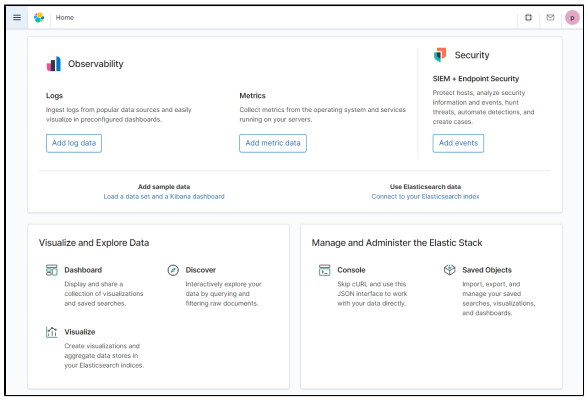
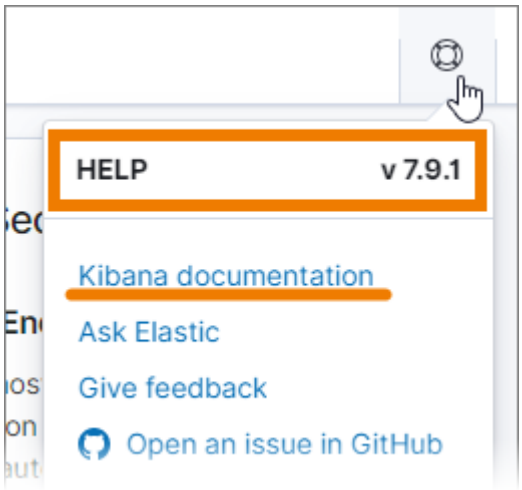
Kibana

Kibana: Analyzing Data



Scheer PAS uses Kibana to view, filter and search the platform log s for all services.

Kibana is an open source analytics and visualization tool designed to work with Elasticsearch. With Kibana you can search, view, and interact with data stored in Elasticsearch indices. You can perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.



On this Page:

Related Pages:

- 3rd Party Tools
  - Keycloak
  - Portainer

Related Documentation:

- API Management
  - Metrics
- OpenDistro
- Official Kibana Documentation
  - Webinar: Getting started with Kibana

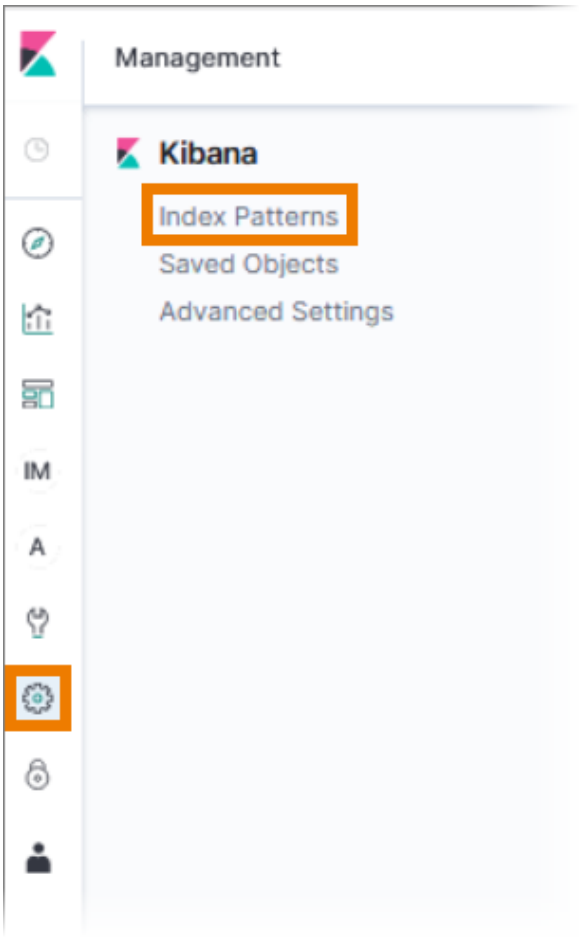
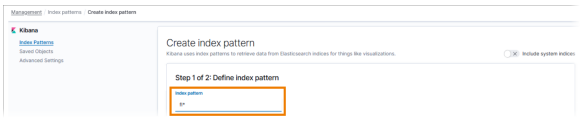
For detailed information on Kibana, its features and how to use them, refer to the Official Kibana Documentation. Please note that **Schneer PAS** does not use the regular Elasticsearch /Kibana installation but the OpenDistro version. Some Kibana features may not be availble in the OpenDistro version.

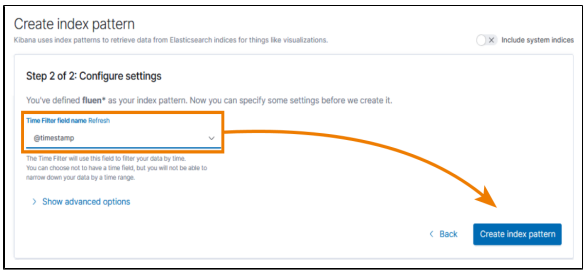
Please note that the official documentation may vary according to different versions of the tool.

Before consulting the documentation check your Kibana version. It is displayed if you open the help menu  where you can also find a direct link to the official documentation.

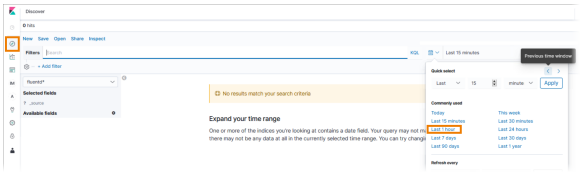
Creating an Index Pattern

Kibana needs to knows which Elasticsearch indices contain the data you want to analyze. So you have to create an index pattern in Kibana first to make sure that data is available. If your Kibana is empty and does not contain an index pattern yet, Kibana asks you to create one. You need to do this only once after the first login, then all users with Kibana permission can view the logs.

	To set the index pattern, open Kibana and log in with the admin user. • Go to **Management** > **Index Patterns**.
	• Click button **Create index pattern**.
	• Set the index pattern name **fl***, then click **Next Step**.



In the next window, open the drop-down list of **Time field** and select **@timestamp**, then click **Create index pattern**.

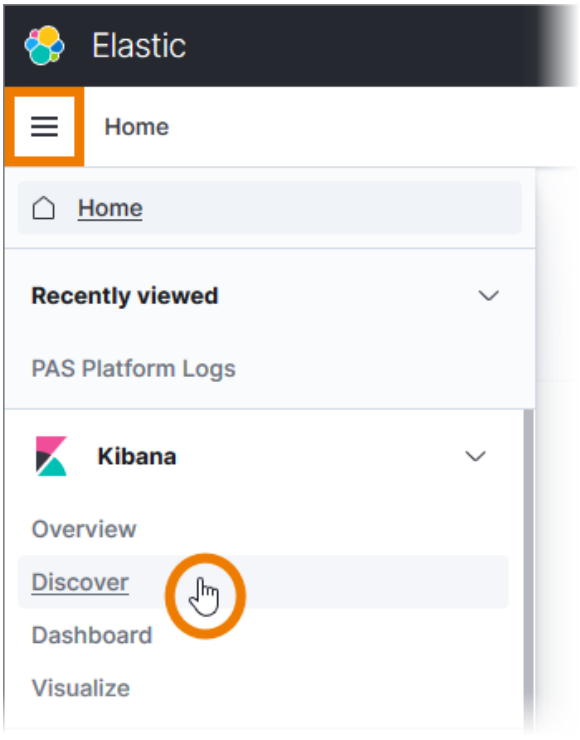


Go to menu **Discover**: Now you can see the service logs.

If no logs are displayed, extend the time range.

For further information refer to page Create an index pattern in the Official Kibana Documentation.

Discover: Searching Your Data

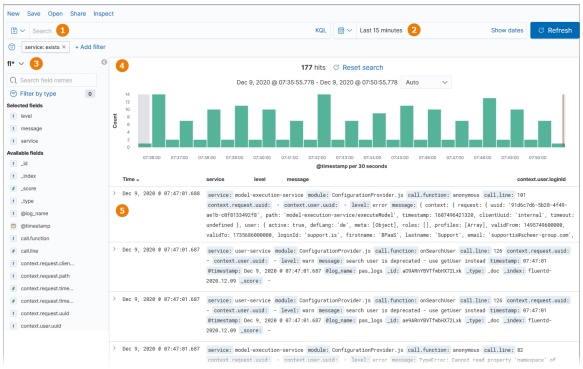


To access the functionalities of Kibana, open the menu ☰ on the Kibana start page.

The **Discover** option allows you:

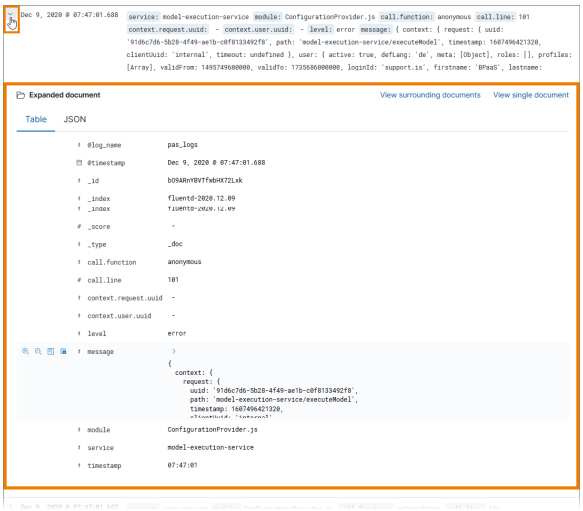
- to select data for exploration.
- to set a time range for the data.
- to search your data with the Kibana Query Language.
- to filter the results.
- to explore the details of your data.
- to view individual documents.
- to create tables that summarize the contents of the data.

The Official Kibana Documentation offers a tutorial on how to use the Discover option.



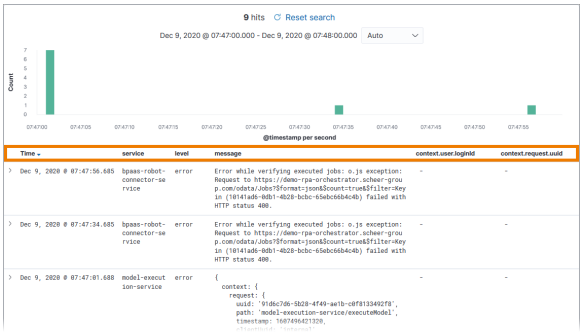
Overview on the **Discover** page in Kibana:

1. **Search Query:**
   Enter your search query here. Visit the official Kibana documentation to get detailed information about the Kibana Query Language (KQL).
2. **Time Range:**
   Click here to set a time range for the data you want to inspect.
3. **Sidebar:**
   Use the sidebar to select your index pattern and to access the list of available fields.
4. **Time Histogramm:**
   Shows the time range of the displayed data.
   To view the count of documents for a given time, drag the mouse over the histogram.
5. **Documents Table:**
   All documents/data available for the set time range are displayed here. You can customize the display and adapt it to your needs.



Expand a document to show the available settings.

To add a setting to the table display, click on its menu item **Toggle column in table**:

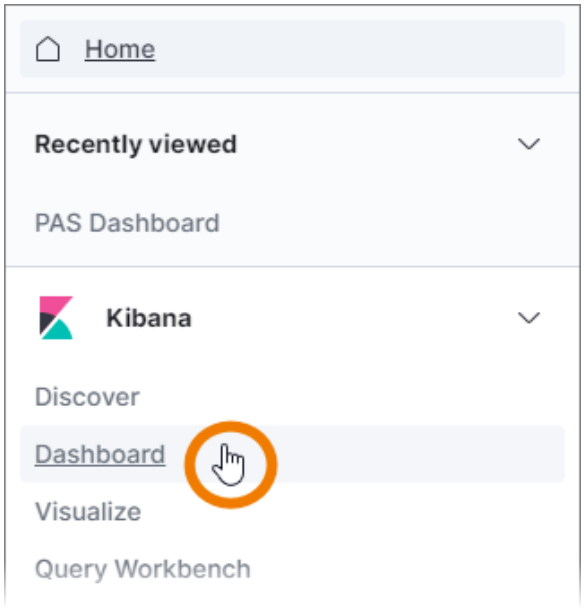


To inspect logs of **Scheer PAS** Node.js services, you can for example select the following settings to display:

- **timestamp** (displayed by default)
- **service** (= name of the service)
- **level** (= log level)
- **message** (= log message)
- **context.user.loginId** (= login name of the user)
- **context.request.uuid** (= UUID of the request)

Once you have created such a query, you are also able to save it for further use, for example in a dashboard.

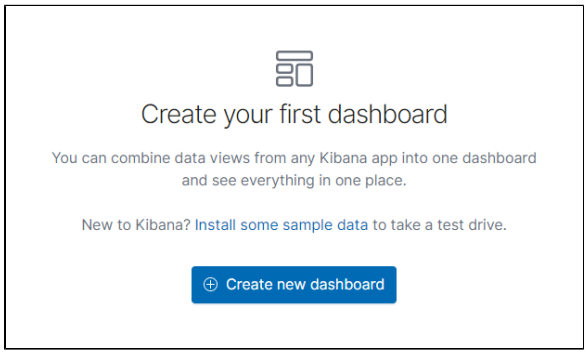
Creating Dashboards



Kibana also offers the possibility to create your own dashboards.

You can add a variety of different panels to inspect and visualize your data, for example area charts, bar and line charts, tree and heat maps, metrics, data tables and many more.

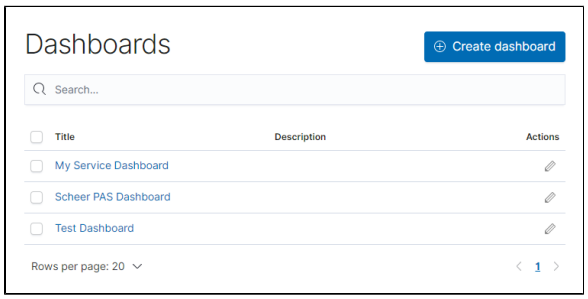
Choose option **Dashboard** in the sidebar to start.



If no dashboards are available, you are asked to create your first dashboard. For example, use a query saved in **Discover** to insert it as block in your dashboard.

Refer to page Dashboard in the Official

Kibana Documentation for detailed information how to create a dashboard.



If you have already created some dashboards, the available dashboards are displayed.

Use the list to open, edit or delete your dashboards.