Alerts

Published: 2020-02-23

Alerts make it easy to learn when important events occur, such as security detections on critical devices or Software License Agreement (SLA) violations. You can configure an alert to watch for specified criteria and generate alerts when conditions are met on specified data sources.

Alert types

You can configure threshold and trend alerts, which monitor a specified metric, or you can configure detection alerts to monitor detections by protocol or category.

Threshold alerts

Threshold-based alerts are generated when a monitored metric crosses a defined value within a specified time interval.

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.

Detection alerts

Detection alerts are generated when a detection on a specified protocol or detection category occurs. Detections are unexpected deviations from normal patterns in device or application behavior or notable activity in your environment. See Detections for more information.

Detection alerts are useful for filtering detections to receive alerts about detection categories and protocols that are important to you. For example, you might want to see alerts about higher risk categories such as actions on objective.

Alert conditions

The alert condition specifies when to generate a threshold or trend alert based on the value of the monitored metric. The alert condition is a combination of settings, such as a time interval, metric value, and metric calculation. When the value of the monitored metric on the assigned data sources meets the alert condition, an alert is generated.

For example, an alert condition might generate a threshold alert when HTTP 500 status codes are observed more than 100 times over a ten minute interval.Or, you might monitor the metric at a per-minute rate to generate an alert when HTTP 500 status codes are observed more than 100 times per minute during a ten minute interval.

The condition for a trend alert includes how to calculate the trend value of the monitored metric. For example, you might generate a trend alert 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.

Tip: You can create an exclusion interval during which alerts are suppressed, even if alert conditions have occurred. For example, you might create an exclusion interval for hours when database backups are performed to prevent recurring or duplicate alerts about high database activity.

Alerts page

All alerts generated during the specified time interval are displayed on the Alerts page. Click **Alerts** at the top of the page to view alerts.

The Alerts page displays the following information for each alert:

Severity

A color-coded indicator of the alert severity level. You can set the following severity levels: Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug.

Alert name

The name of the configured alert. Click the alert name to view alert details.

Source

The name of the data source on which the alert conditions occurred. Click the source name to navigate to the source Overview page.

Time

The time of the most recent occurrence of the alert conditions.

Alert type

Indicates a trend, threshold, or detection alert.

Organize the list of alerts with the filter tools at the top of the Alerts page. You can search the list for an alert name or source name, or filter the list by source type, severity, or alert type.

Tip: Here are some other ways to learn when an alert is generated.

- Add a notification to an alert to send alerts through email or to an SNMP listener.
- Add an Alerts widget to a dashboard to include a table of recent alerts associated with the dashboard sources.

Related topics

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

- Configure a threshold alert
- Configure a trend alert
- Configure a detection alert
- Alerts FAQ
- Intro to Alerts (online training)
- Configure your first alert (online training)