ElasticSearch-connect

Description

Elasticsearch-connect, allows Switch to send, delete and get data from Elasticsearch database.

With **Elasticsearch-connect**, you don't need to have a deep understanding of Elasticsearch's basic functionality, the app does (almost) everything for you.

And if Elasticsearch holds no secrets for you, we've included an "advanced" mode, for specific query and data indexing based on the powerful Lucene query language.

Elasticsearch environment

Elasticsearch is a distributed search and analytics engine, based on Apache Lucene.
It enables efficient storage, retrieval, and analysis of large volumes of data in real-time.
Widely used for full-text search, log data analysis, and as a key component in a wide range of applications.

In tandem with Kibana (Graphic user interface), and or Grafana (powerful dashboards) , you will be able to visualize your queries and build fancy dashboards.

All these applications are open source and can be runned in Docker. See related section for more information (page 05)

Use cases

- Press Productivity and Workload
- Infrastructure Monitoring
- Sales and Marketing Analytics:

Compatibility

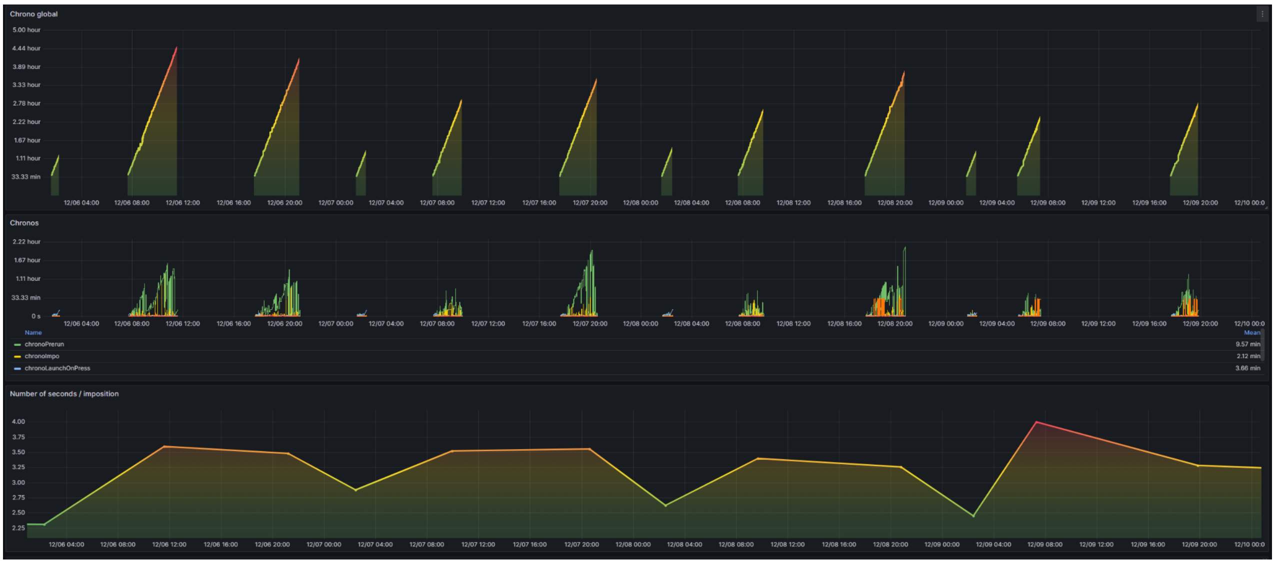
Switch 2023 fall or higher.

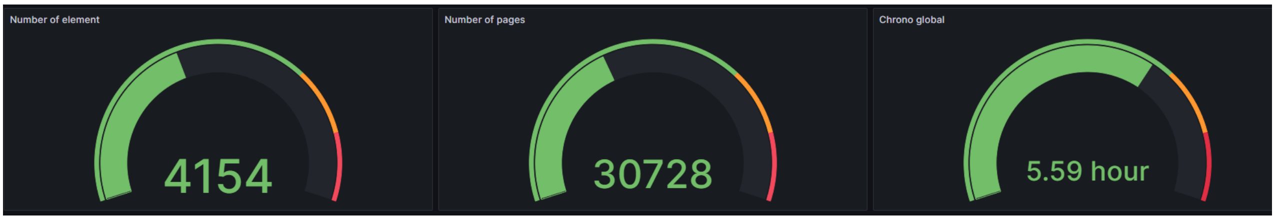
Third party compatibility

Elasticsearch database

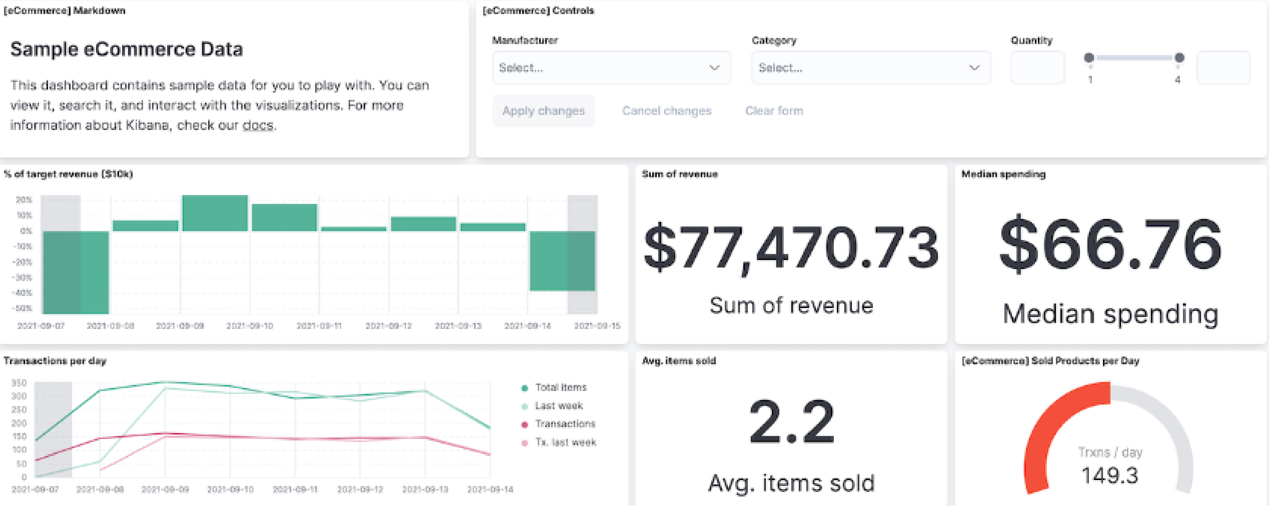
Example of dashboards :

Grafana :





Kibana dashboards :



[eCommerce] Markdown

Sample eCommerce Data

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

Flow element properties

- **Connection properties**
  - **URL**
    URL of your Elasticsearch database.

  - **Port**
    The port of your Elasticsearch database (default 9200).
    When this parameter is set, the application checks whether the address [URL] :[PORT] gives a response.

  - **Username**
    Username that will be used to query Elasticsearch database.
    Default value is "elastic".

  - **Password**
    Password to be used to query Elasticsearch database.
    Default value is “changeme” (see docker-compose section) and should obviously be changed.

    Once set, the application will check if the URL, port, username and password give a successful Elasticsearch response.

- **Index**
  The name of the index that will be used by the app.
  Index names must meet the following criteria :
  - Lowercase only
  - Cannot include \, /, *, ?, " (double quote), <, >, |, “ “ (space character), “,” (coma), #
  - Cannot start with -, _, +
  - Cannot be . or ..
  - Cannot be longer than 255 bytes (note it is bytes, so multi-byte characters will count towards the 255 limit faster)

- **Action**
    - Add data to index
      Will add new data to the index, with 3 modes : Basic, Advanced, From dataset.
        - Timestamp
          An automatic key named @timeStamp will be added, by default current will set the current timeStamp.
        - Mode
            - Basic
              Specify the key and value to be set, with an “=” as a separator.
              Eg : key=value
            - Advanced
              Specify multi-line JSON formatted content.
            - From Dataset
                - Dataset name
                  Specify the name of a JSON dataset that will be used as data.

    - Get data from index
      Retrieves data from the specified Elasticsearch index.
      At least one log connection must be established when using this variable.
        - Request mode
          Work with 2 modes : Basic, Advanced.
            - Basic
                - Request size
                  Specify the maximum number of items you want in return.
                - From date
                - To date
                  Times limit of your request.
            - Advanced
                - JSON request
                  A valid JSON query that respects DSL query notation.
                  More information on Elasticsearch documentation.

    - Delete index
      This action deletes an entire index from Elasticsearch
      Useful for resetting data after test(s).

      Use at your own risk.

- **Output incoming job**
  Indicates whether to send the incoming job to the outgoing data connection(s).
  If the value is "Yes", a data connection must be defined.

Installing

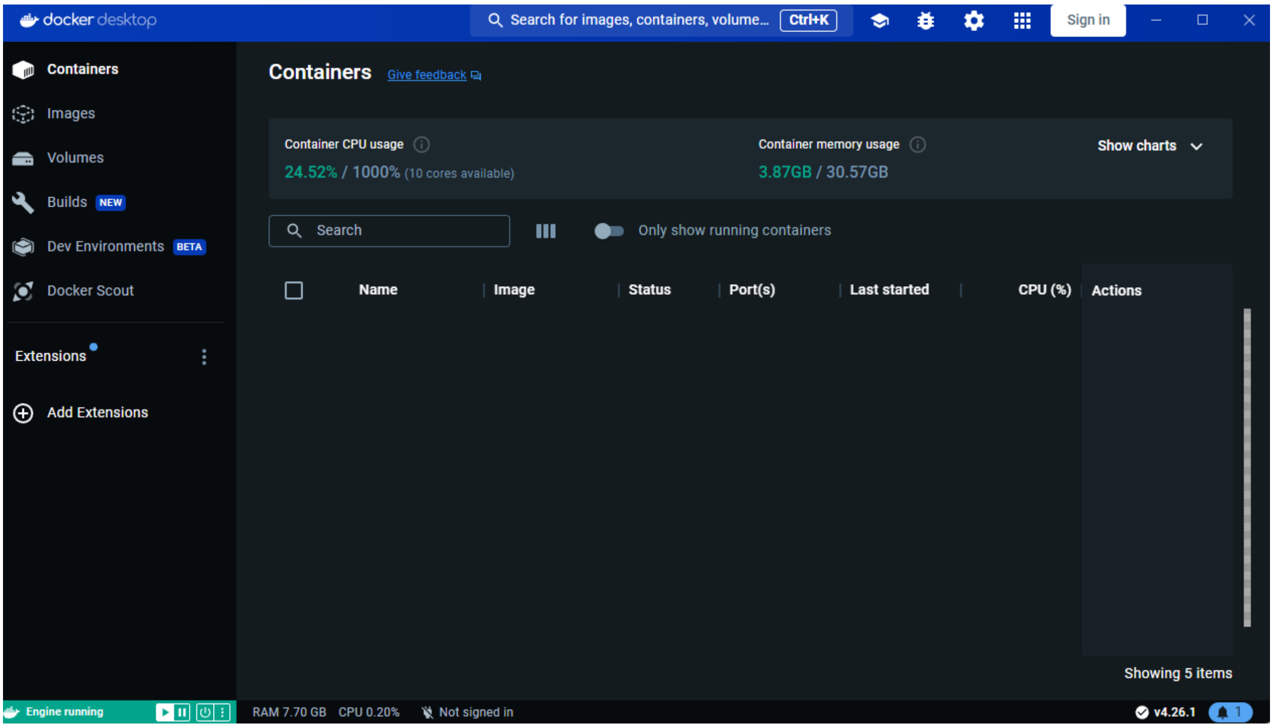
If you do not already have Elasticsearch, you can install it in just a few minutes with little or no computer knowledge.

The tutorial below will help you set up the following docker images :

- Elasticsearch : Open source database
- Kibana : Graphical interface for Elasticsearch, and simple dashboards
- Grafana : Graph creation, complex data manipulation, Dashboard sharing, monitoring…

Prerequisite : Installing Docker

1. Download Docker Desktop here : https://www.docker.com/products/docker-desktop/
2. Install it, follow the instructions, it's as simple as that.
3. Launch docker desktop, and you should see the following interface:



4. Depending on your operating system, you may need to reboot.

Using the docker compose

1. Download the zip file named docker-elk.zip from the application page.

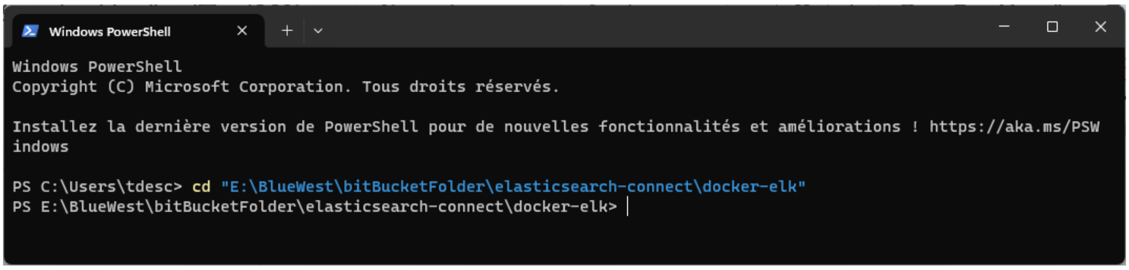
2. Unzip it to the location of your choice, in this exemple,
   "E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk".

3. You can read the Readme inside it for a detailed procedure, or follow the steps below.

4. Open the **.env** file, and change the password "changeme" to something you will remember.

5. Right click on the "docker-elk" top folder and select : "Open in terminal"or use the following command in your favorite terminal

   ```
   cd  "E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk"
   ```

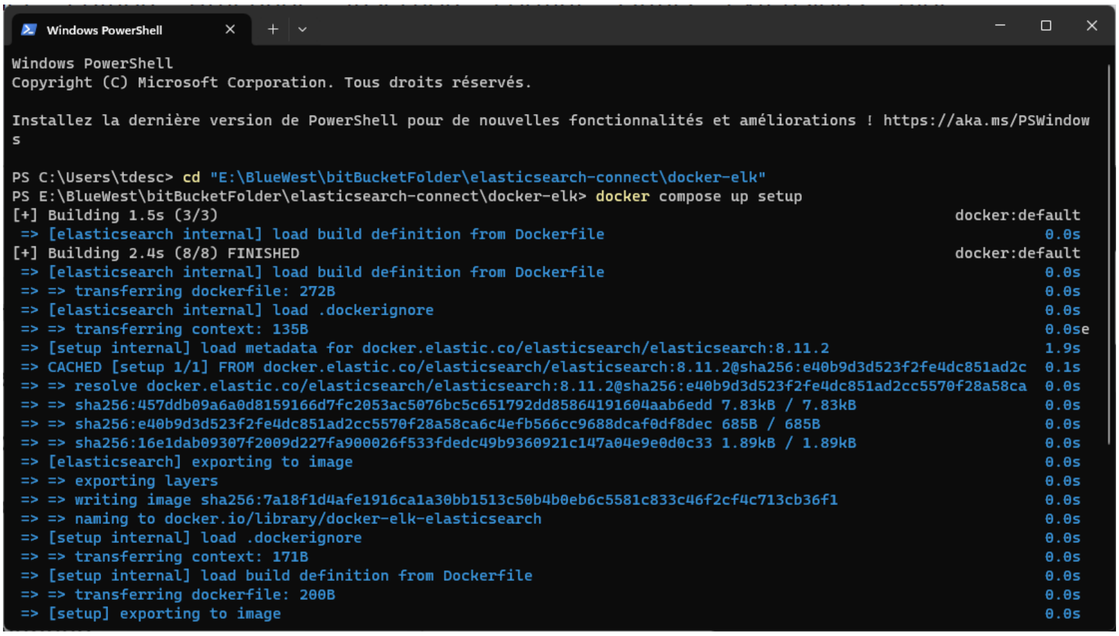
   ```
   Windows PowerShell
   Copyright (C) Microsoft Corporation. Tous droits réservés.

   Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSW
   indows

   PS C:\Users\tdesc> cd "E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk"
   PS E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk> |
   ```

6. Run the following command :

   ```
   docker compose up setup
   ```

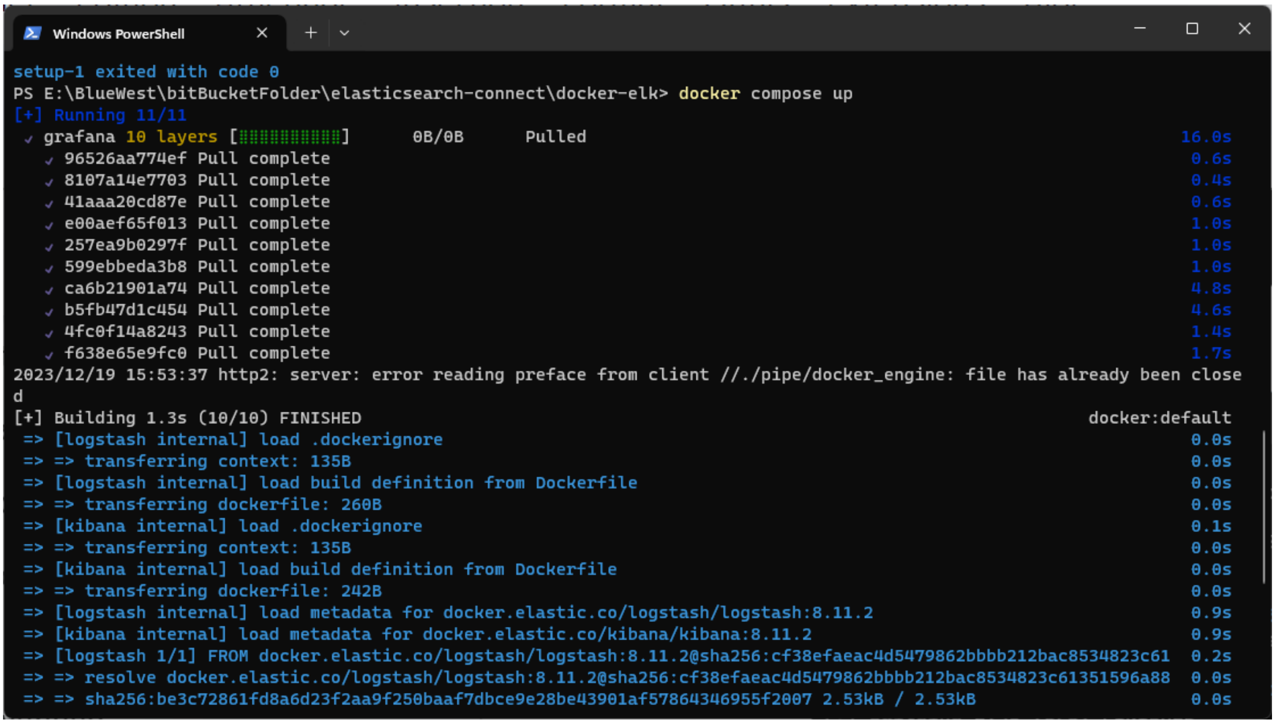
   ```
   Windows PowerShell
   Copyright (C) Microsoft Corporation. Tous droits réservés.

   Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindow
   s

   PS C:\Users\tdesc> cd "E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk"
   PS E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk> docker compose up setup
   [+] Building 1.5s (3/3)                                                                                docker:default
    => [elasticsearch internal] load build definition from Dockerfile                                               0.0s
   [+] Building 2.4s (8/8) FINISHED                                                                       docker:default
    => [elasticsearch internal] load build definition from Dockerfile                                               0.0s
    => => transferring dockerfile: 272B                                                                             0.0s
    => [elasticsearch internal] load .dockerignore                                                                  0.0s
    => => transferring context: 135B                                                                                0.0se
    => [setup internal] load metadata for docker.elastic.co/elasticsearch/elasticsearch:8.11.2                      1.9s
    => CACHED [setup 1/1] FROM docker.elastic.co/elasticsearch/elasticsearch:8.11.2@sha256:e40b9d3d523f2fe4dc851ad2c  0.1s
    => => resolve docker.elastic.co/elasticsearch/elasticsearch:8.11.2@sha256:e40b9d3d523f2fe4dc851ad2cc5570f28a58ca  0.0s
    => => sha256:457ddb09a6a0d8159166d7fc2053ac5076bc5c651792dd85864191604aab6edd 7.83kB / 7.83kB                    0.0s
    => => sha256:e40b9d3d523f2fe4dc851ad2cc5570f28a58ca6c4efb566cc9688dcaf0df8dec 685B / 685B                        0.0s
    => => sha256:16e1dab09307f2009d227fa900026f533fdedc49b9360921c147a04e9e0d0c33 1.89kB / 1.89kB                    0.0s
    => [elasticsearch] exporting to image                                                                           0.0s
    => => exporting layers                                                                                          0.0s
    => => writing image sha256:7a18f1d4afe1916ca1a30bb1513c50b4b0eb6c5581c833c46f2cf4c713cb36f1                     0.0s
    => => naming to docker.io/library/docker-elk-elasticsearch                                                      0.0s
    => [setup internal] load .dockerignore                                                                          0.0s
    => => transferring context: 171B                                                                                0.0s
    => [setup internal] load build definition from Dockerfile                                                       0.0s
    => => transferring dockerfile: 200B                                                                             0.0s
    => [setup] exporting to image                                                                                   0.0s
   ```

   The application and image will be downloaded, and you will be able to see the progression in the terminal.

7. Once done, run the following command :
   `docker compose up`



```
setup-1 exited with code 0
PS E:\BlueWest\bitBucketFolder\elasticsearch-connect\docker-elk> docker compose up
[+] Running 11/11
 ✔ grafana 10 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿]      0B/0B      Pulled                                    16.0s
   ✔ 96526aa774ef Pull complete                                                               0.6s
   ✔ 8107a14e7703 Pull complete                                                               0.4s
   ✔ 41aaa20cd87e Pull complete                                                               0.6s
   ✔ e00aef65f013 Pull complete                                                               1.0s
   ✔ 257ea9b0297f Pull complete                                                               1.0s
   ✔ 599ebbeda3b8 Pull complete                                                               1.0s
   ✔ ca6b21901a74 Pull complete                                                               4.8s
   ✔ b5fb47d1c454 Pull complete                                                               4.6s
   ✔ 4fc0f14a8243 Pull complete                                                               1.4s
   ✔ f638e65e9fc0 Pull complete                                                               1.7s
2023/12/19 15:53:37 http2: server: error reading preface from client //./pipe/docker_engine: file has already been close
d
[+] Building 1.3s (10/10) FINISHED                                                    docker:default
 => [logstash internal] load .dockerignore                                                     0.0s
 => => transferring context: 135B                                                              0.0s
 => [logstash internal] load build definition from Dockerfile                                  0.0s
 => => transferring dockerfile: 260B                                                           0.0s
 => [kibana internal] load .dockerignore                                                       0.1s
 => => transferring context: 135B                                                              0.0s
 => [kibana internal] load build definition from Dockerfile                                    0.0s
 => => transferring dockerfile: 242B                                                           0.0s
 => [logstash internal] load metadata for docker.elastic.co/logstash/logstash:8.11.2           0.9s
 => [kibana internal] load metadata for docker.elastic.co/kibana/kibana:8.11.2                 0.9s
 => [logstash 1/1] FROM docker.elastic.co/logstash/logstash:8.11.2@sha256:cf38efaeac4d5479862bbbb212bac8534823c61  0.2s
 => => resolve docker.elastic.co/logstash/logstash:8.11.2@sha256:cf38efaeac4d5479862bbbb212bac8534823c61351596a88  0.0s
 => => sha256:be3c72861fd8a6d23f2aa9f250baaf7dbce9e28be43901af57864346955f2007 2.53kB / 2.53kB    0.0s
```

The application and image will download additional resources and finalize the application installation

Congratulations, you can now access to :

- Kibana with : http://localhost:5601 (with the login defined in .env file)
- Grafana with : ttp://localhost:3000 (with admin/admin as login/pwd)

Useful resources :

Kibana starting guide	https://www.elastic.co/guide/en/kibana/current/get-started.html
Grafana starting guide:	https://grafana.com/docs/grafana/latest/getting-started/
Elasticsearch datasource in Grafana	https://grafana.com/docs/grafana/latest/datasources/elasticsearch/configure-elasticsearch-data-source/
Elasticsearch query in Grafana	https://grafana.com/docs/grafana/latest/datasources/elasticsearch/query-editor/