Creating Custom Kibana Data Visualizations Using Vega

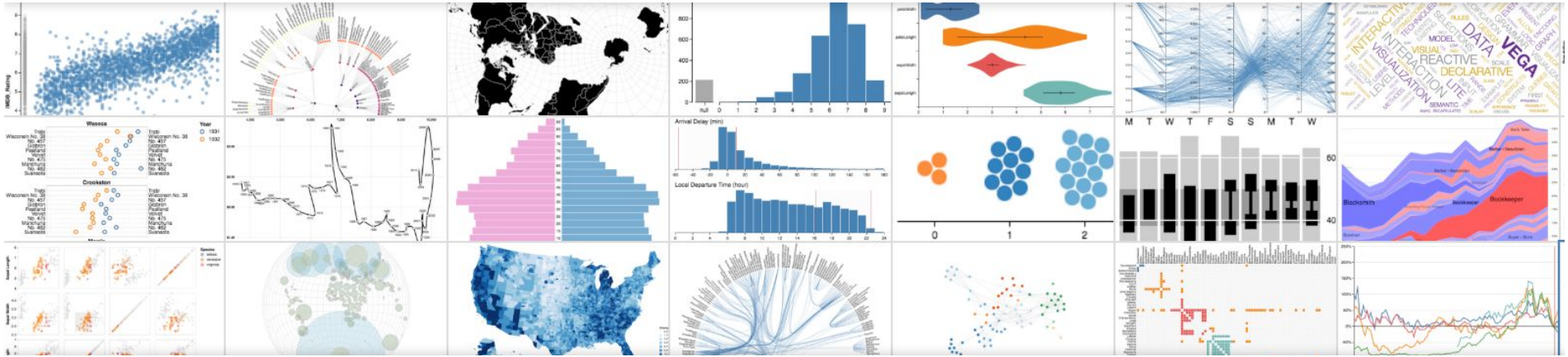
https://github.com/nyurik/kibana-vega-vis

By Yuri Astrakhan @nyuriks

What is Vega?

http://vega.github.io/

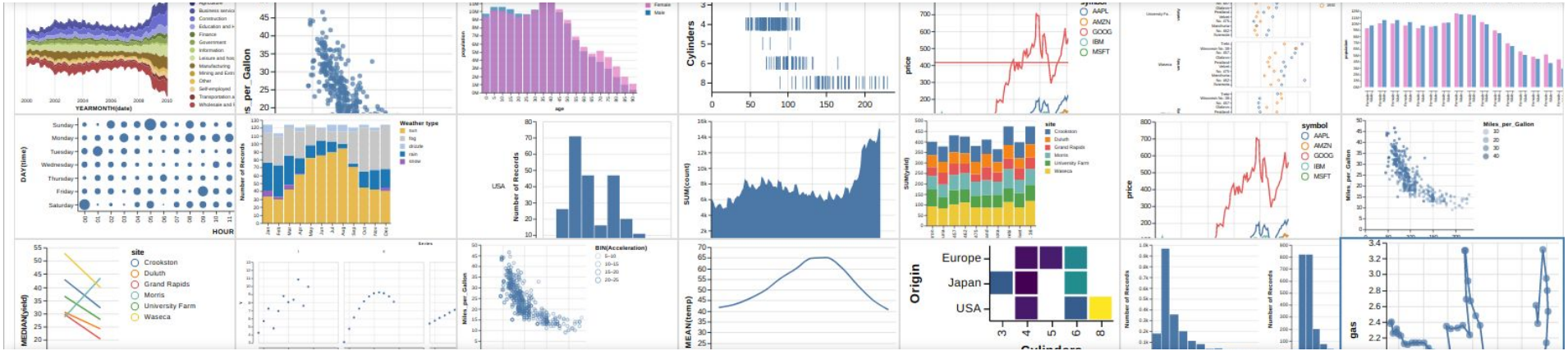
- Vega is a declarative format to make data visualizations
- Visualizations are described in JSON
- Generate interactive views using D3



What is Vega-Lite?

https://vega.github.io/vega-lite/

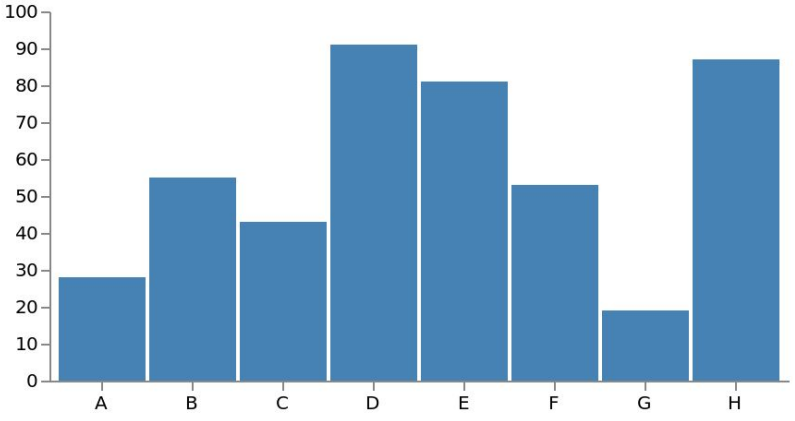
- Higher-level grammar than Vega
- Also in JSON, and shares some Vega concepts
- Allows more rapid data analysis
- “Compiles” into Vega



Benefits

- Custom graphs for power users
- No JavaScript
- Multiple data sources in one graph
- Use any ES and non-ES data sources
- Show data together with a tile-based zoomable map (plugin only)
- Allows community to share custom visualizations

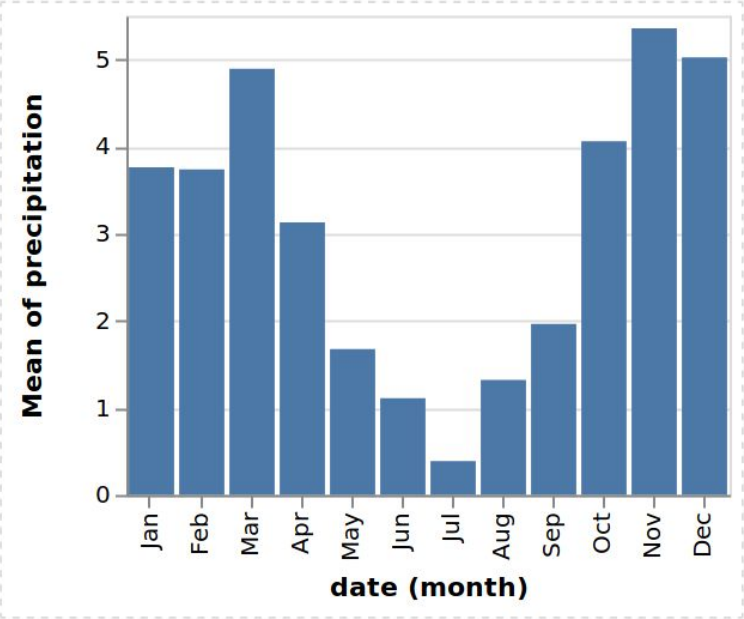
Vega




```
{
  "$schema": "https://vega.github.io/schema/vega/v3.0.json",
  "data": [
    {
      "name": "table",
      "values": [
        {"category": "A", "amount": 28}, {"category": "B", "amount": 55},
        {"category": "C", "amount": 43}, {"category": "D", "amount": 91},
        {"category": "E", "amount": 81}, {"category": "F", "amount": 53},
        {"category": "G", "amount": 19}, {"category": "H", "amount": 87}
      ]
    }
  ],
  "scales": [
    {
      "name": "xscale",
      "type": "band",
      "domain": {"data": "table", "field": "category"},
      "range": "width",
      "padding": 0.05,
      "round": true
    },
    {
      "name": "yscale",
      "domain": {"data": "table", "field": "amount"},
      "nice": true,
      "range": "height"
    }
  ],
  "axes": [
    {"orient": "bottom", "scale": "xscale"},
    {"orient": "left", "scale": "yscale"}
  ],
  "marks": [
    {
      "type": "rect",
      "from": {"data": "table"},
      "encode": {
        "enter": {
          "x": {"scale": "xscale", "field": "category"},
          "width": {"scale": "xscale", "band": 1},
          "y": {"scale": "yscale", "field": "amount"},
          "y2": {"scale": "yscale", "value": 0}
        },
        "update": {"fill": {"value": "steelblue"}},
        "hover": {"fill": {"value": "red"}}
      }
    }
  ]
}
```

Vega-Lite

```
date,precipitation,temp_max,temp_min,wind,weather
2012/01/01,0.0,12.8,5.0,4.7,drizzle
2012/01/02,10.9,10.6,2.8,4.5,rain
2012/01/03,0.8,11.7,7.2,2.3,rain
2012/01/04,20.3,12.2,5.6,4.7,rain
...
```

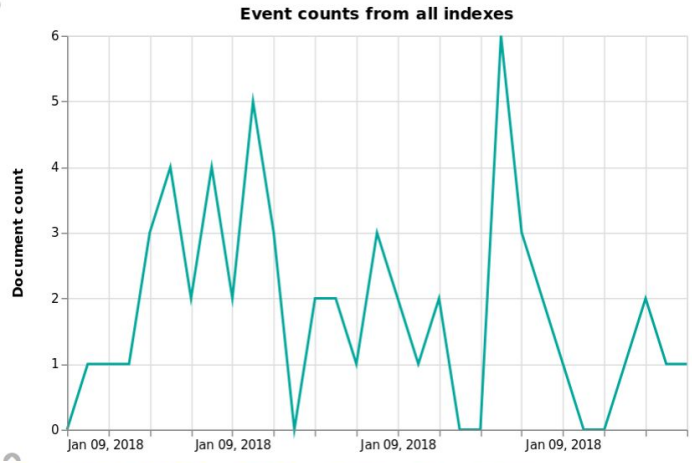



```
{
  "data": {"url": "https://.../seattle-weather.csv"},
  "mark": "bar",
  "encoding": {
    "x": {
      "timeUnit": "month",
      "field": "date",
      "type": "ordinal"
    },
    "y": {
      "aggregate": "mean",
      "field": "precipitation",
      "type": "quantitative"
    }
  }
}
```

Yes, but Elasticsearch?!

```
"index": "_all",
"body": {
  "aggs": {
    "time_buckets": {
      "date_histogram": {
        "field": "@timestamp",
        "interval": {"%autointerval%": true},
        "extended_bounds": {"min": {"%timefilter%": "min"}, "max": {"%timefilter%": "max"}},
        "min_doc_count": 0
      }
    }
  },
  "size": 0
```

```
{
  "$schema": "https://vega.github.io/schema/vega-lite/v2.json",
  "title": "Event counts from all indexes",
  "data": {
    "url": {
      "%context%": true,
      "%timefield%": "@timestamp",
      "index": "_all",
      "body": {
        "aggs": {
          "time_buckets": {
            "date_histogram": {
              "field": "@timestamp",
              "interval": {"%autointerval%": true},
              "extended_bounds": {"min": {"%timefilter%": "min"}, "max": {"%timefilter%": "max"}},
              "min_doc_count": 0
            }
          }
        },
        "size": 0
      }
    },
    "format": {"property": "aggregations.time_buckets.buckets"}
  },
  "mark": "line",
  "encoding": {
    "x": {"field": "key", "type": "temporal", "axis": {"title": false}},
    "y": {"field": "doc_count", "type": "quantitative", "axis": {"title": "Document count"}}
  }
}
```



And Maps...