Metric alerts aggregation type

Last updated by | Lisa Liu | Nov 6, 2020 at 10:35 AM PST

If you ever wonder what to choose while setting up aggregation type for metric based alerts...

I have seen many customers have a question regarding how the “Aggregation Types” in a Metric Alert work. Following explanation might help.

To start, the “Aggregation Type” is basically an aspect of how the Alert’s “Threshold” is utilized.

If we use your screenshot configuration as the example, we have an alert that evaluates every one minute (Frequency) and aggregates data over a 5 minute timeframe (Period). This means that every minute, the alert looks at the data over the last 5 minutes, and then compares those values to your chosen threshold (which here looks to be 80).

The “Aggregation Type” chooses how the data in those 5 minutes is compared to that 80.

- If the “Aggregation Type” is “Average,” it will calculate the average of the values over the 5 minute Period, and compare the Average to your value of 80.
- If the “Aggregation Type” is “Maximum” it will compare the highest value in the 5 minute Period to the chosen threshold of 80.

To explain this with an example, imagine the 5 minutes of values were [75, 80, 65, 90, 60].

- If we used an “Aggregation Type” of “Average,” the calculation would add the above values together and take the Average, which is 74. 74 does not exceed 80, and so the Alert would not fire.
- If we used an “Aggregation Type” of “Maximum” the calculation would find the highest of the above values, and compare 90 to 80, which would cause the Alert to fire.

Ultimately the decision for what Aggregation type should be chosen comes down to what is expected from the Metric values, and what behaviors you are interested in alerting against. Metrics such as CPU Percentage are most often viewed through Averages, whereas counts related to Security events might be more concerned with Maximum values, etc.

How good have you found this content?