

HCP Triaging Alerts 1

Triaging Alerts

Date of Publish: 2019-3-18



<https://docs.hortonworks.com>

Contents

Launch the Alerts User Interface.....	3
Getting Started with the Alerts User Interface.....	3
Viewing Alerts.....	4
Using the Alerts Table.....	4
Configure Table Columns.....	5
Configure Table Row Settings.....	7
Display Additional Alerts Information.....	8
Search Alerts.....	10
Filter Alerts.....	10
Manage Alert Status.....	12
Escalate an Alert.....	16
Group Alerts.....	19
Create a Meta Alert.....	20
Save Your Searches.....	22
View Your Recent and Saved Searches.....	22

Launch the Alerts User Interface

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. 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.

Getting Started with the Alerts User Interface

The Alerts user interface provides mechanisms for viewing alerts, searching and filtering alerts, grouping alerts to facilitate management, and changing alert status. The Alerts user interface defaults to displaying the Alerts table when first opened.

You can use the Alerts user interface tool bar to perform searches and manage the Alerts UI settings.

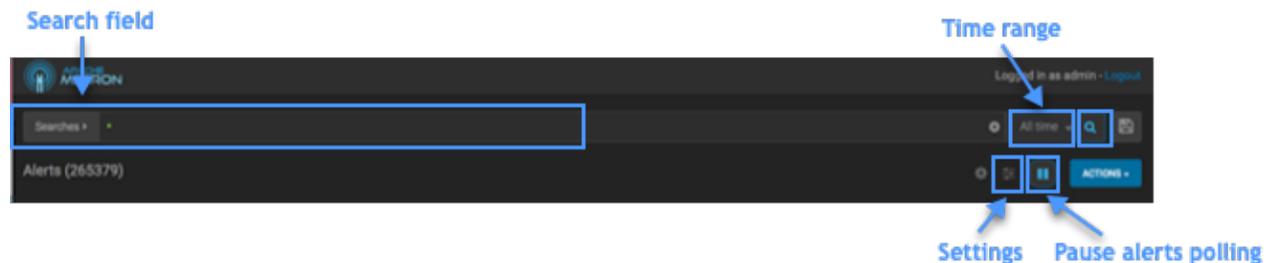


Table 1: Alerts UI Tool Bar

Tools	Description
Search 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.
Settings	You can configure the table row settings in the Alerts table to modify the appearance of the Alerts table and the refresh rate.
Pause alerts	You can pause the Alerts UI polling while you adjust settings or focus on current alerts.
Time range	You can set the time range over which to perform alert polling or choose one of the predefined quick ranges.

You can use the Alerts table to view and manage alerts:

The screenshot displays the Metron Alerts table with the following components:

- Filter panel:** Located on the left, it includes filters for 'watcher_country', 'host', 'ip_addr', 'ip_addr_2', and 'watcher_type'.
- Group and ungroup:** Buttons at the top right of the table for managing alert groups.
- Alert status:** A column on the right side of the table for changing the status of individual alerts.
- Alerts table:** The main table containing columns for 'id', 'timestamp', 'source_type', 'ip_addr', 'watcher_country', 'ip_addr_2', 'host', and 'alert_status'.

Table 2: Alerts Table

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.
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.

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.

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

Alerts (265379)

Filters: enrich...country: 3, host: 10, ip_dst_addr: 9, ip_src_addr: 9, sourceType: 2

Group By: sourceType: 2, ip_src_addr: 10, host: 10, enrich...country: 3, ip_dst_addr: 9

Score	id	Timestamp	sourceType	ip_src_addr	enrich...country	ip_dst_addr	host	alert_status
82	9ed395-6...a51e40bdae	2017-08-31 11:47:55	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	ESCALATE
66	53302-b...2fa5c094d	2017-08-31 11:47:55	dns	192.168.66.1		192.168.66.121	node1	NEW
66	53302-b...34dc1f925	2017-08-31 11:47:55	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	DISMISS
130	7505a-0...e993c968d	2017-08-31 11:47:55	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
64	5536-0...25b707a7	2017-08-31 11:47:55	dns	192.168.66.1		192.168.66.121	node1	NEW
81	49742e-e...a510275699	2017-08-31 11:47:55	dns	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
32	70e9a-6...ac309d74e	2017-08-31 11:47:55	dns	192.168.138.158	US	72.34.49.86	comcastsecurity.com	NEW
14	31a227-0...2132c0e69	2017-08-31 11:47:55	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
64	5797e-f...ae8db0236	2017-08-31 11:47:55	dns	192.168.66.1		224.0.0.251		NEW
39	9c18f-c...df3c95d09	2017-08-31 11:47:55	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
57	366a8-6...219689109d	2017-08-31 11:47:58	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
17	2c850-c...d80e970a8	2017-08-31 11:47:58	dns	192.168.66.1		224.0.0.251		NEW
76	2098-4...9c393804d2	2017-08-31 11:47:58	dns	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
56	5a27f-1...995ed974e5	2017-08-31 11:47:58	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
60	034a-b...329a47499a	2017-08-31 11:47:58	dns	192.168.66.1		224.0.0.251		NEW
20	0982-d...491d0149e	2017-08-31 11:47:58	dns	192.168.138.158		192.168.138.2		NEW
80	5a07f-4...708dc0af19	2017-08-31 11:47:58	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
56	3954-7...eeed9932df	2017-08-31 11:47:58	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
60	afcbda-8...11ba5a243a	2017-08-31 11:47:58	dns	192.168.66.1		192.168.66.121	node1	NEW
64	97c2-0...635dc56726	2017-08-31 11:47:58	dns	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
80	550d-5...bcb00482	2017-08-31 11:47:26	dns	192.168.138.158	FR	62.75.195.236	03af02.cbl...ngrams.in	NEW
46	3179e-9...63d3f3068	2017-08-31 11:47:26	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
32	af6d-9...c09097c14	2017-08-31 11:47:26	dns	192.168.66.1		224.0.0.251		NEW
76	202af-c...e0b8efc9f	2017-08-31 11:47:26	dns	192.168.138.158	RU	95.163.121.204	7ogpnczewn...paysun.com	NEW
64	5b82-6...d4d3204765	2017-08-31 11:47:26	dns	192.168.66.1		192.168.66.121	node1	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

Configure Table ✕

Field	Short Name	Type		
<input checked="" type="checkbox"/> Score		STRING	-	-
<input type="checkbox"/> AA	<input type="text" value="name"/>	BOOLEAN	^	v
<input type="checkbox"/> adapter:geoadapter:begin:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> adapter:geoadapter:end:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> adapter:hostfromjsonlistadapter:begin:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> adapter:hostfromjsonlistadapter:end:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> adapter:threatinteladapter:begin:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> adapter:threatinteladapter:end:ts	<input type="text" value="name"/>	STRING	^	v
<input checked="" type="checkbox"/> id	<input type="text" value="name"/>	STRING	^	v
<input checked="" type="checkbox"/> timestamp	<input type="text" value="name"/>	DATE	^	v
<input checked="" type="checkbox"/> source:type	<input type="text" value="name"/>	STRING	^	v
<input checked="" type="checkbox"/> ip_src_addr	<input type="text" value="name"/>	IP	^	v
<input checked="" type="checkbox"/> enrichments:geo:ip_dst_addr:country	<input type="text" value="name"/>	STRING	^	v
<input checked="" type="checkbox"/> ip_dst_addr	<input type="text" value="name"/>	IP	^	v
<input checked="" type="checkbox"/> host	<input type="text" value="name"/>	STRING	^	v
<input checked="" type="checkbox"/> alert_status	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> answers	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> bro_timestamp	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> comments	<input type="text" value="name"/>	OTHER	^	v
<input type="checkbox"/> dgmlen	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> enrichment joinbolt:joiner:ts	<input type="text" value="name"/>	STRING	^	v
<input type="checkbox"/> enrichments:geo:ip_dst_addr:city	<input type="text" value="name"/>	STRING	^	v

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

A screenshot of the Alerts Settings Panel. The panel has a dark background and is titled "Settings". It contains two sections: "REFRESH RATE" and "ROWS PER PAGE". The "REFRESH RATE" section has seven buttons: "5s", "10s", "15s", "30s", "1m", "10m", and "1h". The "1m" button is highlighted in blue. The "ROWS PER PAGE" section has seven buttons: "10", "25", "50", "100", "250", "500", and "1000". The "25" button is highlighted in blue. At the bottom, there are two toggle switches, both of which are currently turned off. The first toggle is labeled "HIDE Resolved Alerts" and the second is labeled "HIDE Dismissed Alerts".

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

NEW	ESCALATE	
	OPEN	DISMISS
	RESOLVE	

alert_status OPEN

dgmlen 40

enrichments:geo:ip_sr Phoenix

c_addr:city

enrichments:geo:ip_sr US

c_addr:country

enrichments:geo:ip_sr 753

c_addr:dmaCode

enrichments:geo:ip_sr 33.4499

c_addr:latitude

enrichments:geo:ip_sr 5308655

c_addr:locID

enrichments:geo:ip_sr 33.4499,-112.0712

c_addr:location_point

enrichments:geo:ip_sr -112.0712

c_addr:longitude

enrichments:geo:ip_sr 85004

c_addr:postalCode

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.

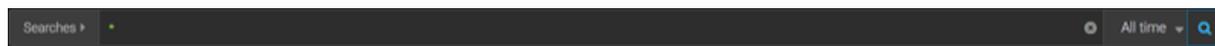
Procedure

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:

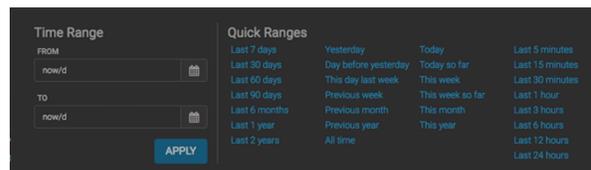
Time Range

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.

The screenshot shows the Armitage Metron Alerts interface. On the left, the 'Filters' panel is expanded to show 'enrichments:geo_dst_addr:country' with three facet values: 'ru' (3799), 'fr' (27187), and 'us' (17649). The 'Alerts (147925)' window displays a table of alerts with columns for Score, ID, timestamp, source.type, ip_dst_addr, enrichments:geo_dst_addr:country, and ip_dst_addr. The table is grouped by source.type (2), ip_dst_addr (10), and host (10). The right sidebar shows the alert status (INITIATE), comments, and a table of actions (NEW, OPEN, DISMISS, RESOLVE).

Score	ID	timestamp	source.type	ip_dst_addr	enrichments:geo_dst_addr:country	ip_dst_addr
-	06af53c9-3...34dc179525	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
-	829ed3f6-6...a514b0bde6	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
-	d633d302-b...2fa5cc094d	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.12
10	f644a688-6...c958cd1ba6	2017-08-30 08:07:59	snort	192.168.66.1		192.168.66.12
-	10a83fa3-8...41395e6201	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	68306c0-4...af6cc68715	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	f63236fe-3...2208f9994	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
-	9af44cc9-c...a9914d7655	2017-08-30 12:43:58	bro	192.168.138.158	US	204.152.254.1
-	0af9d0b6-7...fb113e8bce	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	579f8cb-e...7420f2bae2	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
-	3964e90f-b...a69f439c39	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
-	90403c32-0...2acc4469d8	2017-08-30 12:43:58	bro	192.168.66.1		224.0.0.251
-	68950cee-5...359fca0a78	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
-	609fe112-c...c2619a8a36	2017-08-30 12:43:58	bro	192.168.138.158		192.168.138.2
-	327e865e-1...3c21a1a799	2017-08-30 12:44:06	bro	192.168.138.158	RU	95.163.121.20
-	9abf8379-5...5ec9069f53	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
-	ca06424e-6...40148306a	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
-	779b607e-2...f1365e19e0	2017-08-30 12:44:06	bro	192.168.138.158	US	72.34.49.86
-	3c22460e-a...3ba1451c0b	2017-08-30 12:44:06	bro	192.168.138.158		192.168.138.2
-	e56c2754-b...737a3ecb5e	2017-08-30 12:44:06	bro	192.168.66.1		224.0.0.251



Note:

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

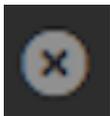
2. You can continue to apply filters to the alerts displayed in the **Alerts** window to further refine the alerts list.

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.

The screenshot shows the Metron Alerts interface. At the top, there's a search bar with the query: `source.type:bro AND ip_dst_addr:95.163.121.204`. Below the search bar, there are filters for `enrich..._country`, `host`, `ip_dst_addr`, and `source.type`. The main area displays a table of alerts with columns: `Score #`, `id #`, `timestamp #`, `source.type #`, `ip_src_addr #`, `enrich..._country #`, `ip_dst_addr #`, `host #`, and `alert_status #`. The table contains 25 rows of alert data, all with a status of 'NEW'.

- 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

AVuKz1_n1LEanKS6qbtb
✕

Status	ESCALATE	
	NEW	DISMISS
	OPEN	
	RESOLVE	

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_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**.

829ed3f6-6034-4969-91c7-87... ✕

Status

NEW	ESCALATE	DISMISS
	RESOLVE	

Comments

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

AVuKz1_n1LEanKS6qbtb
✕

Status	ESCALATE	
	NEW	DISMISS
	OPEN	
	RESOLVE	

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_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

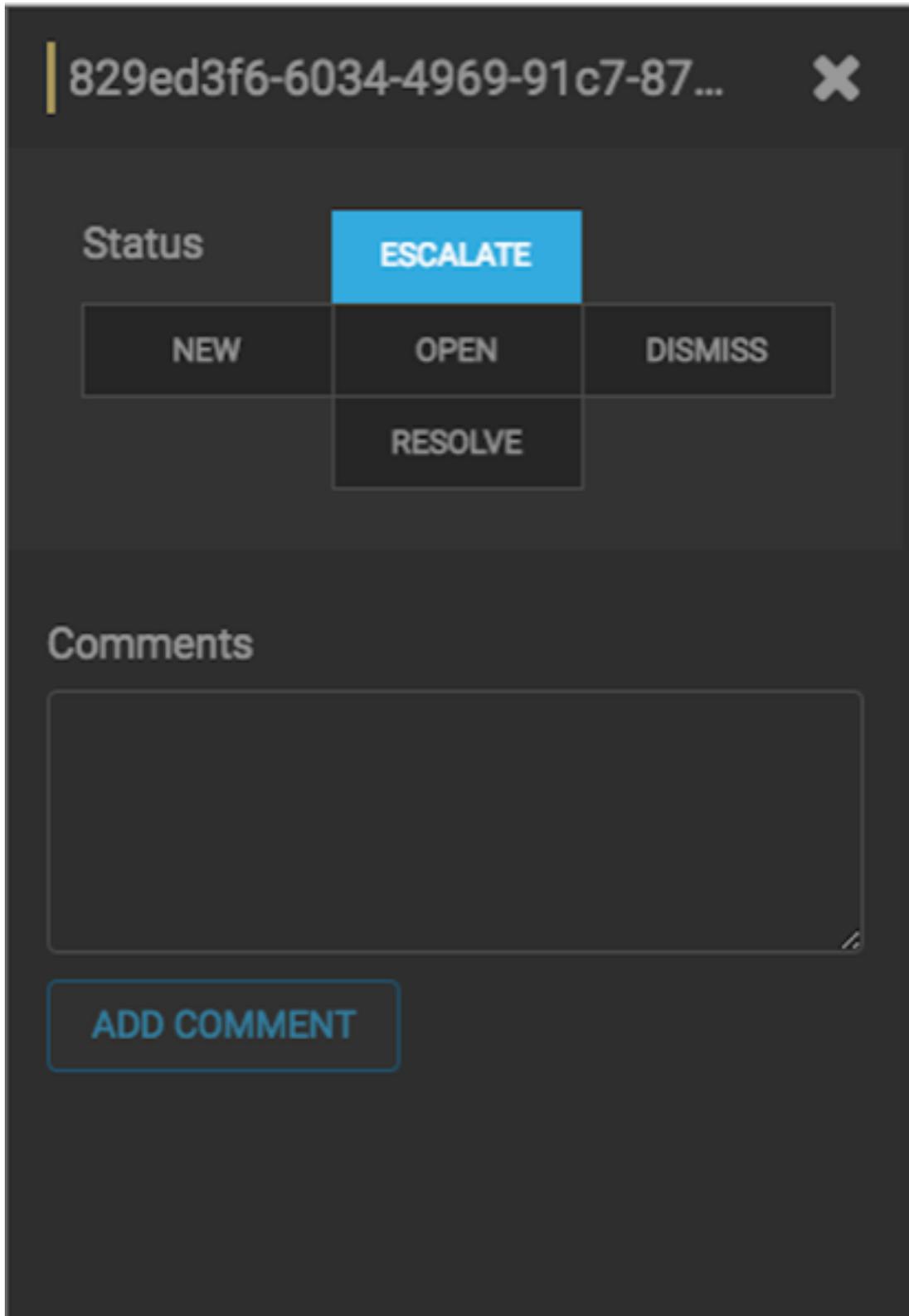
The current alert status is highlighted.



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**.



The screenshot shows a dark-themed alert triaging interface. At the top, there is a header with a yellow vertical bar on the left, a truncated ID '829ed3f6-6034-4969-91c7-87...' in the center, and a close button 'X' on the right. Below the header is a 'Status' section containing a grid of buttons: 'NEW', 'OPEN', 'DISMISS', and 'RESOLVE'. The 'ESCALATE' button is highlighted in blue and is positioned above the 'OPEN' button. Below the status section is a 'Comments' section with a large text input area and an 'ADD COMMENT' button at the bottom.

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.

- 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

- 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.

Score	Id	timestamp	source.type	ip.src_addr	src.host	ip.dst_addr	host	alert.status
10	10a83fa3-6...41395e6201	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
60	60006c0-4...ef0ac68719	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
6	63236fe-3...2208f9994	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.121	node1	NEW
6	6e944ca9-c...a9914d7955	2017-08-30 12:43:58	bro	192.168.138.158	US	204.152.234.221	runlove.us	NEW
0	0d9fd0d6-7...8113ed8ce	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW

- 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.

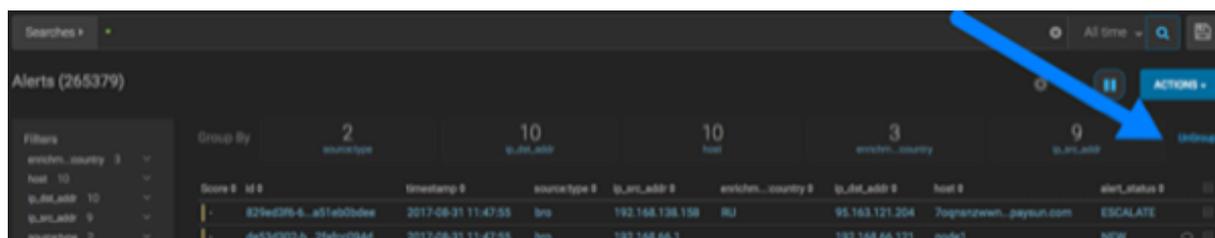
- All features that are available for the Alerts table are available for the tree view.

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 **Groups 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.



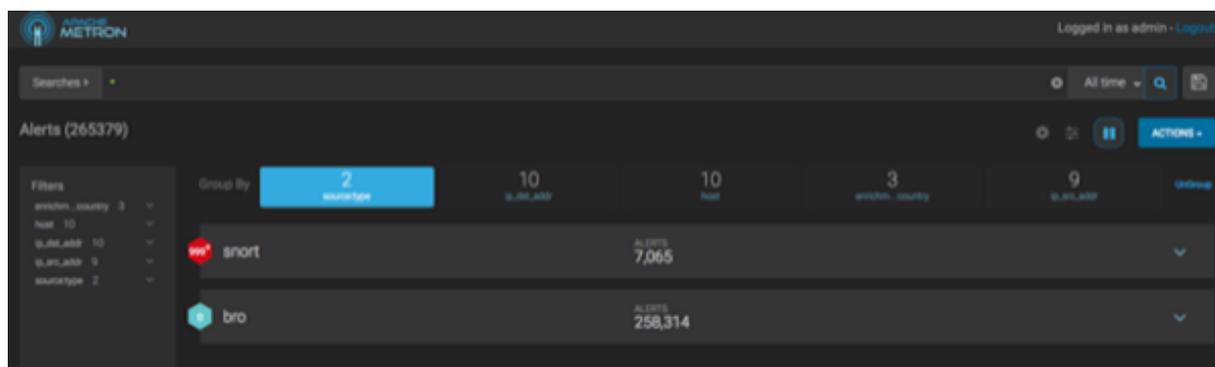
Create a Meta Alert

The meta alert feature enables you to create and 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.

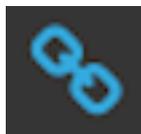
Procedure

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

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



- Use the **Search** and **GroupBy** options to create one or more groups containing alerts on which you want to focus.
- 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.

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

Alerts Information Panel

The screenshot shows a meta alert panel with the following components:

- Alert Name:** AVuKz1_n1LEanKS6qbtb (with a close 'X' button)
- Status Menu:** A grid of buttons for 'NEW' (highlighted in blue), 'ESCALATE', 'OPEN', 'DISMISS', and 'RESOLVE'.
- Alert Details Table:**

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	Seba8dec-278f-4f9f- b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

- 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.

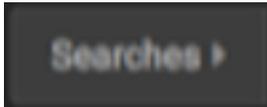
2. When prompted, enter a name for the saved search parameters, then click **Save**.
This will save both the search parameters and the column configurations.

View Your Recent and Saved Searches

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

Procedure

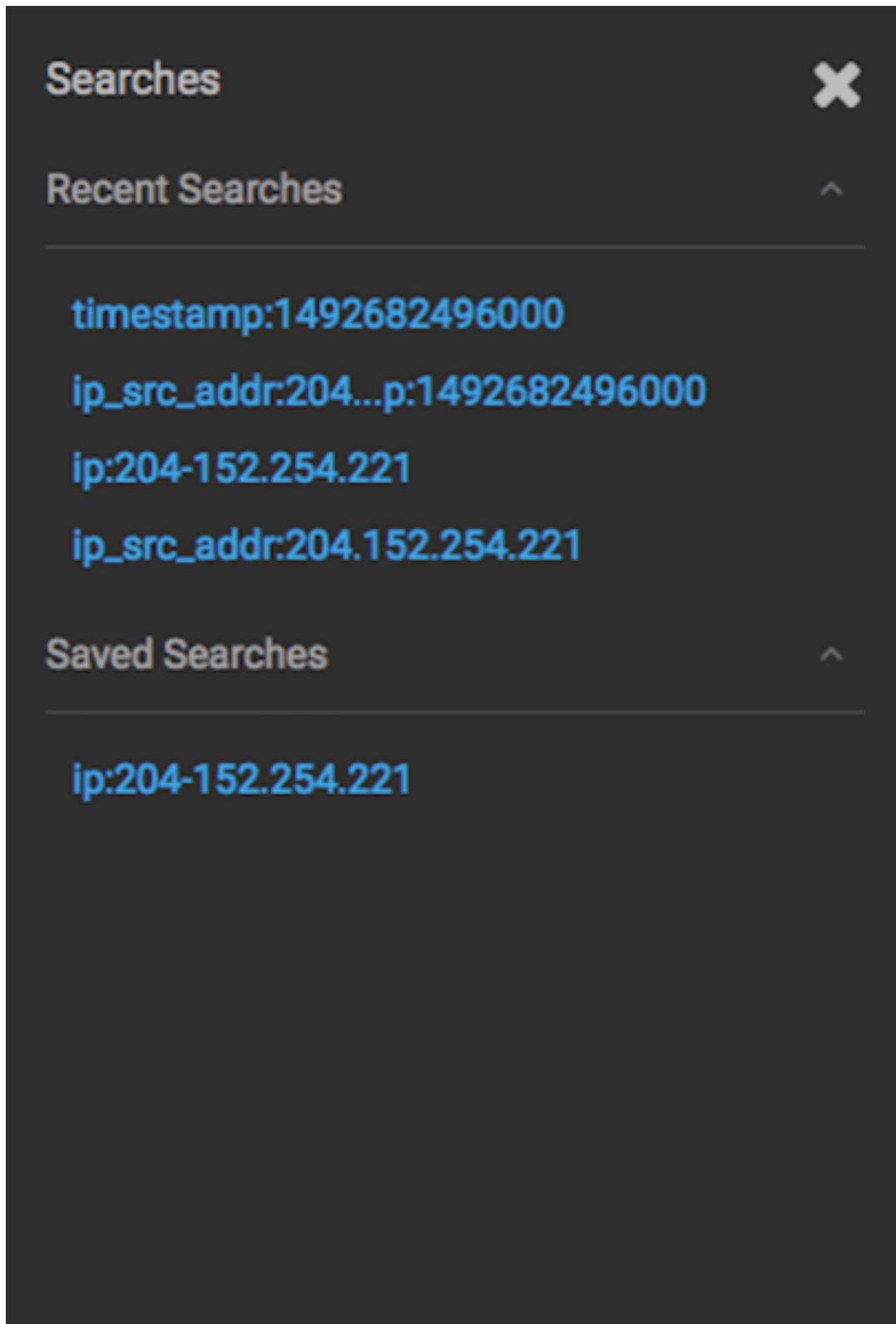
Click the



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.

Saved Searches

The Alerts UI saves a maximum of ten of your most recent 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.