

# sumo logic

## 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

The screenshot displays the Splunk Enterprise interface. On the left is a sidebar with navigation options like 'Recent Searches', 'Dashboards', and 'Data Sources'. The main panel shows a search bar with the query: `sourceCategory=Lab/ApacheAccess`. Below the search bar, a 'Messages' table lists search results. The table has columns for '#', 'Time', 'ip\_address', and 'Message'. The 'ip\_address' column is highlighted, indicating it is the selected field for parsing. The 'Message' column shows log entries from 'Host: apache-prd' with various HTTP requests and responses. The interface also includes a 'Log Explorer' sidebar on the left and a 'Log Console' on the right.

#	Time	ip_address	Message
1	06/15/2023 12:04:34 PM +0000	78.234.33.64	78.234.33.64 - - [2023-06-15 00:40:34.546 +0000] "GET /chopping/chickenfire.jpg HTTP/1.1" 200 5268 "http://www.3img.com/search?q=word2Log&src=00-Search&POM=001106" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_5_8) AppleWebKit/537.51+ (KHTML, like Gecko) Version/5.1.7 Safari/530.37.3" 2/2478586
2	06/15/2023 12:04:34 PM +0000	84.112.91.96	84.112.91.96 - - [2023-06-15 00:40:34.546 +0000] "GET /_news/News/Case_Study.pdf HTTP/1.1" 200 2529 "http://www.soonlogis.com" Mozilla/5.0 (Linux; U; en-US; AppleWebKit/537.5+ (KHTML, like Gecko; Safari/537.5+) Version/6.0 Randact/6 (screen 800x600; retina) 6/6/2008
3	06/15/2023 12:04:34 PM +0000	189.187.162.227	189.187.162.227 - - [2023-06-15 00:40:34.546 +0000] "GET /chopping/chickenfire.jpg HTTP/1.1" 200 5529 "http://www.soonlogis.com" Randact-media/1.1 (http://www.sh.com/worket/Ann) 7/7/2022
4	06/15/2023 12:04:34 PM +0000	181.129.137.178	181.129.137.178 - - [2023-06-15 00:40:29.336 +0000] "GET /blog/index.php HTTP/1.1" 200 8410 "http://www.graylock.com" Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.5407.8 Safari/557.36
5	06/15/2023 12:04:29.336 PM +0000	65.98.119.36	65.98.119.36 - - [2023-06-15 00:40:29.336 +0000] "GET /_css/selector.134358838.css HTTP/1.1" 200 2771 "http://www.3img.com/search?q=word2Log&src=00-Search&POM=001106" Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.5407.8 Safari/557.36
6	06/15/2023 12:04:29.336 PM +0000	8.38.228.115	8.38.228.115 - - [2023-06-15 00:40:29.336 +0000] "GET /_includes/ev/blog/wp-content/plugins/wp-1043768-hofull.php?src=00-Search&POM=001106 HTTP/1.1" 200 7931 "http://www.soonlogis.com" Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0; 3rdParty; 2; 301; MSN 6.0.2.6.54715; 6/6/2008)
7	06/15/2023 12:04:29.336 PM +0000	221.129.19.252	221.129.19.252 - - [2023-06-15 00:40:29.336 +0000] "GET /_media/resource/thumb_video_ay_v2 homepage.jpg HTTP/1.1" 200 7932 "http://www.graylock.com" Galaxy/1.0 (en; Mac OS X 10.5.4; fr; en)
8	06/15/2023 12:04:29.336 PM +0000	49.212.129.16	49.212.129.16 - - [2023-06-15 00:40:29.336 +0000] "GET /_media/resource/thumb_video_ay_v2 homepage.jpg HTTP/1.1" 200 1239 "http://search.yahoo.com/mozilla/feature=764.terragridfirst?ip=ssoonlogis.com&ip=ter" Mozilla/5.0 (compatible; Googlebot/2.0; http://www.google.com/bot.html)

## Parse multi

The screenshot shows the Sumo Logic interface. On the left is a sidebar with navigation options like 'APPS', 'Cloud Security Analytics', and 'Global Intelligence for Amazon S3...'. The main area displays a search query: `sourceCategory=Labs/Apache/Access` and `| parse regex "[?&@_address=](1,3)%-(1,3)%-(1,3)%-(1,3)" multi`. Below the query is a timeline visualization. The 'Messages' section shows a table of log entries with columns for ID, Time, IP address, and Message. The table contains 8 entries, each representing an HTTP request from various sources like '19.174.45.8' and '128.198.198.231'.

ID	Time	IP address	Message
2	06/15/2023 12:53:00 PM +0000	19.174.45.8	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_downloads/DataSet.pdf HTTP/1.1 200 1563 "http://www.su... Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:29.0) Gecko/20101001 Firefox/35.0"
3	06/15/2023 1:04:19:253 PM +0000	128.198.198.231	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_includes/footer/footer_en.php HTTP/1.1 200 2594 "http://www.google.com/url?url=http://log2log.com/&source=web&id=4" Mozilla/5.0 (Macintosh; U; Intel Mac... AppleWebKit/533.21.1 (KHTML, like Gecko) Chrome/19.0.984.28 Safari/536.5"
4	06/15/2023 1:04:19:253 PM +0000	17.235.159.68	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_includes/footer/footer_en.php HTTP/1.1 200 2594 "http://www.google.com" Facebookexternalhit/1.1 (http://www.facebook.com/externalhit_xestext.php)"
5	06/15/2023 1:04:19:253 PM +0000	78.69.152.165	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_media/play/button_gray.png HTTP/1.1 200 5121 "http://www.linkedin.com" Galaxy1.0 [en] (Mac OS X 10.5.5; U; en)"
6	06/15/2023 1:04:19:253 PM +0000	78.235.33.64	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_includes/footer/footer_en.php HTTP/1.1 200 2594 "http://www.graylog.com (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5350 Safari/8536.1"
7	06/15/2023 1:04:19:253 PM +0000	169.167.162.237	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_media/bio_nir.jpg HTTP/1.1 200 2474 "http://www.bing.com/qum/h2logos&rs=16-Search&ID=161108" Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_1 like Mac OS X; en-us) Ap... (KHTML, like Gecko) Version/6.0.5 Mobile/9A5346 Safari/533.2.7"
8	06/15/2023 1:04:19:253 PM +0000	78.235.33.64	Host: apache-gre... User: Http Input = Category: Labs/Apache/Access = GET /_downloads/Case_Study.pdf HTTP/1.1 200 5481 "http://www... Mozilla/5.0 (Macintosh; Intel Mac OS X 10_5_8) AppleWebKit/537.13 (KHTML, like Gecko) Version/5.1.7 Safari/534...

## 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

1 `_sourceCategory=AWS/CloudTrail`  
2 `json "eventTime", "awsRegion"`  
3 `fields eventTime, awsRegion`

100

1:01 PM 1:03 PM 1:05 PM 1:07 PM 1:09 PM 1:11 PM 1:13 PM 1:15 PM

06/15/2023 1:01:42 PM +0000 STATUS Date ELAPSED TIME 00:00:00 RESULTS 584 SESSION 336C26106C3C333 LOAD 0 0 0 06/15/2023 1:16:42 PM +0000

Messages

Search

Page 1 of 24 LogReduce LogCompare

Expand/Collapse

Displayed Fields

- ☒ Time
- ☒ awsRegion
- ☒ eventTime
- ☒ Message

Hidden Fields

- ☐ Collector
- ☐ Size
- ☐ Source
- ☐ Source Category
- ☐ Source Host
- ☐ Source Name

#	Time	eventTime	awsRegion	Message
1	06/15/2023 1:12:37.000 PM +0000	2023-06-15T04:12:37Z	us-east-1	<pre>eventVersion: "1.08", userIdentity: { ... }, eventTime: "2023-06-15T04:12:37Z", eventSource: "kafka.amazonaws.com", eventName: "DescribeClusterV2", awsRegion: "us-east-1", sourceIPAddress: "144.215.219.172", userAgent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.6.0 Safari/537.36", errorCode: "NotFoundException", requestParameters: { ... },</pre>
2	06/15/2023 1:12:34.000 PM +0000	2023-06-15T04:12:34Z	us-east-1	<pre>eventVersion: "1.08", userIdentity: { ... }, eventTime: "2023-06-15T04:12:34Z", eventSource: "kafka.amazonaws.com", eventName: "DescribeClusterV2", awsRegion: "us-east-1", sourceIPAddress: "144.215.219.172", userAgent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.6.0 Safari/537.36", errorCode: "NotFoundException", requestParameters: { ... },</pre>
3	06/15/2023	2023-06-15T04:12:35Z	us-east-1	<pre>Host: 54.218.55.56 - Name: Http Input - Category: Labs/AWS/CloudTrail -</pre>

# Using Nested Array with wildcard

1 `_sourceCategory=AWS/CloudTrail`  
2 `json "resources[*].accountId" as Aid`

100

1:08 PM 1:10 PM 1:12 PM 1:14 PM 1:16 PM 1:18 PM 1:20 PM 1:22 PM

06/15/2023 1:08:04 PM +0000 STATUS Date ELAPSED TIME 00:00:00 RESULTS 87 SESSION 18F0DAD3302C295 LOAD 0 0 0 06/15/2023 1:22:04 PM +0000

Messages

Search

Page 1 of 3 LogReduce LogCompare

Expand/Collapse

Displayed Fields

- ☒ Time
- ☒ Aid
- ☒ Message

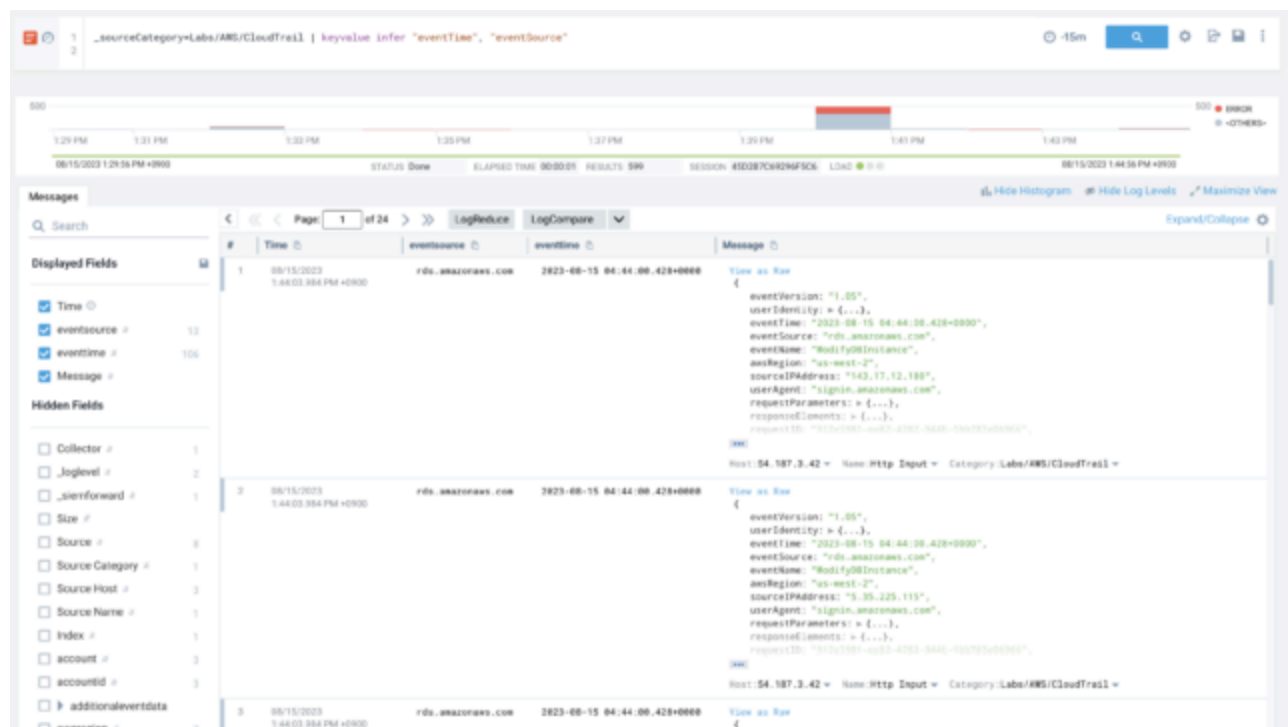
Hidden Fields

- ☐ Collector
- ☐ \_loglevel
- ☐ \_siemforward
- ☐ Size
- ☐ Source
- ☐ Source Category
- ☐ Source Host
- ☐ Source Name
- ☐ Index
- ☐ account
- ☐ additionalEventData
- ☐ awsRegion
- ☐ eventId
- ☐ eventName
- ☐ eventSource

#	Time	Aid	Message
1	06/15/2023 1:17:46.000 PM +0000	<pre>[   "123456789033",   "123456789033" ]</pre>	<pre>eventVersion: "1.06", userIdentity: { ... }, eventTime: "2023-06-15T04:17:46Z", eventSource: "sts.amazonaws.com", eventName: "Invoke", awsRegion: "us-east-2", sourceIPAddress: "230.168.149.149", userAgent: "apiGateway.amazonaws.com", requestParameters: { ... }, responseElements: null, additionalEventData: { ... }, requestID: "c65d9af-8fab-8706-926c-25c40fa16881", eventId: "9f237f83-64a5-4c6a-9d69-6052ab4d651a", readOnly: false, resources: [   {     accountId: "123456789033",     type: "AWS::Lambda::Function",     ARN: "arn:aws:lambda:us-east-1:123456789033:function:dump"   },   {     accountId: "123456789033",     type: "AWS::Kinesis::Stream",     ARN: "arn:aws:kinesis:us-east-2:123456789033:stream/KinesisTest"   } ], eventType: "AwsApiCall", managementEvent: false, recipientAccountId: "123456789033", sharedEventID: "414596ea-b022-45a7-8cb4-60644e711190" }</pre>
2	06/15/2023 1:17:46.000 PM +0000		<pre>Host: 54.212.214.211 - Name: Http Input - Category: Labs/AWS/CloudTrail -</pre>

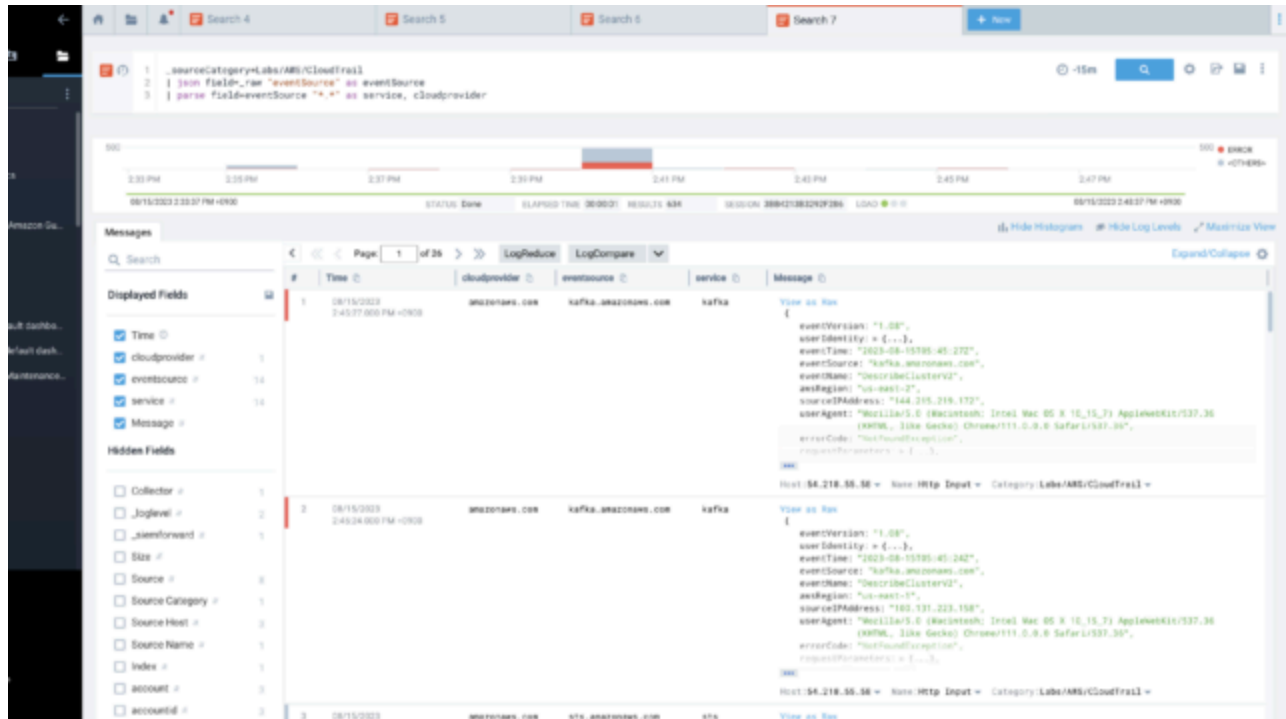
# Parse Keyvalue Formatted Logs

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.



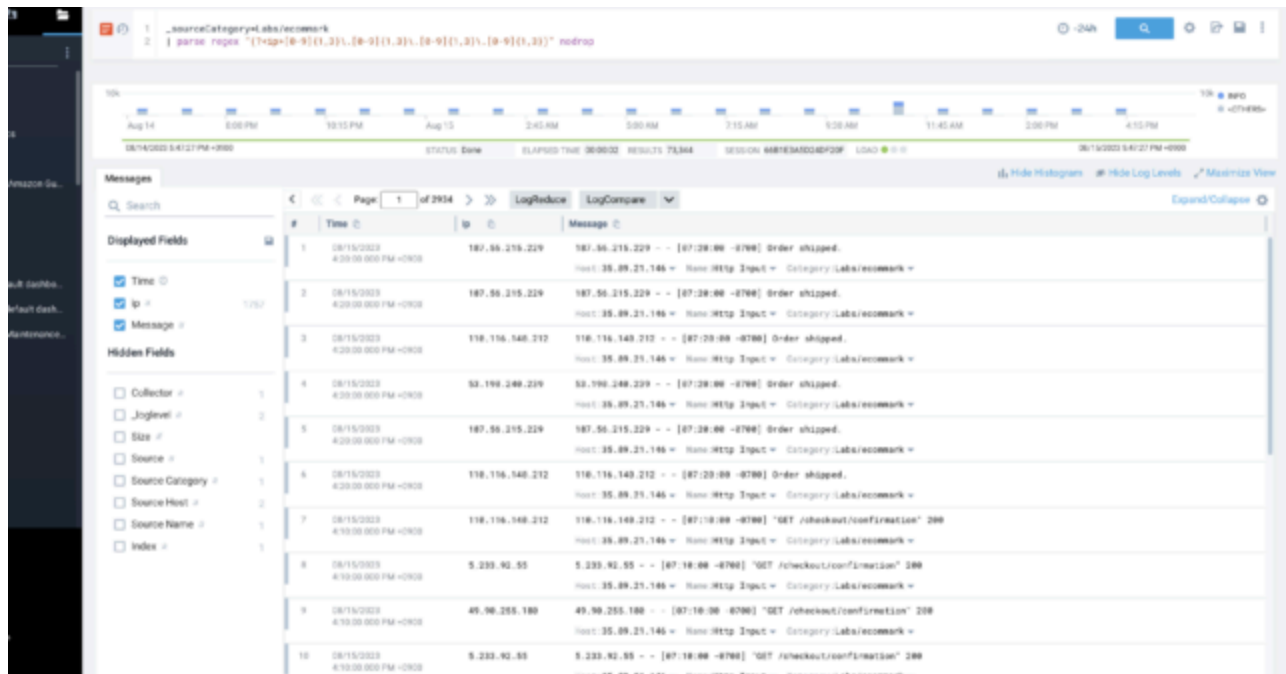
## Parse field option

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



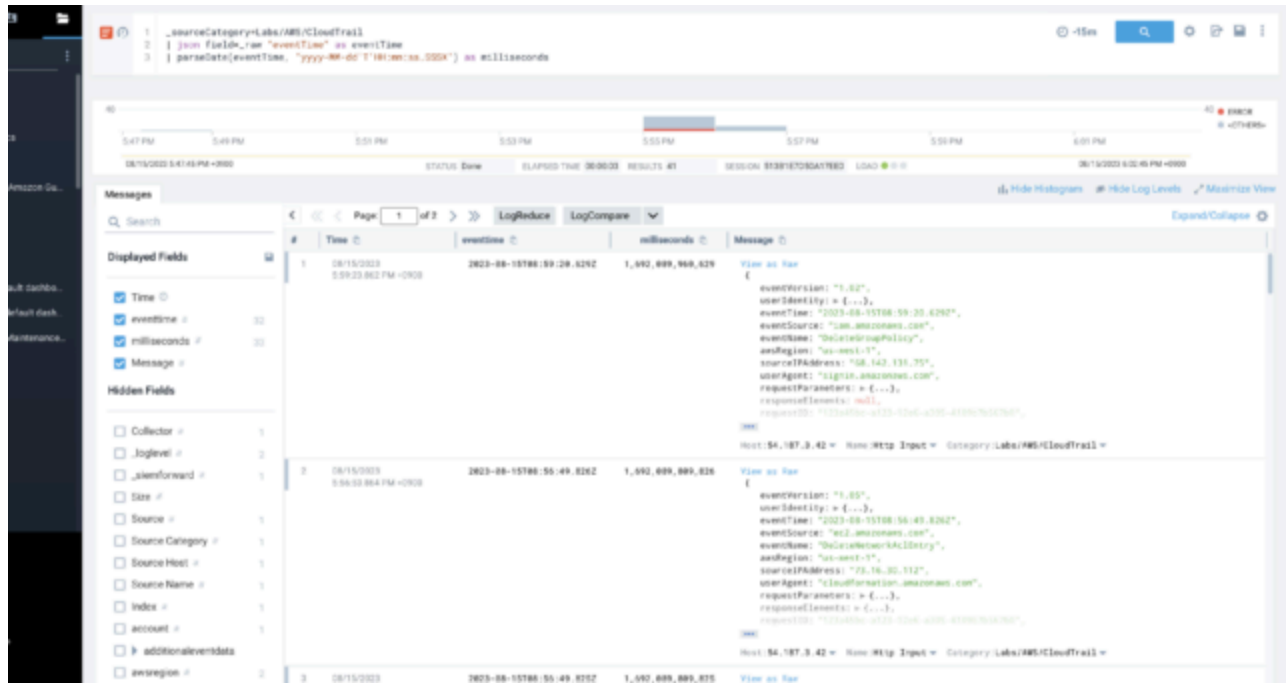
## Parse Nodrop option

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



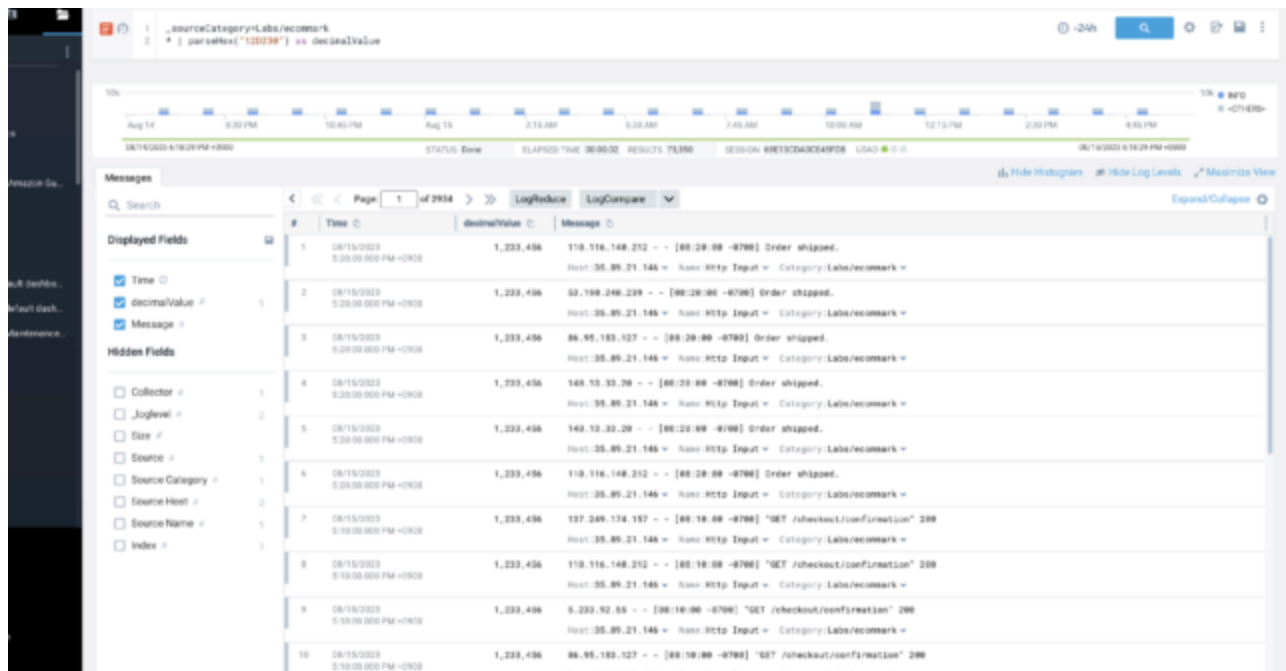
## parseDate

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](#)