title: Creating Logs Alerts description: Step-by-step alert creation instructions for Logs

In a Logs App, *saved queries* are used to save search queries that you want to reuse.

For example, let's say you used *include/exclude filters* to search for *Elasticsearch slowlogs warnings*.

Elasticsearch slowlogs warnings search

Clicking on the bell icon creates a new *saved query*, where filters are transformed into `Query string`.

image alt text

You can save this query as is and use it in future searches.

image alt text

Clicking on the *alert view* icon opens the view where you can edit *saved queries*.

image alt text

The bell icon here means that *saved query* has *alert rule* attached to it.

Let's attach an *alert rule* to the *saved query* we've just created - click on `Edit`.

Enable Alerts

By turning on `Enable alert` toggle *saved query* is expanded into *alert rule*.

image alt text

Let's say we want to get notified if the number of *slowlog warnings* reaches 10 in any 10 minutes. Notice that *Chart Preview* shows the threshold line to help you visualize the threshold value in context.

The field next to threshold value allows you to easily multiply the threshold and thus has a default value of 1, which is neutral for multiplication.

image alt text

Although less applicable in the case of our *slowlog warnings*, `Ignore regularly occurring spikes and dips` tells the algorithm to ignore regular outliers that are not really anomalies, but are caused by regular spikes/dips.

If you wanted to avoid using a specific threshold value and instead get notified when the number of *slowlog warnings* deviates from a continuously computed baseline, you'd change `Alert type` to `Anomaly alert`.

image alt text

Notice that the chart changed to help you get a sense of what would constitute an anomalous value in your case (dots outside the gray *confidence interval*).

The *confidence interval* is an approximation of Sematext Cloud's anomaly detection algorithm, so don't expect each and every red dot on the chart to have triggered the alert.