# Splunk Dashboard Challenge

Helpful links:

1. Dashboard quick reference

<https://www.splunk.com/pdfs/solution-guides/splunk-dashboards-quick-reference-guide.pdf>

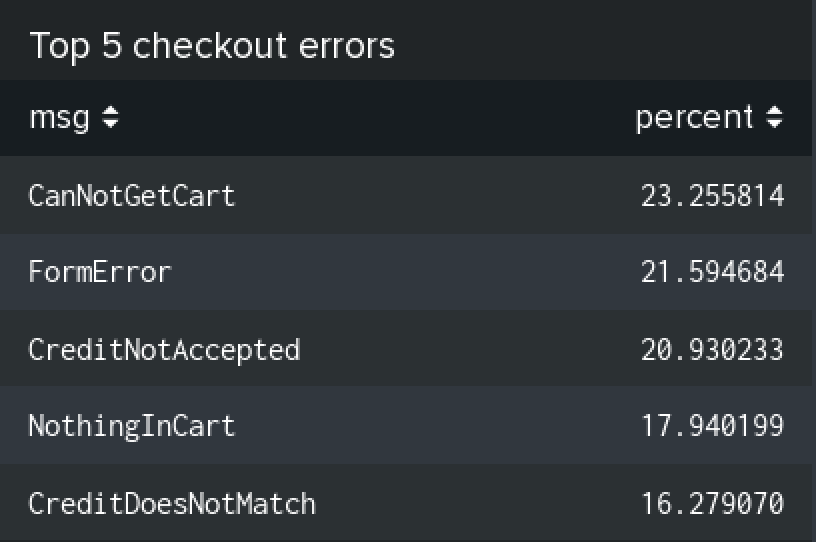
2. Dashboard XML docs

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Viz/PanelreferenceforSimplifiedXML>

3. Configuration options for Charts

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Viz/ChartConfigurationReference>

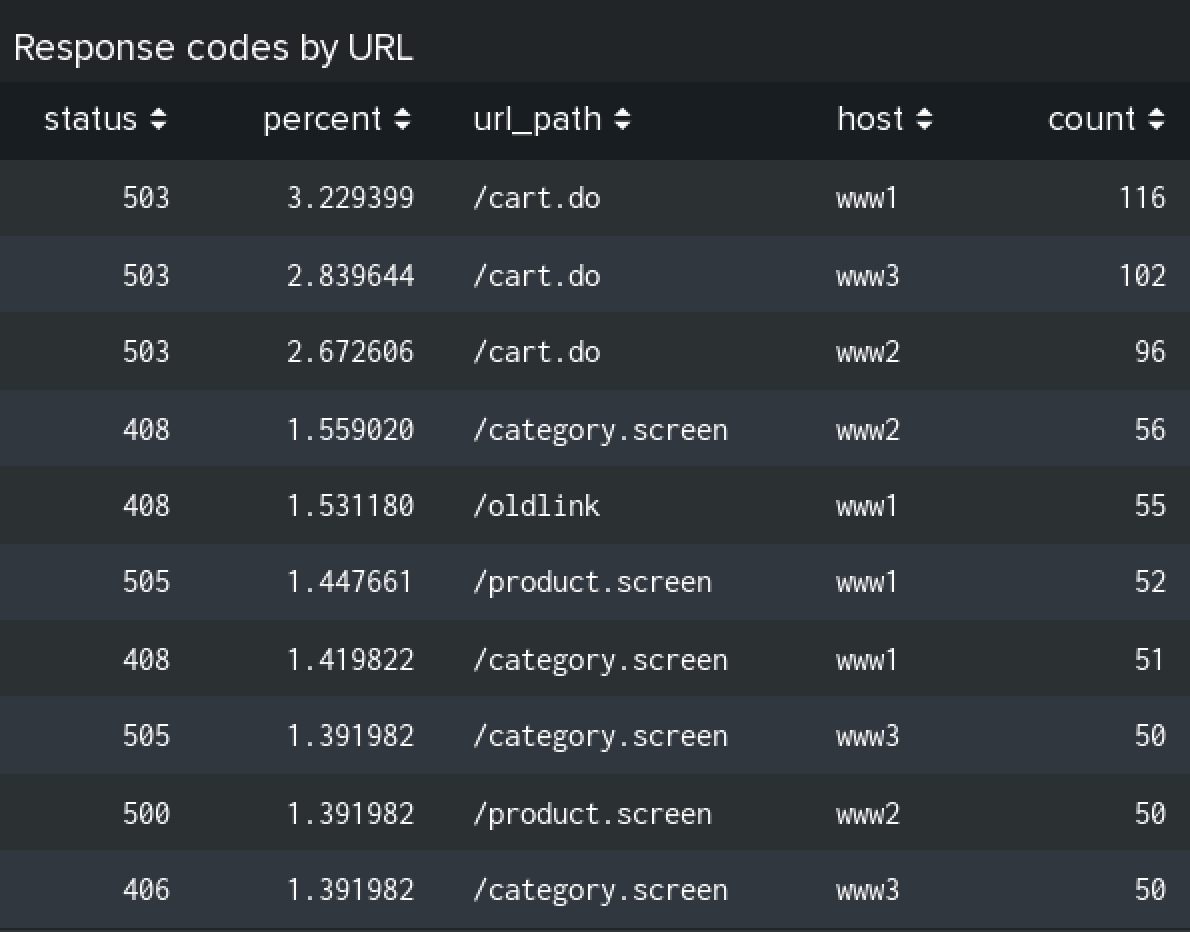
### 1. Top 5 checkout errors by frequency table



### 2. Response codes by URL table

The hard part to this table is grabbing only the important part of the URL. We don't want any query parameters on the url that usually appear after a ? in the URL.

**cart.do**~~?action=purchase&itemId=EST-15&JSESSIONID=SD9SL7FF3ADFF53096~~

~~~~

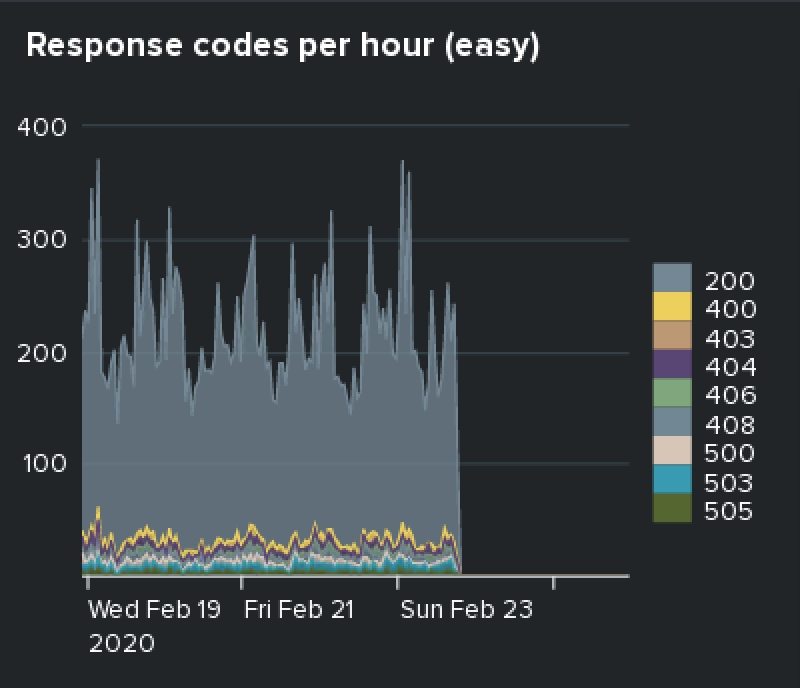
You could improve on the formatting here a bit by rounding the percentage and renaming some column headers.



### 3. Response codes by hour line chart

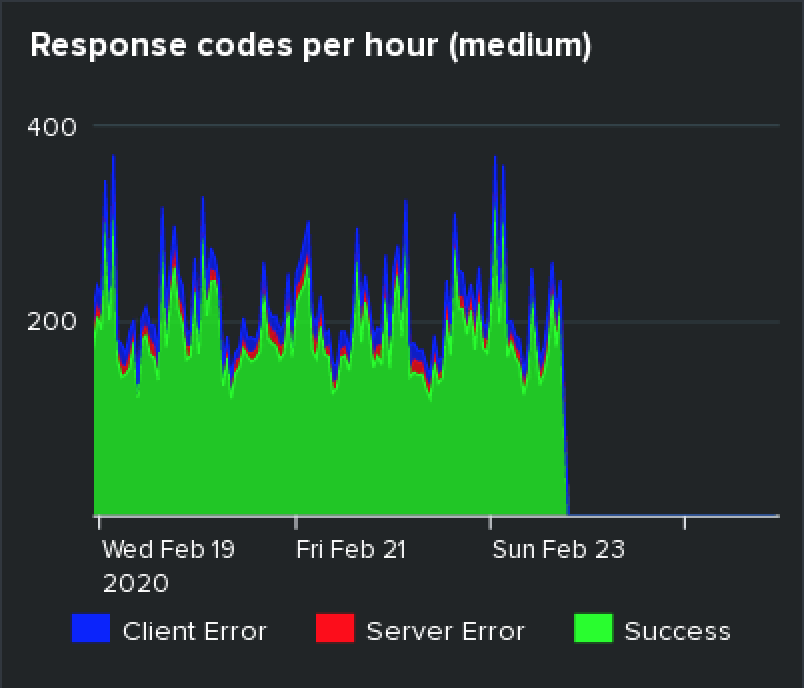
We would like a stacked line graph that allows us to see trends in the number of total requests as well as trends based on the response status code of the requests.

Easy:



Medium:

It would be better if we didn't have soo many different lines to look at. What we really want to know at a glance is how many successes vs server errors vs user errors are occuring. This means we need to merge some series together like below. All status codes in the 200s are success, 400s are user error, and 500s are server error. In addition, we want Successes to be green, user errors to be blue, and server errors to be red.



Hard:

Add a drill down that when you click on a series, it goes to the matching events for that hour. If you click a datapoint on the "Server Error" series, you should only see events with status codes > 500.

