

HCP Triaging Alerts 1

## Triaging Alerts

**Date of Publish:** 2018-10-15

<http://docs.hortonworks.com>

# Contents

<b>Triaging Alerts.....</b>	<b>3</b>
Launch the Alerts User Interface.....	3
Viewing Alerts.....	3
Using the Alerts Table.....	3
Search Alerts.....	7
Filter Alerts.....	8
Manage Alert Status.....	9
Escalate an Alert.....	11
Group Alerts.....	13
Create a Meta Alert.....	14
Save Your Searches.....	16
View Your Recent and Saved Searches.....	16

## 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:

<b>Red</b>	A score of 69 or higher
<b>Orange</b>	A score between 39 and 69
<b>Yellow</b>	A score below 39

The screenshot shows the Metron Alerts table with the following columns: Score, id, timestamp, source type, ip\_addr, enrichment\_country, host, and alert\_status. The table contains 265379 alerts, with the first 10 displayed. The scores are color-coded: Red (69 or higher), Orange (39-69), and Yellow (below 39).

Score	id	timestamp	source_type	ip_addr	enrichment_country	host	alert_status
69	82fad294-4...at14050d4e	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	ESCALATE
69	46532024-...256f0294d	2017-08-01 11:47:55	src	192.168.66.1		192.168.66.121	new
69	06af5249-3...346c179323	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	DISMISS
69	13617026-0...af99305646	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	af993056-0...256f0294d	2017-08-01 11:47:55	src	192.168.66.1		192.168.66.121	new
69	81d4743b-0...af10279839	2017-08-01 11:47:55	src	192.168.136.150	FR	62.75.195.236	new
69	2279a94-0...ac30f84746	2017-08-01 11:47:55	src	192.168.136.150	US	72.34.49.86	new
69	14d15274-0...313050a468	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	04657044-0...af60502356	2017-08-01 11:47:55	src	192.168.66.1		224.0.0.251	new
69	999b19f-0...af3c75a059	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	67984a6b-0...3196991094	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	17c2a850-0...af0ea973a8	2017-08-01 11:47:55	src	192.168.66.1		224.0.0.251	new
69	76923048-0...9a39306a62	2017-08-01 11:47:55	src	192.168.136.150	FR	62.75.195.236	new
69	9496a71-0...999ad714e6	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	cb0d54e-0...526ad7464a	2017-08-01 11:47:55	src	192.168.66.1		224.0.0.251	new
69	20309824-0...4951a2149e	2017-08-01 11:47:55	src	192.168.136.150		192.168.136.2	new
69	8030a714-0...f64e6a4719	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	6c7a3964-7...eae09320f	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	af6a3cda-0...119af6243a	2017-08-01 11:47:55	src	192.168.66.1		192.168.66.121	new
69	646b7d2-0...636a58726	2017-08-01 11:47:55	src	192.168.136.150	FR	62.75.195.236	new
69	89205ad-0...3aca02482	2017-08-01 11:47:55	src	192.168.136.150	FR	62.75.195.236	new
69	4cd176e-0...63a0f30a6	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	225af64-0...cf86267c14	2017-08-01 11:47:55	src	192.168.66.1		224.0.0.251	new
69	767202af-0...ac4646c569	2017-08-01 11:47:55	src	192.168.136.150	RU	95.165.121.204	new
69	6ca73a82-0...af60224760	2017-08-01 11:47:55	src	192.168.66.1		192.168.66.121	new

## 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

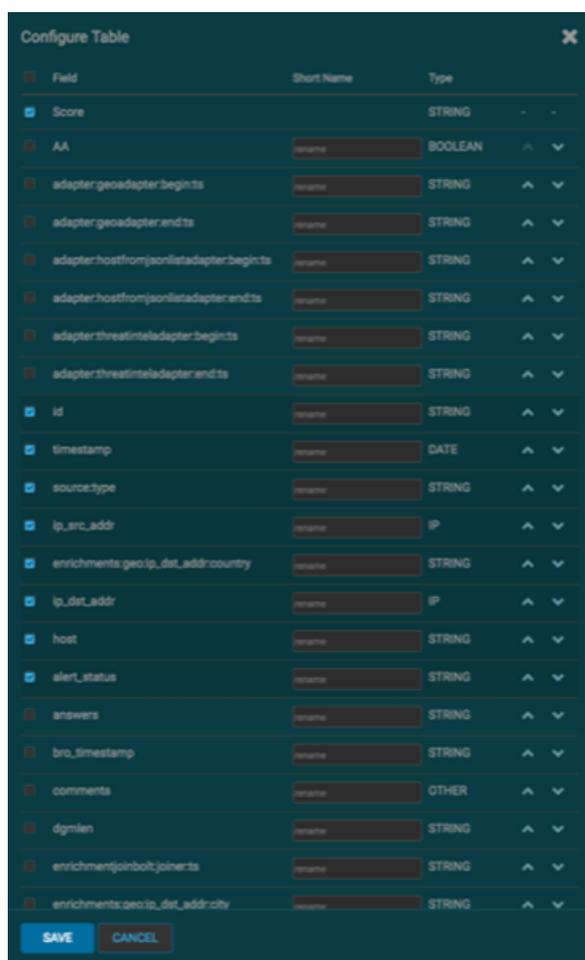
### 1. Click



(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.

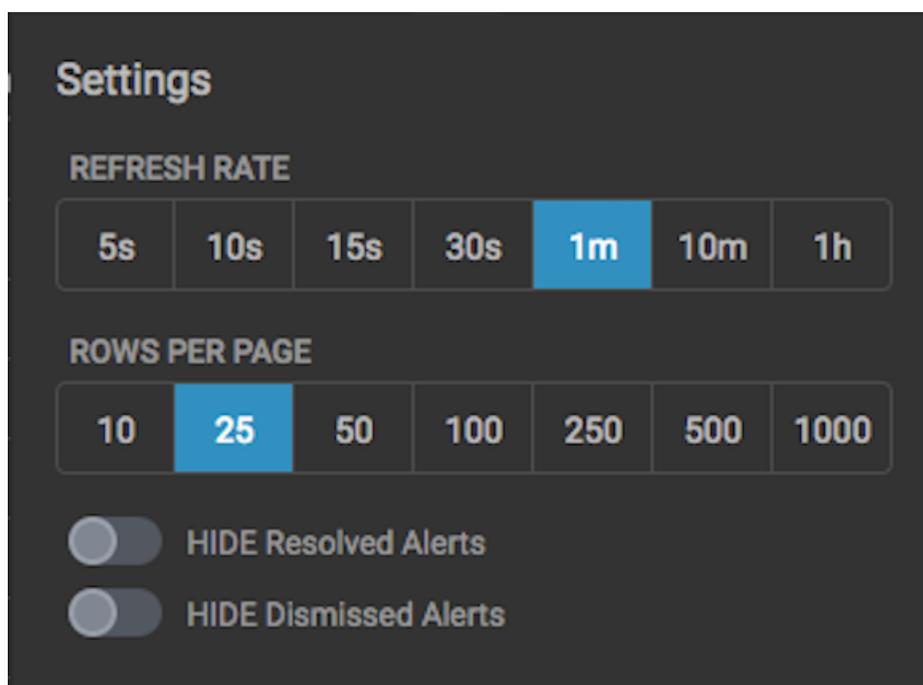
### Procedure

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

AVuKz1\_n1LEanKS6qbtb

Status

- ESCALATE
- NEW
- OPEN
- DISMISS
- RESOLVE

alert_status	OPEN
dgmlen	40
enrichments:geoip_src_addr:city	Phoenix
enrichments:geoip_src_addr:country	US
enrichments:geoip_src_addr:dmaCode	753
enrichments:geoip_src_addr:latitude	33.4499
enrichments:geoip_src_addr:locID	5308655
enrichments:geoip_src_addr:location_point	33.4499,-112.0712
enrichments:geoip_src_addr:longitude	-112.0712
enrichments:geoip_src_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f-b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

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.

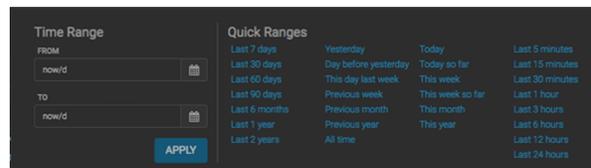
The time-range button defaults to **All time** which displays all alerts corresponding to the Searches parameters. To customize the time range, click the time-range drop-down menu and select one of the following:

**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.

Score	ID	Timestamp	Source Type	IP	Enrichment Country	Geo-Dst-Addr
1	06af3509-3_346c1f9323	2017-08-31 11:47:55	brp	192.168.138.158	RU	95.163.121.20
1	829ed3f6-4_a51eb0b0ee	2017-08-31 11:47:55	brp	192.168.138.158	RU	95.163.121.20
1	da534302-b_3fafcc084d	2017-08-31 11:47:55	brp	192.168.66.1		192.168.66.12
10	8f44a88-4_c93bc078e5	2017-08-30 08:07:59	smart	192.168.66.1		192.168.66.12
1	10e039d-4_41395e0301	2017-08-30 12:43:58	brp	192.168.138.158	FR	62.75.195.239
1	da0006d-4_af0ac08715	2017-08-30 12:43:58	brp	192.168.138.158	FR	62.75.195.239
1	83228fe-3_2208f9994	2017-08-30 12:43:58	brp	192.168.66.1		192.168.66.12
1	9af4ac0e-4_4914e76d5	2017-08-30 12:43:58	brp	192.168.138.158	US	204.192.254.1
1	06f4205-7_8d113ed0ee	2017-08-30 12:43:58	brp	192.168.138.158	FR	62.75.195.239
1	579680e-4_740202ae2	2017-08-30 12:43:58	brp	192.168.66.1		192.168.66.12
1	3964e0f-6_ade9d29c39	2017-08-30 12:43:58	brp	192.168.138.158	RU	95.163.121.20
1	90403d-0_2acfd8b0d8	2017-08-30 12:43:58	brp	192.168.66.1		224.0.0.251
1	8890cee-5_399Aa0a79	2017-08-30 12:43:58	brp	192.168.138.158	RU	95.163.121.20
1	405af112-c_c2619ab356	2017-08-30 12:43:58	brp	192.168.138.158		192.168.138.12
1	327e805e-1_3c21a1a799	2017-08-30 12:44:06	brp	192.168.138.158	RU	95.163.121.20
1	9e095f9-5_5ec9069f53	2017-08-30 12:44:06	brp	192.168.138.158	FR	62.75.195.239
1	ca0424e-6_4014820da	2017-08-30 12:44:06	brp	192.168.138.158	FR	62.75.195.239
1	779a07e-2_f1365e19e0	2017-08-30 12:44:06	brp	192.168.138.158	US	72.34.49.86
1	3c22460e-a_58a14315ab	2017-08-30 12:44:06	brp	192.168.138.158		192.168.138.12
1	e96c2734-b_73742e05de	2017-08-30 12:44:06	brp	192.168.66.1		224.0.0.251

**Note:**

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

- 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`.

The screenshot shows the Metron Alerts interface. At the top, the search bar contains the query: `source.type:bro AND ip_dst_addr:95.163.121.204`. Below the search bar, the Alerts window displays 68863 alerts. The interface includes a filters panel on the left and a table of alert details. The table columns include: Score, @type, @timestamp, @source.type, @ip\_dst\_addr, @host, @source.country, @ip\_src\_addr, @host, and @status. The table shows a list of alerts with their respective scores, timestamps, and status.

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



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

## Manage Alert Status

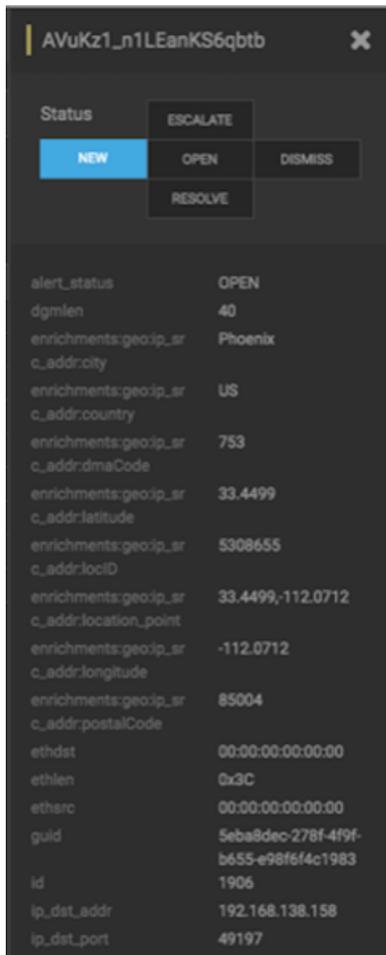
You can manage one or more alerts at a time using the **ACTIONS** menu. You can use the **ACTIONS** to change the status of or dismiss an alert.

### Procedure

- 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 screenshot shows a dark-themed alert triaging interface. At the top, there is a header with a close button (X) and a title 'AVuKz1\_n1LEanKS6qbtb'. Below the header is a 'Status' menu with five options: 'NEW' (highlighted in blue), 'ESCALATE', 'OPEN', 'DISMISS', and 'RESOLVE'. Below the menu is a list of alert details in a key-value format:

alert_status	OPEN
dgmlen	40
enrichments:geoip_src_addr:city	Phoenix
enrichments:geoip_src_addr:country	US
enrichments:geoip_src_addr:dmaCode	753
enrichments:geoip_src_addr:latitude	33.4499
enrichments:geoip_src_addr:locID	5308655
enrichments:geoip_src_addr:location_point	33.4499,-112.0712
enrichments:geoip_src_addr:longitude	-112.0712
enrichments:geoip_src_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f-b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

The current alert status is highlighted.

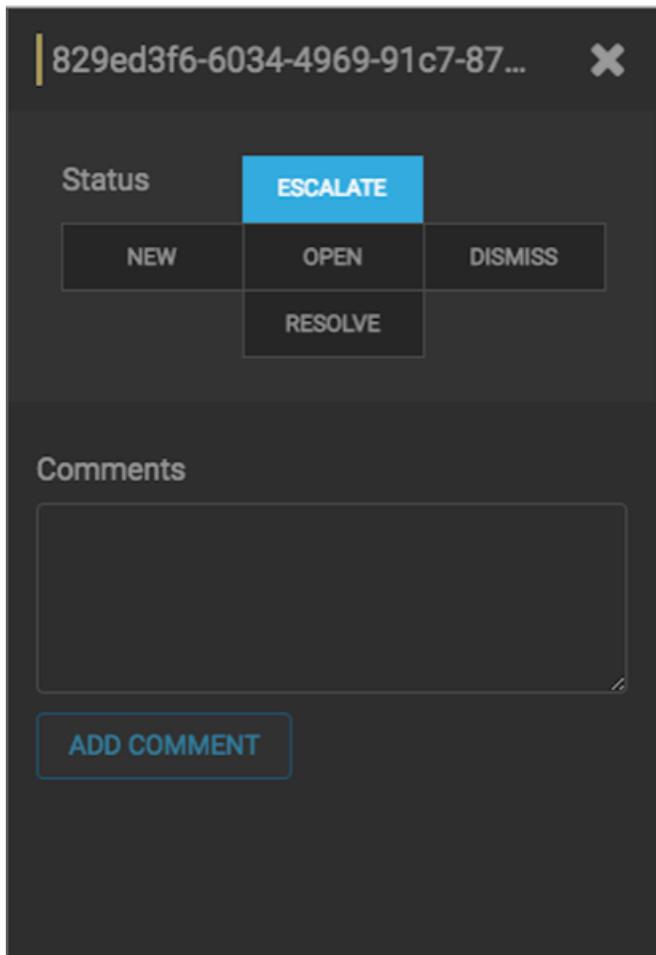
**Note:**

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.

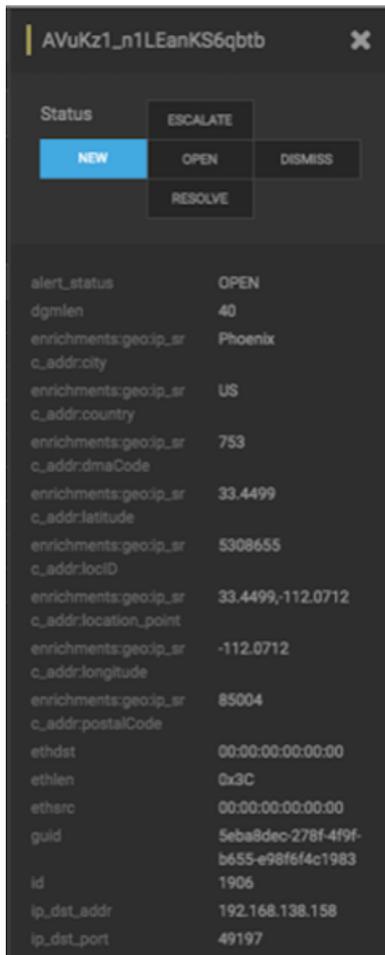
4. To delete a comment, click the comment to delete, then click the trash can icon.  
Click OK in the **Confirmation** dialog box.

## 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 screenshot shows a dark-themed interface for triaging alerts. At the top, there is a header with a close button (X) and a title 'AVuKz1\_n1LEanKS6qbtb'. Below the header is a 'Status' section with a grid of buttons: 'NEW' (highlighted in blue), 'ESCALATE', 'OPEN', 'DISMISS', and 'RESOLVE'. Below the status section is a list of alert details in a key-value format.

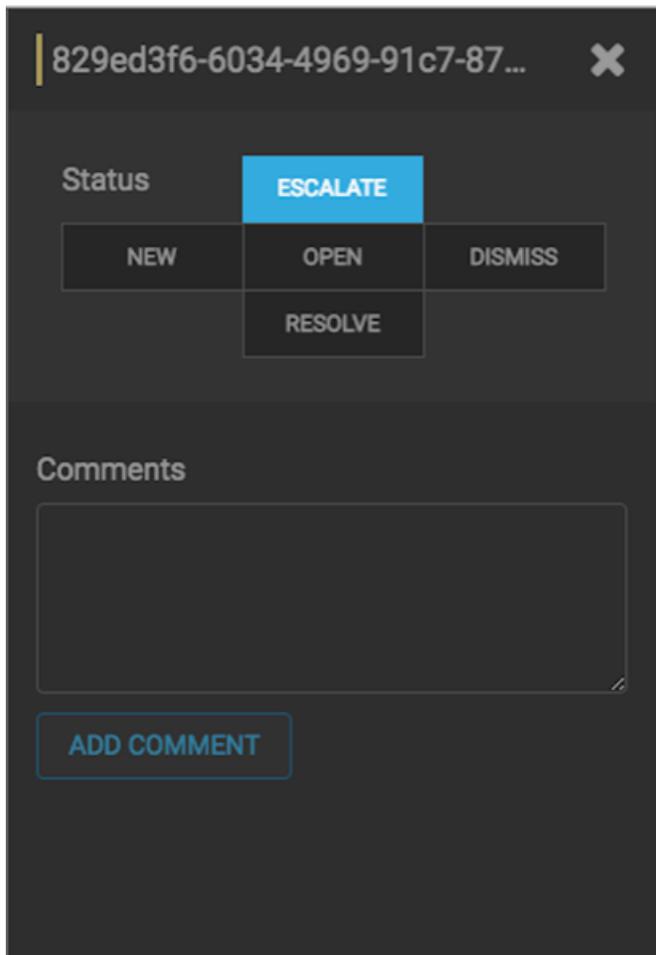
Key	Value
alert_status	OPEN
dgmlen	40
enrichments:geoip_src_addr:city	Phoenix
enrichments:geoip_src_addr:country	US
enrichments:geoip_src_addr:dmaCode	753
enrichments:geoip_src_addr:latitude	33.4499
enrichments:geoip_src_addr:locID	5308655
enrichments:geoip_src_addr:location_point	33.4499,-112.0712
enrichments:geoip_src_addr:longitude	-112.0712
enrichments:geoip_src_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f-b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

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**.



829ed3f6-6034-4969-91c7-87... ✕

Status

NEW OPEN DISMISS

RESOLVE

ESCALATE

Comments

ADD COMMENT

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**.

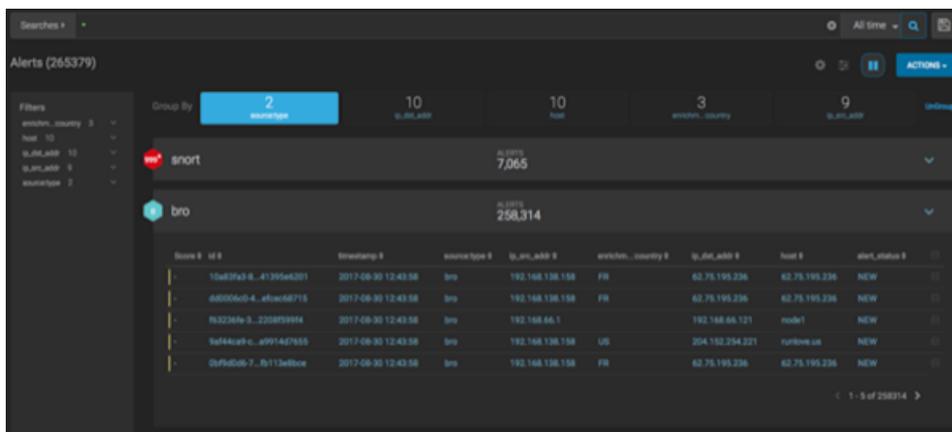
The **Alerts** table view changes to a tree view listing the values of the groups.

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+.

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



- 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.

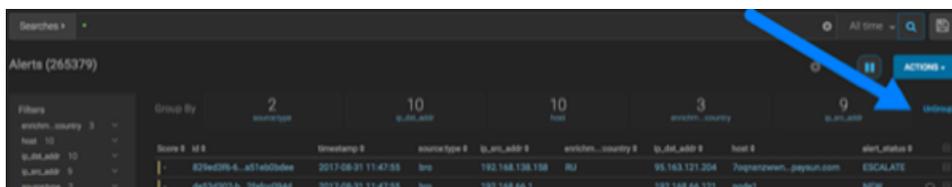
- All features that are available for the Alerts table are available for the tree view.

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.

- 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 **Group By** line.

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



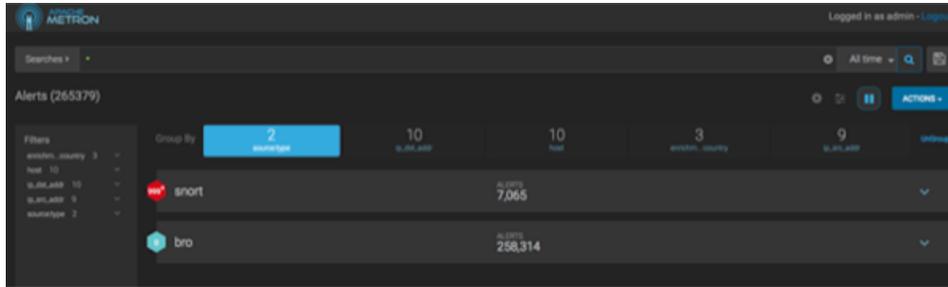
## Create a Meta Alert

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

- 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

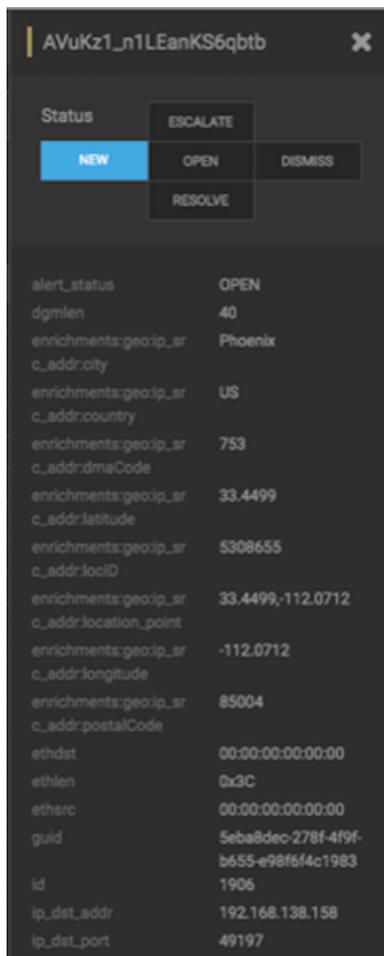


(meta alert icon), then confirm that you wish to create a meta alert with the selected alerts.

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

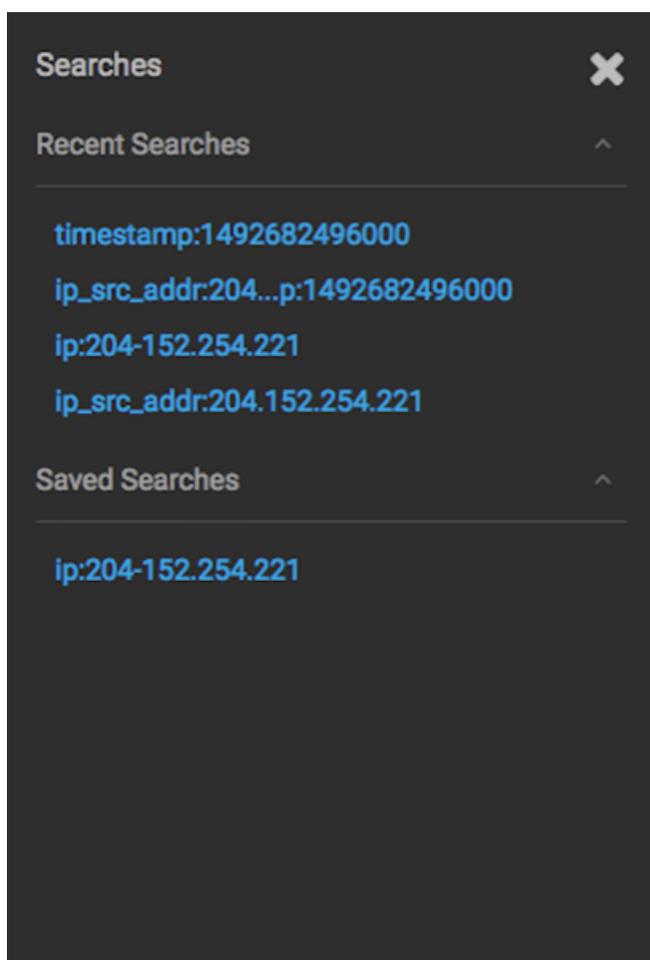
Click the



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.