DRAFT BLOG POST

	Content
Post Title	Exploring an ELK Stack: Part 2: Kibana Visualizations
Post Date	
Attributed To	Peter Welcher
Written By	Peter Welcher
Reviewed By (Name & Date)	Dave Donati (11/4)
Reviewed By (Name & Date)	

Meta Title (55 characters including spaces)	Exploring an ELK Stack: Part 2: Kibana Visualizations
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.

COPY FOR POST:

This is Part 2 of a blog series tutorial about the ELK stack. The prior blog in the series is:

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

Commented [PW1]: Insert link to the prior blog

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!).

This second blog tutorial uses screen captures to cover some basic things you can do with the Kibana visualization tool (the "K" in "ELK). I don't claim deep ELK skills, but I'm

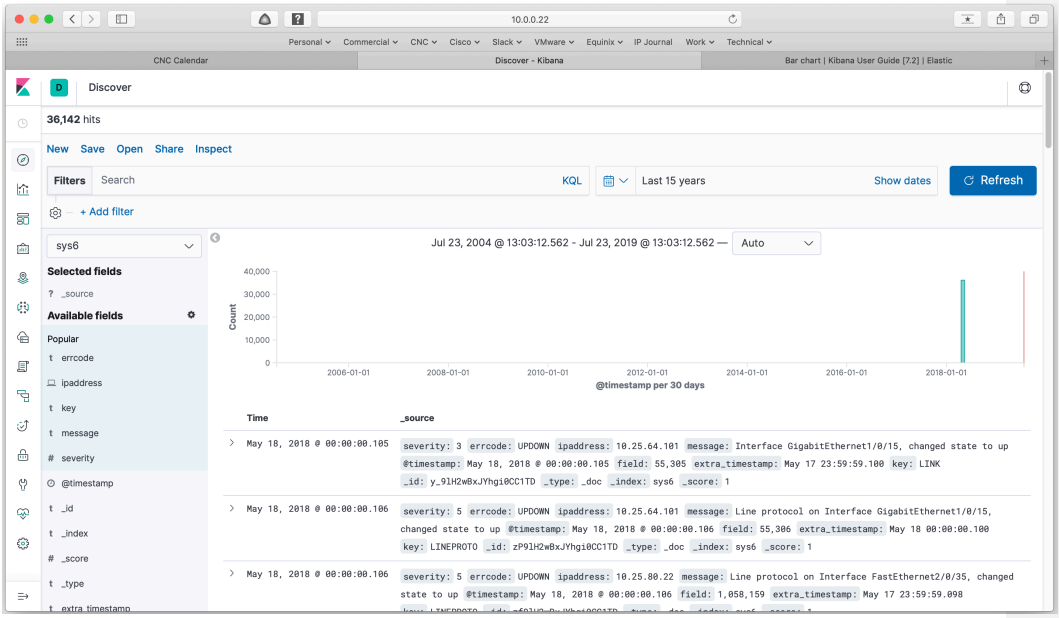
just trying to give some flavor of what you can do with an ELK stack, and help get you started exploring and learning!

Note: This is a long blog (article?), but most of that is screen captures. The rest of this series will be similar.

Recap of Part 1

More specifically, in Part 1 we got some syslog data loaded into Elasticsearch via Kibana, along with a pattern to understand ("grok") the data as fields.

Once that was done, you'll see something like the following screen capture. You can click on the top icon on the left side (the compass) to return to this "Discover" view.

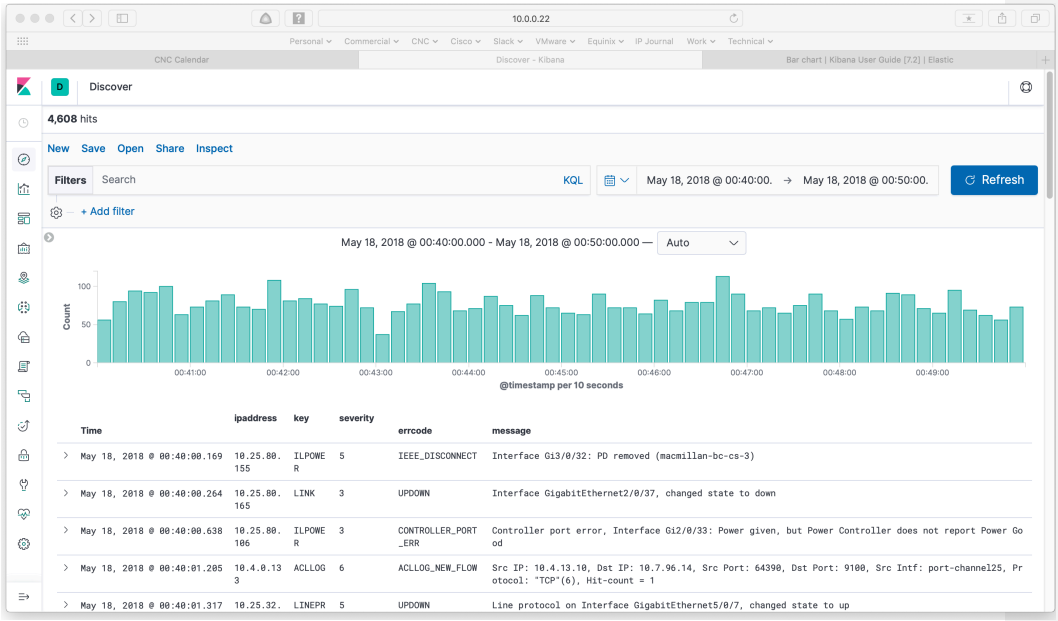


This shows the log data that's been loaded. The words with blue background are the field names the grok pattern assigned.

The top bar chart shows message count over time. This data is from a relatively short period of time.

Working with Log Data

Click repeatedly on the bar in the bar chart to drill down on time. That'll get you to something like the following.

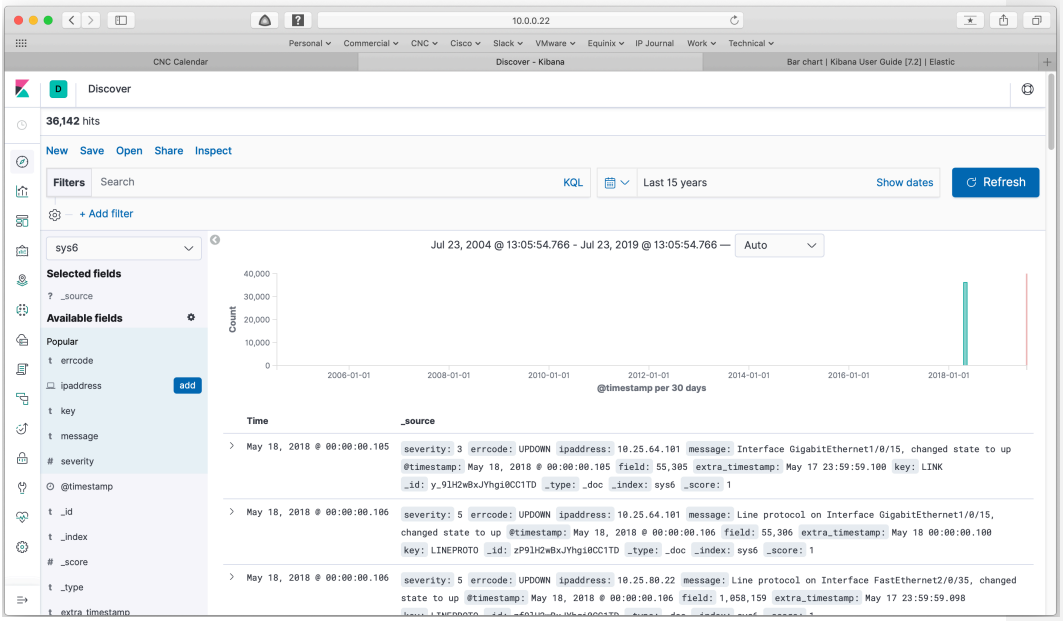


Note the time period range is shown at the top. You can specify the time range in various ways using that and then clicking on Refresh. I suggest exploring it, it's self-explanatory.

What you can also see in the above screen capture is that I adjust to show selected fields only.

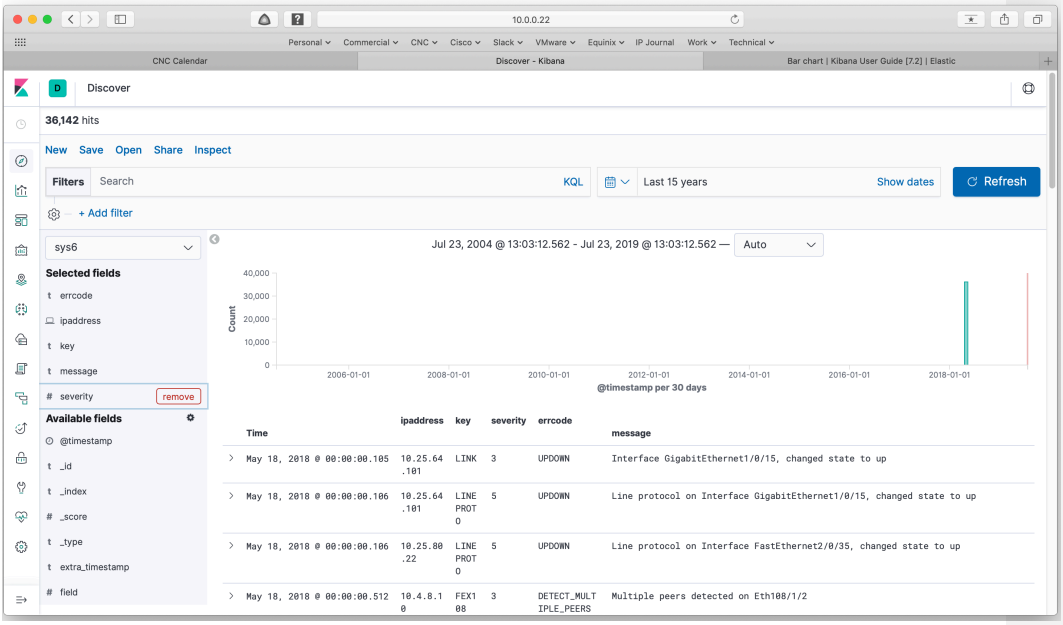
Here's how you do that. On the upper left, expand "Available Fields" if necessary. (Use the '>' icon below the configuration gear icon.) See also the next screen capture.

That lists the fields. Hover the cursor over one and an "Add" button shows up, as can be seen in the next screen capture.



Click add to select certain fields.

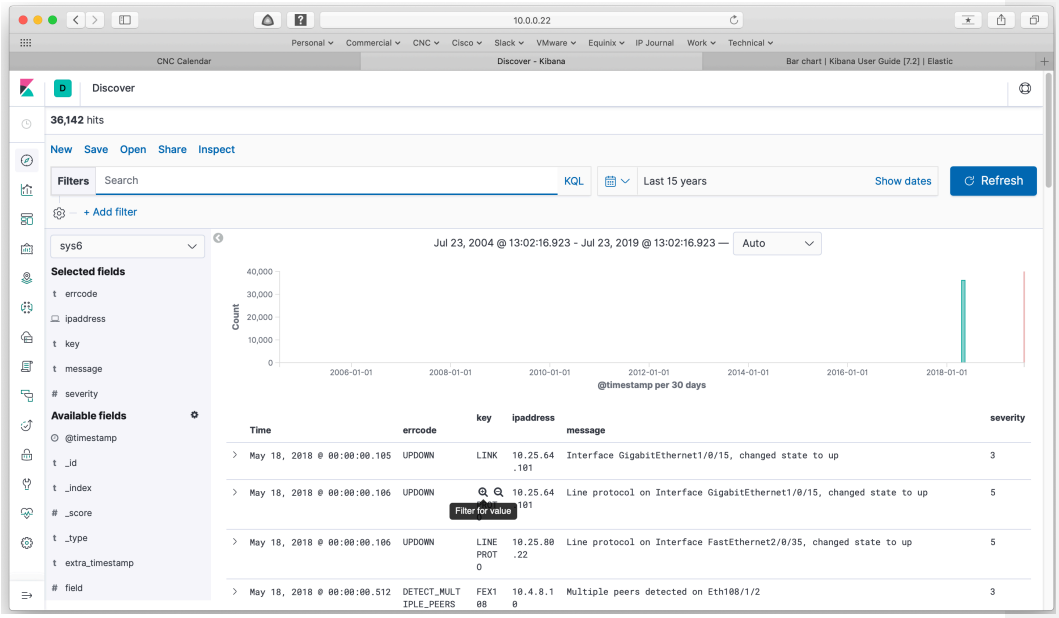
After adding five of them we get the following:



You can see the five I used on the left, under “Selected Fields”.

The timestamp is included *auto-magically*. They show on the right in the order chosen. If you don’t like that order, hover over the column headers and click on the very small left, right arrows (<<, >>) to shift the chosen column over.

If you hover over an entry, you’ll see tiny plus / minus (+, -) signs in circles. See the next screen capture.



Click + to filter on that item. Only lines matching that field will now be shown. This is a quick way to “drill down” and see how often a particular field occurs.

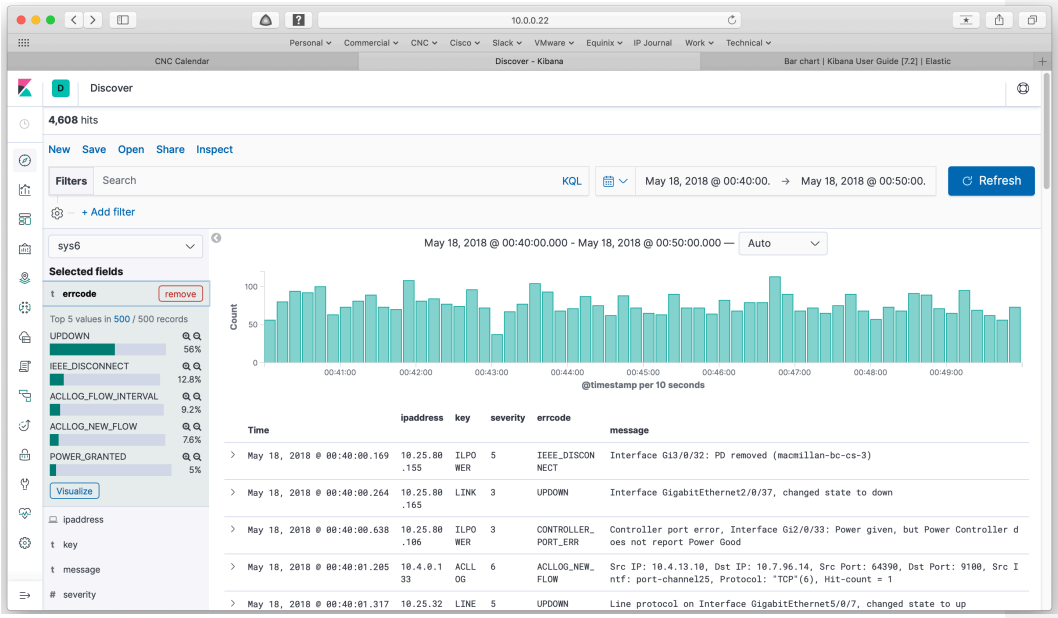
As a practical example based on the above, you might pick UPDOWN and then an IP address filter to see how many link bounces that device had.

Note that if I’d been smart enough to also add an interface filter for the “message” field, you could also filter on the interface. Ok, learning as we go here … This illustrates that your message filter may grok more deeply, and some experimentation may help you find what’s best. If you data lacks a consistent format, that won’t exactly help.

Resuming our tutorial… If you’re hovering over a field / column header, you can click on the little up (^) or down caret to sort on that field.

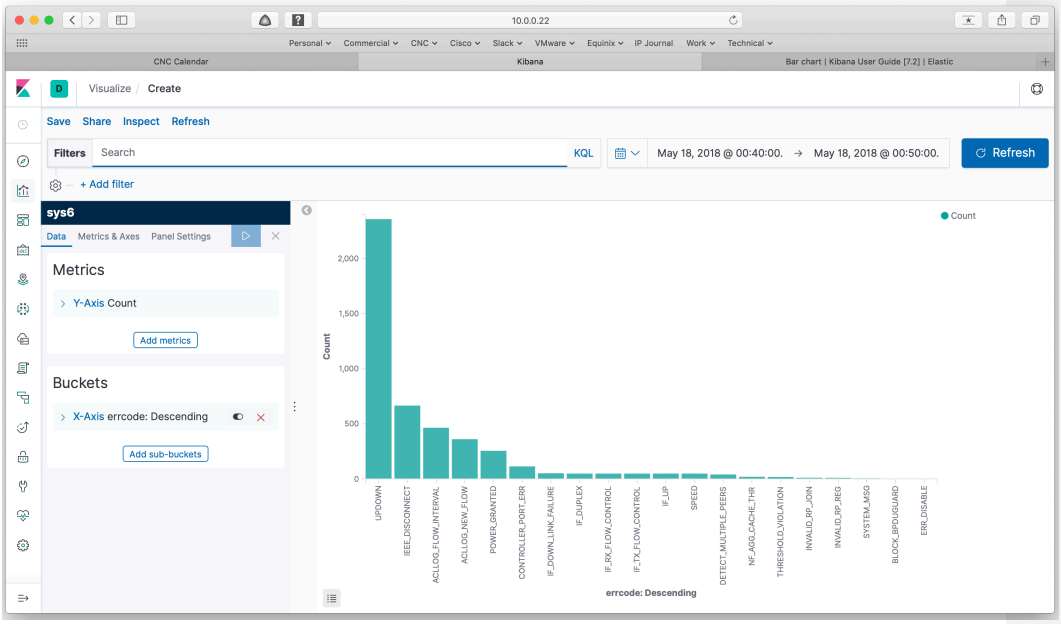
Quick Visualization

More usefully, if you click on the field name on the left, you’ll get a mini bar chart of the top five item counts for the field. The next screen capture shows this, after I clicked on “errcode”.



You can then click the Visualize button (in blue on the left, below the top 5 bar chart) to produce a full-sized bar chart of that item. This is one easy way into Kibana visualization. You can then mess around with the properties of the visualization to see what they do!

Here's what came up when I clicked on Visualize:



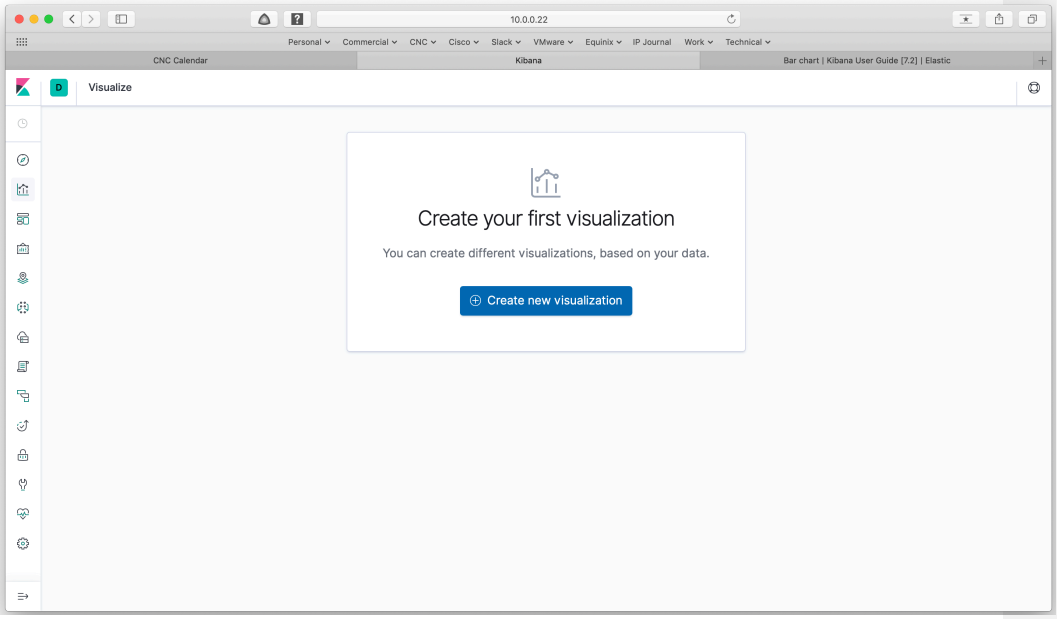
The items along the x-axis are “buckets”. From the controls on the left, you can change the number of items displayed, and other properties.

Notice what we just did: we got a histogram of how often the various Cisco syslog error types occurred. That’s arguably some quick value for our efforts!

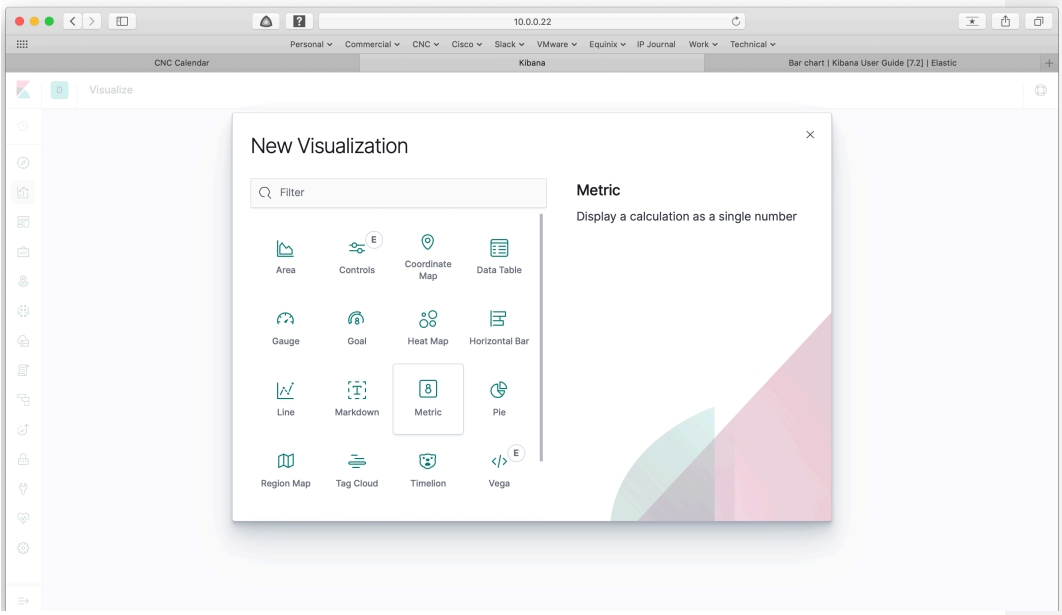
VISUALIZATION

You can also click on Visualize, the second icon on the left vertical strip. Hovering over one of those icons brings up a pop-up title for it.

When you click on Visualize, here’s what comes up:



Of course, you will click on the one button. You then get to choose what type of visualization you want to build.

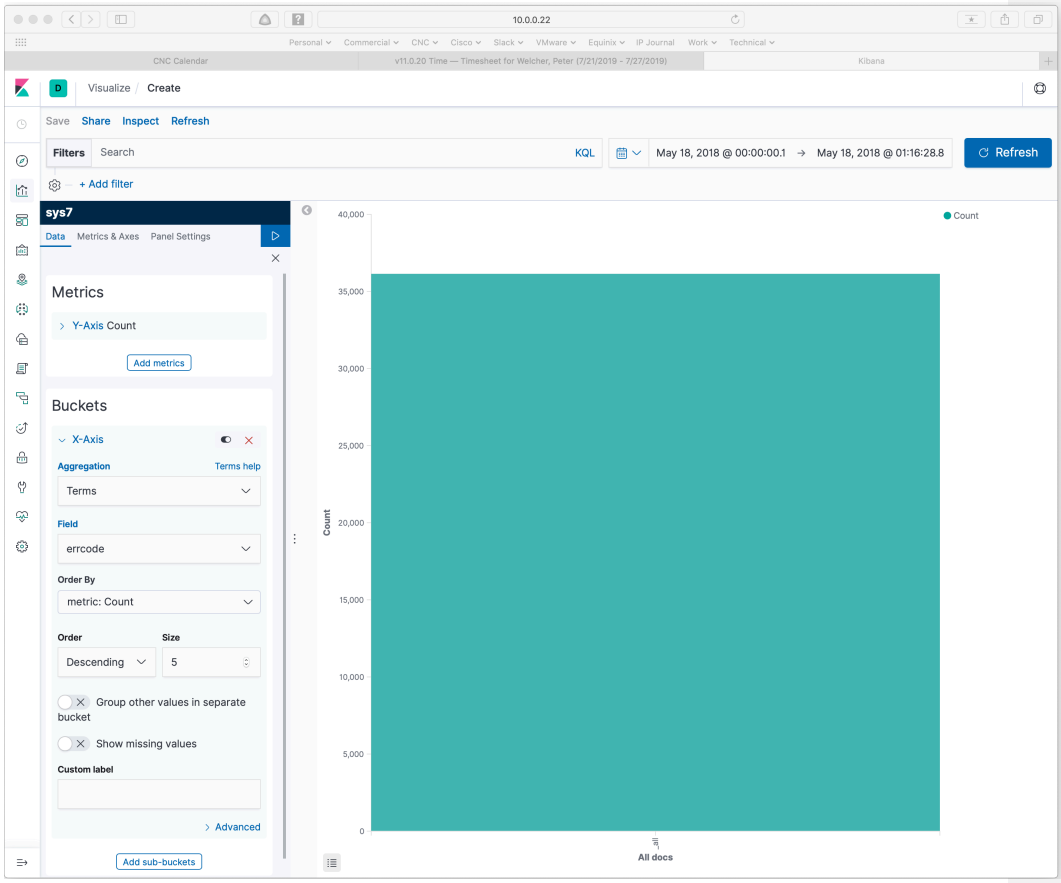


Scrolling vertically shows the remaining options:

This is where the documentation and some of the tutorials listed in the References section below may be useful. They'll give you some ideas of what is possible, and then you can slog through figuring out how to get there.

Next, you pick a type. I picked Vertical Bar.

The below screen capture shows what that brings up. Ok, that's a "mono-bar", not very interesting. But it's a start.

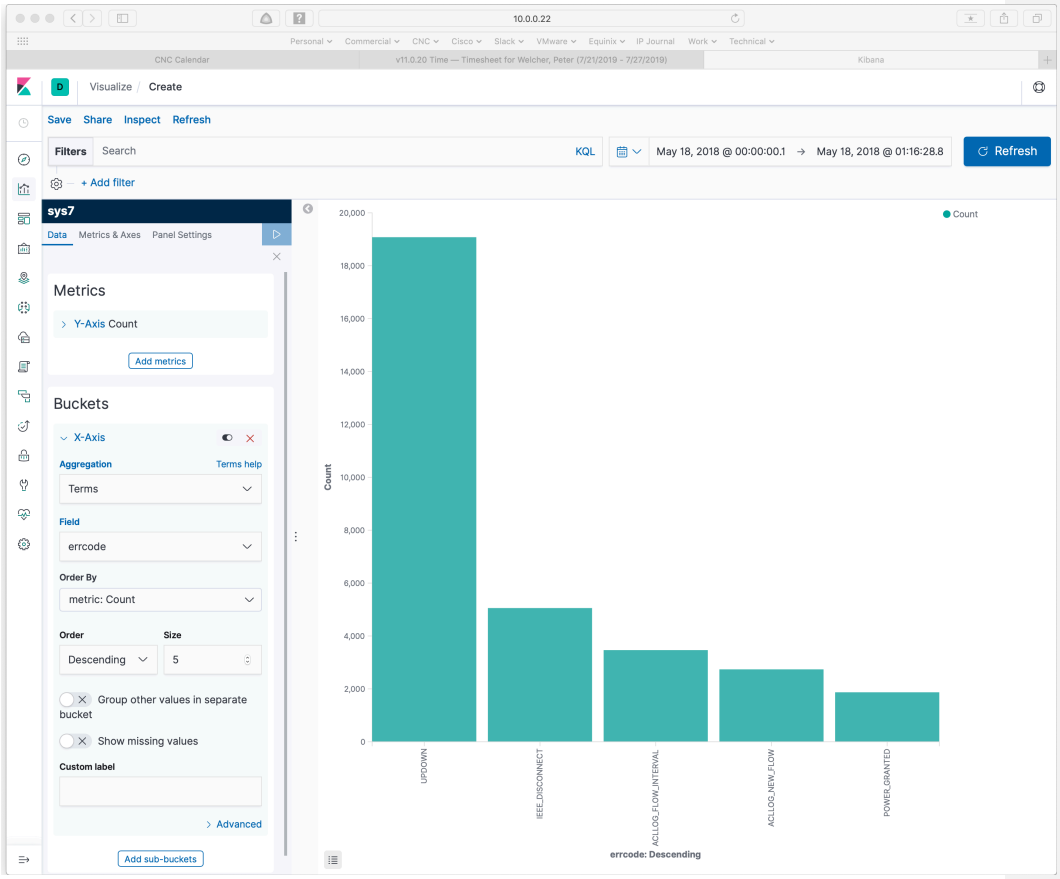


The above shows that since I brought up the mono-bar, I've opened up "Buckets" and changed the Aggregation to "Terms" and set the Field to "errcode" (in the form on the left).

To make that take effect, click on the blue right-facing triangle (up top, to the right of "Panel Settings", within the left panel).

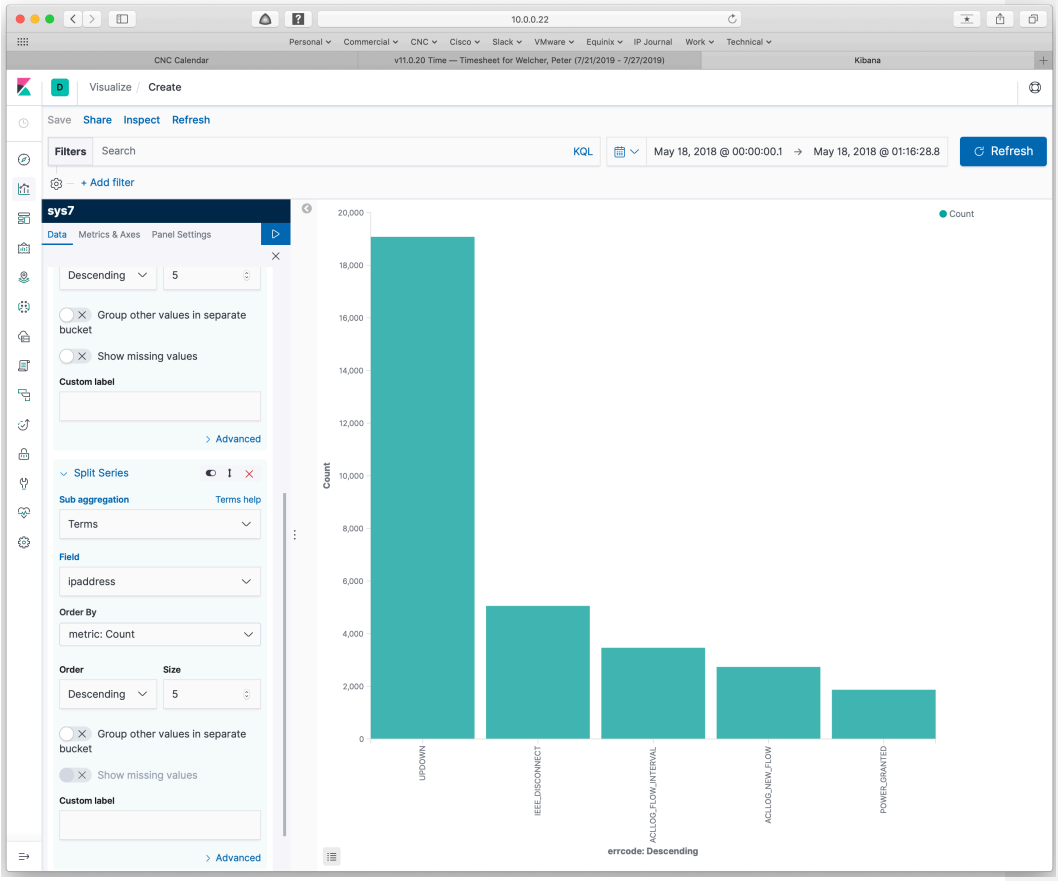
That brings up the following.

It's that easy to get a bar chart (etc.) on any one field. If you want more bars shown, edit the "Size" setting on the left.



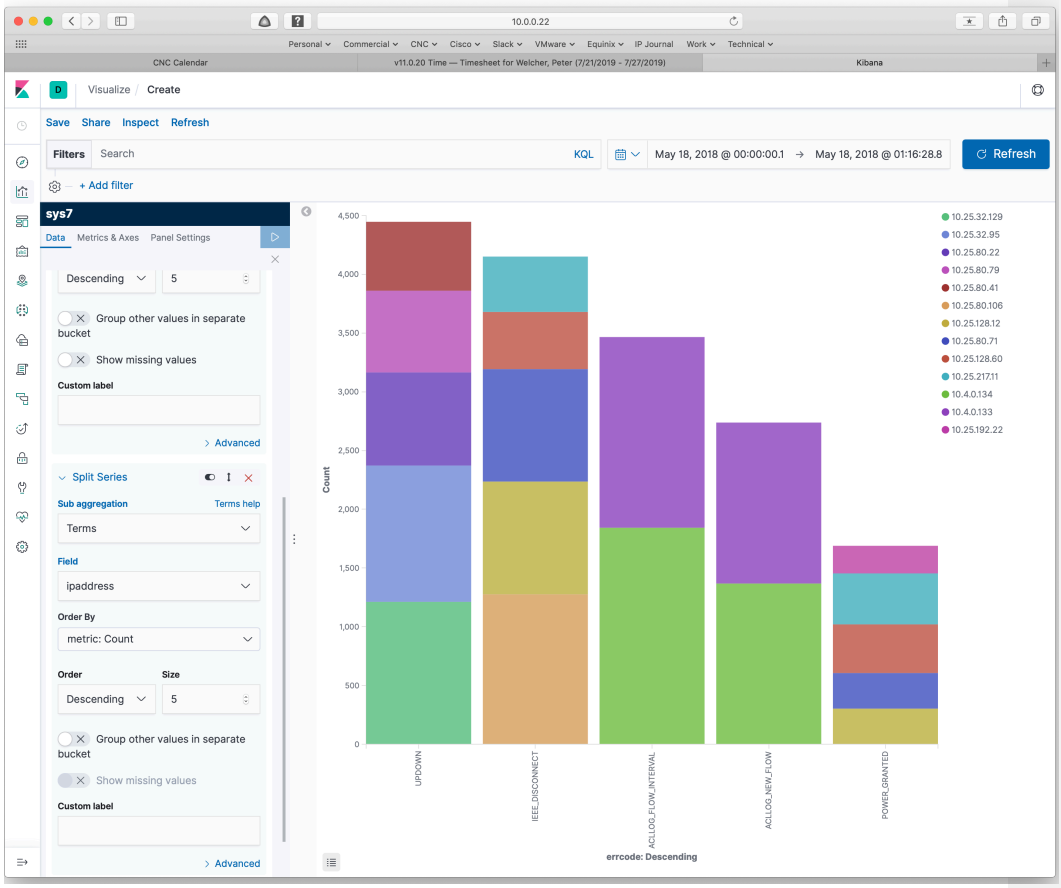
Let's get fancier, just to show something more complex. Click on "Add sub-buckets" at the bottom, and then click on Split Series.

Complete the form as shown in the bottom left of the following screen capture.



Specifically: set the Sub aggregation to “Terms” (unique field values), and Field to “ipaddress”. Then, as before, click the blue arrow to make those settings take effect and update the visualization.

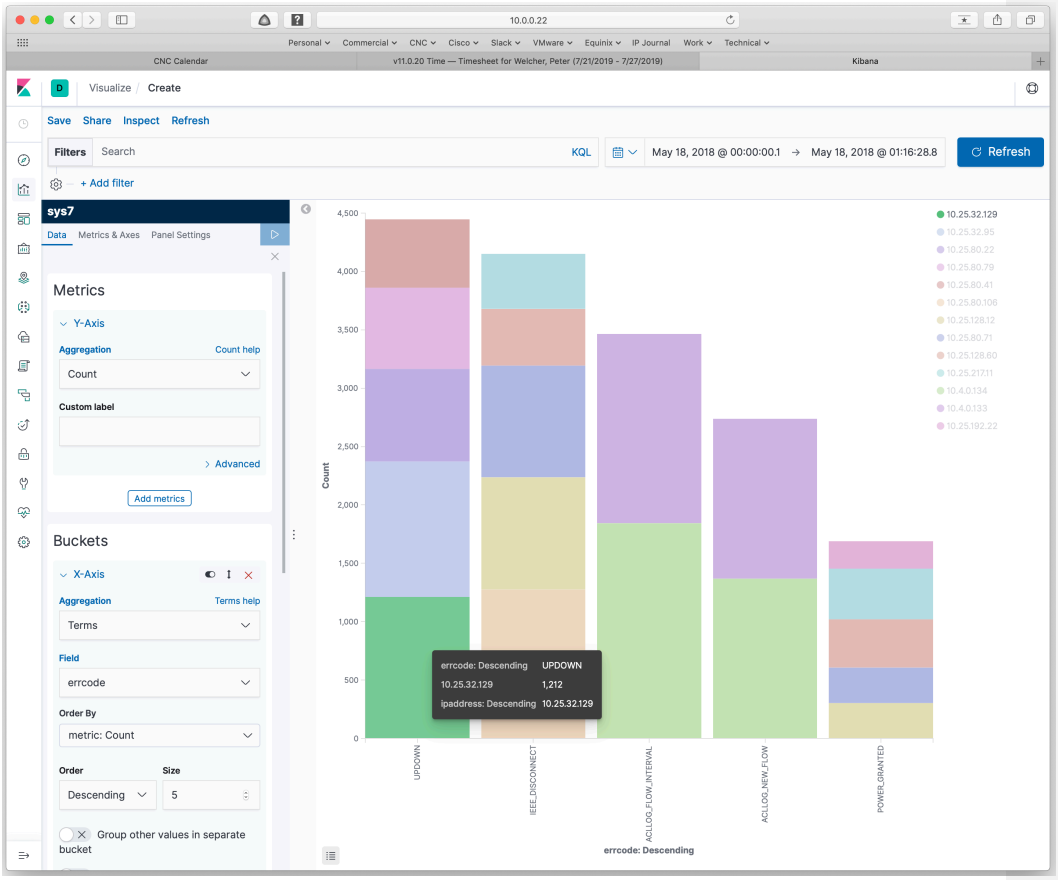
Here’s what comes up, a stacked bar chart:



This shows a bar for each unique syslog message code, in descending total count order. Within each bar, it shows the count of relevant messages per IP address.

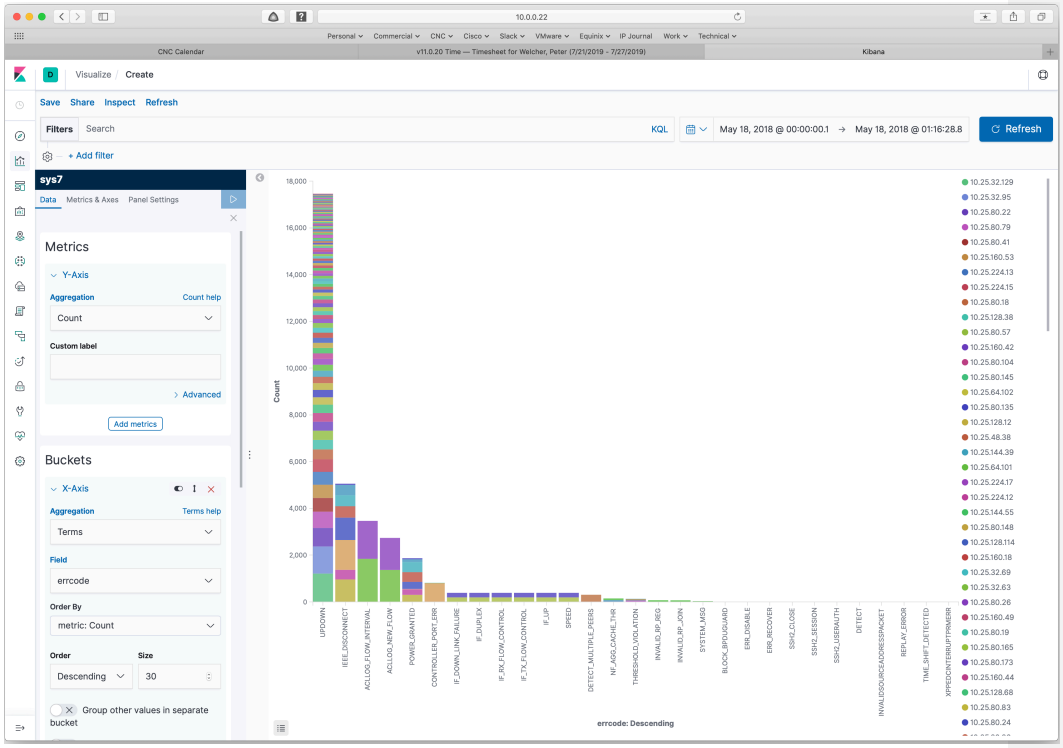
So, for instance, the IP addresses for the bottom two rectangles on the left have the highest UPDOWN bounced interface message counts.

The legend on the right is a bit hard to correlate with the colored rectangles, but if you hover the cursor, you get the necessary info, as shown below:



Note that the shown device above had 1212 interface bounces (well, 1212 divided by 2 if you figure they're up / down pairs) within a 1.25-hour period. I'd want to go fix that!

If you change the "Size" on the left (in two places) you can get this as a 15 x 30. Just to stress the system, I tried 30 x 100 and got the following:



This clearly hits the point of diminishing (visual and usefulness) returns. On the other hand, it gives you a quick way to see the top complaints and complainers in your syslog data, which was the point! By the way, even some of those near the top of the UPDOWN bar might be of interest: 40 events (20 bounces) in 1.25 hours!

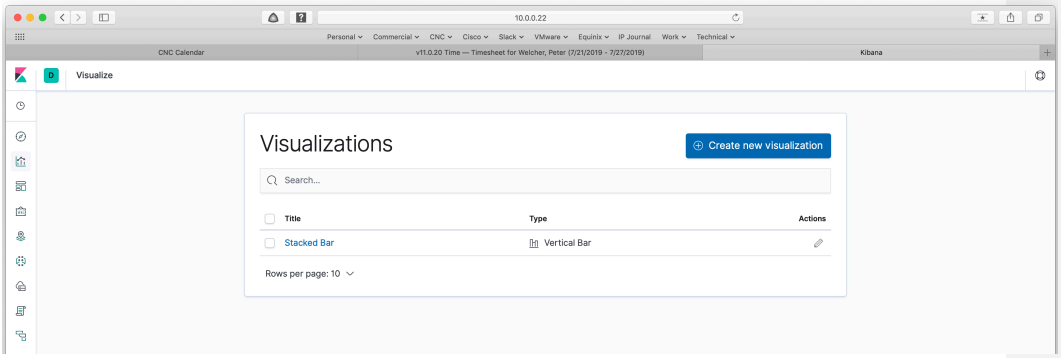
At this point, I'd suggest exploring the other settings tabs on the left, and in general.

If you were running on a VM with the ELK stack installed, or had a container with mounted permanent storage, you'd probably want to save this.

That's not hard to do: click Save in the upper left and provide a name.

Then you'll be able to go back and pull up the graph again. Changing the time window settings would update with more current data.

The below shows what I saw when I clicked on the Visualization icon again: a list of saved visualizations. You probably already guessed: to bring one up, click the link.



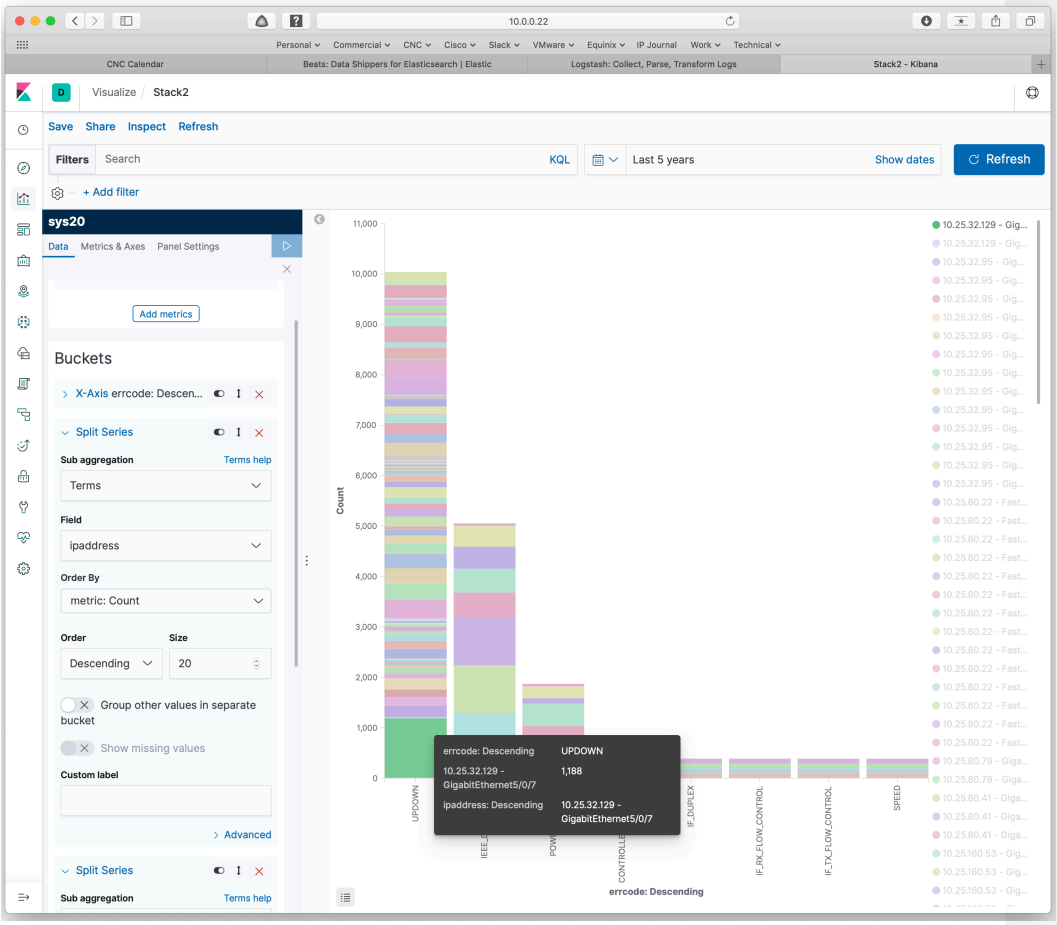
Adding Interfaces

As a late addition, I figured out a quick way to add interfaces to the database and chart. It used the pattern

```
%{TIMESTAMP_ISO8601:timestamp} %{IP:ipaddress} .*?%{INT:field}.*?
.*?%{SYSLOGTIMESTAMP:extra_timestamp}.*%{WORD:key}-(%{WORD:key2})?(-
)?%{INT:severity}-%{WORD:errcode}: (.*?Interface
%{NOTSPACE:interface}[:,] )?%{GREEDYDATA:message}
```

To be fully polished, I'd like to capture the interface as a separate field, plus the full message including the interface, but that'd take some more research / exploration (aka "more fun with patterns").

Using that to re-import the data, and then adding another split series based on the 'interface' field, and making sure we have fair-sized numbers in the sub-aggregation count fields, we can get a "very stacked" bar chart like the following:



That seems like it could be useful!

Choices

Part of the learning experience here is that pattern matching involves choices.

I chose to break out AAAA-5-FOO and AAAA-BBBB-6-BAR into component pieces, which allows counts and graphing of Cisco syslog messages by severity level, grouping, etc.

Not breaking the syslog message code into components also has some advantages, one being that the severity level will show up in the labels at the bottom of the above

bar chart. And note that you can still filter on the -5- pattern if you want to work with / report on specific severity levels.

I explored this further and found https://stackoverflow.com/questions/38606766/how-to-combine-characters-to-create-custom-pattern-in-grok.

The key point is that (?<fieldname>patterns) lets you group patterns and put a field name on the matching data, but you can also embed other field names in the patterns.

Revising the pattern to the following lets us capture both full syslog codes and the components, and the same for interface name and full error message body (which may or may not contain the interface name).

```
%{TIMESTAMP_ISO8601:timestamp} %{IP:ipaddress} .*?%{INT:field}.*?
.*?%{SYSLOGTIMESTAMP:extra_timestamp}.*(?<fullerrcode>%{WORD:key}-
(%{WORD:key2})?(-)?%{INT:severity}-%{WORD:errcode}):
(?<fullmessage>(.*?Interface %{NOTSPACE:interface}[:,] )?%{GREEDYDATA})
```

I'm favorably impressed that this actually took relatively little time to figure out.

I'd have to say, adjusting the regular expressions in Kibana import is a lot simpler and faster than tweaking the PERL script I've been using for syslog reporting. The big difference is that I can quickly edit the pattern in a text editor, paste it in, and keep iterating on the pattern attempt before doing the import to Kibana.

I didn't go back and use this pattern to rewrite this blog, because (a) time, and (b) simpler patterns are probably a better idea when getting started with this.

Conclusion

The above shows how to bring up one kind of visualization in Kibana on our ELK stack. I hope this will prove useful to you!

I do need to note that the above patterns may need some tuning for your syslog format. Over the years, my experience has been that no two sites end up with the same syslog formatting in log files.

Another graphing tool in common use is Grafana. That's something I'd like to explore at another time. I've included a comparison blog in the References section below. There's a reason I wanted to explore Kibana more, which will (I hope) become visible in another blog soon.

References

See also the Part 1 References, which I have elected to not repeat below.

- Documentation about Kibana Visualization: https://www.elastic.co/guide/en/kibana/current/visualize.html
- Logz.io blog comparing Kibana to Grafana (features and use cases): https://logz.io/blog/grafana-vs-kibana/
- Logz.io blog: Kibana Tutorial Part 2: Creating Visualizations: https://logz.io/blog/kibana-tutorial-2/
- Also possibly useful: Logz.io blog about Kibana hacks: https://logz.io/blog/kibana-hacks/
- Logz.io blog: Creating the Perfect Kibana Dashboard: https://logz.io/blog/perfect-kibana-dashboard/
- Digital Ocean: How to Use Kibana Dashboards and Visualizations: https://www.digitalocean.com/community/tutorials/how-to-use-kibana-dashboards-and-visualizations (based on the older version 4 of Kibana, animation how-to demos)

Google or another search engine will also lead you to more resources, including courses and canned visualizations others have developed.

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.