

CCP Triaging Alerts 2.0.0

Investigating Alerts

Date of publish: 2017-11-06

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

- Investigating Alerts Overview..... 4**
 - Filter Alerts..... 4
 - Group Alerts..... 5
 - Create Meta Groups.....8
 - Escalating Alerts..... 10

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.



Note:

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

Searches: source.type:bro

Alerts (55104)

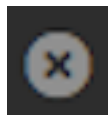
Source #	Timestamp #	source.type #	alert.status #	ip_dst_addr #	ip_dst_port #	ip_src_host #
+	2017-11-17 15:08:25	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:25	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:21	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:16	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:11	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:11	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:10	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:07	bro	NEW	95.163.121.204	80	
+	2017-11-17 15:08:07	bro	NEW	192.168.198.2	53	
+	2017-11-17 15:07:41	bro	NEW	72.34.49.86	80	
+	2017-11-17 15:07:40	bro	NEW	204.152.254.221	80	
+	2017-11-17 15:07:34	bro	NEW	72.34.49.86	80	
+	2017-11-17 15:07:34	bro	NEW	204.152.254.221	80	

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 the **Searches** field.

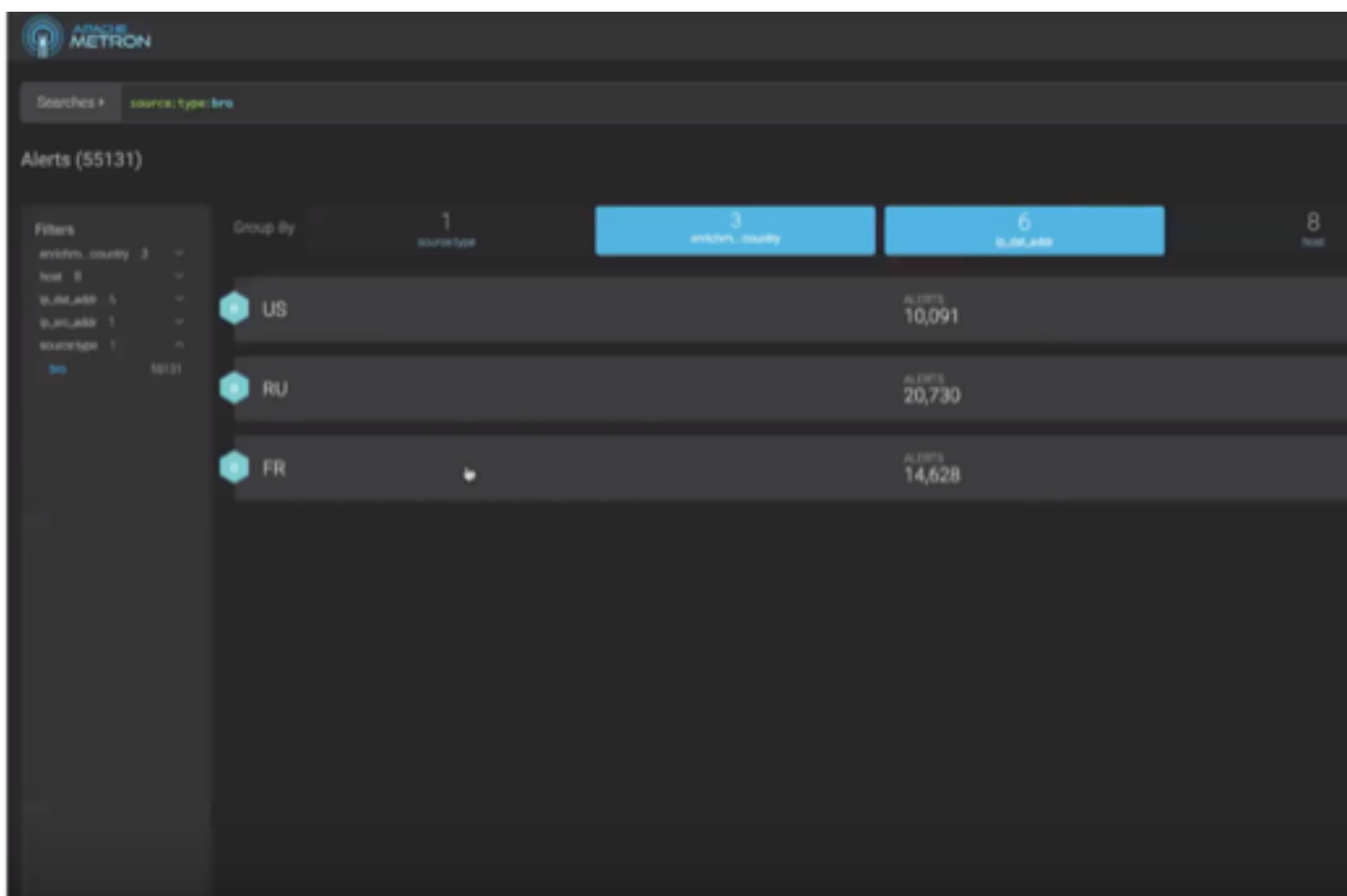
Group Alerts

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.

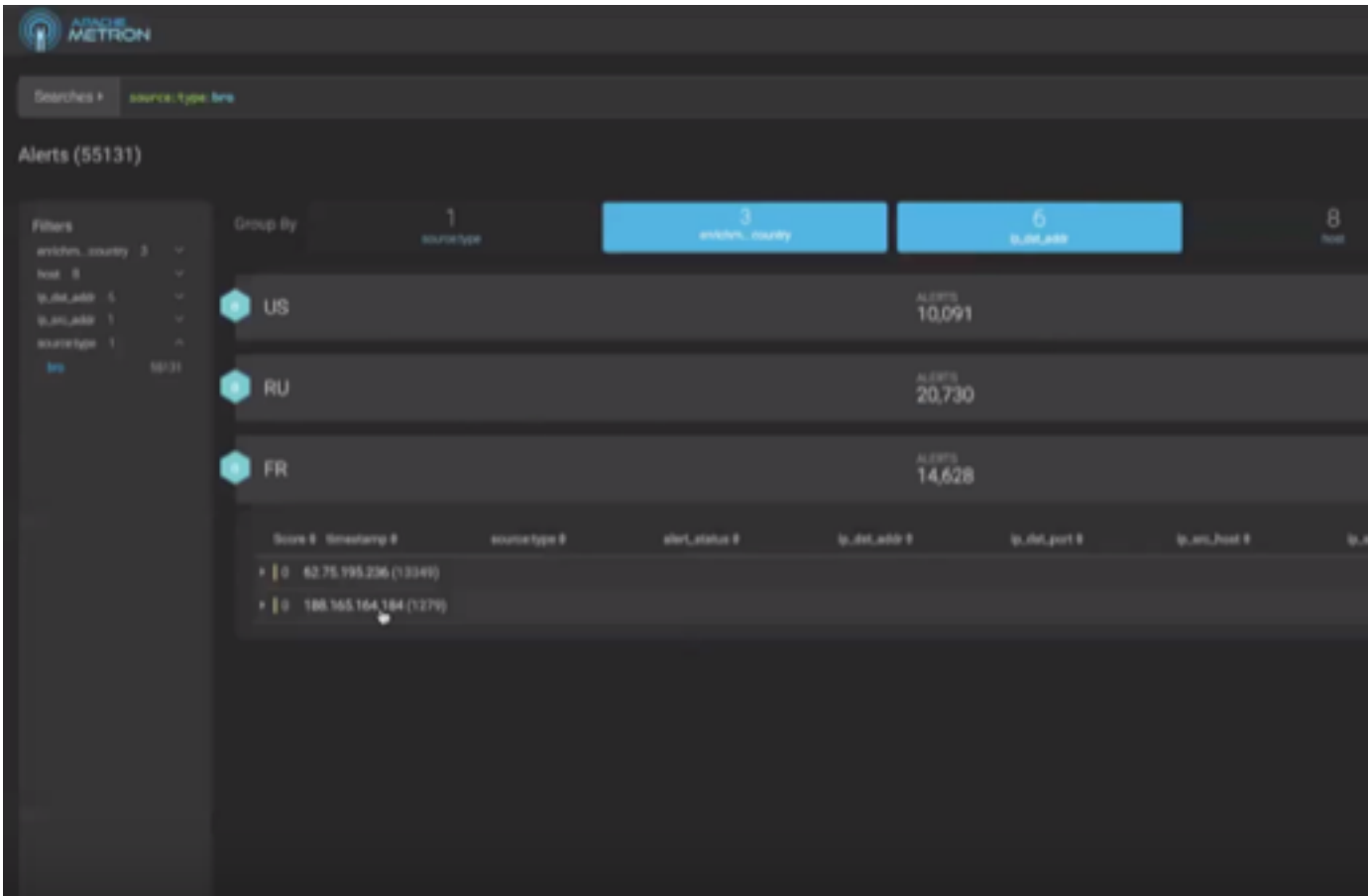
Procedure

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

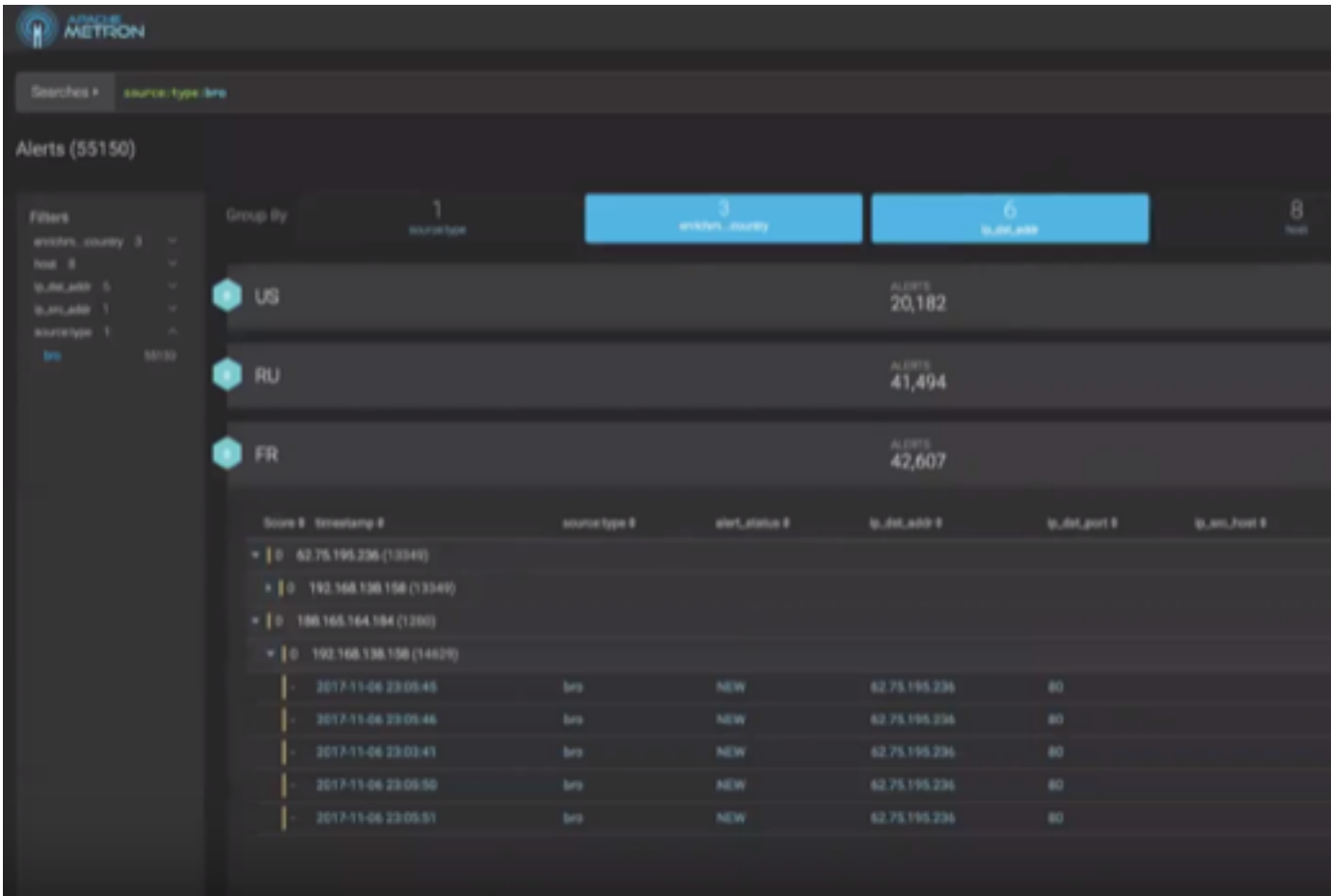
In the following example, you can see that the alerts are now grouped into three countries: US, RU, and FR.



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

AVuKz1_n1LEanKS6qbtb

Status

NEW

ESCALATE

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	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.

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.

AVuKz1_n1LEanKS6qbtb

Status

NEW

OPEN

DISMISS

ESCALATE

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 user interface for triaging alerts. At the top, there is a header bar with a yellow vertical bar on the left, a truncated alert ID '829ed3f6-6034-4969-91c7-87...' in the center, and a close button (X) on the right. Below the header, the 'Status' section contains 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 buttons is a 'Comments' section with a large text input area and an 'ADD COMMENT' button at the bottom.

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**.