1.LogSearch.md

github.com/aniket0609/Sumo_Logic_basic/blob/main/1.LogSearch.md

aniket0609/
Sumo_Logic_basic

1 Contributor 0 Issues 0 Stars 0 Forks

Log Search

Log Search allows you to query and analyze log data sent to Sumo Logic. There are many features to help you use our robust Search Query Language, such as LogCompare, LogReduce, LogExplain, Lookup Tables, Subqueries, and Time Compare. See Get Started with Search to begin exploring your data in Sumo Logic.

Guides

In this section, we'll introduce the following concepts:

Getting started with Log Search

> Start here to begin exploring your data in Sumo Logic.

Search Query Language

> The extensive Sumo Logic query options help you gain valuable insight into your log messages.

Search Cheat Sheets

> Cheat sheets provide examples of useful search queries for different use cases.

LogReduce

> Quickly assess activity patterns for things like a range of devices or traffic on a website.

LogCompare

> Easily compare log data from different time periods to detect major changes or anomalies.

Lookup Tables

> Learn about Lookup tables and the search operators you can use with them.

Live Tail

> Real-time live feed of log events associated with a Source or Collector.

Behavior Insights

> Gain behavioral insight of your environment using LogReduce operators.

Subqueries

> Filter and evaluate conditions for a query when you may not be sure of the exact filter.

ⓘ Note

To interact with other Sumo Logic users, post feedback, or ask a question, visit the Sumo Logic Community Search & Query Forum.

Partitions and Views

Logs collected by Sumo Logic are indexed in Partitions and Scheduled Views. In addition, there are internal indexes such as Health Events, Archive, Audit, and Volume indexes.

- A Partition stores your data in an index separate from the rest of your account data so you can optimize searches, manage variable retention, and specify certain data to forward to S3. See how to Run a Search Against a Partition.
- Scheduled Views speed the search process subsets of your data by functioning as a pre-aggregated index. See how to Run a Search Against a Scheduled View.
- Health Events monitor the health of your Collectors and Sources. See how to Search Health Events.

- Archive allows you to forward log data from Installed Collectors to Amazon S3 buckets to collect at a later time. See how to Search ingested Archive data.
- Audit and Event Audit provide information on the internal events that occur in Sumo Logic. See how to search the Audit and Audit Event Index.
- Data Volume gives you visibility into how much data you are sending to Sumo Logic, allowing you to proactively manage your systems' behavior and to fine tune your data ingest with respect to the data plan for your Sumo Logic subscription. See Data Volume Index for details.

Data Tiers

Data Tiers provide the ability to allocate data to different storage tiers based on the frequency of access: Continuous, Frequent, and Infrequent.

Traces

Traces are collected with SumoLogic Kubernetes Collection or a standalone OpenTelemetry collector through an HTTP Traces Source.