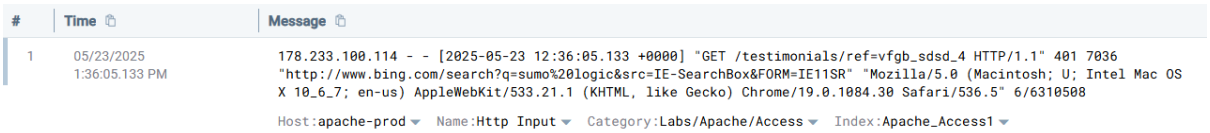
Parsing logs in SUMO Logic is crucial because it modifies the raw log data into structured fields. That makes the search queries more accurate with better results.

Examples

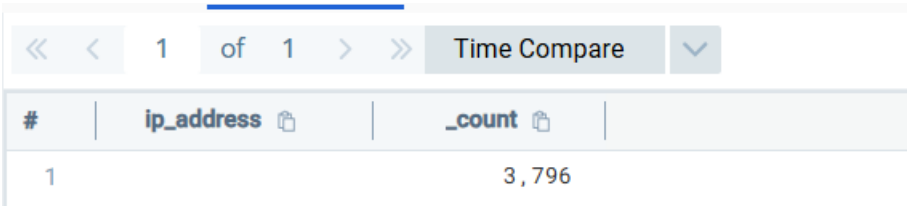
In the first example, we will perform an unparsed log search. As a result, we will receive unparsed logs from the source category starting with “Labs/Apache” within the last 15 minutes.

*Query - _sourcecategory=Labs/Apache/**



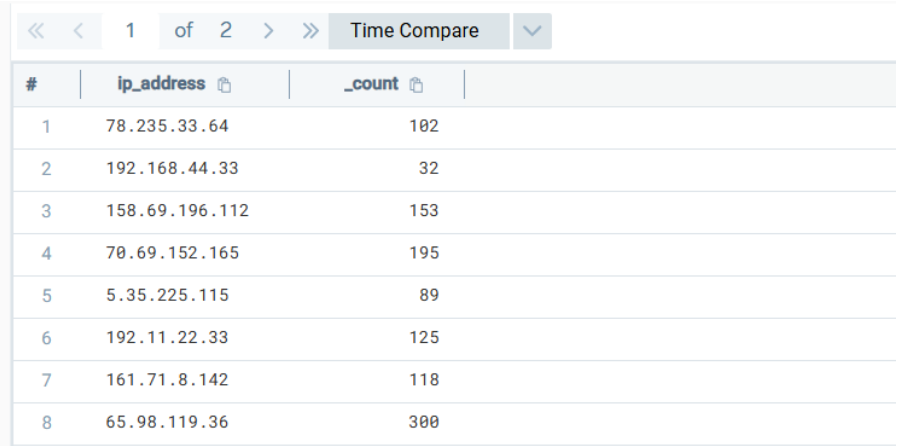
Under the message section, we can notice the IP address 178.233.100.114. Being an unparsed log, SUMO will not recognize this IP address as a separate field. Therefore, a result of a search query to count the occurrence of each IP address will bring back a general result.

*Query - _sourcecategory=Labs/Apache/**
| count by ip_address



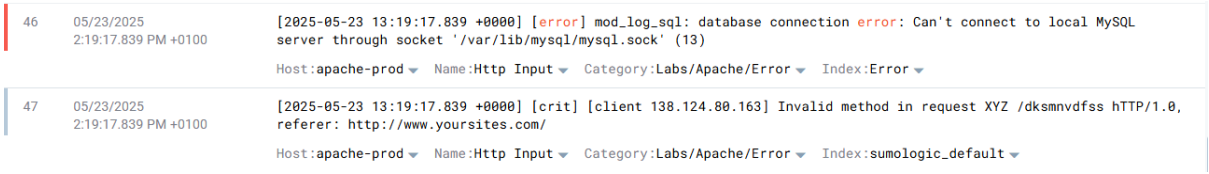
In the second example, we will use a query parsed with the help of a regular expression (RegEx). A regular expression looks for a given pattern and returns the requested result creating a specific field. Using a query below, we can see the desired outcome.

*Query - _sourceCategory=Labs/Apache/**
| parse regex
"(?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| count by ip_address



For the third example, we can use the unparsed Apache/Error source category first.

Query - _sourceCategory=Labs/Apache/Error



From the unparsed search result, we want to individualize two entities: the first one will be the client IP address, and the second will be the mod_log_sql message. To refine our search query, we have to input the text below in the search field.

_sourceCategory=Labs/Apache/Error
*| parse "[client *]" as client_ip nodrop*
*| parse "mod_log_sql: *" as message nodrop*

In the final search, we see separate fields for the client_ip and mod_log_sql message. In SUMO Logic, by default, when using the “parse” command, only log lines that match the pattern are kept. “Nodrop” keyword prevents this behaviour by not “dropping” those log lines, but showing every log instead.