Configure trend alert settings

Published: 2020-02-23

You can configure alert settings that monitor when a specific metric deviates from normal trends observed by the system. When the conditions configured by the alert settings are met, the ExtraHop system generates a trend alert, which you can view on the Alerts page.

Trend alerts are useful for monitoring metric trends such as unusually high round-trip times or storage servers experiencing abnormally low traffic, which might indicate a failed backup. For example, you can configure trend alert settings that generate alerts when a spike (75th percentile) in HTTP web server processing time lasts longer than 10 minutes, and where the metric value of the processing time is 100% higher than the trend.

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 trend 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 Alerts Configuration window.
4. Enter a unique name for the alert configuration in the **Name** field.
5. Click **Trend**.
6. Select the metric you want to monitor.
   a) Click the Select metric icon.
   b) Click the source of the metric, such as 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.

      Depending on the metric you select, the Key pattern field appears, which 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.
   e) Click **OK**.
   f) If you have selected a dataset or sampleset metric, additional metrics options are available as described in Dataset and sampleset metric options for trend alerts.
7. 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 trend threshold.
8. Select one of the following firing modes:

   Edge-Triggered

   An edge-triggered alert is generated only once when the alert conditions is 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.
9. In the Alert When section, specify the following options that define the alert expression:

   Metric calculation

   Specifies the method by which the metric should be calculated, which are described in Metric calculation options for trend alerts. It is important to note that the alert configuration does not

disable incompatible options the way the Metric Explorer does. Be sure to select the median or a percentile calculation when adding a dataset metric or you might issue unintended alerts.

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 will never be generated. To create an alert configuration with a zero value, select the **<** (less than) operator and type a value of `1`.

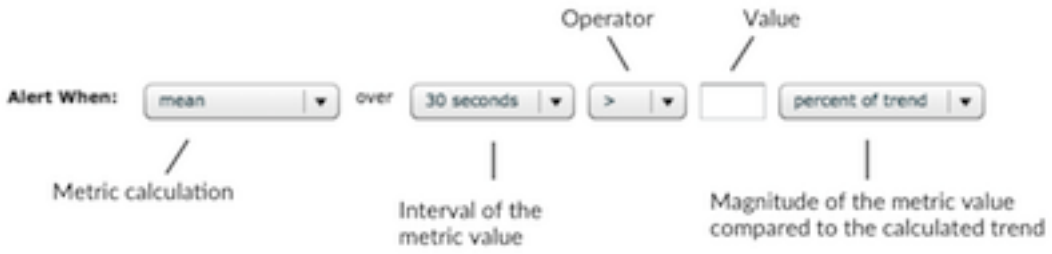
Value

Specifies the trend value that will issue an alert. The observed metric is compared to a specified trend value.

For example, if measured in percentages, a trend value of 100 means that the alert is generated when the observed metric matches the trend. A trend value of 150 means that the alert is generated when the observed metric is 50% above the trend. Likewise, enter a value of 50 for 50% below trend.

Measure

Specifies the unit by which the value is measured.



For example, to issue an alert when the standard deviation of the observed metric over a 60 minute interval is equal to a trend value of 25%, set the following Alert When values:

- **Metric calculation: std. deviation**
- **Interval: 60 minutes**
- **Operator: ==**
- **Value:** `125`
- **Measure: percent of trend**

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

10. Click the Trend Settings tab and configure trend-specific settings for the alert.
    a) In the **Window** field, select the calculation window for the trend from the options described in Window options for trend alerts.
    b) In the **Lookback** field, specify the number of minutes of lookback, which refers to how far back you can look up historical data.
    c) In the Weighting Model section, select and configure the model you want from the options described in Weighting model options for trend alerts.
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.

Dataset and sampleset metric options for trend alerts

This section describes the additional options available for trend alert configurations that monitor dataset and sampleset metrics.

Option	Description
Merge	Merges all the datasets and applies the trending function to one superset of data. For example, a 30-second aggregation roll up, or metric cycle, contains a single dataset for each 30-second interval. Therefore, a 30-minute interval has 60 datasets. You can generate a baseline for the trend from these datasets with one of the following methods: • Determine the mean, median, or nth percentile of each dataset, and perform a trend calculation on this value. For example, you might want to determine the moving average (trend function) of the 95th percentile of processing time. • Merge all of the datasets together into one large dataset and perform a trend calculation on this value. For example, you might want to merge the datasets, then calculate the trimean (trend function) of the combined dataset.
Mean	Calculates the mean of each dataset.
Percentile	Calculates a percentile of each dataset as specified in the **Percentile Value** field.
Standard Deviation	Calculates the normal deviation compared to the current trend alert through the same standard deviation parameters as the trend. The parameters can be absolute or relative, as specified in the **Normalization** field. **Absolute** Displays the standard deviation as a constant. **Relative to Mean** Displays the standard deviation relative to the mean. **Note:** If not calculated as standard deviation, the selected dataset metric is calculated as an absolute sample.

Metric calculation options for trend alerts

This section describes the metric calculation options available when configuring the alert conditions for trend alerts.

Option	Description
mean	Specifies the mean value of the metric. Only select this option for sampleset metrics, such as server processing time (`tprocess`) by server.
median	Specifies the 50th percentile value of the metric. Only select this option for sampleset metrics, such as server processing time (`tprocess`) or round trip time (rtt).
25th percentile	Specifies the 25th percentile value of the metric. Only select this option for sampleset metrics, such as server processing time (`tprocess`) or round trip time (`rtt`).
75th percentile	Specifies the 75th percentile value of the metric. Only select this option for sampleset metrics, such as server processing time (`tprocess`) or round trip time (`rtt`).
count (total)	Specifies the count or total of the metric values as an absolute value.
std. deviation	Calculates the normal deviation compared to the current metric. Only select this option for sampleset metrics, such as server processing time (`tprocess`) by server.
ANY	Generates the alert when any of the specified conditions are present.
ALL	Generates the alert when all of the specified conditions are present.
NONE	Generates the alert when none of the specified conditions are present.

Window options for trend alerts

This section describes the Window field options available on the Trend Settings tab that you configure when configuring a trend alert.

Option	Description
Same Hour of Week	Calculates the trend within a specified 1-hour window each week.
Same Hour of Day	Calculates the trend within a specified 1-hour window each day.
Minute Rolling Average	Calculates the trend based on the average of the data gathered each minute within a specified amount of time from the present time.
Hour Rolling Average	Calculates the trend based on the average of the data gathered each hour within a specified amount of time from the present time.

Weighting model options for trend alerts

This section describes the weighting model options are available when configuring trend alerts.

Option	Description
Mean	Specifies the manner in which to calculate the average. **Linear Average** Calculates the average with all data points weighted equally. **Single Exponential** Calculates the average with the most recent data points weighted more heavily. **Double Exponential** Calculates the average with the most recent data points weighted the most heavily. For linear averages, the most recent value is weighted at 1 times the oldest value by default. For single and double exponential means, enter a number to weight the most recent value.
Percentile	Specifies the percentile value to be referenced as a basis for creating the trend. **Percentile** Calculates the trend with data points from a user-specified percentile. **Min Value** Calculates the lowest data point gathered during the time interval. **Max Value** Calculates the highest data point gathered during the time interval.
Regression	Specifies monitoring for increasing trends. **Linear** Calculates steadily increasing trends based on previous trends that are equally incremental. **2nd Degree Polynomial** Calculates exponentially accelerating trends by projecting a curve with the following equation: `y = ax2 + bx + c`
Standard Deviation	Calculates the normal deviation compared to the current trend. **Type** Applies a sample-based or population-based standard deviation.

Option	Description
	Normalization Displays the standard deviation relative to the mean. **Note:** If a trend is a standard deviation, the same parameters as the trend are applied to alert configurations associated with that trend. If the trend is not a standard deviation, then the alert is calculated as "sample" and "absolute".
Static Value	Calculates based on the specified static value. This option is useful to plot constant lines for SLAs.
Time Delta	Applies the oldest trend to calculate a time range based on the lookback window.
Trimean	Calculates the weighted average of the 25th, 50th, and 75th percentile values.
Winsorized Mean	Replaces the most outlying values with the highest and lowest remaining values. Values above the 90th percentile become the same value as the 90th and values below the 10th percentile become the same value as 10th.