

SSI v2 5.4 Kibana 3 vs Kibana 4

We are currently at a stage where Kibana 4 has just been released.

The early release is less usable in some ways than Kibana 3, however if we stay on Kibana 3 - every dashboard we create will need to be recreated when we eventually migrate to Kibana 4.

This page tries to list the features of interest to us to try to decide on one approach vs another.

- [Links to Sample Dashboards](#)
- [Summary](#)
- [Security via Shield](#)
- [Colour scheme](#)
- [Removing filters](#)
- [Amending filters](#)
- [Adding an adhoc filter](#)
- [Controlling what fields are visible in the Events table](#)
- [Sharing a panel across dashboards](#)
- [Exporting data from a Dashboard view](#)
- [Dashboard creation](#)
- [Panel legend positioning](#)
- [Panel sizing](#)
- [Miscellaneous](#)

Links to Sample Dashboards

Please use your winaproach login and do not modify these dashboards.

Kibana 3 for Acceptance : <http://fumap303.os.amadeus.net:8080/kibana-dev/#/dashboard/elasticsearch/CML%20-%20Acceptance%20-%20UAT>

Once you load, please change the time range from the drop down to custom values 15JUN - 15JUL, as we only have old data.

Kibana 4 for Acceptance : [http://fumatv01.os.amadeus.net:5601/#/dashboard/CML-Acceptance-UAT?_g=\(\)](http://fumatv01.os.amadeus.net:5601/#/dashboard/CML-Acceptance-UAT?_g=())

Summary

Please refer the points in detail, this is just a handy recap.

The outcome is that we recommend Kibana 3 is used.

Item	Kibana 3	Kibana 4	Comments
Shield	Supported	Supported	Shield does not provide a way to control which users can load which dashboards. So Not relevant
Colour Scheme	Good	Not great https://github.com/elastic/kibana/issues/2906	Kibana 3 has a better colour scheme
Removing filters	Easy	Less user friendly	Addressable with user training
Amending filters	Easy	Not yet possible - no quick fix https://github.com/elastic/kibana/issues/1583	Could block migration to Kibana 4
Adding an adhoc filter	Easy	Less user friendly https://github.com/elastic/kibana/issues/2521	Expand event table to be able to add the filter Could block migration to Kibana 4
Controlling what fields are visible in the Events table	Easy	Less user friendly https://github.com/elastic/kibana/issues/2521	Actual table on Discover tab has to be modified and this may not be easy for non DEV in case of Kibana 4. Could block migration to Kibana 4 Note this item goes hand in hand with "Adding an Adhoc filter"
Sharing a panel across dashboards	No	Yes	Note both allow using "Save As" and start your new dashboard as a copy of an existing one

Export data from a dashboard	No	Not yet possible https://github.com/elastic/kibana/issues/1992	DMT internship could potentially address this for either version.
Dashboard creation			We will ask non DEV what they find easier. This is not a migration blocker, rather a question of training
Panel legend positioning	Good	Not great https://github.com/elastic/kibana/issues/1673 https://github.com/elastic/kibana/issues/572 https://github.com/elastic/kibana/issues/1618	Could block migration to Kibana 4
Panel sizing	Not great	Easy	Can use the mouse to change the panel size in Kibana 4.
Create Histograms on multiple files	No	Yes	
Color scheme for Histograms	Yes	No	
Time display - GMT	Yes	Not possible	This will be an issue because we use GMT in Log viewer and Winapproach. Could block migration to Kibana 4

Security via Shield

Issue : Given the vast number of users in completely different departments, we wanted to find a way to avoid one department accidentally deleting or overwriting a dashboard belonging to another department.

And potentially a user deleting a dashboard for his department or saving some corrupt changes leading to the dashboard not being usable for the rest.

From <https://www.elastic.co/guide/en/shield/current/kibana.html>, both Kibana 3 and Kibana 4 allow Shield, so this is OK.

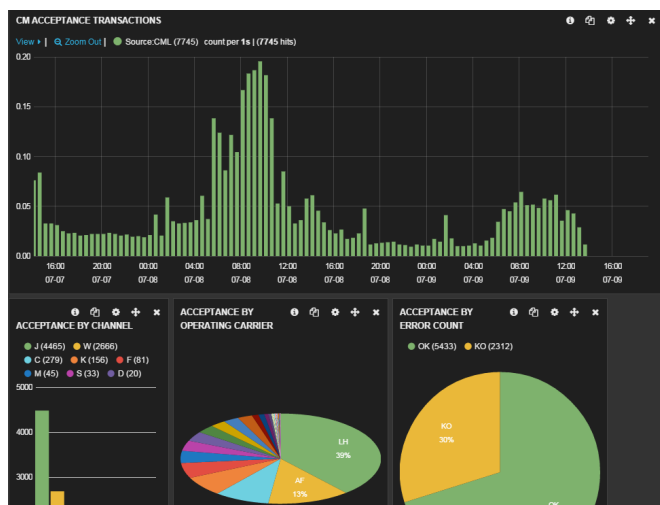
Kibana and Shield currently do not provide a way to control which users can load what dashboards, and so in fact we dont think this addresses the issue we face at all.

Colour scheme

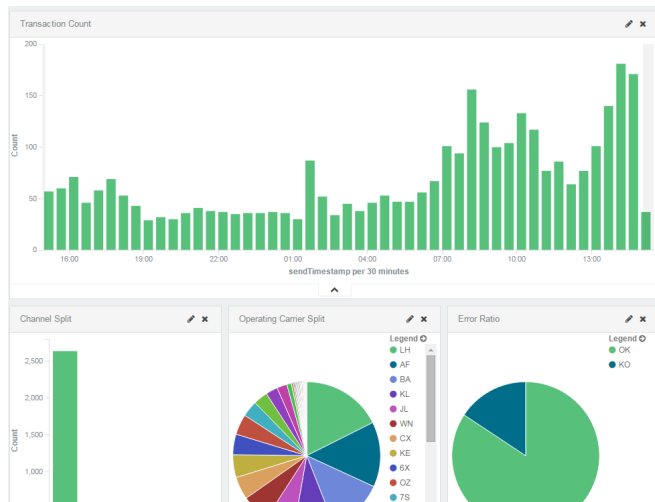
Issue : The default colour scheme of Kibana 4 is light and the gridlines in the background of histograms do not appear. This makes it less usable than Kibana 3

This is an open issue in the Kibana 4 backlog and targetted for delivery in release 4.3.0, <https://github.com/elastic/kibana/issues/2906>

Kibana 3 display



Kibana 4 display



Removing filters

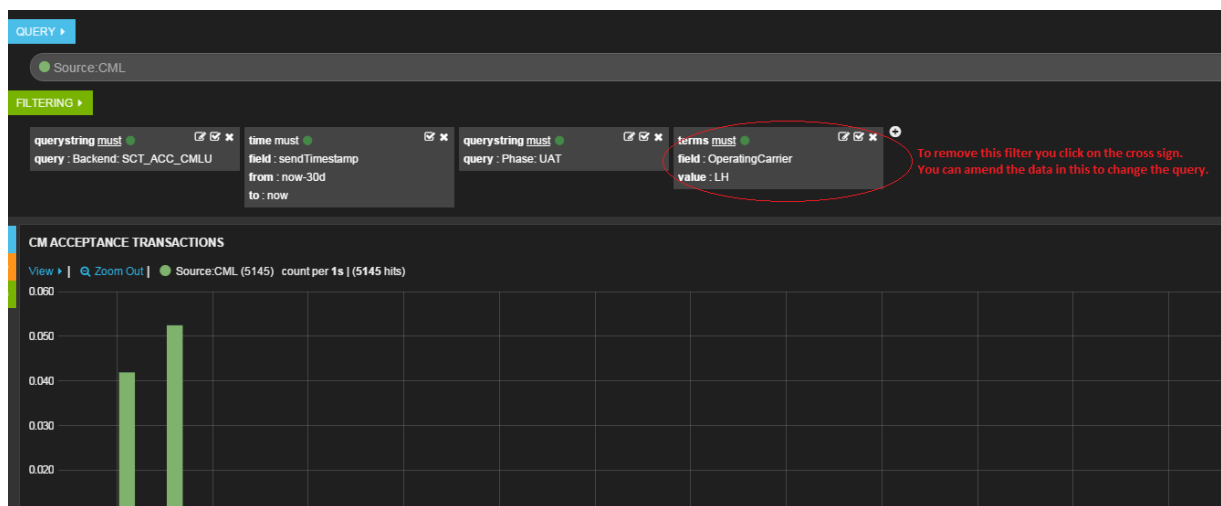
Issue : Assume you are on a dashboard and you filtered the display for an airline.

Say you want to remove the filter so you see the display for all airlines.

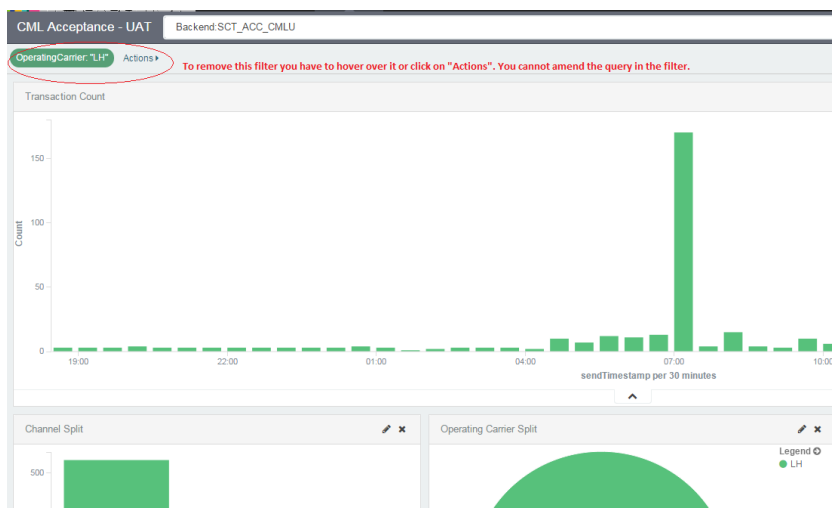
Kibana 3 you can just click on the cross icon.

Kibana 4 is less user friendly than Kibana 3, the filter removal however is just a question of training.

Kibana 3 display



Kibana 4 display



Amending filters

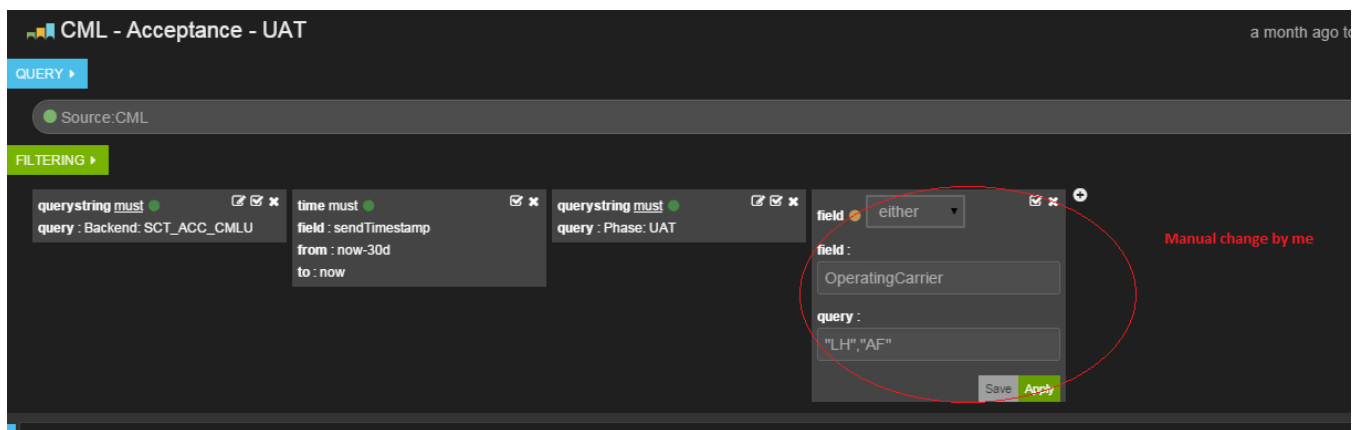
Issue : Assume you are on a dashboard and you want to filter the display by two airlines.

In Kibana 3 you can filter by one airline, then amend the filter to pull out data for 2 airlines.

In Kibana 4 you are not allowed to amend the filters and you cant do this.

There is an open issue tracking this but a fix is unlikely to be soon : <https://github.com/elastic/kibana/issues/1583>

Kibana 3 display



Adding an adhoc filter

Issue : There is a dashboard created but you want to filter on some fields which dont have their own pie charts etc, so dont explicitly appear in the dashboard panel for easy filtering.

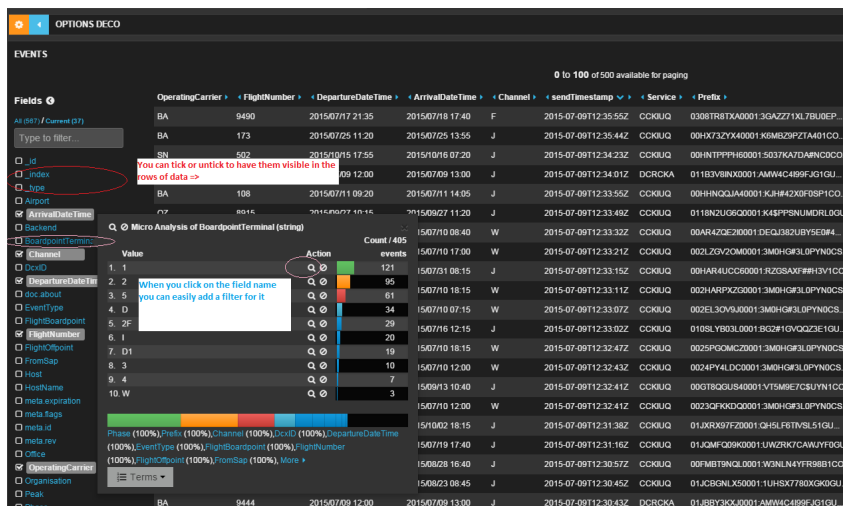
Kibana 3 has a handy Fields list which shows every field in the data pulled out and makes it easy to control what fields get displayed on the dashboard (by ticking or unticking).

Kibana 3 Fields list also lets you click on the Field name and filter by it.

Kibana 4 It does not look so usable as you need to expand one of the rows and then see the other data or filter on a field which is not explicitly displayed on the dashboard.

Could be related to open issue <https://github.com/elastic/kibana/issues/2521>

Kibana 3 display



Kibana 4 display

Acceptance Event Table								
1 2 3 4 5 ...10 »								
Time	OperatingCarrier	FlightNumber	DepartureDateTime	ArrivalDateTime	Channel	Prefix	Service	Transac
August 4th 2015, 19:33:37.000	OZ	8915	2015/10/25 10:15	2015/10/25 11:20	J	00947RBWQW0001:X3#18ZEE\$SRF1QXFMSCSMJ:12	CCKIUQ	-
Link to /funmon04082015/docs/Document/bsat401_140236564948736								
Table	JSON							
✚ Airport	Q Q	GMP						
✚ ArrivalDateTime	Q Q	2015/10/25 11:20						
✚ Backend	Q Q	SCT_ACC_CMLU						
✚ BoardpointTerminal	Q Q	0						
✚ Channel	Q Q	J						
✚ DocID	Q Q	X3#18ZEE\$SRF1QXFMSCSMJ						
✚ DepartureDateTime	Q Q	2015/10/25 10:15						
✚ EventType	Q Q	CML_ACC						
✚ FlightBoardpoint	Q Q	GMP						
✚ FlightNumber	Q Q	8915						

You have to expand the row to see all the fields or add a filter for a field which is not in an explicit dashboard panel.

Controlling what fields are visible in the Events table

Issue : Dashboards have an Event table section which shows all the actual logged data.

Not every field is part of a histogram or bar chart, but could be relevant in a particular investigation. For readability, not every field will be visible by default.

Kibana 3 has a Fields list which shows every field in the data pulled out and makes it easy to control what fields get displayed on the dashboard (by ticking or unticking).

Kibana 4 you have to go to the Discover tab, load the event table and add the field.

A best practise in Kibana 4 will be to ensure any Event table always adds All the fields relevant to that Document type.

However note the list of fields visible is **everything in the index**. i.e. if we have multiple document types in the same Index, dashboard creators should ensure they don't add irrelevant fields to their Event table.

Again, see open issue <https://github.com/elastic/kibana/issues/2521>

Kibana 3 Event table

OPTIONS DECO

EVENTS

0 to 100 of 500 available for paging

Fields

All (67) / Current (37)

Type to filter...

☐ _id

☐ _index

☐ _type

☐ Airport

☒ ArrivalDateTime

☐ Backend

☐ BoardpointTerminal

☒ Channel

☐ DocID

☒ DepartureDateTime

☐ doc.about

☐ EventType

☐ FlightBoardpoint

☐ FlightOffpoint

☐ Host

☐ HostName

OperatingCarrier	FlightNumber	DepartureDateTime	ArrivalDateTime	Channel	sendTimestamp	Service	Prefix	TransactionStatus	TransactionErrors.Errors
BA	9490	2015/07/17 21:35	2015/07/18 17:40	F	2015-07-09T12:35:55Z	CCKIUQ	0308TR8TXA0001:3GAZZ71XL7BUDEP...	OK	
BA	173	2015/07/25 11:20	2015/07/25 13:55	J	2015-07-09T12:35:44Z	CCKIUQ	00HX73ZYX40001:K6MBZ9P2TA01CO...	OK	
SN	502	2015/10/15 17:55	2015/10/16 07:20	J	2015-07-09T12:34:23Z	CCKIUQ	00HNTPPPH60001:5037KA7DAMNCO...	OK	
BA	9444	2015/07/09 12:00	2015/07/09 13:00	J	2015-07-09T12:34:01Z	DCRCKA	011B3V8NX0001:AMW4C489FJG1GU...	KO	["Error": "18231 - Passenger no...
BA	108	2015/07/11 09:20	2015/07/11 14:05	J	2015-07-09T12:33:55Z	CCKIUQ	00HHNQJMA0001:KJH#42X0F0SP1CO...	OK	
OZ	8915	2015/09/27 10:15	2015/09/27 11:20	J	2015-07-09T12:33:49Z	CCKIUQ	0118N2UGG0001:K45PPSNUMDRL0GU...	OK	
AF	7529	2015/07/10 07:10	2015/07/10 08:40	W	2015-07-09T12:33:32Z	CCKIUQ	00AR4ZQE20001:DEQJ382UBYSEB#4...	OK	
LH	8284	2015/07/10 16:00	2015/07/10 17:00	W	2015-07-09T12:33:21Z	CCKIUQ	002LZOV2OM0001:3M0HGF3LOPYNDCS...	OK	
JL	1261	2015/07/31 07:10	2015/07/31 08:15	J	2015-07-09T12:33:15Z	CCKIUQ	00HAR4UC60001:RZOSAXF##H3V1CO...	OK	
LH	8075	2015/07/10 17:35	2015/07/10 18:15	W	2015-07-09T12:33:11Z	CCKIUQ	002HARPXZG0001:3M0HGF3LOPYNDCS...	OK	
LH	8083	2015/07/10 06:30	2015/07/10 07:15	W	2015-07-09T12:33:07Z	CCKIUQ	002EL3OV9J0001:3M0HGF3LOPYNDCS...	OK	

Kibana 4 Event table

CML Event Table

1 2 3 4 5 ...10 »

Time	OperatingCarrier	FlightNumber	DepartureDateTime	ArrivalDateTime	Channel	Prefix	Service	TransactionErrors.Errors	Boardp
▶ August 5th 2015, 15:03:08.000	LH	8214	2015/08/06 17:30	2015/08/06 19:00	W	00LDN43WTD0001:1YK6MCXXY3A81A5X8WY3X J7:3	CCKIUQ	-	2
▶ August 5th 2015, 15:03:08.000	WN	1134	2015/08/12 10:50	2015/08/12 12:40	J	001ZNBB4PV0001:3M4BDM3ES211QXFSMCS MJ:10	CCKIUQ	-	N
▶ August 5th 2015, 15:03:04.000	BA	2931	2015/08/05 06:40	2015/08/05 08:15	F	024HNSNA1C0001:NY80SYLB8Q431C4C5QAX# 07:11	CCKIUQ	-	-
▶ August 5th 2015, 15:02:58.000	LH	8214	2015/08/06 17:30	2015/08/06 19:00	W	00L87S1RDJ0001:1YK6MCXXY3A81A5X8WY3X J7:2	CCKIUQ	-	2
▶ August 5th 2015, 15:02:54.000	6X	906	2015/08/10 10:40	2015/08/10 13:15	J	010902Z6Q0001:6Y6Z88SEFU011G08Y34TYI7:29	CCKIUQ	-	2
▶ August 5th 2015, 15:02:46.000	KL	893	2015/08/22 21:30	2015/08/23 14:05	J	01JXSO58LM0001:42P8RZ37W4ZU0G08Y34TY I7:23	CCKIUQ	-	-
▶ August 5th 2015, 15:02:42.000	6X	4013	2015/08/10 22:45	2015/08/11 19:35	C	00KDNJ2JPI0001:3EPLHWA3C7M0Q0XFSMCS MJ:19-1	HSFREQ	-	-
▶ August 5th 2015, 15:02:33.000	6X	1434	2015/08/12 07:55	2015/08/12 09:10	C	0028HZ2A6670001:9F3J8I10H10XFSMCS MJ:14-1	HSFREQ	{ "Error": "17336 - Record in use - Re-enter"	1

Kibana 3 adding an element to Event table

EVENTS

0 to 100 of 500 available for paging

Fields

All (67) / Current (37)

Type to filter...

☐ _id

☐ _index

☐ _type

☐ Airport

☒ ArrivalDateTime

☐ Backend

☐ BoardpointTerminal

☒ Channel

☐ DocID

☒ DepartureDateTime

☐ doc.about

☐ EventType

☐ FlightBoardpoint

☒ FlightNumber

☐ FlightOffpoint

☒ FromSap

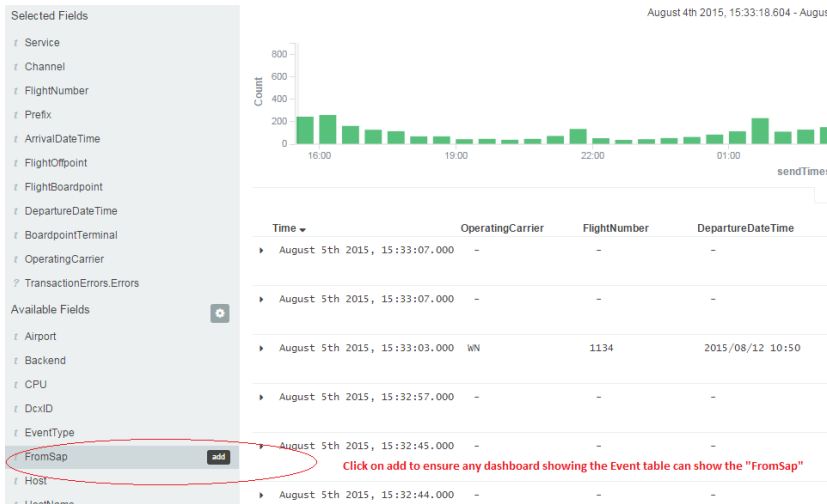
☐ Host

☐ HostName

OperatingCarrier	FlightNumber	DepartureDateTime	ArrivalDateTime	Channel	sendTimestamp	Service
BA	9490	2015/07/17 21:35	2015/07/18 17:40	F	2015-07-09T12:35:55Z	CCKIUQ
BA	173	2015/07/25 11:20	2015/07/25 13:55	J	2015-07-09T12:35:44Z	CCKIUQ
SN	502	2015/10/15 17:55	2015/10/16 07:20	J	2015-07-09T12:34:23Z	CCKIUQ
BA	9444	2015/07/09 12:00	2015/07/09 13:00	J	2015-07-09T12:34:01Z	DCRCKA
BA	108	2015/07/11 09:20	2015/07/11 14:05	J	2015-07-09T12:33:55Z	CCKIUQ
OZ	8915	2015/09/27 10:15	2015/09/27 11:20	J	2015-07-09T12:33:49Z	CCKIUQ
AF	7529	2015/07/10 07:10	2015/07/10 08:40	W	2015-07-09T12:33:32Z	CCKIUQ
LH	8284	2015/07/10 16:00	2015/07/10 17:00	W	2015-07-09T12:33:21Z	CCKIUQ
JL	1261	2015/07/31 07:10	2015/07/31 08:15	J	2015-07-09T12:33:15Z	CCKIUQ
LH	8075	2015/07/10 17:35	2015/07/10 18:15	W	2015-07-09T12:33:11Z	CCKIUQ
LH	8083	2015/07/10 06:30	2015/07/10 07:15	W	2015-07-09T12:33:07Z	CCKIUQ
WN	708	2015/07/16 09:40	2015/07/16 12:15	J	2015-07-09T12:33:02Z	CCKIUQ
LH	8075	2015/07/10 17:35	2015/07/10 18:15	W	2015-07-09T12:32:47Z	CCKIUQ
LH	8075	2015/07/10 11:00	2015/07/10 12:00	W	2015-07-09T12:32:43Z	CCKIUQ
LH	50	2015/09/13 09:50	2015/09/13 10:40	J	2015-07-09T12:32:41Z	CCKIUQ

Tick "FromSap" to see data in Event table

Kibana 4 adding an element to Event table (can be avoided by following a best practise)



Sharing a panel across dashboards

Issue : In Kibana 3 you cannot share a panel created in 1 dashboard in another dashboard. You can always do a "Save as" and start your new dashboard as a copy of an existing one and then amend it.

In Kibana 4 you are able to share existing visualisations across Dashboards.

If multiple dashboards need to change an existing panel, in Kibana 3 you have to change each dashboard, while in Kibana 4 you only change the visualisation once.

On the flip side once you change a visualisation you impact every dashboard using the same visualisation in Kibana 4.

Exporting data from a Dashboard view

Issue : It would be great to get the raw data corresponding to a dashboard time window (of course subject to size constraints)

Kibana 3 offers no data export facility.

Kibana 4 plans to offer data export to CSV facility, open issue <https://github.com/elastic/kibana/issues/1992>

Current data export in Kibana 4 is restricted to the Discover tab, and actually only gives the Timestamp and Counts - not all the raw data.

Note an option could be progress the DMT internship tool to allow anyone to input query parameters and filters visible in a dashboard, and to get the raw data.

Dashboard creation

Issue : Dashboard creation usability

In Kibana 3 searching and visualisation is combined so it may be easier for non technical users to amend dashboards.

In Kibana 4 you first need to go to Discover tab and do your search, then to Visualise tab and add your visualisation then finally to Dashboard tab and add your Visualisation to the Dashboard.

You can just save a copy of an existing dashboard then amend in both Kibana 3 and Kibana 4. Note Kibana 4 if you export a dashboard from one region to another you need to export every visualisation too.

You are able to share existing visualisations across Dashboards - this is not possible in Kibana 3

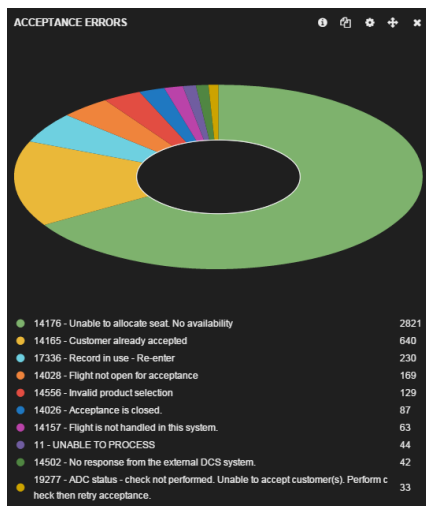
Panel legend positioning

Issue : Kibana 4 does not let us control the size or position of the legends in a panel and the default placement leads to truncation for items like error messages.

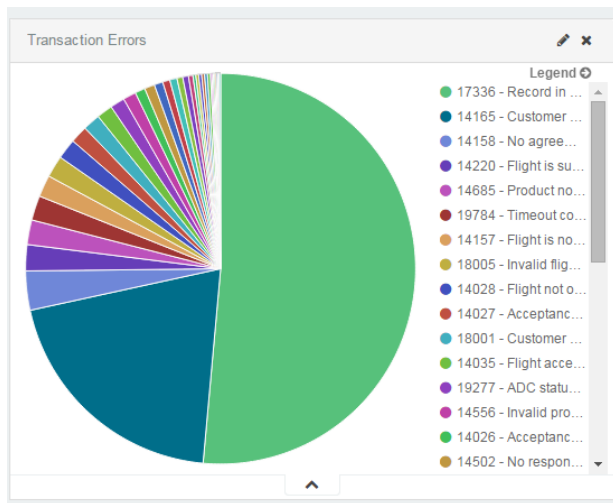
Kibana 3 displays the legend in a better way.

Open issues exist on Kibana 4 to improve this : <https://github.com/elastic/kibana/issues/1673>, <https://github.com/elastic/kibana/issues/572>, <https://github.com/elastic/kibana/issues/1618>

Kibana 3 display



Kibana 4 display



Panel sizing

Issue : Not a big issue, more of a comment.

Kibana 4 lets you use the mouse and drag to resize a panel on a dashboard.

Kibana 3 does not let you do that - you have to edit the options of that panel to resize it.

Miscellaneous

This is to try to list the Kibana 4 benefits listed on the web, i.e. features which are not available in Kibana 3 :

Search highlights , Enhanced Elastic Search Aggregation, Scripted Fields, Dynamic Dashboard, Separation of Client-Server, more powerful visualisations

<http://logz.io/blog/5-great-reasons-to-upgrade-to-kibana-4/>

<https://www.timroes.de/2015/02/07/kibana-4-tutorial-part-3-visualize/>