Parse Operators

dev.classmethod.jp/articles/i-tried-hands-on-some-of-the-parse-operators-of-sumo-logic

HemanthKumar R August 15, 2023

目次

Introduction

Hemanth of Alliance Department here. The blog focuses on sumo logic parse operators. The different way to analyse logs in the sumo logic by the parse operators.

Sumo Logic

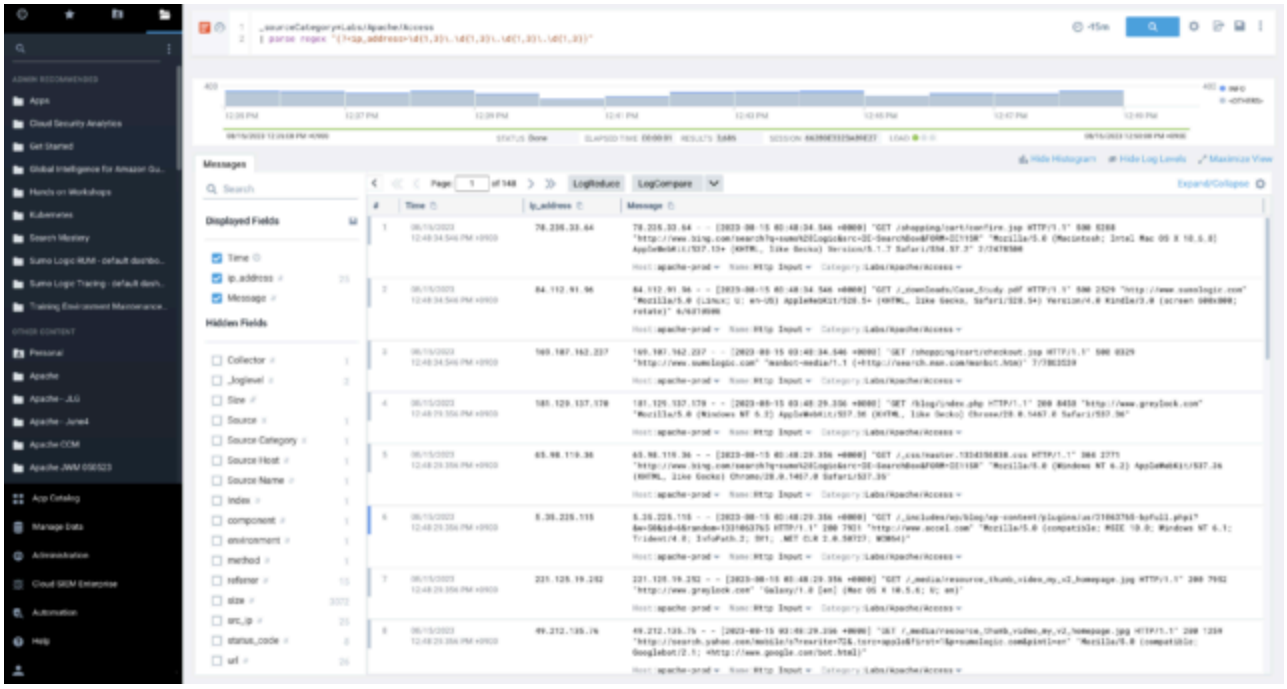
Before going further let's understand what sumo logic is. A cloud-based log management and analytics software called Sumo Logic enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational and security insights.

The ability to manually and ad-hoc extract fields from log messages within a query is provided via parse operators.One of technique to make the most of data is using this method. Let's explore some of the parse operators that Sumo Logic offers.

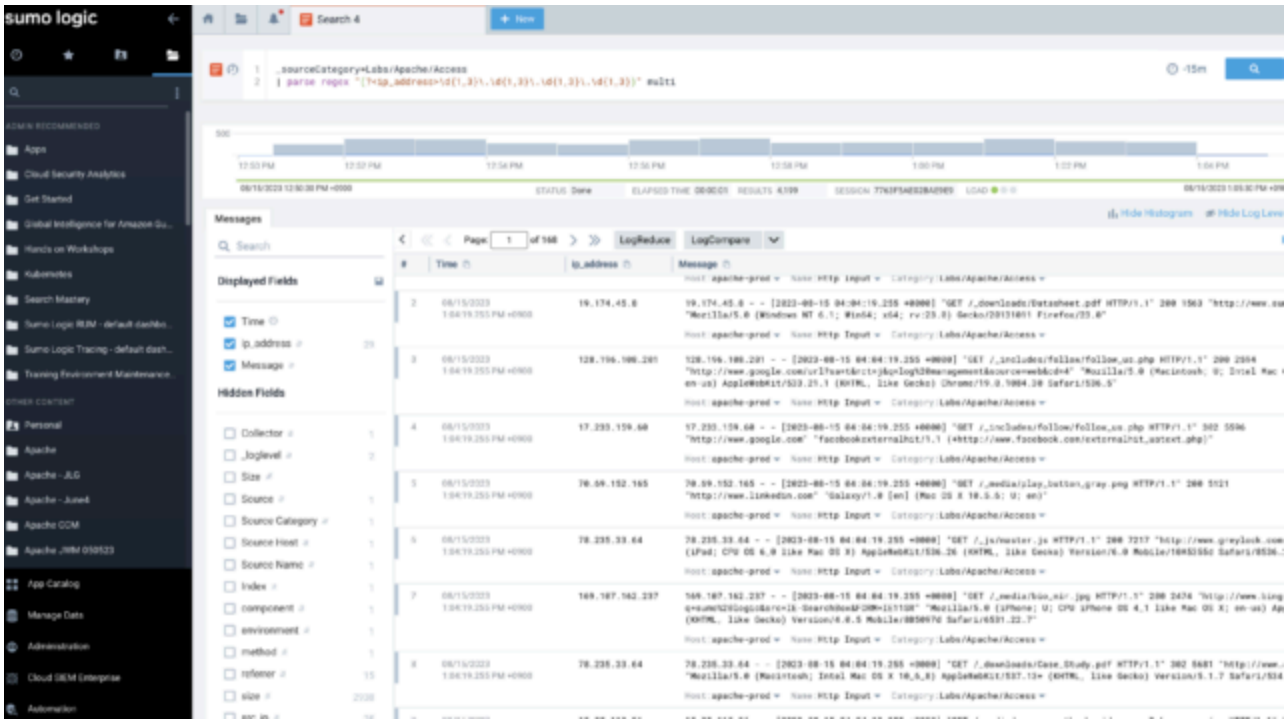
Parse Variable pattern using Regix

The Parse Regex operator, also known as the extract operator, is designed for users who are familiar with the syntax of regular expressions. You may easily extract complex data from log lines with this operator.

Parsing a simple IP address



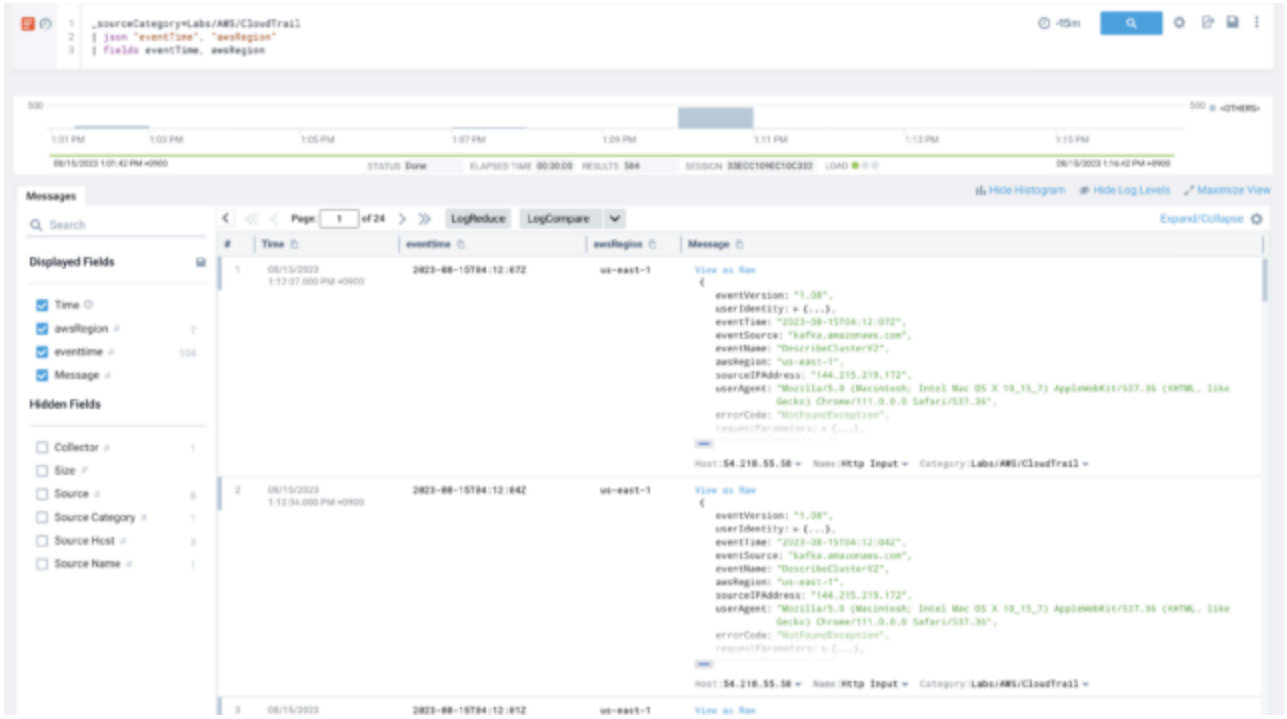
Parse multi



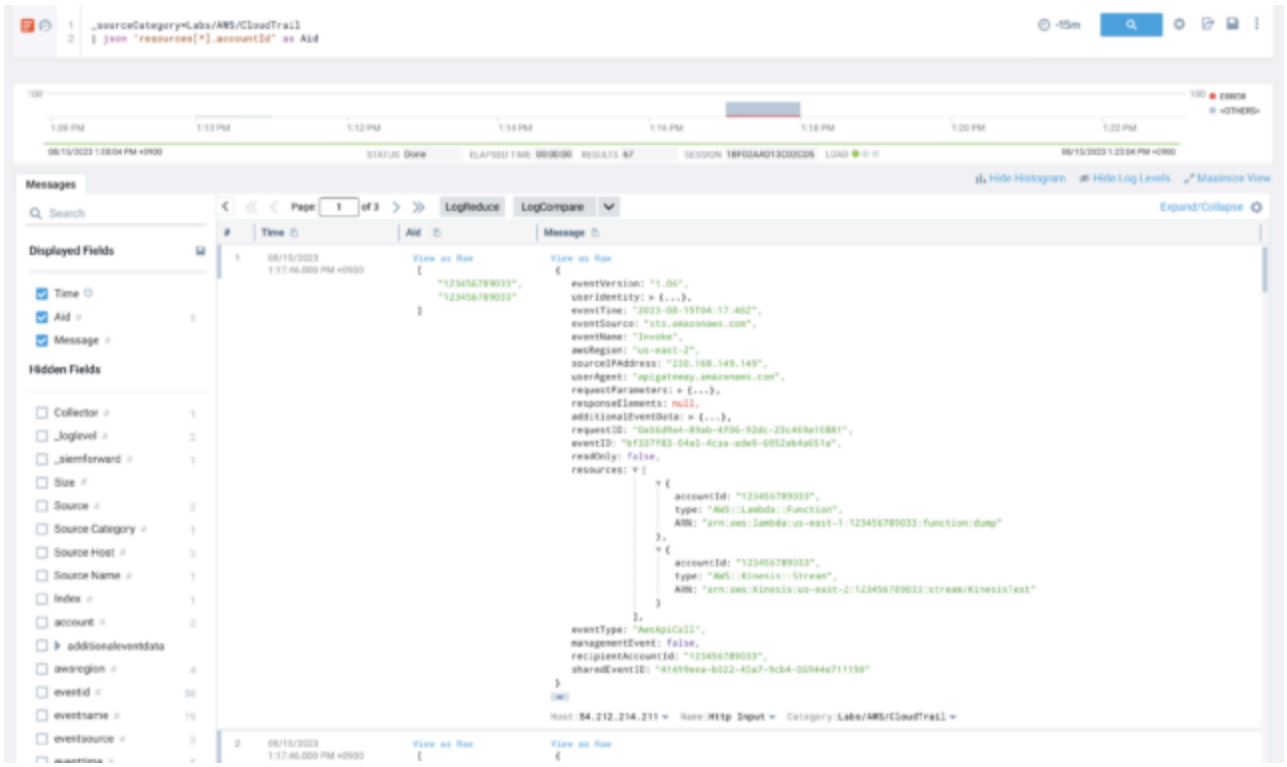
Parse JSON Formatted Logs

JSON logs are full of structured data. The JSON operator, combined with strong JSONPath expressions, allows you to precisely extract certain values from these logs.

Extracting multiple fields

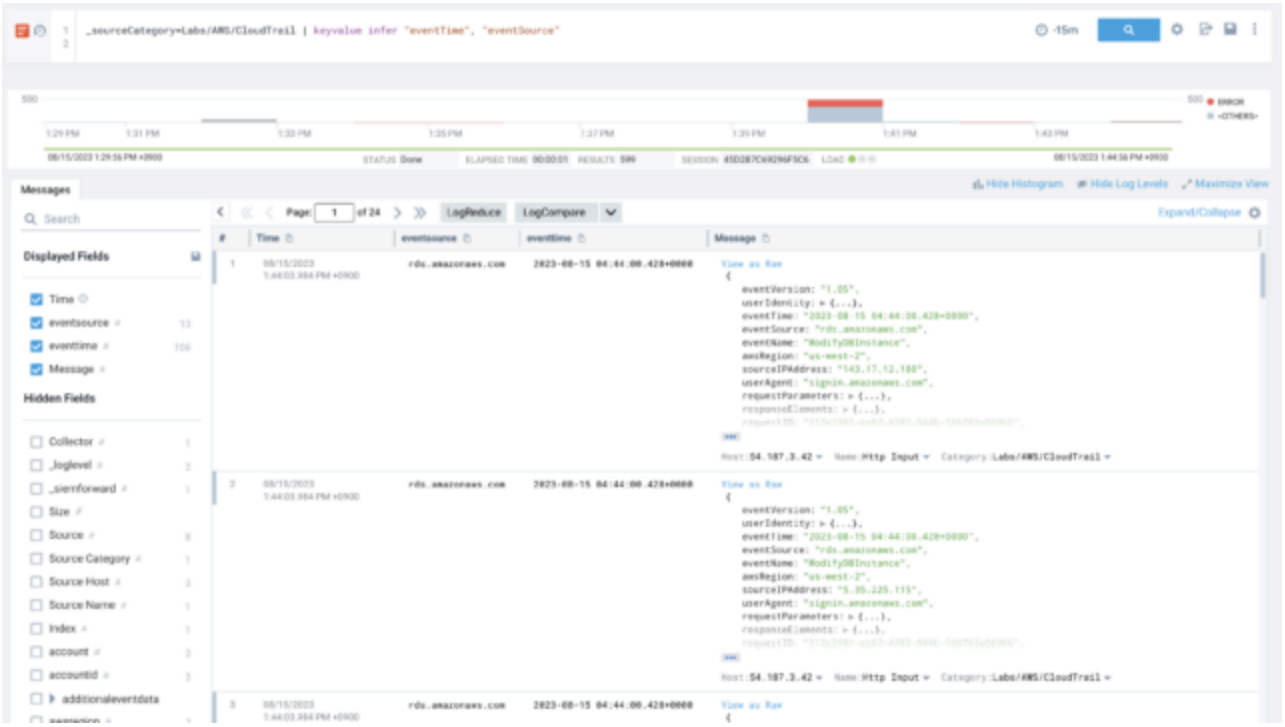


Using Nested Array with wildcard



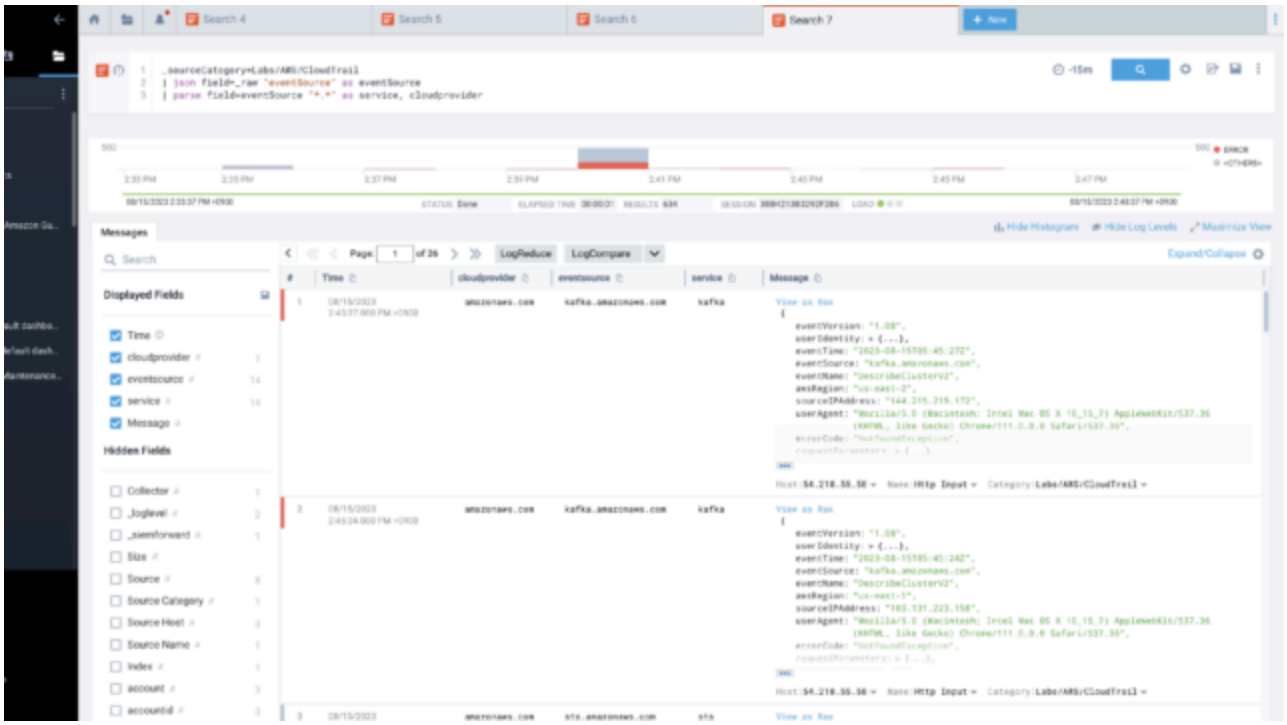
Parse Keyvalue Formatted Logs

Key-value pairs are a common structure for log files. By defining the key associated with each value, the key-value operator enables you to extract values from a log message.



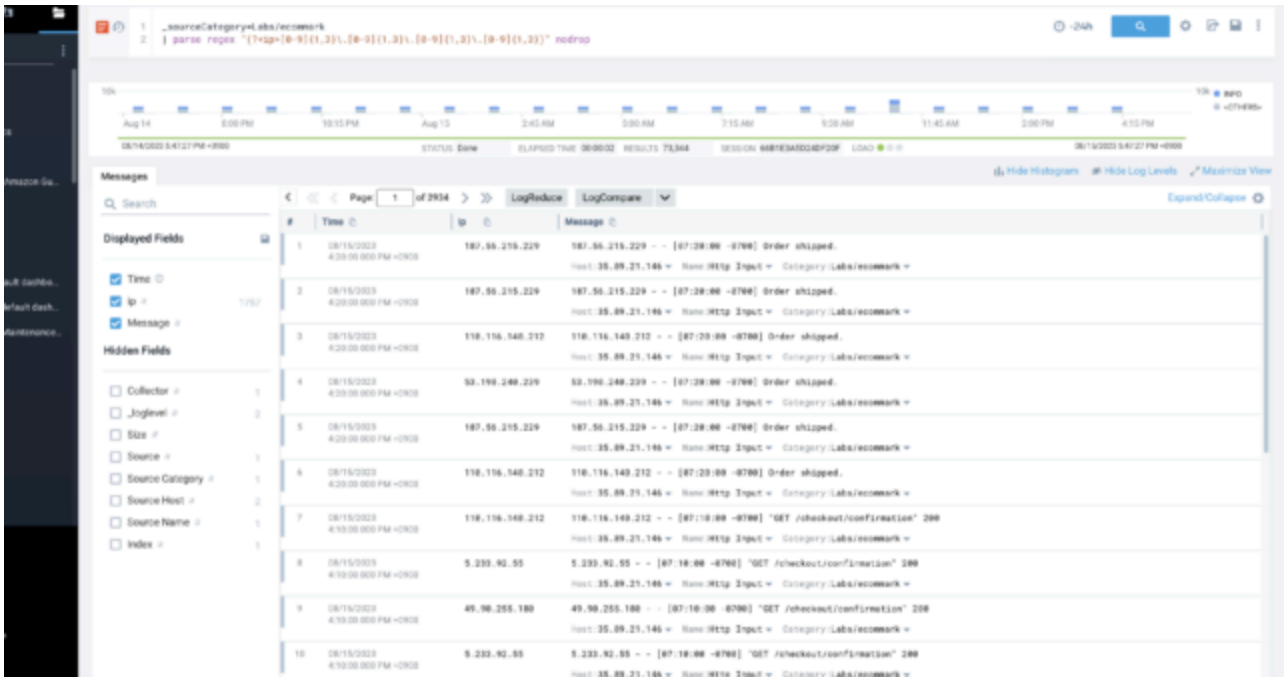
Parse field option

This is the idea of using the "field" syntax to parse previously extracted fields or metadata fields..



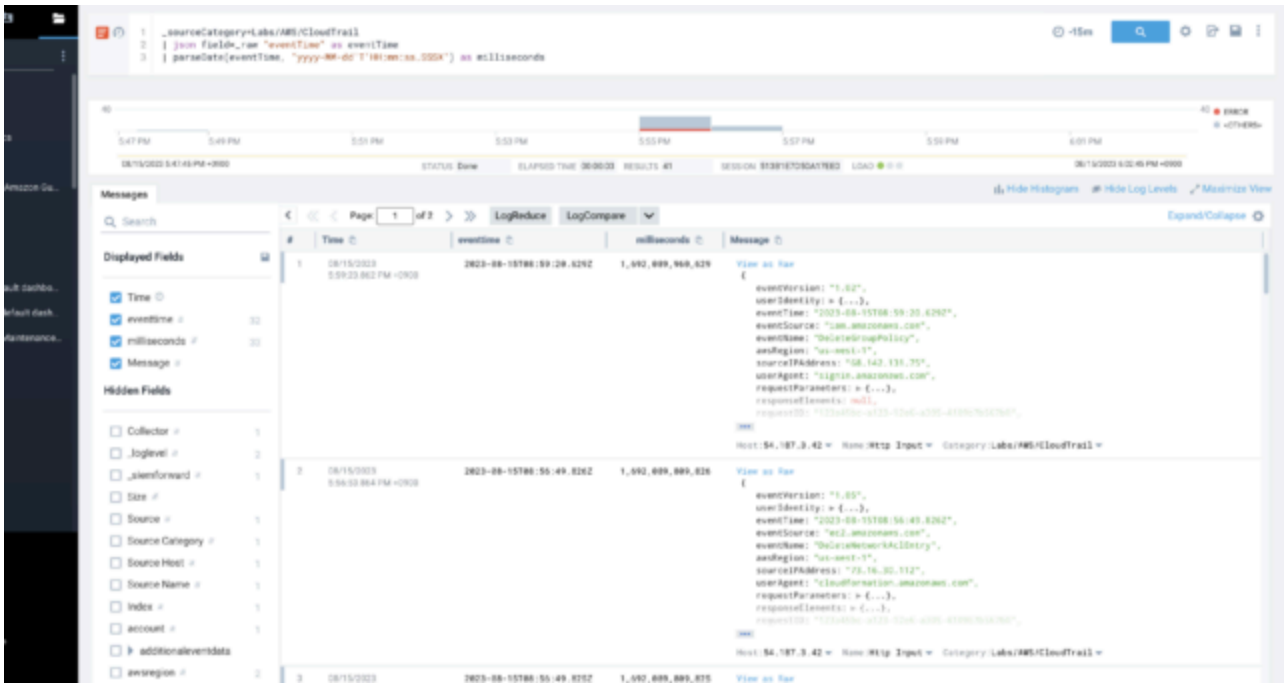
Parse Nodrop option

Even unmatched segments of parse expressions are included in the results with the Nodrop option, ensuring that no valuable data is lost.



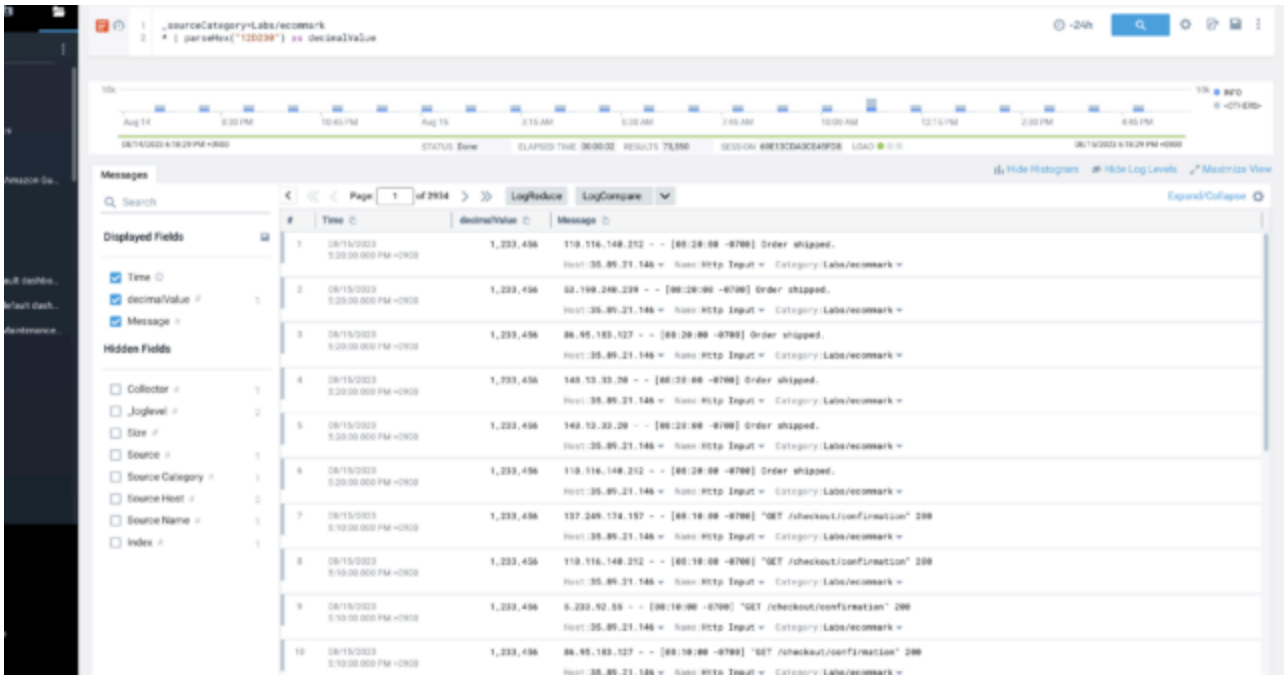
parseDate

The parseDate operator extracts date and time information from strings, delivering millisecond-accurate timestamps.



parseHex

The parseHex operator makes it simple to convert hexadecimal strings into numerical values.



Conclusion

I hope you now have a better knowledge of parse operators. These are some of the operators available that can be used to transform raw data into meaningful insights.

EVENTS

【1/29（木）】クラスメソッドの会社説明会を開催します

開催前

【1/28（水）】クラスメソッドの新卒向け会社説明会を開催します

開催前

【CMグループ/エンド直案件特集】ITフリーランス向け 「CMパートナーズ」 説明会 by クラスメソッド

開催前

【2/5（木）東京】オペレーターの生産性を50%アップ！見て、聞いて、納得できるAIコールセンター実演セミナー

開催前

【2/25（水）】AI駆動開発、実際どうなの？【実践編】～現場でぶつかる課題と乗り越え方～

開催前

【1/29（木）】今日から始めるAWSセキュリティ対策 3ステップでわかる実践ガイド

開催前

セミナー一覧　会社説明会一覧　勉強会一覧