datapunctum

ElasticSPL

Explore ElasticSPL Features

- Ad-hoc querying: Query Elasticsearch using either DSL or Lucene search statements for time-series or aggregated data.
- Query saving and sharing: Save your DSL or Lucene queries and easily share them with other users.
- Query customization: Configure your DSL or Lucene queries with replacements to adapt queries to the current requirement on the fly.
- Interactive explorer dashboard: Create DSL or Lucene queries and preview results using an interactive explorer dashboard.
- Access control: Enjoy the peace of mind of Role-Based Access Control.
- Multiple instances management: Easily manage multiple Elasticsearch instances and saved queries.

Download ElasticSPL from Splunkbase

To try out unlimited number of connections, request a free 30-day trial key.

splunk> Partnerverse

What is **ElasticSPL?**

Introducing ElasticSPL by Datapunctum – a powerful solution that enables you to streamline your data analysis and gain new insights from your existing data sources. With ElasticSPL, you can harness the query capabilities of Elasticsearch from the Splunk Search interface, allowing you to display results and visualisations easily. ElasticSPL provides your environment with custom Splunk commands that enable you to access data stored in Elasticsearch with minimal effort.

Why **ElasticSPL?**

By utilizing ElasticSPL as a bridge between Splunk and Elasticsearch, you can gain valuable insights and a comprehensive view of your data. This is especially useful for organizations that need to work with data from multiple sources. ElasticSPL makes integrating data from Elasticsearch into Splunk functions such as dashboards and visualizations easy.

The ElasticSPL Workbench allows users to explore data, run, update and create saved queries, and leverage events, statistics, and visualizations to gain insights into your data even faster. ElasticSPL is designed to operate with all flavours of Elasticsearch, from OpenSearch, over Open Distro to Elasticsearch Cloud.

With ElasticSPL, you can quickly identify trends and patterns across multiple data sources, enabling you to make informed decisions and optimize your operations. By seamlessly integrating with both Splunk and Elasticsearch, ElasticSPL is a must-have tool for any organization seeking to maximize its data analysis capabilities.

data SOLUTIONS

Reseller:
4Data Solutions
Zeppelin Building • 3rd Floor • 59-61 Farringdon Road
London, EC1M 3JB
+44 330 128 9180 • info@4datasolutions.com

Datapunctum AG • Badenerstrasse 47 • CH-8004 Zurich
+41 44 500 73 01 • info@datapunctum.com