

Search on Snowflake



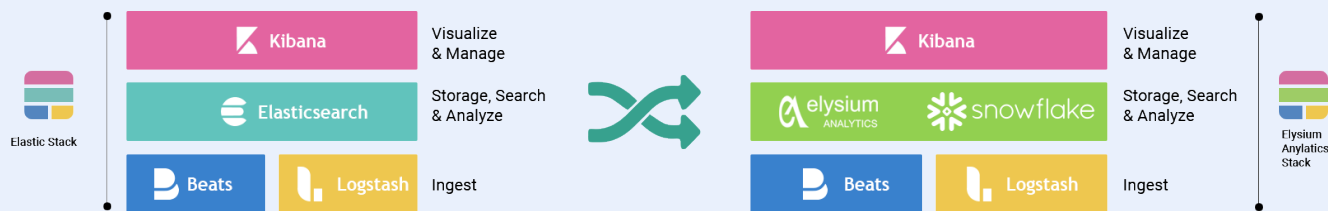
Search with Kibana on Snowflake

With download numbers in the hundreds of millions, Elasticsearch is arguably the most popular search application today. It provides near real-time scalable search, supports multitenancy, and has proven to be a valuable tool for search on large datasets. Combined with Logstash (for data collection and log-parsing), Kibana (for analytics and visualization), and Beats (a collection of lightweight data shippers), the four products are designed for use as an integrated solution; they are referred to as the "Elastic Stack," providing a powerful tool to store and access large amounts of data. So, what's not to like? It is open source, it has good documentation, and a great community behind it providing support. It is scalable and reliable, and proven itself in many situations, processing billions of data points on a daily basis. It also provides easy interaction, with its RESTful interface and many common languages.

However, as companies are scaling out of Elasticsearch, they often run into challenges: While Elastic Stack is available as open source, most enterprises will license the software to get a commercially supported solution. Adding the cost of configuring, managing, and monitoring the solution adds overhead, and keeping up with adding hardware also gets costly very quickly. If you run Elasticsearch in the cloud, you will be facing many of the same issues with scaling compute and storage as your data volume grows. Making sure you have the optimal kind of hardware requires planning and fine-tuning as the system scales. Significant effort is required to maintain the infrastructure that powers Elasticsearch, as well as managing the data.



Search with Kibana on Snowflake



By combining a best-practice data science platform with free text search, any information — structured and unstructured — can be retrieved from billions of log lines. With the best aspects of Snowflake and the Kibana interface, you have an easy-to-use and scalable search solution.

If you are already using Elasticsearch and are concerned about the overhead cost of configuring, managing, and monitoring the solution, as well as keeping up with adding hardware as your data volume grows, we can help you out with simple migration to a true cloud-scale, cost-effective platform. The Elasticsearch indexes are mapped to the Elysium Open Data Model, and you will be up and running, loading data in a very short time.

The screenshot displays the Elysium search interface. At the top, a search bar shows the query: `* - SRC_HOST: sncm32 and SRC_TYPE: System and EVENT_ID: 3`. The results show 9,029 hits for the time range from Jan 1, 2020 @ 07:28:32.41 to Jun 6, 2020 @ 07:28:56.33. A bar chart visualizes the event time per hour, with significant peaks around 2020-09-12 00:00 and 2020-09-12 12:00. Below the chart, a table of log entries is displayed, with columns for parent, event, and source. The table shows multiple entries with detailed fields like `EVENT_ID`, `EVENT_TIME`, `EVENT_TYPE`, and `EVENT_STATUS`. A sidebar on the left provides navigation and field selection options.



Fully Managed

Elysium Analytics is a fully-managed service that makes it easy for you to deploy, secure, and run searches cost-effectively at scale. With Elysium Analytics Search, you only pay for what you use – there is no upfront cost or usage requirements and no operational overhead.



Improve Productivity

Improve your SOC team's productivity to enable search on all your data on Snowflake at cloud scale. Elysium Analytics is pre-configured and ready to go on all the data you have in your Snowflake data warehouses with the instant and near-infinite performance, concurrency, and scale your organization requires. Compute usage is billed on a per-second basis, with a minimum of 60 seconds.



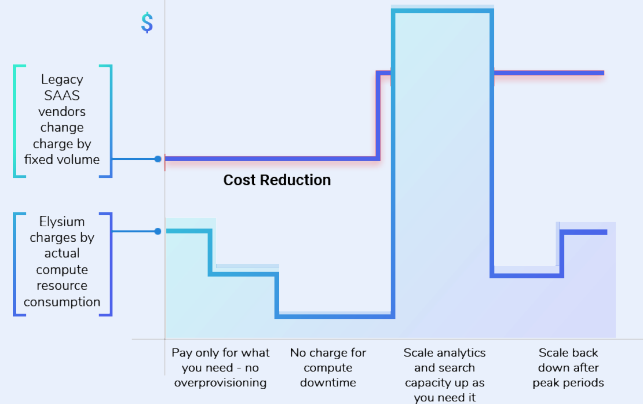
Stay with Kibana

Leveraging the familiar Kibana interface, you can quickly start accessing all your data with the flexibility you are used to from Kibana. No setup or deployment required. You can easily change your search parameters, fine-tune search relevance, and apply new settings at any time. As your volume of data and traffic fluctuates, Elysium Analytics seamlessly scales to meet your needs.



Scalable & Cost-Effective

Elysium Analytics Search offers powerful cloud-scaling as the demand for processing grows. As your data or query volume changes, you can easily scale your compute resources up or down as needed and it goes to zero when you are done with your task. We only charge for the resources you use.



How to Search Your Log Data



You can interactively search and explore your data with a pre-defined index pattern by simply entering your search criteria in the Query Bar. By default, you use Kibana's standard query language, which features autocomplete and a simple, easy-to-use syntax. Additionally, Kibana's legacy query language, based on Lucene query syntax, is also available under the options menu in the Query Bar. With the pre-configured index pattern, you can interactively explore your data in Discover, analyze your data in charts, tables, gauges, tag clouds, and more in Visualize.

When submitting a search request, the histogram, Documents table, and Fields list are updated to reflect the search results. The total number of hits, or matching events, is shown in the toolbar. Sort the table by the values in any indexed field. The Documents table shows the first 500 hits. By default, the hits are listed in reverse chronological order, with the newest documents shown first. You can reverse the sort order by clicking the Time column header. You can also sort the table by the values in any indexed field.

How to Load Your Log Data

Setting up data ingestion is often a time consuming and challenging task when you have multiple sources of log data from cloud and on-premises sources. We have made the process of collecting, parsing, enriching and loading your data simple.

If you already are loading data to Elasticsearch, we will add the Elysium Analytics plugin to your existing Logstash enabling it to write logs directly to Elysium Analytics Open Data Model on Snowflake. Similarly, if you are already collecting data over Kafka or to Splunk or other log management solutions today,



we will configure your existing implementations to forward data directly to Elysium Analytics open data model on snowflake while maintaining the data flow to your legacy applications in parallel with zero disruption to existing solution. However, if you are not collecting log data for log analysis today, we will set you up and handle everything for you from end to end.

Built for the Cloud



Built for the Cloud

Fast time to value, near-zero maintenance, built-in product security, and an architecture that scales storage and compute resources independent of each other, up and down, and automatically.



Cost-Effective

Only pay for the compute you use and store all your data for long periods at rates as low as \$23/TB/month after compression.



Reliable

Automatic monitoring and recovery running on Kubernetes cluster as fully managed services. Search traffic is distributed across Availability Zones with full redundancy.



High Performance DB

Low latency and high throughput performance at large scale through optimized storage of backend database with time sliced micro partitions and horizontal and vertical autoscaling.



Rich Search Features

Supports powerful search features:

- Free text, Boolean, and Faceted search
- Auto complete suggestions
- Geospatial search
- Highlighting



Secure

Strong cryptographic authentication of users to prevent unauthorized access to your data. Supports HTTPs and integrated with LDAP/AD/Identify Access Management (IAM)



Speed and Scale

Scale to petabytes of stored data and automatically adjust compute up or down for fast performance and query results.




Fully Managed


Zero provisioning needed on this fully managed custom search services but you are still in control of the auto scaling policy


About Elysium Analytics

Elysium Analytics is a machine learning based log analysis solution for security-minded, mid-sized to large enterprises who are challenged by the volume of security log data today, both from an infrastructure as well as an analytics and detection perspective. We have simplified onboarding of data, provided a scalable data lake analytics platform, and search on a pay-as-you-go basis. Since we are built on top of Snowflake, our SaaS solution is truly a cloud scale security analytics platform that removes the barriers from ingesting, contextualizing, searching, analyzing, and storing log data with a cost-effective and low-risk service. Unlike other log analysis vendors in the market, our SaaS offering is licensed on a usage basis, lowering cost and removing financial risk. You pay a low price for storage, and compute is billed by the minute of usage. Additionally, we have an open platform with no vendor lock-in, customizable analytics models, as well as APIs for end user development of analytics models.



 Elysium Analytics, Inc. 2550 Great America Way, Santa Clara, CA 95054

 elysiumanalytics.ai

 Phone: +1 (669) 209-0801

 info@elysiumanalytics.ai