SSI v2 5.4 Kibana 3 cheatsheet

Links

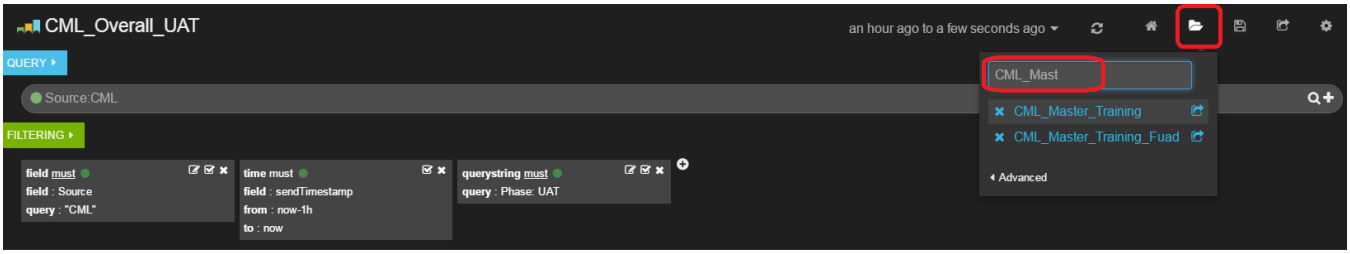
Video of Kibana session (unfortunately WEBEX failed to capture the audio) : https://amadeusworkplace-my.sharepoint.com/personal/amuni_amadeus_com/Documents/BOX/Kibana/Kibana_07FEB17.wrf

Links to all regions for ES/Kibana : SSI v2 5.4 List of Elastic Search Regions, note we are using **Kibana 3**

List of critical DCS dashboards : SSI v2 5.4 DCS Critical Dashboards PRD

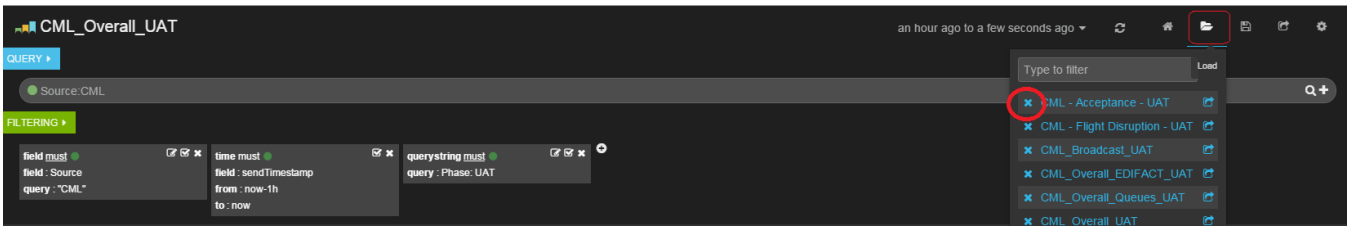
Loading an existing dashboard

Click on the Load icon, and start typing the name of the dashboard you want



Deleting a dashboard

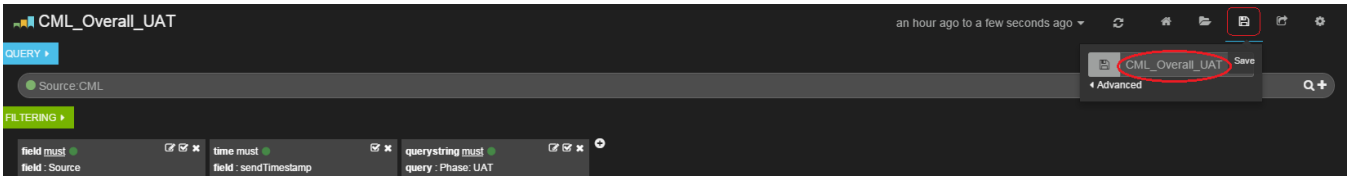
Click on the Load icon, look for the dashboard you want to delete, then click on the cross - X.



Save a dashboard as something else

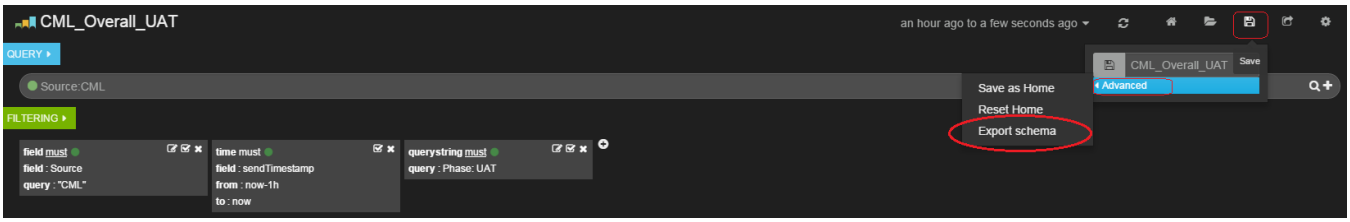
Click on the Save icon, then put the new name and click on the save icon to the **left** of the dashboard name.

There should be a green banner at the end then telling you your changes are saved.



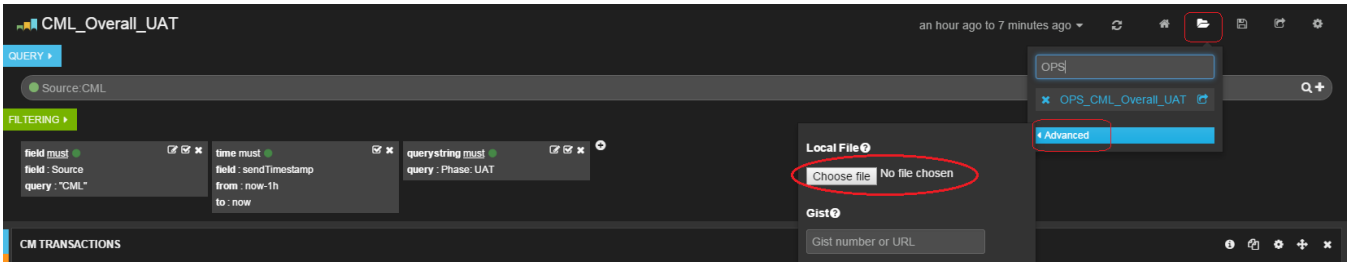
Export your dashboard

Click on the Save icon, then on Advanced, then select Export schema



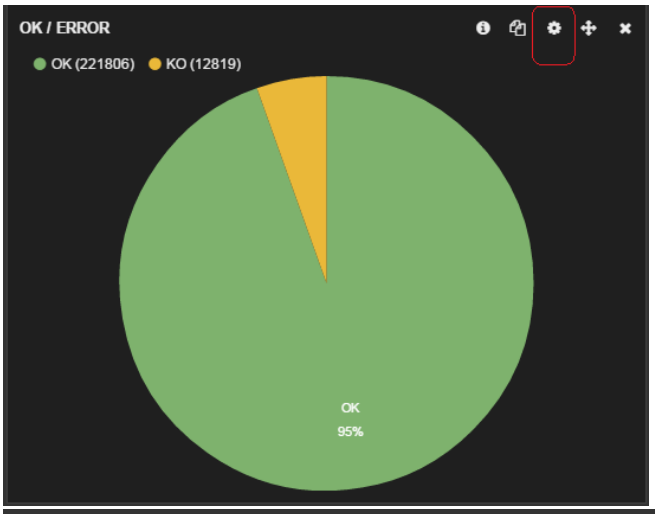
Import a dashboard

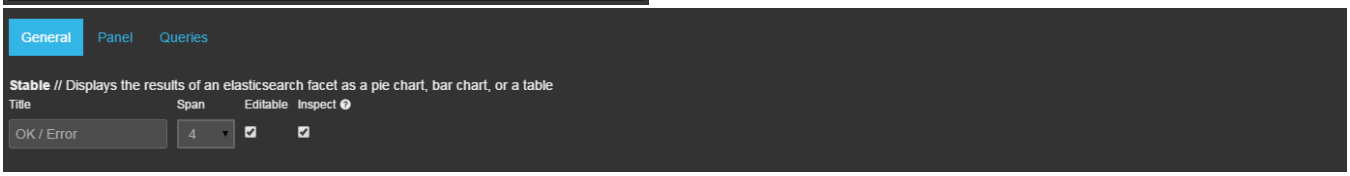
Click on the Load icon, then on Advanced, then select Local file and supply your local Json dashboard.



Modify a panel

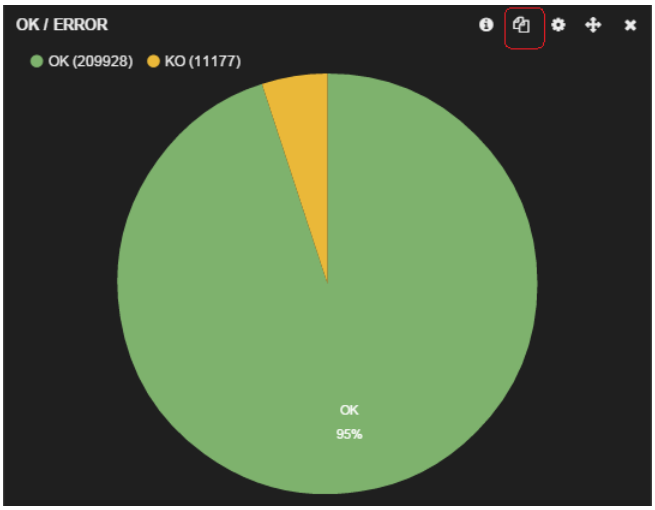
Click on the Configure icon and then change any aspect you want - the title, the display etc. There are 3 panels.





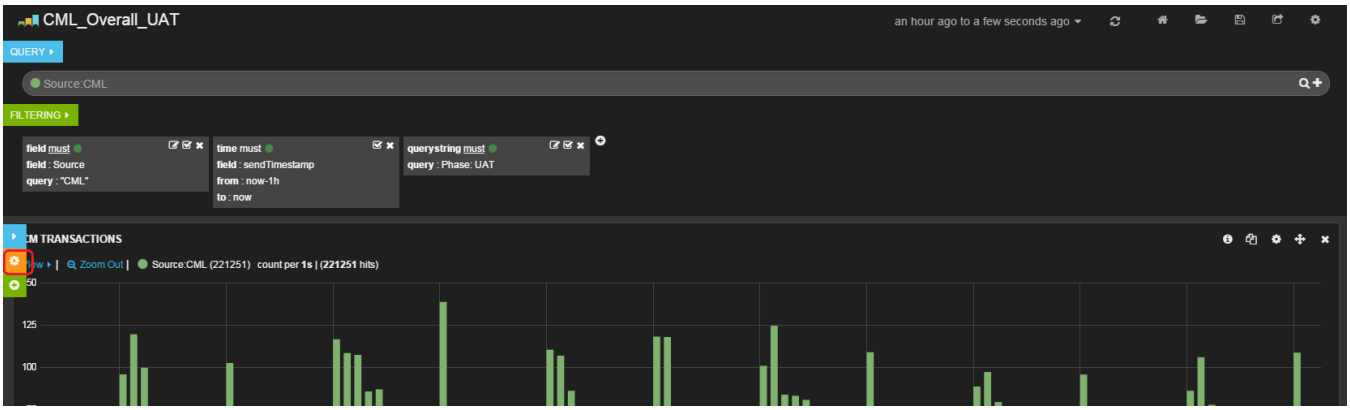
Duplicate a panel

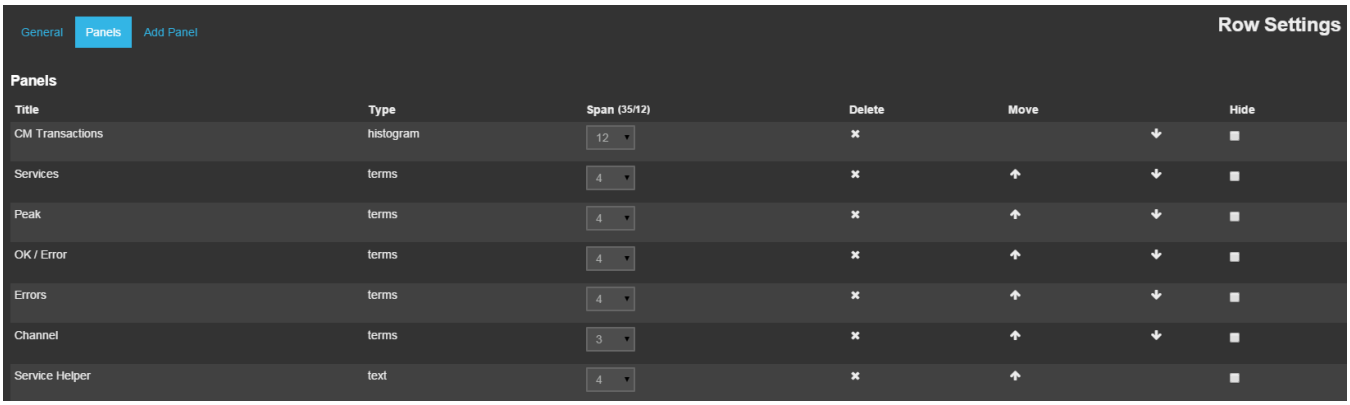
Click on the Duplicate icon, then change the elements in the new panel item created on your dashboard via the Configure icon.



Rearrange panels

Click on the Configure icon near the Histogram, then use the Panels tab to rearrange.

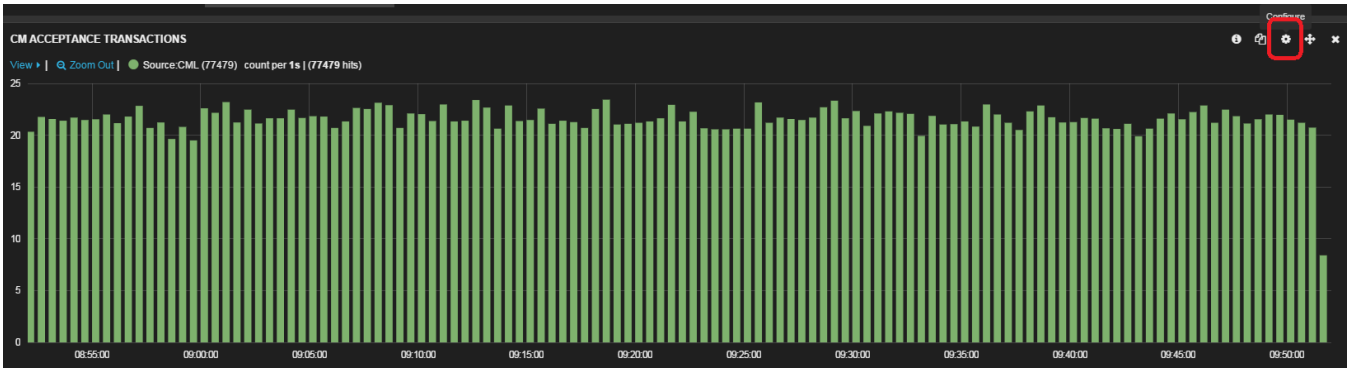




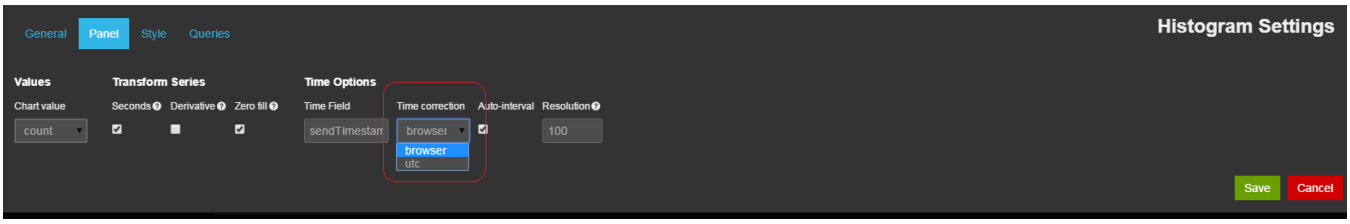
Local vs UTC time

You can configure the histogram to show items in local or UTC. The recommendation is to always have your histogram in UTC,

Click the Configure icon near the top right of the histogram.

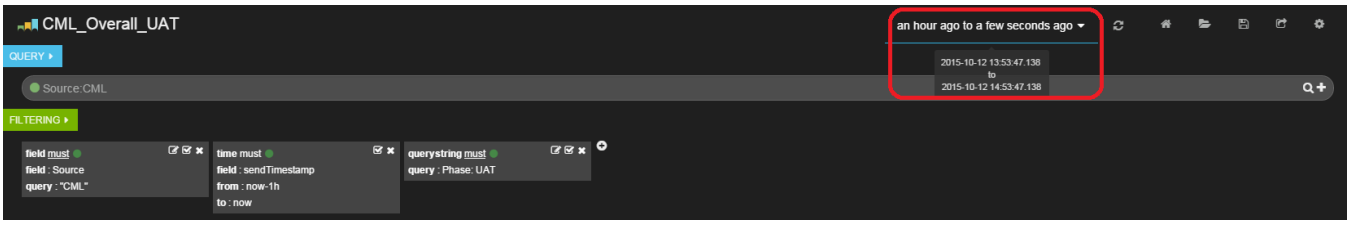


Go to Panel, and choose UTC or Browser as needed. Choosing Browser will give you local time.



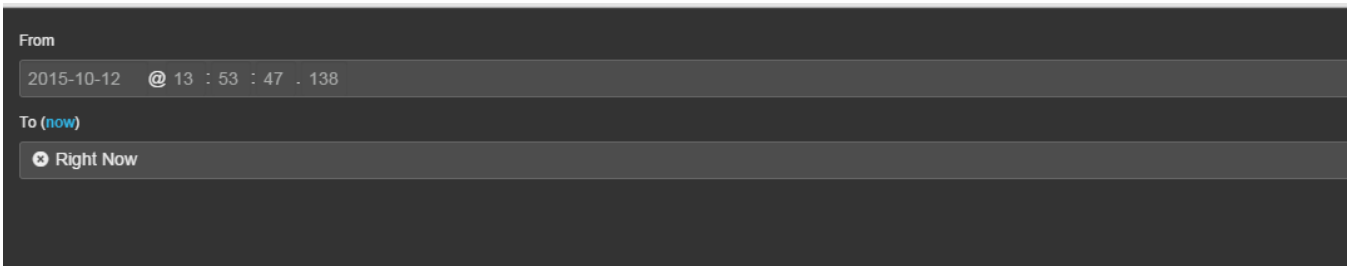
Pulling out data for a specific time period

Click on the arrow in the time period on the top right of your dashboard



Choose Custom

Enter the date and time you want and click on Apply

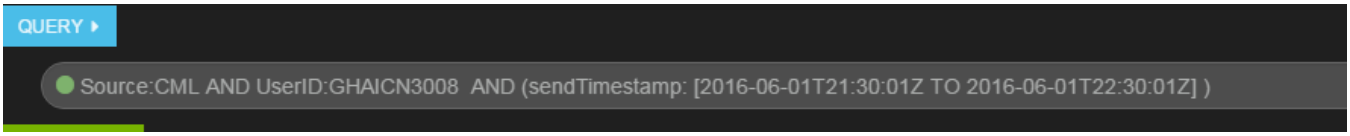


Note your input is Local time, and then the subsequent display in the Histogram is then converted to UTC (as we always choose UTC and not browser time in our dashboards).

Unfortunately Kibana doesnt let us choose an input in UTC for the time input.

Noted there is also a way to specify an explicit time input in the Query line, if needed

e.g. Source:CML AND Host:* AND sendTimestamp:[2016-06-01T21:30:01Z TO 2016-06-01T22:30:01Z]

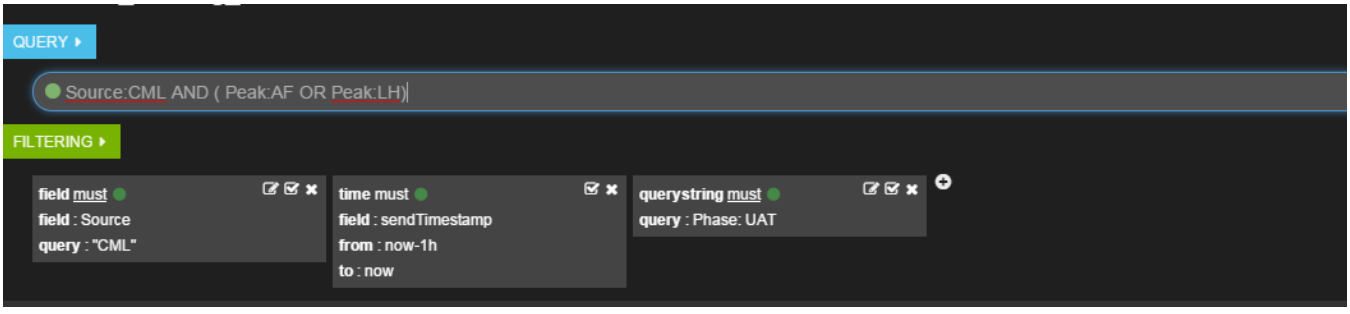


Pulling out data for multiple airlines

Here i am using the Peak as an example and pulling out data for LH and AF

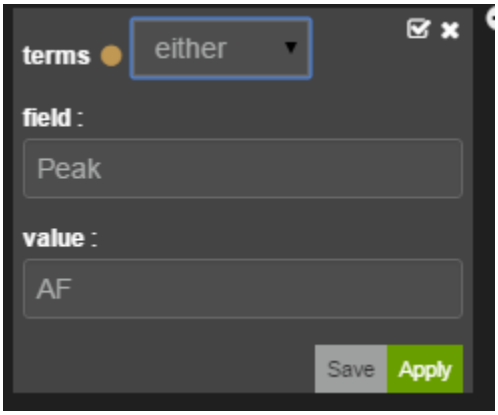
Method 1

The easiest way will be to perform a query (refer the queries section for more details)

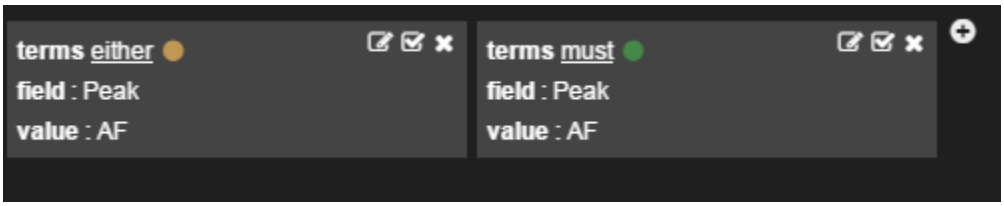


Method 2

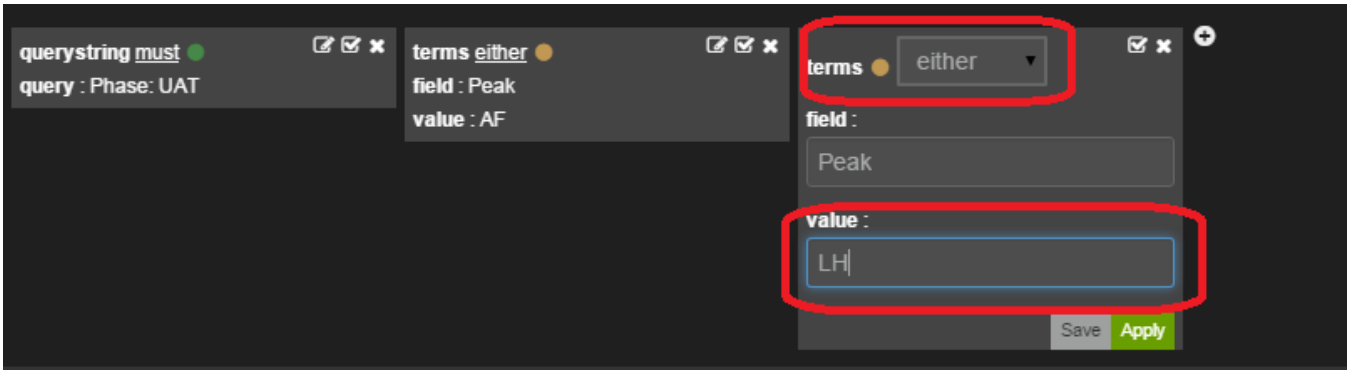
Filter for the first Airline via the Piechart as usual, and change the filter to "Either"



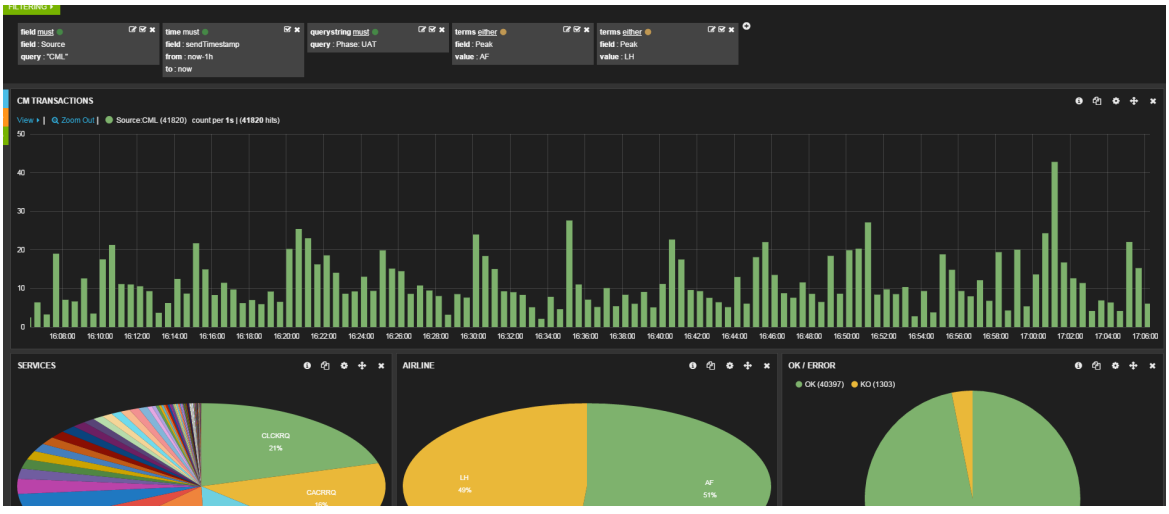
Click on the Piechart again, that will add a copy of the existing filter.



Now Edit the new filter - put "Either" and change the value to LH

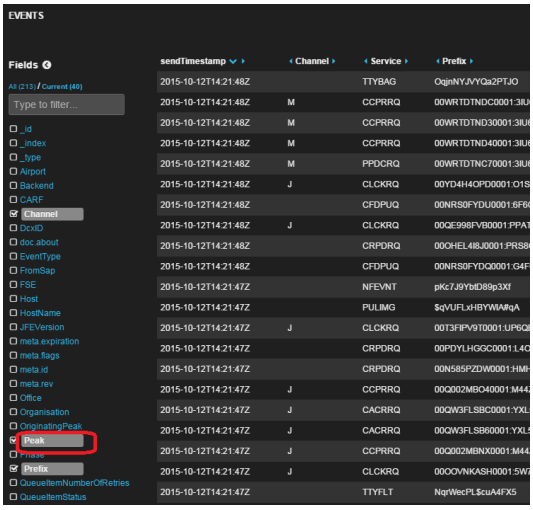


Click on apply and you will have the data filtered for LH and AF

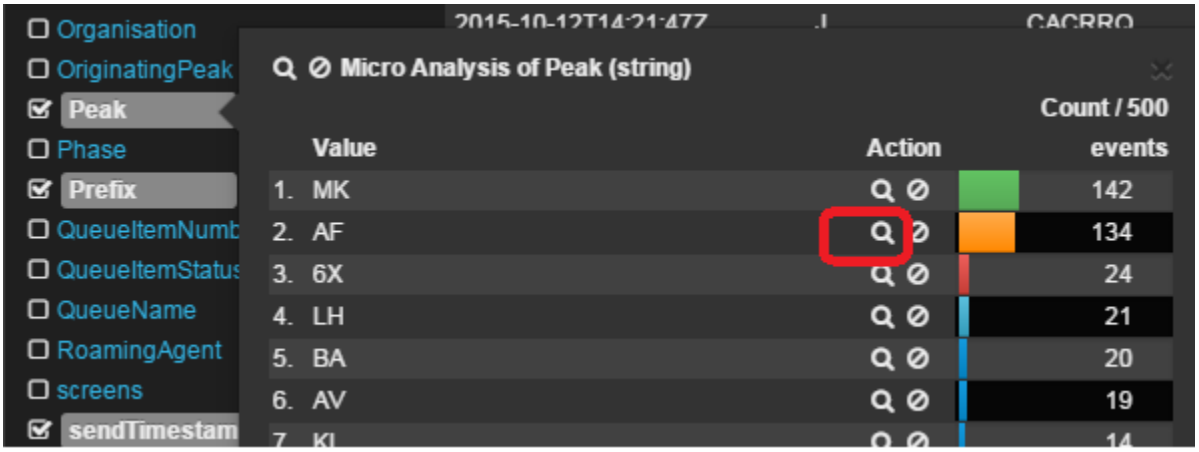


Method 3 (this only works when you add a filter via the Events table)

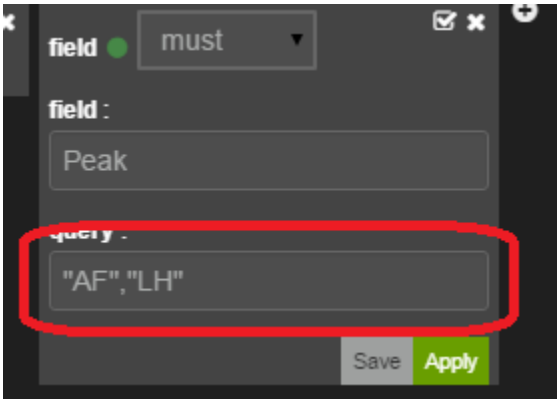
Go to the Events table and click on the field Peak



Click on the magnifying glass icon - this will add a filter for "AF" Peak **at the top of your dashboard**



Go to the top of your dashboard, find this Peak filter, and edit to add the other airline too, separated by a comma



Click on apply and you will now have the data filtered for AF and LH

How to get the FE and BE logs

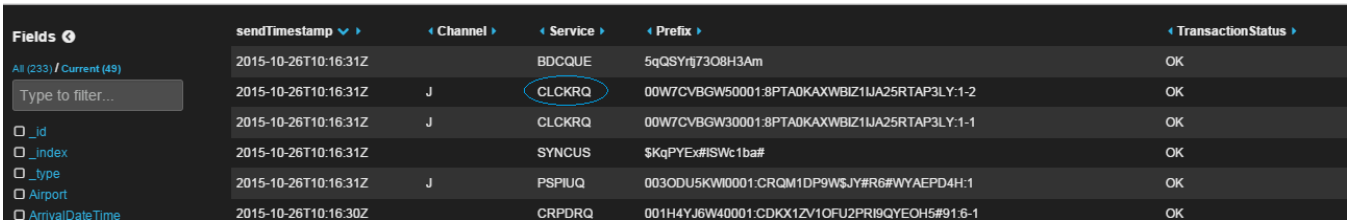
Method 1 Use any logviewer that works, put the timestamp and CARF/Prefix from the dashboard

We do not have an API from ALF which lets us build the logsearch URL on the fly (they need us to send the whole data in the payload itself, which is a lot).

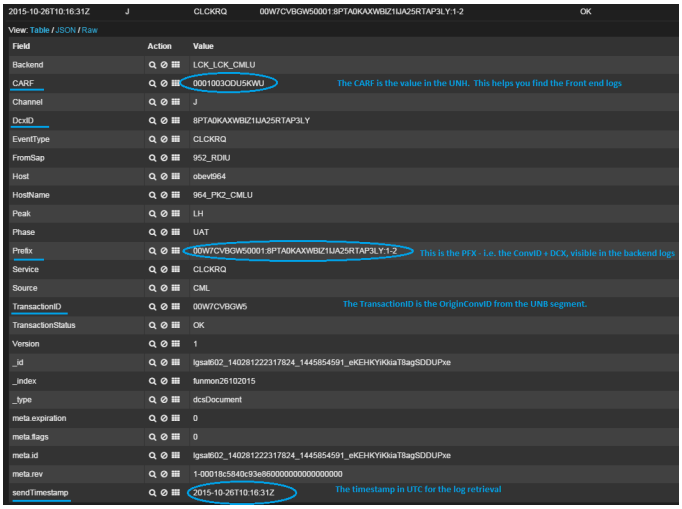
Here is how you can get the logs yourself for any item you see on the dashboard.

We will get the logs for CLCKRQ as an example

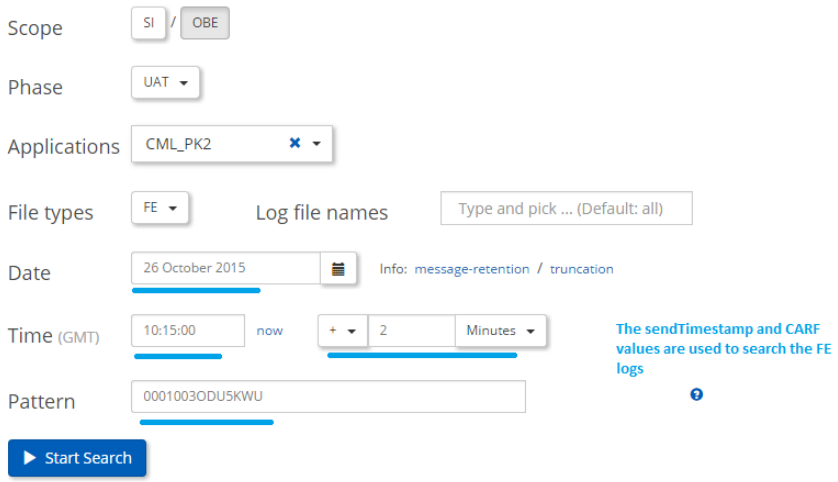
1) Click on a row you are interested in to expand it. .



2) Use the relevant data to get either the FE log or the BE log

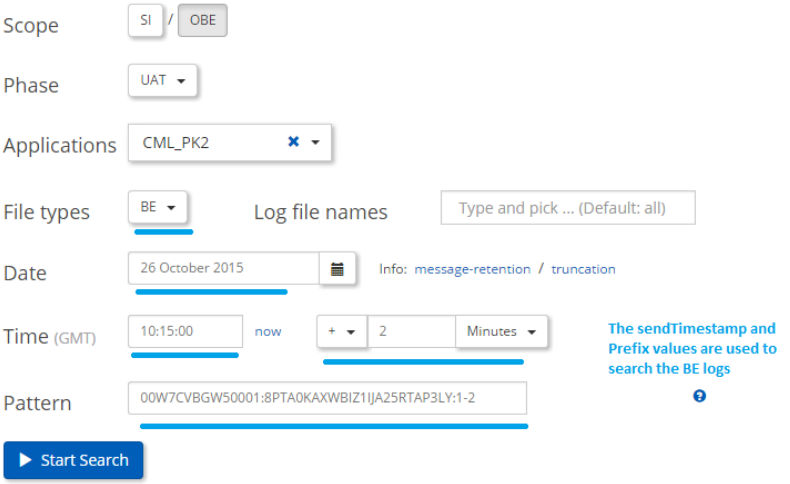


3) e.g. using the CARF to get the FE log



This results in the following, and you can get the Backend log from the FE log

4) e.g. using the Prefix to get the BE log (**or all logs - just choose ALL instead of BE**)



This results in the following

Method 2 Use the ALFHelper (note uses the new ALF ..which is unstable)

1. Click on a row you are interested in to expand it
2. Copy the JSON
3. Put it in http://fumatv01.os.amadeus.net:9090/ALFHelper/
4. When you click on View Front End Log or View Backend Log, it builds an input to the new ALF. The search response then depends on whether the new ALF works or not..

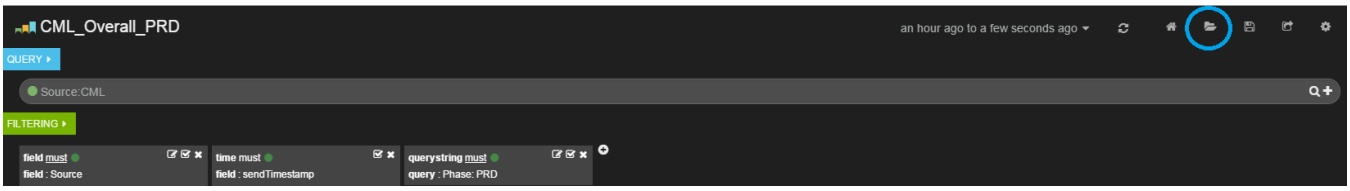
Method 3 Use Tampermonkey script

You may want to consider click, select, right click + click approach using a custom Tampermoneky script "Kibana ALF search".

1. Go to a Kibana dashboard and find a table with CARF's you want to search
2. click on the row you want to search: you will see "View: Table / JSON / Raw" - click on **Raw** which will show you a raw JSON data
3. select all the JSON data
4. right-click and you should see Tampermonkey sub-menu - select "Kibana - search by CARF in ALFv3" from there
5. this will open a separate window with ALFv3 page with pre-filled values: you can adjust them (perhaps the time span) and then click Submit

Seeing available dashboards or Opening a dashboard

Use the Load icon, then type the name. CML dashboards start with CML_ , FML ones with FML_ , all as per naming conventions here : SSI v2 5.4 Architecture and Basics#Dashboardnamingconventions



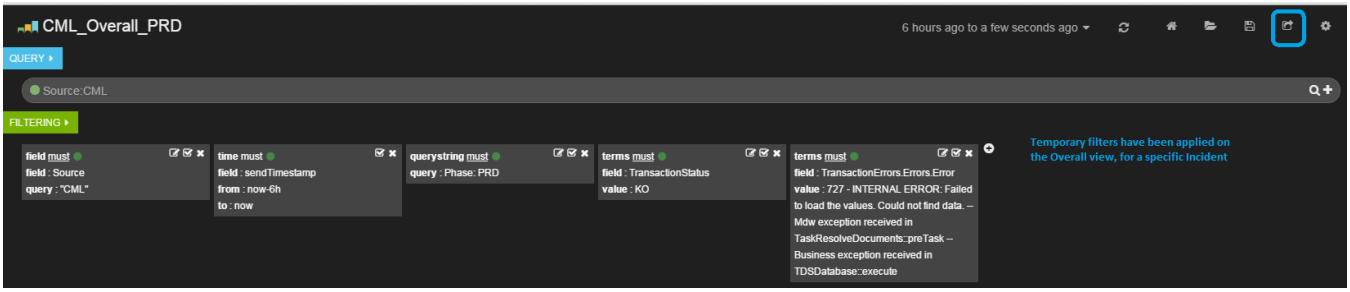
Click on the dashboard name and NOT on the "x" to the left of the name (clicking on the "x" deletes the dashboard)

Sharing a temporary view

Say you have an incident, and you filter for an error / some airlines.

You can share this temporary view that you are seeing with everyone, without saving it and impacting the existing basic dashboard. It will be available even after the incident.

To do this, click on the Share icon, then copy the link.



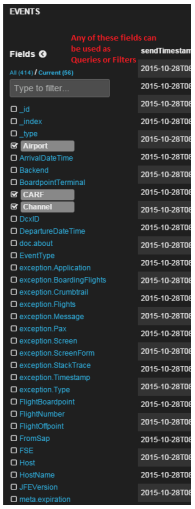
Queries

Queries are a lot more powerful and are the ones responsible for retrieving the data you see. Filters are applied on top of queries.

Its good to have a performant query, which is specific and targetted.

Any fields that you see in the logged JSON can be used in your Queries (refer the Event table visible at the bottom of each Dashboard)

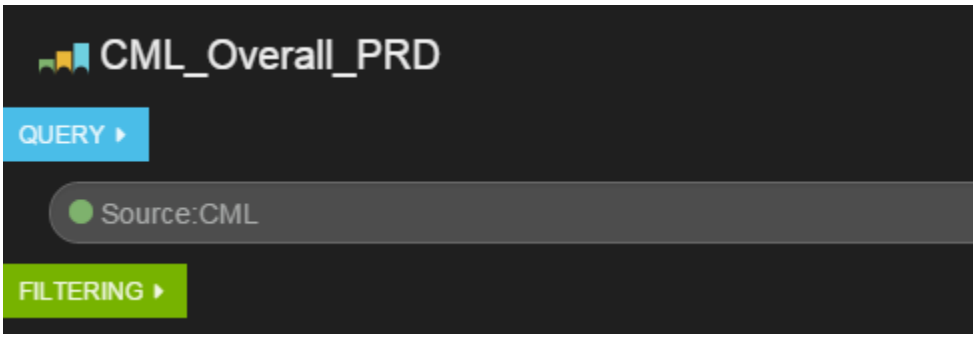
You can have multiple queries, and compare two different transactions all in the same dashboard.

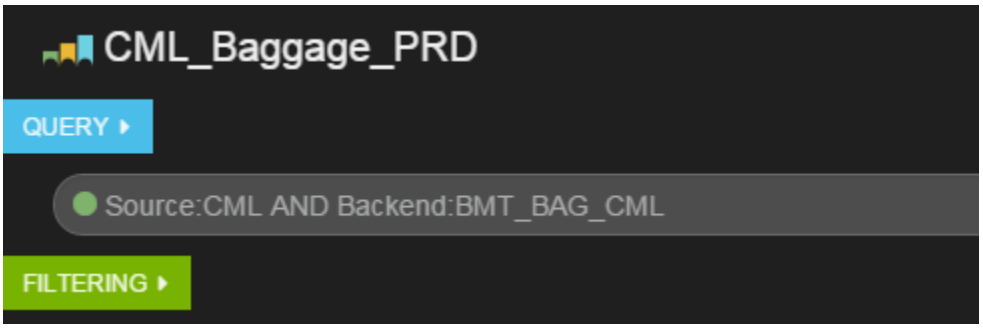


For example, an dashboard showing all CML transactions will have a query **Source:CML**

A dashboard for an area like Baggage, which wants to pull out all the Baggage related transactions can have a more targetted query by saying **Source: CML AND Backend:BMT_BAG_CML**

For more details on Query Syntax - please refer : https://www.elastic.co/guide/en/kibana/3.0/queries.html and also https://www.mjt.me.uk/posts/kibana-101/

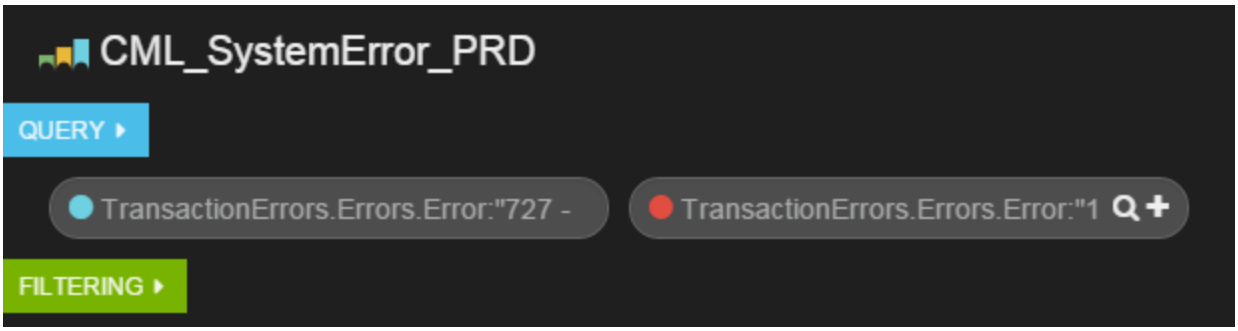




Multiple queries

Multiple queries are allowed too - but it is upto you to decide if your dashboard really needs to fire multiple queries.

Please aim to have queries targetting specific fields so that your dashboard is performant.

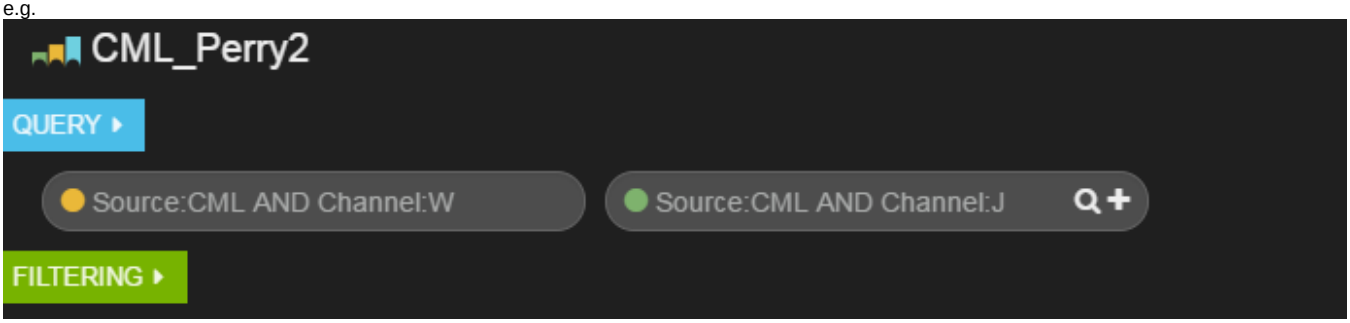


Multiple query example - compare elapsed time of FM activity vs CM Get pax :

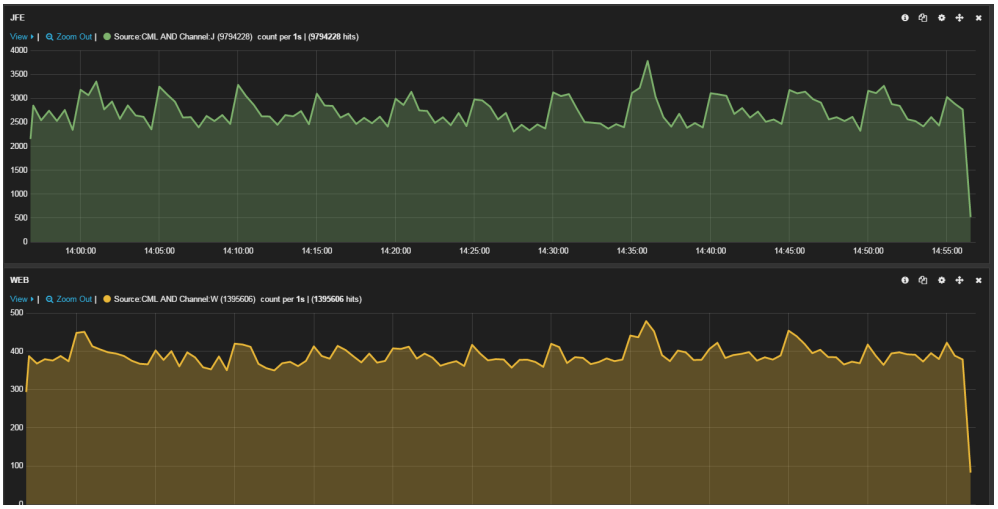
Multiple queries - choosing what to chart

When your dashboard has multiple queries, you can choose a specific one per chart if you want. By default all queries are selected.

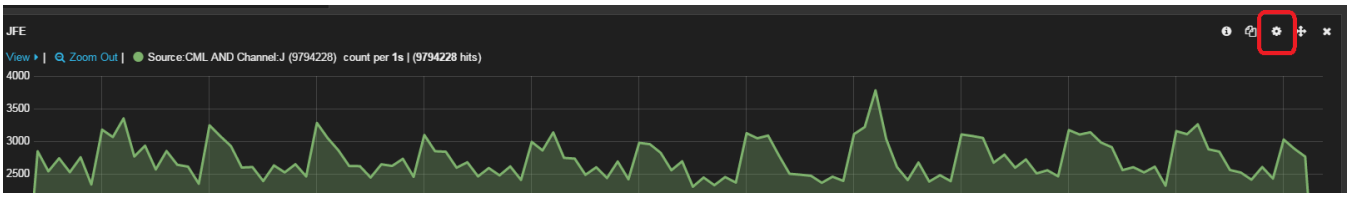
e.g.

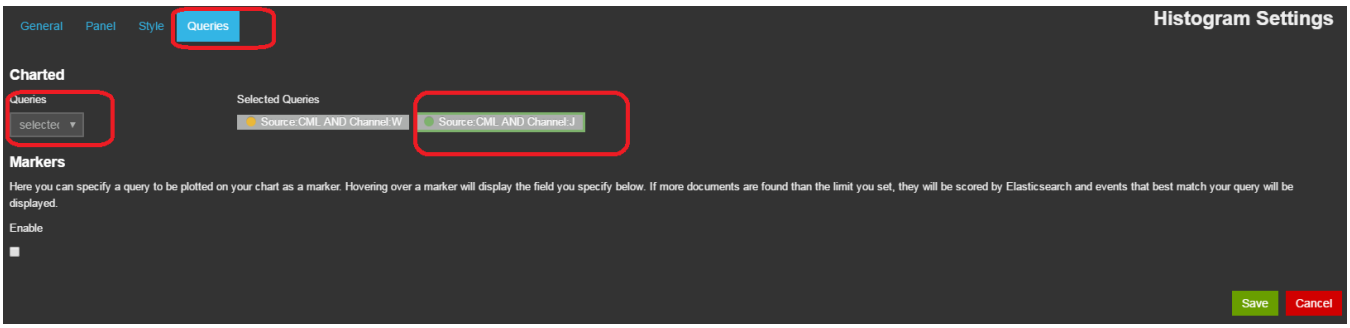


Histogram 1 - charts only query 1 and Histogram 2 charts only query 2



Go to settings for each histogram, and just select the queries you want to chart. Save, then Save the dashboard.



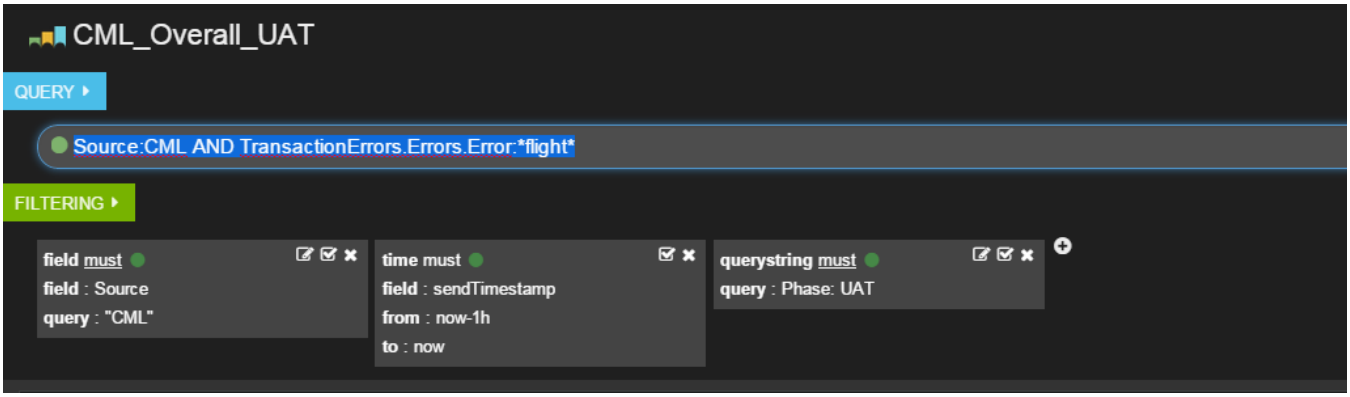


Pull out multiple error messages using a wildcard

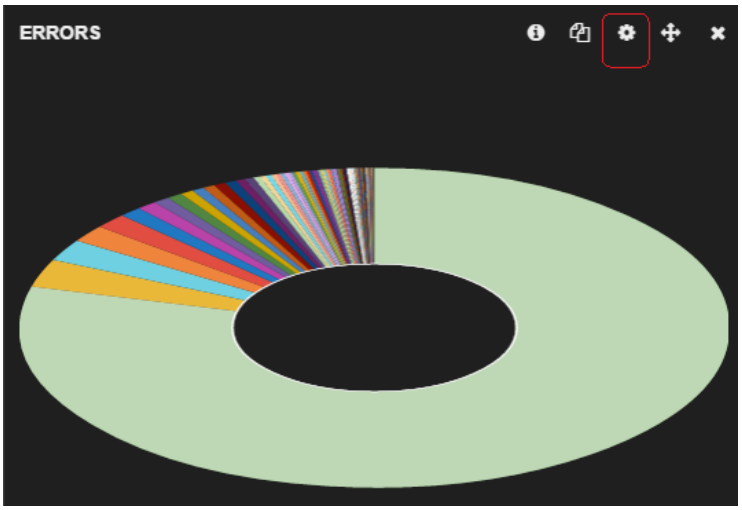
This is indeed possible via a Query.

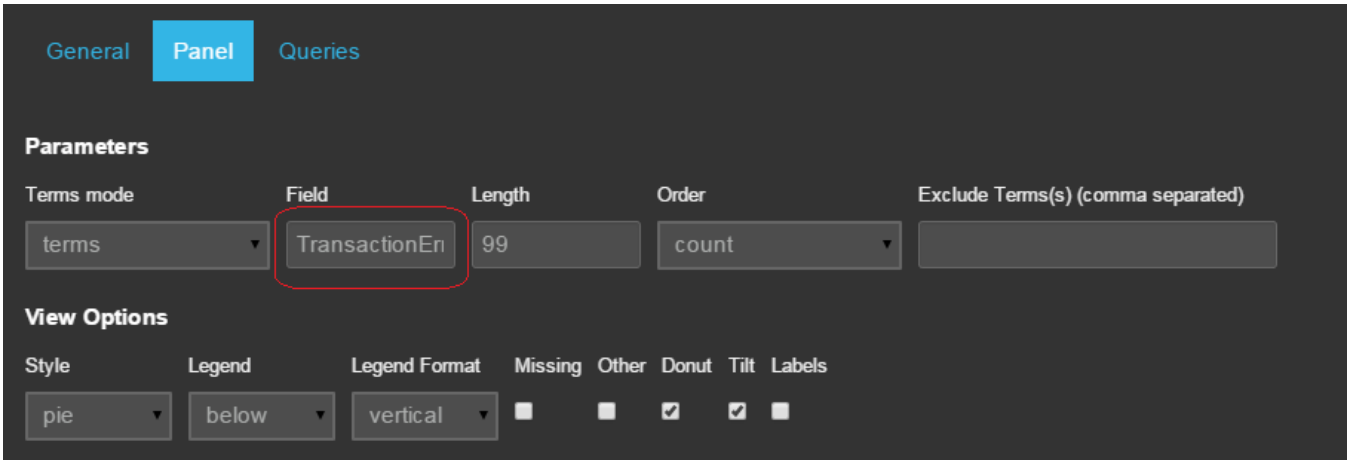
e.g. see the input for showing all the errors with "flight" in the error message text for CML

Source:CML AND TransactionErrors.Errors.Error:*flight*



Note to know the field name to pull out for errors, i clicked the configure icon on the Errors chart, went to the Panel tab, and copied the value in "Field"





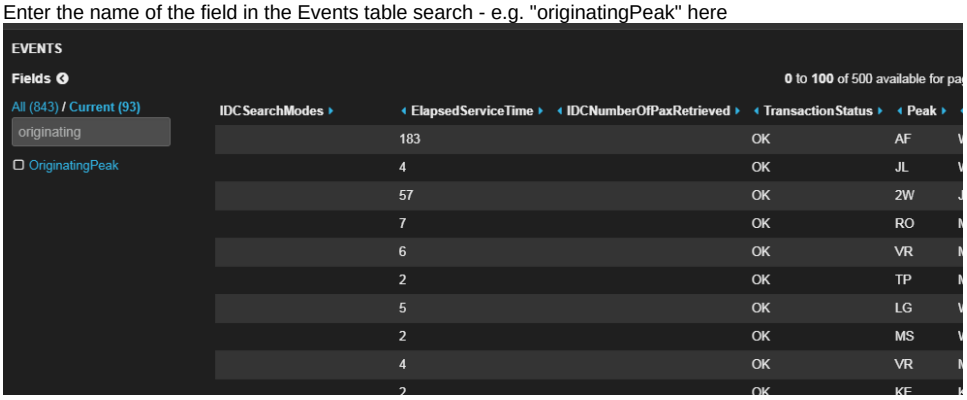
For more help on wildcards : https://www.elastic.co/guide/en/elasticsearch/guide/current/_wildcard_and_regexp_queries.html

Lucene Syntax : https://lucene.apache.org/core/2_9_4/queryparsersyntax.html

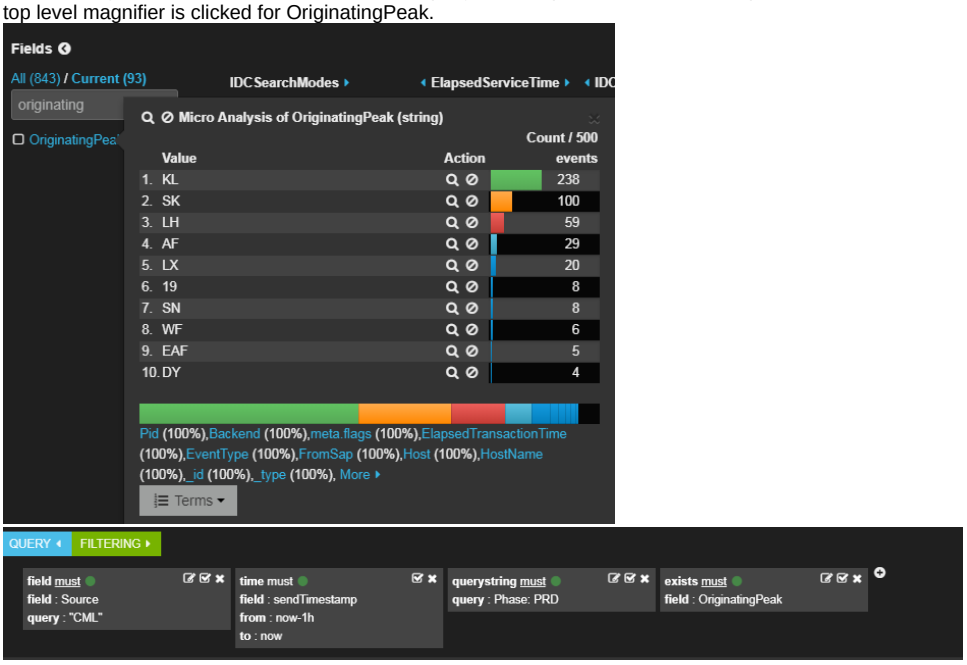
Check if exists or does not exist

You can add this by using the field list in the Events table.

1. Enter the name of the field in the Events table search - e.g. "originatingPeak" here



2. Click on the field
3. Use the magnifier to add an "exists" filter to the query at the top - this adds a filter to pull out all rows where the field is populated : e.g. here the top level magnifier is clicked for OriginatingPeak.



4. Similarly, you can click on the no-entry symbol to add a filter for does not exist - i.e. pull out all rows where the field is not populated

Filter by Peak

There is no easy way to wildcard and filter by Peak number.

(i think its potentially resource intensive and so at the Operations end the mappings/templates are not setup to support wildcarding for all fields - the only one wildcards work on is the Error text)

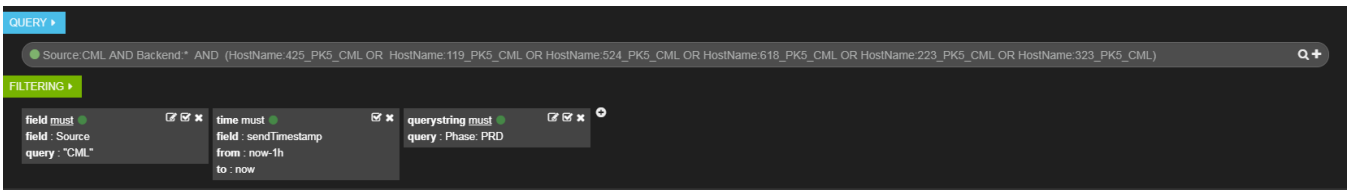
If you need to filter by Peak its best to use the **Host** or **HostName** fields - its cumbersome, but the only way currently.

The HostName always has the *_PEAKn_CML in the name, so the pie chart can give you the names to filter on.
Alternatively, use the SI viewer and pull out the nodes for a CML Peak, and then use the node names in your query.

e.g. for CML Peak 5 add (HostName:425_PK5_CML OR HostName:119_PK5_CML OR HostName:524_PK5_CML OR HostName:618_PK5_CML OR HostName:223_PK5_CML OR HostName:323_PK5_CML) to the query

i.e. your full query becomes :

Source:CML AND Backend:* AND (HostName:425_PK5_CML OR HostName:119_PK5_CML OR HostName:524_PK5_CML OR HostName:618_PK5_CML OR HostName:223_PK5_CML OR HostName:323_PK5_CML)

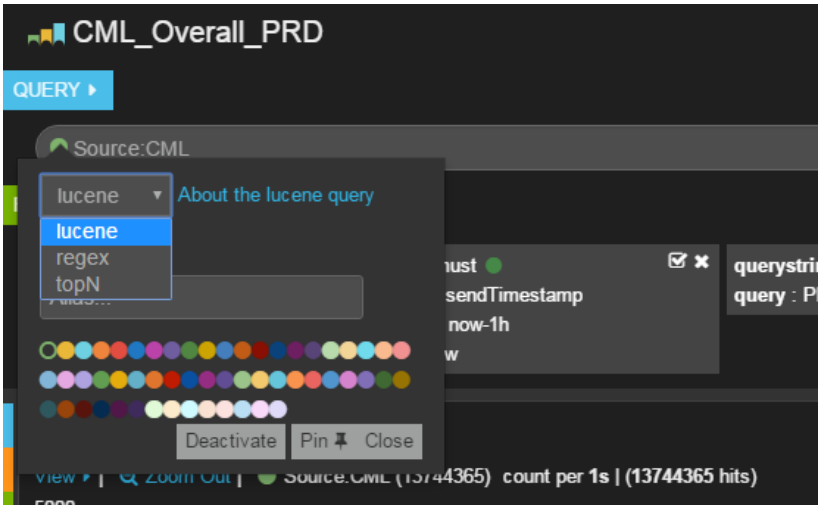


Choosing Query syntax as Lucene / REGEX / TopN

Click on the coloured dot in the query section and choose from a drop down

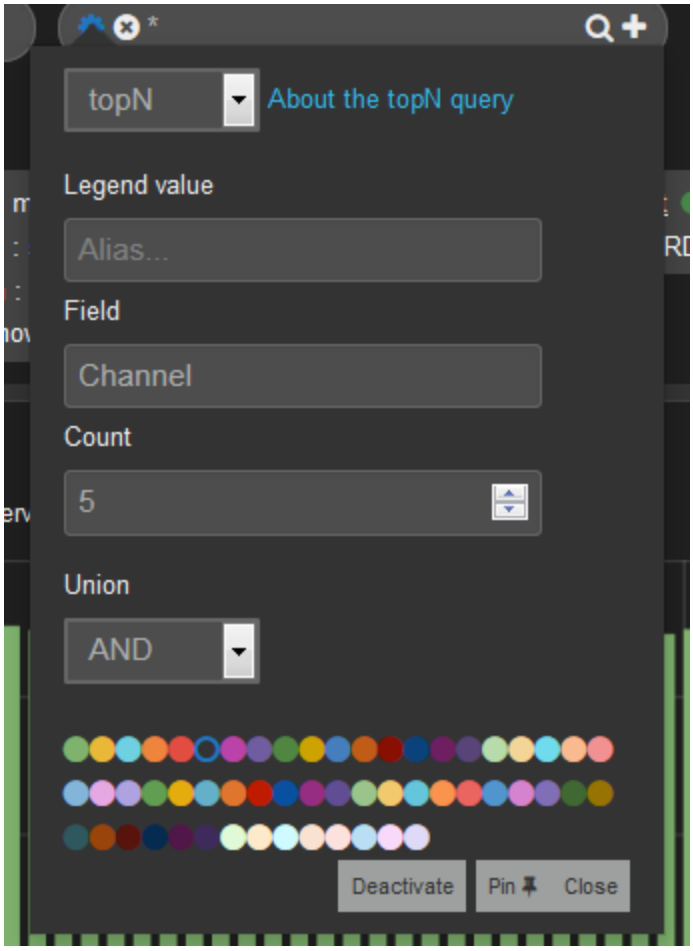
regex syntax links : https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html

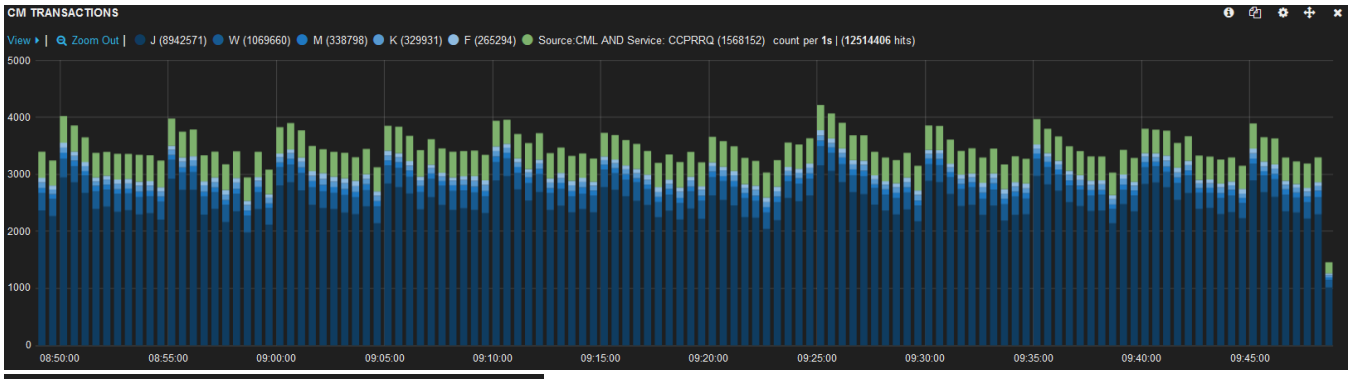
Noted open issue on Kibana 3 - hardcodes the _all field for regex queries, leading to them not being usable : https://github.com/elastic/kibana/issues/631. Can do manual curl command though.

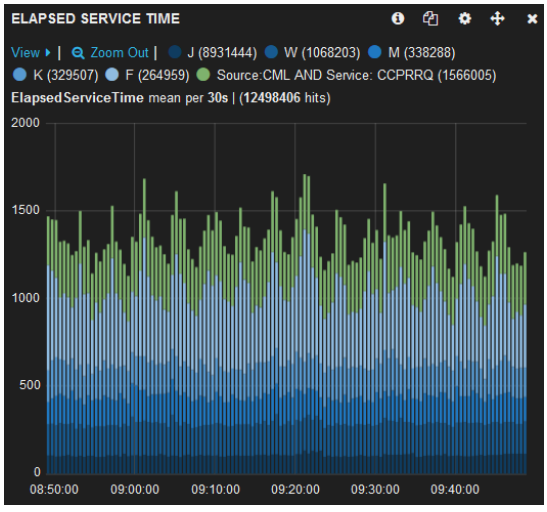


Using topN queries

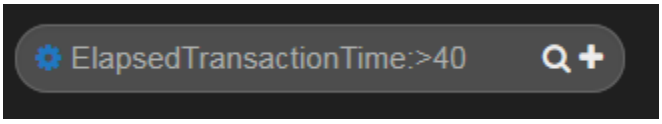
The top N query finds the most popular terms in a field and uses them to compute new queries. In the example we would see the repartition of transactions per channel:

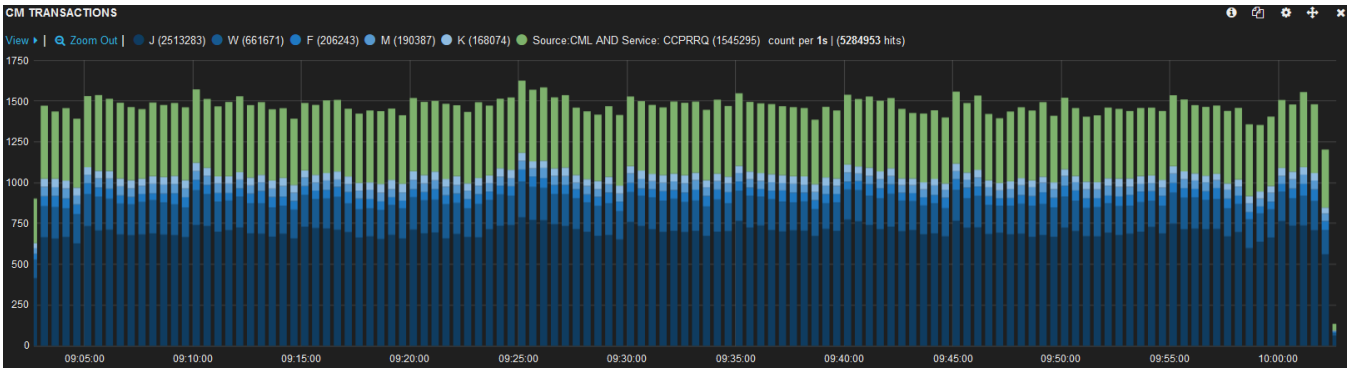

topN
About the topN query
Legend value
Alias...
Field
Channel
Count
5
Union
AND
Deactivate
Pin
Close


CM TRANSACTIONS
View | Zoom Out | J (8942571) W (1069660) M (338798) K (329931) F (265294) Source:CML AND Service: CCPRRQ (1568152) count per 1s | (12514406 hits)
5000
4000
3000
2000
1000
0
08:50:00
08:55:00
09:00:00
09:05:00
09:10:00
09:15:00
09:20:00
09:25:00
09:30:00
09:35:00
09:40:00
09:45:00


ELAPSED SERVICE TIME
View | Zoom Out | J (8931444) W (1068203) M (338288)
K (329507) F (264959) Source:CML AND Service: CCPRRQ (1566005)
ElapsedServiceTime mean per 30s | (12498406 hits)
2000
1500
1000
500
0
08:50:00
09:00:00
09:10:00
09:20:00
09:30:00
09:40:00

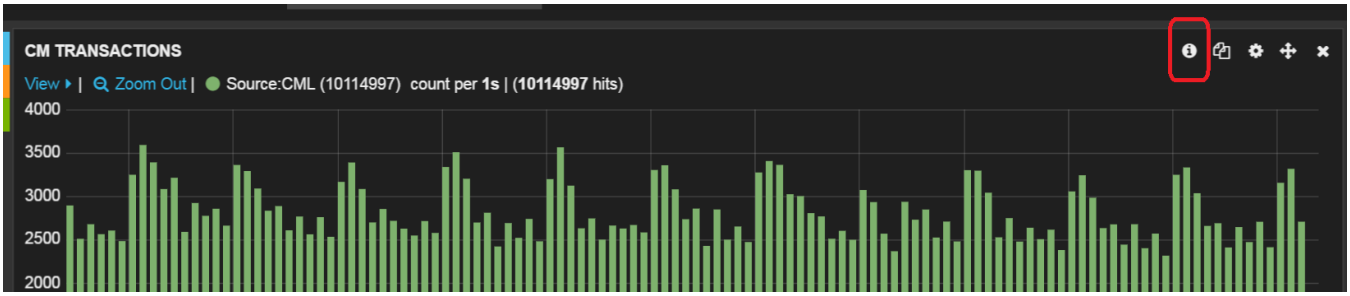
We can also add extra filters to the query that is built from that top N. For example, we could see what of those transactions have an ElapsedTransactionTime higher than 40ms:





Inspecting the query Kibana is building

Click the "i" on the Histogram



Fix Events Table not loading data issue

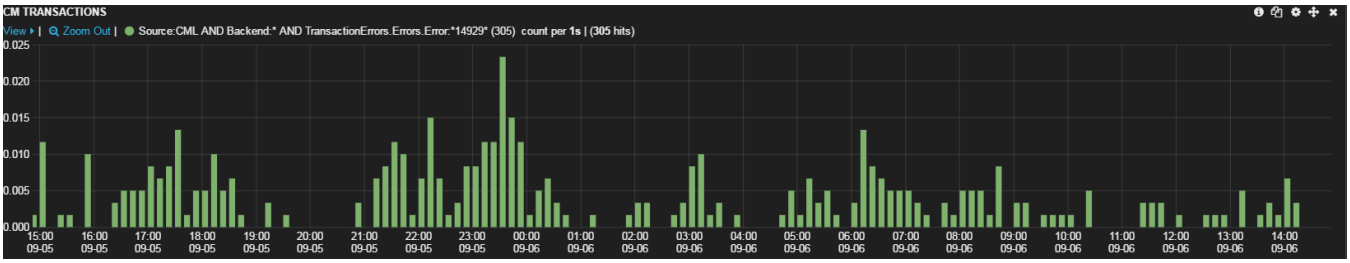
This is due to a specific ongoing bug (PTR 11736118)

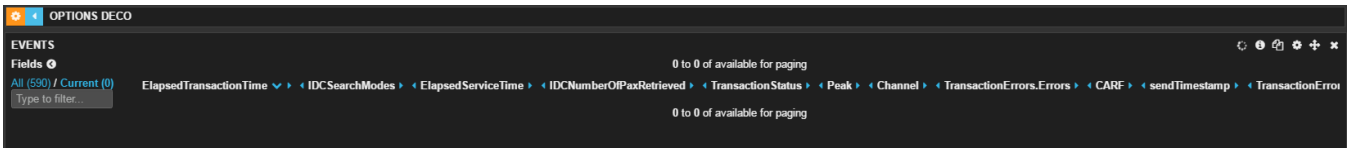
The Events table displayed in the bottom section of Kibana dashboards is useful to get information like the CARF, timestamp etc, which in turn helps you get the logs.

A field called ElapsedTransactionTime is not defined correctly as an integer on all nodes.

While Operations fix this, we notice there are some dashboards which erroneously try to sort the Event table by ElapsedTransactionTime - there is no good reason for doing this anyway.

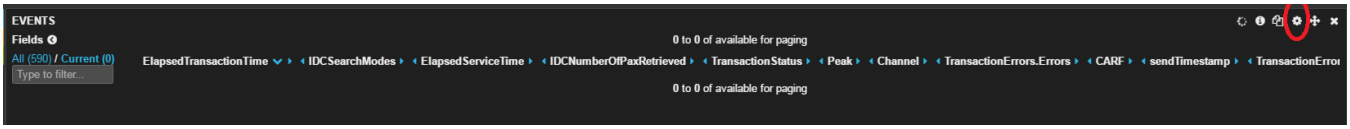
This results in exceptions, and no data is displayed in the Events table, though the Histogram at the top of the dashboard shows occurences.

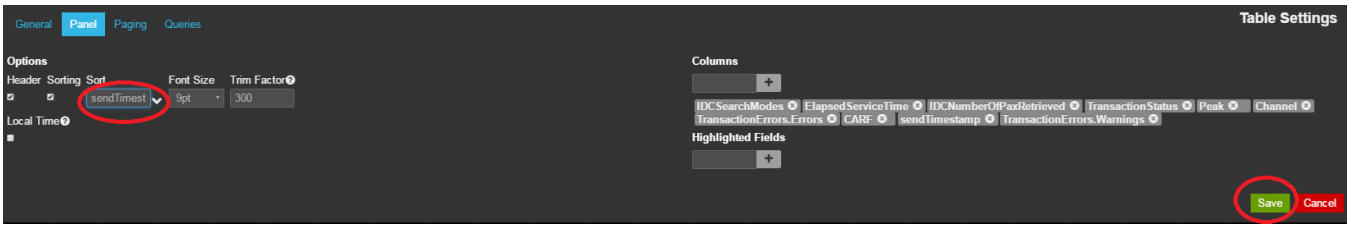




To fix this

- Click on the settings icon in the Events section
- Go to the Paging tab
- Remove the ElapsedTransactionTime from the Columns part, and change the Sort field to **sendTimestamp** instead of ElapsedTransactionTime
- Save, then Save the dashboard itself.
- Reload the dashboard





+ save the dashboard as usual (watch out for the green banner)

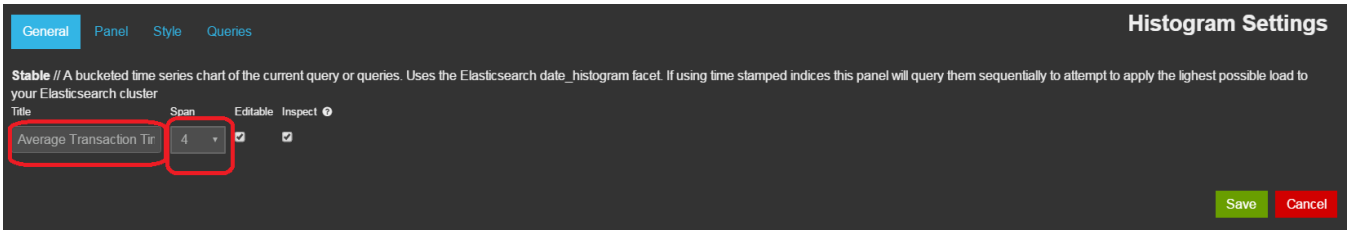
Charting the Elapsed time

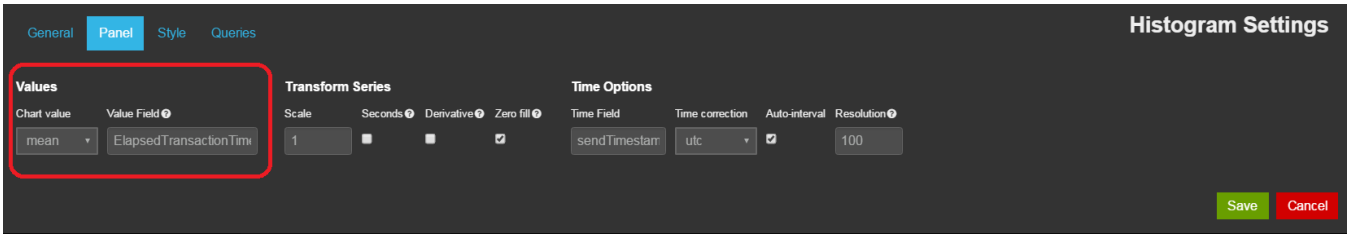
Note any field you want to chart like this should be mapped as integer (refer TR 13185379: ACM:SWA3001:PRD: Use integers in functional monitoring as an example)

A good dashboard to use as an example is : http://fumapv01.os.amadeus.net:8080/kibana-prd/#/dashboard/elasticsearch/CML_LoadMonitor_PRD

If your ElapsedTime field is mapped as an integer, this is how you can chart the Mean / Max times

1. Duplicate the main Transactions histogram so you get one more
2. Modify the properties of your new histogram - give it a Title and adjust the Span if you want on the General tab, Put a chart value of mean Or max on the Panel tab, put the value field on the Panel tab
3. Save, and then save your dashboard to get the green banner as usual





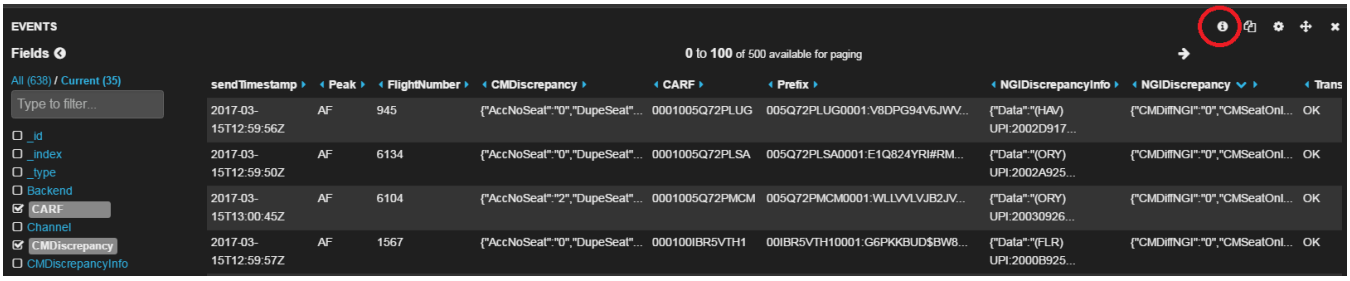
If you want a chart of **max** values, just choose max above in the Chart value part.

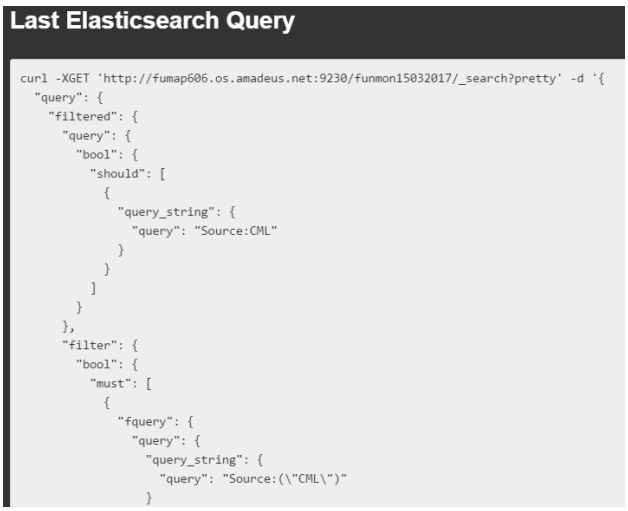
A simple export

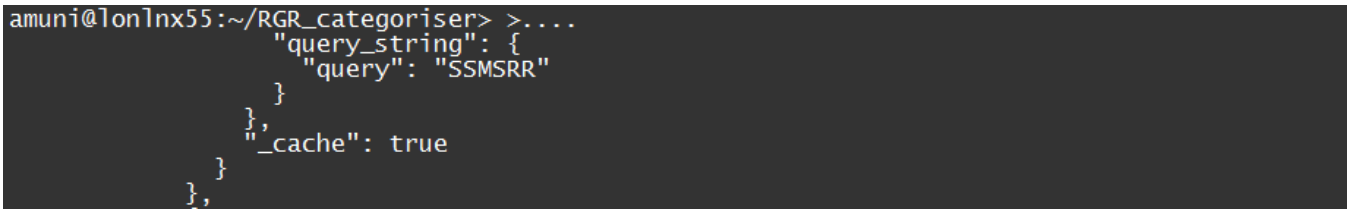
Exporting data is meant to be easy with future versions of Kibana, but for Kibana 3 we have a hack that may help.

Go to the bottom, to the events table and click on the "i" icon.

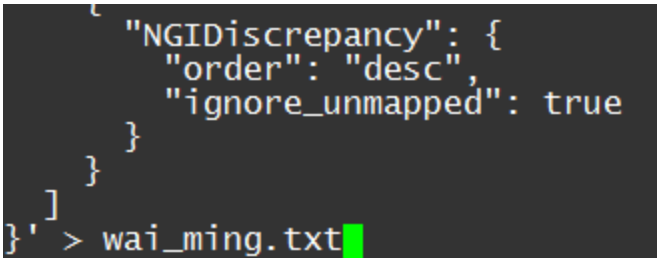
Copy the query , run from a linux box and just pipe the output to a .txt.







...ensure you put the whole query, and just pipe the output to .txt.



Note links on the web to export (nothing tried - no time)

http://stackoverflow.com/questions/18892560/is-there-any-way-in-elasticsearch-to-get-results-as-csv-file-in-curl-api?noredirect=1&lq=1

https://github.com/mobz/elasticsearch-head

Other useful links with some examples available at Querying ElasticSearch

For kibana 4 : https://github.com/minewhat/es-csv-exporter

And an old PR for Kibana 3 : https://github.com/elastic/kibana/pull/1463

A useful tool used to export ES queries to CSV can be found is es2csv.
The script the way it's implemented has the drawback that tries to store all the hits, so be careful with the query.

Otherwise it's quite easy to change it locally to eventually consider filters.