Alerts

Published: 2017-11-16

Alerts make it easy to inform your teams when there are network, device, or application anomalies or Software License Agreement (SLA) violations. You can configure threshold and trend alert settings to track a specified metric and issue alerts when configured conditions are met. When an alert is generated, you can configure the ExtraHop system to send an email message or an SNMP trap to designated people in your organization. You can also configure time ranges in which alerts are suppressed, such as weekends, to reduce unnecessary alerts.

Alert types

You can configure threshold and trend alert settings in the ExtraHop Web UI. The ExtraHop system also generates alerts through anomaly detection, which is available with a subscription to the ExtraHop Addy™ service.

Threshold alerts

Threshold-based alerts are generated when a monitored metric crosses a defined value in a time period. Threshold alerts are useful for monitoring occurrences such as error rates that surpass a comfortable percentage or SLA-violations.

Trend alerts

Trend-based alerts are generated when a monitored metric deviates from the normal trends observed by the system. 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.

Trend alert settings are more complex than threshold alerts, and are useful for metrics where thresholds are difficult to define.

Anomalies

Anomalies are unexpected deviations from normal patterns in device or application behavior. Unlike threshold and trend alerts, which require you to configure alert conditions, anomalies are automatically detected by ExtraHop Addy. Addy is a cloud-based service that applies machine learning techniques to detect anomalies in your IT environment.

The focus of this topic is for threshold and trend alerts and how to configure them in the ExtraHop Web UI, but you can learn how to get started with Addy in the ExtraHop Addy User Guide.

Alert conditions

An alert is generated when the alert conditions that you configure are met. There are three areas of consideration that make up the alert conditions: the monitored metric, the firing mode, and the alert expression.

Monitored metric

Specifies the metric tracked by the alert configuration. The ExtraHop system watches for instances when the value of the metric crosses a defined threshold or diverges from the trend. Threshold alert settings can track a top-level or detail metric, but trend alert settings only track a top-level metric.

Firing mode

Specifies how often an alert is generated. Specify the edge-triggered alert option to issue a single alert when conditions are met even if the condition is ongoing. Specify a level-triggered alert option to issue alerts at specified intervals for as long as the conditions are true.

Alert expression

Specifies when to issue an alert. A series of options, such as the time interval, the metric value, and the rate, are combined to determine the alert expression. For example, you can set options to issue

a threshold alert when the value of the monitored metric falls below 100 per second in a 1 minute interval. Options available for an alert expression vary by alert type and other configuration settings.

The values for each area are combined to determine the alert conditions; as the system monitors the specified metric, if the alerts conditions are met, the system issues an alert based on the specified firing mode and the alert type.

For example, the following alert conditions result in a threshold alert when an HTTP 500 status code is observed more than 100 times during a ten minute period:

- **Monitored metric:** `extrahop.device.http_server:status_code?500`
- **Firing mode: Edge-triggered**
- **Alert expression:** Value over **10 minutes >** `100` **per interval**

Or, you can specify a per second, minute, or hour rate. For example, the following alert conditions result in a threshold alert when an HTTP 500 status code is observed more than 30 times per minute during a 10 minute period:

- **Monitored metric:** `extrahop.device.http_server:status_code?500`
- **Firing mode: Edge-triggered**
- **Alert expression:** Value over **10 minutes >** `30` **per minute**

The alert conditions for a trend alert are slightly different than for a threshold alert. The following settings result in a trend alert when a spike (75th percentile) in HTTP web server processing time that lasts longer than 10 minutes, and where the metric value of the processing time is 100% higher than the trend:

- **Monitored metric:** `extrahop.device.http_server:tprocess`
- **Firing mode: Edge-triggered**
- **Alert expression: 75th percentile** over **10 minutes >** `200` **percent of trend**

Optional alert configuration settings

Notifications

You can add notifications to an alert configuration, which enable you to review alerts with high priority severity settings through email or SNMP. When the alert is generated, notifications are emailed to specified addresses or sent to an SNMP listener.

The alert notifications contain information such as the severity level of the alert, the source, the alert conditions, and when the alerts was generated. For more information, see Add a notification to an alert.

Exclusion intervals

You can define a time in which alerts are suppressed through an exclusion interval. When an exclusion interval is assigned to an alert configuration, alerts will be suppressed from the Alert History, email notifications, and SNMP listener.

For example, an exclusion interval enables you to prevent recurring, duplicate alerts in the Alert History about high database activity during hours the database is backed up. For more information, see Create an exclusion interval for alerts.

Alert History

After you have configured settings for an alert or two, you can check out the Alert History for any generated alerts. You access the Alert History from the Metrics page in the ExtraHop Web UI.

The Alert History contains an entry for each alert generated during the time range specified in the Time Selector. The history also displays the name of the generated alert, the source of the alert, and the time of the most recent occurrence. Click the name of the source to view source pages, or click the name of the alert to view additional alert details.

For threshold alerts, the Alert Details window displays the following information:

Name
The name of the alert configuration.

Expression
The metric, time interval, operator, and alert conditions that were defined when the alert was configured.

Value
The value of the metric at the time the alert was generated. This value can be compared against the alert expression.

Description
The optional user-defined description of the alert.

For trend alerts, the Alert Details window displays the following information:

Name
The name of the alert configuration.

Alert Conditions
The type of alert, time interval, operator, or percentage of the trend that were defined when the alert was created.

View at Time of Alert
Displays the alert graph from when the alert was generated.

View Current State
Displays the alert graph of the current trend state of the alert.

Related topics

Check out the following guides and resources that are designed to familiarize new users with our top features.

- Configure threshold alert settings
- Configure trend alert settings
- Intro to Alerts (online training)
- Configure your first alert (online training)