

[Sumo Logic] Logarithmic Operator Cheat Sheet: Naver Blog

bl blog.naver.com/PostView.naver



[Monitoring](#)

[Sumo Logic] Logarithmic Operator Cheat Sheet

[Tech Tour](#) July 27, 2020, 2:29 AM

Previously, we covered how to install and verify the Collector for log collection using the Summo Logic. This blog post will cover how to query the massive amount of collected log data for the data you need.

The Log Operators Cheat Sheet in SumoLogic is a guideline that explains the available parsers, aggregators, search operators, and mathematical expressions to use in your queries.

<https://help.sumologic.com/05Search/Search-Cheat-Sheets/Log-Operators-Cheat-Sheet>

[Log Operators Cheat Sheet](#)

[The Search Operators cheat sheet provides a list of available Sumo Logic parsers, aggregators, search operators, and mathematical expressions with links to full details for each item.](#)

help.sumologic.com

Let me give you a representative example.

1) Parsing - parse

Store the contents inside "" in the user label . # The label variable will be used later for sorting , grouping , and other functions . | parse "User=*" as user

2) Parsing - parse/regex

#Using regular expressions to extract data needed for search in log lines | parse regex field = url "[0-9A-Za-z-]+\\. (? < domain > [A-Za-z-]+\\. (? : co\\. uk | com | com\\. au)) / . * "

3) Aggregator - avg

Provides the average value for a field with numeric values, grouped by value after by | avg (request_received) by _timeslice

4) Aggregator - count

#Group - Output the total value in By format | count by url #When counting only unique values, excluding duplicates | count_distinct (referrer) by status_code

5) Aggregator - min, max

#Print the largest value in the data set | max (request_received) by hour

6) Search - accum

accum = accumulative -> used in dashboards

_sourceCategory = IIS (Wyatt OR Luke) | parse "[user=*]" as cs_username | timeslice by 1m | count as requests by _timeslice , cs_username | sort by _timeslice asc , cs_username | accum requests as running_total

7) Search - limit

Define the number of search data

| count by _sourceCategory | sort by _count | limit 5

8) Math - abs, round, ceil, ...

```
| abs ( - 1.5 ) as v // v = 1.5 | round ( ( bytes / 1024 ) / 1024 ) as MB | ceil ( 1.5 ) as v // v = 2 | floor  
( 1.5 ) as v // v = 1 | max ( 1 , 2 ) as v // v = 2 | min ( 1 , 2 ) as v // v = 1 | sqrt ( 4 ) as v // v = 2 | cbrt  
( 8 ) as v // v = 2
```