SUMO Logic statistical operators DIFF and SMOOTH are used in queries to detect changes over time and reduce noise in time series data. They are very useful in anomaly detection and trend analysis.

DIFF Operator

- Calculates the difference between a specified value in a current time slice and a previous time slice.
- The following query '| count by _timeslice
  | diff(_count) as count_change' will count the difference in log ingestion, which could be useful in noticing spikes and drops.

SMOOTH Operator

- Counts the moving average to make trends more visible
- The following query '| count by _timeslice
  | smooth count as smoothed_count' will let you see the rolling average of all the requests.

Example

In the first example, we use the diff operator. We will query all the logs from the Labs/Apache/Access server, divide them into 1-minute time bins, count the number of logs per minute, sort them, started by the oldest first and count the difference between each time bin.

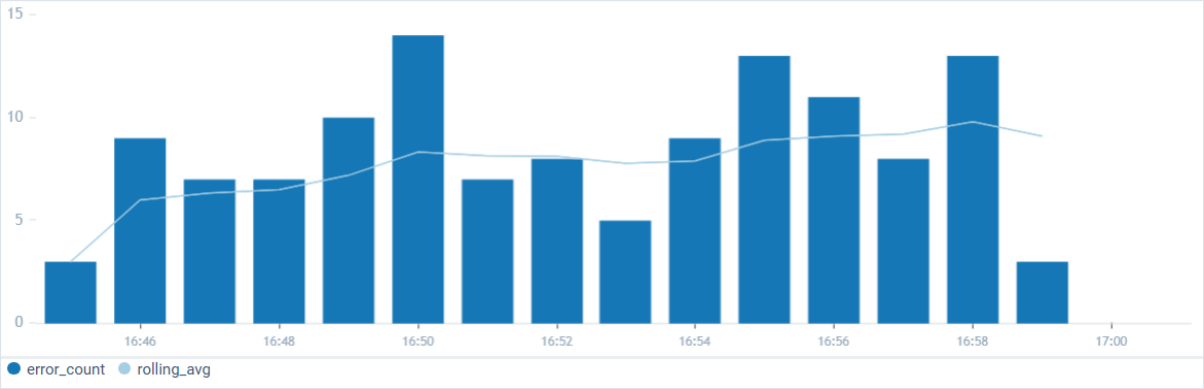
Query - _sourceCategory=Labs/Apache/Access
| timeslice 1m
| count by _timeslice
| sort by _timeslice asc
| diff _count

#	Time	_count	_diff
1	05/23/2025 4:42:00.000 PM +0100	139	
2	05/23/2025 4:43:00.000 PM +0100	254	-115
3	05/23/2025 4:44:00.000 PM +0100	275	-21
4	05/23/2025 4:45:00.000 PM +0100	249	26
5	05/23/2025 4:46:00.000 PM +0100	258	-9
6	05/23/2025 4:47:00.000 PM +0100	209	49
7	05/23/2025 4:48:00.000 PM +0100	196	13
8	05/23/2025 4:49:00.000 PM +0100	226	-30
9	05/23/2025 4:50:00.000 PM +0100	364	-138

In the _diff column, we can see the difference between each 1-minute time bin.

In the second example, we will count the number of failed attempts (error 404), count the rolling average, and present them in a visual graph.

Query - _sourceCategory=Labs/Apache/Access and status_code=404
| timeslice 1m
| count as error_count by _timeslice
| sort by _timeslice asc
| smooth error_count as rolling_avg



In this graph, we can see the error count in the blue columns and the rolling average in the thin blue line.