SUMO Logic conditional operators IF and SUM are often used together to create aggregations. They are used to generate results as counts, averages, and sums based on a defined query. They are used very often in dashboards or alerts.

IF operator

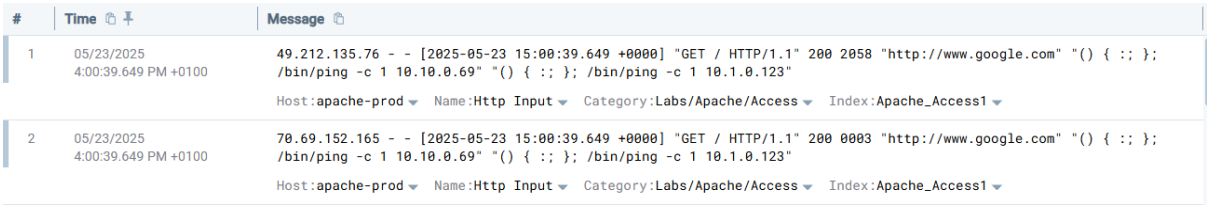
- Allows you to evaluate if a condition is true or false and return different values based on this factor.
- Using a query '| if(status_code=500, 1, 0) as is_error' will return 1 if status_code is 500, otherwise, it's 0.

SUM operator

- This operator adds up values in the field.
- Using a query '| if(status_code=500, 1, 0) as error_flag
  | sum(error_flag) as total_500_errors' will count how many times error 500 has occurred.

We can see how those operators work on an example. In the first step, we will query all of the Labs/Apache/Access logs.

Query - _sourceCategory=Labs/Apache/Access



#	Time	Message
1	05/23/2025 4:00:39.649 PM +0100	49.212.135.76 - - [2025-05-23 15:00:39.649 +0000] "GET / HTTP/1.1" 200 2058 "http://www.google.com" "() { :; }; /bin/ping -c 1 10.10.0.69" "() { :; }; /bin/ping -c 1 10.1.0.123" Host:apache-prod Name:Http Input Category:Labs/Apache/Access Index:Apache_Access1
2	05/23/2025 4:00:39.649 PM +0100	70.69.152.165 - - [2025-05-23 15:00:39.649 +0000] "GET / HTTP/1.1" 200 0003 "http://www.google.com" "() { :; }; /bin/ping -c 1 10.10.0.69" "() { :; }; /bin/ping -c 1 10.1.0.123" Host:apache-prod Name:Http Input Category:Labs/Apache/Access Index:Apache_Access1

We can see unparsed logs with the status code 200 in the log message. In the next step, we will parse the status code as a separate field.

Query - _sourceCategory=Labs/Apache/Access
*| parse "HTTP/1.1\" * " as status_code*

#	Time	status_code	Message
1	05/23/2025 4:02:39.650 PM +0100	200	17.233.159.60 - - [2025-05-23 15:02:39.650 +0000] "GET / HTTP/1.1" 200 2474 "http://www.google.com" "() { :; }; /bin/ping -c 1 10.10.0.69" "() { :; }; /bin/ping -c 1 10.1.0.123" Host:apache-prod Name:Http Input Category:Labs/Apache/Access Index:Apache_Access1
2	05/23/2025 4:02:39.650 PM +0100	200	65.98.119.36 - - [2025-05-23 15:02:39.650 +0000] "GET / HTTP/1.1" 200 2347 "http://www.google.com" "() { :; }; /bin/ping -c 1 10.10.0.69" "() { :; }; /bin/ping -c 1 10.1.0.123" Host:apache-prod Name:Http Input Category:Labs/Apache/Access Index:Apache_Access1

As a result, the status code is visible in a separate field. In the last step, we will count the number of status code 200 (meaning that the request to the server was successful) and status code 404 (indicating that the requested source could not be found).

Query - _sourceCategory=Labs/Apache/Access
*| parse "HTTP/1.1\" * " as status_code*
| if(status_code=200, 1, 0) as successes
| if(status_code=404, 1, 0) as client_errors

| sum(successes) as success_cnt, sum(client_errors) as client_errors_cnt

#	success_cnt	client_errors_cnt
1	2,541	101

In the final step, we can see the number of successful requests, and the number of requests with status code 404 (Not Found).