Configure threshold alert settings

Published: 2018-11-12

You can configure threshold alert settings that monitor when a specific metric crosses a defined boundary. When the conditions configured in the alert settings are met, the ExtraHop system generates a threshold alert, which you can view in the Alert History.

Threshold alerts are useful for monitoring occurrences such as SLA-violations or error rates that surpass a comfortable percentage. For example, you can configure threshold alert settings that generate alerts when an HTTP 500 status code is observed more than 100 times during a ten minute period.

Before configuring alert settings, determine which metric you want to monitor and the conditions the metric must meet for the ExtraHop system to generate a threshold alert.

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon and then click **Alerts**.
3. Click **New** to open the Alert Configuration window.
4. Enter a unique name for the alert configuration in the **Name** field.
5. Click **Threshold**.
6. From the Detail section, specify the type of metric you want to monitor.

   Top-level

   Specifies the top-level metric, such as an HTTP response or DNS request.

   Detail

   Specifies the detail metric, such as the URI of an HTTP response.
7. Select the metric you want to monitor.
   a) Click the Select metric icon.
   b) Click the source of the metric, such as an application.
   c) Click the protocol of the metric, such as HTTP, NetFlow, or custom.

      Depending on the source and metric type, some protocols contain secondary groups for client and server metrics.
   d) Locate and click the metric you want to monitor.

      Additional fields appear depending on the metric you select:

      - The Key pattern field enables you to further refine the metric, such as to specify the definition of a custom metric. The key pattern is interpreted as a regular expression and must adhere to Perl-Compatible Regular Expression (PCRE) syntax.
      - The Data point field displayed for top-level metrics enables you to specify a percentile value for the metric.
      - The Data point field displayed for detail metrics enables you to specify a mean value plus a standard number of deviations for a metric.
8. Optional: To monitor the value of the selected metric divided by a secondary metric, click the **Ratio** checkbox and select a secondary metric from the field provided.

   For example, divide the number of DNS response errors by the total number of DNS responses to monitor the percentage of errors that exceed a specified threshold.
9. Select one of the following firing modes:

   Edge-Triggered

   An edge-triggered alert is generated only once when the alert conditions are true. The alert is generated again only if conditions are true after the metric value has returned to normal conditions twice.

Level-Triggered

A level-triggered alert is generated continuously while the alert conditions are true for the specified time period.

10. In the Alert When section, specify the following options that define the alert expression:

Interval

Specifies the length of the time interval.

Operator

Specifies how to compare the interval to the value.

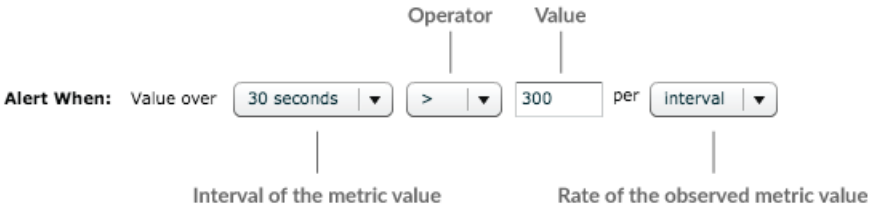
Note: The ExtraHop system does not record values of zero for metrics. Instead, the ExtraHop system observes a lack of values. If you specify a value of zero in your alert configuration, the alert never generates. To create an alert configuration with a zero value, select the **<** (less than) operator and type a value of `1`.

Value

Specifies the number of metric occurrences to watch for.

Rate

Specifies the rate in which metric occurrences happen.



For example, to issue an alert when the value of the observed metric crosses the threshold more than 10 times per minute in a 30 minute interval, set the following values in the Alert When options:

- **Time interval: 30 minutes**
- **Operator: >**
- **Value:** `10`
- **Rate: minute**

The Alert When options work with the Firing Mode options to determine how many times an alert should be generated.

11. Click **OK**.

Next steps

- Alerts cannot be generated until you assign an alert configuration to a source.
- Assign an exclusion interval to an alert to suppress alerts during specific times.
- Add a notification to an alert configuration to receive emails or SNMP traps when an alert is generated.