BLOG POSTS

	Content
Post Title	Exploring an ELK Stack: Part 3: Dashboards
Post Date	
Attributed To	Peter Welcher
Written By	Peter Welcher
Reviewed By (Name & Date)	Dave Donati (11/19)
Reviewed By (Name & Date)	

Meta Title (55 characters including spaces)	Exploring an ELK Stack: Part 3: Dashboards
Meta Description (156 characters including spaces)	
Target Keywords	
Categories	Technology
Tags	N/A
Call to Action	N/A
Image	Put a brief description of what the image should be or note that a file is attached. DO NOT paste the image into this Word doc; send it as a separate file.

Note: Naming convention for files as they go back and forth

- Original writer names file with "_V1" at the end (e.g., blogtitle_V1)
- First reviewer, makes edits and renames with initials at end (e.g., blogtitle_V1_af)
- If another reviewer, again add initials to end to keep the string of reviewers (e.g., blogtitle_V1_af_pw)
- When original writer gets it post back with edits, she makes revisions and saves the file as V2 (e.g. blogtitle_V2) – then reviewers continue as above with initials
- When post is complete, it is saved with "Final" and the post date at the end (e.g. blogtitle_FINAL_022012)

Copyright © 2018. All Rights Reserved.

COPY FOR POST:

This is Part 3 of a blog series tutorial about the ELK stack. The prior blogs in the series are:

- Exploring an ELK Stack Part 1: Importing Data and Patterns
- Exploring an ELK Stack: Part 2: Kibana Visualizations

Commented [PW1]: Insert link

Commented [PW2]: Insert link

Part 1 introduced the ELK stack and covered getting some data into Elasticsearch via a new experimental Kibana feature. It also lightly covered Logstash grok patterns, and some web tools for working with them (regular expressions made easier!).

Part 2 covered some basic things you can do with the Kibana visualization tool (the "K" in "ELK).

This blog walks through creating a Kibana dashboard.

WHY DO DASHBOARDS?

By way of motivation, I've been seeing more and more ELK or Grafana-based dashboards in sites where I consult. The dashboards show KPIs (Key Performance Indicators), often derived from log data. These might include:

- Web front-end hits per second
- Web ad hits per second, by collecting location
- Web query response time
- Average time to authenticate (for a service offering)

The general idea is to watch measures reflecting user experience / service delivery, so as to be able to respond quickly when there's a problem. Alerts are usually also set up to notify key personnel, but that's a separate topic.

Regarding dashboard content, I've been reading the book Practical Monitoring: Effective Strategies for the Real World, by Mike Julian. It covers the KPI and Monitoring topic in detail. Recommended!

While it is more application focused, it could easily apply to the network management side of Operations as well. It also seems to agree (in a generic way) with my opinion, as to why most current network management tools are not providing the information and value they should. But that's a topic (rant?) for another blog!

For what it's worth, the Kibana developers did a good job of making the dashboard creation process intuitive, so you'll probably find this a quick read.

In comparison, I'd have to describe the Part 1 data import topic as being fairly straightforward, except for the patterns. Regular expressions are **never** simple!

Regarding Part 2, the creation of a visualization took a little getting used to but helped. I hope it did so for you too! I do have the feeling other forms of visualization

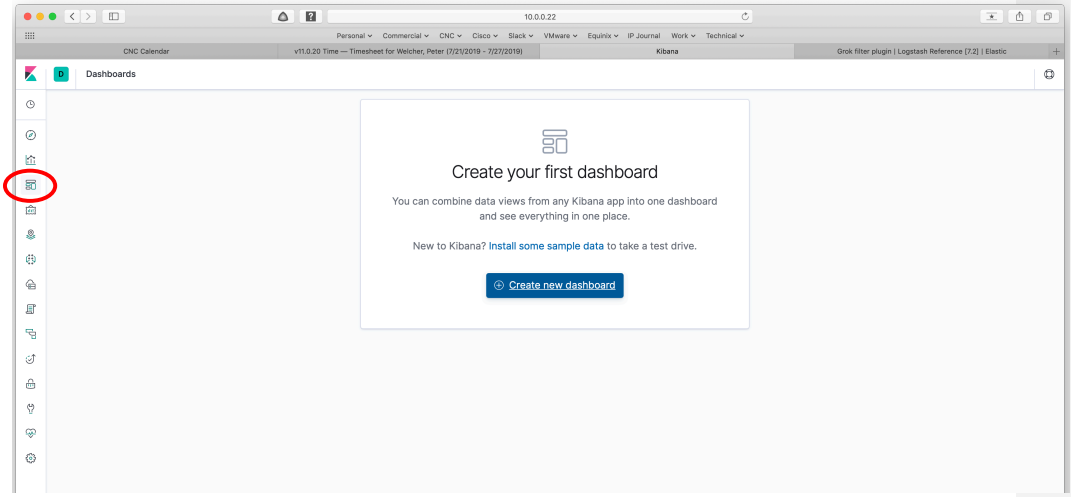
Copyright © 2018. All Rights Reserved.

will also take some experimentation, but I don't plan to document them better for Elastic (the company behind ELK, note: elastic.co, not .com).

Let's Build a Dashboard

The third icon on the left leads to Visualizations (not counting the recent icon and the main Kibana page logo / icon).

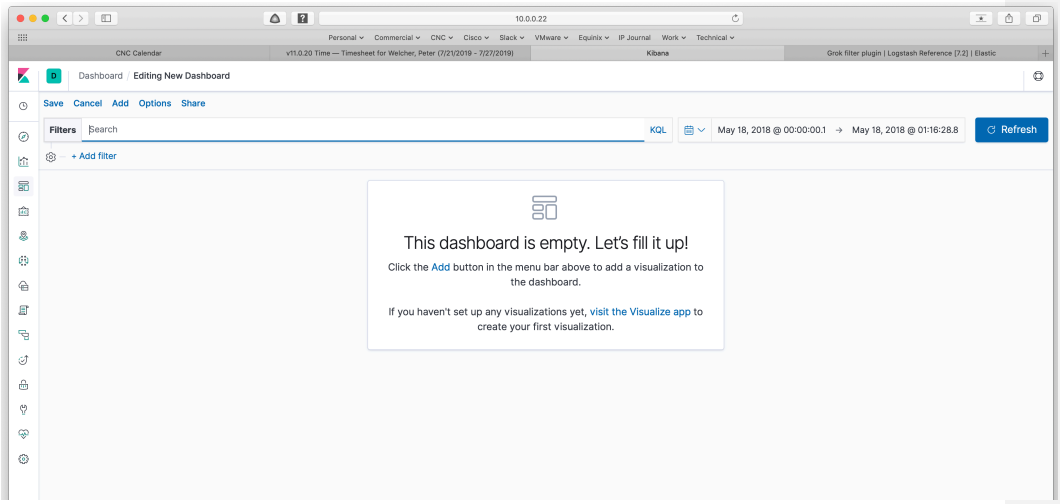
Clicking on the icon brings up the following page.



In case you hadn't already guessed: click on the blue button to proceed.

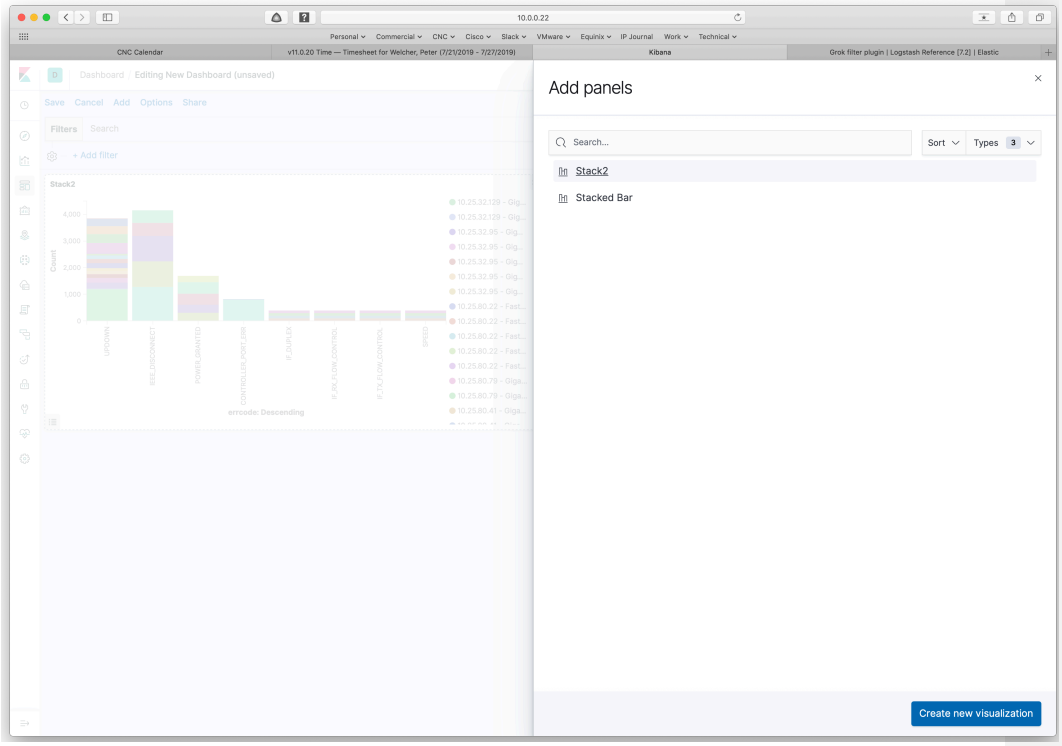
Here's what comes up:

Copyright © 2018. All Rights Reserved.



Click on Add. That brings up the following screen:

Copyright © 2018. All Rights Reserved.

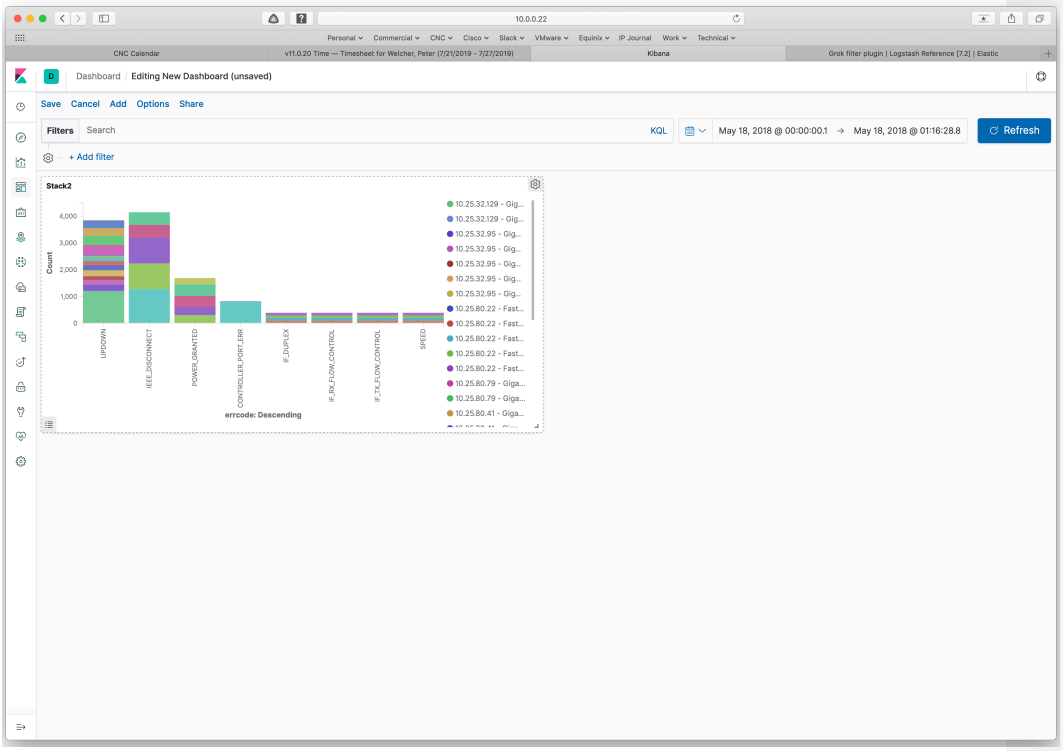


In the background, you can see one of my previously saved visualizations. The list of saved visualizations is visible in the right half of the screen. You can either pick one of them or click the blue button at the bottom right to add a new visualization.

In this case, I clicked on Stack2. If you have a saved visualization, go ahead and use that. If not, skip ahead to creating a new visualization, as described further below (section header “Adding Another”).

The result of picking a saved visualization is a default placement on the dashboard that is being built (edited), as seen below.

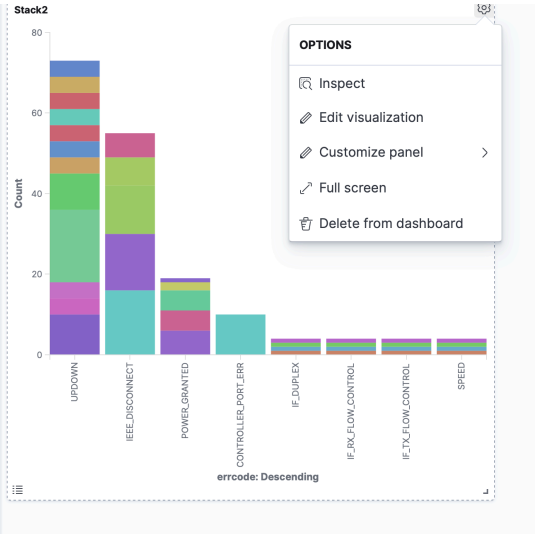
Copyright © 2018. All Rights Reserved.



Clicking and dragging the bottom right corner re-sizes the added visualization. You can also click and drag (grab) the top region of the item and drag it to another position on the dashboard.

The gear icon in the upper right of the item allows you to make changes, etc. See the following screen capture.

Copyright © 2018. All Rights Reserved.



The bullet point icon on the bottom left lets you turn the legend display on and off. If you compare the right side of the two above screen captures, the legend is turned on in the first, and is turned off in the second.

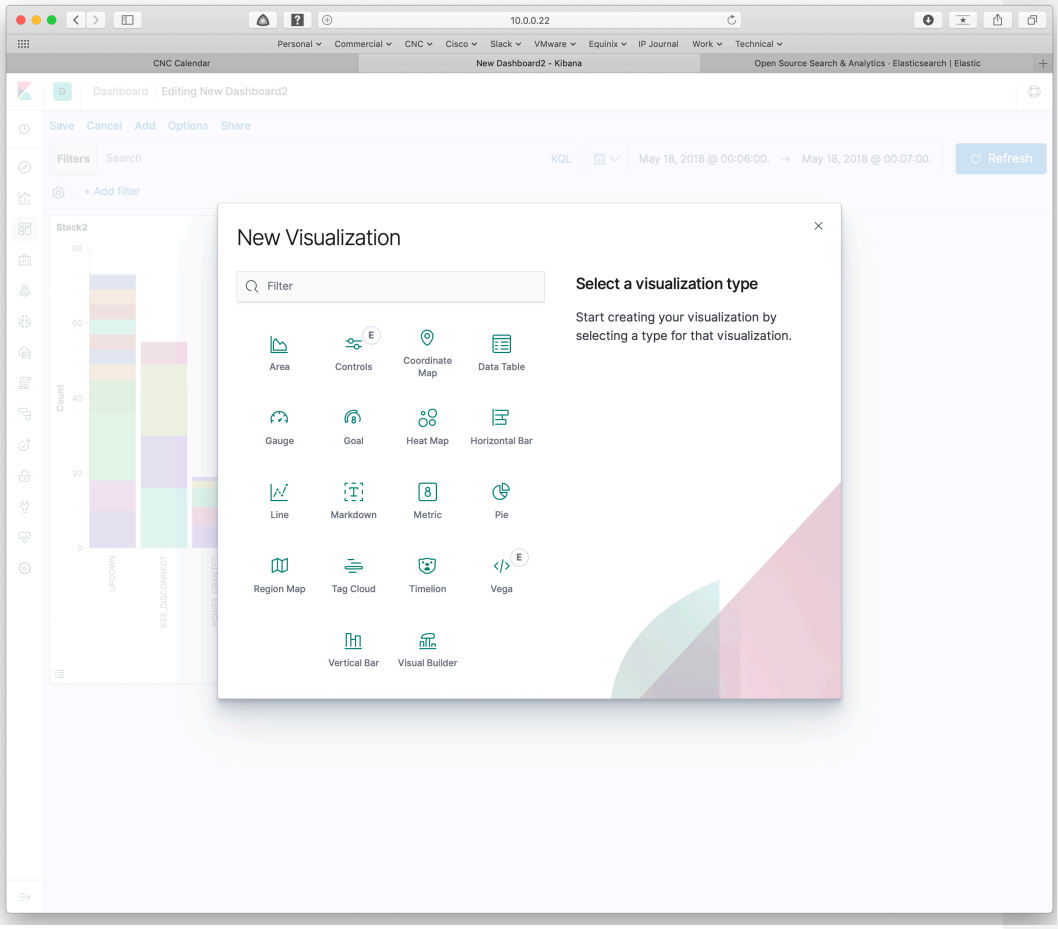
Adding Another Visualization

To add another visualization to the dashboard, click Add in the menu at the top (to the right of Save). That brings up the same Add Panels box as shown earlier. This time let's add a new visualization. Click on the bottom right "Create New Visualization" button to do so.

That brings up the following screen, which we've seen before (Part 2 of this blog series).

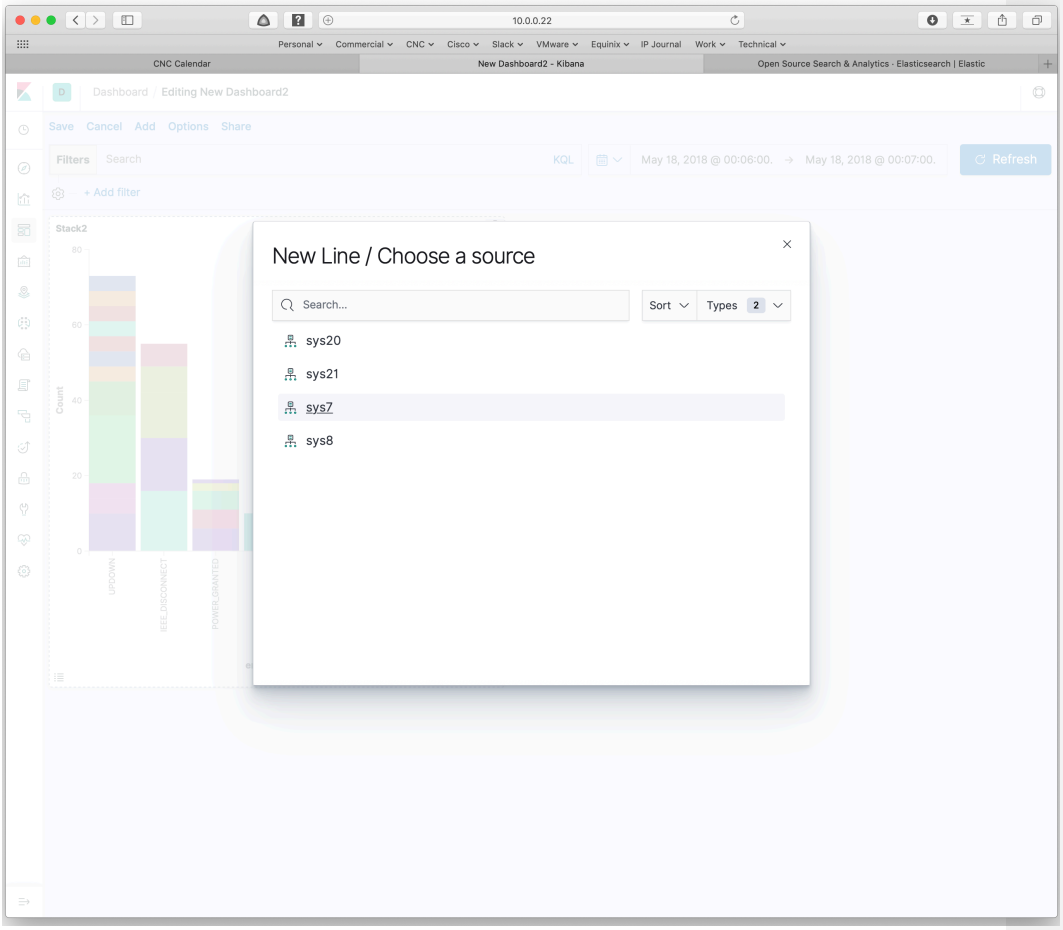
Commented [PW3]: Insert link

Copyright © 2018. All Rights Reserved.



For the sake of experimentation, I clicked on Line, which leads to being asked for the source data.

Copyright © 2018. All Rights Reserved.

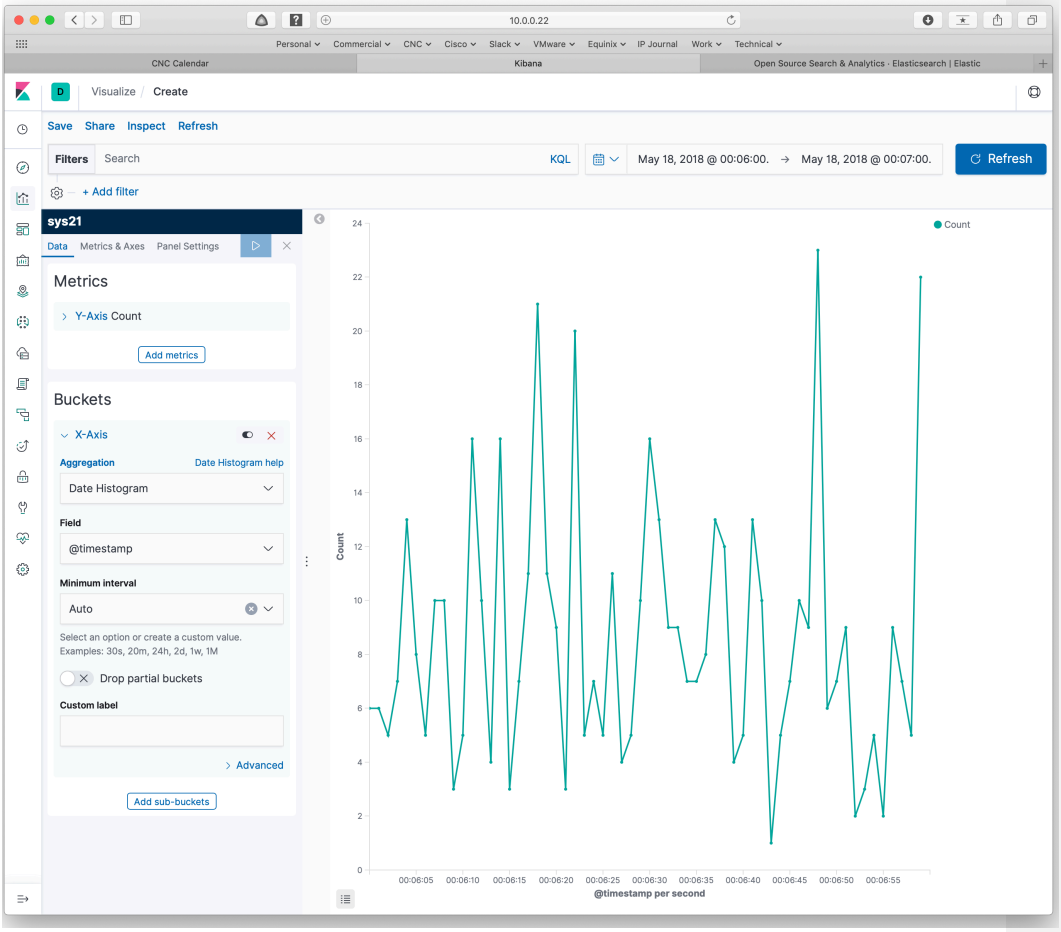


Picking one then brings up the new visualization screen we've seen before (blog #2 in the series).

Commented [PW4]: Insert link

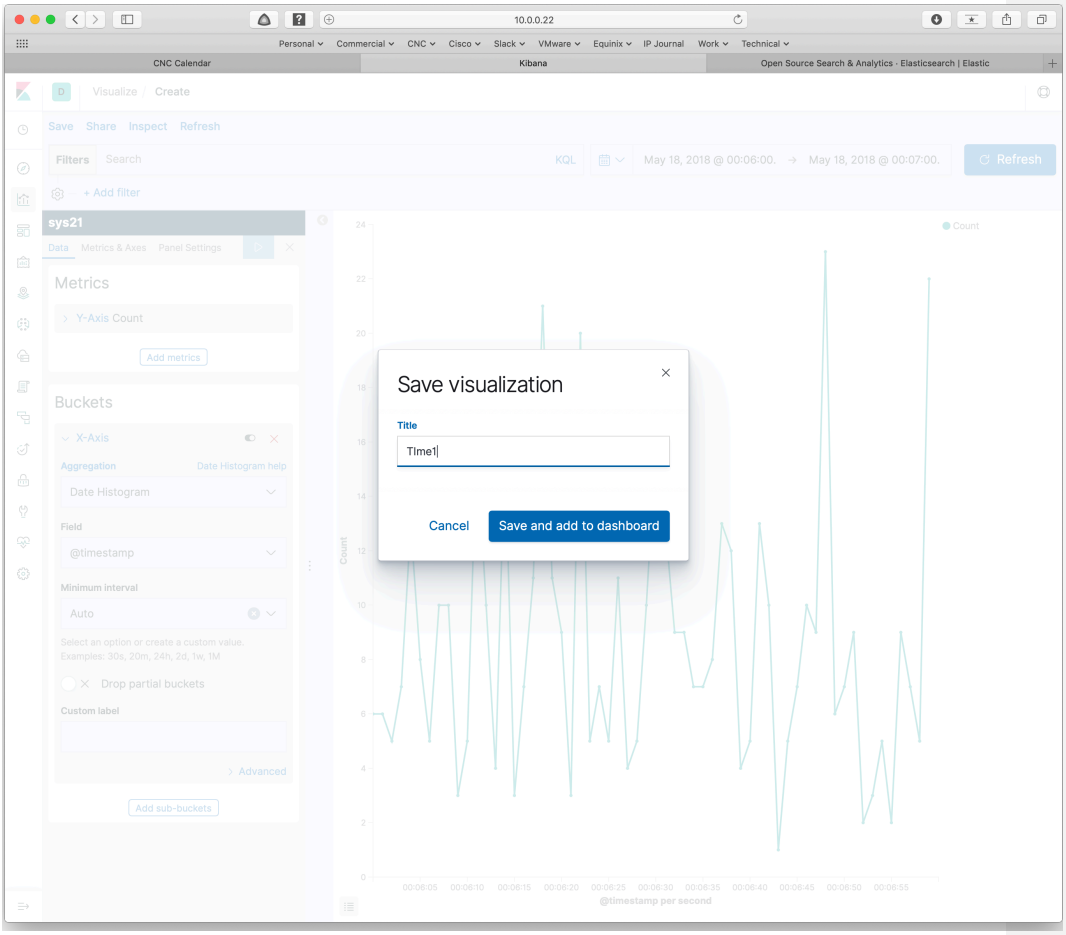
I filled in the form as shown below and clicked the blue right arrow button to accept the settings, producing the line graph shown at the right.

Copyright © 2018. All Rights Reserved.



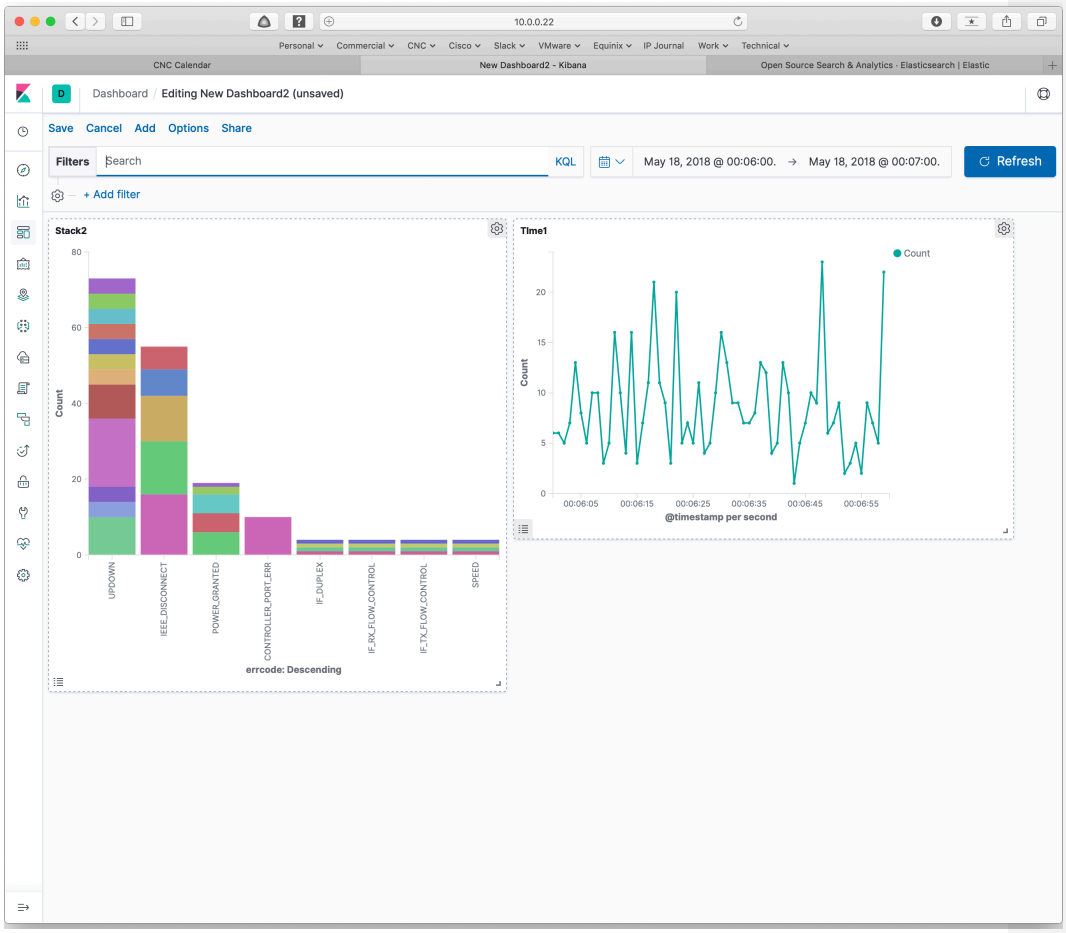
You then click on Save, to save the new visualization as part of the dashboard.

Copyright © 2018. All Rights Reserved.



Give it a name, then click the blue button to add to the dashboard.

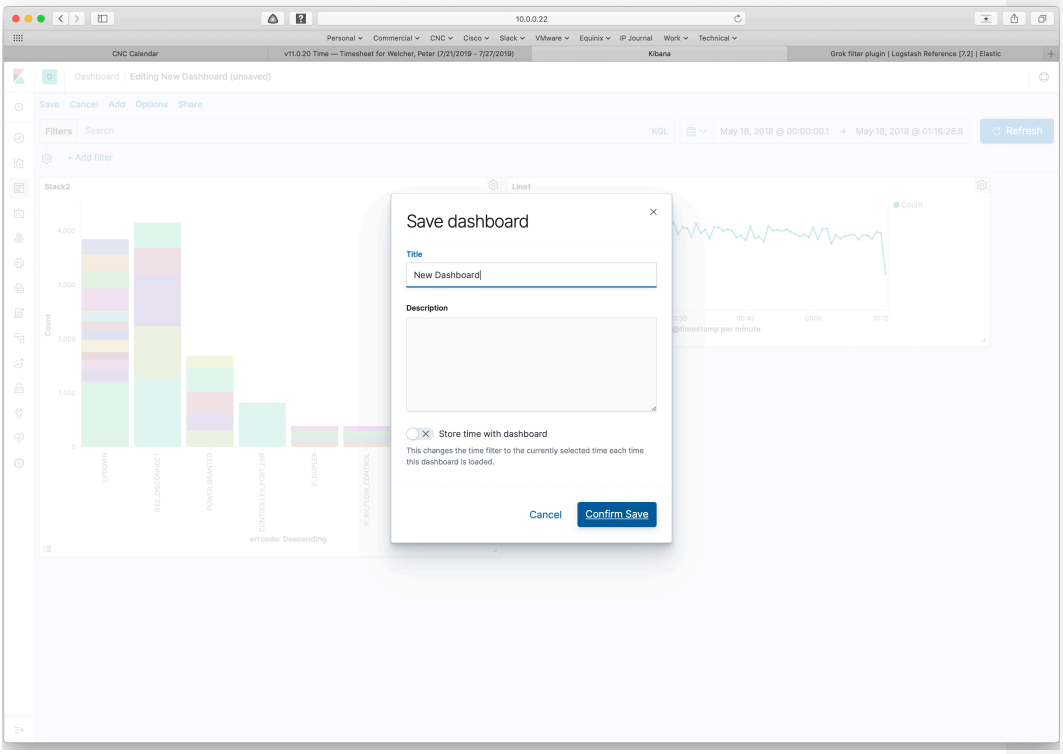
Copyright © 2018. All Rights Reserved.



SAVE THE DASHBOARD

Click Save (upper left menu) to save the entire dashboard. That brings up the following screen:

Copyright © 2018. All Rights Reserved.



Supply a name and click on Confirm Save. And that's it!

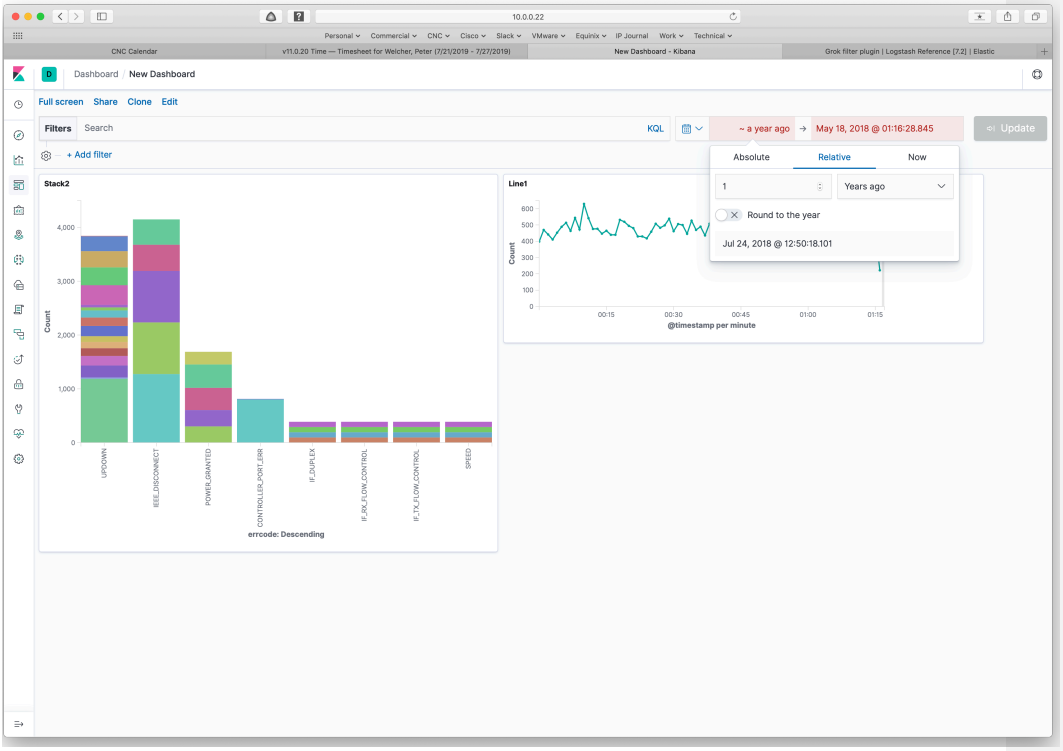
Making Changes

If you want to make changes, the top menu bar for a dashboard has an "Edit" item. Click on it to Edit!

Note that for a live (auto-updating) dashboard, one would probably want a relative time interval such as the last N minutes or such. This is set for the entire dashboard. That allows users to zoom in on a specific time period if they wish. Of course, if left on a time interval in the past, the dashboard will no longer be updating and showing you current state!

The following screen shows how to set up a relative time interval.

Copyright © 2018. All Rights Reserved.



In the above, also note the top menu items “clone” and “share”.

Conclusion

Working with Kibana dashboards is that simple!

Exercise for the reader: what would provide you with the most value in a dashboard? What KPIs would best tell you when there is a problem in your network? What are the highest priority applications at your site? How does the network relate to those?

References

See also the Part 1 and Part 2 blogs’ Reference sections.

- The documentation: https://www.elastic.co/guide/en/kibana/current/dashboard-getting-started.html
- Digital Ocean tutorial: https://www.digitalocean.com/community/tutorials/how-to-use-kibana-dashboards-and-visualizations

Copyright © 2018. All Rights Reserved.

The following links are from companies providing ELK or ELK-like services. In Part 1, I mentioned that ELKaaS and consulting / toolkits might be something to consider.

- Canned ELK objects and ELKaaS: https://logz.io/kibana-td/
- Managed monitoring plus AI aaS: https://www.sumologic.com/blog/elk-stack-vs-sumologic/ or https://www.sumologic.com/wp-content/uploads/elk-stack-vs-sumologic.pdf

COMMENTS

Comments are welcome, both in agreement or constructive disagreement about the above. I enjoy hearing from readers and carrying on deeper discussion via comments. Thanks in advance!

Hashtags: #CiscoChampion #TechFieldDay #TheNetCraftsmenWay

Twitter: @pjwelcher

Disclosure Statement

[INSERT the usual IMAGES HERE: 20 Year CCIE and Cisco Champions **2019** as per recent blogs]

NETCRAFTSMEN SERVICES

Did you know that NetCraftsmen does network /datacenter / security / collaboration design / design review? Or that we have deep UC&C experts on staff, including @ucguerilla? For more information, contact us at <<insert suitable link here>>.

SOCIAL MEDIA:

Facebook: Like, comment or share our status using this link.

Twitter: Like and RT our tweet using this link.

LinkedIn: Like, comment or share our status using this link.

Copyright © 2018. All Rights Reserved.