Alerts

Published: 2019-06-13

Alerts make it easy to inform your teams when critical network, device, or application events occur, such as Software License Agreement (SLA) violations. You can configure alert settings to track specified criteria and generate alerts when configured conditions are met.

When an alert is generated, you can also direct 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.

Alerts are displayed on the Alerts page, which enables you to quickly assess the severity of the alert and view the source of the alert.

Alert types

You can configure threshold and trend alert settings in the ExtraHop Web UI. The ExtraHop system also generates alerts from detections, which are available with an optional license.

Detection alerts

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

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

Detection alerts are useful for filtering detections by protocol or source so that you can receive alerts that only apply to a subset of detections you want to view.

Threshold alerts

Threshold-based alerts are generated when a monitored metric crosses a defined value in a time period. You can specify a top-level or a detail metric as the threshold.

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.

Alert conditions

An alert is generated when the alert conditions that you configure are met. The areas of consideration are different depending on the alert type. For detection alerts, the monitored protocols and the firing mode are considered. For threshold or trend alerts, the monitored metric, the firing mode, and the alert expression are considered.

Monitored protocols

Specifies which protocols are watched by the alert configuration. The ExtraHop system generates an alert only if a detection is identified from traffic that is over a specified protocol.

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 can 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:

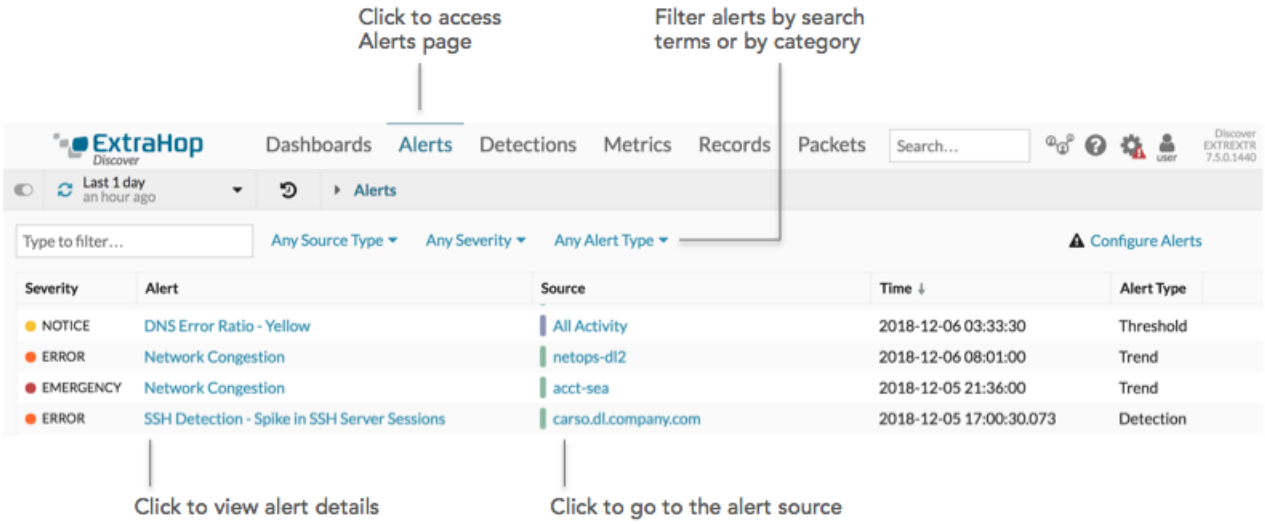
• **Monitored metric:** `extrahop.device.http_server:tprocess`

• **Firing mode: Edge-triggered**

• **Alert expression: 75th percentile** over **10 minutes >** `200` **percent of trend**

Alerts page

After you have configured settings for an alert, you can view all generated alerts on the Alerts page or you can view alerts generated from a specific source on an Alerts widget for the selected time interval.



The Alert History page displays the following information for each entry:

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 alert specified in the alert configuration settings. Click the source name to navigate to the source and display the protocol page that correlates to the tracked metric.

Source

The name of the data source on which the alert conditions occurred. Click the source name to navigate to the source and display the protocol page that correlates to the tracked metric.

For example, if an alert configuration tracks when the HTTP processing time exceeds a specific threshold, click the source link to go to the HTTP protocol page of the source device or application.

If an alert is associated with multiple protocols, the link goes to the Overview page of the source instead of the protocol page.

Time

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

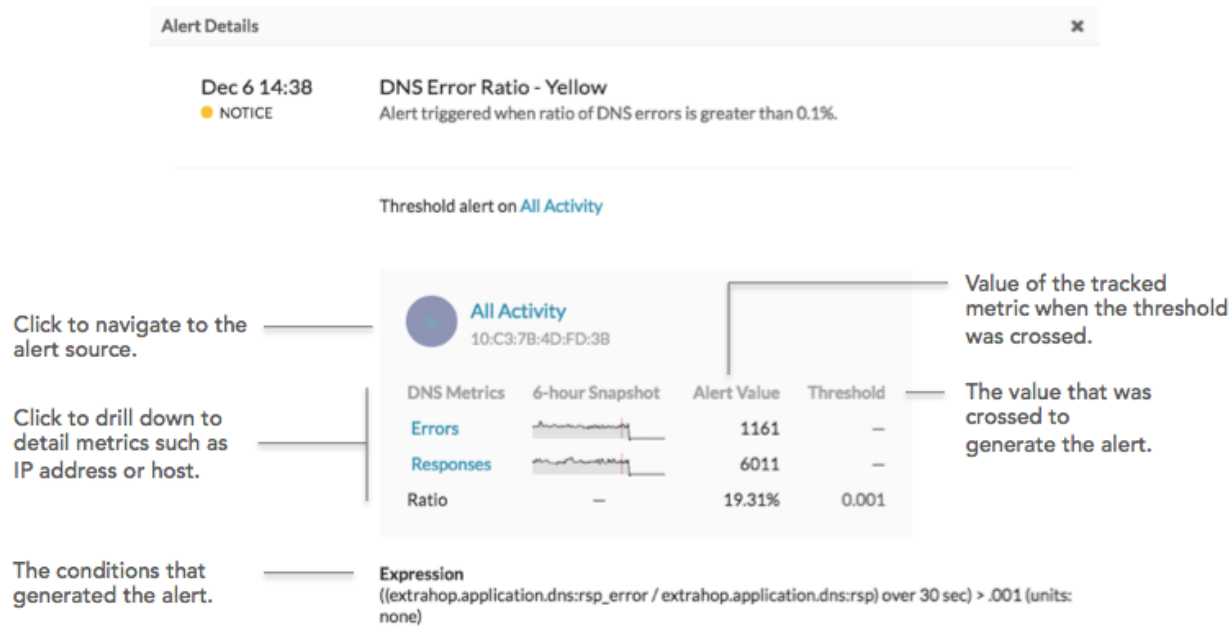
Alert type

Indicates a trend, threshold, or detection alert.

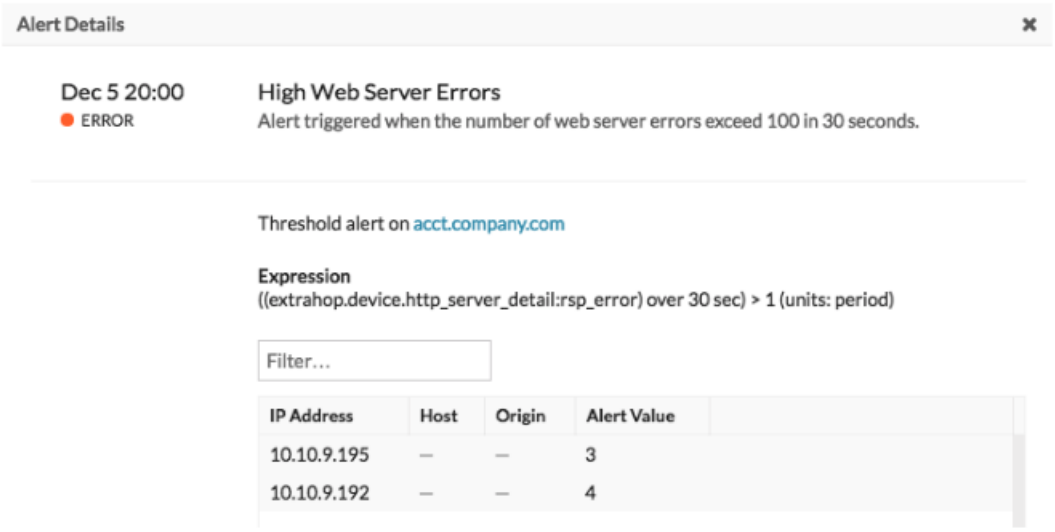
Alert details

Click an alert name to view alert details in a new window. The details provided for an alert are based on the alert type and configuration.

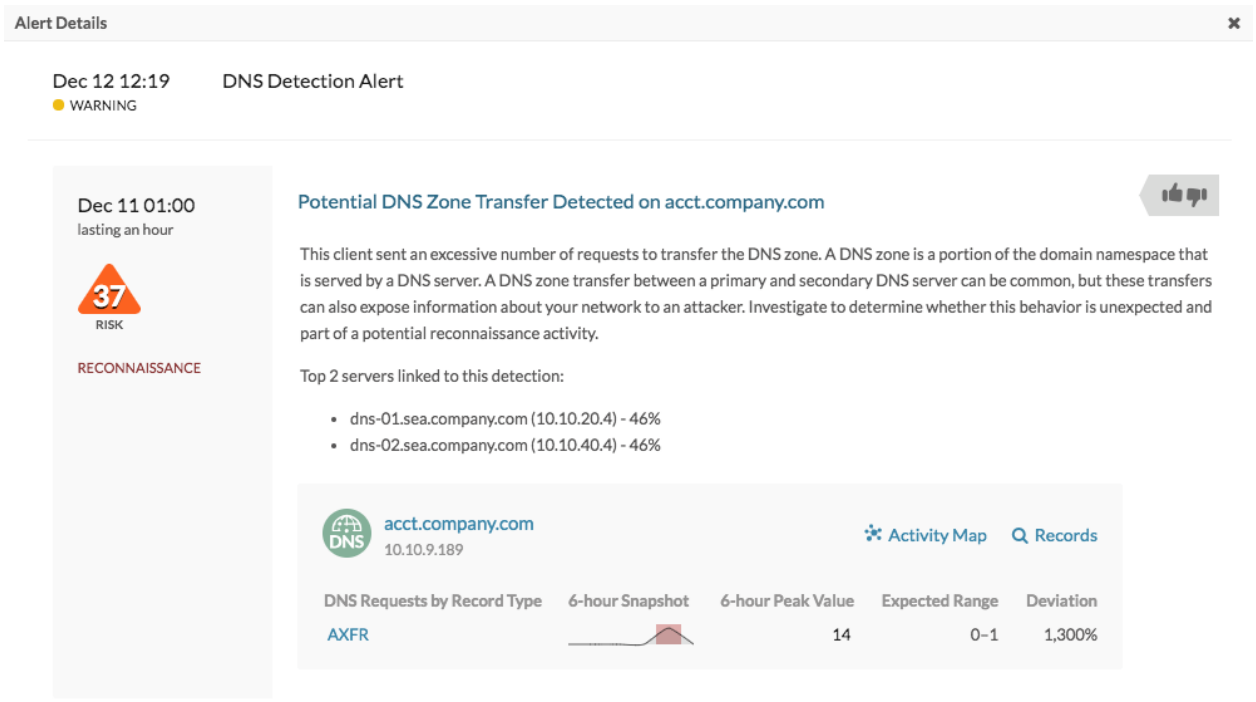
The following example shows a threshold alert configured to track a ratio, which monitors the value of a primary metric divided by a secondary metric. You can click the tracked metrics to drill down and investigate detail metrics.



The next example shows an alert that tracks a detail metric; the value of the metric for each alert occurrence is provided.

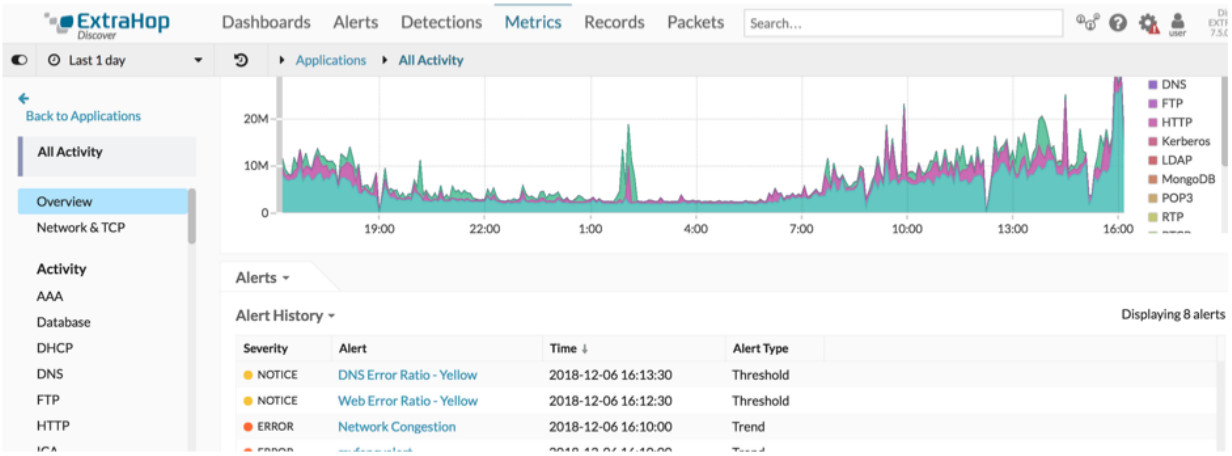


If you configure a detection alert, the Alert Details window displays details about the detection, which are described in View details about a detection.



Alert History widget

The Overview page for each application, device, and network displays an Alerts History widget if any alerts were generated from that source during the selected time interval.



For example, if you assigned an alert configuration to a device group, you can go to the Overview page of an individual device and see if any alerts were generated from the device during the selected time interval.

The Alerts widget provides the same information and links that are on the Alerts page, such as alert name, severity, type, and time.

Alert 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 configuration.

Exclusion intervals

You can define a time interval during which alerts are suppressed, even though alert conditions have occurred. If you assign an exclusion interval to an alert, the alert will not appear on the Alerts page and the ExtraHop system does not sent email notifications about the alert.

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

Related topics

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

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