Alastria ELK

Install and use ELK to read quorum alastria logs.

https://github.com/netmanito/elk-docker/tree/quorum

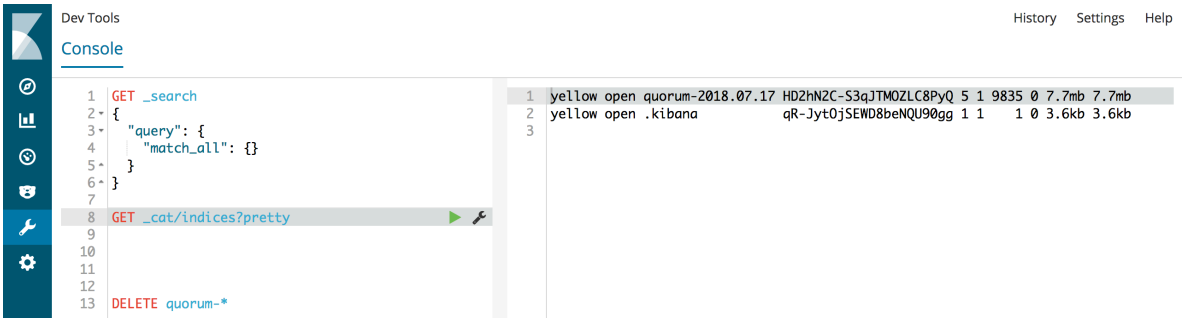
Download quorum branch from GitHub

Deploy the docker service and run it.
Make sure you've the quorum logs visible on the docker containers.

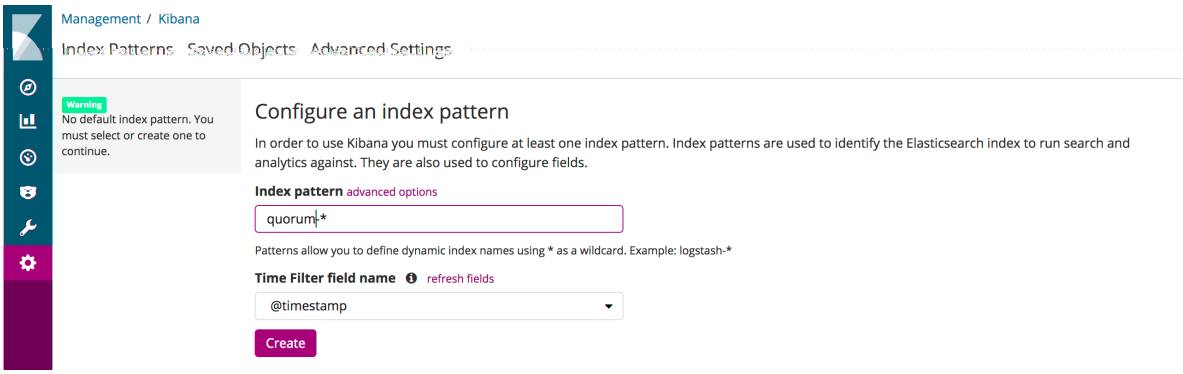
Review docker-composer.yml and Dockerfile.
Only editing docker-compose.yml volume section should be enough to make it work by it's own.

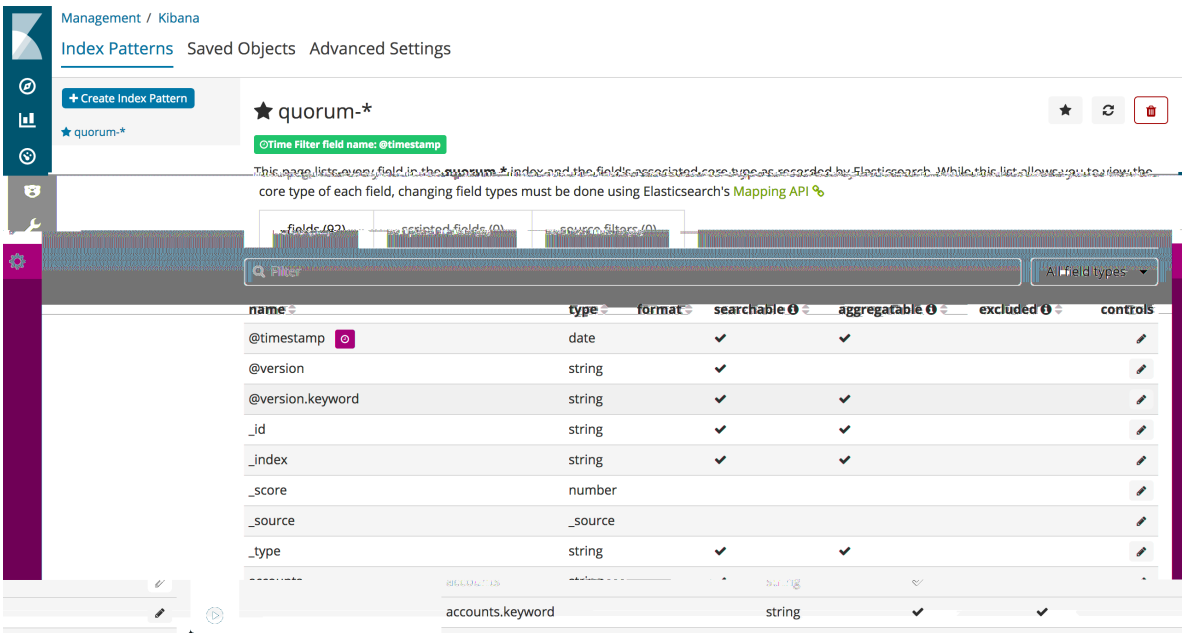
Once working ...

First check if you're indexing data, there should be 2 indices as shown in the picture below.

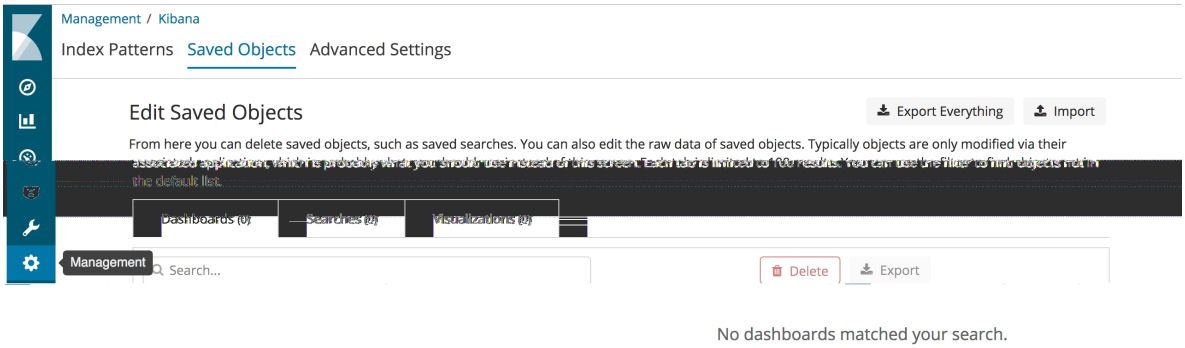


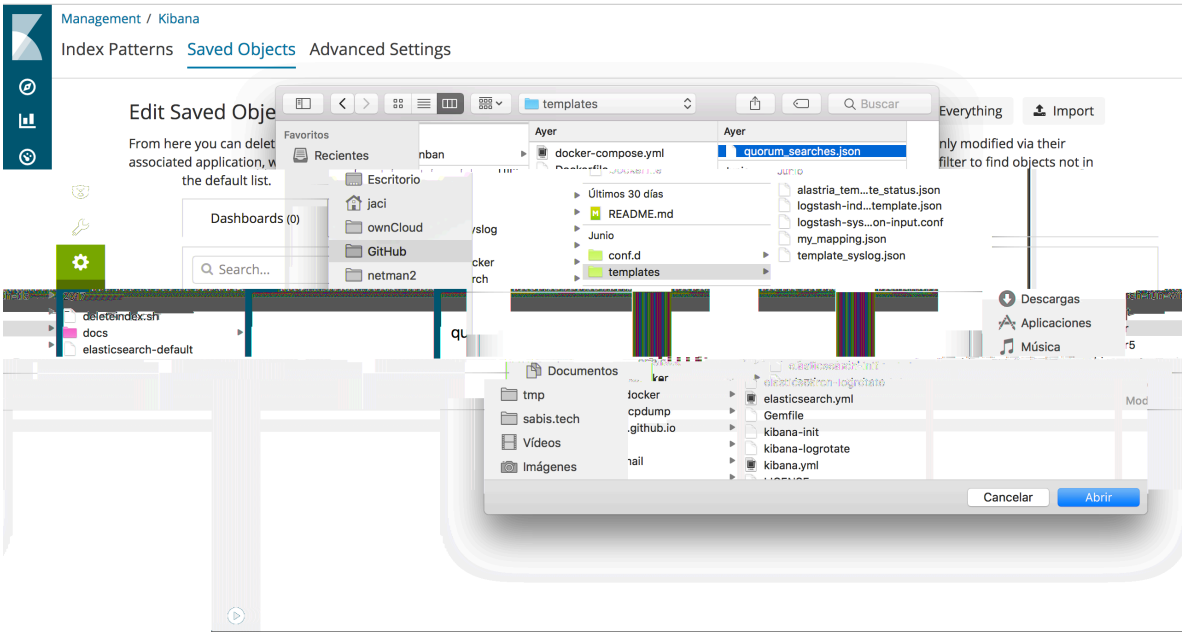
If quorum_YYYY-mm-dd is available, get to Manage section and create the Index-Pattern.

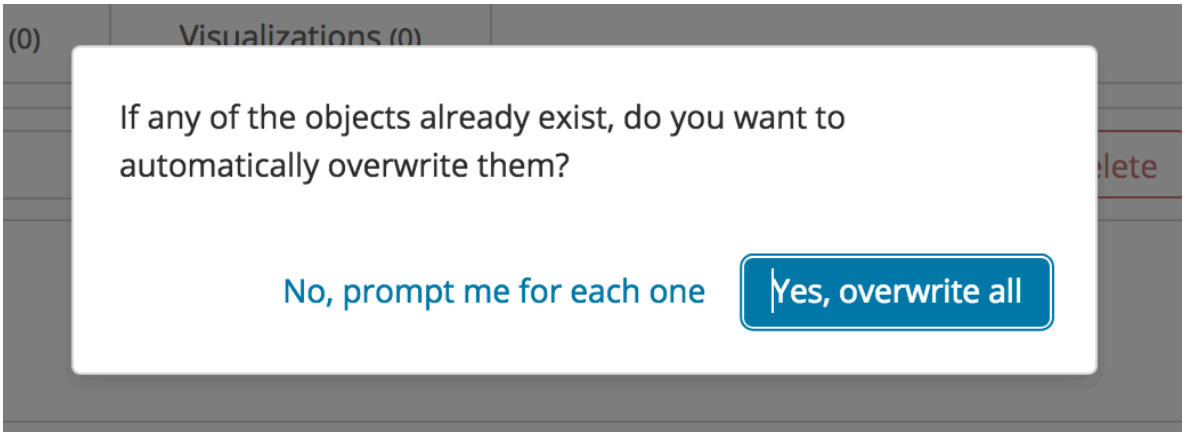




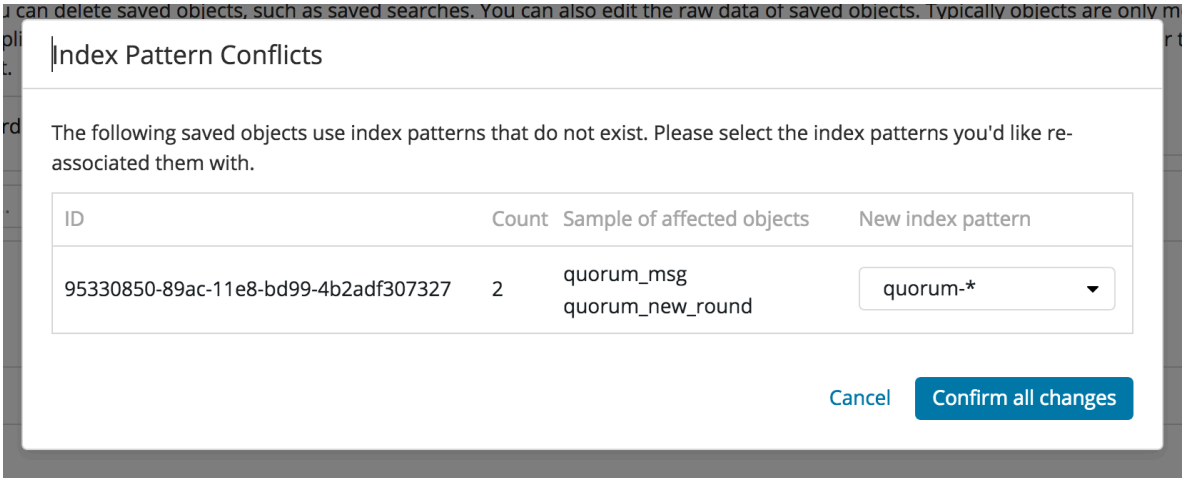
Then go to *Saved Objects* and **import** *templates/quorum_searches.json*
Now you'll have some saved searches and graphs.



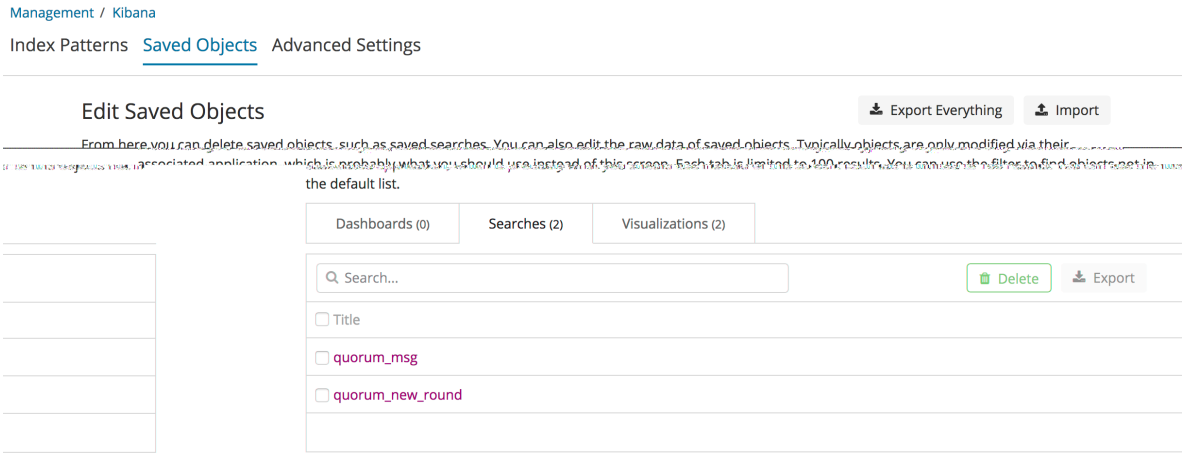




Once you press Yes, and overwrite, It could be possible to receive a message of pattern conflicts, just confirm all changes and it'll work.

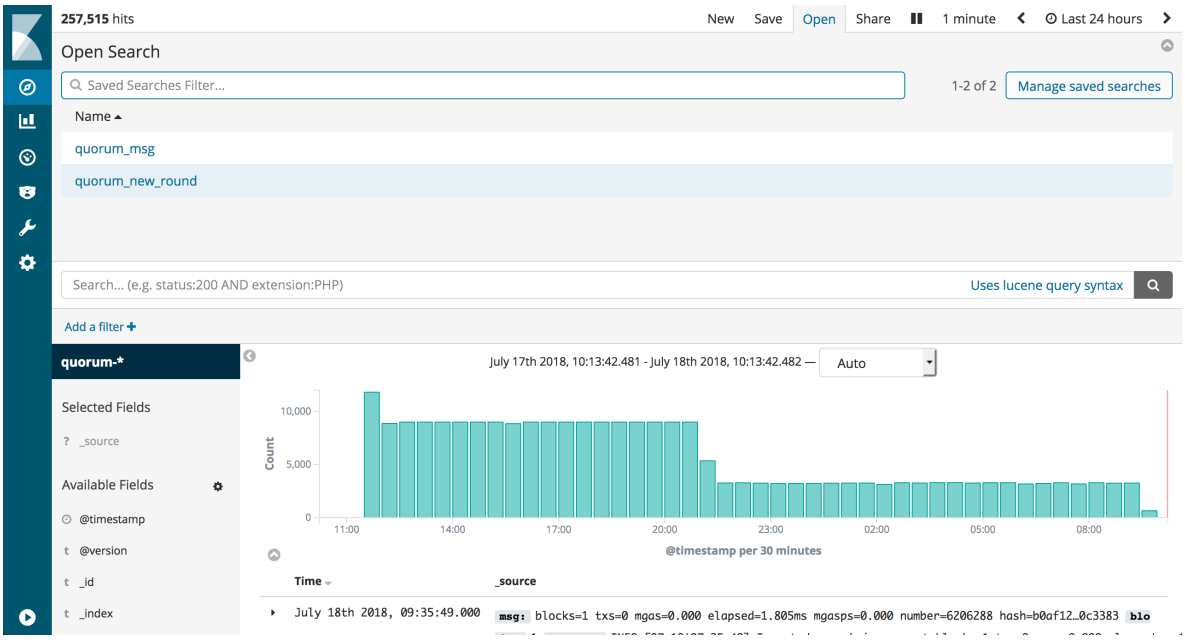


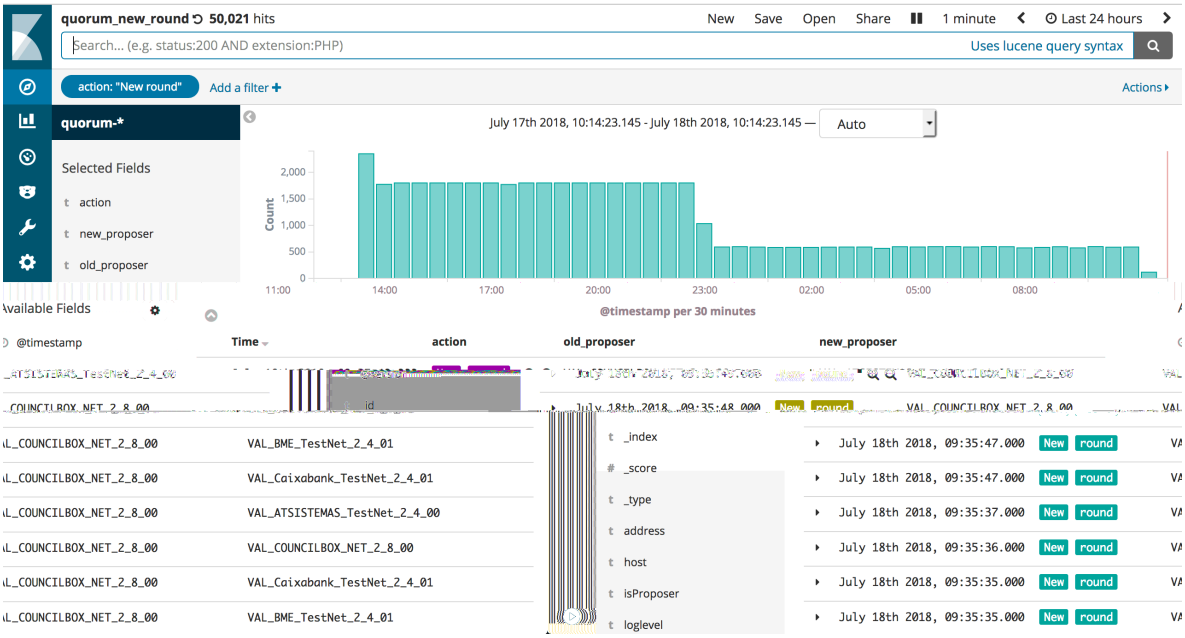
Once objects are imported, you'll see 2 saved Searches and 2 Visualizations. You can press on to see them in action or go over the left buttons.



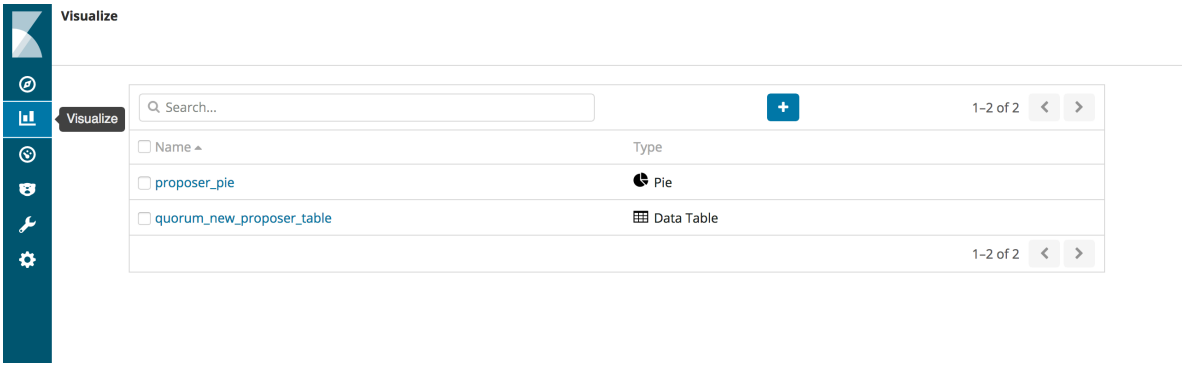
Go to discovery, press open and select quorum_new_round to see al messages

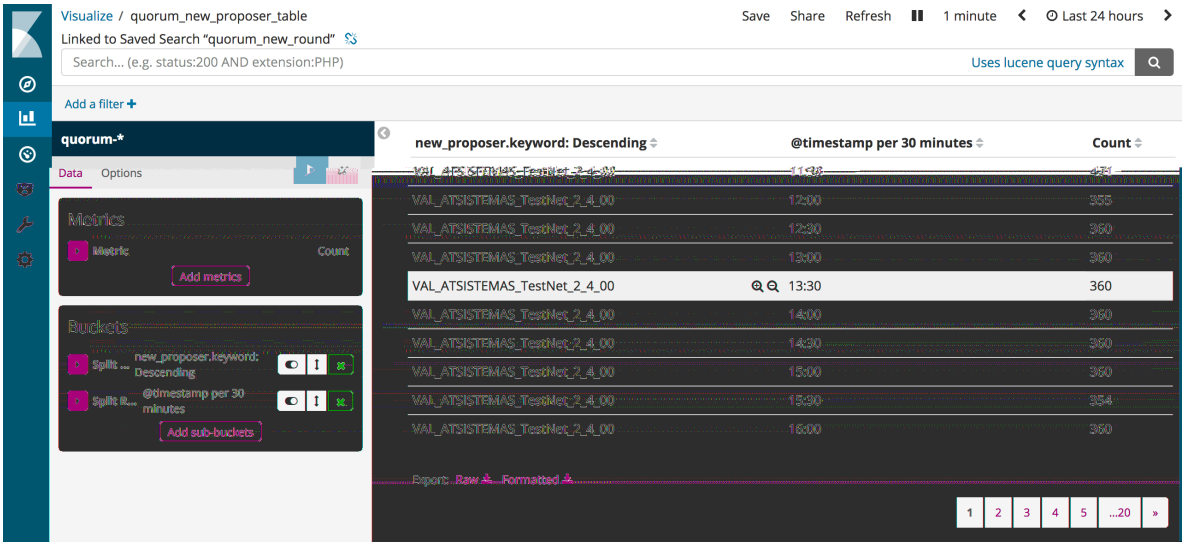
from ‘new round’ action.

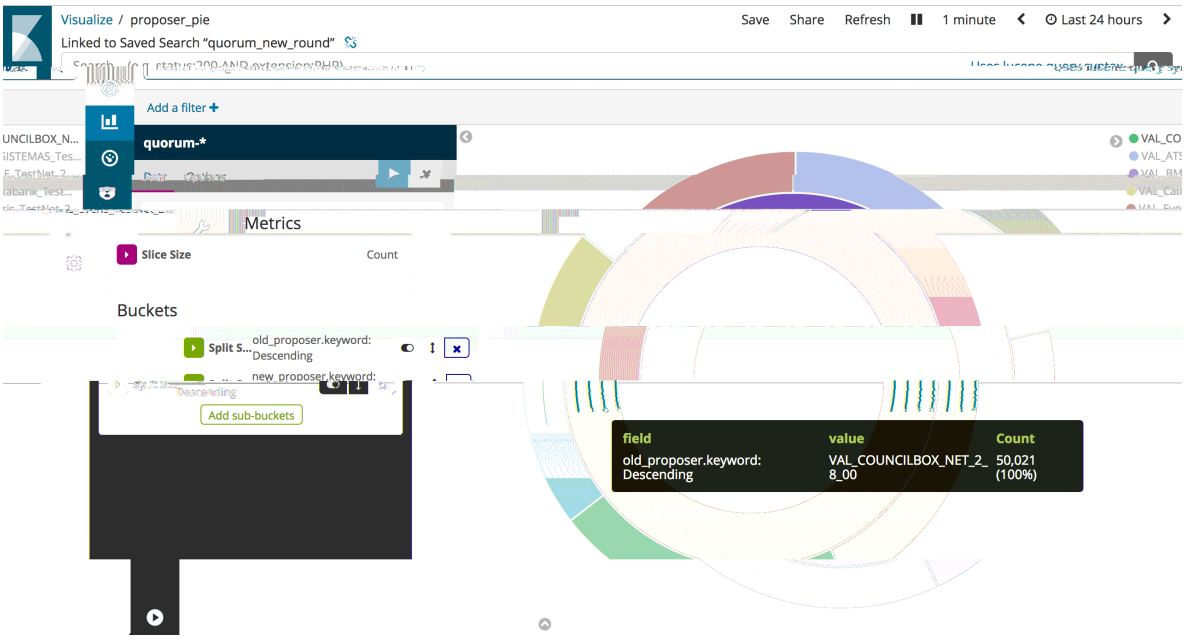




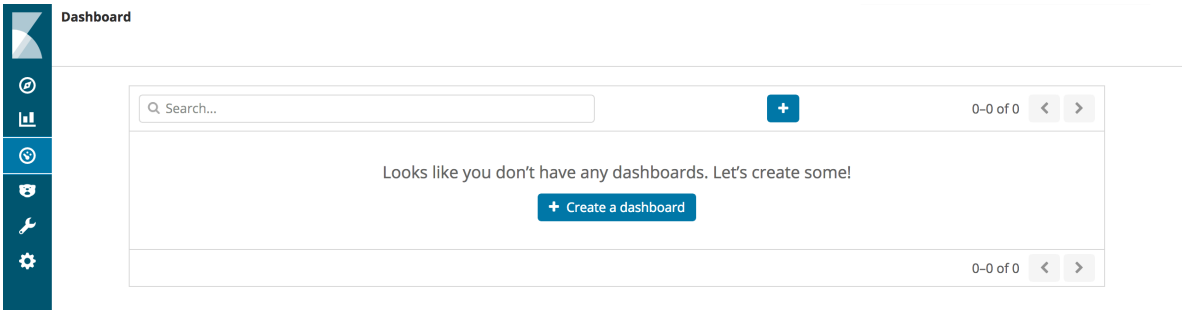
To watch visualisations, select the visualisation button and open any of the saved graphs.



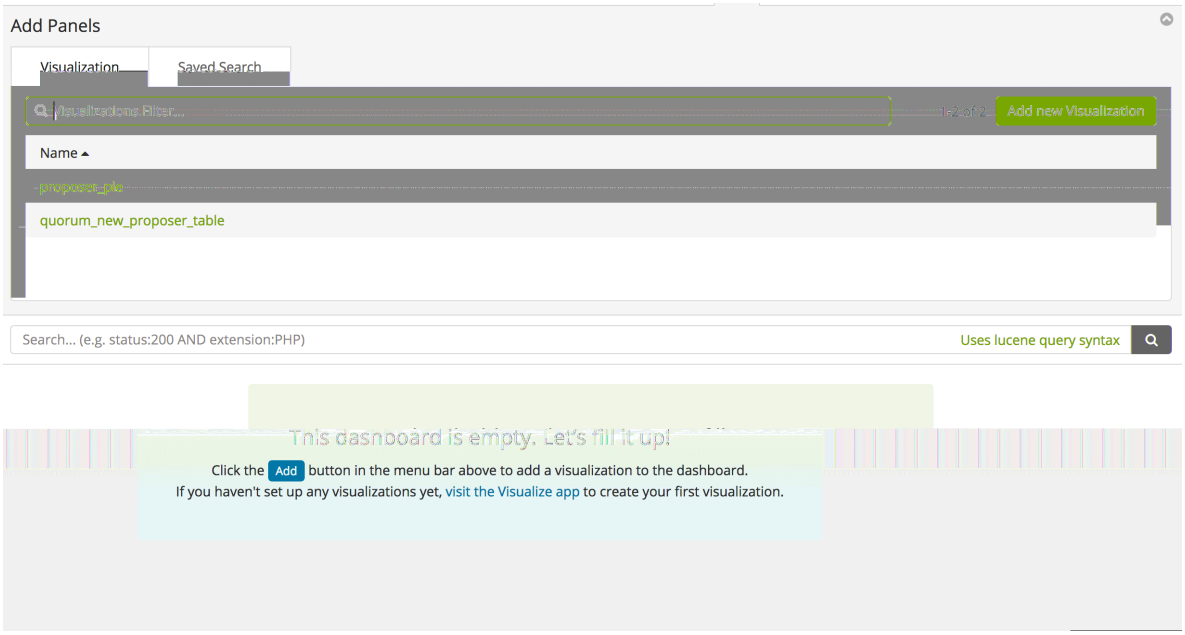




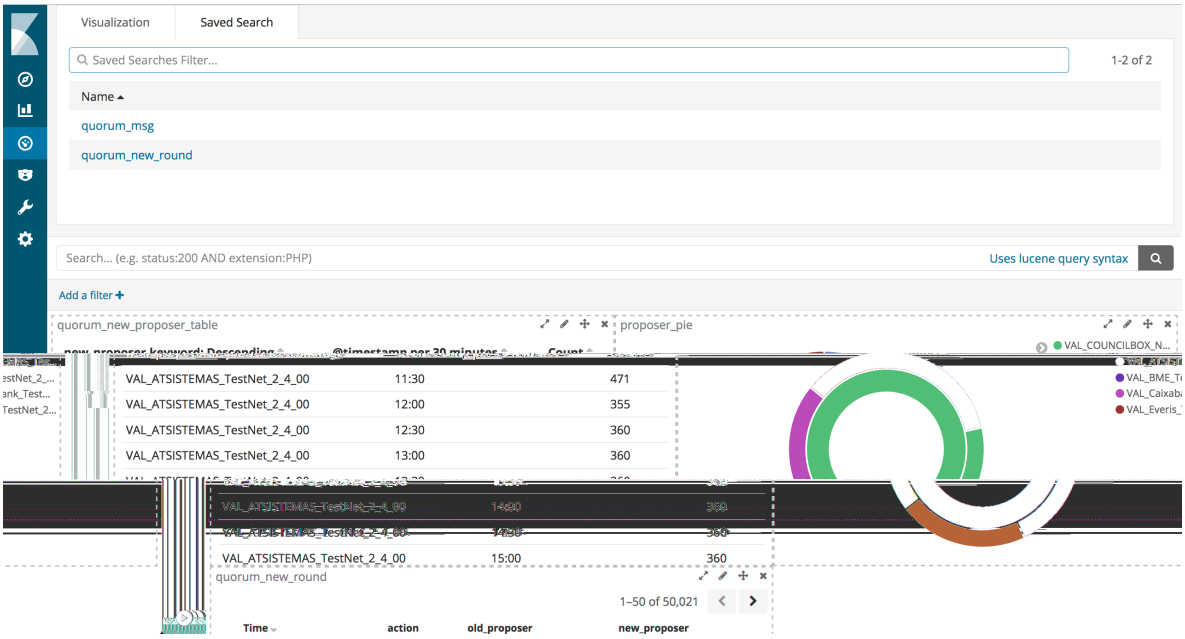
Create a Dashboard



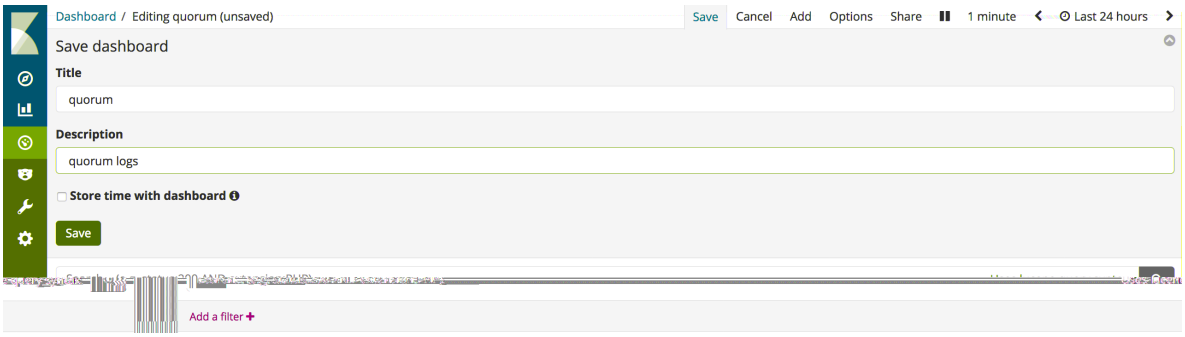
Press create dashboard button.



Click de add button and select visualisations and searches. They'll be added bellow and you'll be able to move them.



Once you've all the elements, press save on the top and give it a name.



Now your dashboard is ready.