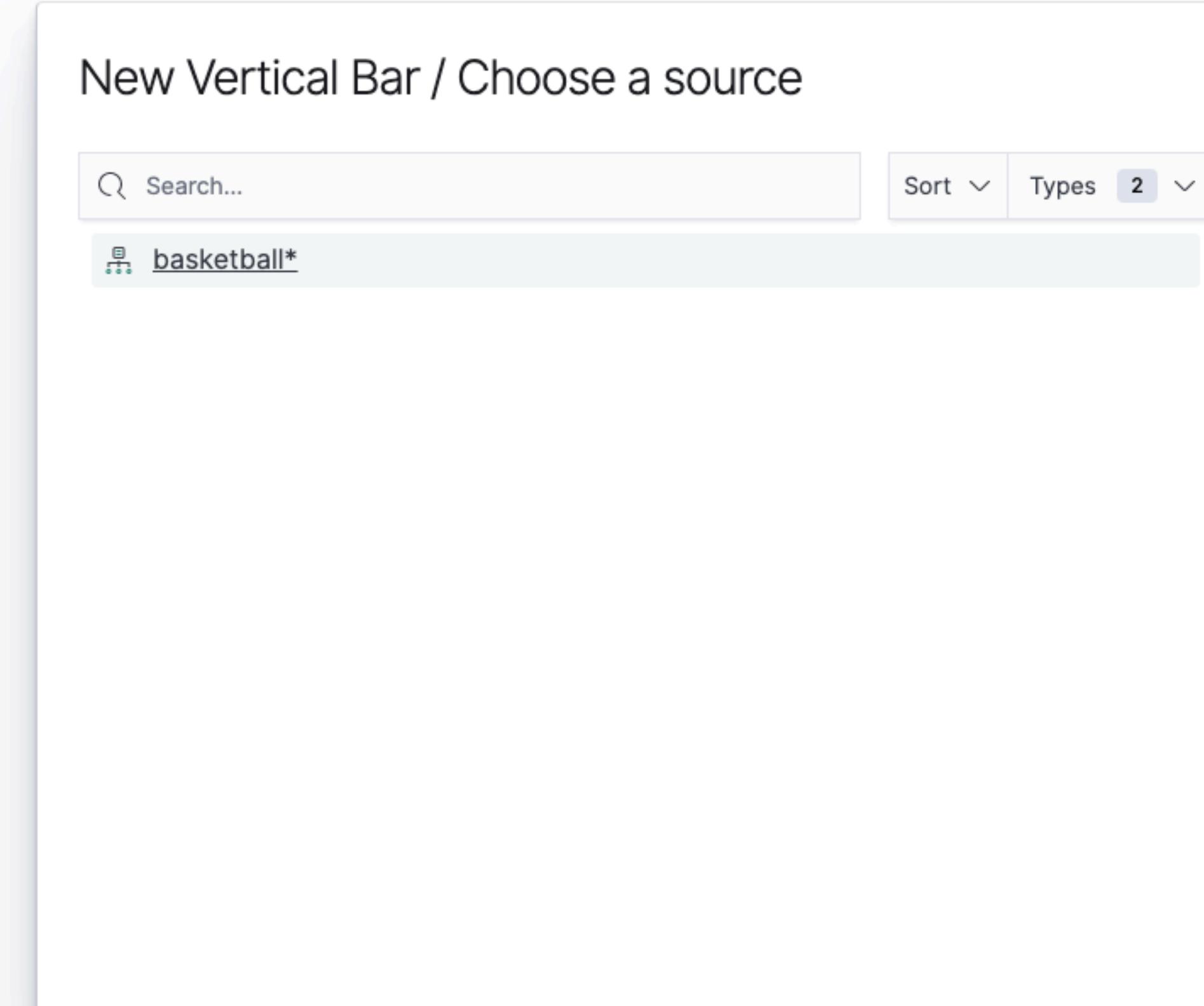
시크릿 모드 admin

☰ Visualize

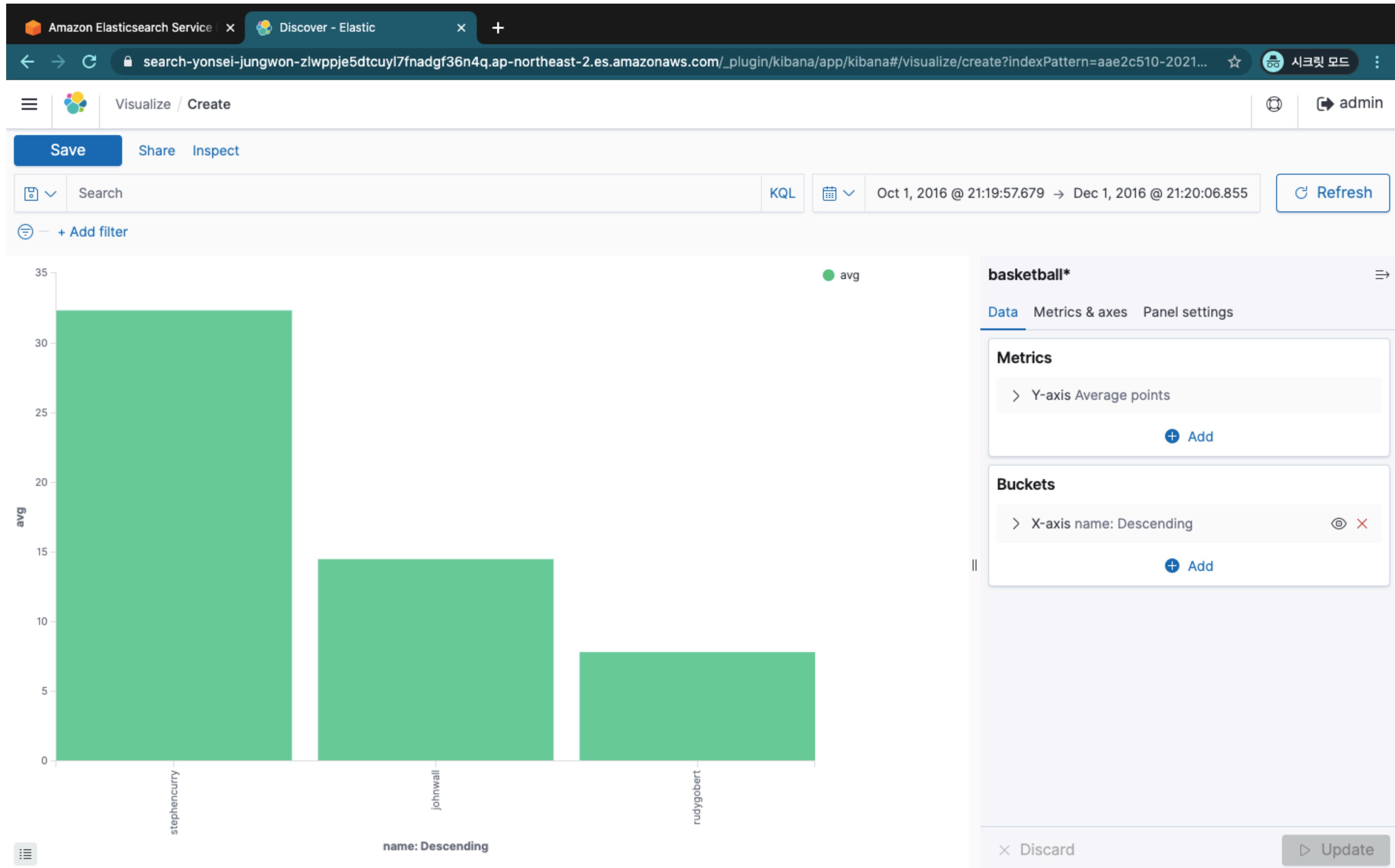
New Vertical Bar / Choose a source

Search... Sort Types 2

basketball*



Metric과 Buckets 설정



The screenshot shows the Kibana Visualize interface. At the top, there are tabs for "Amazon Elasticsearch Service" and "barchart - Elastic". The URL in the browser is `search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:1m),time:(from:'now-1h',to:'now'))&_sourceType=es`. On the right side of the header, there are icons for "시크릿 모드" (Secret Mode) and "admin".

The main area is titled "Visualizations". It features a search bar labeled "Search..." and a "Create visualization" button. Below these are two columns of data:

<input type="checkbox"/> Title	Type	Description	Actions
<input type="checkbox"/> barchart	Vertical Bar		

At the bottom left, it says "Rows per page: 20" with a dropdown arrow. At the bottom right, there are navigation arrows for the first page.

Pie Chart 고르기

Amazon Elasticsearch Service | X barchart - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:1m))&_indexPattern=&_sourceType=discover 시크릿 모드 admin

New Visualization

Filter

Area Controls Coordinate Map Data Table

Gauge Goal Heat Map Horizontal Bar

Line Markdown Metric Pie

Region Map TSVB Tag Cloud Timelion

Vega Vertical Bar

Pie
Compare parts of a whole

Actions

1 >

This screenshot shows the Kibana visualization selection interface. A modal window titled 'New Visualization' is open, displaying a grid of visualization types. The 'Pie' type is highlighted with a blue border and a tooltip explaining it 'Compare parts of a whole'. Other visible types include Area, Controls, Coordinate Map, Data Table, Gauge, Goal, Heat Map, Horizontal Bar, Line, Markdown, Metric, Region Map, TSVB, Tag Cloud, Timelion, Vega, and Vertical Bar. The background shows a blurred view of the Kibana dashboard.

마찬가지로 Basketball 고르기

Amazon Elasticsearch Service | X barchart - Elastic +

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pause:!,interval:10s),time:(from:now-1h,until:now))&_sourceType=visualization

Visualize

New Pie / Choose a source

Search... Sort Types 2

basketball*

Title

barchart

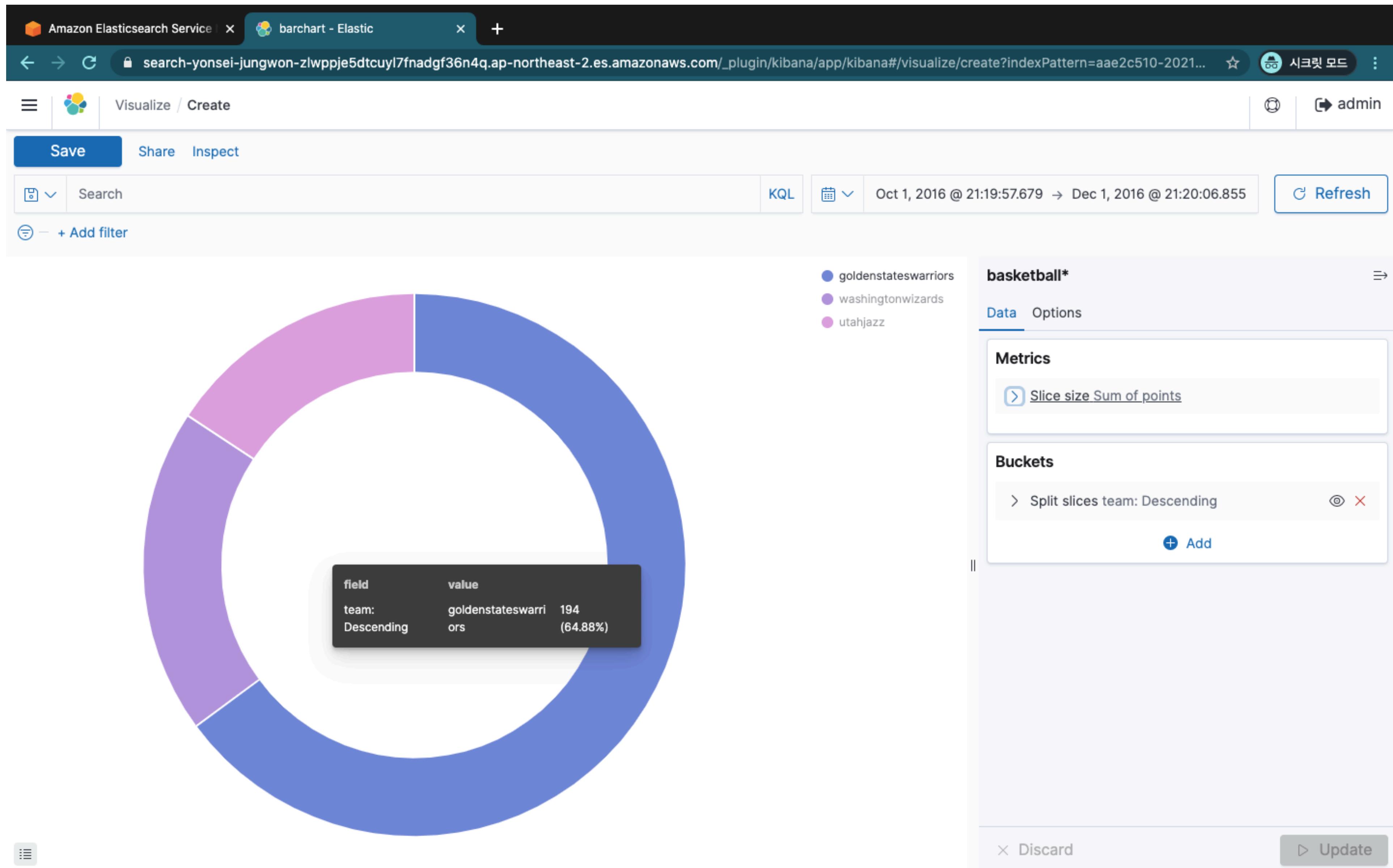
Rows per page

Actions

visualization

1

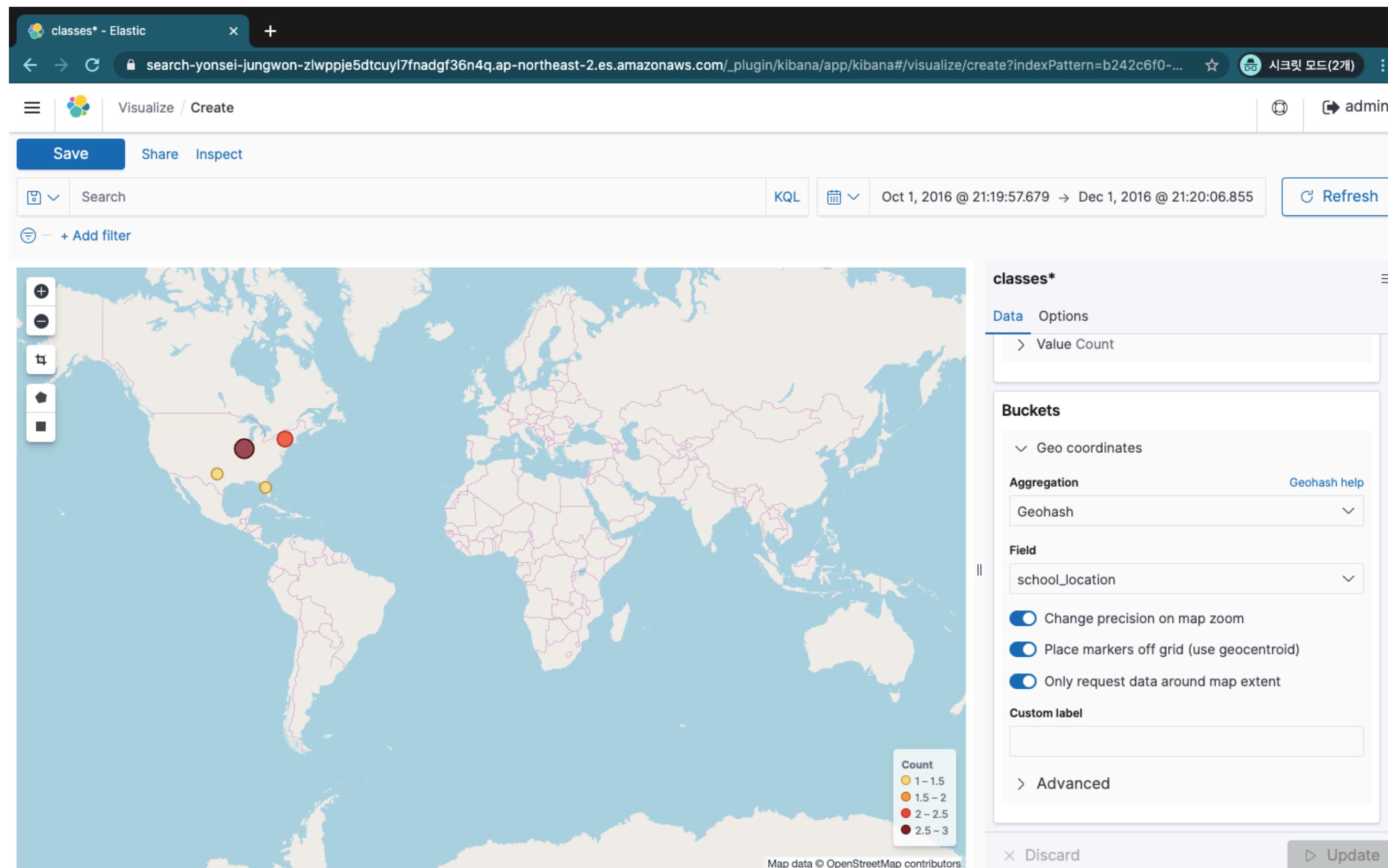
Metric과 Bucket 설정!



Kibana Visualize

Coordinated Map

- 위도와 경도 데이터를 활용하여, 지도상에 해당하는 데이터 포인트를 출력!



Stack Management 클릭

The screenshot shows the Kibana interface for managing index patterns. The top navigation bar includes tabs for 'Discover - Elastic' and '+'. The URL is `search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns?_g=(fi...)`. On the right, there are icons for 'Secret Mode (2)' and a user 'admin'. The left sidebar has a tree view with sections like 'Recently viewed', 'Kibana' (with options for Anomaly Detection, SQL Workbench, Alerting, Discover, Dashboard, Visualize), 'Management' (with Index Management, Dev Tools, Stack Management selected), 'Security', 'Tenants', 'Account', and 'Dock navigation'. The main content area is titled 'patterns' with a search bar and a 'Create index pattern' button.

인덱스 패턴 생성!

The screenshot shows the Kibana interface for managing index patterns. The title bar indicates the user is on the 'Discover - Elastic' tab. The URL in the address bar is [https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns?_g=\(fi...](https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns?_g=(fi...). The top navigation bar includes icons for back, forward, search, and refresh, along with a 'Secret Mode(2개)' button and a user 'admin'. The left sidebar under 'Kibana' has links for 'Index Patterns' (which is selected and highlighted in blue), 'Saved Objects', and 'Advanced Settings'. The main content area is titled 'Index patterns' with a help icon. It features a search bar labeled 'Search...', a table header 'Pattern ↑', and a single row for 'basketball*' which is marked as 'Default'. Below the table are buttons for 'Rows per page: 10' and navigation arrows (< 1 >). A large blue button on the right says '+ Create index pattern'. The bottom of the page shows the full URL again: https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns/.

Discover - Elastic

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_pattern?_g=(filt... ☆ 🔑 시크릿 모드(2개) :

Stack Management / Index patterns / Create index pattern admin

Kibana

[Index Patterns](#)

Saved Objects
Advanced Settings

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

Step 1 of 2: Define index pattern

Index pattern

classes*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >,].

✓ Success! Your index pattern matches 1 index.

classes

Rows per page: 10 ▾

> Next step

Discover - Elastic

search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_pattern?_g=(filt... ☆ 시크릿 모드(2개) :

Stack Management / Index patterns / Create index pattern admin

Kibana

[Index Patterns](#)

Saved Objects
Advanced Settings

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

[Include system indices](#)

Step 2 of 2: Configure settings

You've defined **classes*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

submit_date

The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

[Show advanced options](#)

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

잘 들어갔는지 확인!

classes* - Elastic

Stack Management / Index patterns / classes*

Kibana

Index Patterns

Saved Objects

Advanced Settings

Time Filter field name: 'submit_date'

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

Fields (16) Scripted fields (0) Source filters (0)

Search All field types

Name	Type	Format	Searchable	Aggregatable	Excluded
Professor	string		●		✎
Professor.keyword	string		●	●	✎
_id	string		●	●	✎
_index	string		●	●	✎
_score	number				✎
_source	_source				✎
_type	string		●	●	✎
major	string		●		✎
professor	string		●		✎
rating	number		●	●	✎

시각화 선택!

classes* - Elastic

search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/management/kibana/index_patterns/b242... ☆ 시크릿 모드(2개) :

Stack Management / Index patterns / classes*

Home

Recently viewed

- barchart

Kibana

- Anomaly Detection
- SQL Workbench
- Alerting
- Discover
- Dashboard
- Visualize

Management

- Index Management
- Dev Tools
- Stack Management

Security

Tenants

Account

Dock navigation

close

es*

Field name: 'submit_date'

This page lists every field in the classes* index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Search Mapping API.

(16) Scripted fields (0) Source filters (0)

All field types

	Type	Format	Searchable	Aggregatable	Excluded
submit_date	string		●		
category.keyword	string		●	●	
category	string		●	●	
score	string		●	●	
id	number				
text._source	_source				
text	string		●	●	
label	string		●		
value	string		●		
order	number		●	●	

[https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize/create?indexPattern=aae2c510-2021-11eb-80a3-41c3cf16869f&type=pie&_g=\(filters:\(\),refreshInterval:\(paus...](https://search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize/create?indexPattern=aae2c510-2021-11eb-80a3-41c3cf16869f&type=pie&_g=(filters:(),refreshInterval:(paus...)

새 시각화 생성!

classes* - Elastic

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pa... ☆ 🔑 시크릿 모드(2개) ⋮

☰ |  Visualize | admin

Visualizations

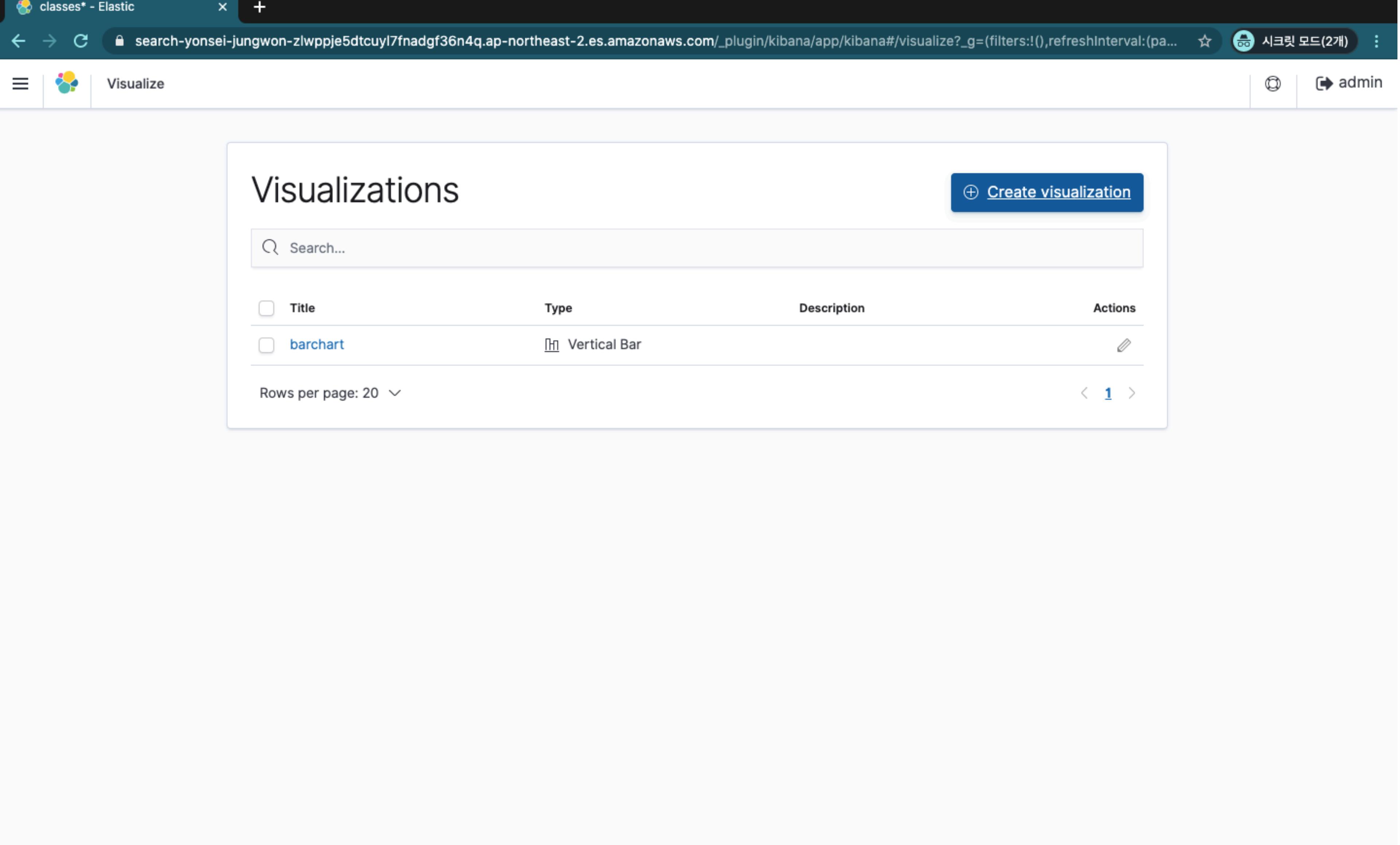
+ Create visualization

Search...

<input type="checkbox"/>	Title	Type	Description	Actions
<input type="checkbox"/>	barchart	Vertical Bar		

Rows per page: 20 ▾

< 1 >



Coordinate Map 선택

classes* - Elastic

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pa... ☆ 🔑 시크릿 모드(2개) :

Visualize admin

New Visualization

Filter

Area Controls Coordinate Map Data Table

Gauge Goal Heat Map Horizontal Bar

Line Markdown Metric Pie

Region Map TSVB Tag Cloud Timelion

Vega Vertical Bar

Coordinate Map

Plot latitude and longitude coordinates on a map

Actions

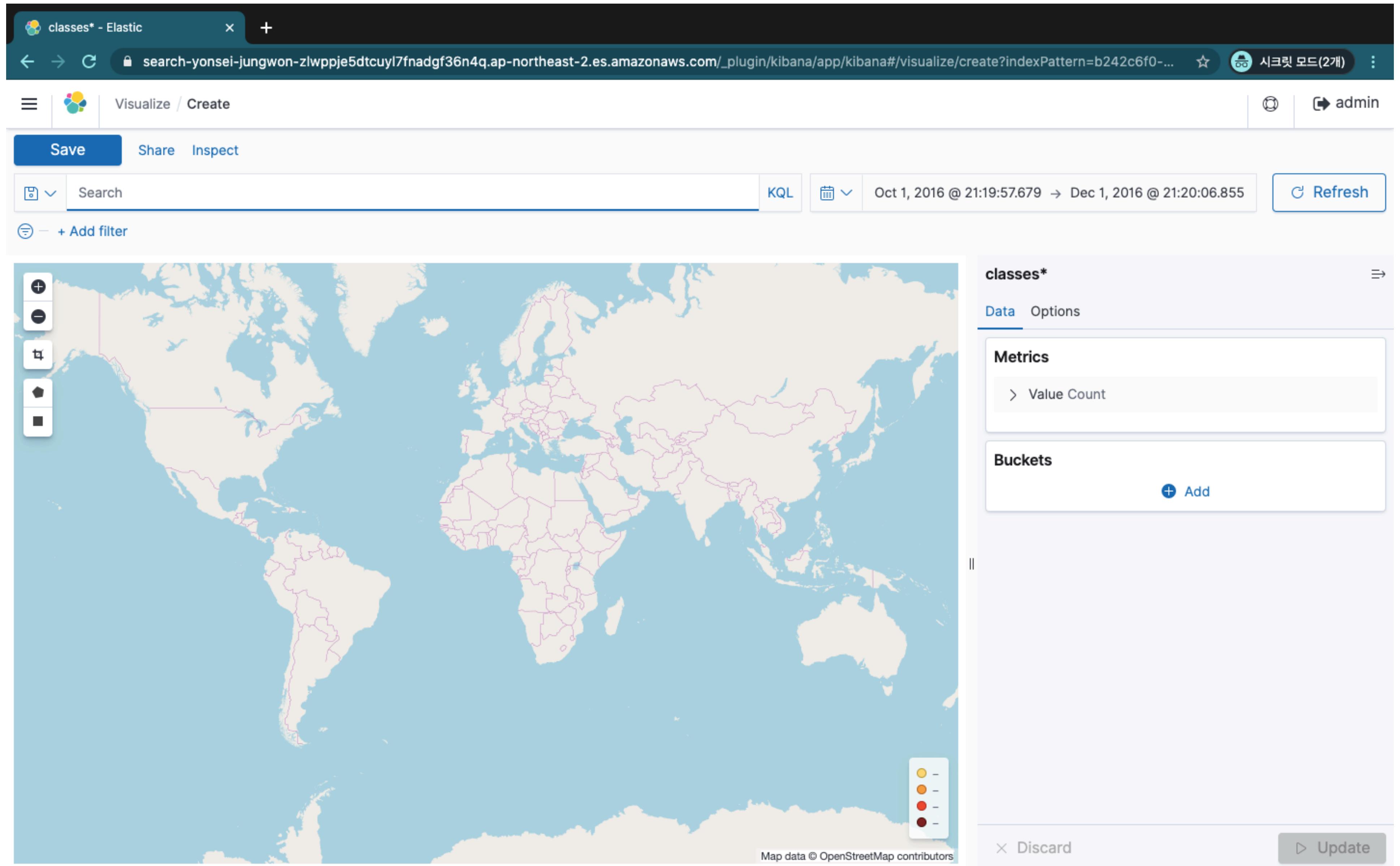
1 >

The screenshot shows the Kibana interface for creating a new visualization. A modal window titled 'New Visualization' is open, displaying a grid of visualization types. The 'Coordinate Map' option, which plots latitude and longitude coordinates on a map, is highlighted with a light blue border. To the right of the grid, there is a detailed description of the 'Coordinate Map' visualization and an 'Actions' sidebar containing a single item labeled '1 >'. The background shows the main Kibana dashboard with various search and visualization filters.

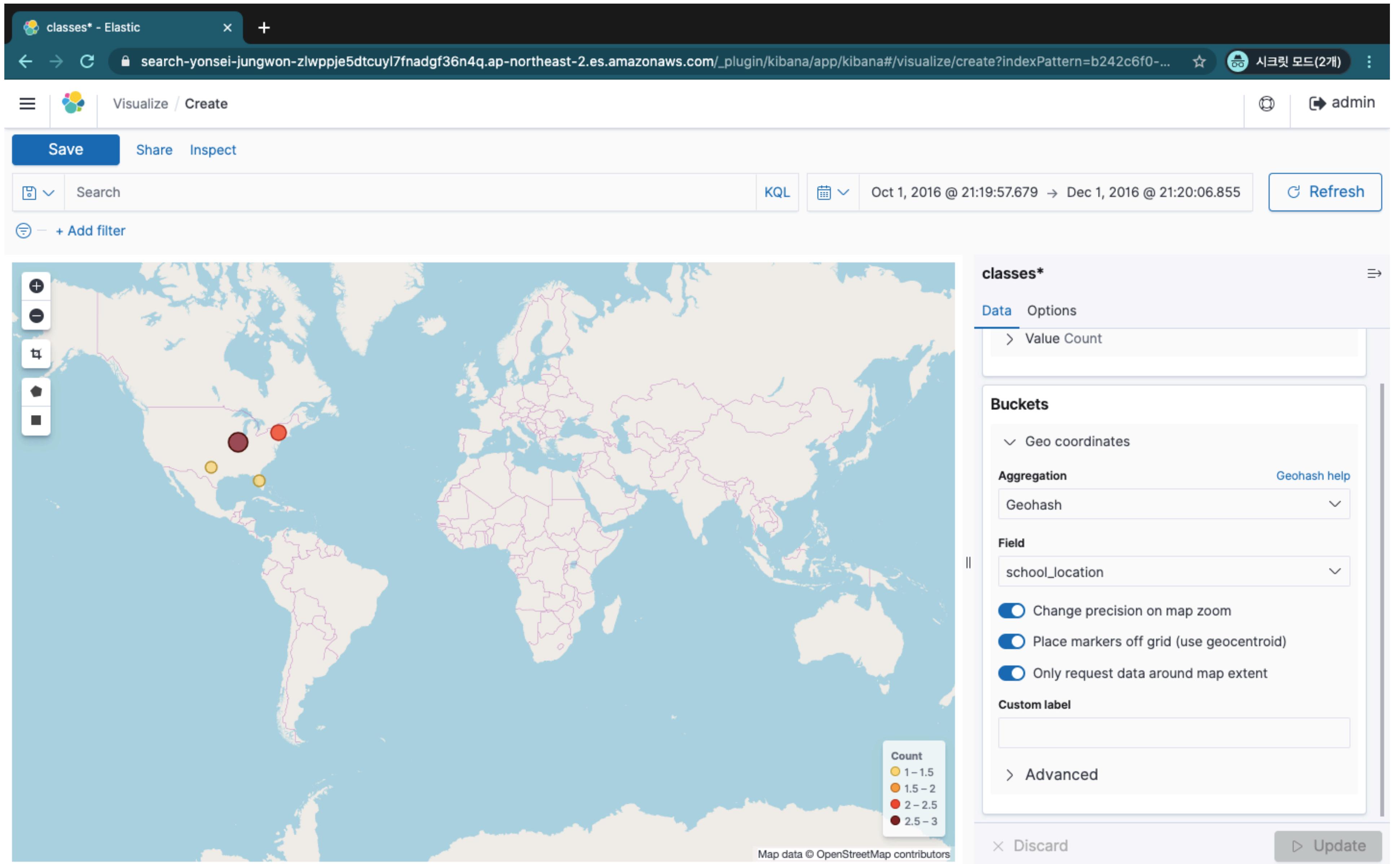
Classes 선택

The screenshot shows the Kibana interface with a search bar at the top containing the URL: `search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize?_g=(filters:!(),refreshInterval:(pa...)`. Below the search bar, there are navigation icons and a user profile for 'admin'. A modal window titled 'New Coordinate Map / Choose a source' is open in the center. The modal contains a search bar with placeholder 'Search...', a 'Sort' dropdown, and a 'Types' dropdown set to '2'. Two items are listed in the results: 'basketball*' and 'classes*'. To the right of the results, there is a 'Actions' section with a pencil icon and a page number indicator '1'. On the left side of the main Kibana interface, there is a sidebar with sections like 'Visualize', 'Search...', 'Title', 'barchart', and 'Rows per page'.

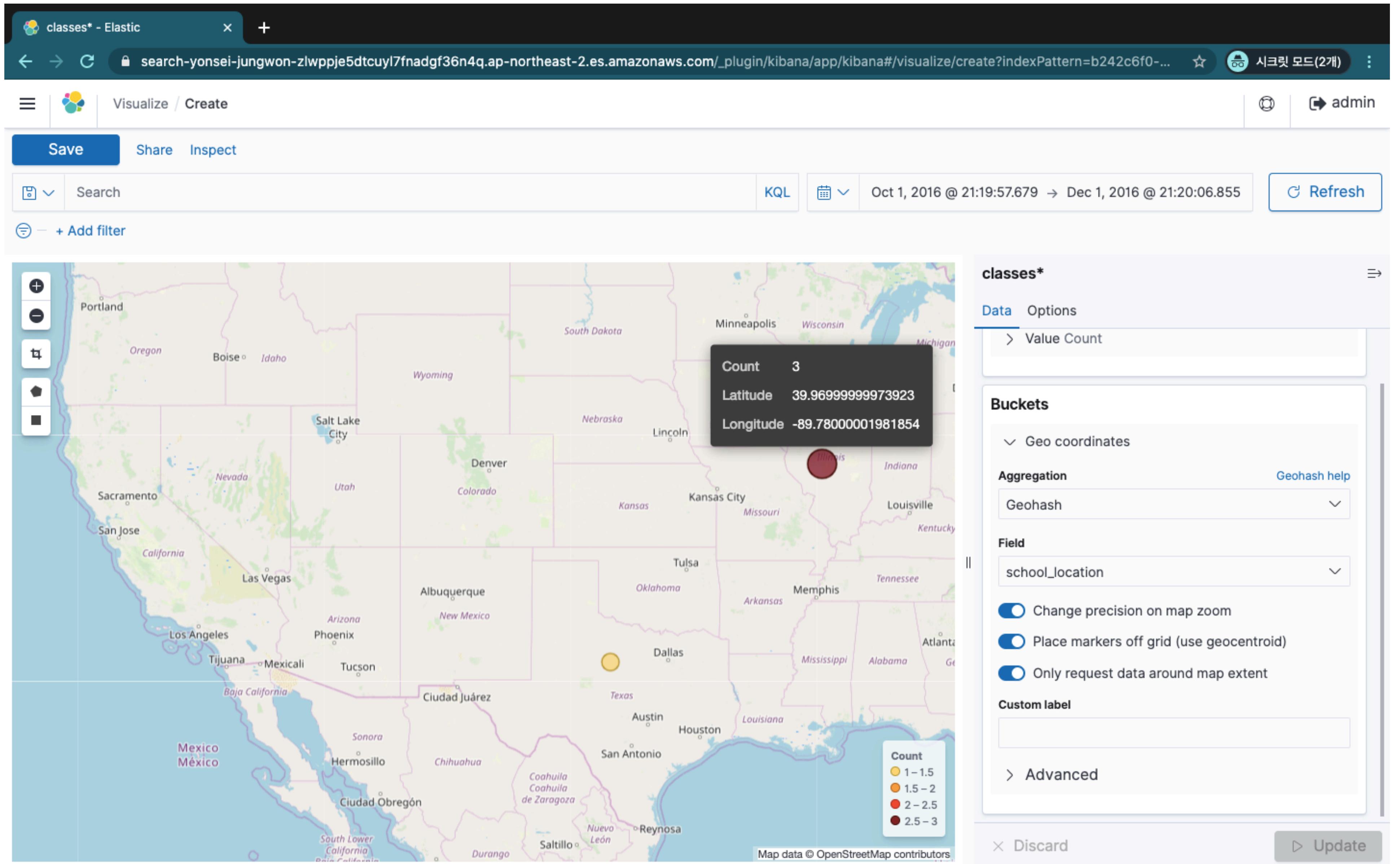
Metric 설정



Buckets 설정

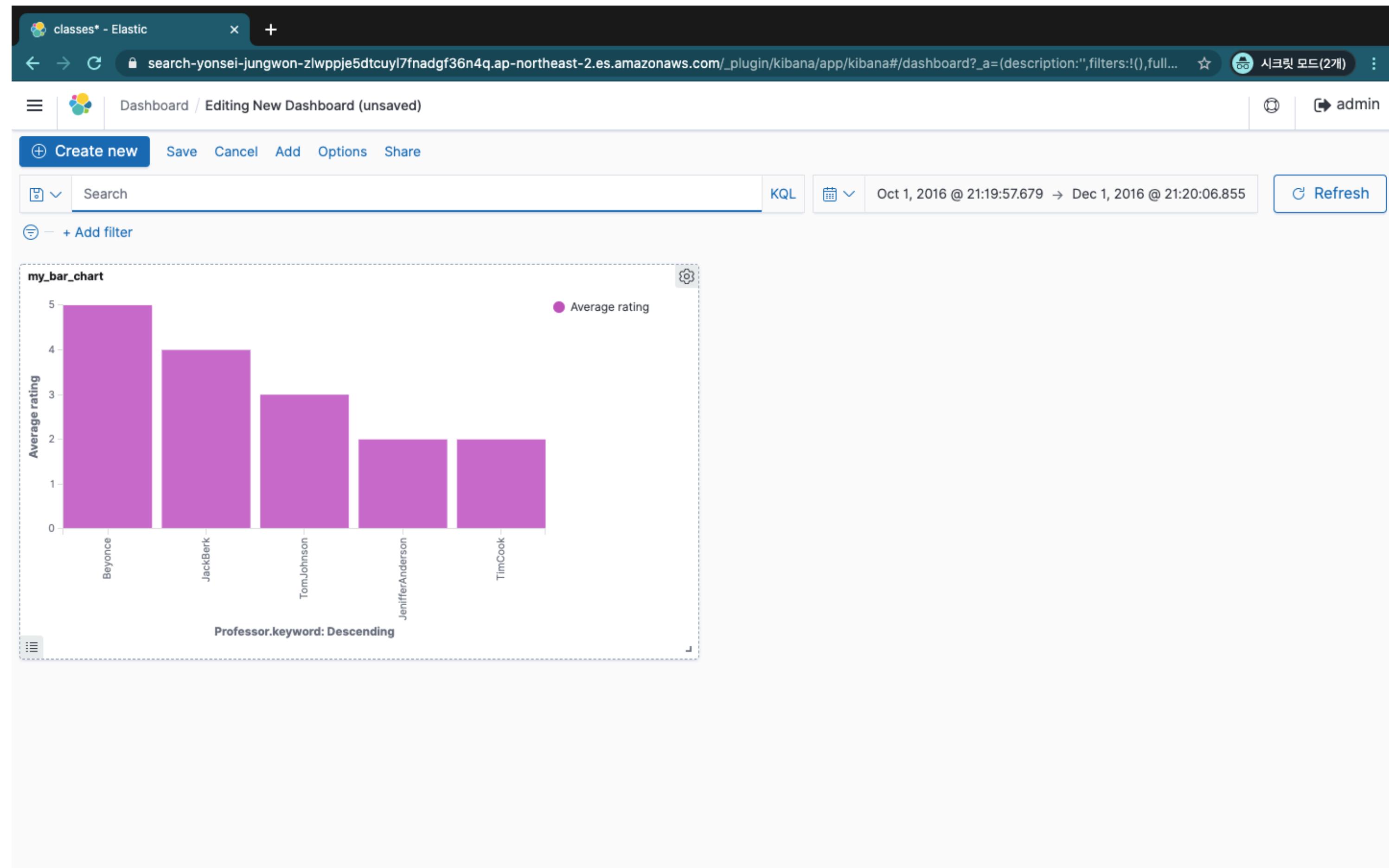


짜잔!

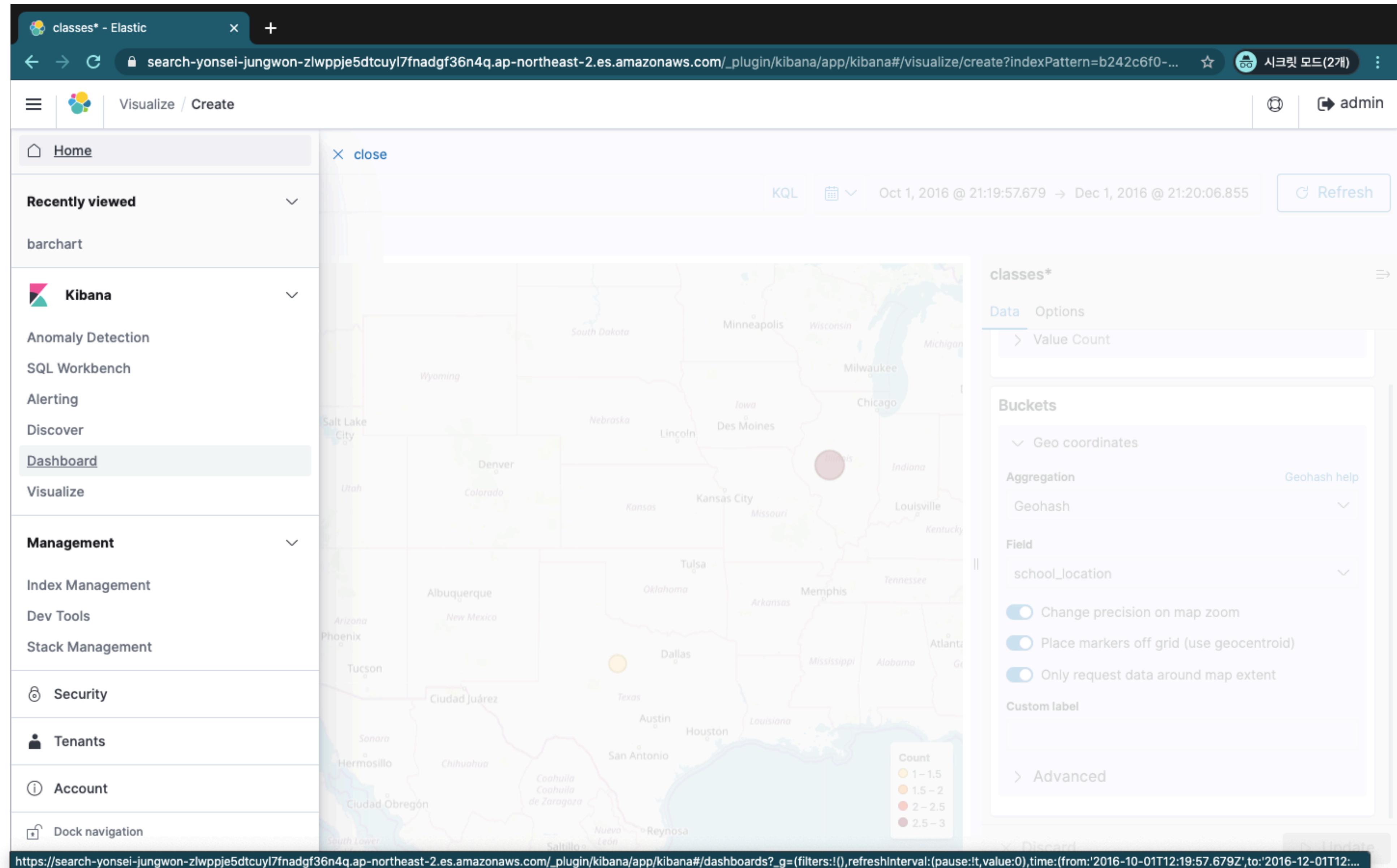


Kibana Dashboard

생성한 시각화나 각종 수치들을 한눈에!



Dashboard 클릭!



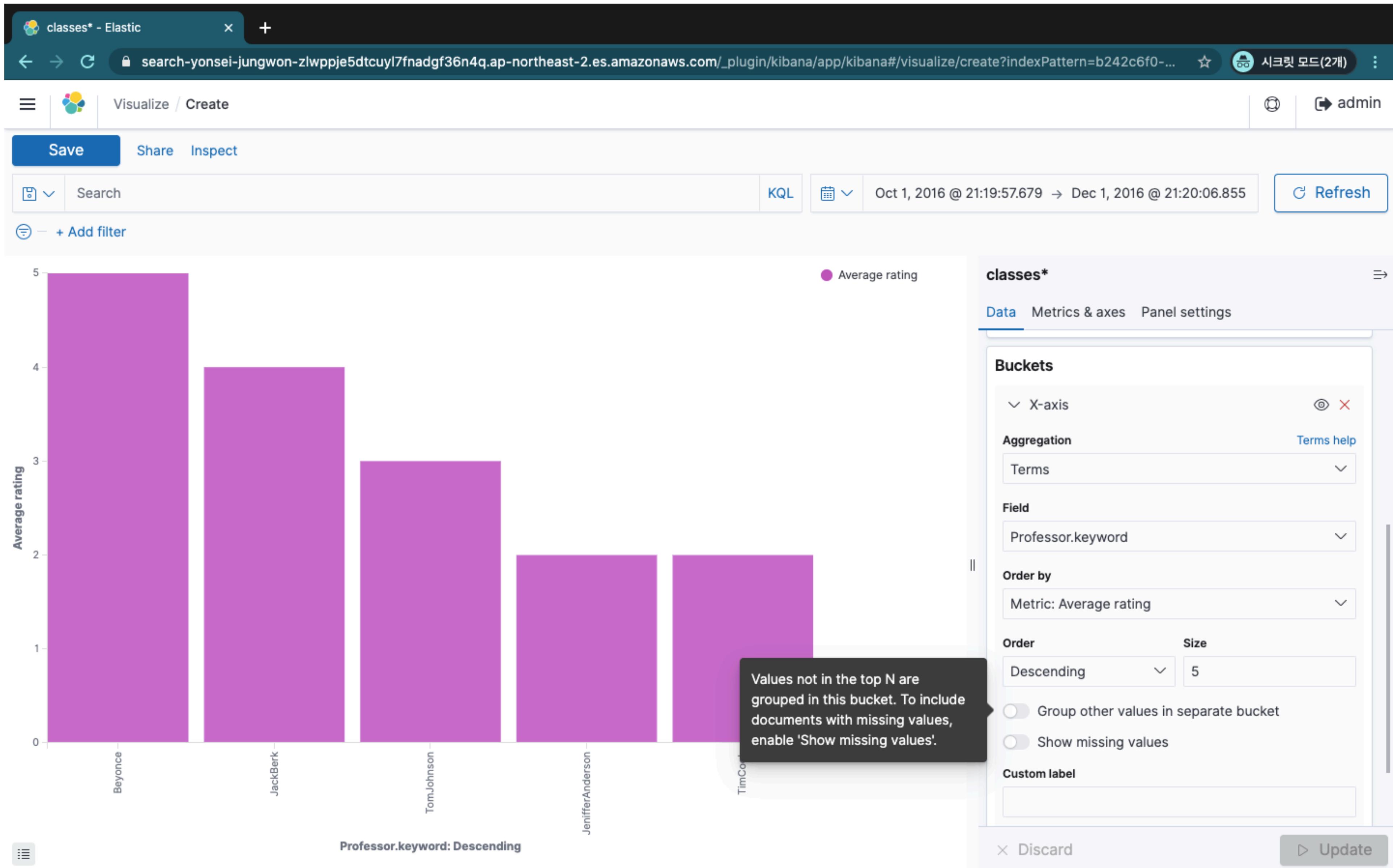
Create New 또는 Add an existing 클릭 (여기선 Create New)

The screenshot shows the Kibana interface for editing a new dashboard. At the top, there's a header bar with the title 'classes* - Elastic' and a search bar containing the URL 'search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/dashboard?_g=(filters:!(),refreshInterval:(p...'. Below the header, the main area is titled 'Dashboard / Editing New Dashboard'. A prominent blue button labeled '+ Create new' is visible. To its right are 'Save', 'Cancel', 'Add', 'Options', and 'Share' buttons. Below these buttons are search and KQL filters, with the date range set from 'Oct 1, 2016 @ 21:19:57.679' to 'Dec 1, 2016 @ 21:20:06.855'. A 'Refresh' button is also present. In the center of the dashboard area, there's a dashed box containing the text 'Add an existing or new object to this dashboard' and another '+ Create new' button. The overall interface is clean and modern, typical of a web-based analytics tool.

Classes 선택

The screenshot shows a Kibana dashboard editing interface. A modal window titled "New Vertical Bar / Choose a source" is open in the center. The modal contains a search bar with placeholder "Search...", a "Sort" dropdown, and a "Types" dropdown set to "2". Below the search bar, there are two items listed: "basketball*" and "classes*". At the bottom left of the modal is a "Create new" button. In the background, the main dashboard interface is visible, showing a sidebar with "Create new", "Save", "Cancel", "Add", and "Options" buttons, and sections for "Search" and "+ Add filter". A message at the bottom of the sidebar says "Add an existing or new object to this dashboard". The top of the screen shows the browser title "classes* - Elastic" and the URL "search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/dashboard?_g=(filters:!(),refreshInterval:(p...". On the right side of the dashboard, there are user profile icons for "admin" and "시크릿 모드(2개)".

적당히 Metric과 Bucket 설정으로 왼쪽과 같은 Vertical Chart 만들기!



저장!

classes* - Elastic

← → C 🔒 search-yonsei-jungwon-zlwppje5dtcuyl7fnadgf36n4q.ap-northeast-2.es.amazonaws.com/_plugin/kibana/app/kibana#/visualize/create?indexPattern=b242c6f0-...

Visualize / Create

Save Share Inspect

KQL Oct 1, 2016 @ 21:19:57.679 → Dec 1, 2016 @ 21:20:06.855 Refresh

+ Add filter

Average rating

Beyonce

JackBerk

TomJohnson

JenifferAnderson

TimCook

Professor.keyword: Descending

Save visualization

Title: my_bar_chart

Description:

Add to dashboard after saving

Cancel Save and return

classes*

Data Metrics & axes Panel settings

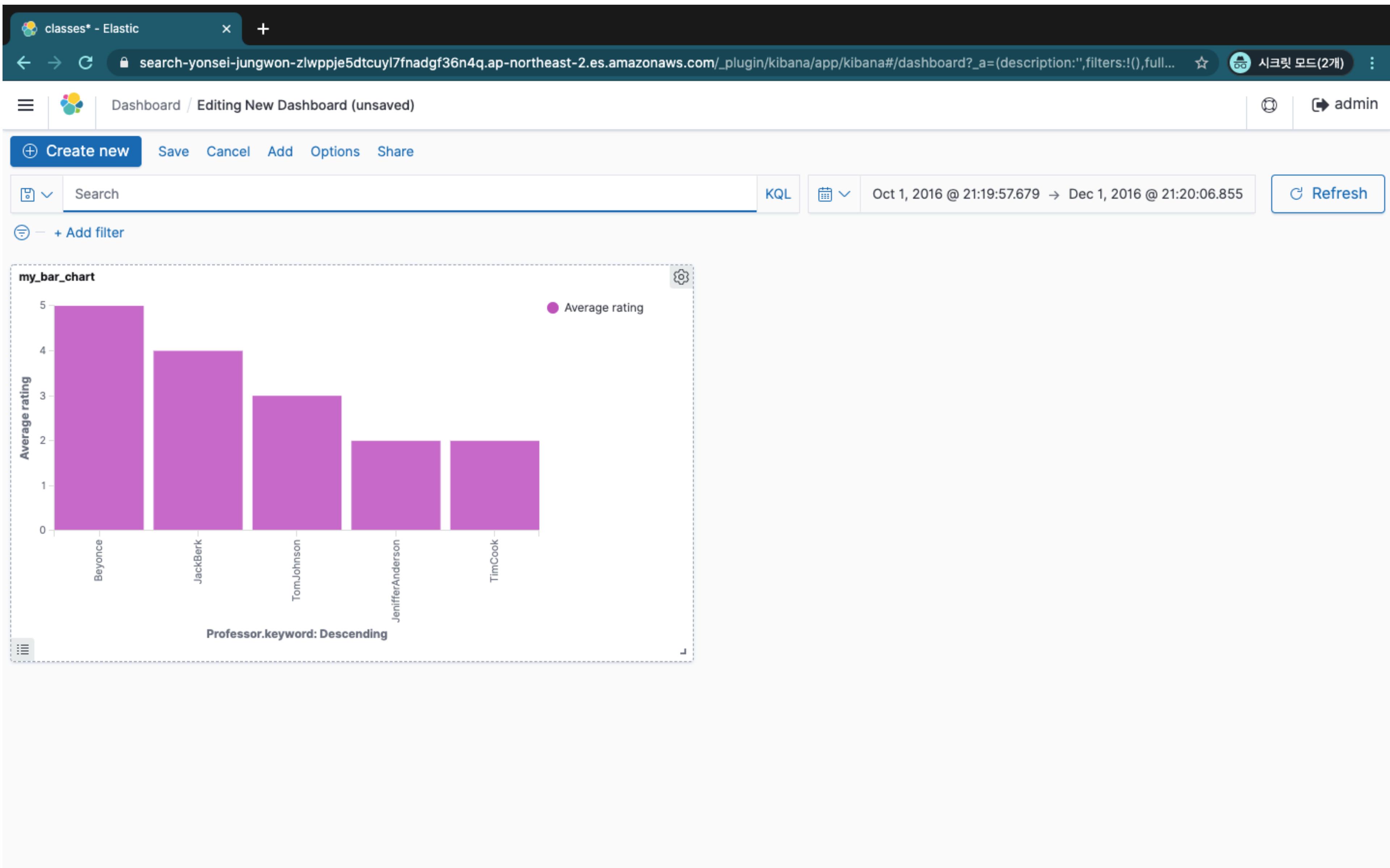
Buckets

- X-axis
- Aggregation
- Terms
- Field Professor.keyword
- Order by Metric: Average rating
- Order Size
- Descending
- Group other values in separate bucket
- Show missing values
- Custom label

Discard Update

The screenshot shows the Kibana visualization creation interface. A modal window titled "Save visualization" is open, prompting the user to enter a title ("my_bar_chart") and description. There is a checked checkbox for "Add to dashboard after saving". At the bottom of the modal are "Cancel" and "Save and return" buttons. In the background, a bar chart is displayed with five bars representing different professor keywords. The Y-axis is labeled "Average rating" and ranges from 0 to 5. The X-axis is labeled "Professor.keyword: Descending" and lists the professors: Beyonce, JackBerk, TomJohnson, JenifferAnderson, and TimCook. The bars are colored pink. On the right side of the screen, the visualization configuration panel is visible, showing settings for buckets, aggregation, terms, field selection (Professor.keyword), order by (Metric: Average rating, Size, Descending), and various grouping and missing value options. The overall interface is dark-themed.

짜잔! 같은 방식으로 다양한 차트들을 한눈에 볼 수 있습니다!

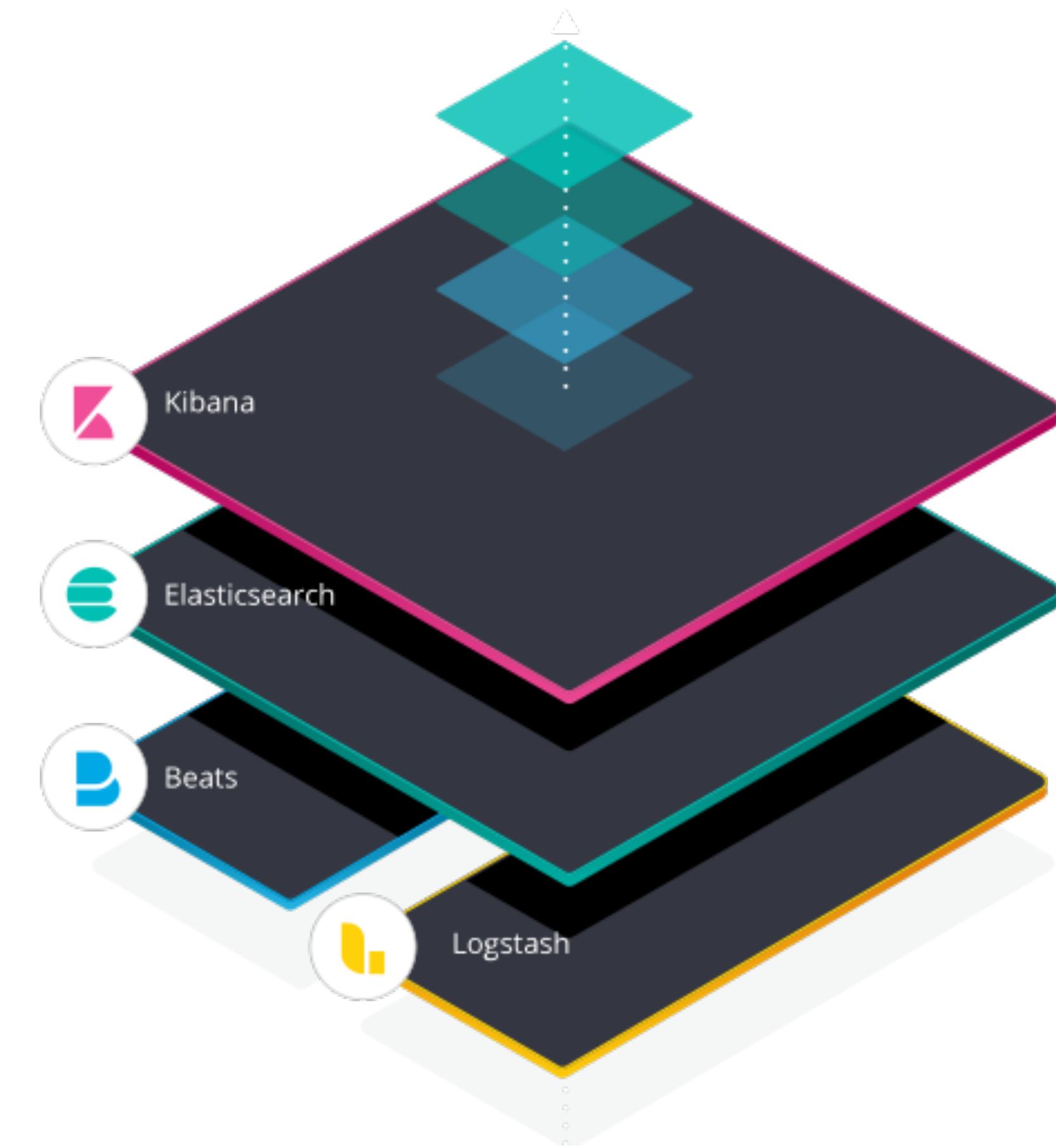


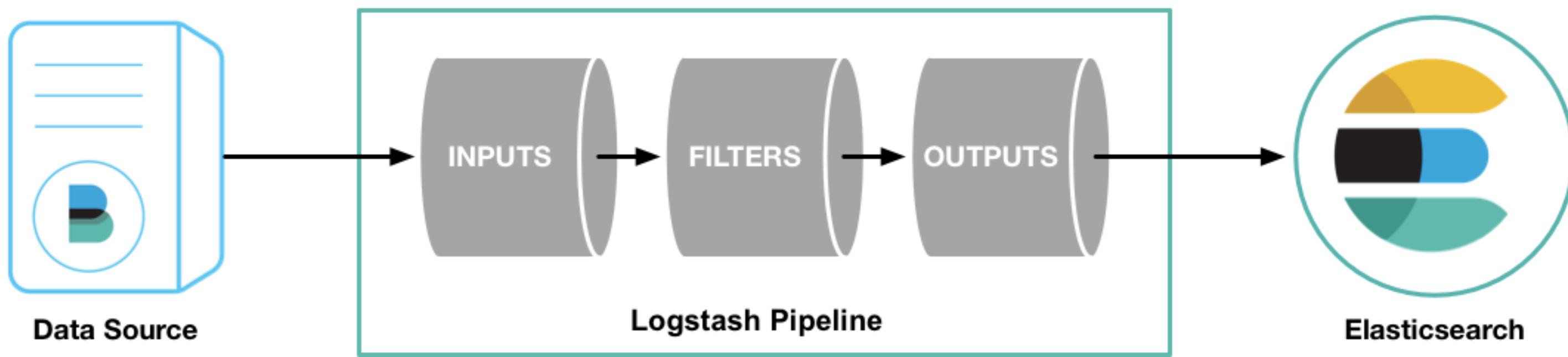
LOGSTASH

ELK Stack

Elasticsearch, Logstash, Kibana

- Elasticsearch
 - 검색 및 분석 엔진
- Logstash
 - 데이터 처리 파이프라인
 - 여러 소스에서 동시에 데이터를 수집 및 변환
- Kibana
 - 차트와 그래프를 이용해 데이터 시각화
- Beat
 - 파일 추적
 - Beat가 추가됨으로써 ELK Stack에서 Elastic Stack으로!





Logstash

Things to do

- Educate 계정을 이용해서 EC2 t2.medium으로 인스턴스 하나 생성
- Security Group에 8080 포트 열어두기
- 강의자료에서 제공된 명령어 입력
- stdinput and stdoutput test
- http input test
- 강의자료에서 제공된 logstash.conf파일을 이용하여, ELK 스택 완성!

E.O.D