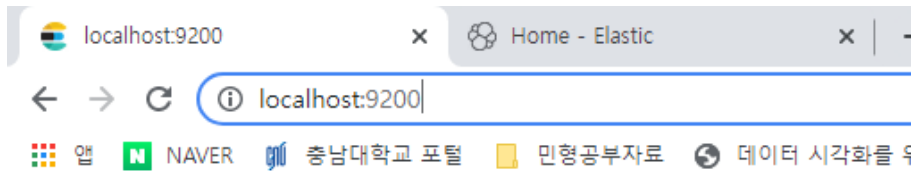


# Grafana와 ElasticSearch 연동하기

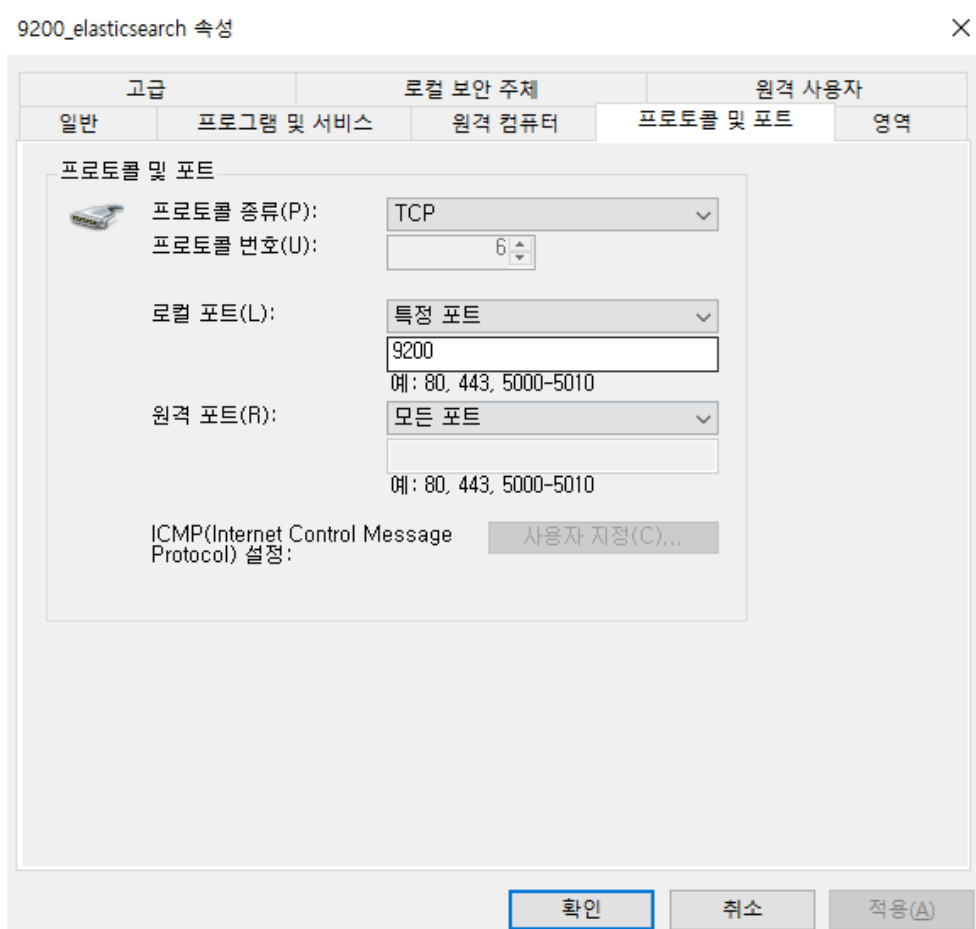
1.local에 깔려있는 ElasticSearch 포트(9200)의 방화벽을 뚫어준다.

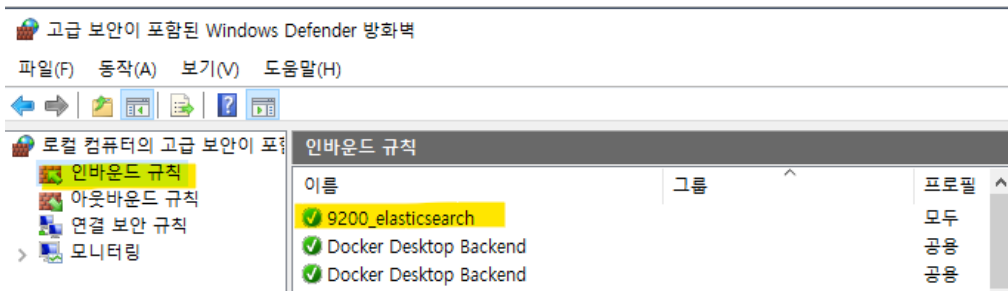
ElasticSearch 포트가 9200번이다.



```
{
  "name" : "DESKTOP-G9DVJ1H",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "S-HBUR16Rwiq719k5rVljw",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

방화벽 뚫는 방법 : <https://wiki.mcneel.com/ko/zoo/window7firewall>





2.cmd창에서 localhost에 해당되는 ip 주소를 얻어온다.

cmd창에 `ipconfig`를 치면 값이 나온다.

```
C:\Users\MongTa>ipconfig
```

명령 프롬프트

```

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

무선 LAN 어댑터 로컬 영역 연결* 10:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

무선 LAN 어댑터 Wi-Fi:

연결별 DNS 접미사 . . . . . :
링크-로컬 IPv6 주소 . . . . . : fe80::cc60:bbed:c2a9:3f40%11
IPv4 주소 . . . . . : 172.30.1.92
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . : 172.30.1.254

이더넷 어댑터 Bluetooth 네트워크 연결:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

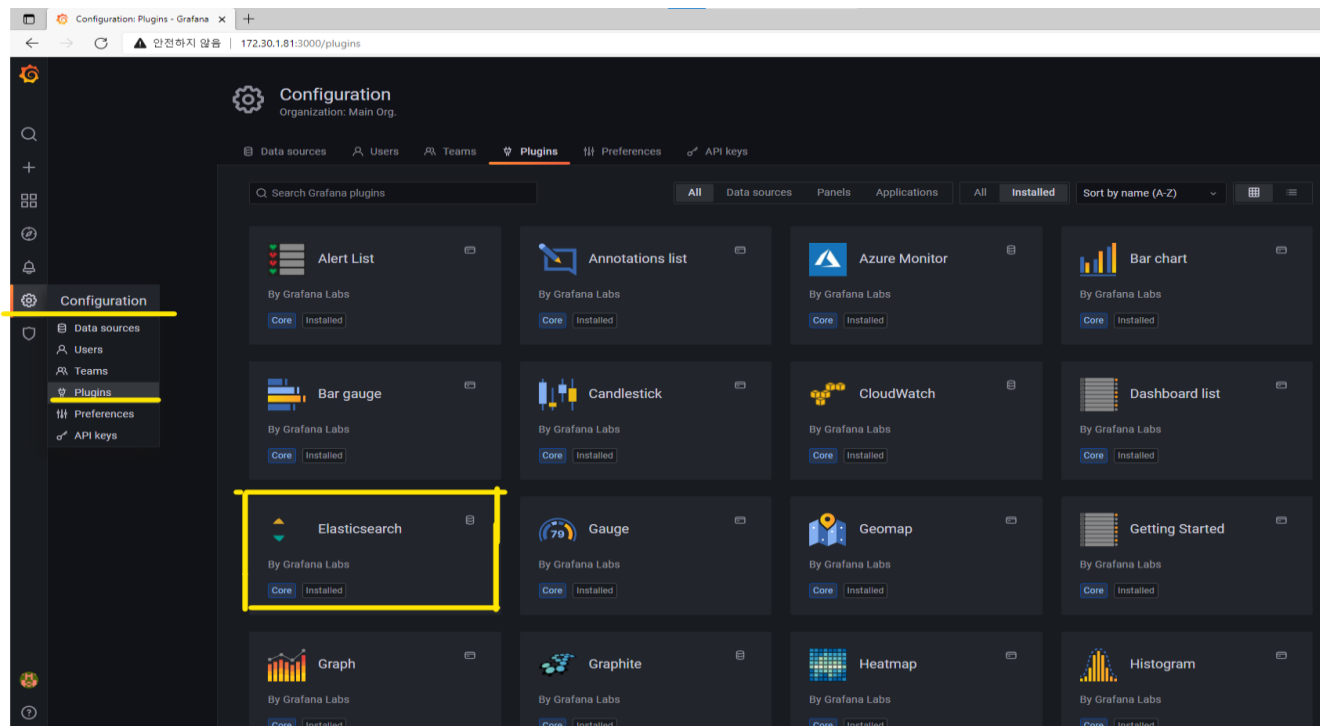
C:\Users\MongTa>

```

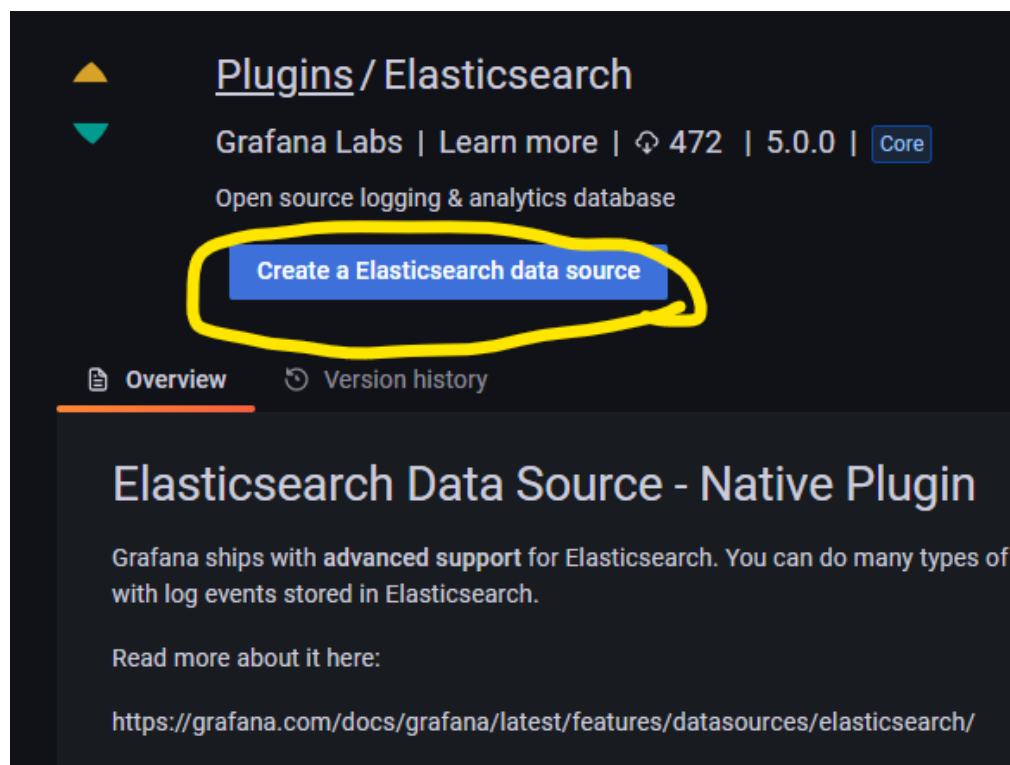
맨 밑의 무선 LAN 어댑터 Wi-Fi의 기본 게이트웨이가 localhost에 해당되는 ip주소이다.

나는 172.30.1.92임을 알 수 있다.

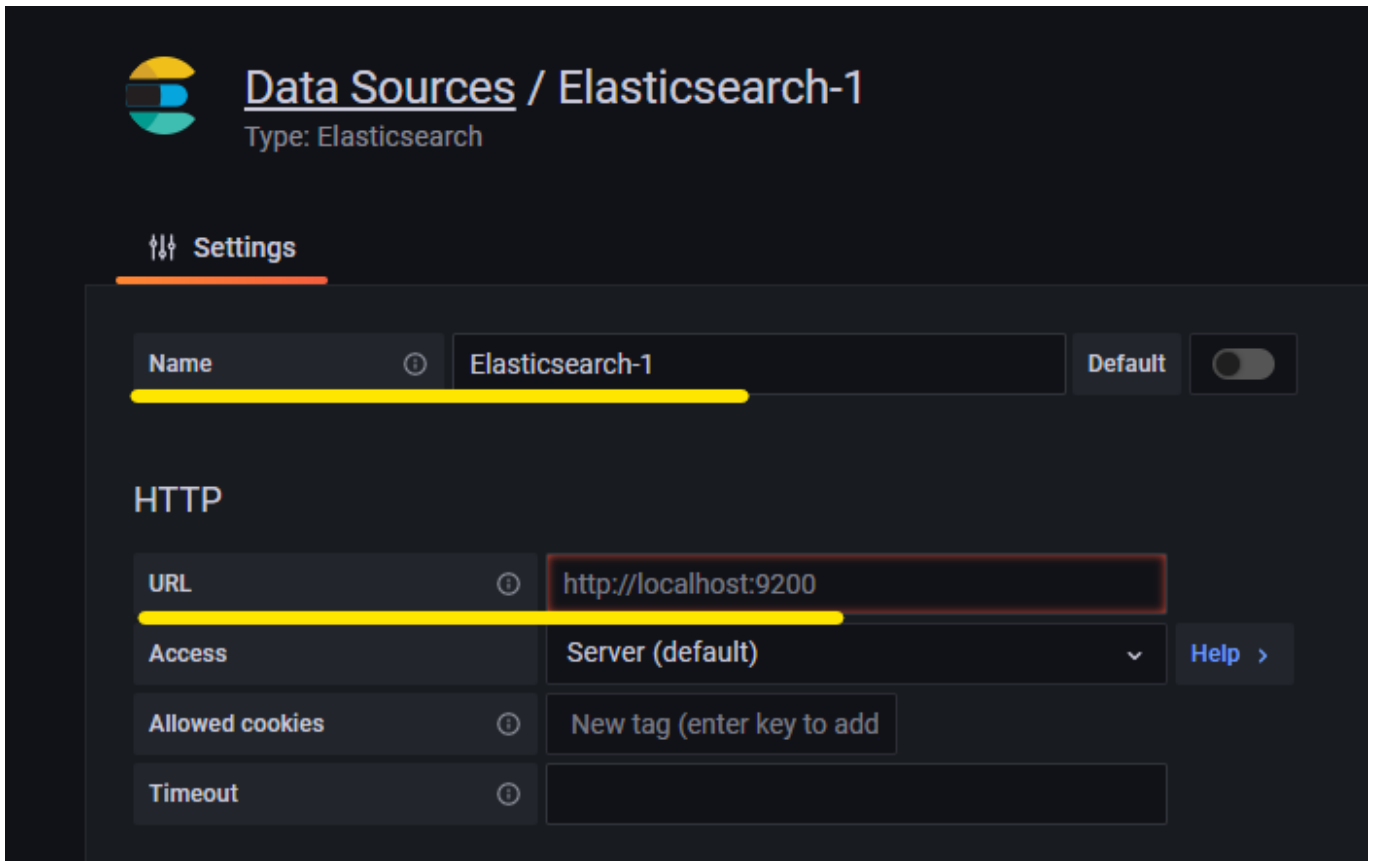
3.Grafana에서 해당되는 부분에 들어간다.



4.Create a Elasticsearch data source를 클릭한다.



5.Name과 URL을 바꾸어준다.



**Data Sources / Elasticsearch-1**  
Type: Elasticsearch

**Settings**

**Name** ⓘ Elasticsearch-1 **Default** ☐

**HTTP**

**URL** ⓘ http://localhost:9200

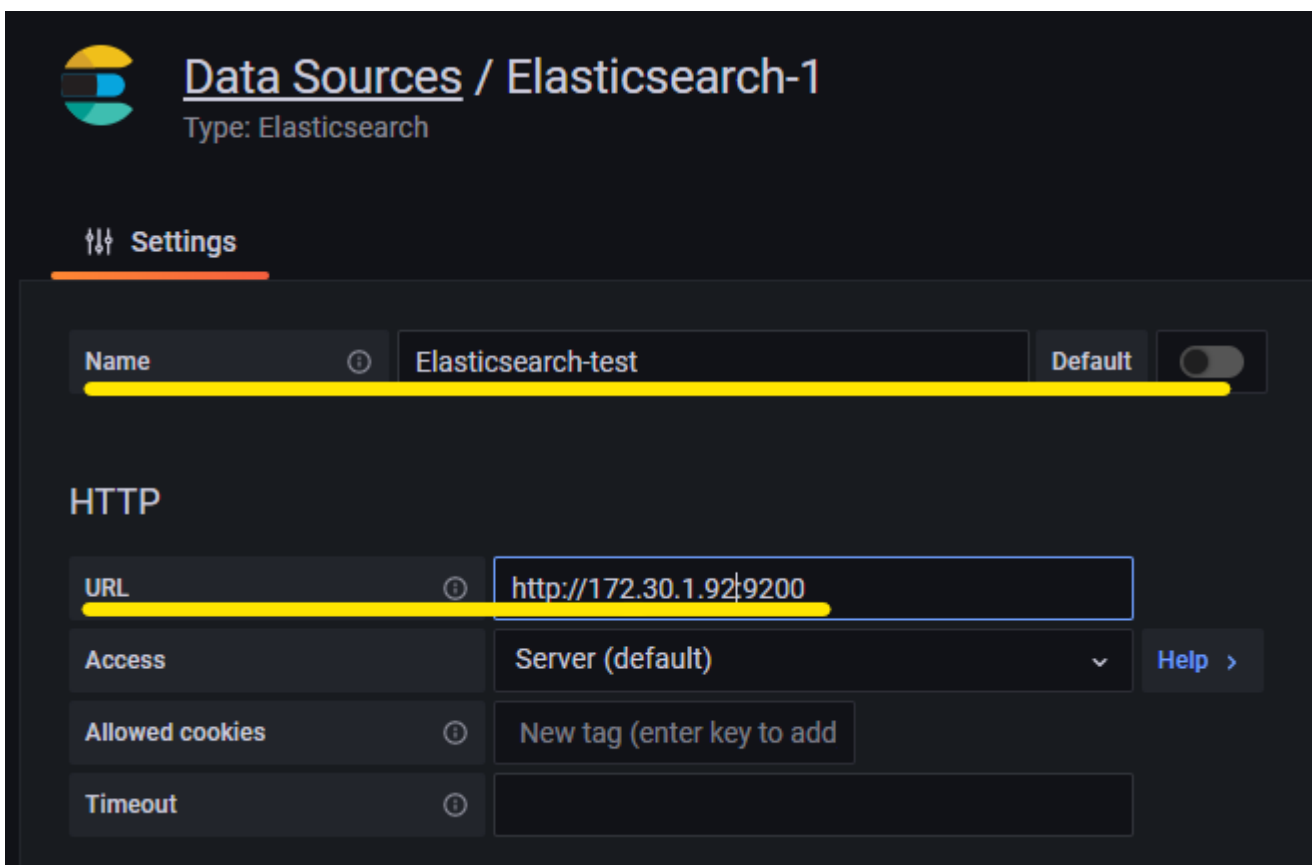
**Access** Server (default) **Help** >

**Allowed cookies** ⓘ New tag (enter key to add)

**Timeout** ⓘ

Name은 자신이 원하는 값으로 변경하면 되며,

URL은 "http://172.30.1.92:9200"으로 바꾸어 준다. (2참고)



**Data Sources / Elasticsearch-1**  
Type: Elasticsearch

**Settings**

**Name** ⓘ Elasticsearch-test **Default** ☐

**HTTP**

**URL** ⓘ http://172.30.1.92:9200

**Access** Server (default) **Help** >

**Allowed cookies** ⓘ New tag (enter key to add)

**Timeout** ⓘ

6.Index name과 Version을 바꾸어준다.

### Elasticsearch details

Index name	kmh_test4	Pattern	No pattern ▾
Time field name	@timestamp		
Version	7.10+ ▾		
Max concurrent Shard Requests	5		
Min time interval ⓘ	10s		
X-Pack enabled	<input type="checkbox"/>		

Stack Management

Saved objects

Management

Ingest ⓘ  
Ingest Node 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

## Saved Objects

Manage and share your saved objects.

Search...

<input type="checkbox"/>	Type	Title
<input type="checkbox"/>	...	Advanced Settings [7.15.2]
<input type="checkbox"/>	tag	tag
<input type="checkbox"/>	kmh_test1	kmh_test1
<input type="checkbox"/>	kmh_test4	kmh_test4
<input type="checkbox"/>	map	map
<input type="checkbox"/>	kmh_test*	kmh_test*
<input type="checkbox"/>	index patterns	newsletter*
<input type="checkbox"/>	kmh_test4*	kmh_test4*
<input type="checkbox"/>	my_shape*	my_shape*
<input type="checkbox"/>	kmh_test4_discover	kmh_test4_discover
<input type="checkbox"/>	kmh_test_version	kmh_test_version

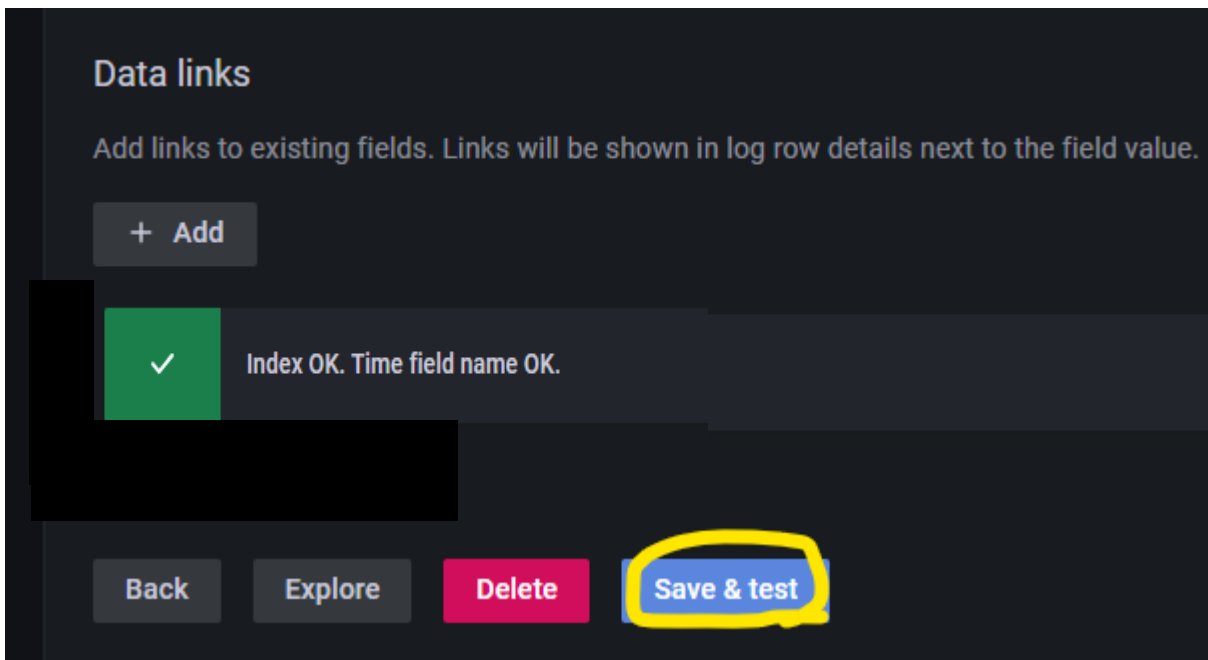
Index name은 Index patterns로 바꾸어 주며,

Version은 내가 설치한 elasticsearch 버전에 맞게 바꾸어 주면 된다.

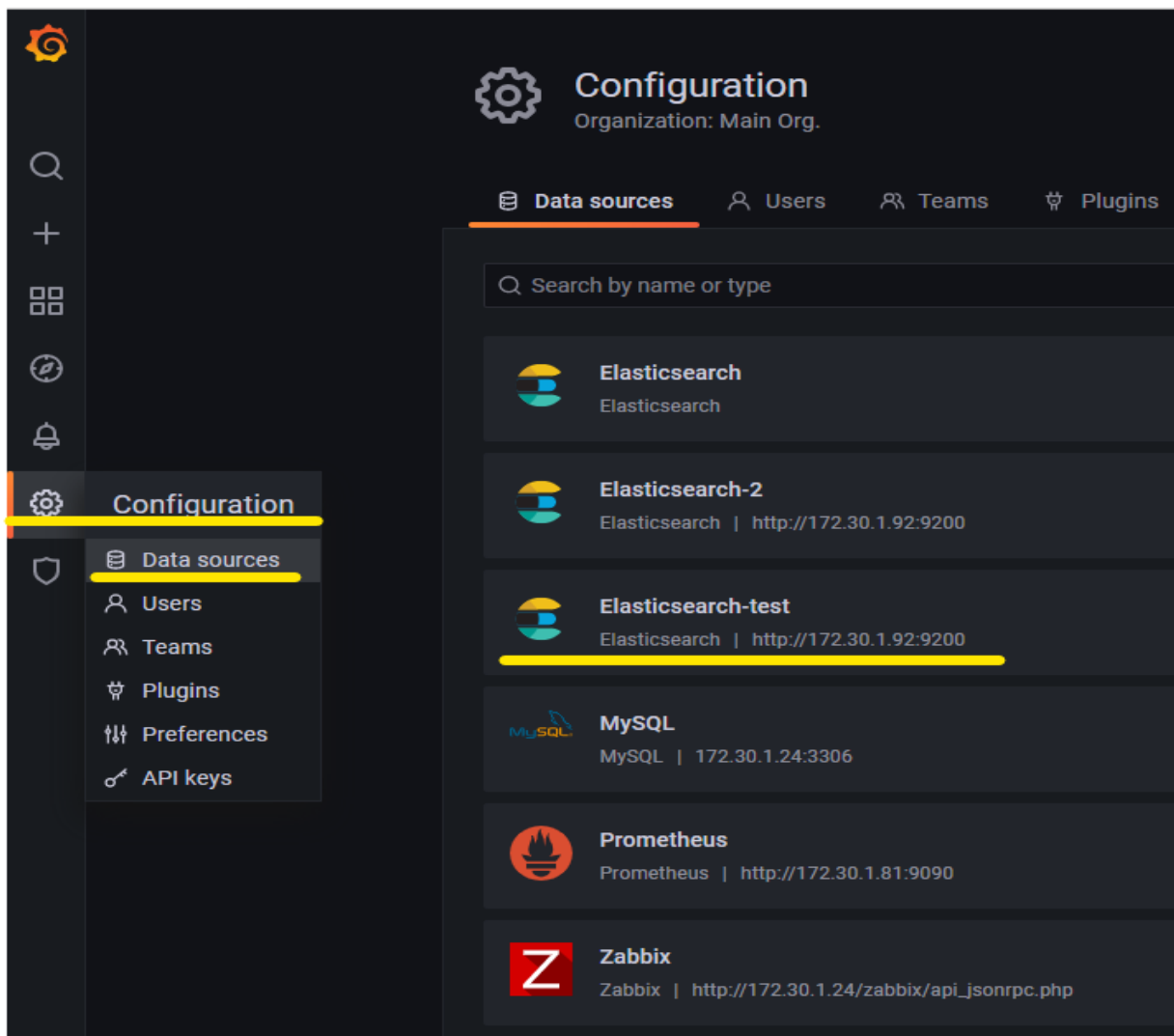
나는 최근 버전을 깔았으므로 7.10을 선택하였다.

7. 맨 마지막의 Save & test 를 눌러준다.

위에 초록색 화살표가 나오면서 Index OK. Time field name OK.가 나온다면 성공한 것이다.



8. Configuration > Data sources 에 들어가시면 방금전에 내가 만든 데이터가 들어가있음을 알 수 있다.



9. Standard options > Unit > Boolean

Standard options > Unit > Time

Standard options > Unit > bytes 등을 변환하여 원하는 꼴로 나타낼 수 있다.

The screenshot shows the Grafana 'MySQL status' dashboard. The main panel displays 'Off' in large green text. The right sidebar shows the 'Standard options' menu with 'Unit' set to 'On / Off'. The 'Query' panel shows the data source 'Elasticsearch\_kml' and the query 'Lucene Query'.

homework\_ES\_to\_GF / Edit Panel

Table view ☐ Fill Actual Last 6 hours

MySQL status

Off

Query 1 Transform 0

Data source Elasticsearch\_kml Query options MD = auto = 223 Interval = 2m Query inspector

Query Lucene Query Alias Alias Pattern

Metric (3) Sum mysql.status.bytes.received Options

Group By Date Histogram @timestamp Interval: auto

+ Query + Expression

Standard options

Unit On / Off

Temperature > True / False

Time > Yes / No

Throughput > On / Off

Velocity >

Volume >

Boolean >

auto

Display name Change the field or series name none

Color scheme From thresholds (by value)

No Value What to show when there is no value

The screenshot shows the Grafana 'Uptime' dashboard. The main panel displays '18.0 day' in large green text. The right sidebar shows the 'Standard options' menu with 'Unit' set to 'milliseconds (ms)'. The 'Query' panel shows the data source 'Elasticsearch\_kml' and the query 'Lucene Query'.

homework\_ES\_to\_GF / Edit Panel

Table view ☐ Fill Actual Last 6 hours

Uptime

18.0 day

Query 1 Transform 0

Data source Elasticsearch\_kml Query options MD = auto = 223 Interval = 2m Query inspector

Query Lucene Query Alias Alias Pattern

Metric (1) Max system.uptime.duration.ms Options

Standard options

Unit milliseconds (ms)

Pressure > microseconds (μs)

Radiation > milliseconds (ms)

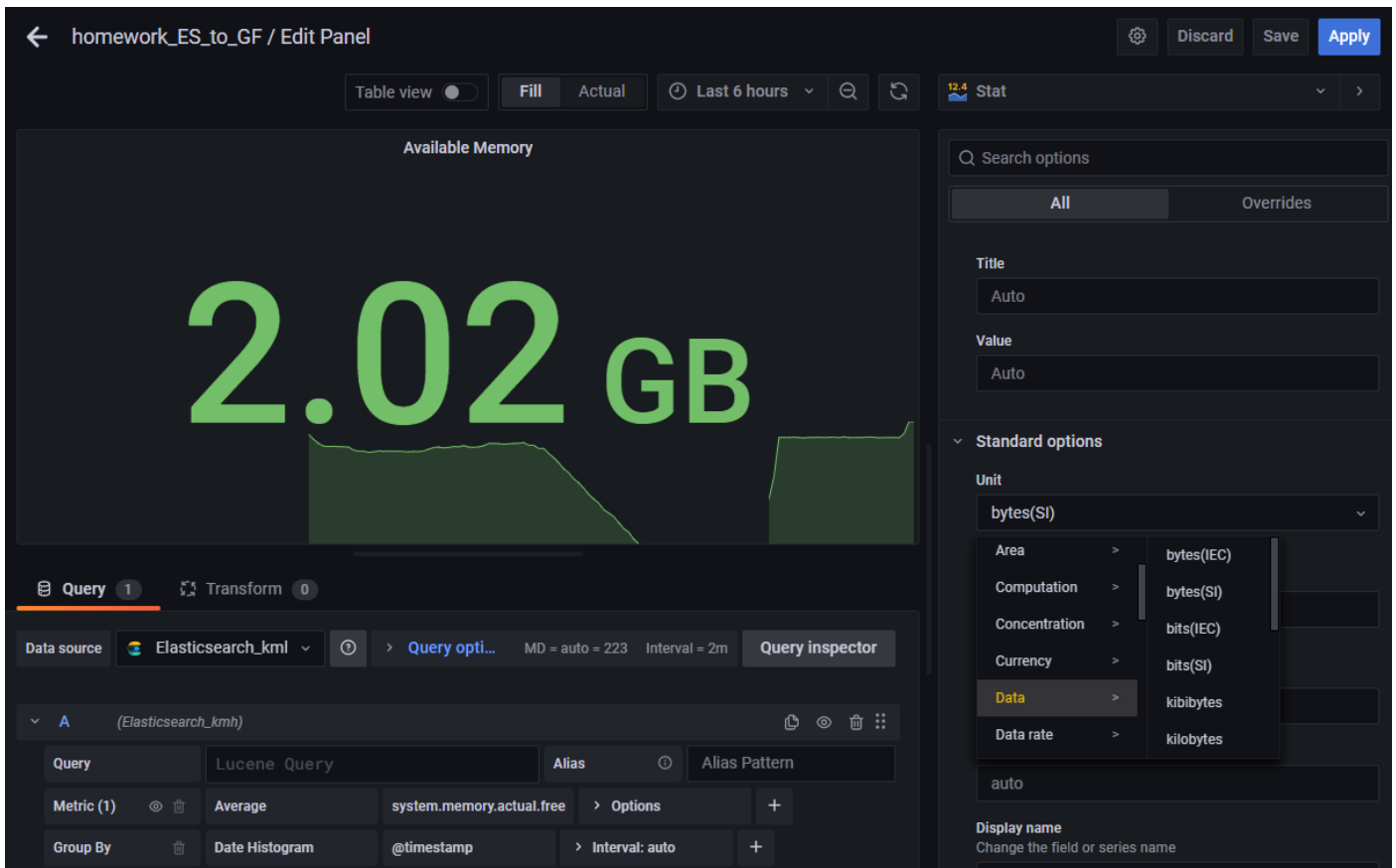
Rotational Speed > seconds (s)

Temperature > minutes (m)

Time > hours (h)

Throughput > days (d)

auto



10. Transform > Add field from calculation 을 이용하여 여러 값의 사칙연산을 할 수 있다.

Replace all fields를 이용해 여러 값을 사칙연산한 값만 불러올 수 있다.

