Anomalies Presentation Logic

Anomalies are presented using similar formats, however, there are some changes in their presentation according to the expected usage of the page in the Anodot app. For an overview of the basic Anodot workflow and the importance of anomalies, see Anodot Workflow.

This article includes:

Common Guidelines

The below guidelines are valid across Anodot's applications.

- **Anomaly Presentation Logic**

  Anomaly Starting Point: Once an anomaly is detected, Anodot draws a line starting from the previous data point within the baseline to the anomalous data point that is outside the baseline. This is done in order to allow the user to visualize the starting point of the issue.
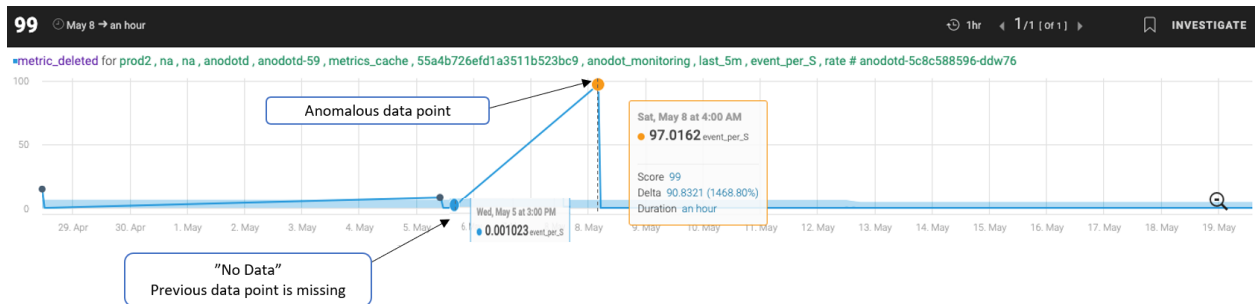
 Anomaly End Point: The last anomalous data point will be outside the baseline.
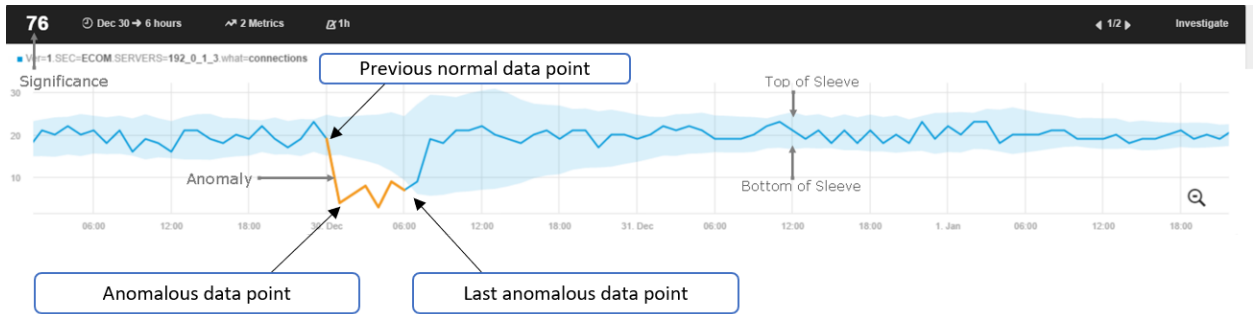
- **Anomaly Presentation when Missing Data Points ("No Data")**
  Anodot draws the anomaly line and starts from the "normal" data point, but because of the missing data, the anomaly is presented as follows:

  - If the detected anomaly **is one data point** and the previous data point is absent ("No Data"- missing data) the representation uses an orange anomaly dot.

- If the detected anomaly is **more than one data point** and the previous data point is absent ("No Data"- missing data) the representation uses an orange anomaly line, starting from the first anomalous data point and connecting the next anomalous data points.
- There are cases where the baseline is a decimal value and the data point is very close to, yet outside of the baseline. The presentation in these cases shows as if the anomalous data point is in the baseline, due to these very close values, yet it's not. In the below example: baseline values are very low= 0.00540721787838732 - 0.14335659430727773 and the point value 0 ->, so the point is out of the baseline.
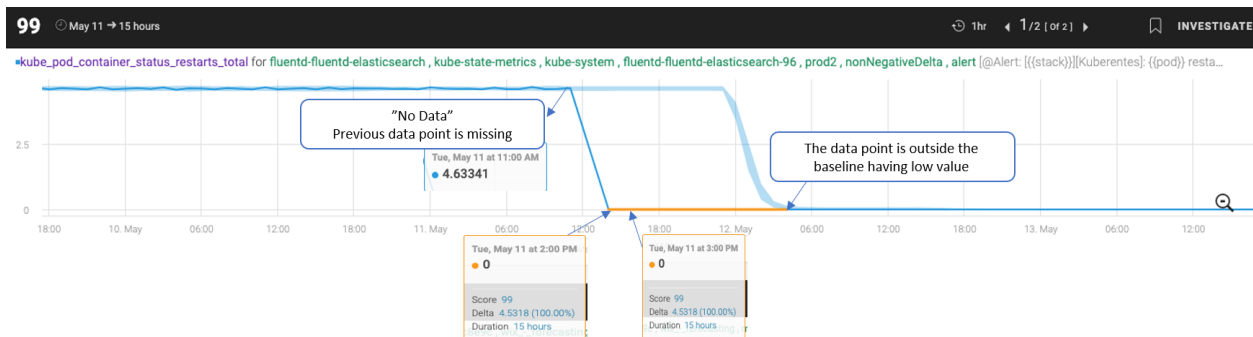
Simulating Alert Data

When defining the metrics for your Anomaly or Static alert, you can choose to dynamically load simulated alert data you select for each metric; the displayed data simulates the estimated number of alerts that will be generated according to the metric selected and the alert condition. This metric data is automatically displayed in the main content area of the Create New Alert screen.

Anomalies Presentation Guidelines
The anomalies coloring represents inspected anomalies that will or won't trigger the alert according to the alert conditions.

- **Orange marked Anomaly:** Represent anomalies that **meet** the alert conditions and **will** trigger an alert.
- **Gray marked Anomalies:** Represent anomalies that **don't meet** the alert conditions and **won't** trigger an alert.

In the example below, you can see two anomalies that look similar yet they have different characteristics such as Score. Duration, and Delta.

One of them met the alert condition and is therefore presented in the alert simulation as orange; the other one didn't meet the condition and is presented in gray (the anomaly that didn't meet the condition is marked in red in the anomaly tooltip).
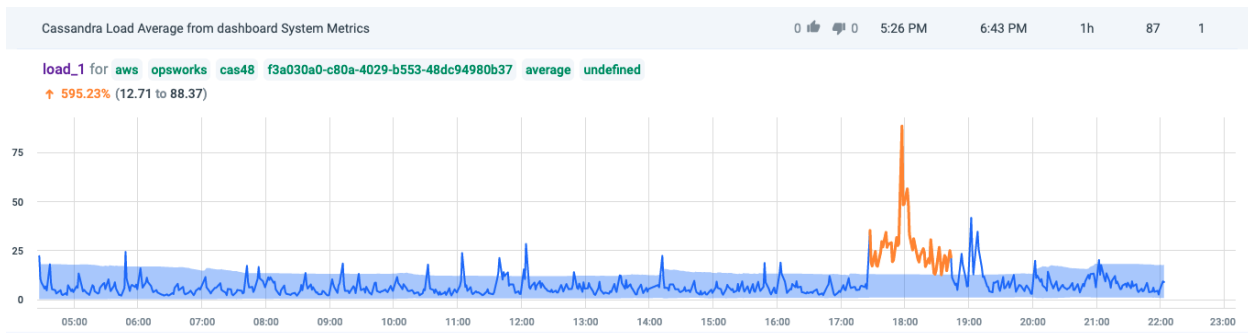

Viewing Anomalies in the Alert Console

The Alert Console is the repository of all your Anodot alerts.

Anomalies Presentation Guidelines
The alert contains the chart with the anomaly that triggered the alert marked in orange. Additional anomalies on the alerted metrics can be explored as part of the investigation, since they are not part of the alert.

Using the Anomalies Dashboard (Anoboards)

The Anomalies page is the central repository of anomalies, each displayed as a customized Anomalies dashboard (Anoboard) that shows anomalies in a predefined set of metrics and time range.

Upon an alert notification, click **Investigate** within the notification to start the analysis. The Anomap and chart for the specific anomaly opens, together with other metrics that are in the same anomalies group.

The context for the analysis are the anomalies that are part of the alert; the **Anomalies Line Charts** displays one or a group of metrics simultaneously **for a specified time range**. Each instance of the anomaly is displayed in a separate chart.

Each anomaly over time will have its own individual chart. The investigation upon an alert will lead to the relevant anomaly chart that triggered the alert.

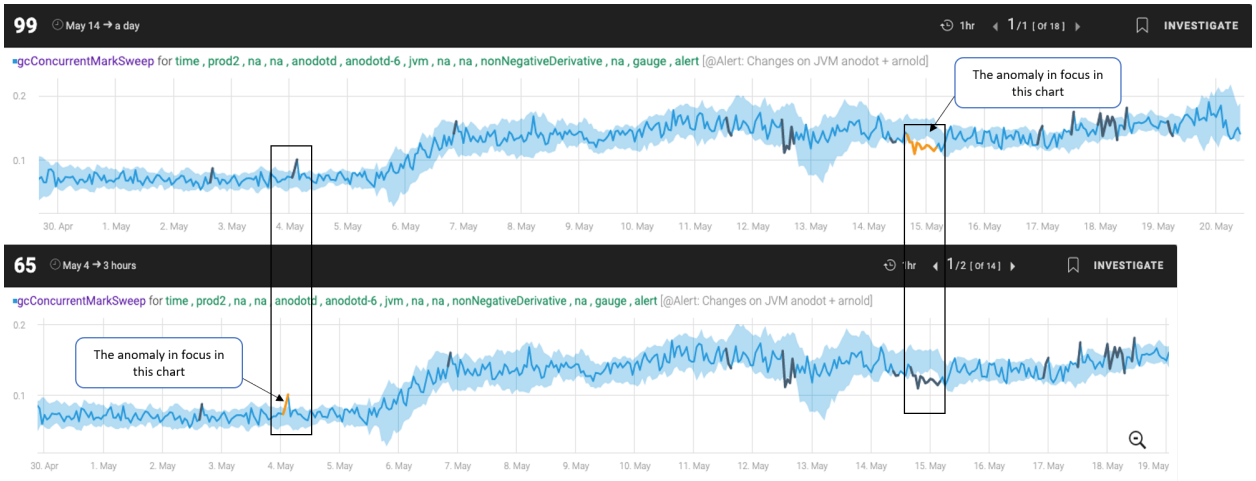**Anomalies Presentation Guidelines**

Alert Scenario

- **Orange marked Anomaly:** If the anomaly was opened from an alert investigation, the orange marked anomaly represents the anomaly that triggered the alert.
- **Dark blue marked Anomalies:** These are additional anomalies on the same metric, but not relevant for this particular alert.
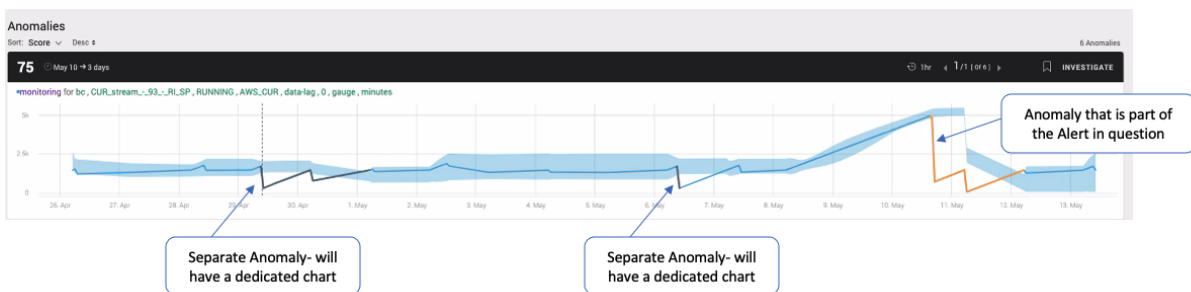
Anomalies Investigation Scenario

- **Orange marked Anomaly:** If investigating Anomalies without the alert context, each chart represents an individual anomaly according to the selected time range and anomalies criteria.

- **Dark blue** marked Anomalies: These are additional anomalies on the same metric, each will have a separate chart that is presented according to the selected time range and anomalies criteria.

Viewing anomalies in Email

Anodot supports various notification channels for the alerts generated in Anodot.

Anomalies Presentation Guidelines
The alert message contains only the anomaly that triggered the alert marked in orange.