Triaging Alerts

Date of Publish: 2018-10-15

http://docs.hortonworks.com

Contents

Triaging Alerts

When an event violates your threat intelligence thresholds, you are sent an alert that you can view in the Hortonworks Cybersecurity Platform (HCP) Alerts user interface, enabling you to evaluate the severity of the violation and manage it accordingly.

Launch the Alerts User Interface

The Alerts user interface is bundled with HCP and installed with the Ambari management pack.

Before you begin

- Elasticsearch must be up and running and should have alerts populated by HDP topologies.
- The Alerts UI defaults to port 4201. If you are already using port 4201 for another purpose, you must change the default port for the Alerts UI to another port number.

Procedure

1. Display the **Ambari** user interface.
2. In the Services pane, select **Metron**.
3. From the **Quick Links** menu, choose **Alerts UI**.

   Note: There is no login module for the Alerts UI.

Viewing Alerts

The Alerts user interface defaults to displaying the Alerts table when first opened. You can modify the alerts displayed in the Alerts table to help identify issues.

Table 1: Alerts UI Tools and Purposes

Tools	Description
Alerts table	The Alerts table displays the alerts generated by the HCP framework. The Alerts UI polls for alerts and refreshes the Alerts table at an interval that you can configure.
Searches field	You can search for alerts using the search bar above the Alerts table. The search tool follows the Lucene syntax which supports a rich query language.
Filters	The Alerts UI currently provides five filters that you can apply to alerts. You can use these filters to refine the list of alerts and collect additional information on the alerts.
Alert status	You can change the status of or dismiss an alert.
Group By	You can group alerts so you can apply filters, status, etc. on multiple alerts at a time.
Meta Alerts	The meta alert feature enables you to create a system entity that contains a collection of filtered alerts.

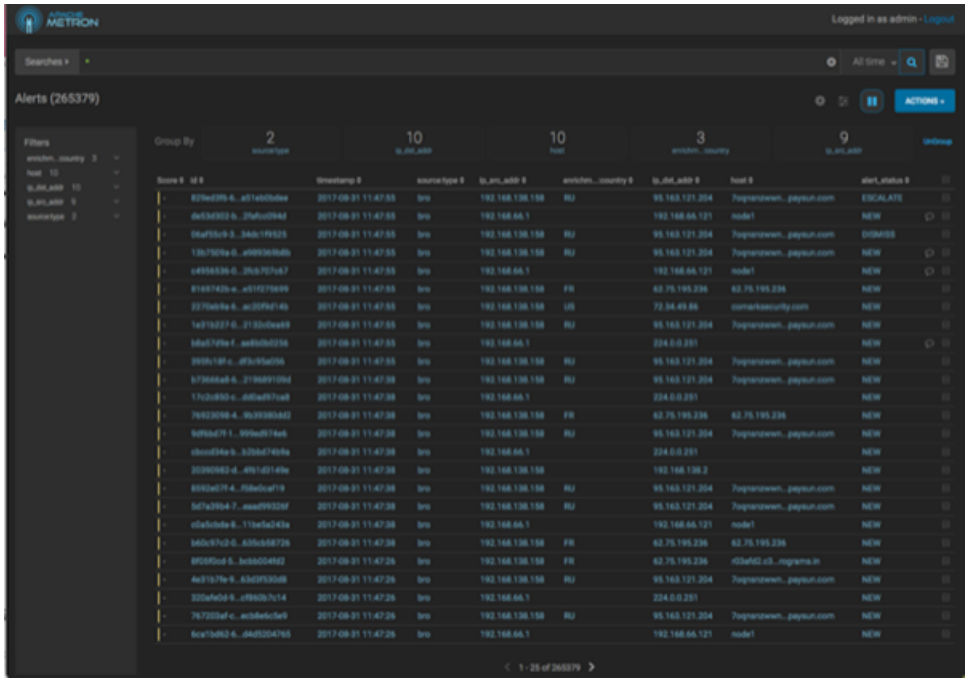
Using the Alerts Table

The Alerts table displays the alerts generated by the HCP framework. The Alerts UI polls for alerts and refreshes the Alerts table at an interval that you can configure. This polling is paused whenever you open any configuration panels or use the **Searches** field.

By default, the alerts table shows the recent alerts at the top. For example, alerts are sorted descending on timestamp. For information on modifying these configurations.

The Alerts table also provides the threat intelligence score for each alert. Next to the score is a bar that indicates the severity of the score:

Red	A score of 69 or higher
Orange	A score between 39 and 69
Yellow	A score below 39



Configure Table Columns

You can configure the table columns in the Alerts table to customize the type of information you display. You can modify the information that shows in each column, the title of the column, and the order in which the columns are displayed.

Procedure

1. Click

   (gear icon).

   The Alerts UI displays the Configure Table that lists all the columns available across all the valid search indexes.

   Alerts Configure Table

2. Select the fields you want to display and unselect the fields you do not want to display.
3. You can rename the column titles by entering a new name in the **Short Name** column.
   For example, 'enrichments:geo:ip_dst_addr:country' can be renamed to 'Dst Country'.
   This is just for display convenience and the changes are not propagated to any system in HCP.
4. You can also configure the order in which the selected columns will appear in the table by using the arrow icons.
5. Click **Save** to save your changes and dismiss the **Configure Table** panel.
6. You can pause the Alerts UI polling by clicking the

   (pause button).

Configure Table Row Settings

You can configure the table row settings in the Alerts table. You can use this feature to modify the appearance of the Alerts table and the refresh rate.

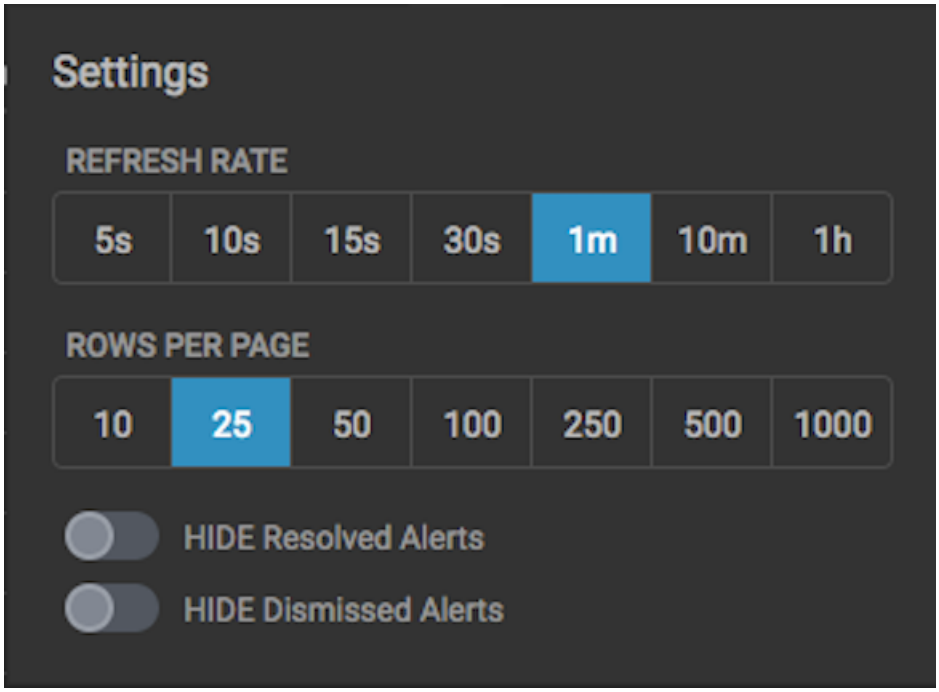
Procedure

1. Click the

   (slides icon) at the top of the table to display the Settings dialog box.

   Alerts Settings Panel



2. To modify the rate at which the Alerts table is refreshed with new alert information, choose a value under **Refresh Rate**.
3. To modify the number of rows displayed in the Alerts table, choose a value under **Rows Per Page**.

   Note: The number of rows that are visible in the Alerts table is restricted by the size of your browser window.
4. To hide resolved alerts or dismissed alerts, click the slide button next to the appropriate action.

   HIDE Resolved Alerts and HIDE Dismissed Alerts are non-functional features in this release.

Display Additional Alerts Information

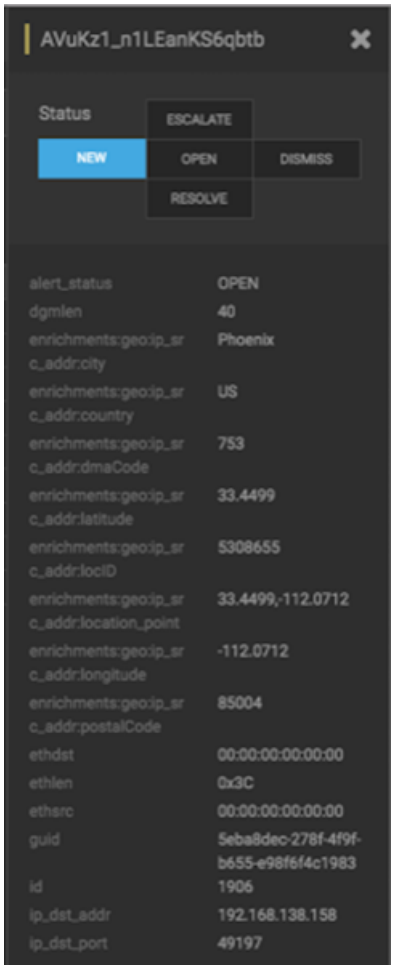
In addition to displaying alert information in the Alerts table, you can display all the information about the alert in Elasticsearch in a separate panel.

Procedure

1. Select an alert by clicking on empty space in the alert row.

   The Alerts UI displays a panel listing all available data in Elasticsearch about the alert.

   Alerts Information Panel



2. The Status states at the top of the panel display the current status of the alert.

Search Alerts

You can search for alerts using the search bar above the Alerts table. The search tool follows the Lucene syntax which supports a rich query language.

Procedure

1. To search on an item that is displayed in the Alerts table, simply click on the item and it will display in the **Searches** field.

   Searches Field

2. You can also directly type in the **Searches** field to enter search criteria.

   For example, you can enter source:type:snort.

3. To remove an item in the **Searches** field, mouse over the information in the **Searches** field until an **x** appears at the end of the text. Click on the **x** to remove the search filter and the operator following or preceding it.
4. To clear the entire **Searches** field, click the **x** at the end of the field.
5. You can specify the time range of your search by using the time range selector on the far right of the **Searches** field.

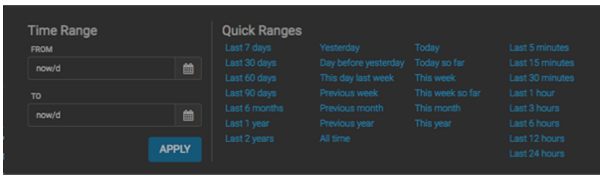
Note:

The time-range selector is not available if you put a timestamp in the **Searches** field.

The time-range button defaults to **All time** which displays all alerts corresponding to the Searches parameters. To customize the time range, click the time-range drop-down menu and select one of the following:

Time Range	Enables you to choose the start and end dates and times for your search.
Quick Ranges	Provides a list of pre-specified time ranges that you can choose.

Time Selector Dialog Box



After you make your choice, the time-selector label will reflect your selection.

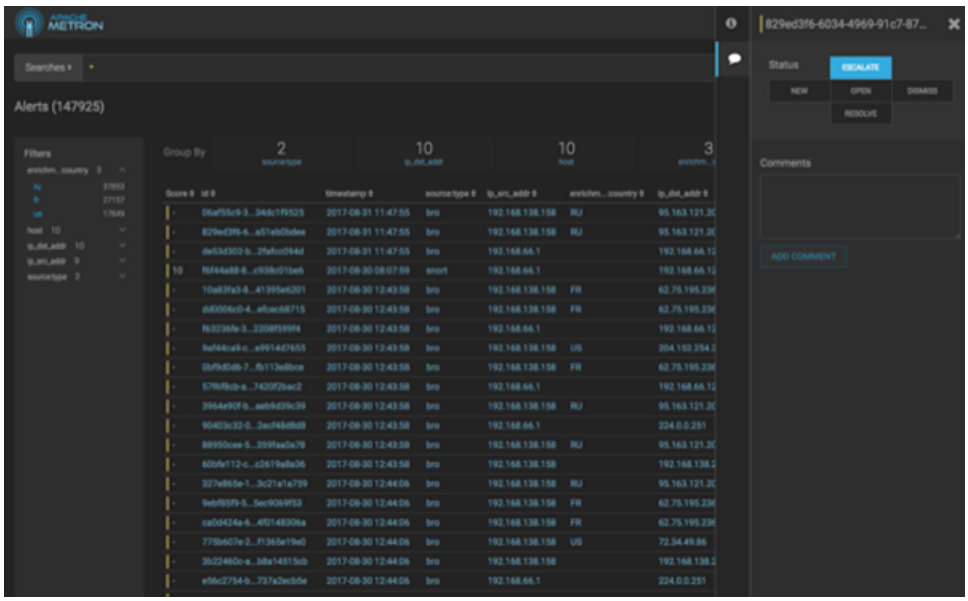
Filter Alerts

The Alerts UI currently provides five filters that you can apply to alerts. You can use these filters to refine the list of alerts and collect additional information on the alerts. These filters are listed in the **Filters** panel on the left of the **Alerts** window.

Procedure

1. Click one of the filters in the **Filters** panel on the left of the window.

   The Filter expands to list all of the facet values contained in the filter. For example, in the following figure, the **enrichments:geo_dst_addr:country** filter contain the countries Russia, France, and USA.



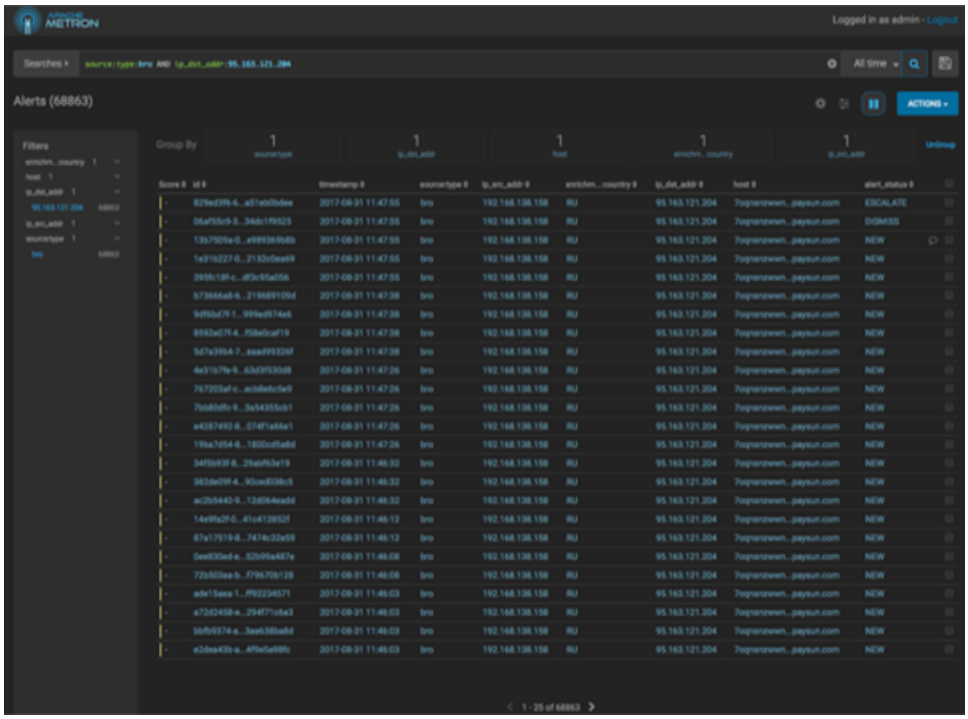
Note:

The UI displays the number of alerts corresponding to each facet next to the facet.

2. You can continue to apply filters to the alerts displayed in the **Alerts** window to further refine the alerts list.

   As you select filters and facets, they are displayed in the **Searches** field.

   For example, in the following figure, we've applied the source.type filter with the bro facet and then the ip_dst_addr filter with the IP address 95.163.121.204.



3. To clear filters that have been populated to the **Searches** field, click

   (delete icon) at the end of the **Searches** field.

Manage Alert Status

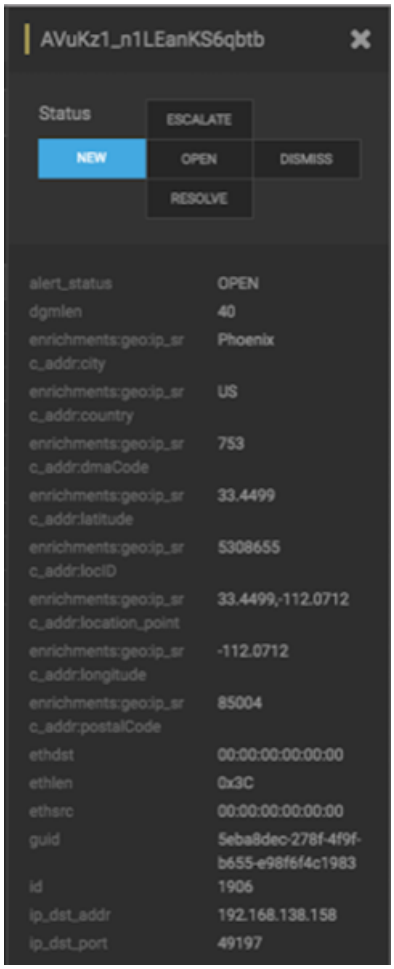
You can manage one or more alerts at a time using the **ACTIONS** menu. You can use the **ACTIONS** to change the status of or dismiss an alert.

Procedure

1. Select an alert by clicking on empty space in the alert row.

   The Alerts UI displays a panel listing the status of the alert all available data in Elasticsearch about the alert.

   Alerts Information Panel



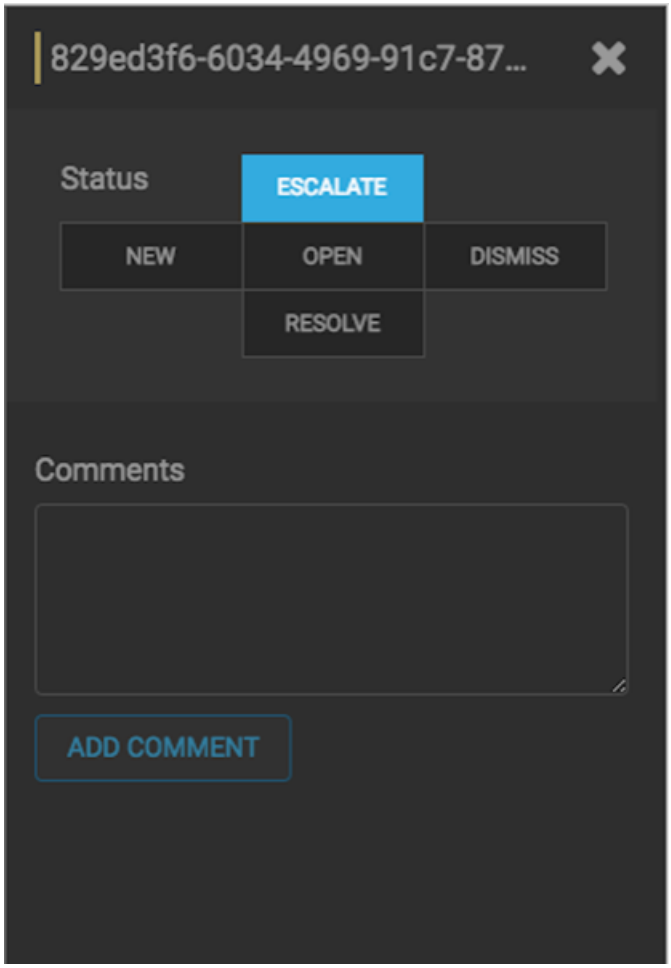
The current alert status is highlighted.

Note:

To manage more than one alert at a time, click the check boxes at the end of alert rows, then select the action you want to perform from the ACTIONS menu.

2. Click the new status you want to apply to the alert, then dismiss the panel.
3. You can also add a comment to this action by clicking

(Comment button), entering your comment in the **Comments** field, and clicking **ADD COMMENT**.



The Alerts UI indicates that an alert has one or more comments by displaying

(comment icon) next to the alert status in the **Alerts** window.

Note:

You cannot add a comment to an alert contained in a meta alert. You can only add comments to the meta alert.

4. To delete a comment, click the comment to delete, then click the trash can icon.
   Click OK in the **Confirmation** dialog box.

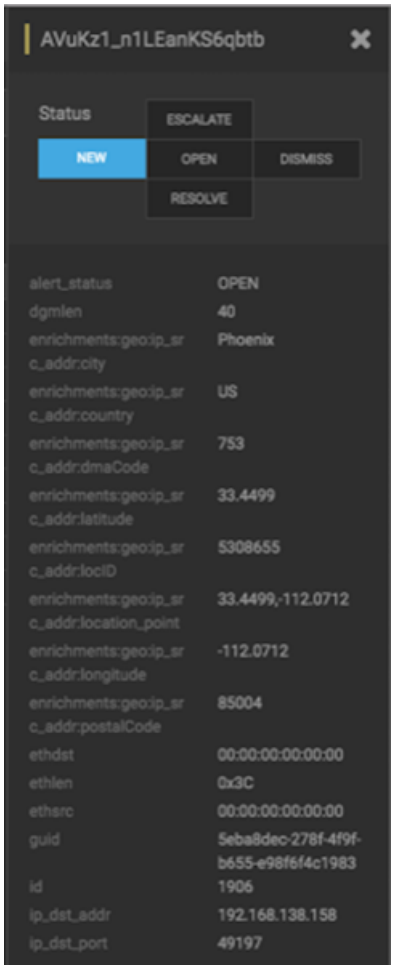
Escalate an Alert

You can escalate one or more alerts at a time to create an event that can be tracked by an external ticketing system.

Procedure

1. Select an alert by clicking on empty space in the alert row.
   The Alerts UI displays a panel listing the status of the alert all available data in Elasticsearch about the alert.

   Alerts Information Panel

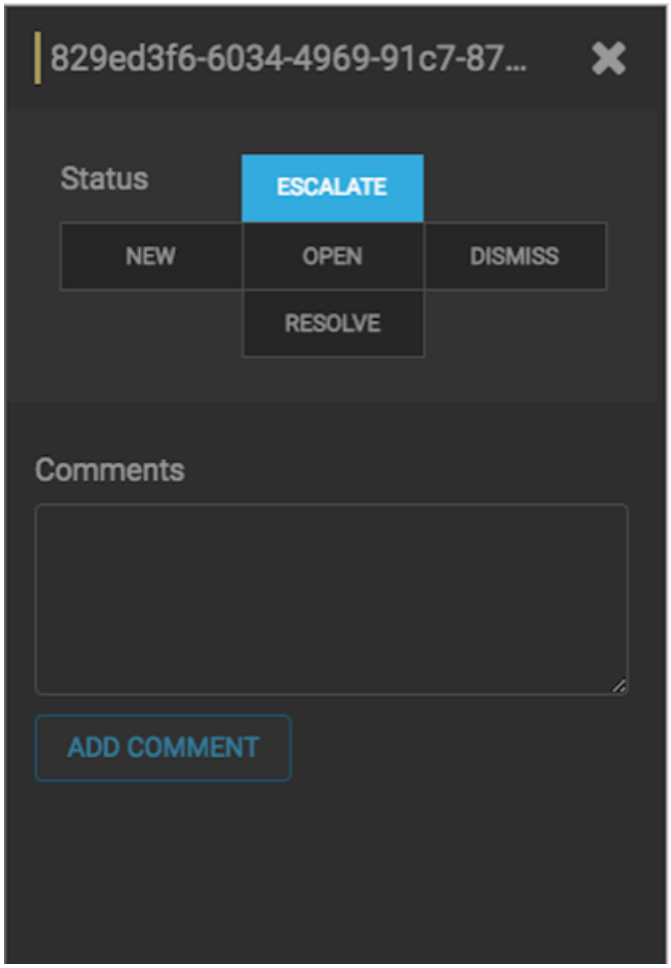


The current alert status is highlighted.

Note:

To manage more than one alert at a time, click the check boxes at the end of alert rows, then select the action you want to perform from the ACTIONS menu.

2. Click **Escalate**.



HCP writes the event to a Kafka escalation topic. An external orchestration software can pick up the event from the topic and use the API to create an incident or append to an existing incident.

3. You can also add a comment to this action by clicking

(Comment button), entering your comment in the **Comments** field, and clicking **ADD COMMENT**.

Group Alerts

You can group alerts so you can apply filters, status, etc. to multiple alerts at a time.

Procedure

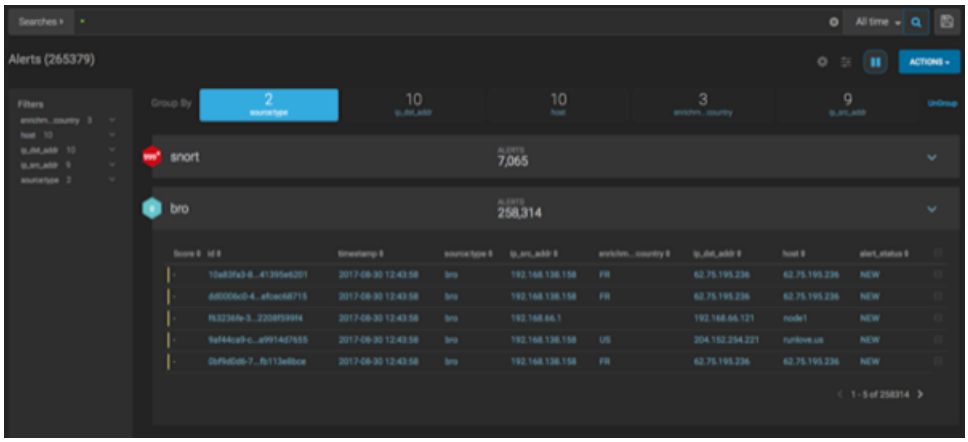
1. Click one of the groups listed by **Group By**.

   The **Alerts** table view changes to a tree view listing the values of the groups.

   In the following example, the group is source.type and the values are Snort and Bro.

Note: The icon to the left of the value provides the cumulative severity score for all the alerts in the value. If the score exceeds 999, then the value displays as 999+.

2. Click one of the values to list the alerts for that value.



3. You can click an alert to add it to the Searches field.

Note: Searches will search through all the groups, not just the group containing the alert.

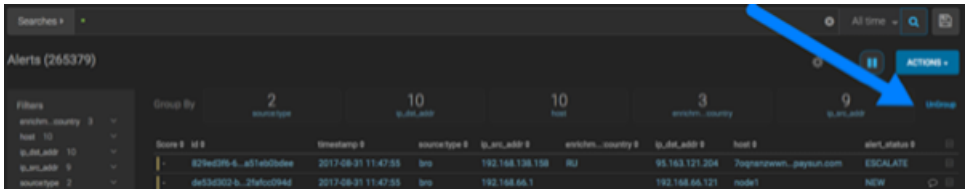
4. All features that are available for the Alerts table are available for the tree view.

For example, if you apply an action, such as Escalate, to an alert, it will apply to all alerts within the group. Similarly, if you search for a parameter, it will search all alerts within the group.

5. You can continue to refine your alerts by applying additional groups.

You can change the order in which the groups are applied to the alerts by clicking and dragging the groups on the **Groups By** line.

6. To ungroup your alerts and return to the Alerts window, click Ungroup which is located on the far right of the list of groups.



Create a Meta Alert

The meta alert feature enables you to create a save a group of filtered alerts. Like the group feature, you can group filtered alerts that pertain to an incident. However, with meta alert, you can save your grouping, creating a system entity, to view it later. Also, when you filter alerts, if a relevant alert is contained in a meta alert, the entire meta alert will be included in the filter results.

Procedure

1. Click one of the groups listed by **Group By**.

The **Alerts** table view changes to a tree view listing the values of the groups.

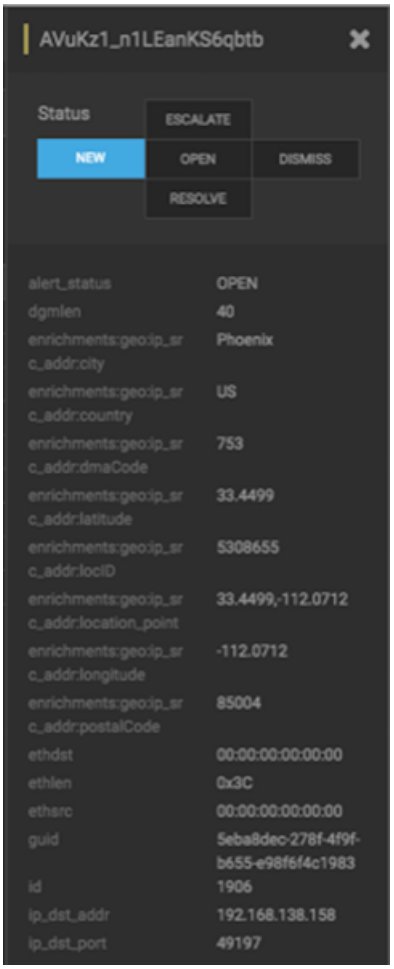
2. Use the **Search** and **GroupBy** options to create one or more groups containing alerts on which you want to focus.
3. When you have selected a group of alerts that you want to focus on, click

(meta alert icon), then confirm that you wish to create a meta alert with the selected alerts.

The meta alert disappears from the tree view. You can still see the meta alert in the alerts table view.

4. You can rename your meta alert by completing the following steps:
   a) Display the Alerts UI display panel by clicking on empty space in the meta alert row.

      Alerts Information Panel



   b) Click the current meta alert name at the top of the panel and enter your new meta alert name.
   c) Dismiss the panel by clicking the X in the upper right corner of the panel.

Save Your Searches

You can save your Alert searches for future reuse.

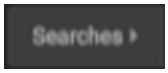
Procedure

1. To save a search, click the
   
   (save button) next to the **Searches** field.
2. When prompted, enter a name for the saved search parameters, then click **Save**.
   This will save both the search parameters and the column configurations.

View Your Recent and Saved Searches

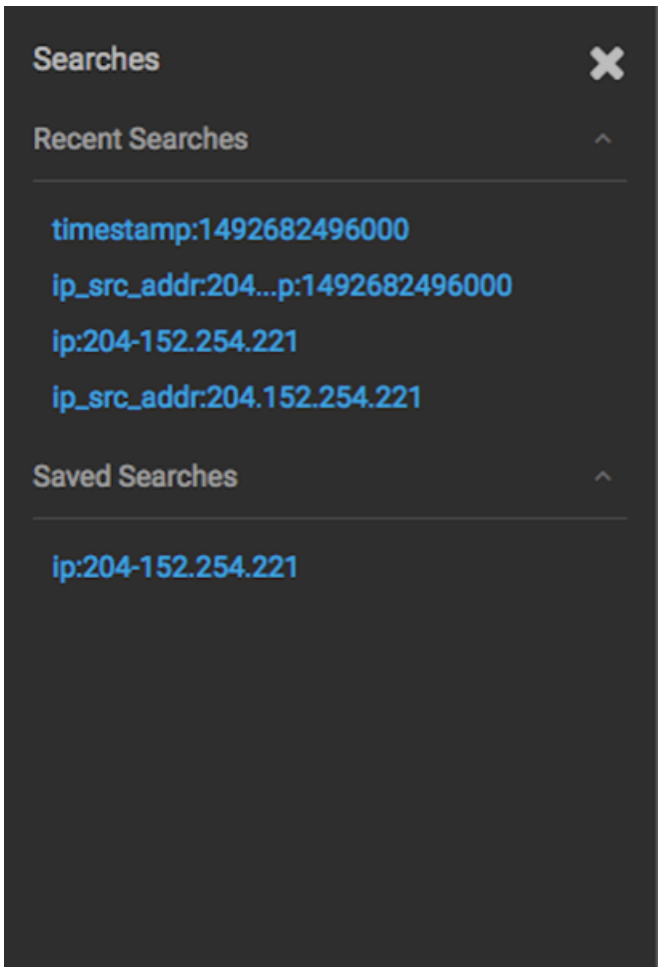
You can view both your recent searches and saved searches in the Alerts UI.

Procedure

Click the


button to the left of the **Searches** field.
The Alerts UI displays the Searches panel.

Searches Panel



The **Searches** panel lists two types of searches:

Recent Searches	This is a list of your most recent searches. To display the saved search, simply click on the search name. The Alerts UI saves a maximum of ten of your most recent searches.
Saved Searches	This is a list of your saved searches. To display the saved search, simply click on the search name. You can delete any of these saved searches by clicking the trash can icon that becomes visible when you mouse over each saved search.