CCP Triaging Alerts 2.0.0

Investigating Alerts

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

Investigating Alerts Overview

The Alerts user interface frequently produces large amounts of data. You can use features of the Alerts UI to refine and investigate the alert information to identify malicious events.

Filter Alerts

The first Alerts UI feature you can use to focus your data is **Filters**. You can use **Filters** to choose the type of data you are viewing.

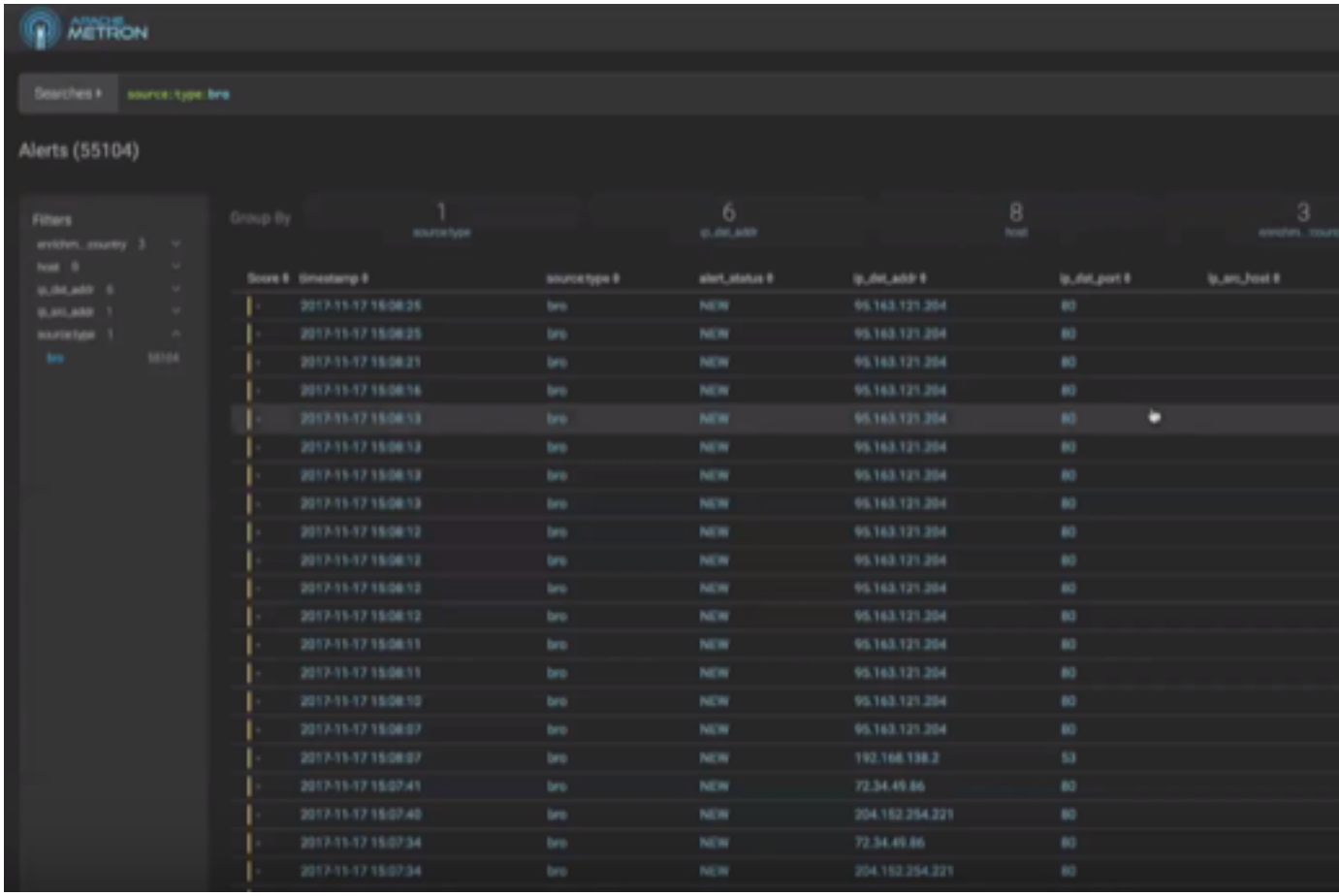
Procedure

1. In the **Filters** panel on the left of the window, click the Bro filter.

   The central panel of the Alerts UI displays all of the Bro data it has received.

   Note:

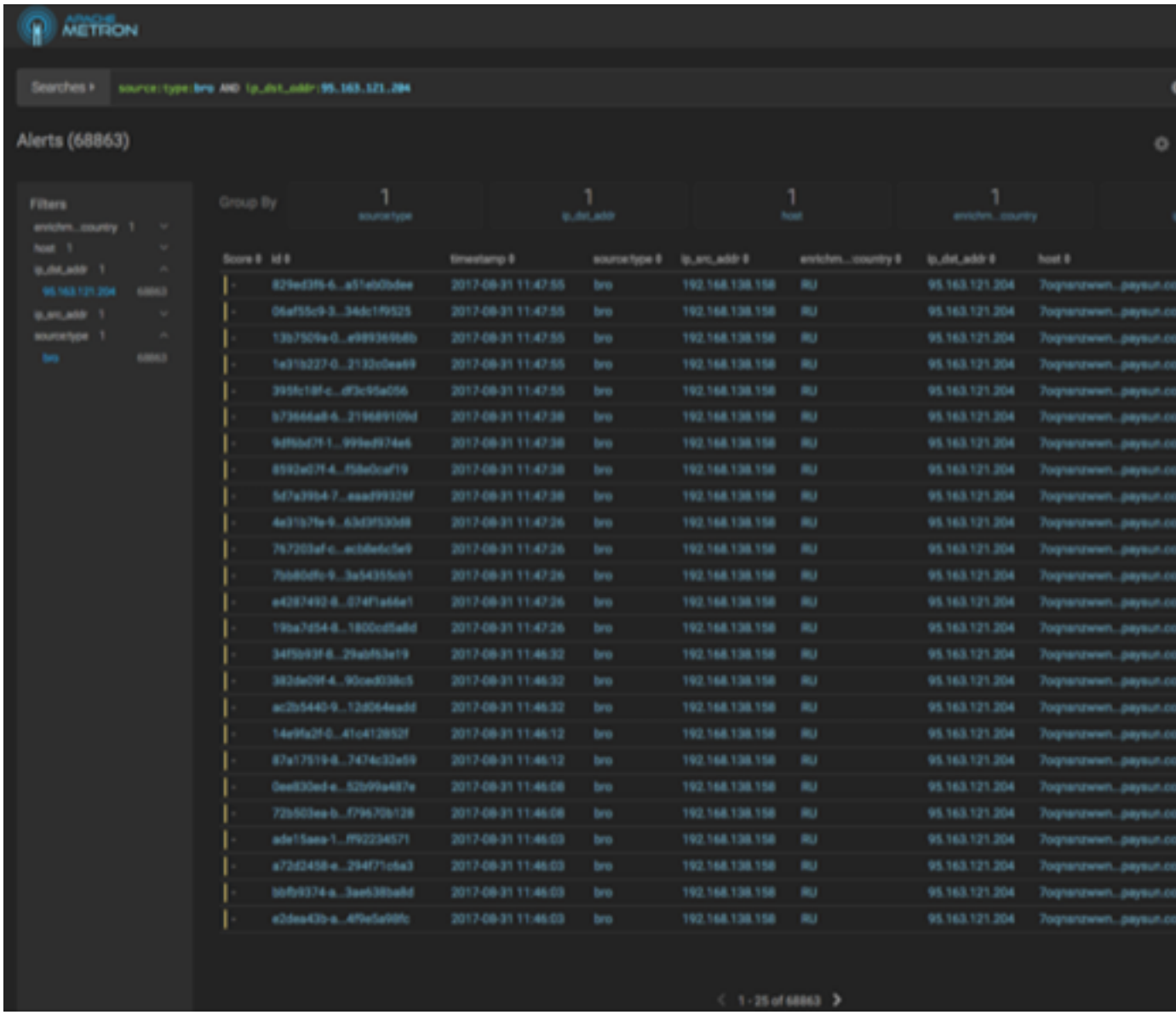
   Next to the Bro filter, the UI displays the total number of Bro alerts.



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.

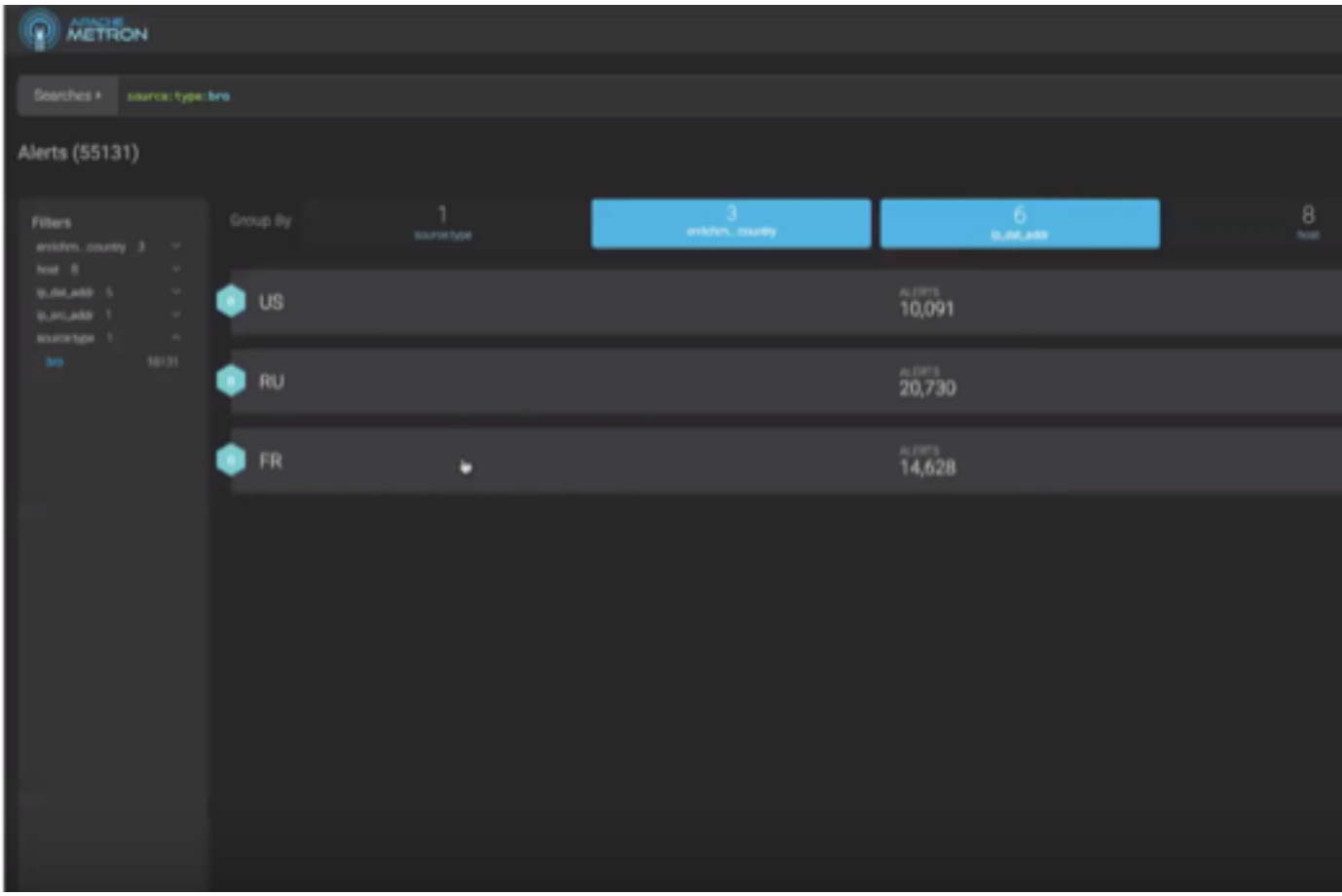
Group Alerts

Frequently, there are a large number of alerts contained in each of the **Filters**. To further refine the alert data, you can use the **Group By** feature. In addition to limiting the type of data you are viewing, you can apply searches, status, etc. to all the alerts in a group at the same time.

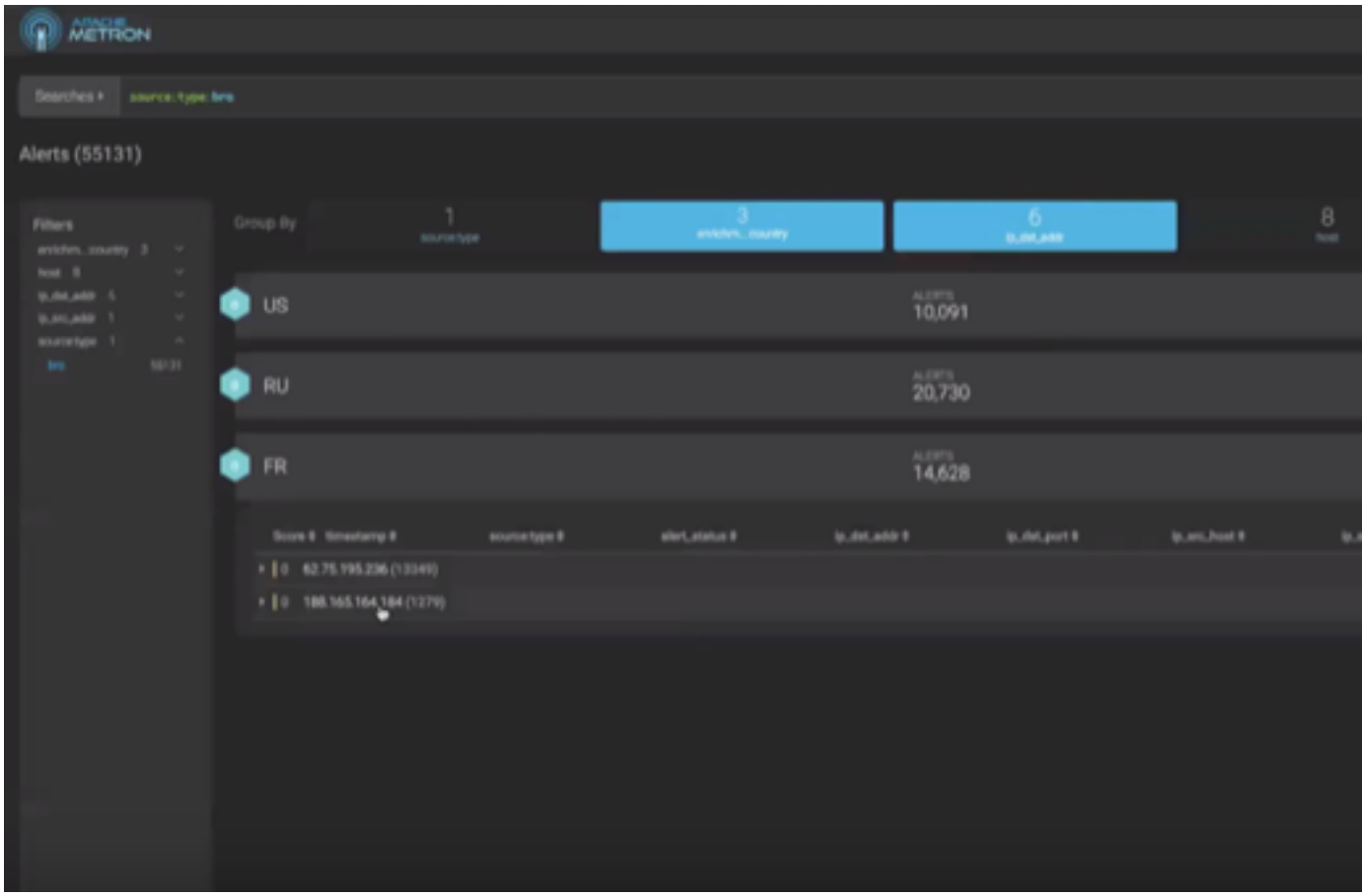
Procedure

1. Click **enrichment:country** in the **Group By** section at the top of the UI to group your Bro filtered data by country.

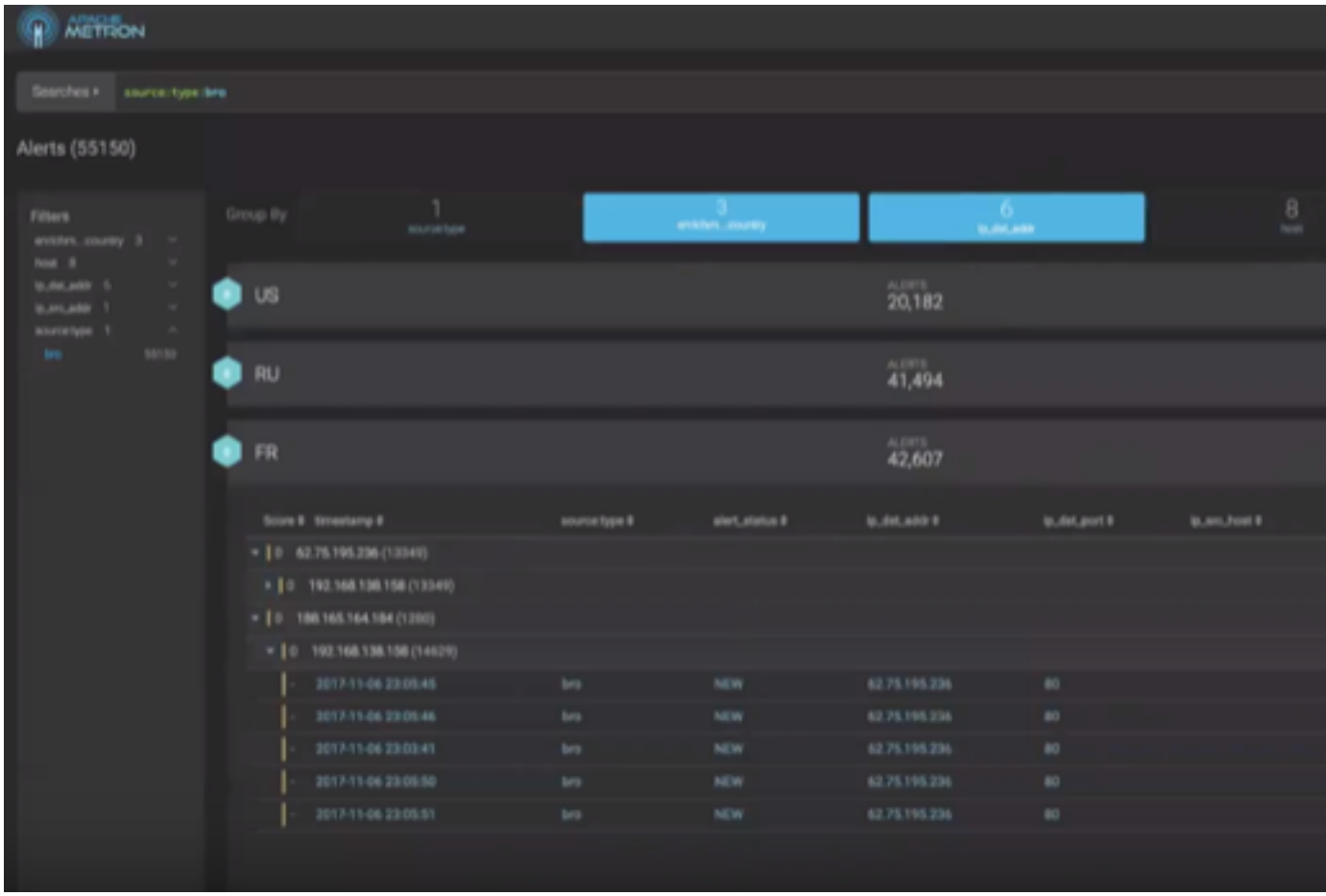
   In the following example, you can see that the alerts are now grouped into three countries: US, RU, and FR.



2. Click on the FR (France) group to see the IP addresses listed for the country:



3. You can click on the IP addresses to display Bro alerts for a specific host:



4. You can apply search parameters to the grouped information to display more granular information.

Create Meta Groups

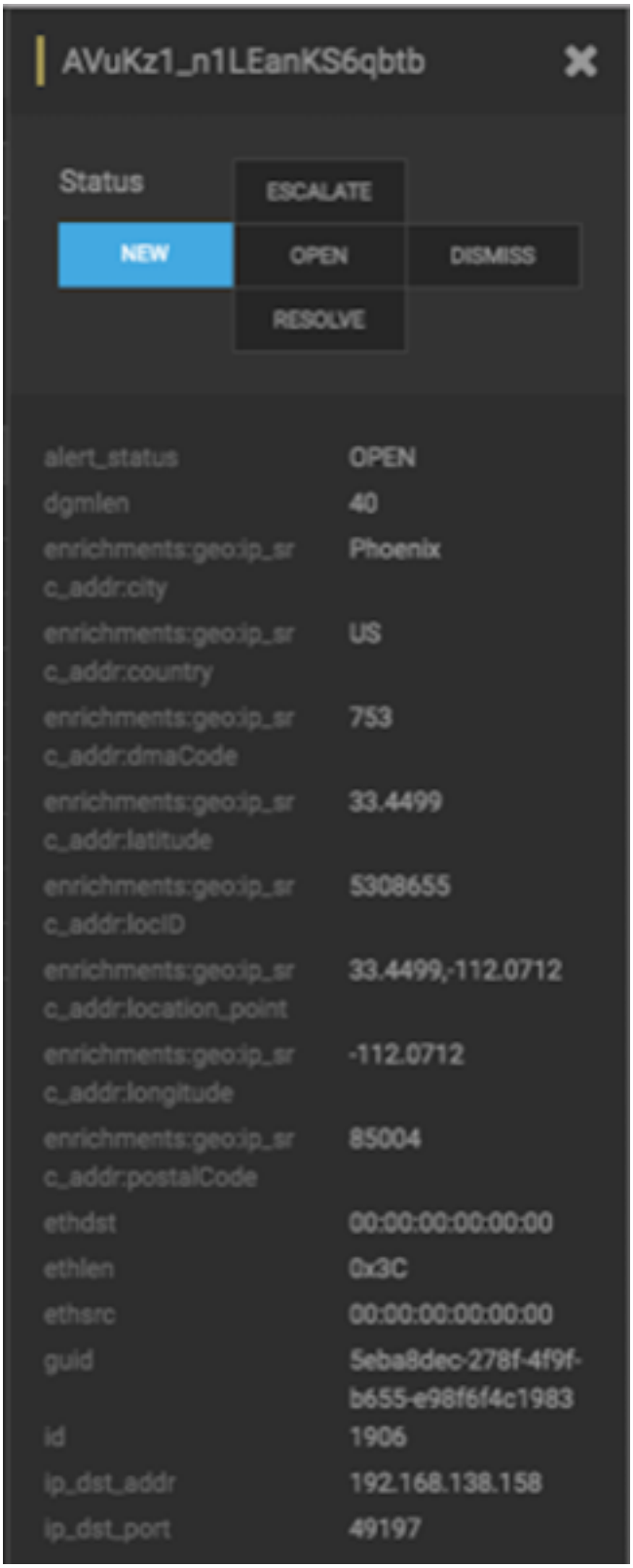
Another way you can group filtered alerts is by creating meta alerts. This enables you to deal with the group as a single instance. You can create meta alerts at any of the various levels of groups.

Procedure

1. Select a groups of alerts on which you want to focus, then click  (meta alert icon) and confirm that you wish to create a meta alert.

   The meta alert disappears from the tree view. You can still see the meta alert in the alerts table view.
2. 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.

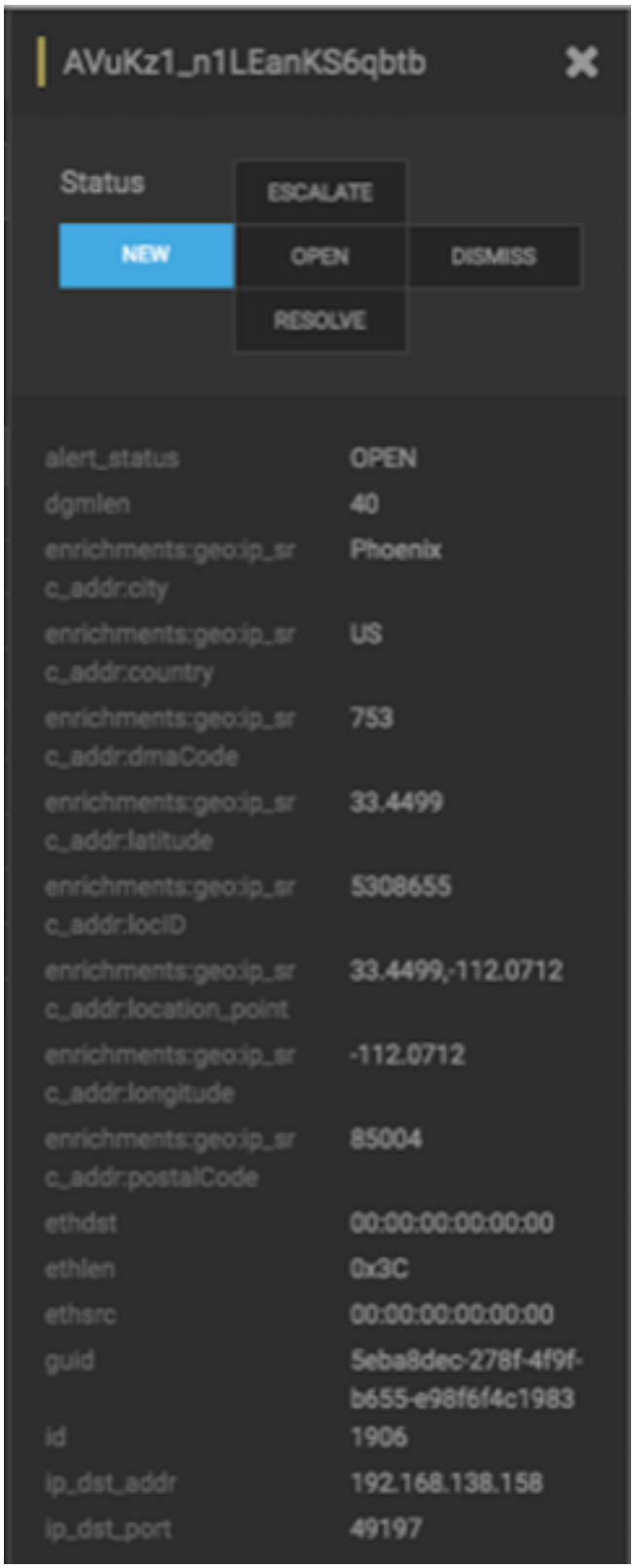
Escalating Alerts

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.

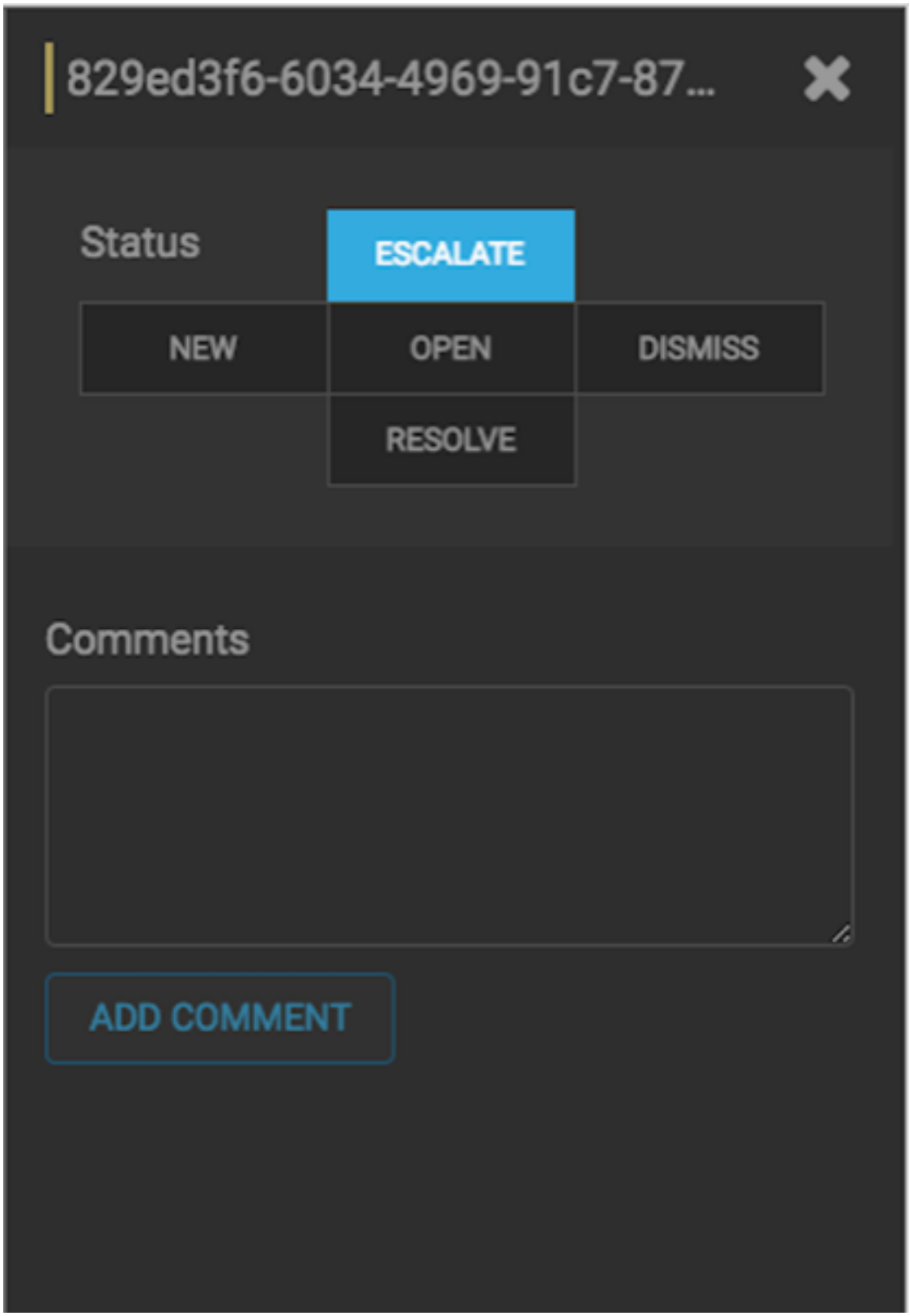


The current alert status is highlighted.

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**.



CCP 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**.