AI기법과 활용

Week-10. Elastic Stack

2022-Summer 서중원

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 값들을 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

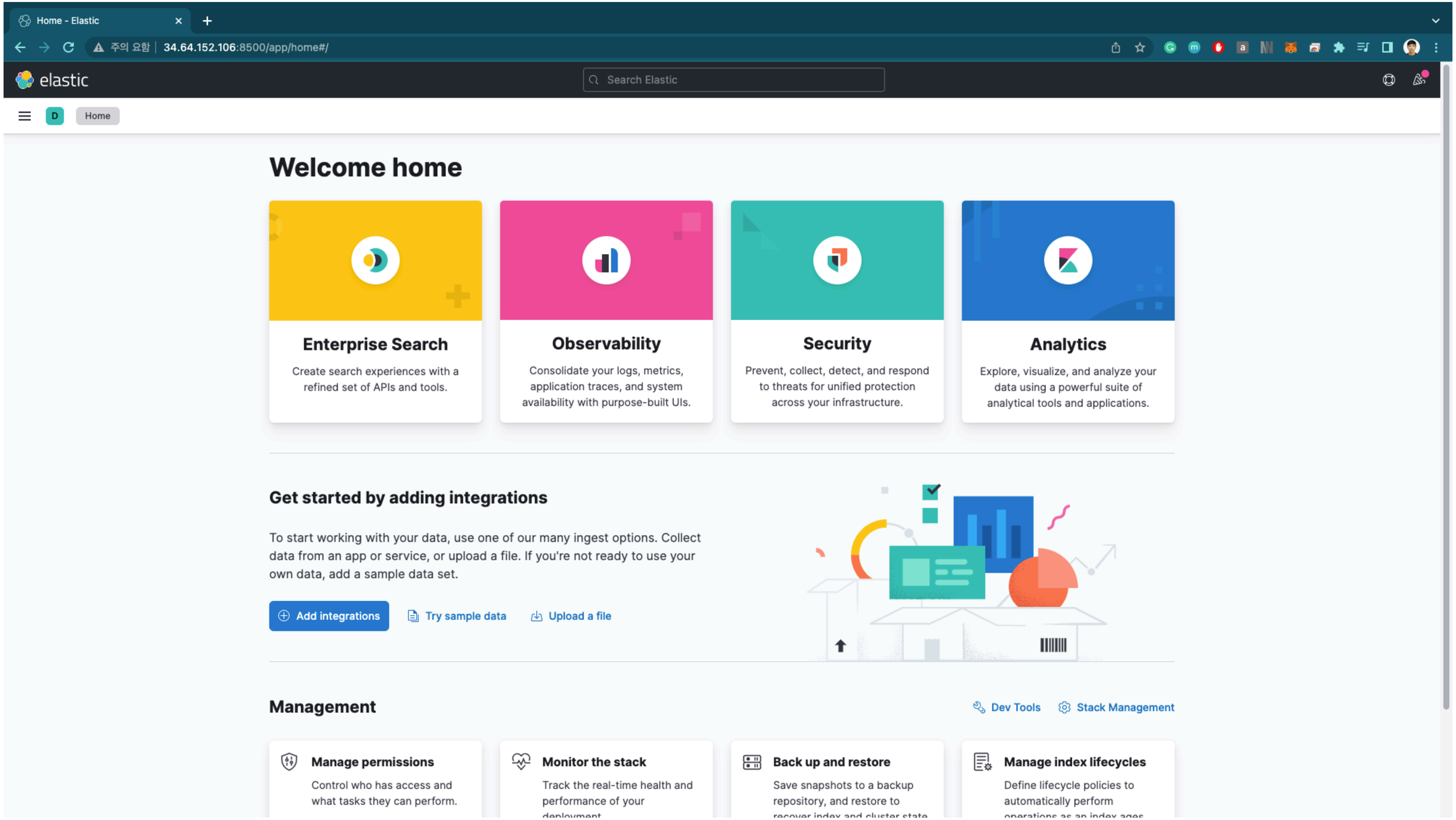
Bucket Aggregation 이란?

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

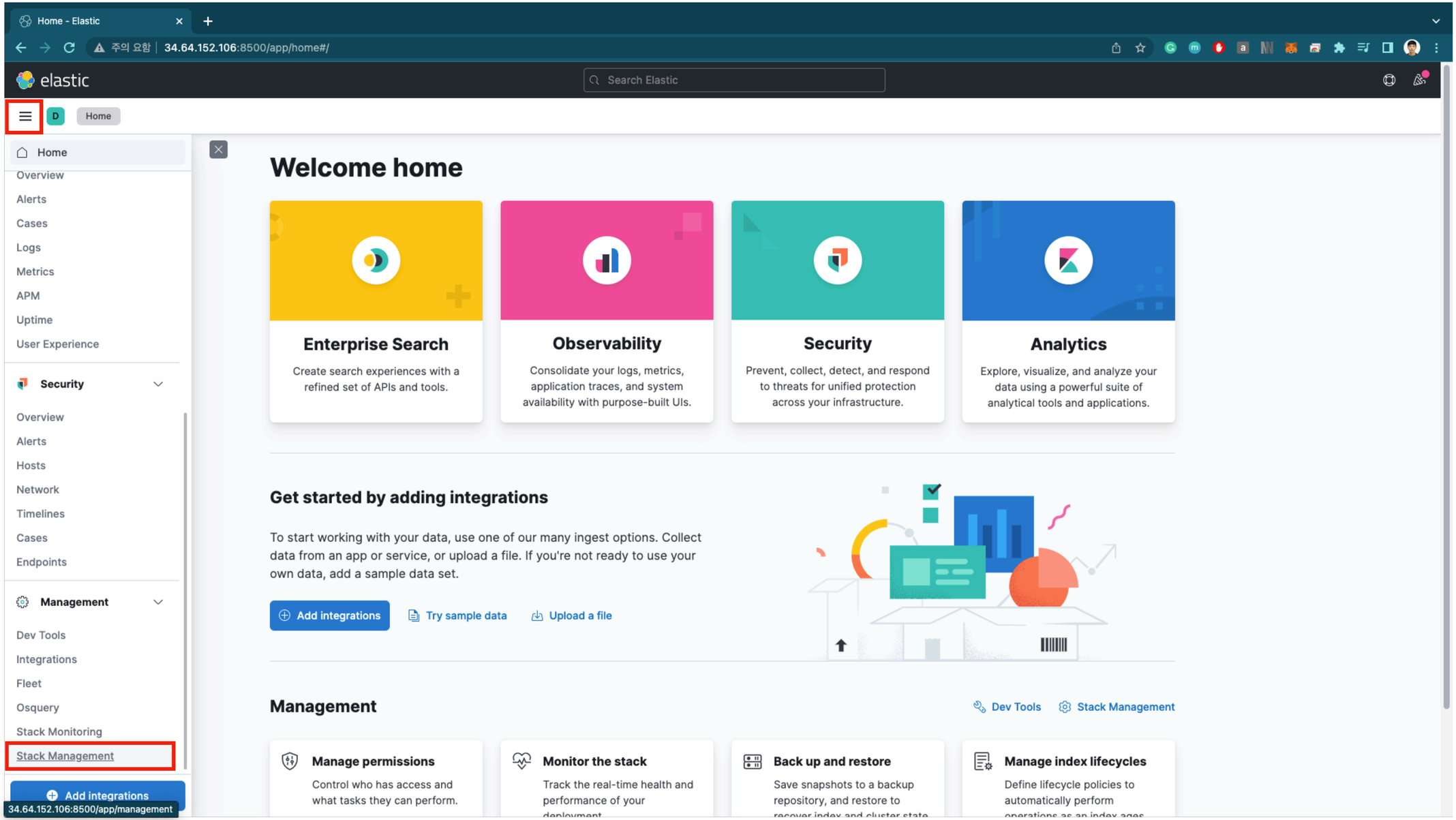
```
body = {
    "size" : 0,
    "aggs" : {
        "team_stats" : {
            "terms" : {
                "field" : "team"
            },
            "aggs" : {
                "stats_score" : {
                    "stats" : {
                        "field" : "points"
                    }
     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

Kibana

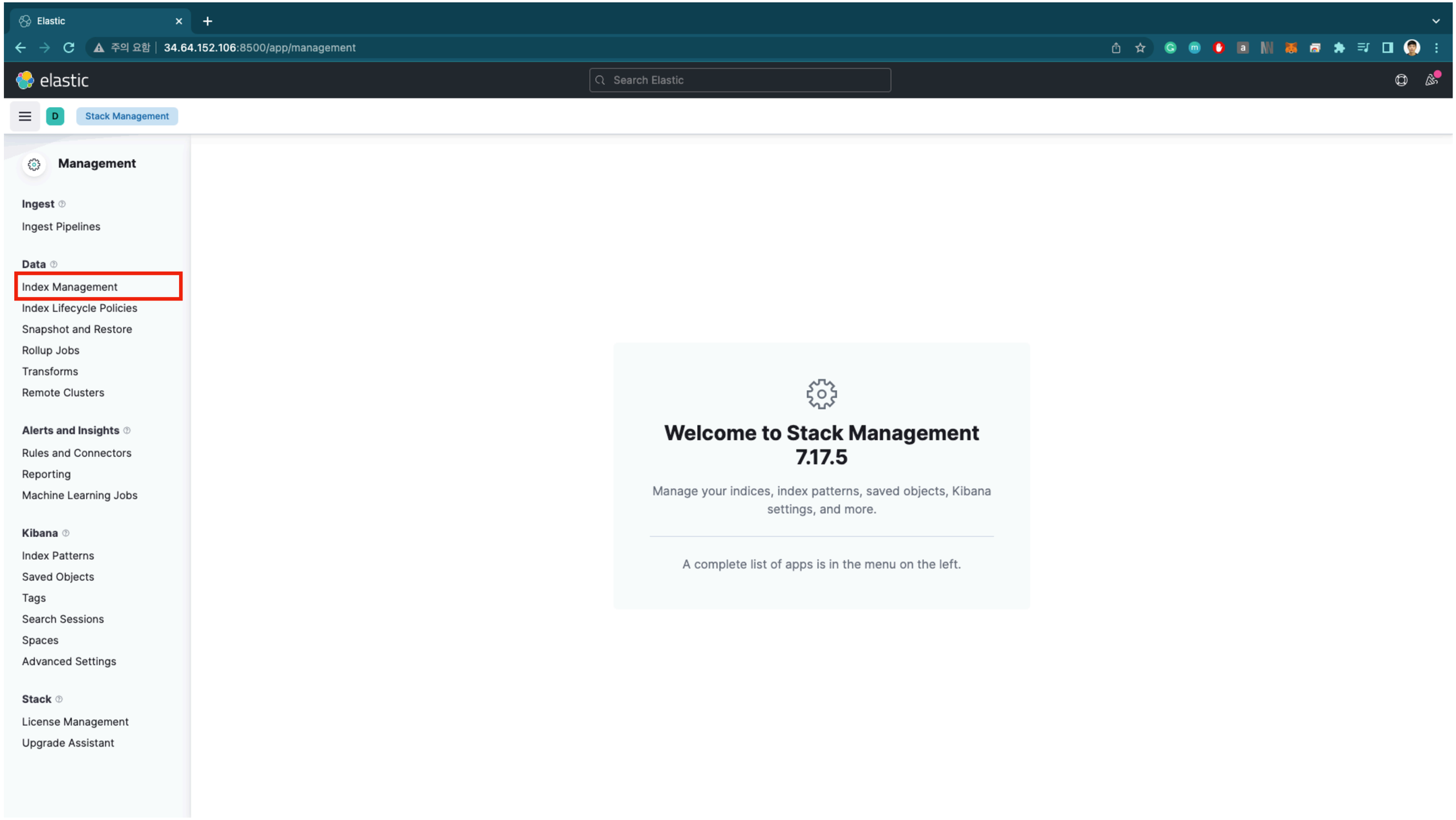
본인의 IP:8500으로 키바나로 이동



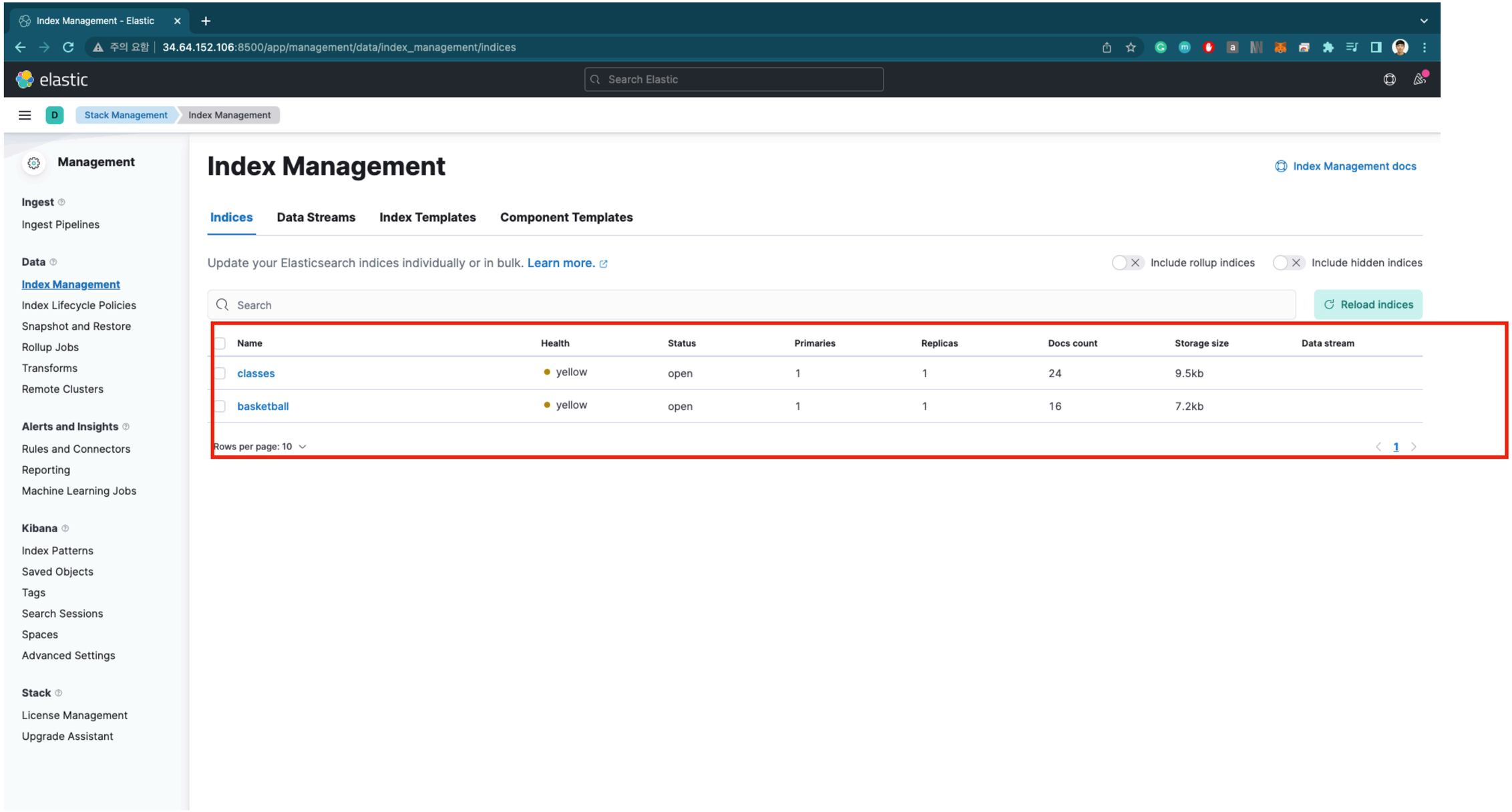
좌측의 메뉴화면에서 Stack Management 클릭후, 그동안 생성한 인덱스들이 잘 들어갔는지 확인



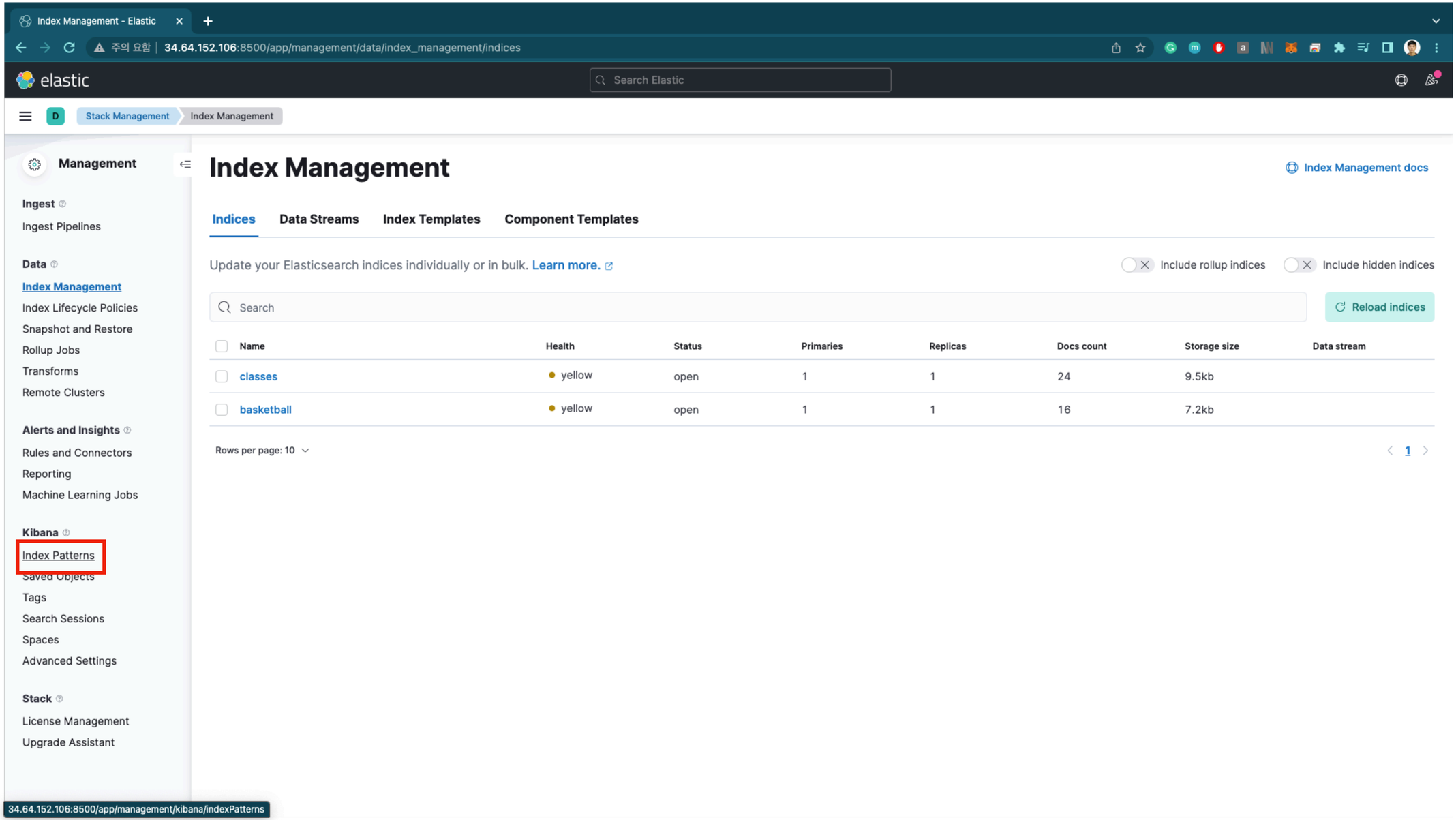
Index Management 클릭



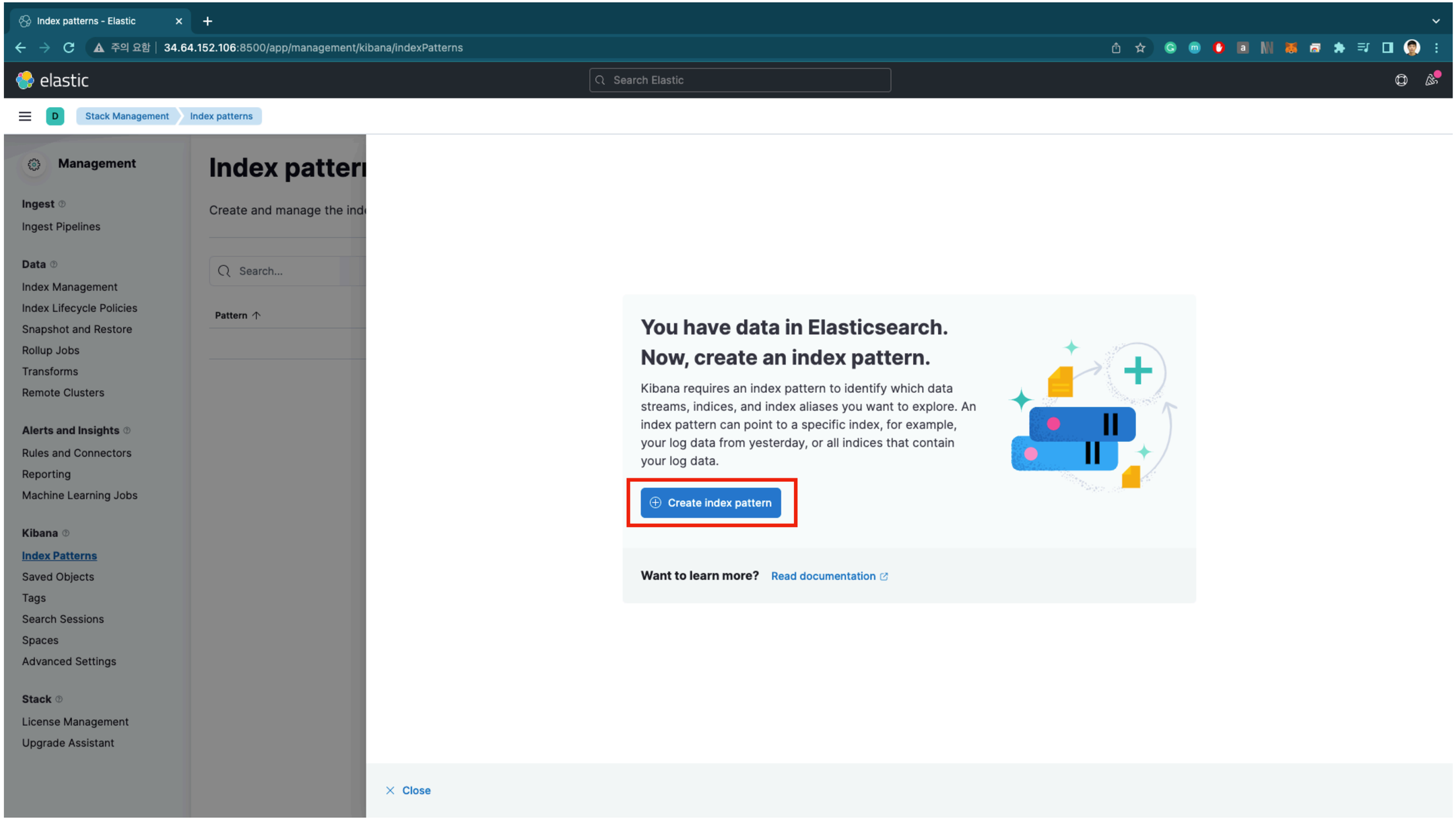
잘들어갔네요!


Index Management - Elastic
주의 요함 | 34.64.152.106:8500/app/management/data/index_management/indices
elastic
Search Elastic
D
Stack Management
Index Management
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
Index Management
Index Management docs
Indices
Data Streams
Index Templates
Component Templates
Update your Elasticsearch indices individually or in bulk. Learn more.
Include rollup indices
Include hidden indices
Search
Reload indices
Name
Health
Status
Primaries
Replicas
Docs count
Storage size
Data stream
classes
yellow
open
1
1
24
9.5kb
basketball
yellow
open
1
1
16
7.2kb
Rows per page: 10
1

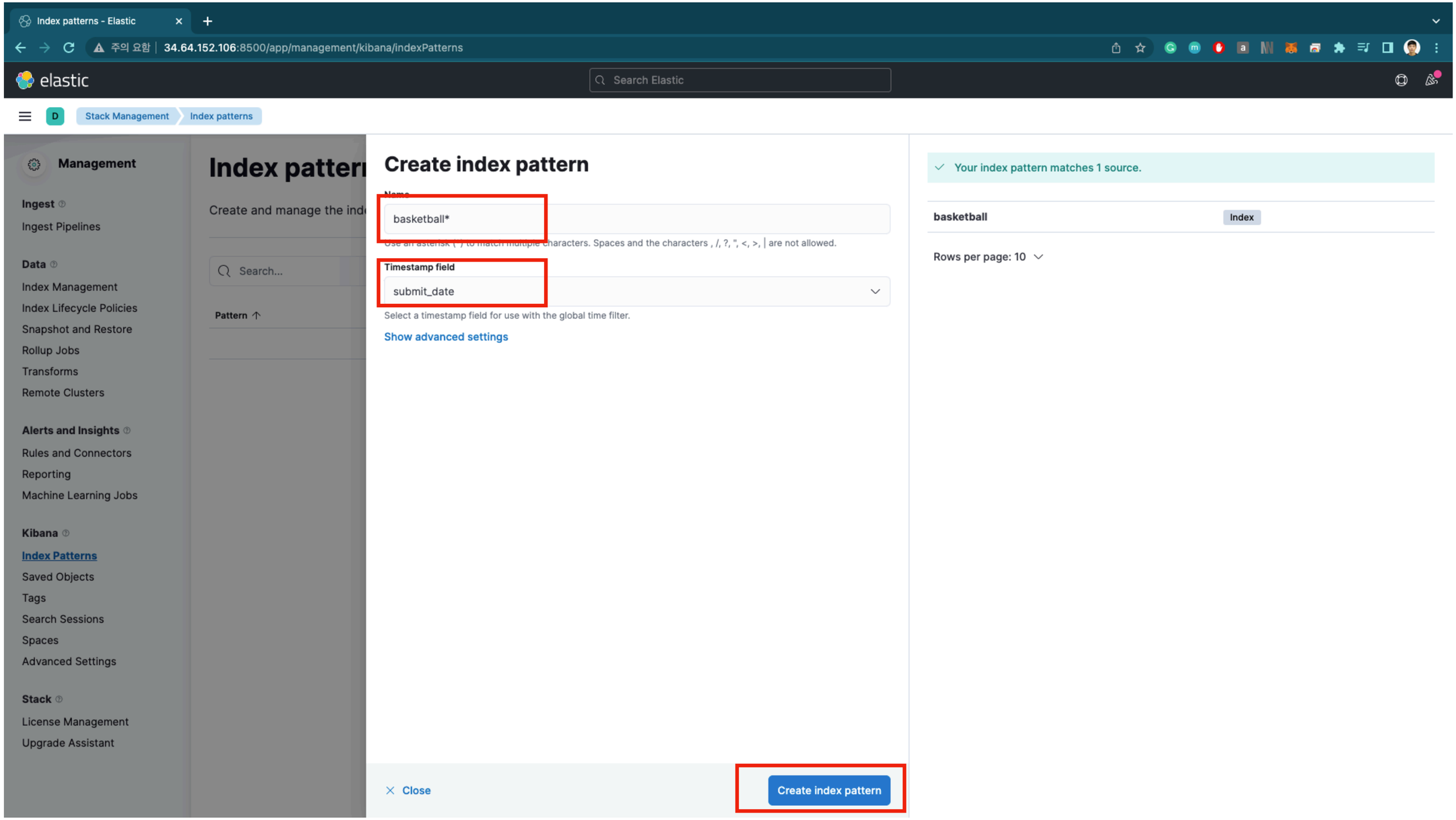
Index Patterns 클릭



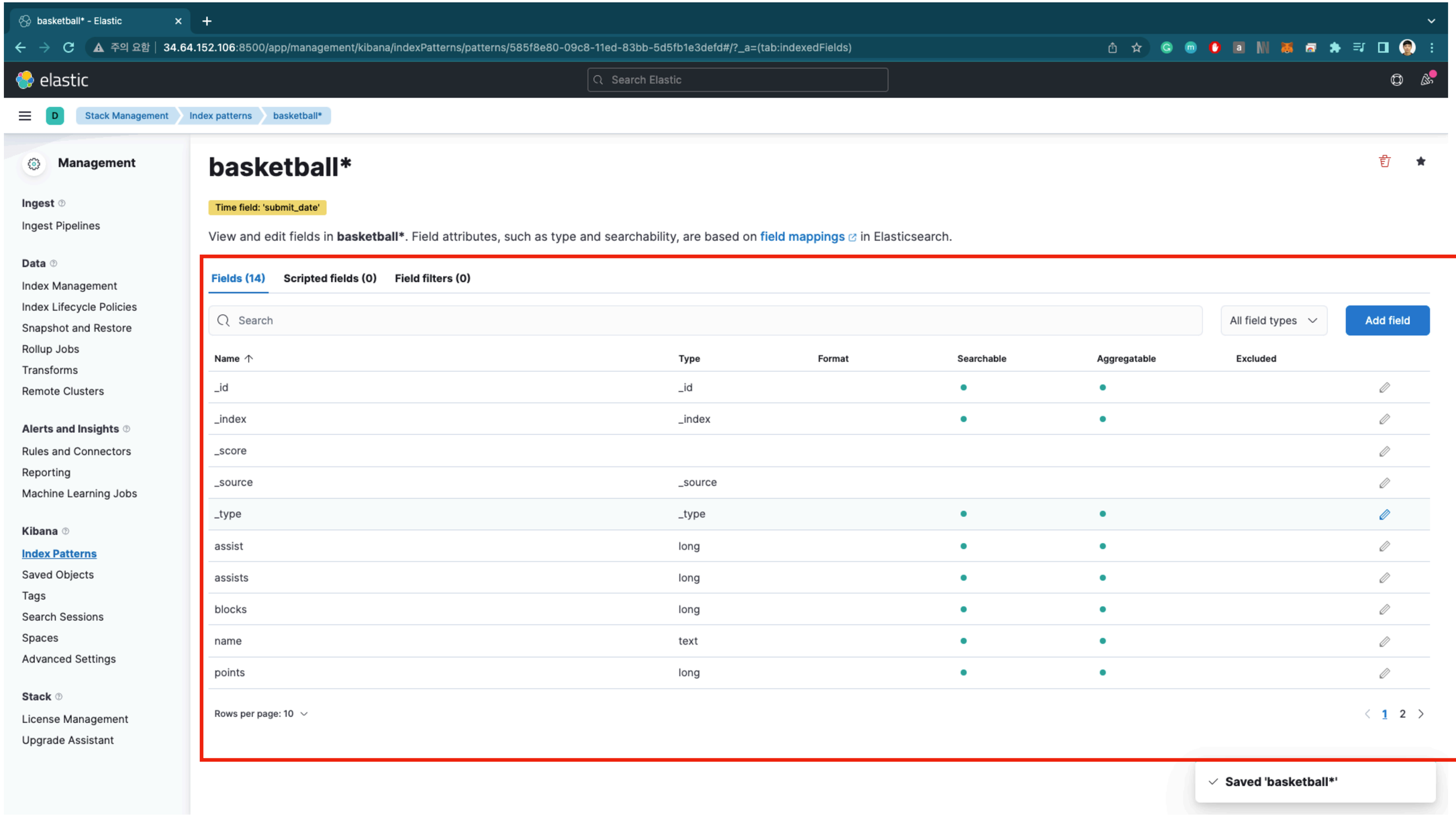
Index Pattern 생성



basketball 입력, submit_date 선택

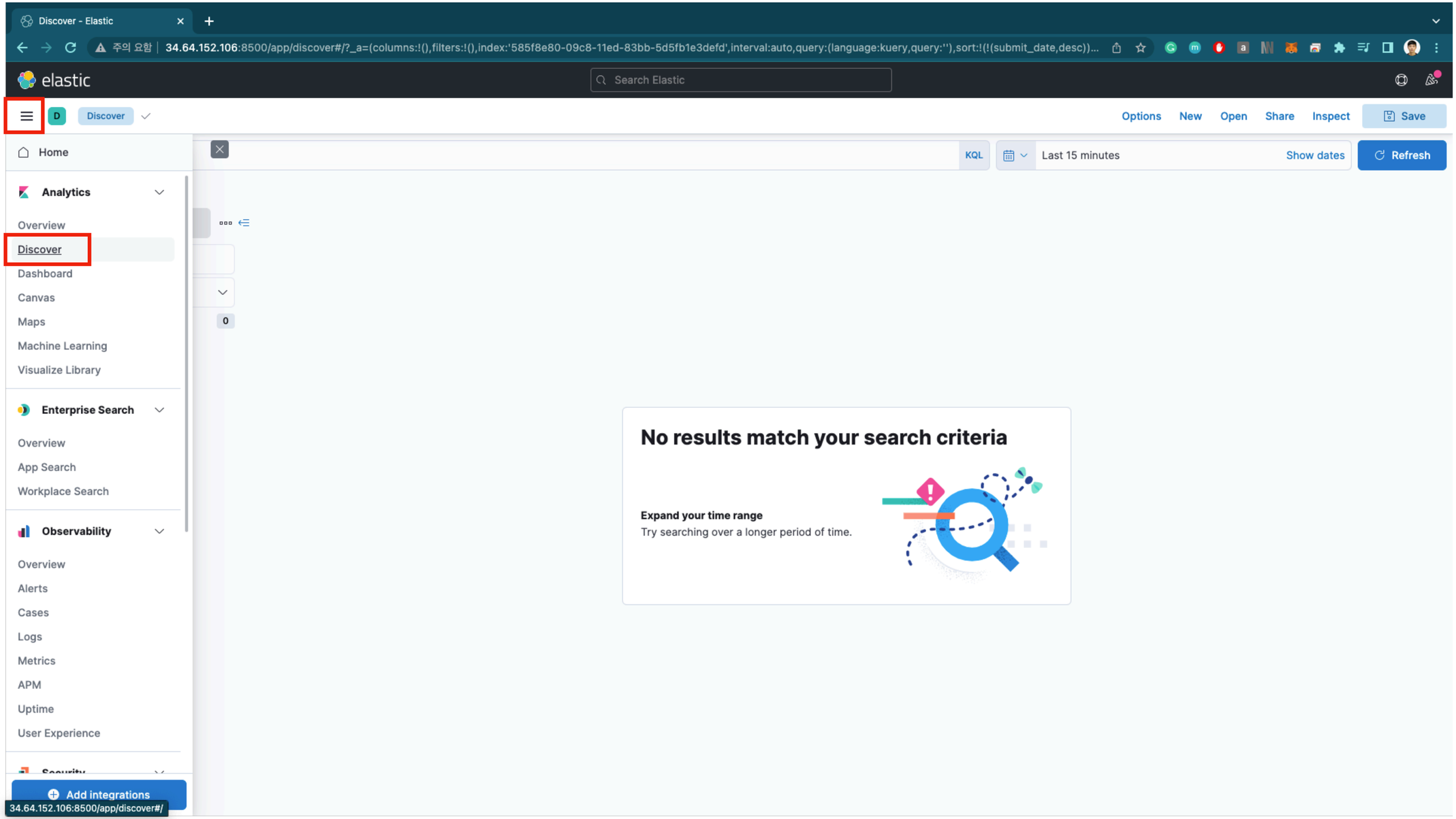


각각의 필드가 보입니다!

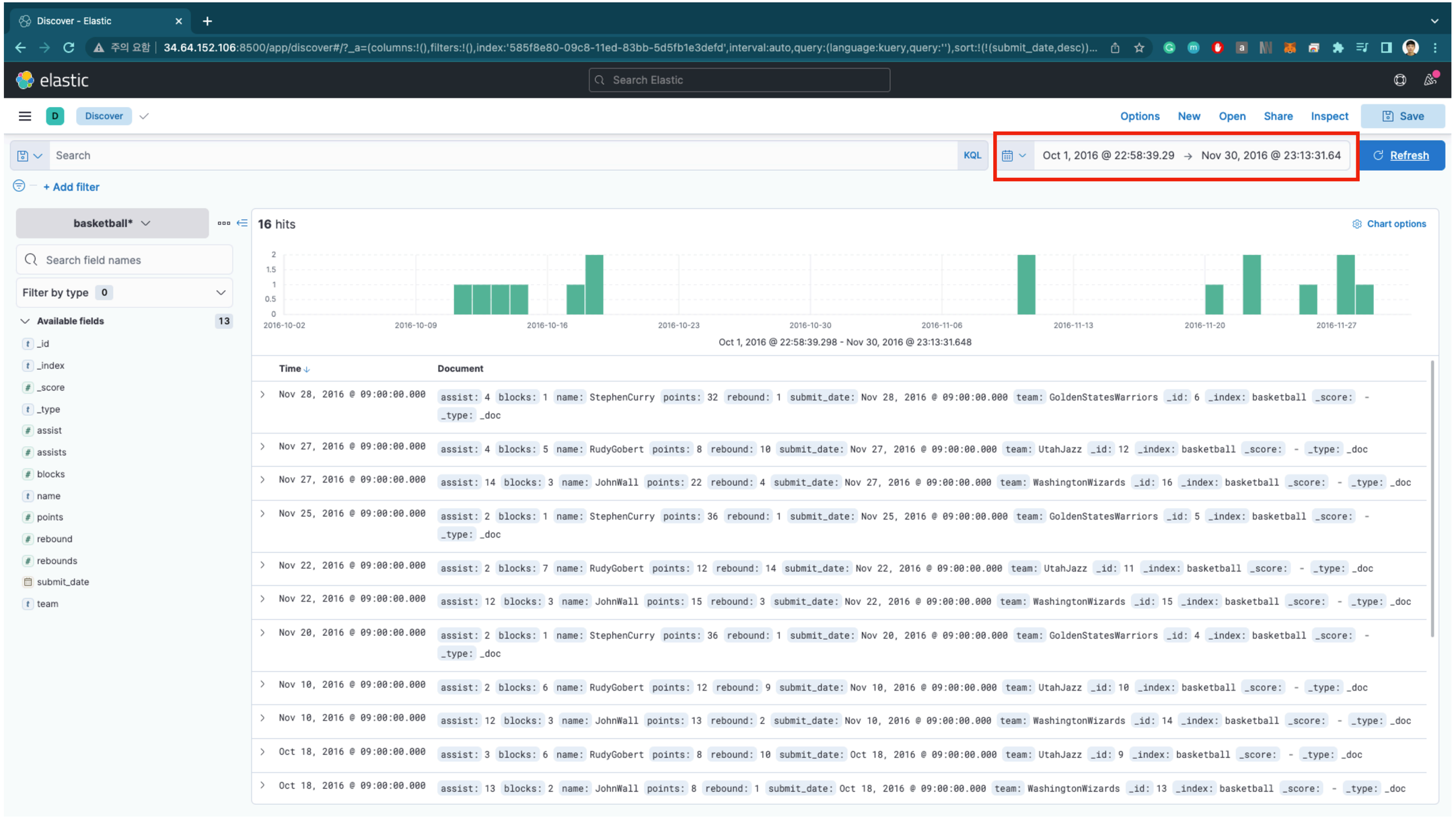

basketball* - Elastic
주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns/patterns/585f8e80-09c8-11ed-83bb-5d5fb1e3defd#/?_a=(tab:indexedFields)
elastic
Search Elastic
D
Stack Management
Index patterns
basketball*
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
basketball*
Time field: 'submit_date'
View and edit fields in basketball*. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (14)
Scripted fields (0)
Field filters (0)
Search
All field types
Add field
Name
Type
Format
Searchable
Aggregatable
Excluded
_id
_id
_index
_index
_score
_source
_source
_type
_type
assist
long
assists
long
blocks
long
name
text
points
long
Rows per page: 10
1
2
Saved 'basketball*'

Kibana Discover

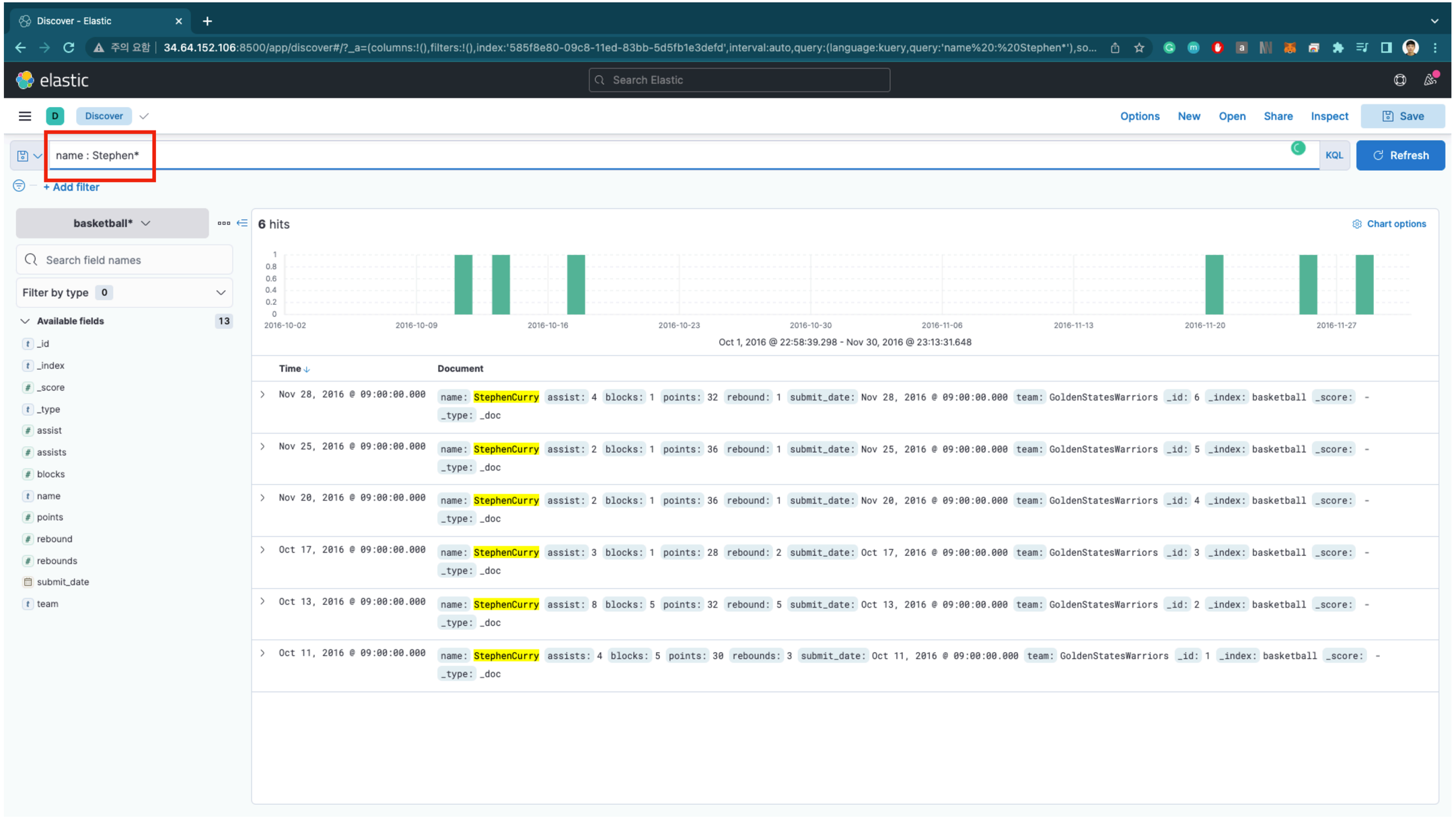
Discover로 이동



2016년 10월 1일 부터 11월 30일까지로 설정

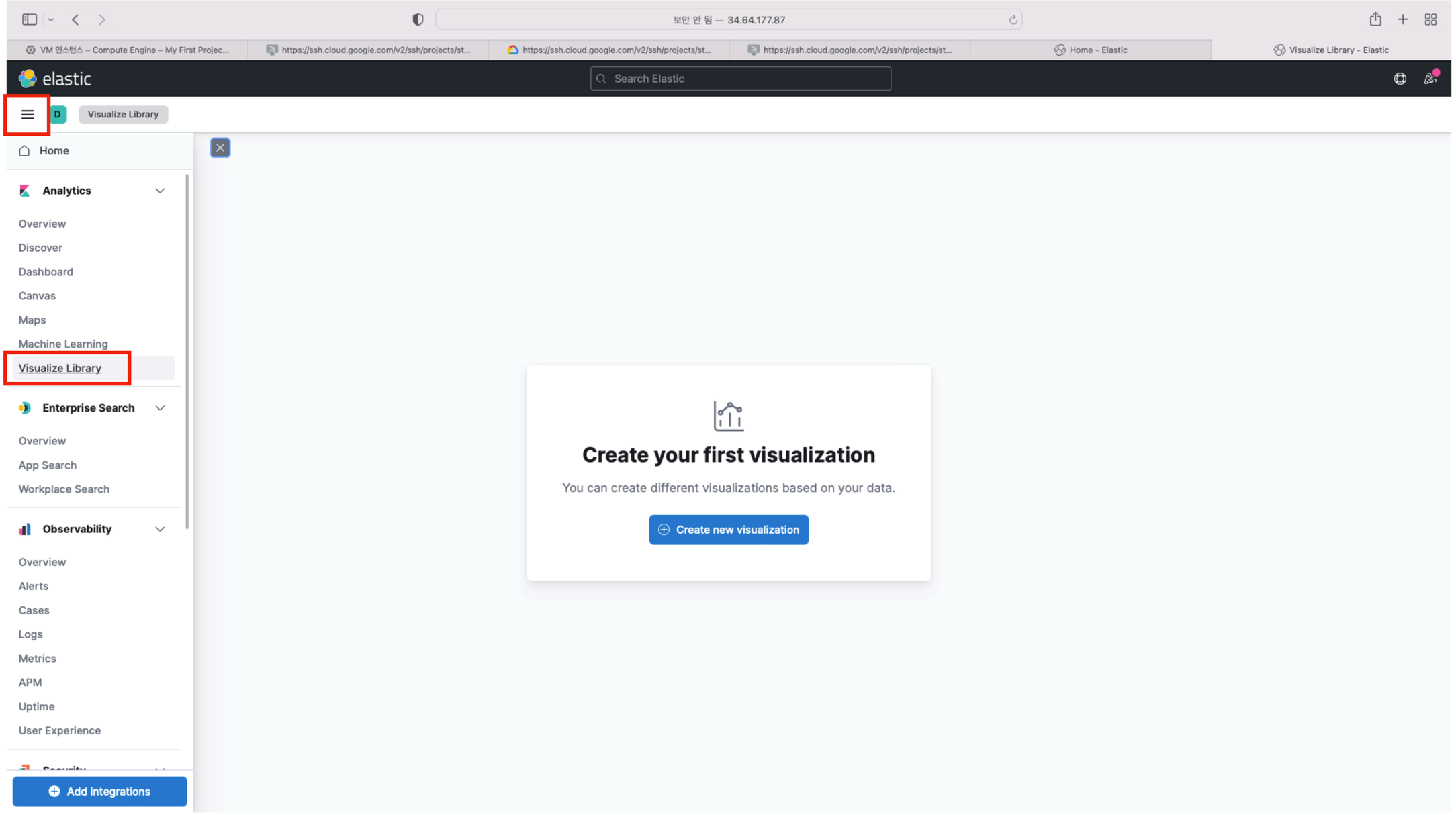


name: Stephen* 으로 검색을 합니다.

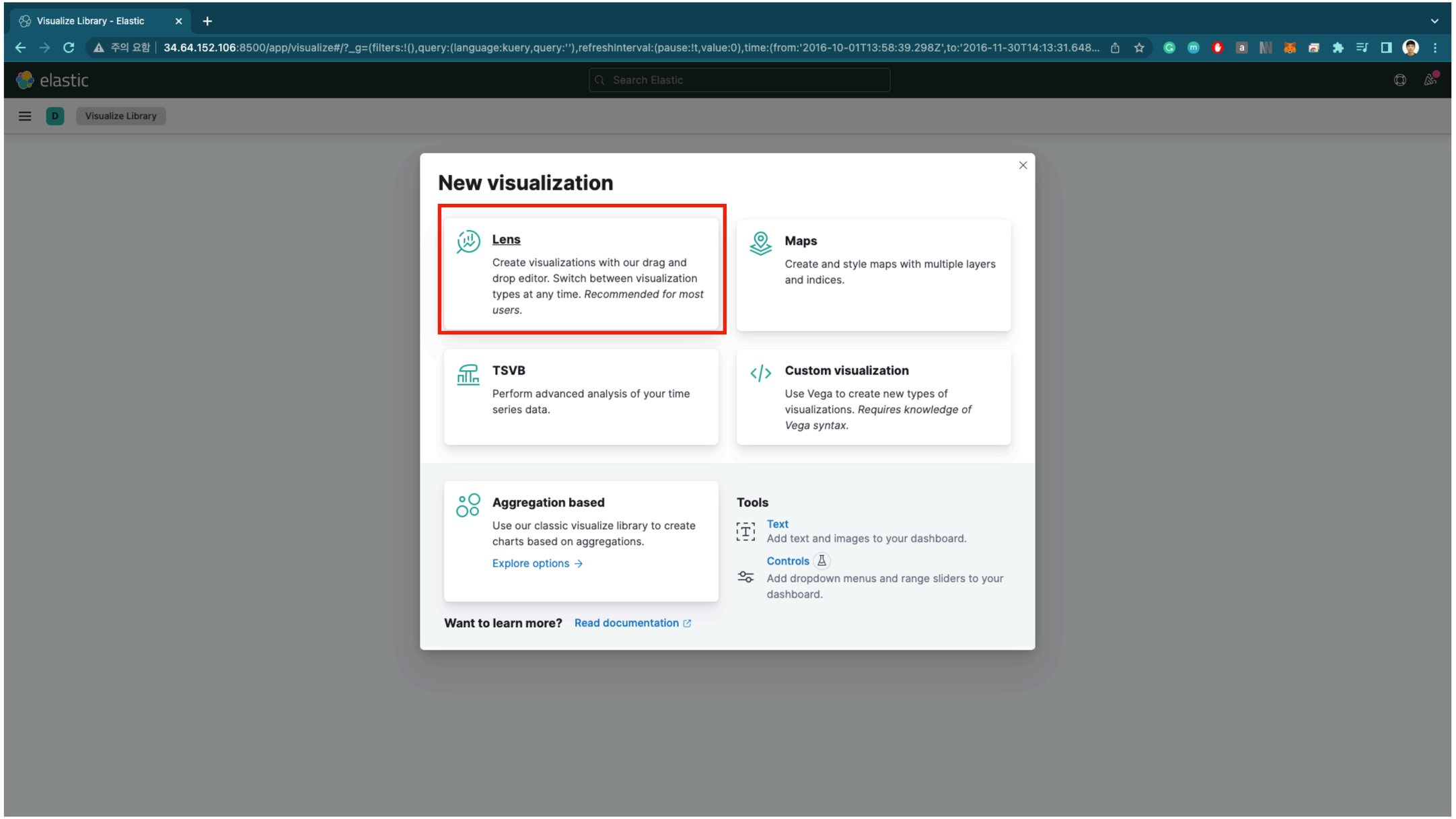


Kibana Visualize

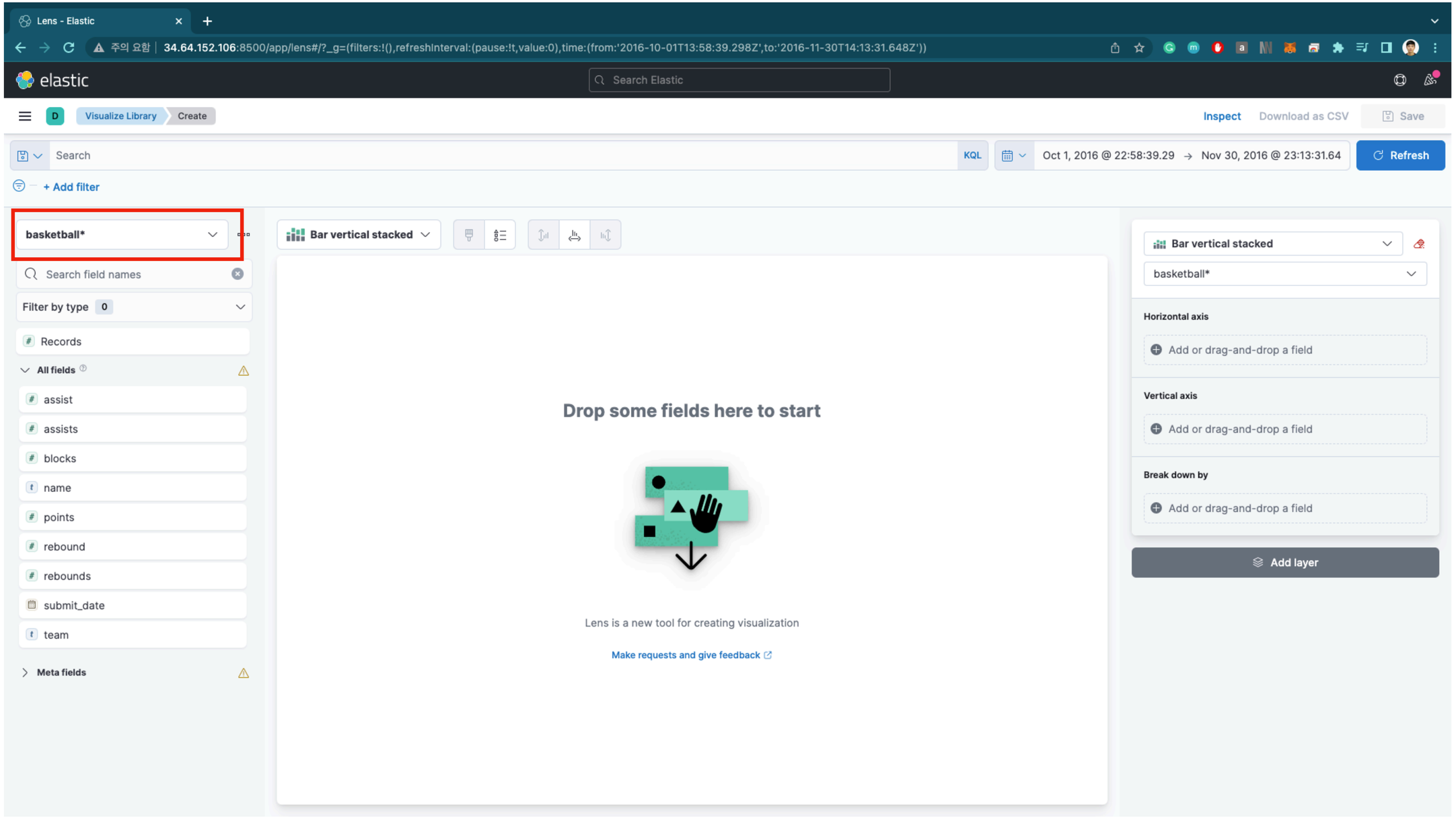
Visualize Library로 이동



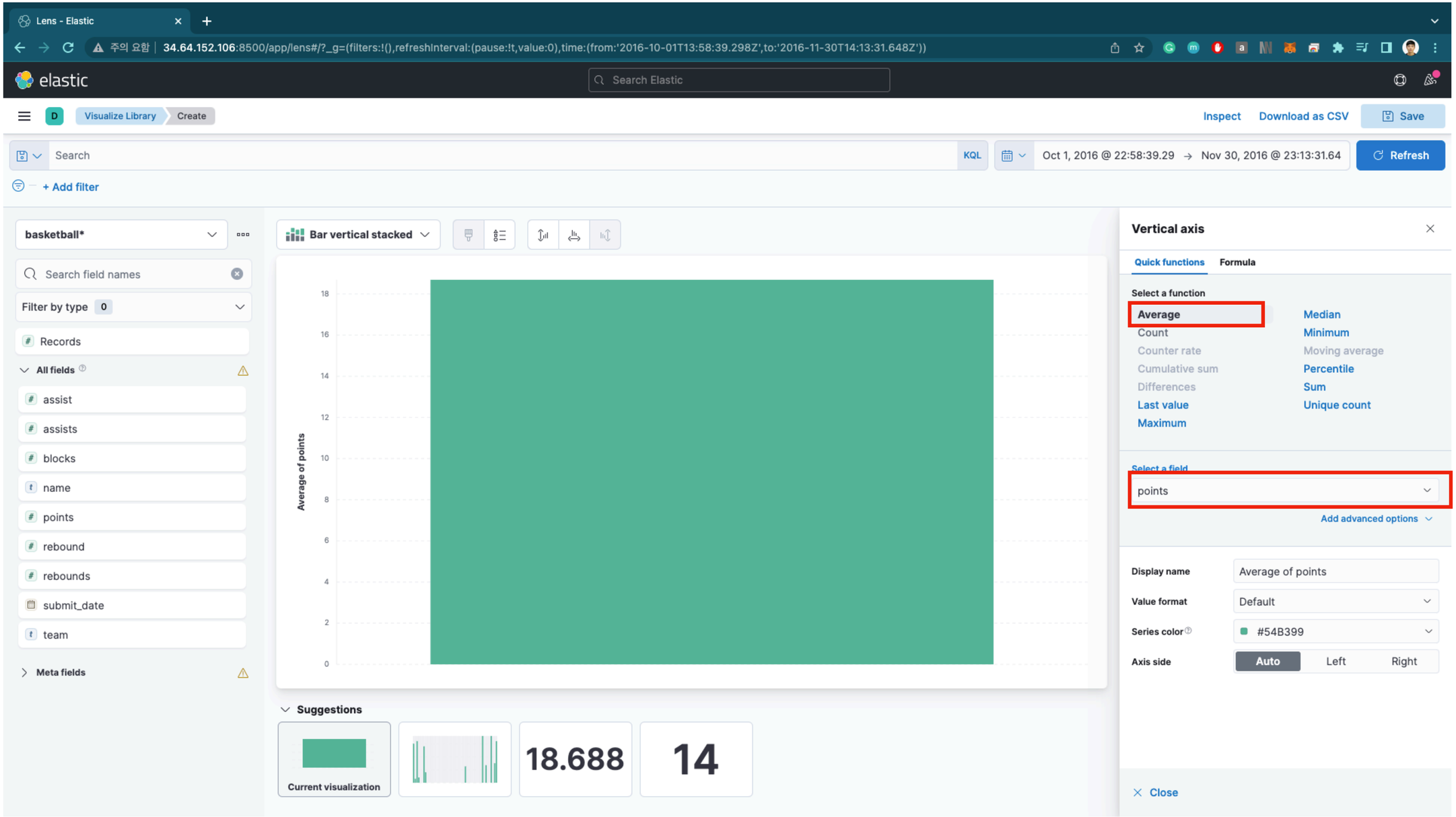
Lens 선택


Visualize Library - Elastic
주의 요함 | 34.64.152.106:8500/app/visualize#/?_g=(filters:!(),query:(language:kuery,query:''),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648...
elastic
Search Elastic
D
Visualize Library
New visualization
Lens
Create visualizations with our drag and drop editor. Switch between visualization types at any time. Recommended for most users.
Maps
Create and style maps with multiple layers and indices.
TSVB
Perform advanced analysis of your time series data.
Custom visualization
Use Vega to create new types of visualizations. Requires knowledge of Vega syntax.
Aggregation based
Use our classic visualize library to create charts based on aggregations.
Explore options →
Tools
Text
Add text and images to your dashboard.
Controls
Add dropdown menus and range sliders to your dashboard.
Want to learn more?
Read documentation

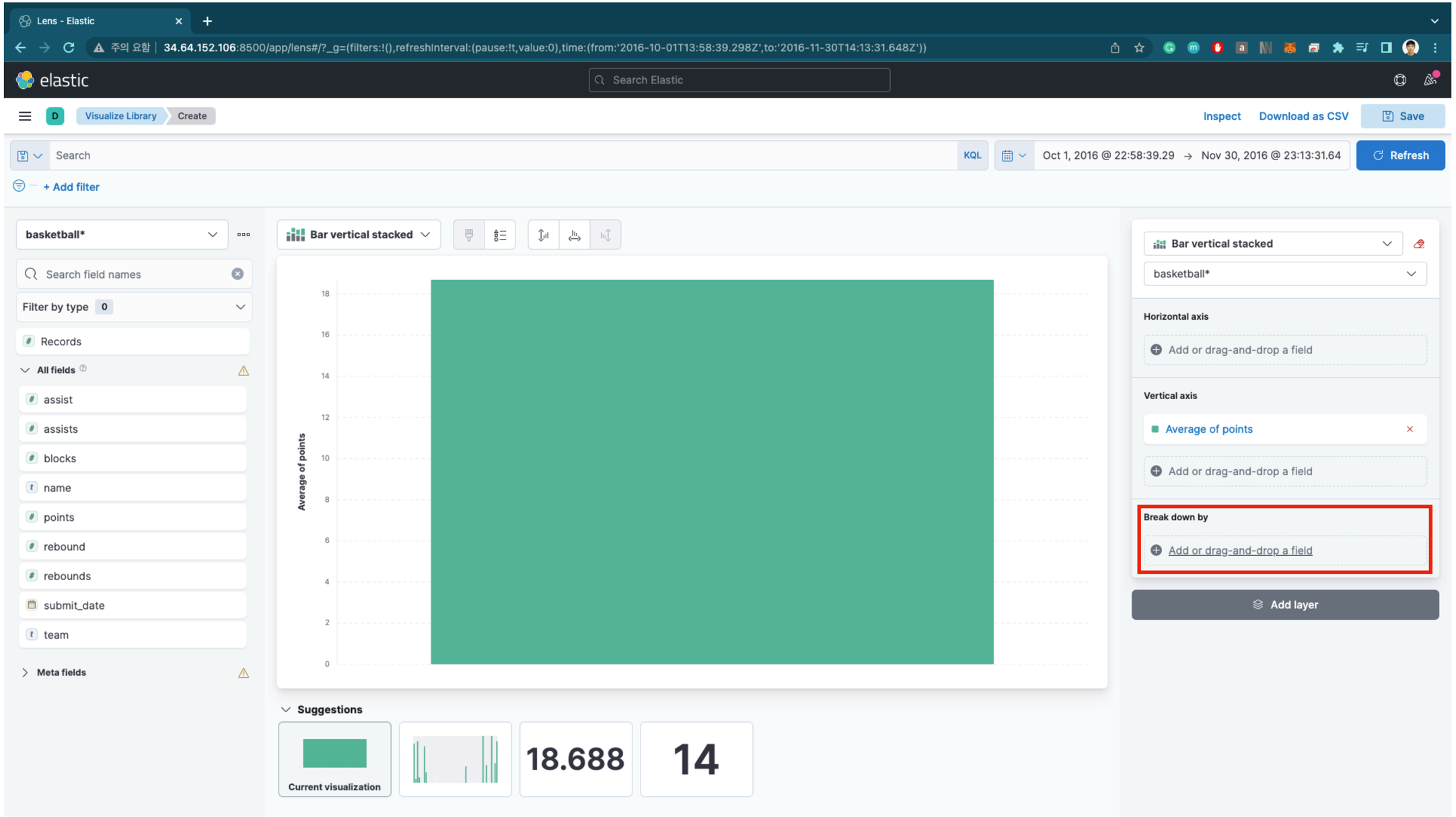
Basketball 선택



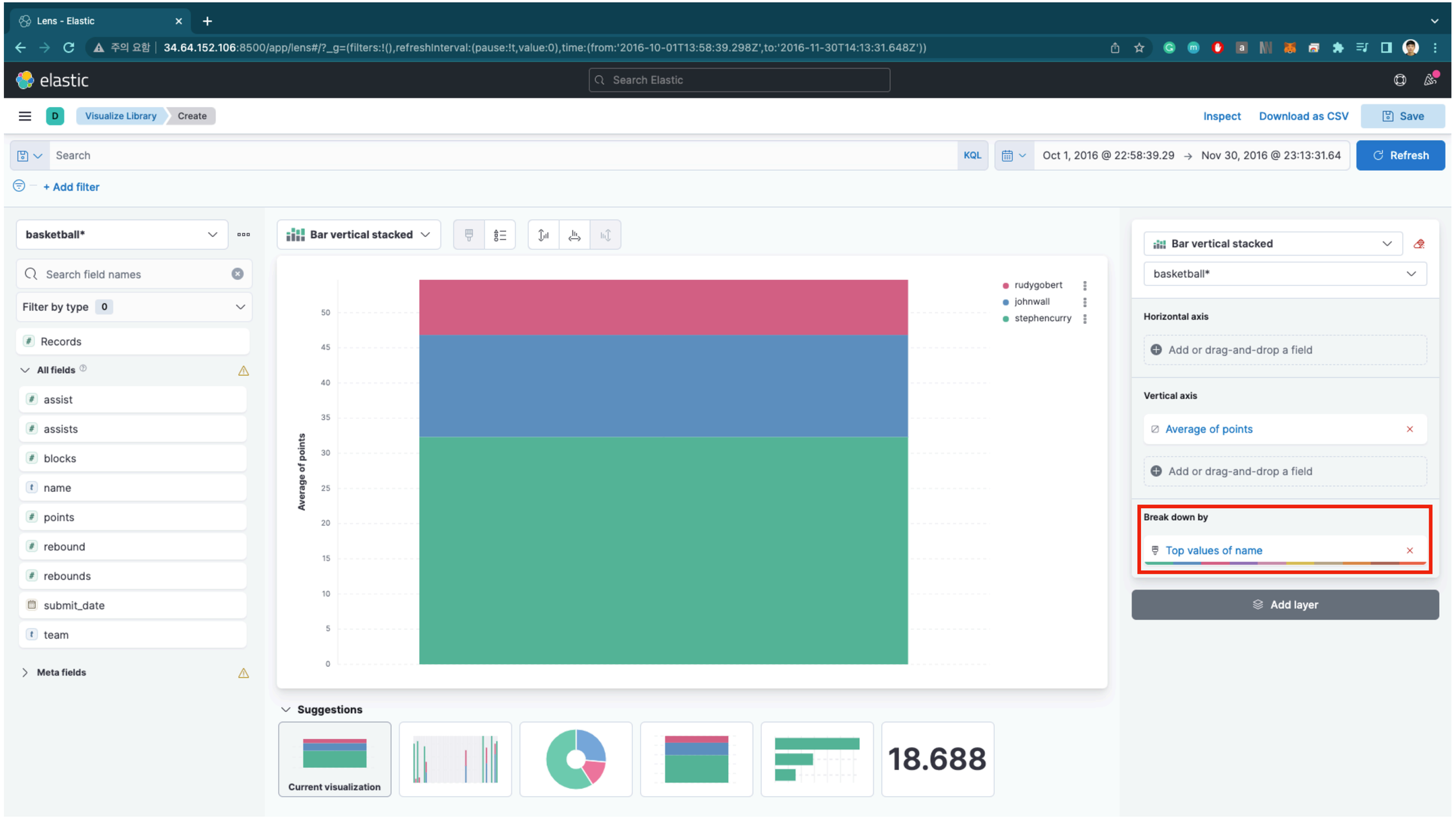
Vertical Axis를 오른쪽과 같이 세팅



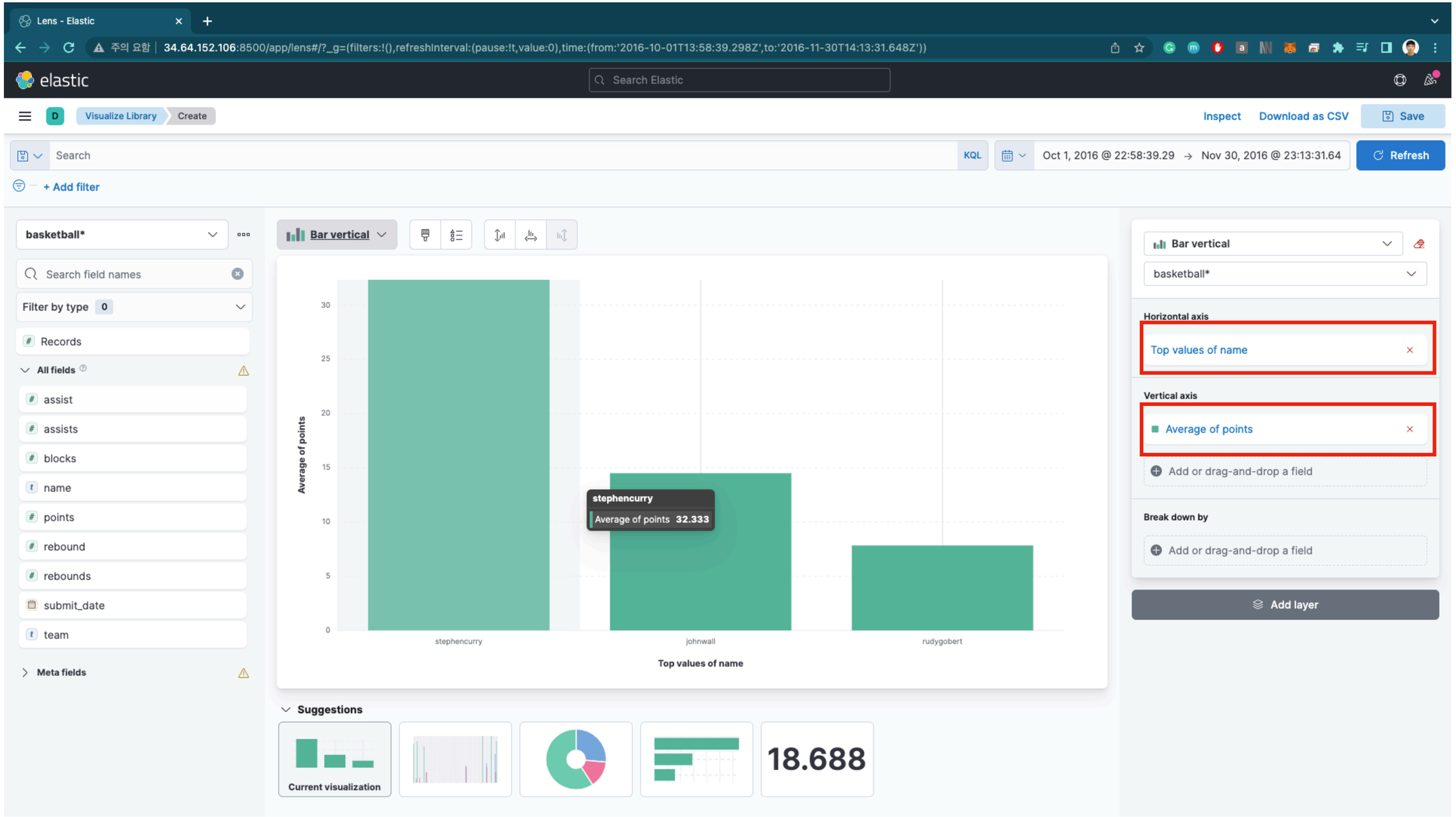
Break down by 세팅



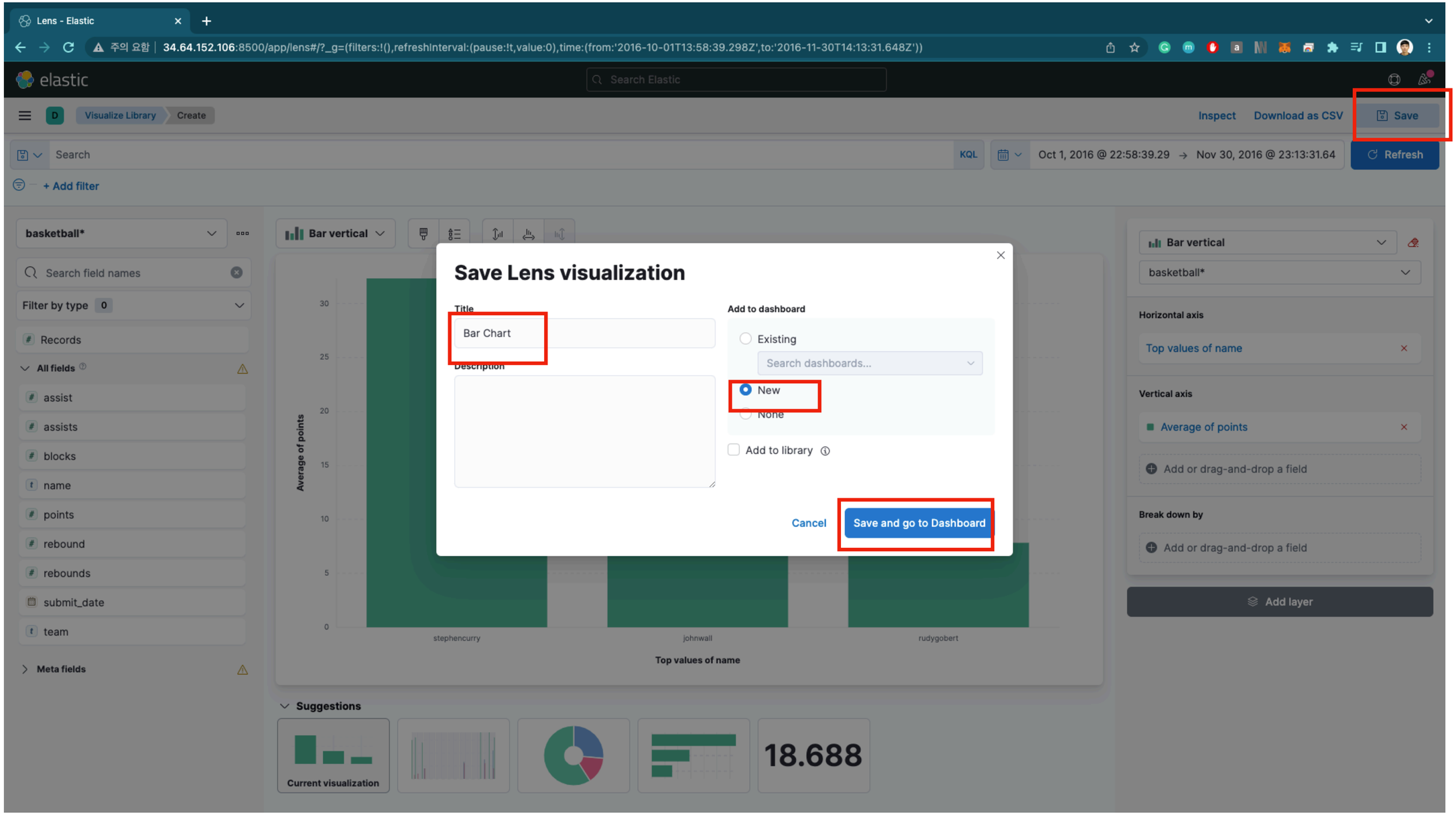
선수별 평균 득점


Lens - Elastic
34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Visualize Library
Create
Inspect
Download as CSV
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
basketball*
Search field names
Filter by type 0
Records
All fields
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team
Meta fields
Bar vertical stacked
Average of points
rudygobert
johnwall
stephencurry
Suggestions
Current visualization
18.688
Bar vertical stacked
basketball*
Horizontal axis
Add or drag-and-drop a field
Vertical axis
Average of points
Add or drag-and-drop a field
Break down by
Top values of name
Add layer

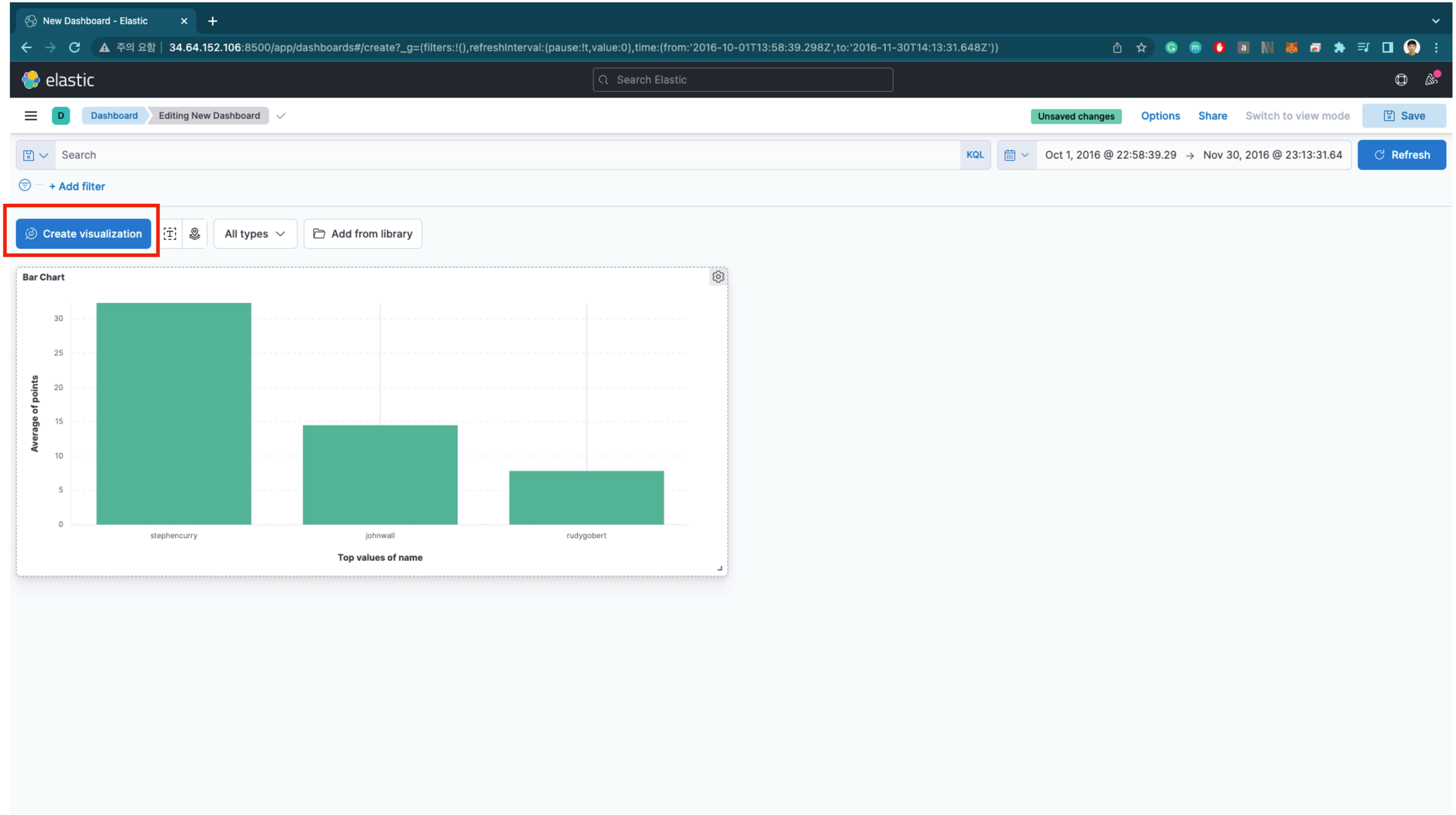
일반 바차트로 변경


Lens - Elastic
34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Visualize Library
Create
Inspect
Download as CSV
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
basketball*
Search field names
Filter by type 0
Records
All fields
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team
Meta fields
Bar vertical
Average of points
30
25
20
15
10
5
0
stephencurry
Average of points 32.333
stephencurry
johnwall
rudygobert
Top values of name
Suggestions
Current visualization
18.688
Bar vertical
basketball*
Horizontal axis
Top values of name
Vertical axis
Average of points
Add or drag-and-drop a field
Break down by
Add or drag-and-drop a field
Add layer

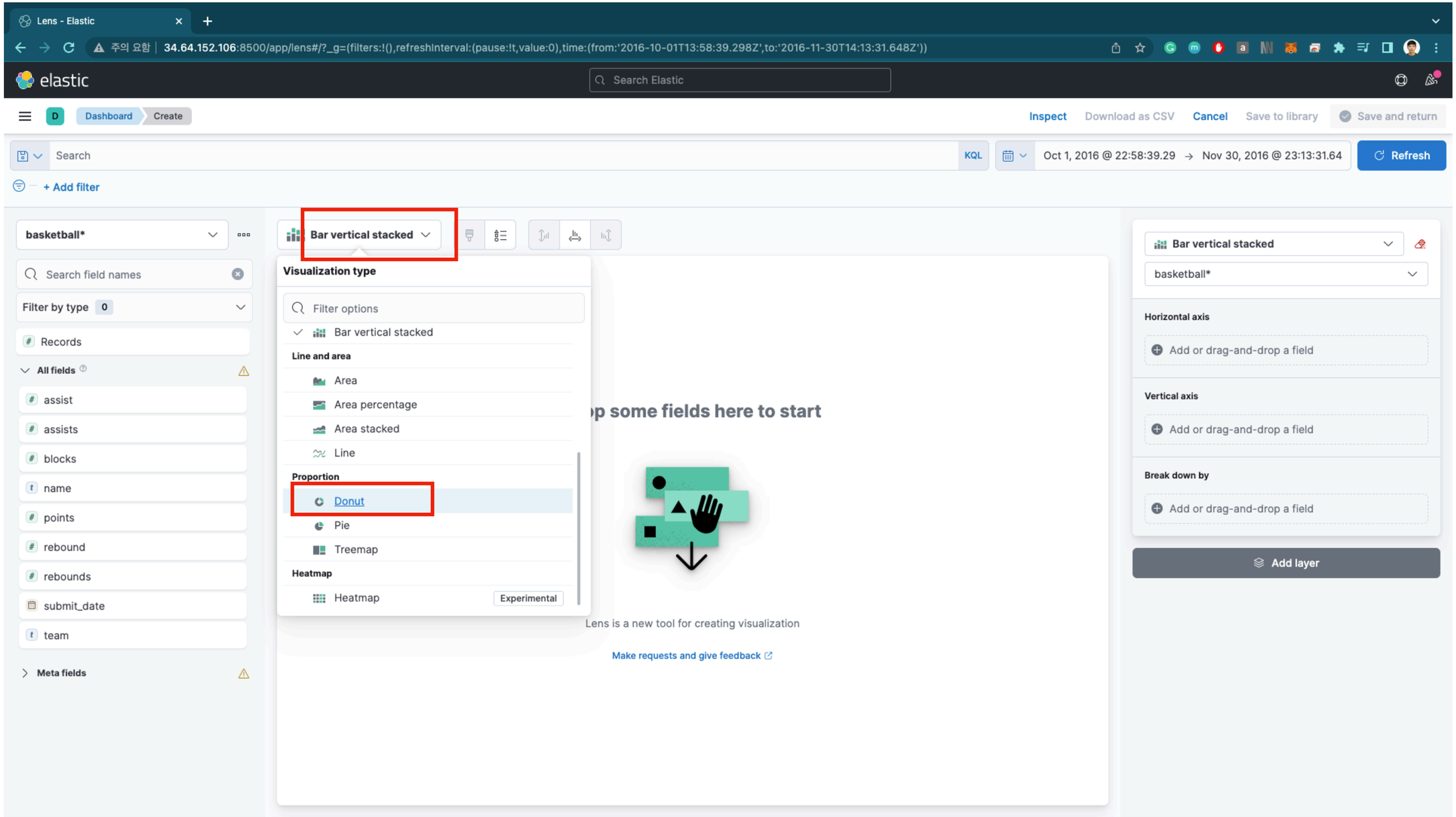
저장


Lens - Elastic
34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Visualize Library
Create
Inspect
Download as CSV
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
basketball*
Search field names
Filter by type 0
Records
All fields
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team
Meta fields
Bar vertical
Save Lens visualization
Title
Bar Chart
Description
Add to dashboard
Existing
Search dashboards...
New
None
Add to library
Cancel
Save and go to Dashboard
Average of points
stephencurry
johnwall
rudygobert
Top values of name
Horizontal axis
Top values of name
Vertical axis
Average of points
Add or drag-and-drop a field
Break down by
Add or drag-and-drop a field
Add layer
Suggestions
Current visualization
18.688

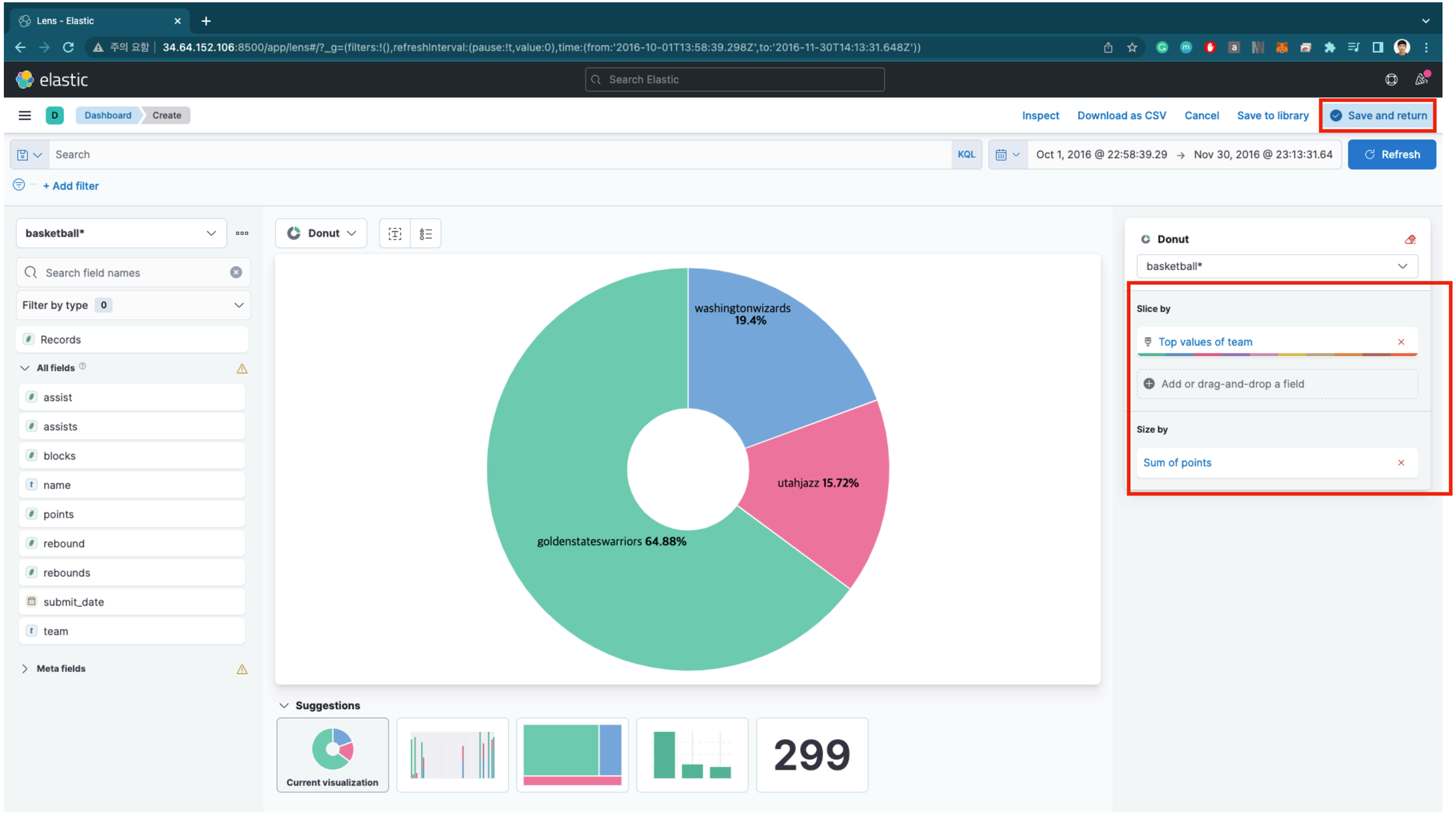
차트들을 한번에 보기 위한 대시보드 생성



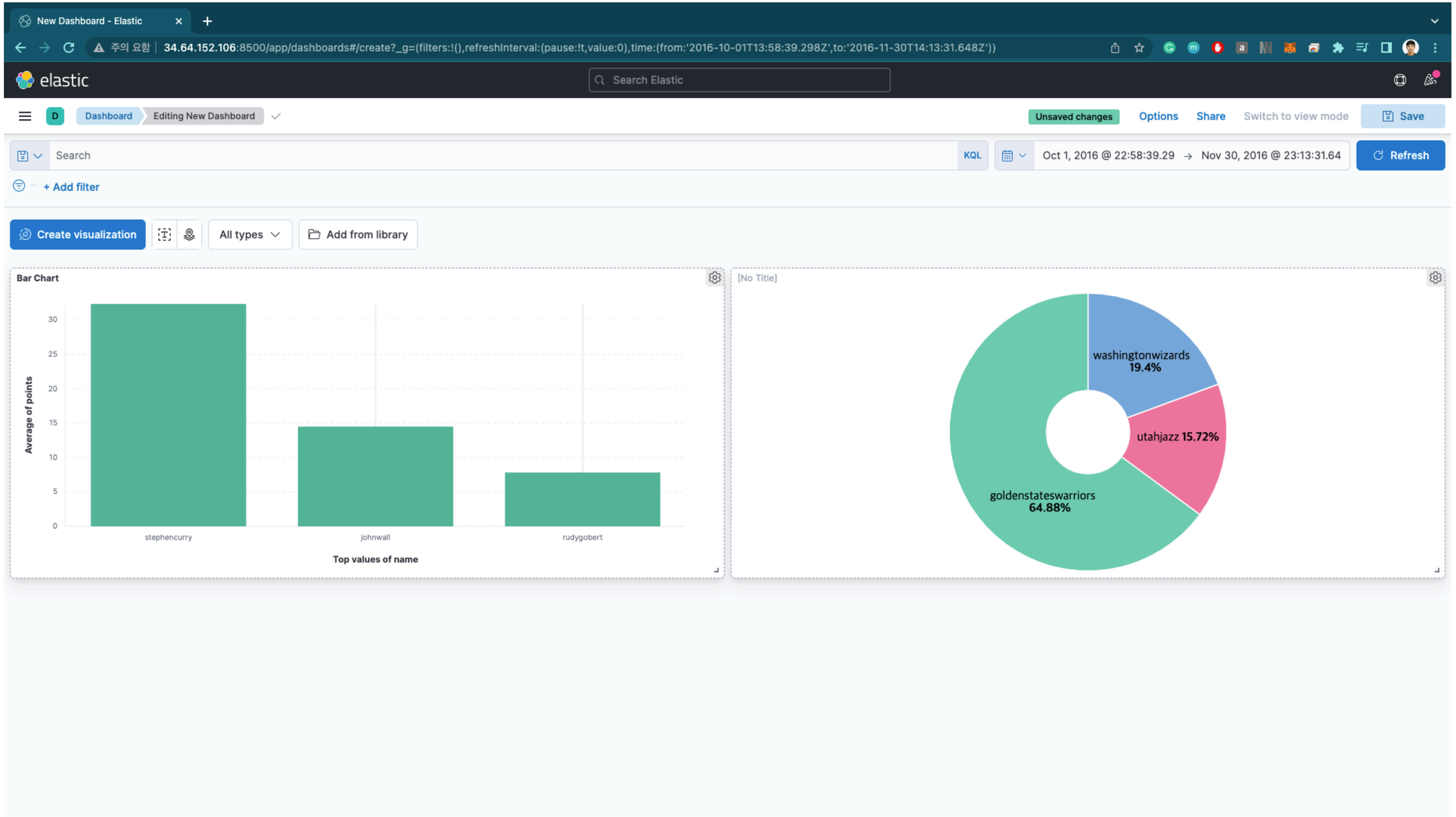
이번에는 도넛차트 생성


Lens - Elastic
34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Dashboard
Create
Inspect
Download as CSV
Cancel
Save to library
Save and return
Search
KQL
Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
basketball*
Search field names
Filter by type 0
Records
All fields
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team
Meta fields
Bar vertical stacked
Visualization type
Filter options
Bar vertical stacked
Line and area
Area
Area percentage
Area stacked
Line
Proportion
Donut
Pie
Treemap
Heatmap
Heatmap
Experimental
op some fields here to start
Lens is a new tool for creating visualization
Make requests and give feedback
Bar vertical stacked
basketball*
Horizontal axis
Add or drag-and-drop a field
Vertical axis
Add or drag-and-drop a field
Break down by
Add or drag-and-drop a field
Add layer

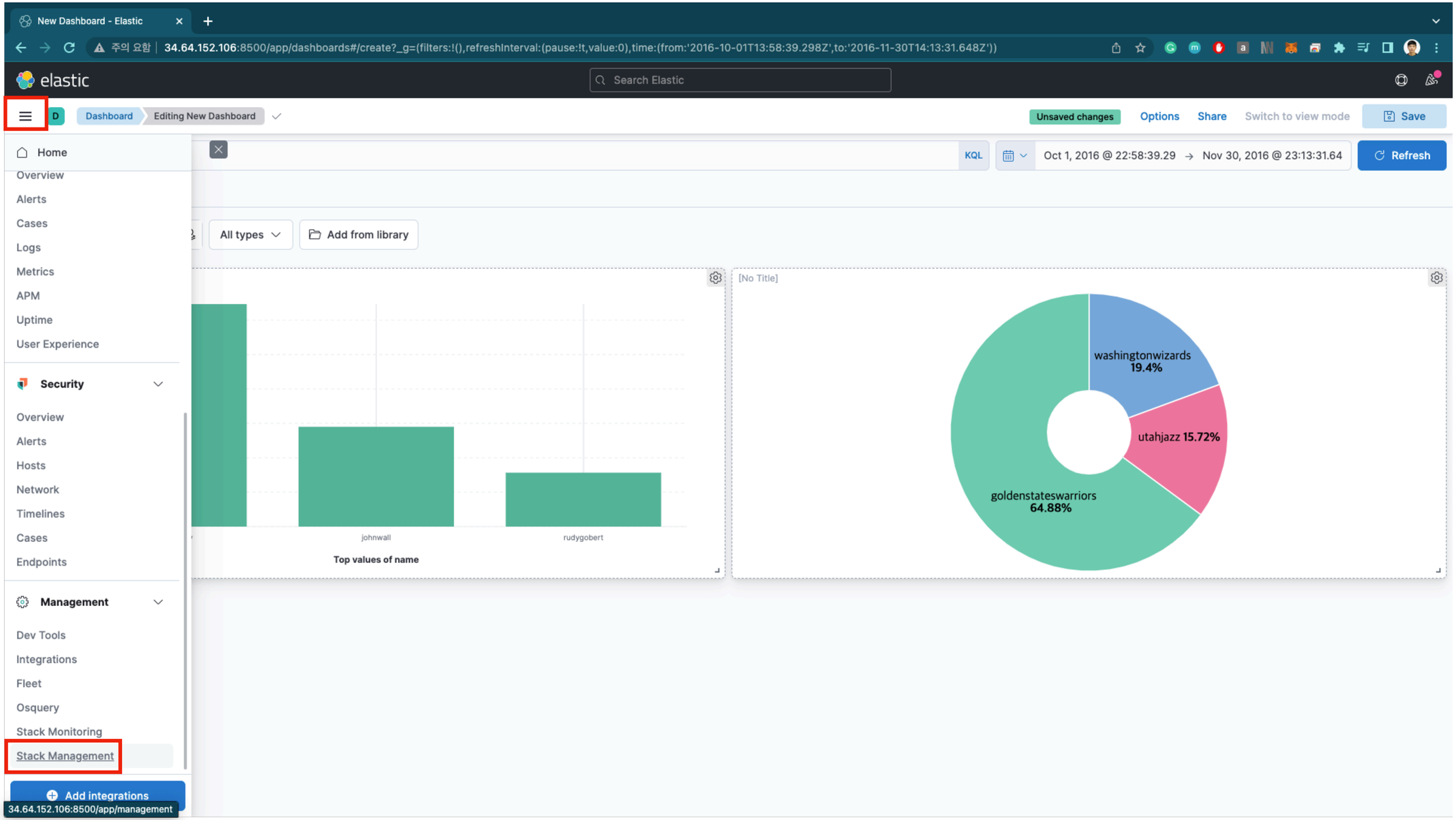
값을 오른쪽과 같이 구성


Lens - Elastic
34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Dashboard
Create
Inspect
Download as CSV
Cancel
Save to library
Save and return
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
basketball*
Search field names
Filter by type 0
Records
All fields
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team
Meta fields
Donut
washingtonwizards 19.4%
utahjazz 15.72%
goldenstateswarriors 64.88%
Suggestions
Current visualization
299
Donut
basketball*
Slice by
Top values of team
Add or drag-and-drop a field
Size by
Sum of points

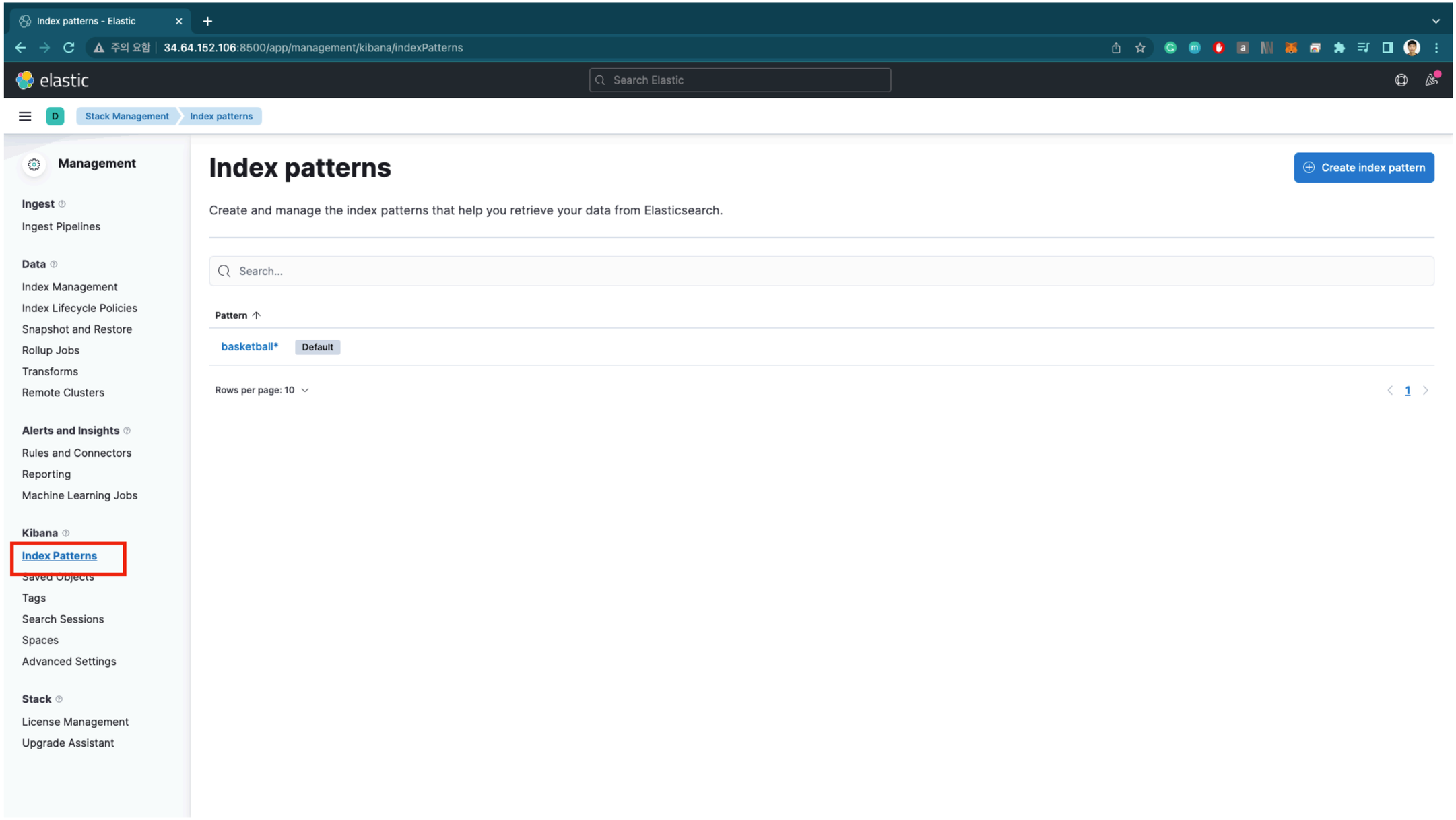
대쉬 보드에 도넛 차트도 추가



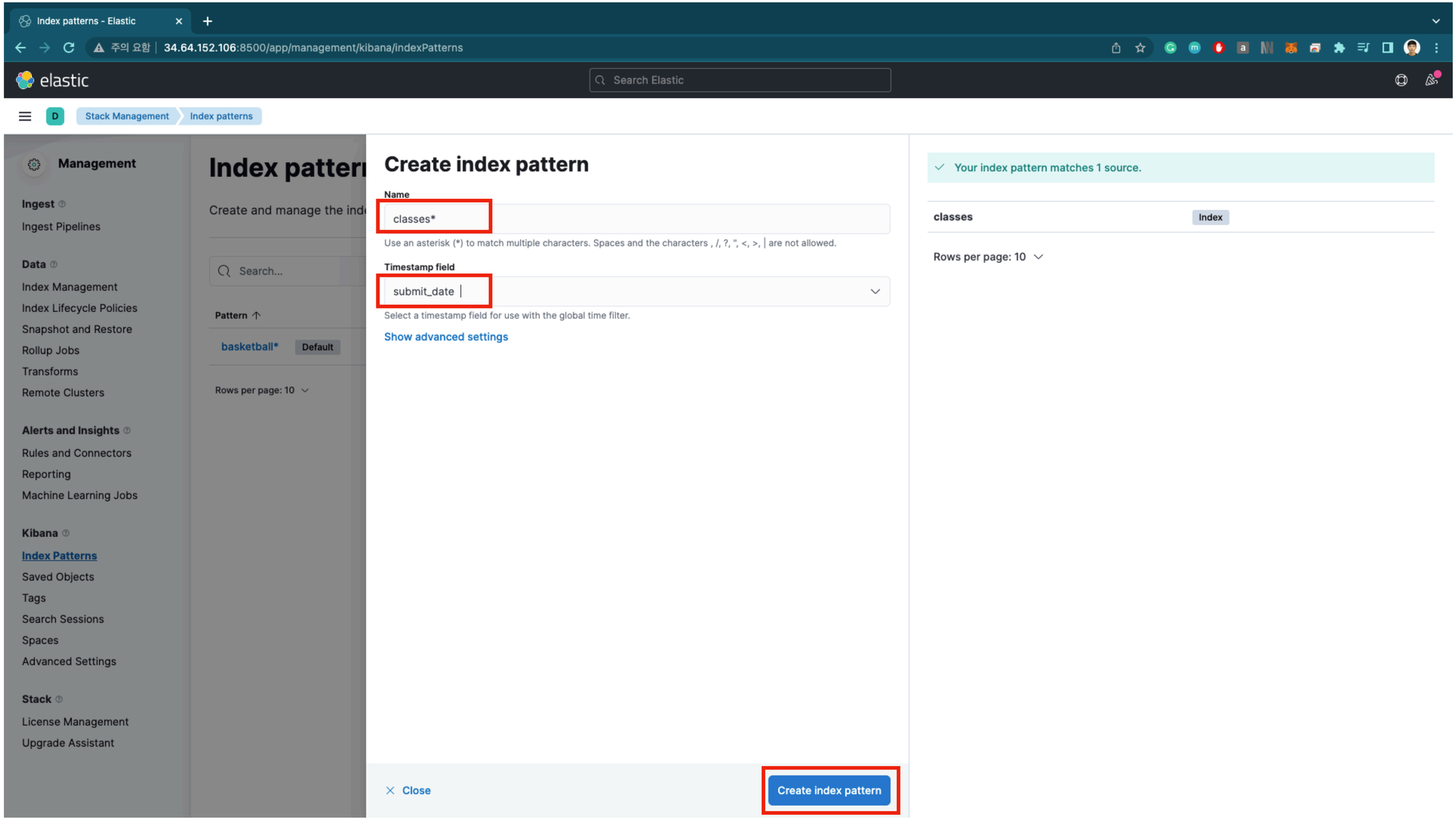
다른 인덱스도 세팅


New Dashboard - Elastic
34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Dashboard
Editing New Dashboard
Unsaved changes
Options
Share
Switch to view mode
Save
Home
Overview
Alerts
Cases
Logs
Metrics
APM
Uptime
User Experience
Security
Overview
Alerts
Hosts
Network
Timelines
Cases
Endpoints
Management
Dev Tools
Integrations
Fleet
Osquery
Stack Monitoring
Stack Management
Add integrations
34.64.152.106:8500/app/management
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
All types
Add from library
johnwall
rudygobert
Top values of name
[No Title]
washingtonwizards
19.4%
utahjazz 15.72%
goldenstateswarriors
64.88%

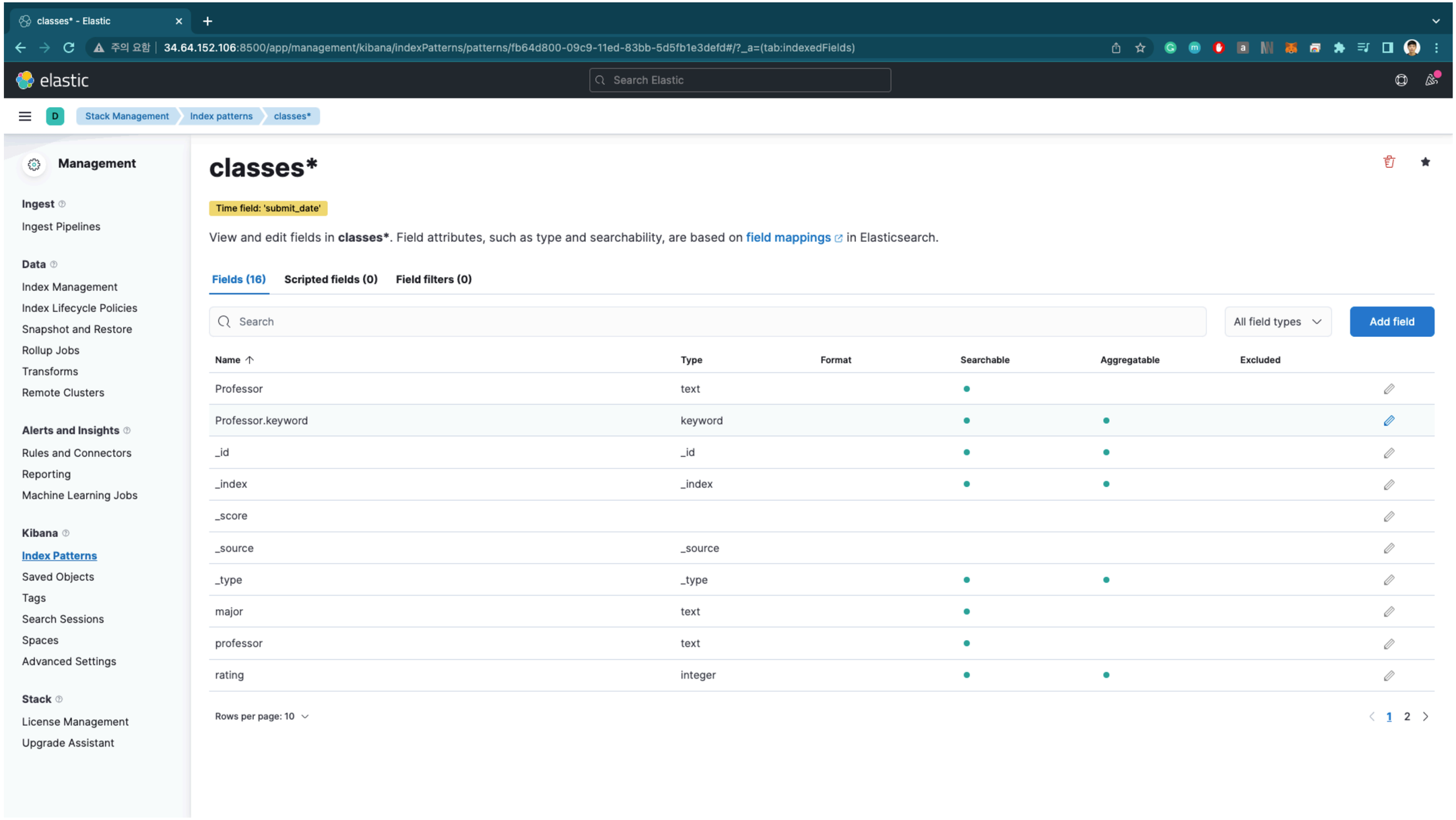
새로운 인덱스 패턴 세팅


Index patterns - Elastic
주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns
elastic
Search Elastic
D
Stack Management
Index patterns
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
Index patterns
Create index pattern
Create and manage the index patterns that help you retrieve your data from Elasticsearch.
Search...
Pattern
basketball*
Default
Rows per page: 10
1

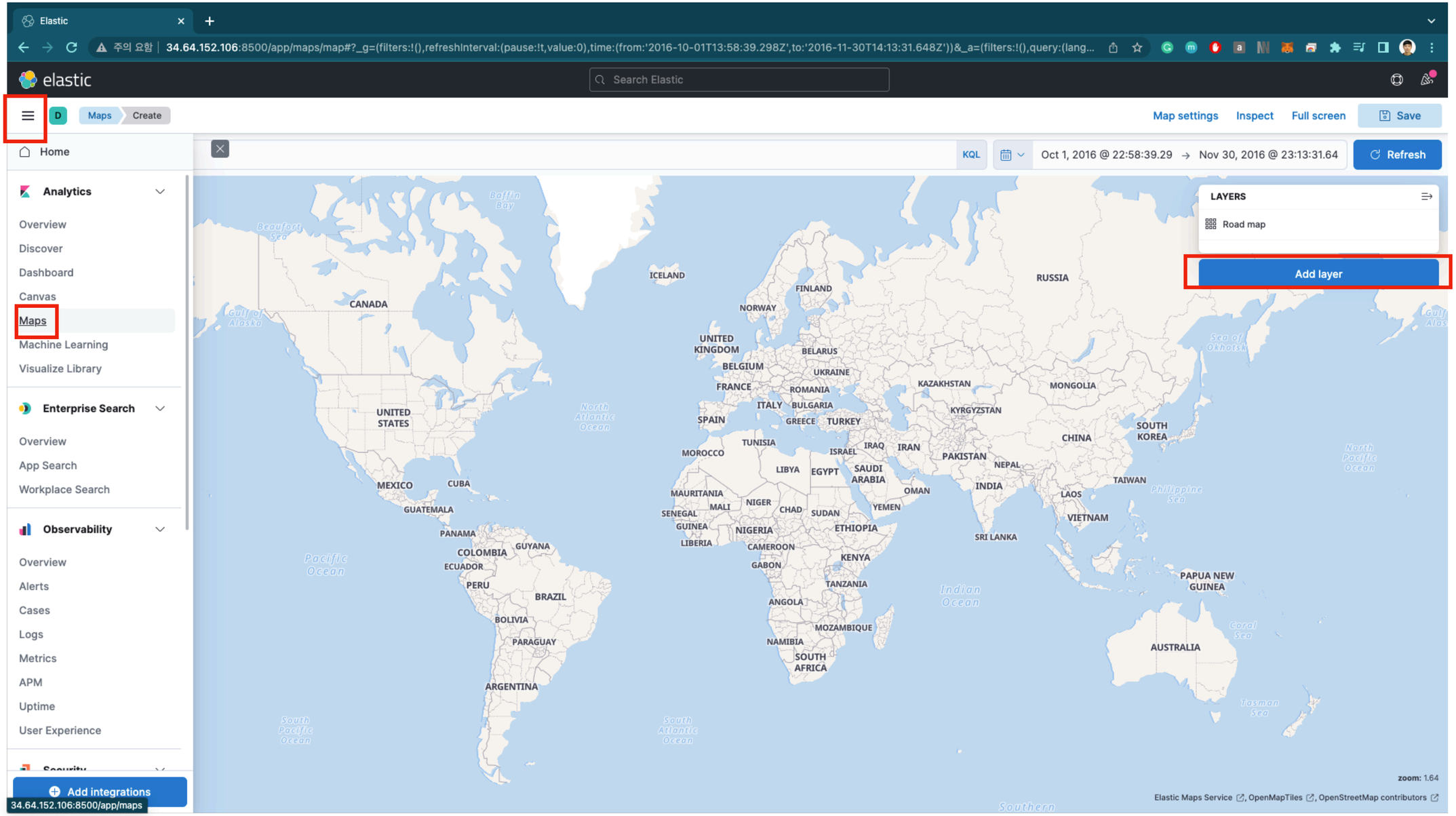
class 입력


Index patterns - Elastic
주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns
elastic
Search Elastic
D
Stack Management
Index patterns
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
Index patter
Create and manage the ind
Search...
Pattern
basketball*
Default
Rows per page: 10
Create index pattern
Name
classes*
Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.
Timestamp field
submit_date
Select a timestamp field for use with the global time filter.
Show advanced settings
Close
Create index pattern
Your index pattern matches 1 source.
classes
Index
Rows per page: 10

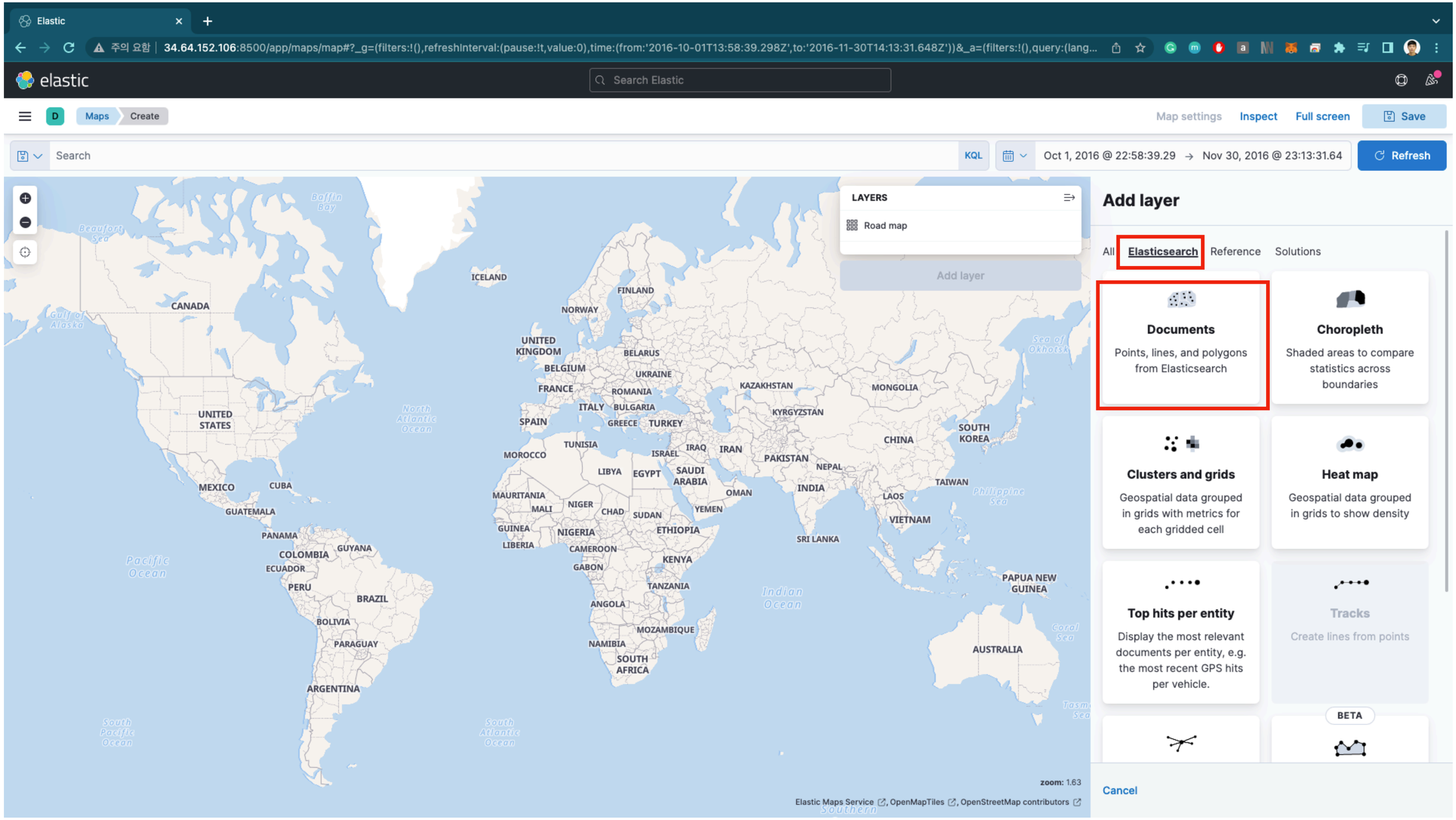
잘 설정되었네요!


classes* - Elastic
주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns/patterns/fb64d800-09c9-11ed-83bb-5d5fb1e3defd#/?_a=(tab:indexedFields)
elastic
Search Elastic
D
Stack Management
Index patterns
classes*
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
classes*
Time field: 'submit_date'
View and edit fields in classes*. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (16)
Scripted fields (0)
Field filters (0)
Search
All field types
Add field
Name
Type
Format
Searchable
Aggregatable
Excluded
Professor text
Professor.keyword keyword
_id _id
_index _index
_score
_source _source
_type _type
major text
professor text
rating integer
Rows per page: 10
1
2

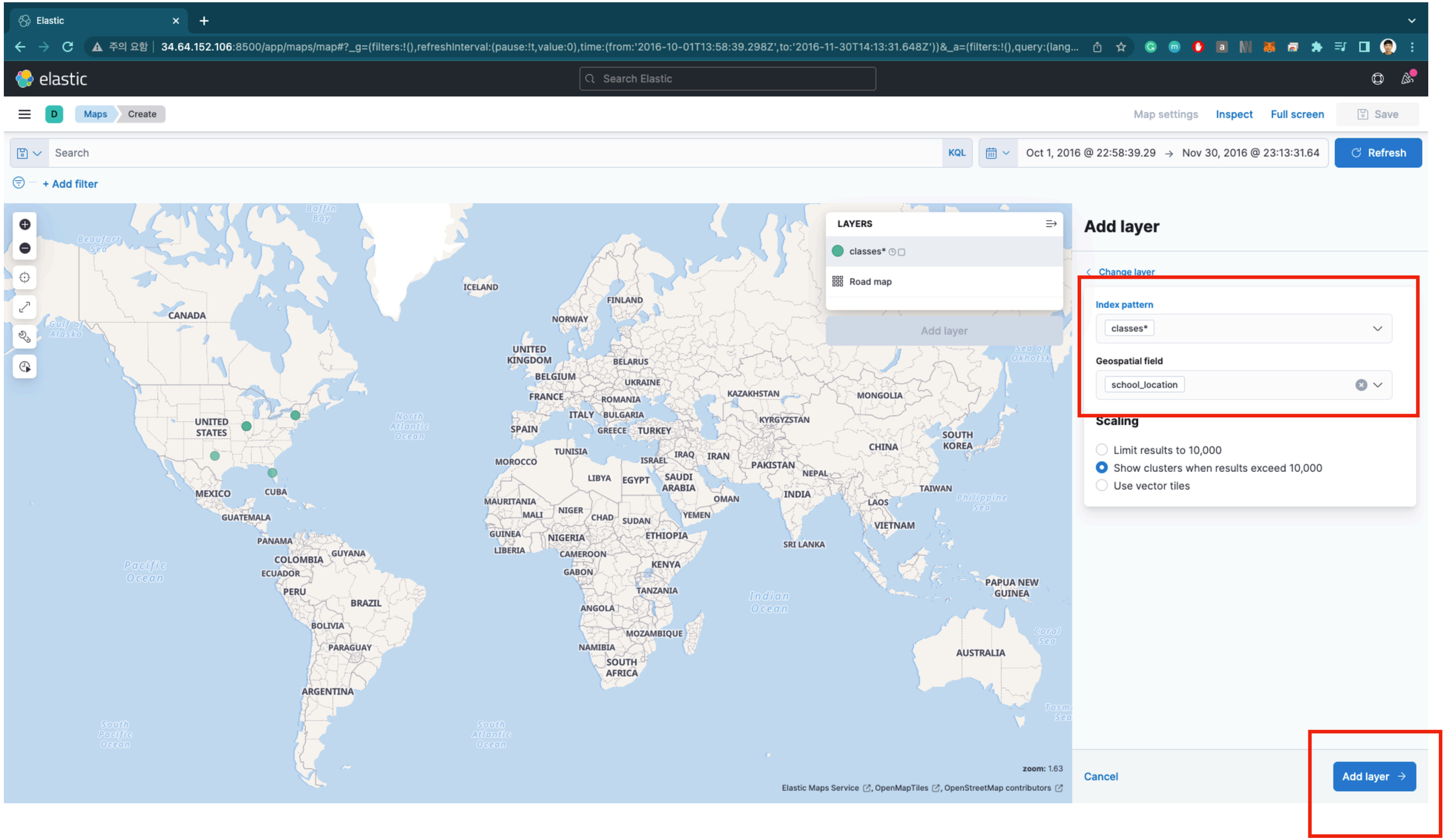
이번에는 지도 세팅


Elastic
34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...
elastic
Search Elastic
D
Maps
Create
Map settings
Inspect
Full screen
Save
Home
Analytics
Overview
Discover
Dashboard
Canvas
Maps
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Alerts
Cases
Logs
Metrics
APM
Uptime
User Experience
Add integrations
34.64.152.106:8500/app/maps
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
LAYERS
Road map
Add layer
zoom: 1.64
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

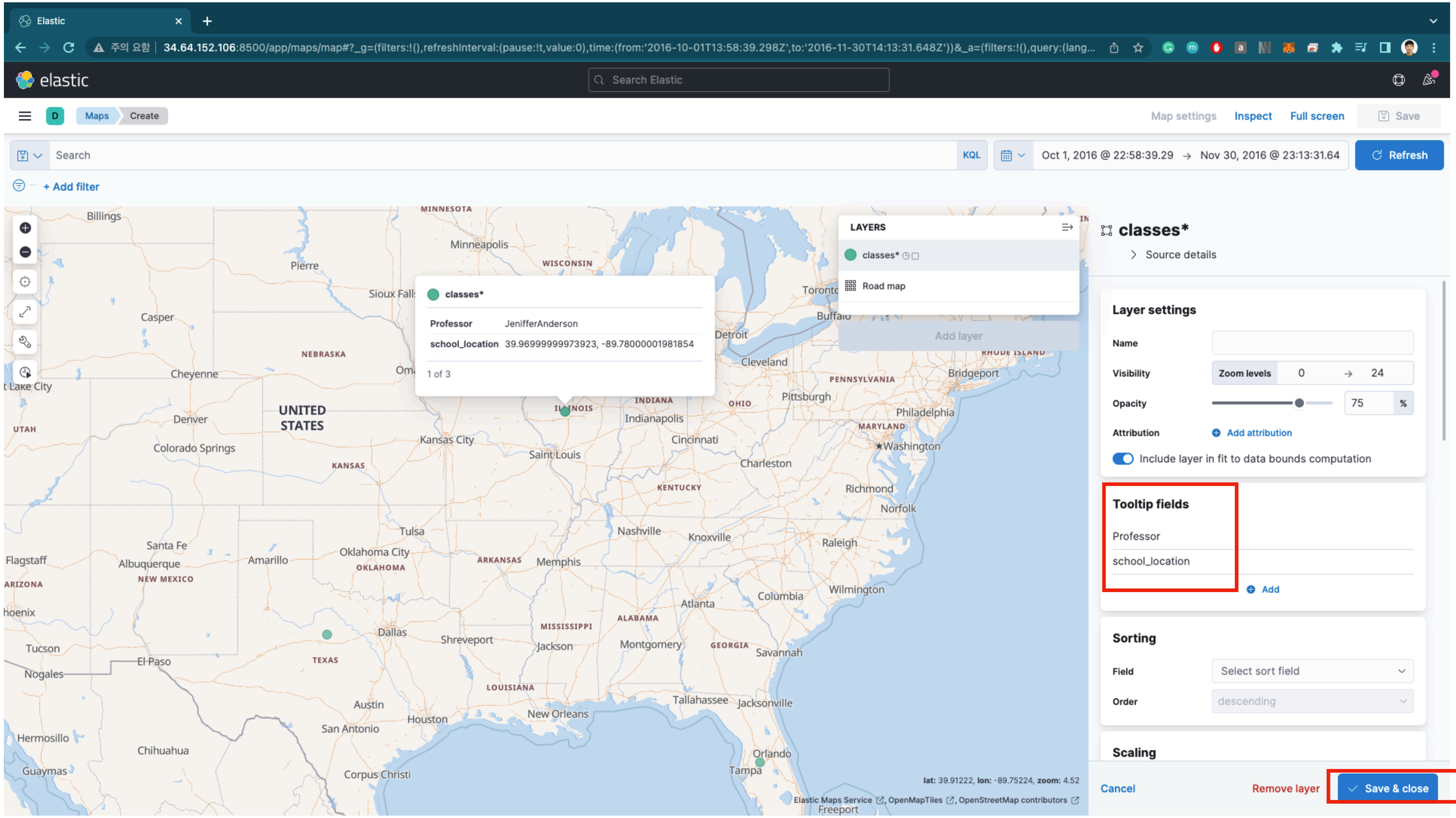
Elasticsearch에 저장된 Document 선택



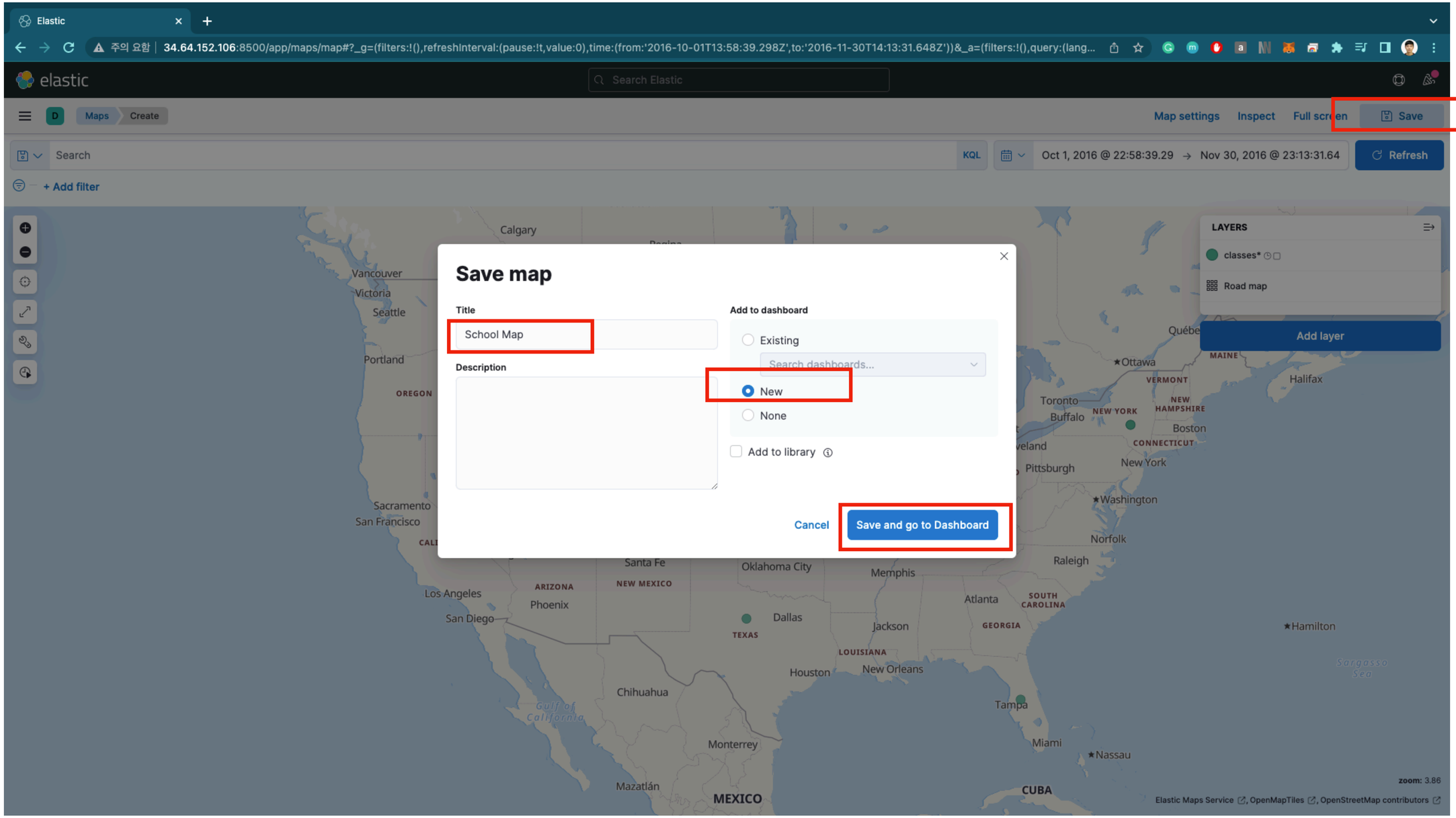
classes 선택


Elastic
34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...
elastic
Search Elastic
D
Maps
Create
Map settings
Inspect
Full screen
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
LAYERS
classes*
Road map
Add layer
Add layer
Change layer
Index pattern
classes*
Geospatial field
school_location
Scaling
Limit results to 10,000
Show clusters when results exceed 10,000
Use vector tiles
Cancel
Add layer
zoom: 1.63
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

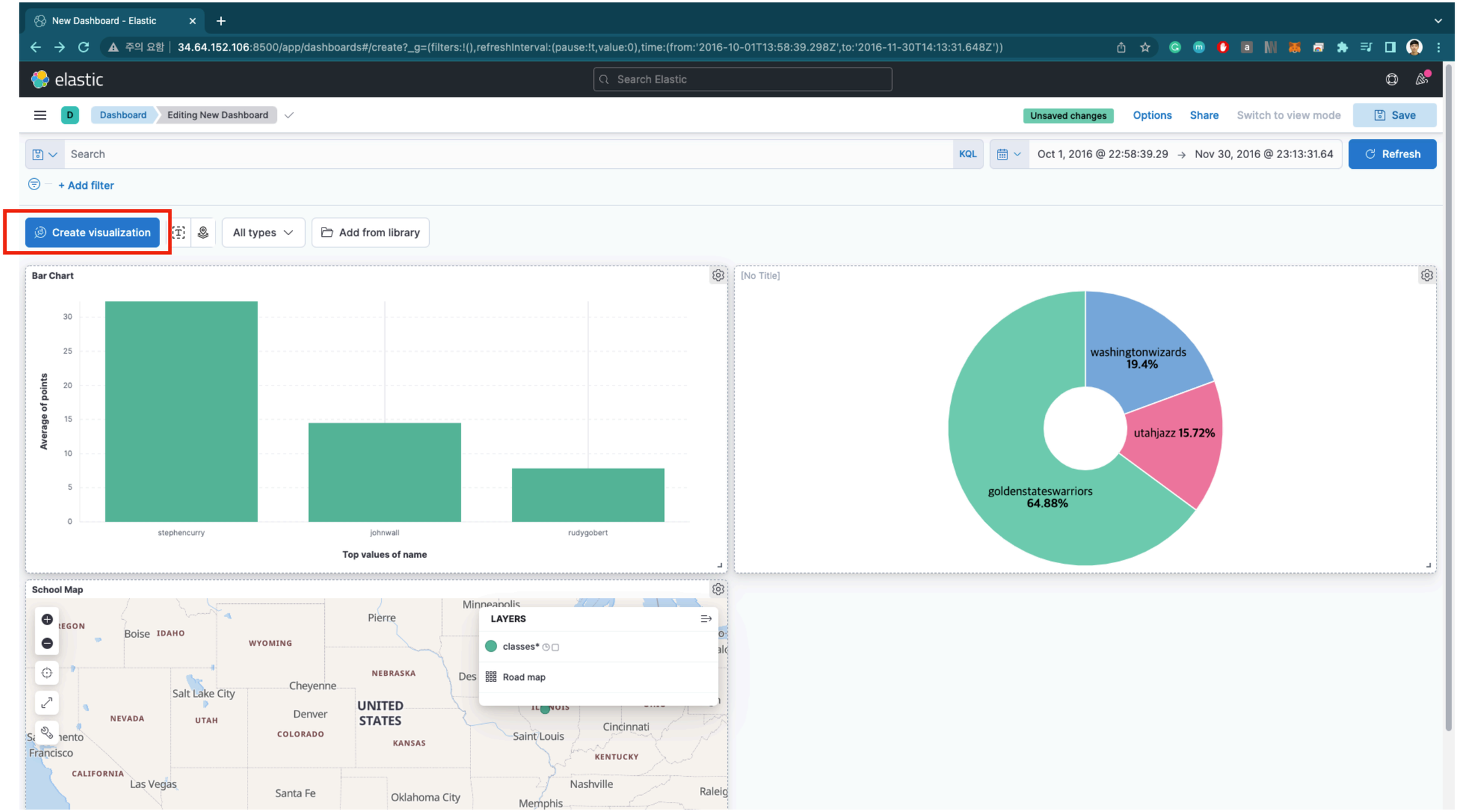
지도에서 데이터 확인


Elastic
34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...
elastic
Search Elastic
D
Maps
Create
Map settings
Inspect
Full screen
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
classes*
Professor JenifferAnderson
school_location 39.96999999973923, -89.78000001981854
1 of 3
LAYERS
classes*
Road map
Add layer
classes*
Source details
Layer settings
Name
Visibility
Zoom levels 0 24
Opacity
75 %
Attribution
Add attribution
Include layer in fit to data bounds computation
Tooltip fields
Professor
school_location
Add
Sorting
Field
Select sort field
Order
descending
Scaling
Cancel
Remove layer
Save & close
lat: 39.91222, lon: -89.75224, zoom: 4.52
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
UNITED STATES
Billings
Minneapolis
Pierre
Sioux Falls
Casper
Cheyenne
Denver
Colorado Springs
Kansas City
Saint Louis
Indianapolis
Cincinnati
Pittsburgh
Cleveland
Detroit
Buffalo
Toronto
Philadelphia
Washington
Bridgeport
Charleston
Richmond
Norfolk
Raleigh
Knoxville
Nashville
Memphis
Atlanta
Columbia
Wilmington
Savannah
Montgomery
Jackson
Shreveport
Dallas
Oklahoma City
Tulsa
Amarillo
Albuquerque
Santa Fe
Flagstaff
Tucson
El Paso
Nogales
Austin
Houston
San Antonio
New Orleans
Tallahassee
Jacksonville
Orlando
Tampa
Hermosillo
Chihuahua
Guaymas
Corpus Christi
Freeport
Lake City
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
ARKANSAS
LOUISIANA
MISSISSIPPI
ALABAMA
GEORGIA
KENTUCKY
INDIANA
OHIO
PENNSYLVANIA
MARYLAND
WISCONSIN
MINNESOTA
UTAH
ARIZONA
NEW MEXICO

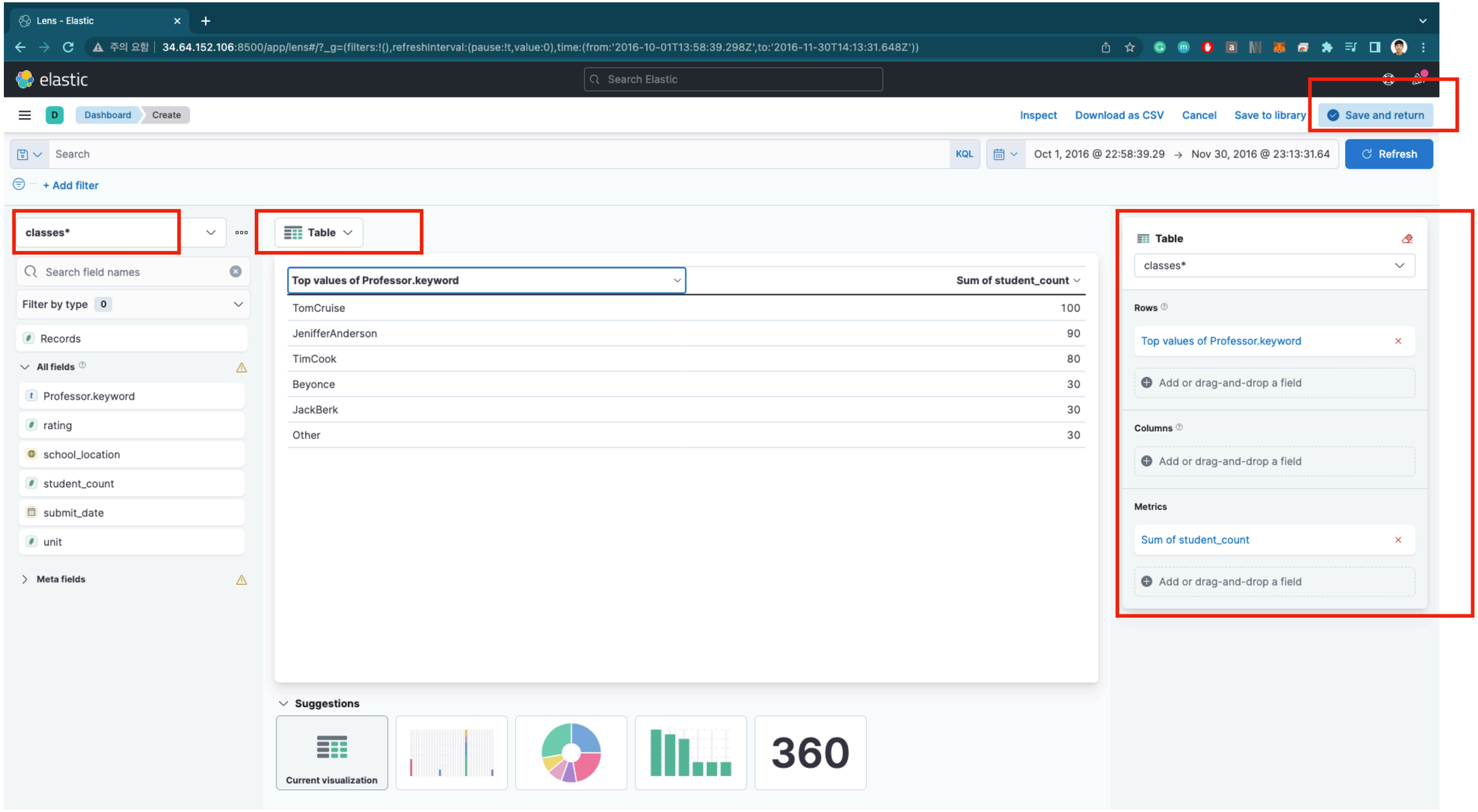
지도도 대쉬보드에 저장


Elastic
34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...
elastic
Search Elastic
Maps
Create
Map settings
Inspect
Full screen
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
LAYERS
classes*
Road map
Add layer
Save map
Title
School Map
Description
Add to dashboard
Existing
Search dashboards...
New
None
Add to library
Cancel
Save and go to Dashboard
Calgary
Vancouver
Victoria
Seattle
Portland
OREGON
Sacramento
San Francisco
Los Angeles
San Diego
Phoenix
ARIZONA
Santa Fe
NEW MEXICO
Dallas
TEXAS
Oklahoma City
Memphis
Atlanta
SOUTH CAROLINA
GEORGIA
Jackson
LOUISIANA
Houston
New Orleans
Chihuahua
Monterrey
Mazatlán
MEXICO
Gulf of California
Tampa
Miami
Nassau
CUBA
Toronto
Buffalo
NEW YORK
Pittsburgh
New York
Boston
CONNECTICUT
VERMONT
NEW HAMPSHIRE
MAINE
Ottawa
Halifax
Washington
Norfolk
Raleigh
Hamilton
Sargasso Sea
zoom: 3.86
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

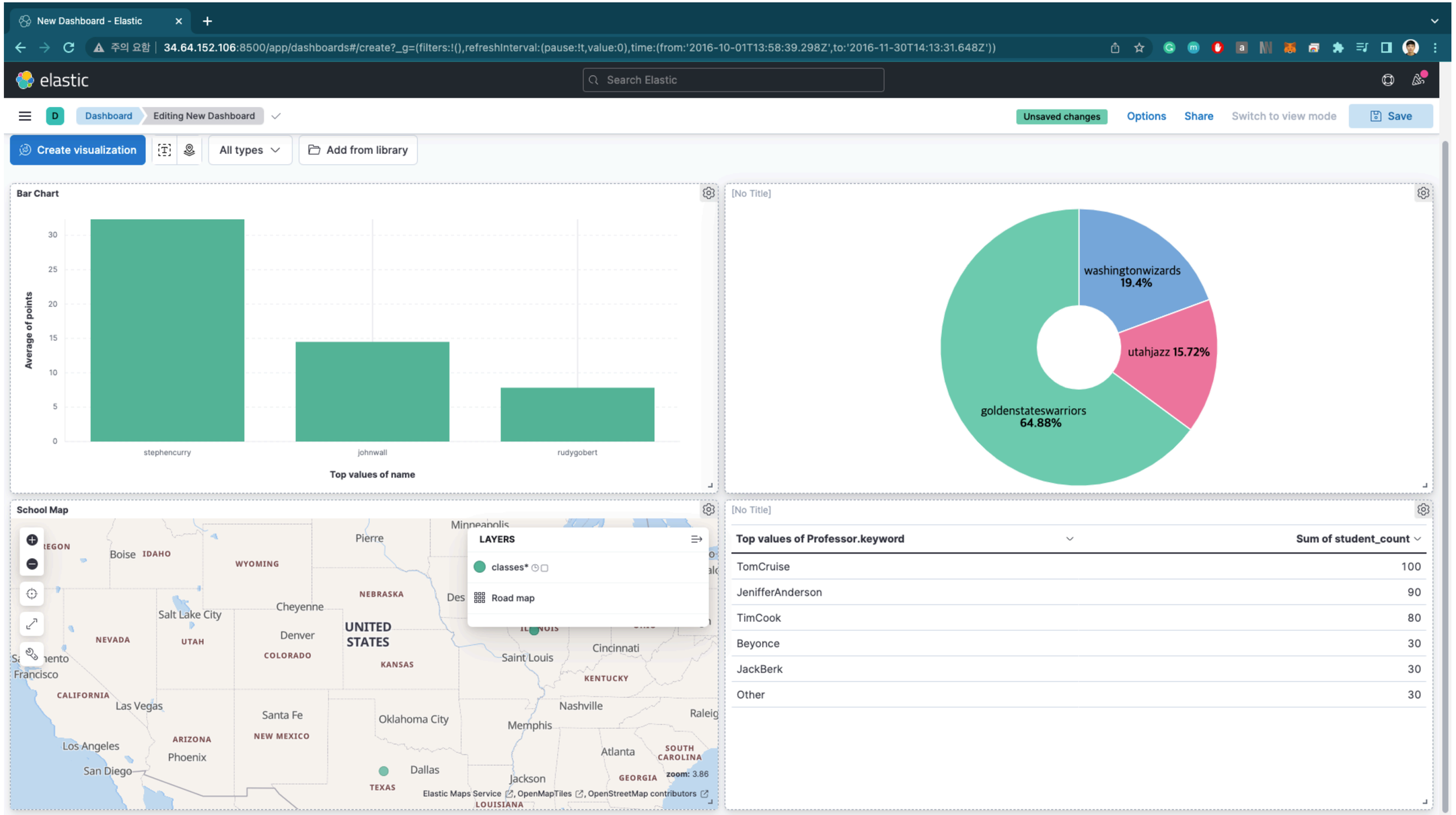
짜잔


New Dashboard - Elastic
34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
D
Dashboard
Editing New Dashboard
Unsaved changes
Options
Share
Switch to view mode
Save
Search
KQL
Oct 1, 2016 @ 22:58:39.29
Nov 30, 2016 @ 23:13:31.64
Refresh
+ Add filter
Create visualization
All types
Add from library
Bar Chart
Average of points
30
25
20
15
10
5
0
stephencurry
johnwall
rudygobert
Top values of name
[No Title]
washingtonwizards
19.4%
utahjazz 15.72%
goldenstateswarriors
64.88%
School Map
LAYERS
classes*
Road map
Minneapolis
Pierre
Boise
IDAHO
WYOMING
NEBRASKA
Cheyenne
Salt Lake City
Denver
UNITED
STATES
NEVADA
UTAH
COLORADO
KANSAS
Saint Louis
Cincinnati
KENTUCKY
CALIFORNIA
Las Vegas
Santa Fe
Oklahoma City
Nashville
Memphis

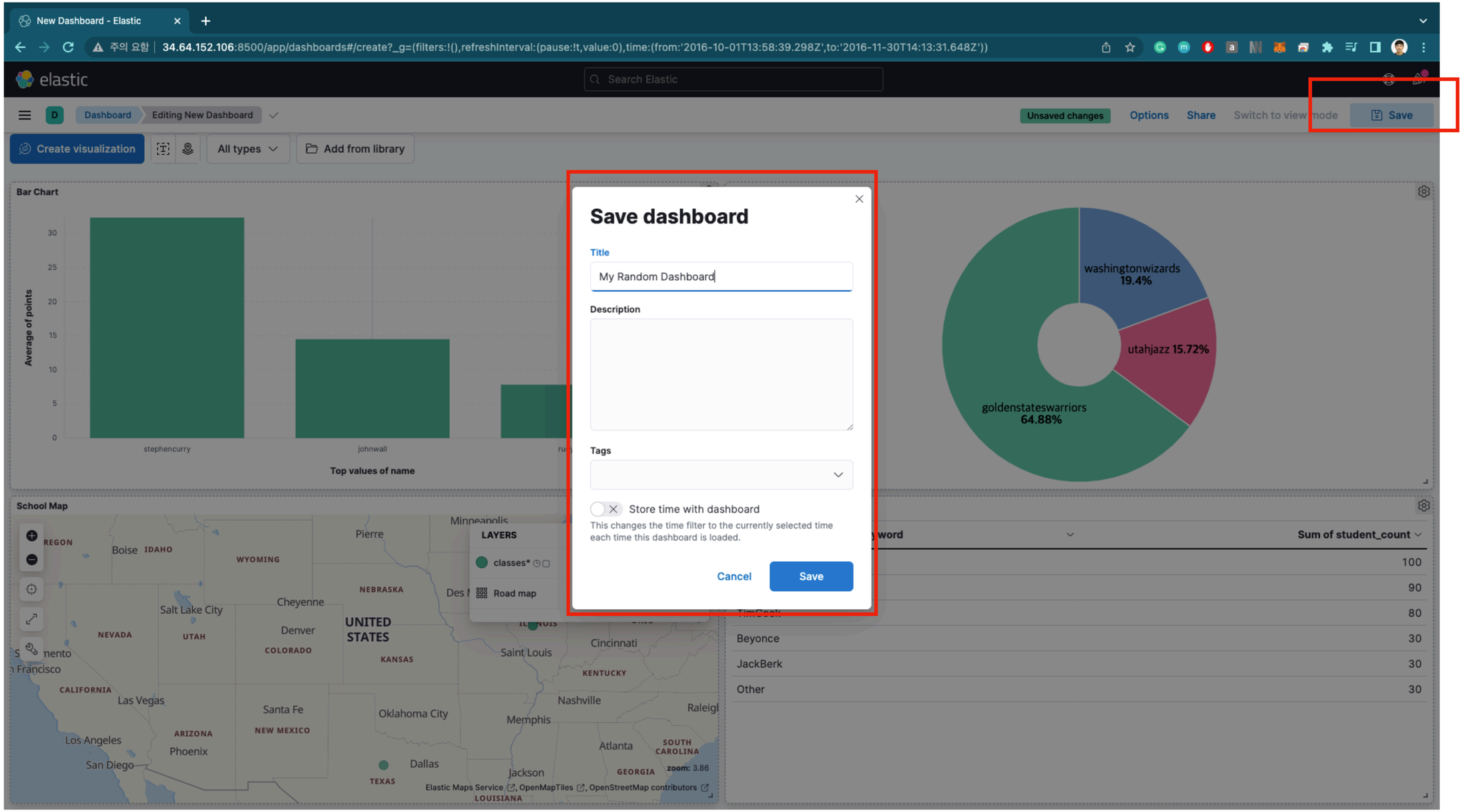
이번에는 테이블 형태의 시각화 추가



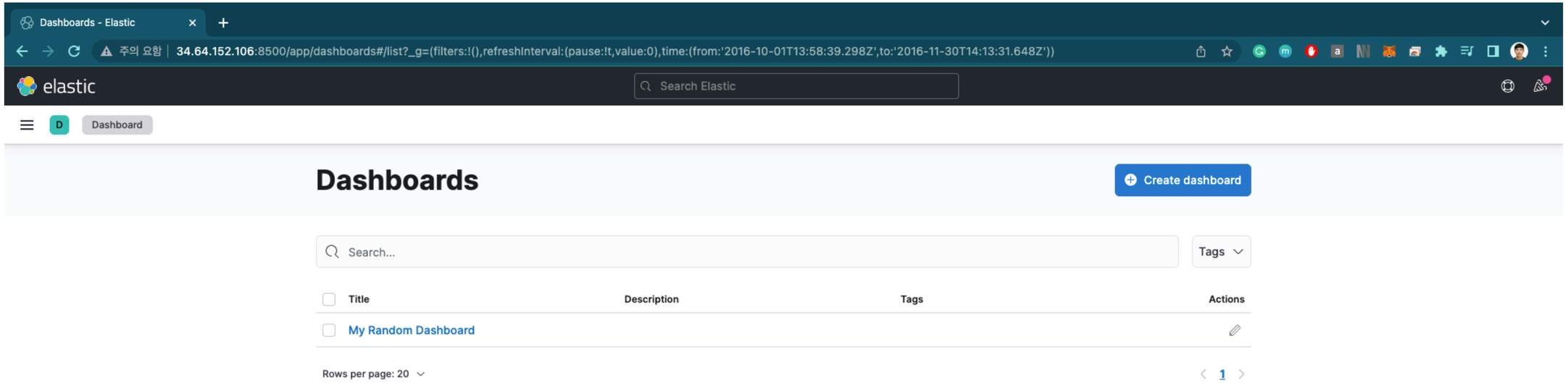
짜잔


New Dashboard - Elastic
34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Dashboard
Editing New Dashboard
Unsaved changes
Options
Share
Switch to view mode
Save
Create visualization
All types
Add from library
Bar Chart
Average of points
30
25
20
15
10
5
0
stephencurry
johnwall
rudygobert
Top values of name
[No Title]
washingtonwizards
19.4%
utahjazz 15.72%
goldenstateswarriors
64.88%
School Map
LAYERS
classes*
Road map
Minneapolis
Pierre
Boise
IDAHO
WYOMING
NEBRASKA
Cheyenne
Salt Lake City
NEVADA
UTAH
Denver
COLORADO
UNITED STATES
KANSAS
Saint Louis
Cincinnati
KENTUCKY
Nashville
Memphis
Raleig
Francisco
CALIFORNIA
Las Vegas
Santa Fe
NEW MEXICO
Oklahoma City
ARIZONA
Phoenix
Los Angeles
San Diego
Dallas
TEXAS
Atlanta
SOUTH CAROLINA
GEORGIA
Jackson
LOUISIANA
zoom: 3.86
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
[No Title]
Top values of Professor.keyword
Sum of student_count
TomCruise 100
JenifferAnderson 90
TimCook 80
Beyonce 30
JackBerk 30
Other 30

대쉬보드 저장!


New Dashboard - Elastic
34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
Dashboard
Editing New Dashboard
Unsaved changes
Options
Share
Switch to view mode
Save
Create visualization
All types
Add from library
Bar Chart
Average of points
stephencurry
johnwall
Top values of name
Save dashboard
Title
My Random Dashboard
Description
Tags
Store time with dashboard
This changes the time filter to the currently selected time each time this dashboard is loaded.
Cancel
Save
washingtonwizards 19.4%
utahjazz 15.72%
goldenstateswarriors 64.88%
School Map
LAYERS
classes*
Road map
Sum of student_count
100
90
80
Beyonce 30
JackBerk 30
Other 30
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

짜잔!

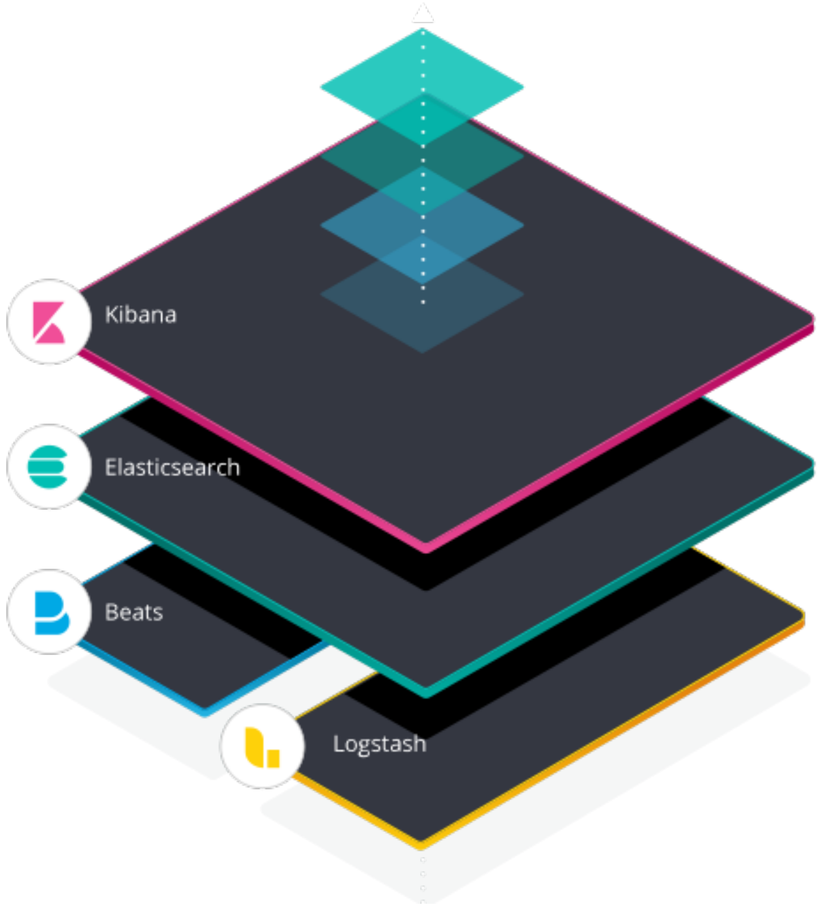

Dashboards - Elastic
주의 요함 | 34.64.152.106:8500/app/dashboards#/list?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))
elastic
Search Elastic
D
Dashboard
Dashboards
Create dashboard
Search...
Tags
Title
Description
Tags
Actions
My Random Dashboard
Rows per page: 20
1

LOGSTASH

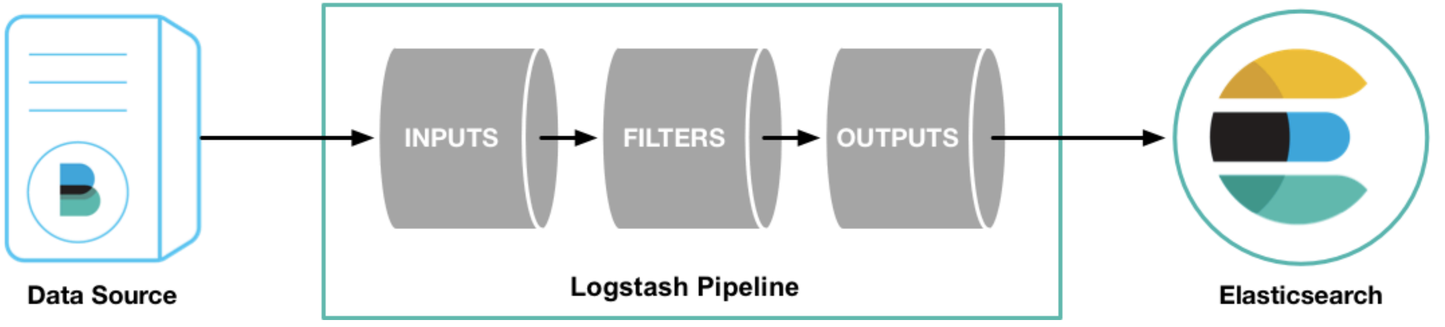
ELK Stack

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!

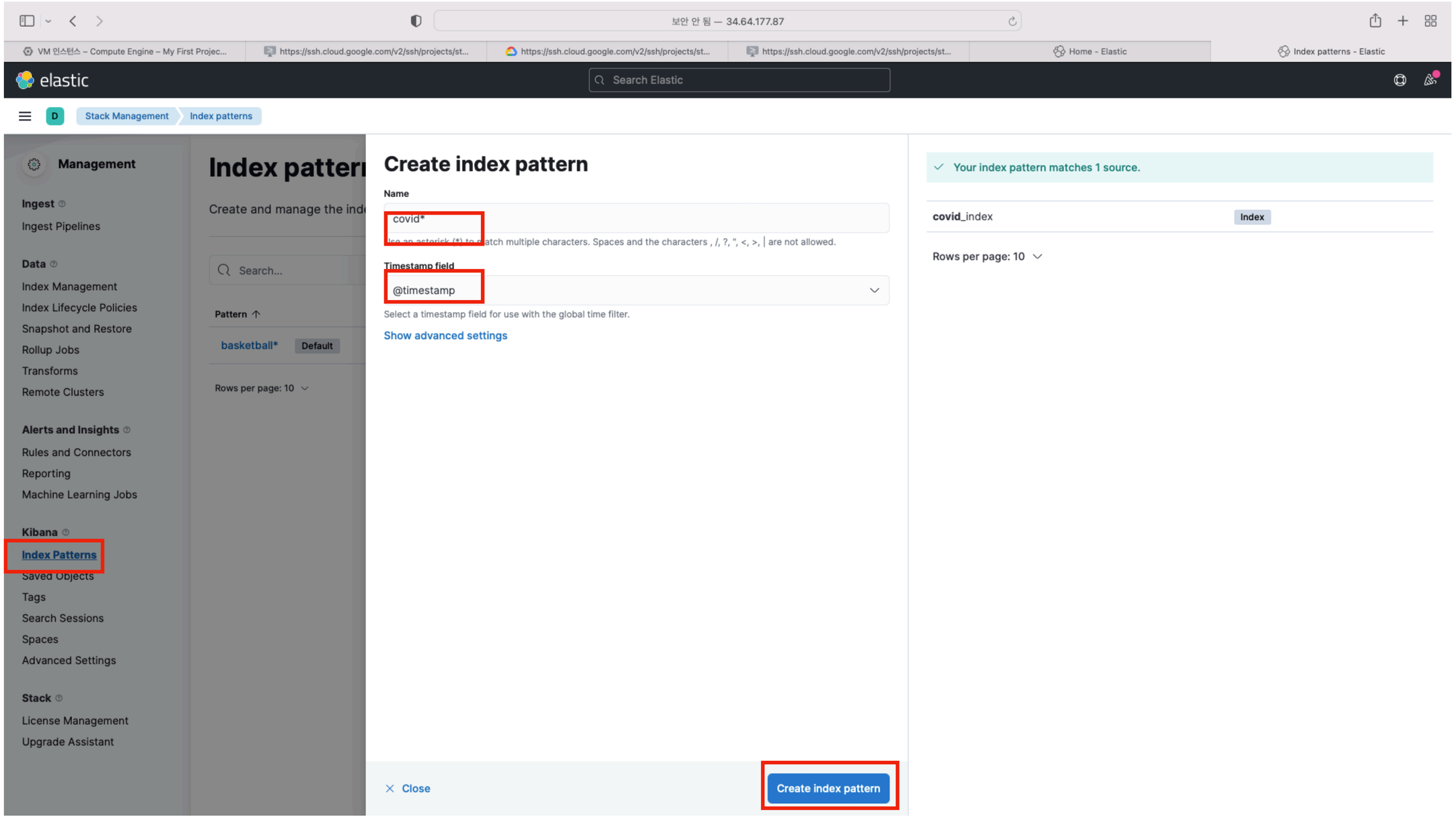


https://www.elastic.co/kr/what-is/elk-stack

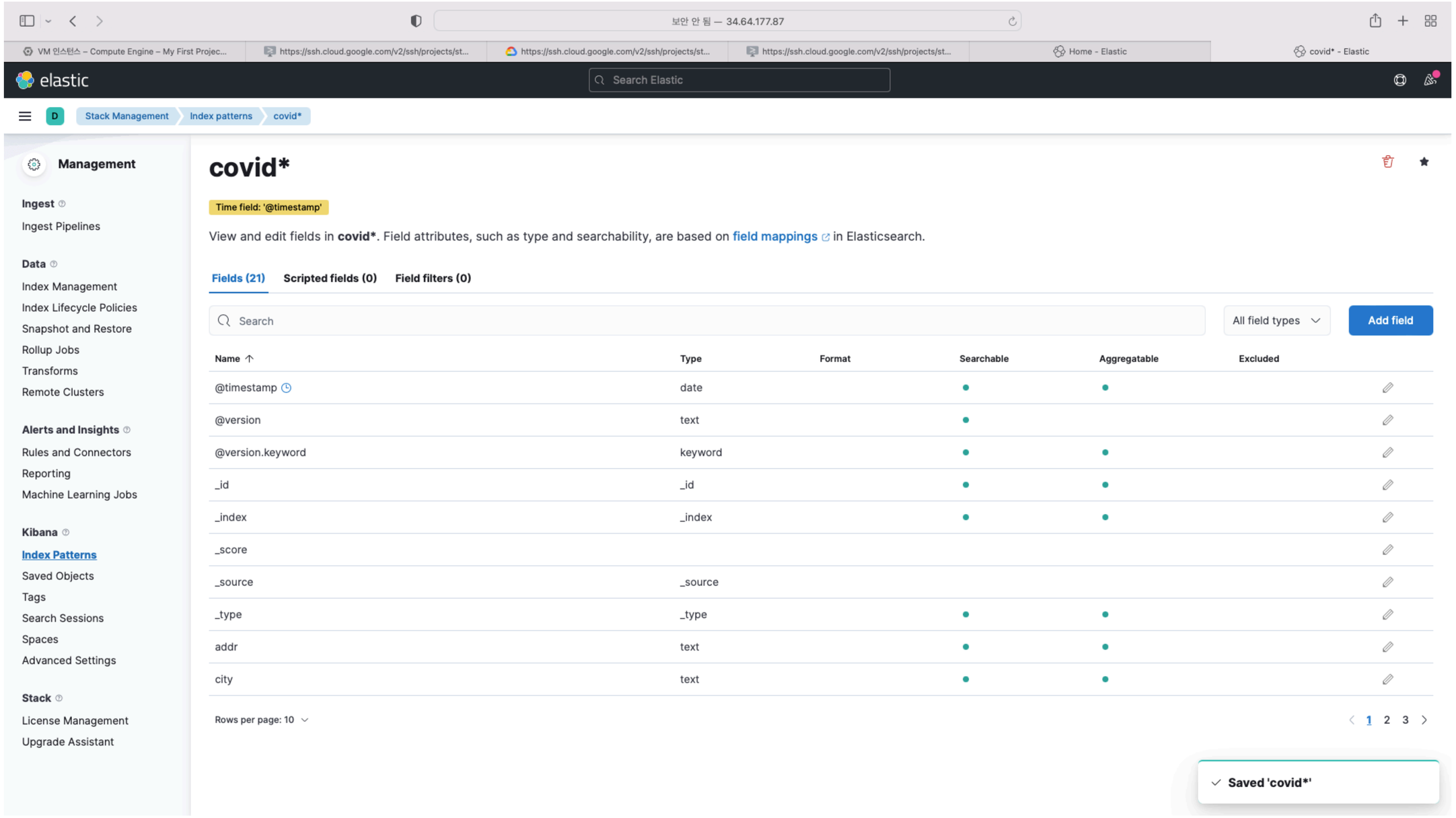


https://www.elastic.co/guide/en/logstash/current/first-event.html

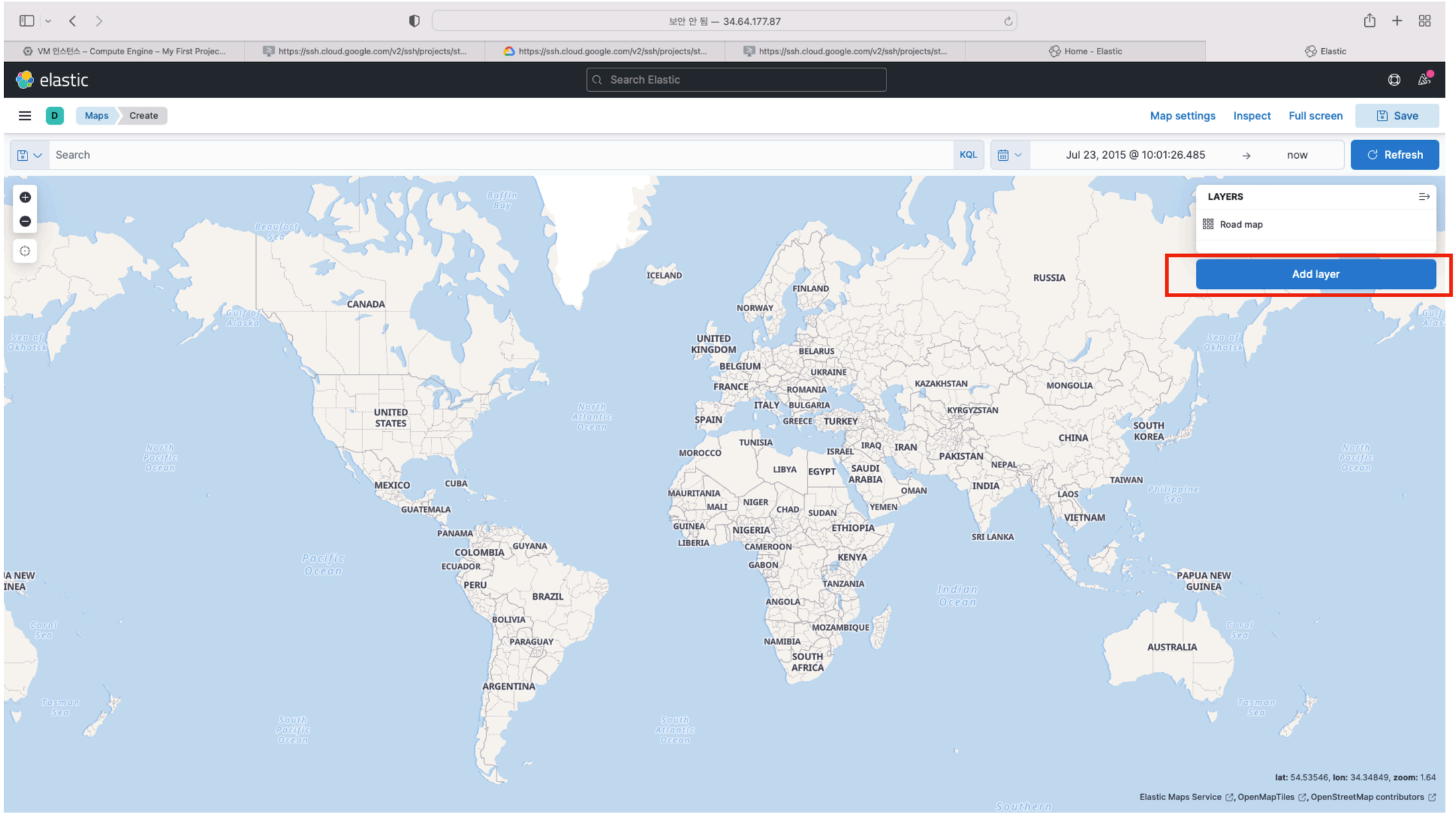
Covid 인덱스 추가


보안 안 됨 — 34.64.177.87
VM 인스턴스 – Compute Engine – My First Projec...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
Home - Elastic
Index patterns - Elastic
elastic
Search Elastic
D
Stack Management
Index patterns
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
Index patter
Create and manage the ind
Search...
Pattern
basketball*
Default
Rows per page: 10
Create index pattern
Name
covid*
Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.
Timestamp field
@timestamp
Select a timestamp field for use with the global time filter.
Show advanced settings
Close
Create index pattern
Your index pattern matches 1 source.
covid_index
Index
Rows per page: 10

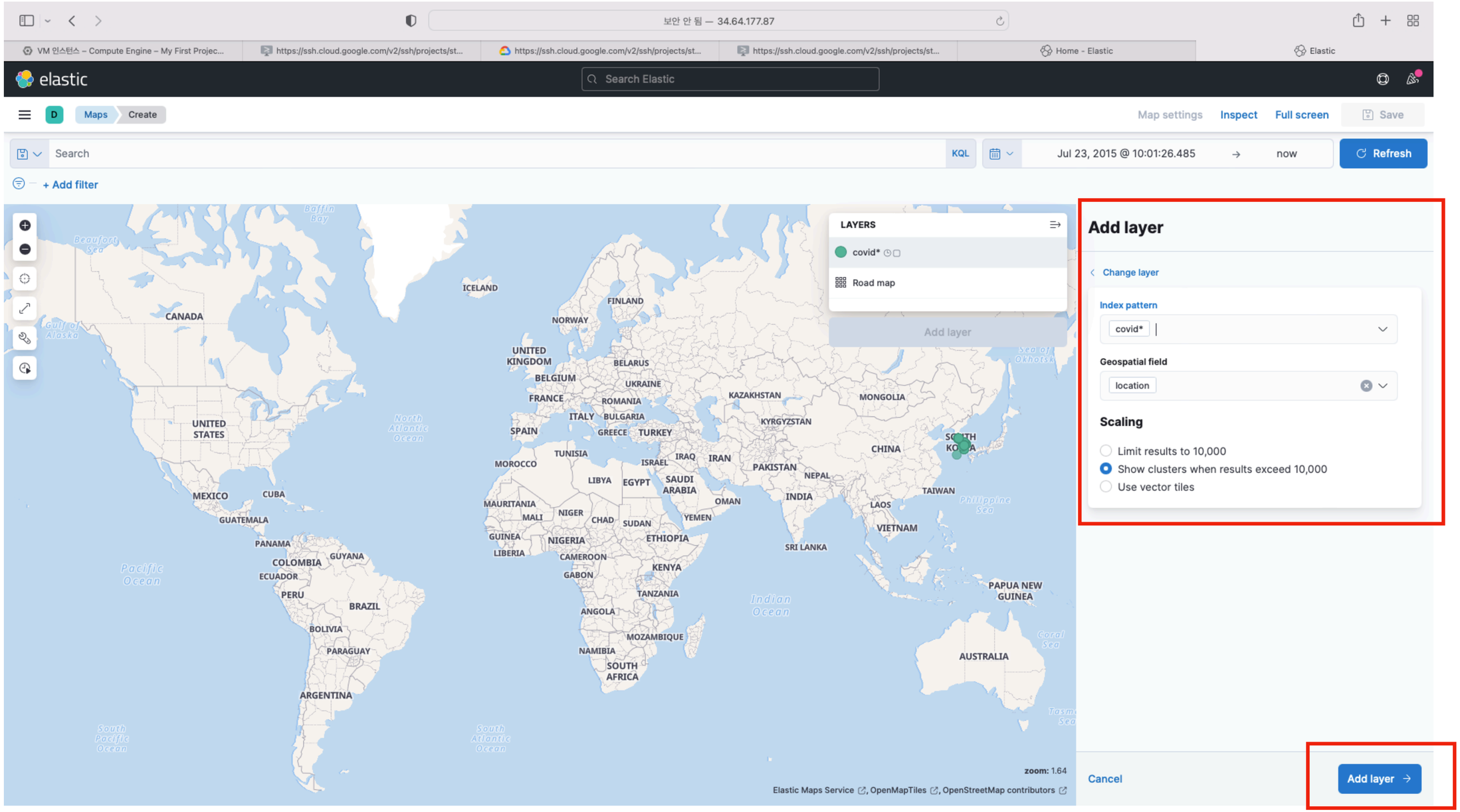
필드 확인


보안 안 됨 — 34.64.177.87
VM 인스턴스 – Compute Engine – My First Projec...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
Home - Elastic
covid* - Elastic
elastic
Search Elastic
D
Stack Management
Index patterns
covid*
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
covid*
Time field: '@timestamp'
View and edit fields in covid*. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (21)
Scripted fields (0)
Field filters (0)
Search
All field types
Add field
Name
Type
Format
Searchable
Aggregatable
Excluded
@timestamp
date
@version
text
@version.keyword
keyword
_id
_id
_index
_index
_score
_source
_source
_type
_type
addr
text
city
text
Rows per page: 10
1
2
3
Saved 'covid*'

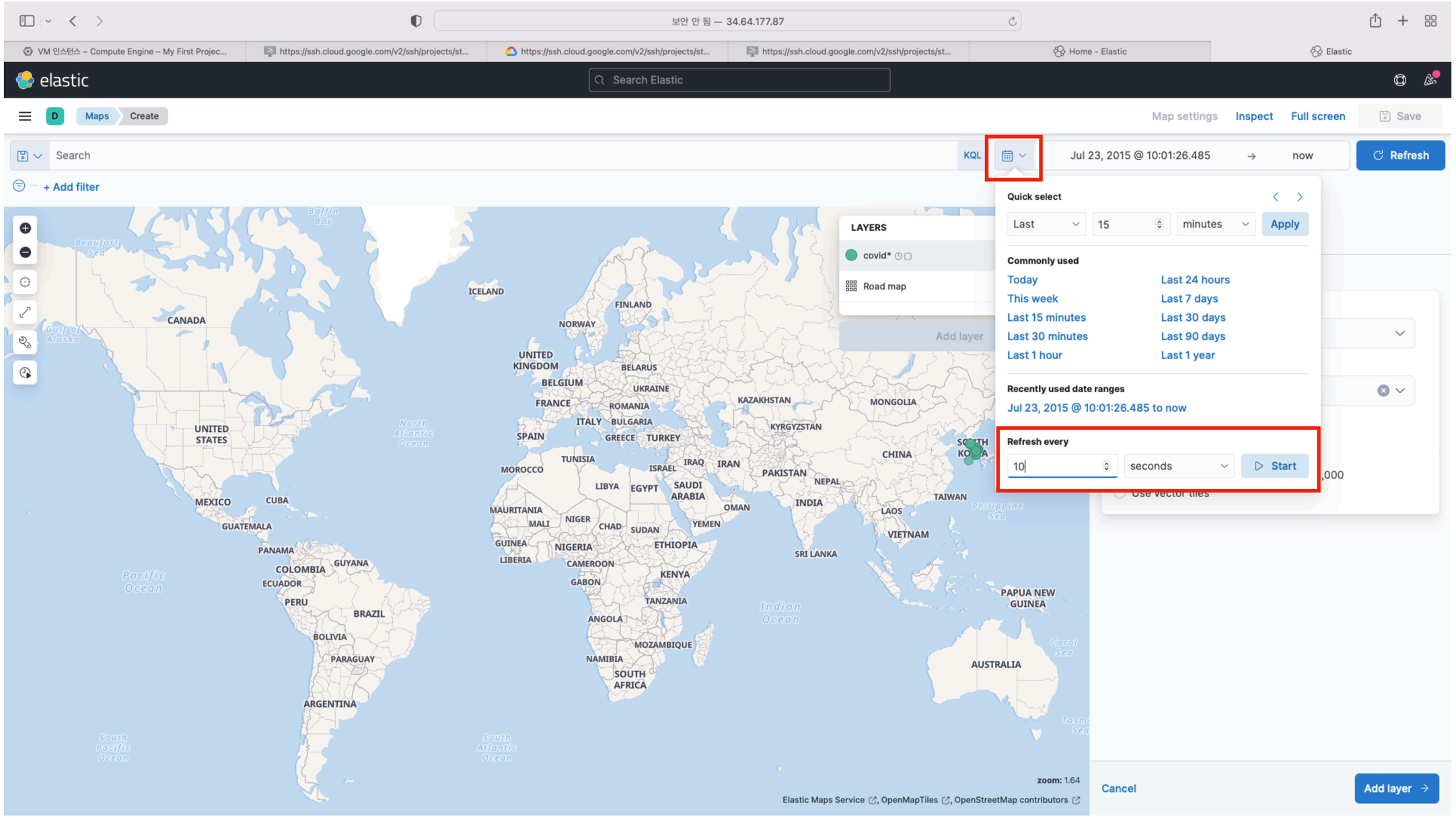
지도로 다시 이동


elastic
Search Elastic
D
Maps
Create
Map settings
Inspect
Full screen
Save
Search
KQL
Jul 23, 2015 @ 10:01:26.485
now
Refresh
LAYERS
Road map
Add layer
lat: 54.53546, lon: 34.34849, zoom: 1.64
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

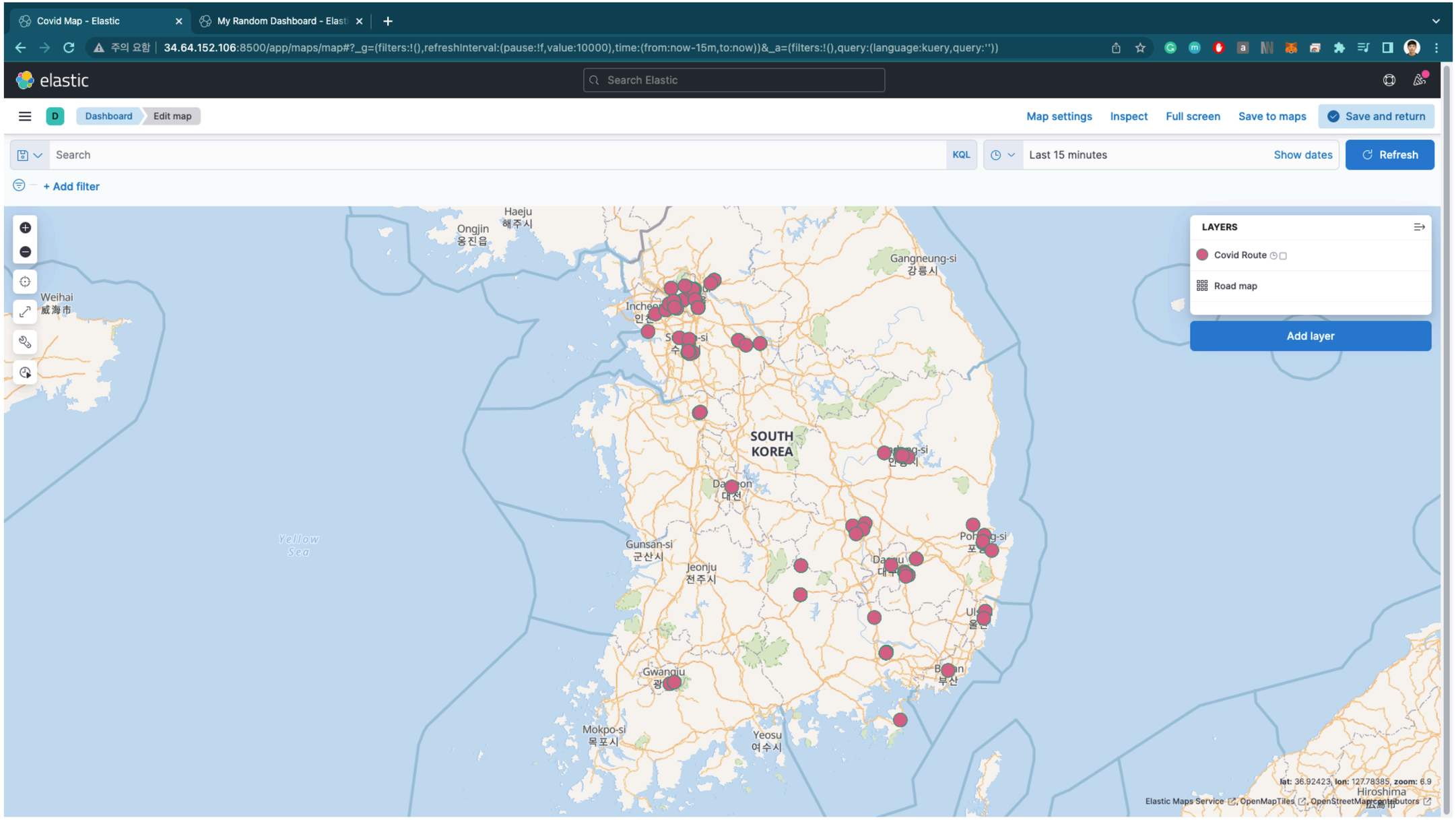
Covid 인덱스로 추가



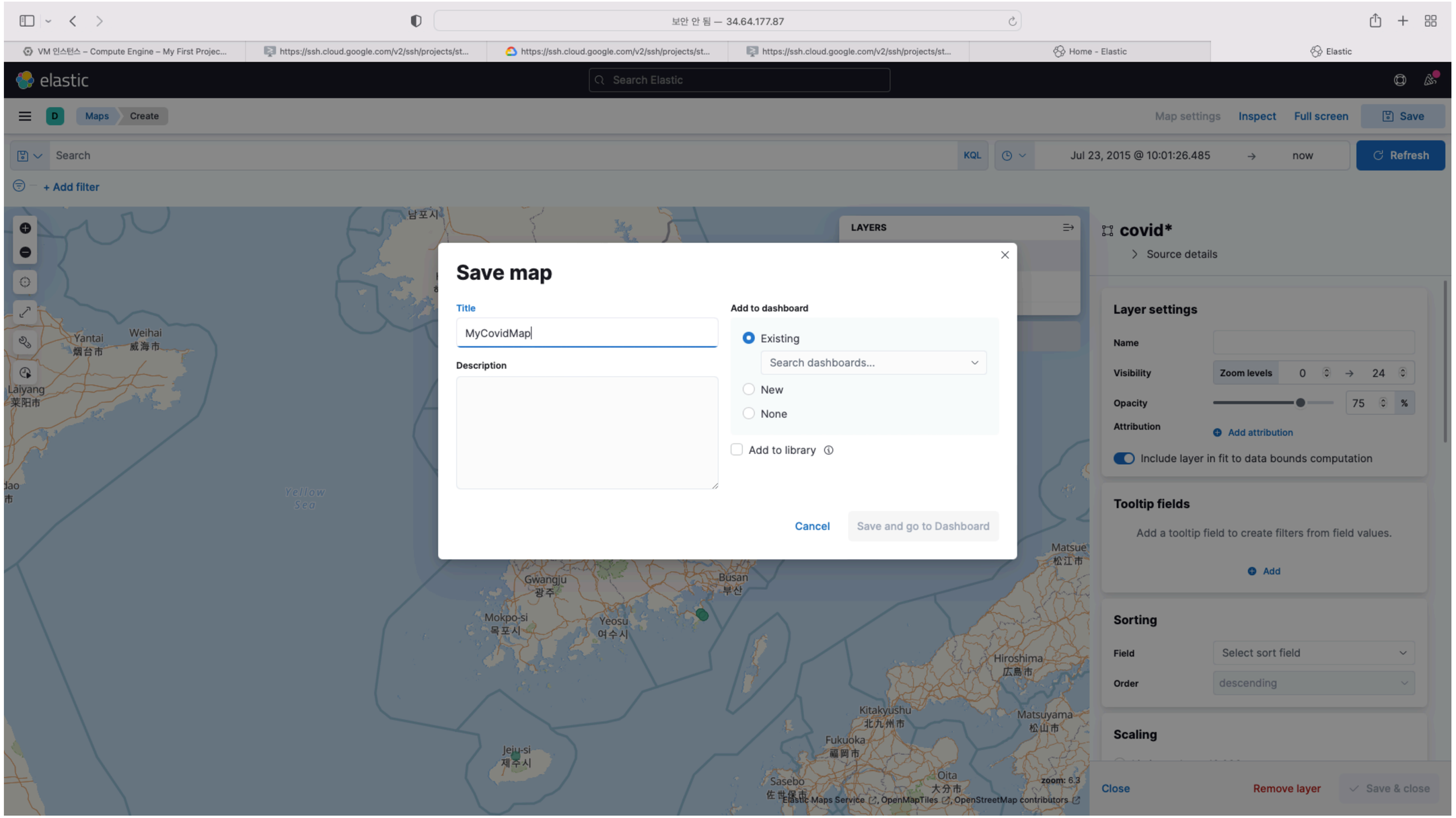
Refresh Every 10 seconds



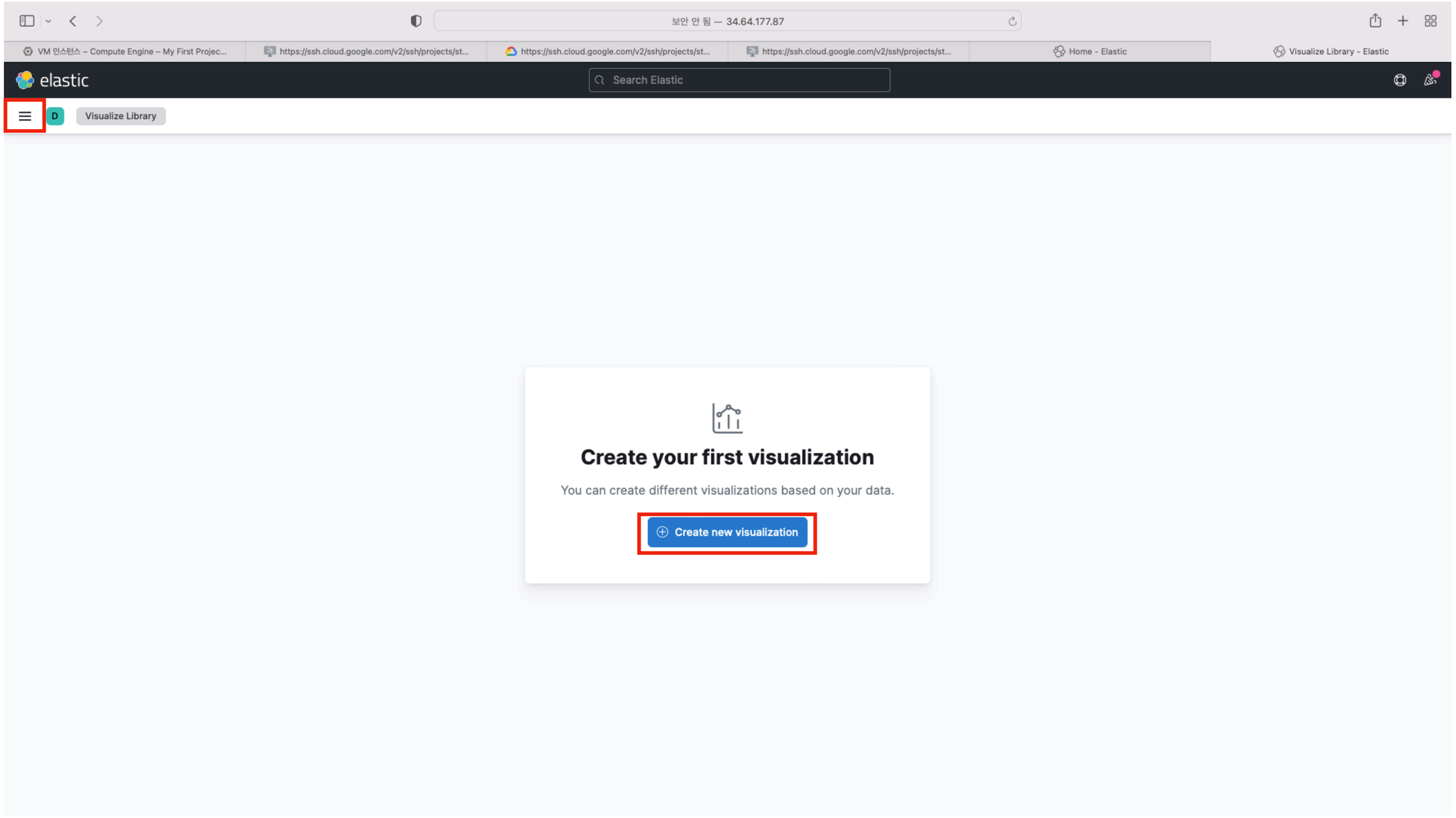
감상


Covid Map - Elastic
My Random Dashboard - Elasti
주의 요함 | 34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!f,value:10000),time:(from:now-15m,to:now))&_a=(filters:!(),query:(language:kuery,query:''))
elastic
Search Elastic
D
Dashboard
Edit map
Map settings
Inspect
Full screen
Save to maps
Save and return
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
LAYERS
Covid Route
Road map
Add layer
SOUTH KOREA
Haeju
해주시
Ongjin
옹진읍
Weihai
威海市
Yellow Sea
Gangneung-si
강릉시
Gunsan-si
군산시
Jeonju
전주시
Gwangju
광주
Mokpo-si
목포시
Yeosu
여수시
Hiroshima
lat: 36.92423, lon: 127.78385, zoom: 6.9
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

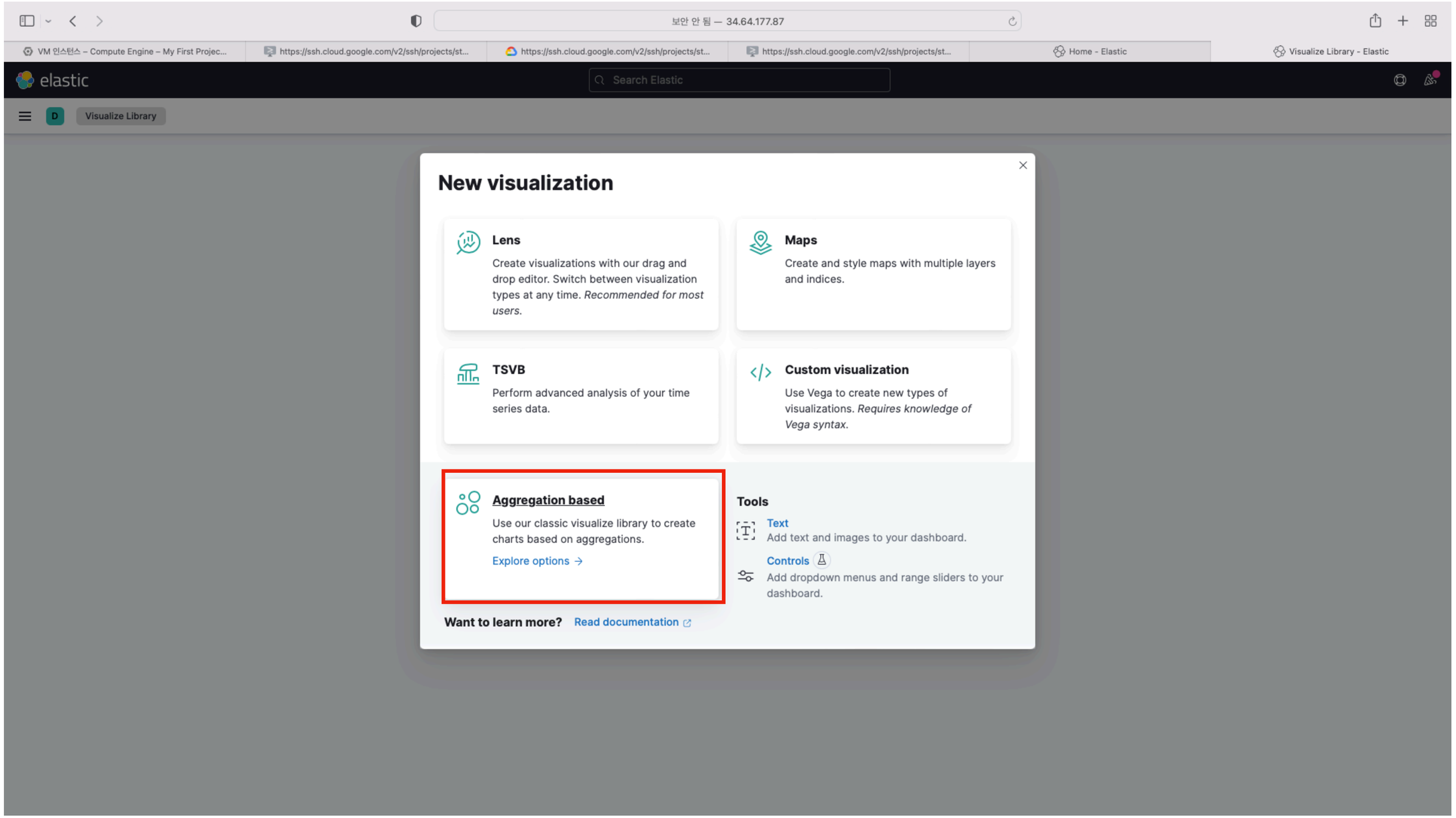
대쉬보드에 저장


보안 안 됨 — 34.64.177.87
VM 인스턴스 – Compute Engine – My First Projec...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
Home - Elastic
Elastic
elastic
Search Elastic
D
Maps
Create
Map settings
Inspect
Full screen
Save
Search
KQL
Jul 23, 2015 @ 10:01:26.485
now
Refresh
+ Add filter
LAYERS
covid*
Source details
Save map
Title
MyCovidMap
Description
Add to dashboard
Existing
Search dashboards...
New
None
Add to library
Cancel
Save and go to Dashboard
Layer settings
Name
Visibility
Zoom levels
0
24
Opacity
75
%
Attribution
Add attribution
Include layer in fit to data bounds computation
Tooltip fields
Add a tooltip field to create filters from field values.
Add
Sorting
Field
Select sort field
Order
descending
Scaling
Close
Remove layer
Save & close
Yantai
烟台市
Weihai
威海市
Laiyang
莱阳市
Yellow Sea
Gwangju
광주
Busan
부산
Mokpo-si
목포시
Yeosu
여수시
Jeju-si
제주시
Matsue
松江市
Hiroshima
広島市
Kitakyushu
北九州市
Matsuyama
松山市
Fukuoka
福岡市
Sasebo
佐世保市
Oita
大分市
zoom: 6.3
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

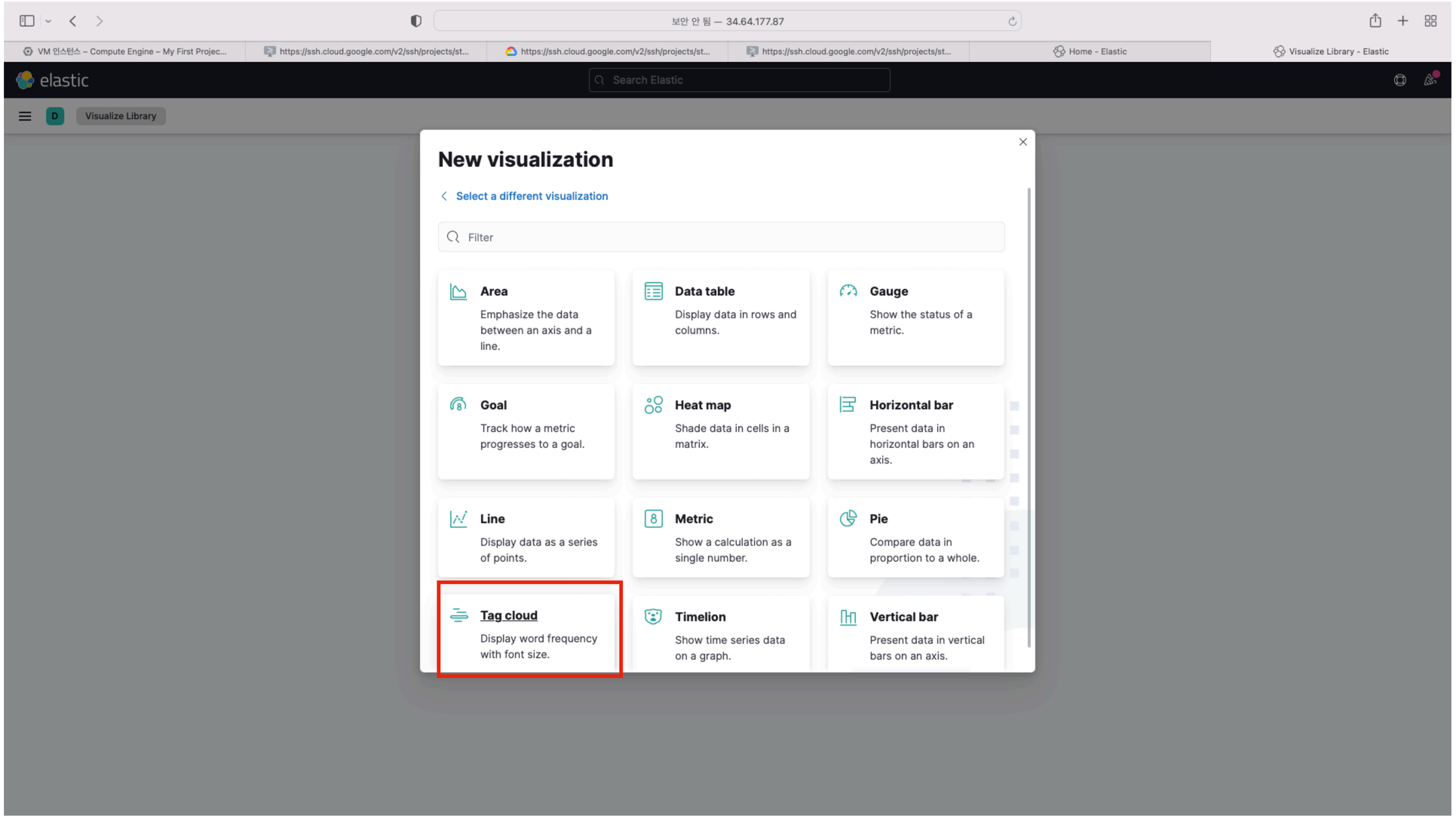
Visualize Library로 다시 이동



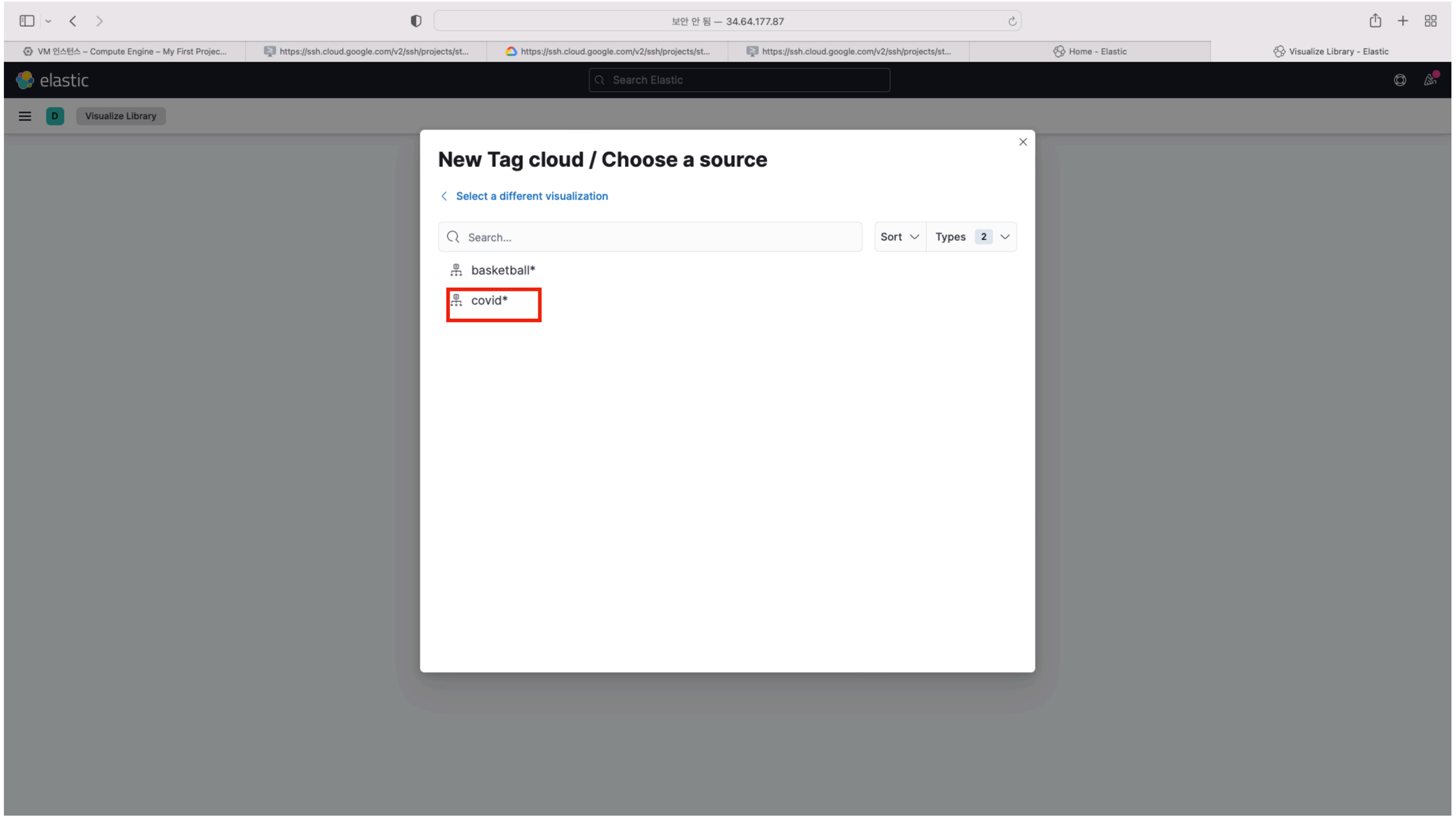
Aggregation based 선택



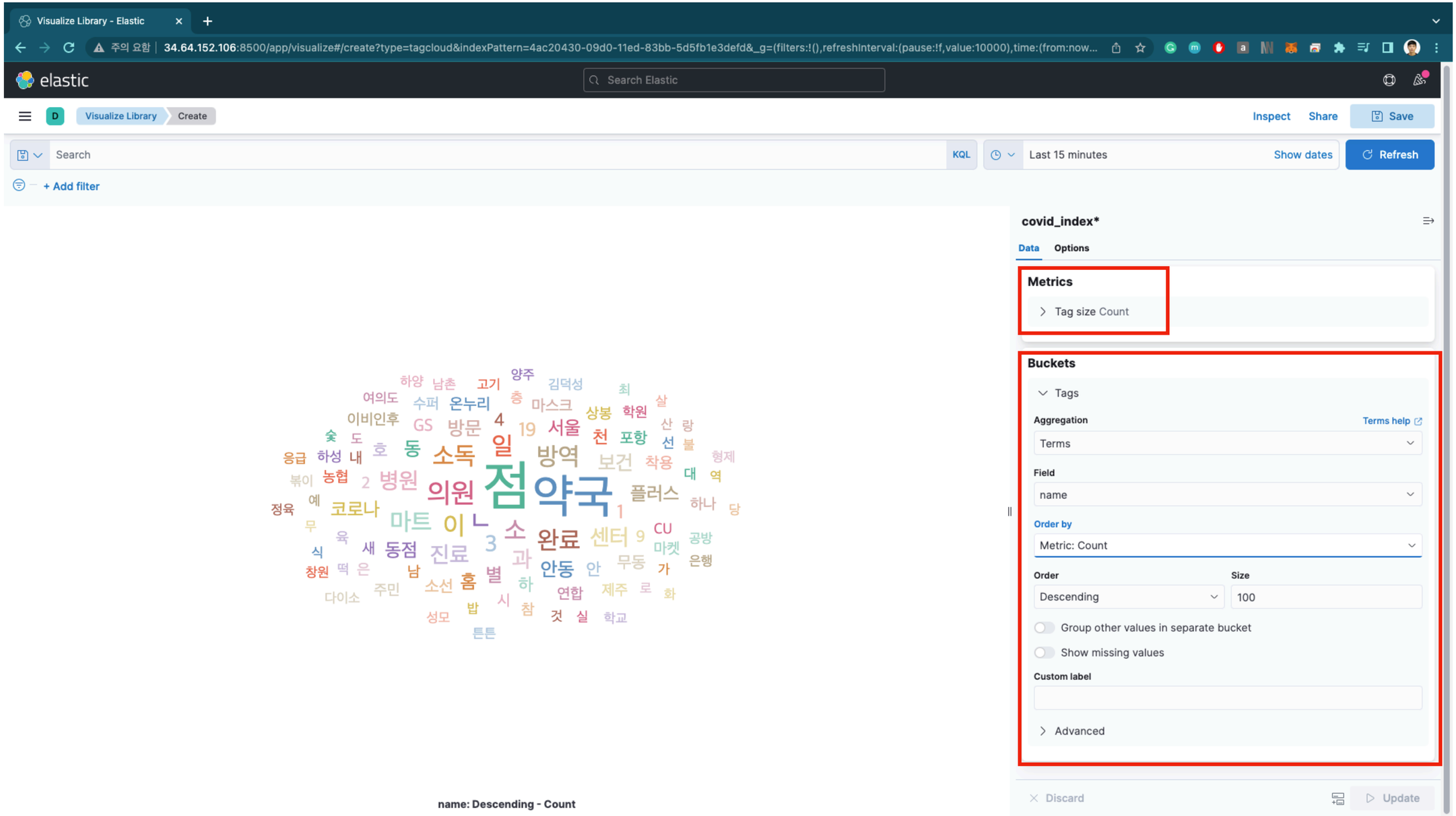
Tag cloud 선택


보안 안 됨 — 34.64.177.87
VM 인스턴스 – Compute Engine – My First Projec...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
Home - Elastic
Visualize Library - Elastic
elastic
Search Elastic
D
Visualize Library
New visualization
Select a different visualization
Filter
Area
Emphasize the data between an axis and a line.
Data table
Display data in rows and columns.
Gauge
Show the status of a metric.
Goal
Track how a metric progresses to a goal.
Heat map
Shade data in cells in a matrix.
Horizontal bar
Present data in horizontal bars on an axis.
Line
Display data as a series of points.
Metric
Show a calculation as a single number.
Pie
Compare data in proportion to a whole.
Tag cloud
Display word frequency with font size.
Timelion
Show time series data on a graph.
Vertical bar
Present data in vertical bars on an axis.

Covid 선택


보안 안 됨 — 34.64.177.87
VM 인스턴스 – Compute Engine – My First Projec...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
https://ssh.cloud.google.com/v2/ssh/projects/st...
Home - Elastic
Visualize Library - Elastic
elastic
Search Elastic
D
Visualize Library
New Tag cloud / Choose a source
Select a different visualization
Search...
Sort
Types 2
basketball*
covid*

오른쪽과 같이 옵션설정!


Visualize Library - Elastic
34.64.152.106:8500/app/visualize#/create?type=tagcloud&indexPattern=4ac20430-09d0-11ed-83bb-5d5fb1e3defd&_g=(filters:!(),refreshInterval:(pause:!f,value:10000),time:(from:now...
elastic
Search Elastic
D
Visualize Library
Create
Inspect
Share
Save
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
name: Descending - Count
covid_index*
Data
Options
Metrics
Tag size Count
Buckets
Tags
Aggregation
Terms help
Terms
Field
name
Order by
Metric: Count
Order
Descending
Size
100
Group other values in separate bucket
Show missing values
Custom label
Advanced
Discard
Update

E.O.D