A collection of content for learning Sumo Logic

dev.classmethod.jp/articles/sumo-logic-learning-list

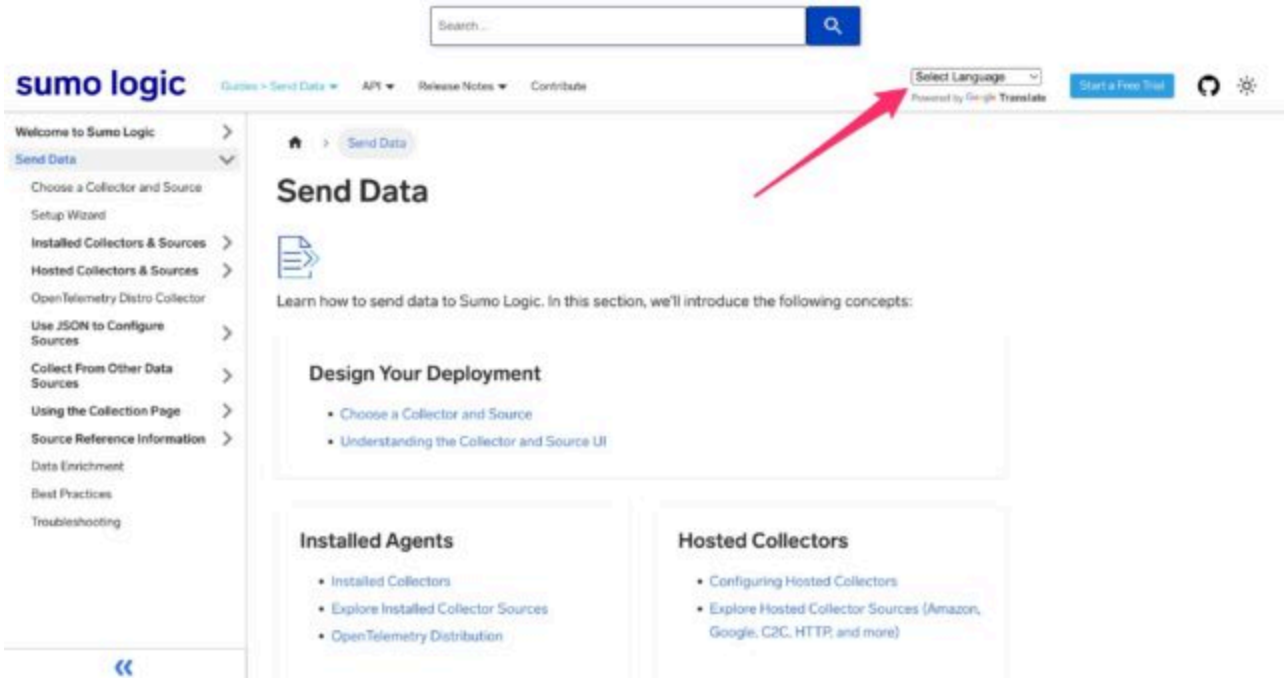
酒井剛

January 30, 2023

If you're thinking about getting started with Sumo Logic, you'll want to learn how to use it efficiently. So, I'd like to summarize the reference locations for each topic, mainly from the official Sumo Logic documentation **, to learn the basics of log analysis .**

Official Sumo Logic Documentation

Each help page has an embedded option to select Google Translate, so please select it if you want to view the page in Japanese.



Regarding log import

Understand the available log ingestion methods

Installed Collector

Learn about Installed Collectors and how to install them on each OS.

Learn about the sources you can configure for an Installed Collector and how to configure them

Hosted Collector

Learn how to set up a Hosted Collector and configure various sources

Learn best practices for source categories

See our blog on designing source categories

Regarding log analysis

Search Basics

Understand the structure of queries when searching logs and understand the general feel of queries

Understand the metadata used within Sumo Logic

Know what wildcards you can use in your queries

Learn basic log search best practices

Learn about the automatic analysis function for JSON format logs

Learn the basic rules of search

Learn how to narrow down the target period when searching logs

How to view the search screen

Check the explanations for each button/output location on the search screen

Check the contents of the field display section on the search screen

Learn how to drill down using the simple statistics function in the field display section of the search screen.

Learn how to toggle the visibility of search screen fields and how they appear

Search query list

See a list of search operators you can use in your queries

See a list of analytical operators available for use in queries

See a list of group/aggregation operators available in queries

Search Use Cases

See examples of common search use cases

View analysis examples and use cases for Apache, Cisco ASA, Microsoft IIS, and Windows Events

Check out the cheat sheet when you forget how to use search operators

Regarding metrics

Metrics Basics

Learn about metadata for metrics

How to read the Metrics Search screen

Learn how to interpret each item on the Metric Search screen, which panels are configurable, how to set metric thresholds, and the basics of metric queries.

Analyzing metrics

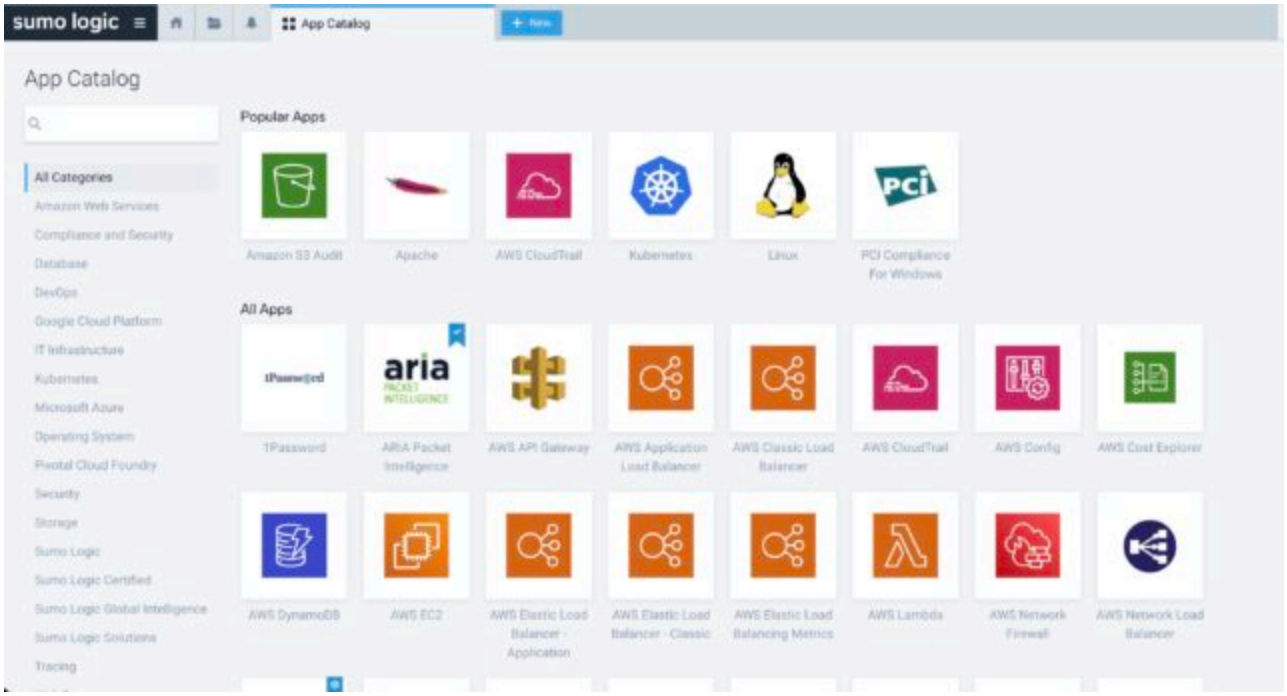
See a list of metric operators available for use in queries

Regarding the use of the app

App List

See a list of available apps and dashboard overview on the subpage

You can also check the list in the App Catalog in the Admin Console.



Alert function

Learn the difference between Alerts (Scheduled Search) and Alerts (Monitor)

Alerts (Scheduled Search)

Learn how to create alerts using Scheduled Searches and send various alerts on the subpage.

Alerts (Monitor)

Learn how to create a Monitor

Learn how to check the status and manage your Monitor

Learn how to use Webhooks to integrate alert results with third parties like PagerDuty and Slack.

About the Dashboard Feature

Dashboard (New)

Learn how to create a Dashboard (New)

Understand the ability to drill down from panels in the Dashboard (New)

Learn how to create filters for Dashboard (New)

Learn how to set the time period for Dashboard (New)

Dashboard (New) Panel

Learn how to create different panels

About Sumo Logic Management Features

Content sharing

Learn how to share dashboards and alerts with others

FER (Field Extraction Rules)

Learn how to normalize (pre-parse) your logs to improve log search performance and query manageability

Users and Roles

Learn about the different roles on the subpage, how to create users and assign roles to them.

Learn how roles can control who can access (view or search) collected log data.

Managing captured logs

Learn how to monitor the volume of logs being ingested and the status of log ingestion

Scheduled View

> Learn how to use Scheduled Views to improve searches for queries that take a long time to return results, such as searches for large logs over long periods of time or searches for log queries with complex queries.

summary

This time, we have compiled links to documents to help you learn the basics of how to configure Sumo Logic. We hope you will use this as a mapping to search for documents based on your purpose.