Why did my CloudWatch alarm trigger when its metric doesn't have any breaching data points?

Issue

My Amazon CloudWatch alarm changed to the ALARM state. When I check the alarm metric, I don't see any breaching data points. However, the event history for the alarm shows the breaching data point.

Short Description

CloudWatch alarms evaluate metrics based on data points available at a specific moment. Each subsequent alarm evaluation might use different aggregated data points, because new data points continue to flow into the CloudWatch metric. You might not be able to see a breaching data point that triggered your alarm if that data hasn't flowed into the metric yet. When you review the event history later, you can see the complete set of data points, which have now flowed into the metric.

Resolution

To observe a breaching data point in your CloudWatch alarm metric's graph, change the Statistic to Maximum/Minimum.

To help prevent an alarm from changing to the ALARM state, configure an "M out of N" alarm where Evaluation Period and Datapoints to Alarm have different values. This configuration makes alarms evaluate more aggregated data points and changes the alarm state only if at least a certain number of data points (M) is breaching in a given set of data points (N). For more information, see [Create a CloudWatch Alarm Based on a CloudWatch Metric](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ConsoleAlarms.html) and [Configuring How CloudWatch Alarms Treat Missing Data](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html#alarms-and-missing-data).

Example of how to observe a breaching data point

Example alarm configuration:

* Standard resolution alarm (evaluates the metric every minute)
* Metric is CPUUtilization
* Threshold is 65%
* Statistic is Average
* Period is 60 seconds
* Evaluation Period is 1
* Detailed Monitoring is enabled for the monitored Amazon Elastic Compute Cloud (Amazon EC2) instance

When the example alarm evaluation period 12:00:00 - 12:01:00 UTC starts, the following data points are available to the metric:

Sample-1: 12:00:07 UTC, data-point: 89.76470588235294

Sample-2: 12:00:11 UTC, data-point: 27.926666666666664

Sample-3: 12:00:19 UTC, data-point: 54.57142857142857

Sample-4: 12:00:35 UTC, data-point: 95.473333333333336

The average of those data points is 66.934, which breaches the threshold of 65%. This triggers a change to the ALARM state. The alarm's event history lists the aggregated data point exceeding the threshold as the reason for the state change.

When the alarm is evaluated again later, additional data points have flowed in for the minute 12:00:00 - 12:01:00 UTC. For example:

Sample-1: 12:00:07 UTC, data-point: 89.76470588235294

Sample-2: 12:00:11 UTC, data-point: 27.926666666666664

Sample-3: 12:00:19 UTC, data-point: 54.57142857142857

Sample-4: 12:00:35 UTC, data-point: 95.473333333333336

Sample-5: 12:00:37 UTC, data-point: 15.18181818181819

Sample-6: 12:00:41 UTC, data-point: 10.26490

The average of the new data points is 48.864, which doesn't breach the threshold of 65%. The alarm now changes to the OK state. The alarm's event history lists the aggregated data point being below the threshold as the reason for the state change.

You might not see the breaching data point in your CloudWatch metric's graph now, even though the alarm triggered. If you view the CPUUtilization metric's graph, the Average is listed as 48.864 (not 66.934). This is because by now all the relevant data points for evaluation have flowed into the metric.

If you change the CloudWatch metric graph's Statistic to Maximum, you can now see the breaching data point 95.473 at 12:00:00 UTC.

Note: If your alarm is configured to trigger when data falls below the threshold, change the CloudWatch metric graph's Statistic to Minimum.

Example of how to configure an "M out of N" alarm

Example alarm configuration:

* Standard resolution alarm (evaluates the metric every minute)
* Metric is CPUUtilization
* Threshold is 65%
* Statistic is Average
* Period is 120 seconds
* Evaluation Period is 2 out of 3
* Detailed Monitoring is enabled for the monitored EC2 instance

Note that the example alarm configuration is similar to the first example. However, the evaluation period checks 2 out of 3 available data points before triggering the alarm. The period is also reduced because of the increased evaluation period.

When the alarm period starts at 12:00:00 UTC, the following data points are available to the CloudWatch metric:

Sample-1: 12:00:07 UTC, data-point: 89.76470588235294

Sample-2: 12:00:11 UTC, data-point: 27.926666666666664

Sample-3: 12:00:19 UTC, data-point: 54.57142857142857

Sample-4: 12:00:35 UTC, data-point: 95.473333333333336

CloudWatch looks for data points that are older than the 12:00:00 UTC because of the increased evaluation period:

11:58:00 UTC, Average=41.874304539920

11:59:00 UTC, Average=5.230773650991253

12:00:00 UTC, Average=66.93403361344538

The aggregated data point at 12:00:00 UTC breaches the threshold. However, the alarm remains in the OK state and doesn't change to the ALARM state. This behavior happens because only 1 out of 3 data points breach the threshold, whereas 2 out of 3 are required to trigger the alarm.

Related Information

[Using Amazon CloudWatch Alarms](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html)