.conf2015

Visualizing Data from the Ground Up: Raw Data to Interactive Graphics with Splunk

Marshall Agnew

Software Developer at Splunk

splunk>

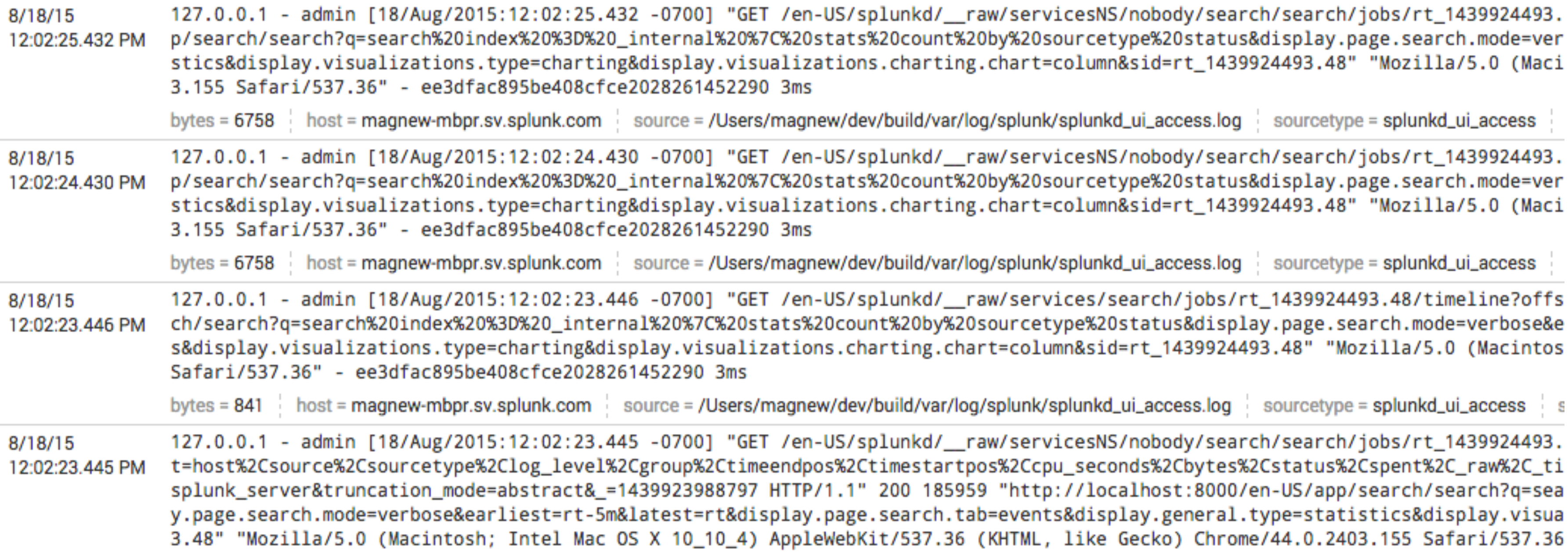
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Why Visualization Matters

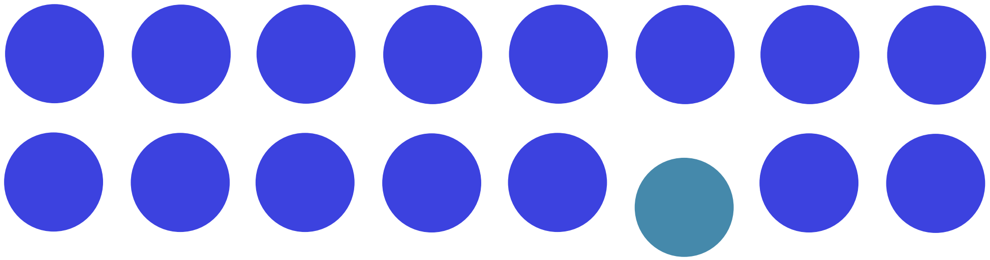
Splunk excels at understanding machine data



```
8/18/15           127.0.0.1 - admin [18/Aug/2015:12:02:25.432 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493.
12:02:25.432 PM   p/search/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=ver
                  stics&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Maci
                  3.155 Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms
                  bytes = 6758 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access |

8/18/15           127.0.0.1 - admin [18/Aug/2015:12:02:24.430 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493.
12:02:24.430 PM   p/search/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=ver
                  stics&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Maci
                  3.155 Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms
                  bytes = 6758 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access |

8/18/15           127.0.0.1 - admin [18/Aug/2015:12:02:23.446 -0700] "GET /en-US/splunkd/__raw/services/search/jobs/rt_1439924493.48/timeline?offs
12:02:23.446 PM   ch/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=verbose&e
                  s&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Macintos
                  Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms
                  bytes = 841 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access | s

8/18/15           127.0.0.1 - admin [18/Aug/2015:12:02:23.445 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493.
12:02:23.445 PM   t=host%2Csource%2Csourcetype%2Clog_level%2Cgroup%2Ctimeendpos%2Ctimestartpos%2Ccpu_seconds%2Cbytes%2Cstatus%2Cspent%2C_raw%2C_ti
                  splunk_server&truncation_mode=abstract&_=1439923988797 HTTP/1.1" 200 185959 "http://localhost:8000/en-US/app/search/search?q=sea
                  y.page.search.mode=verbose&earliest=rt-5m&latest=rt&display.page.search.tab=events&display.general.type=statistics&display.visua
                  3.48" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.155 Safari/537.36
```

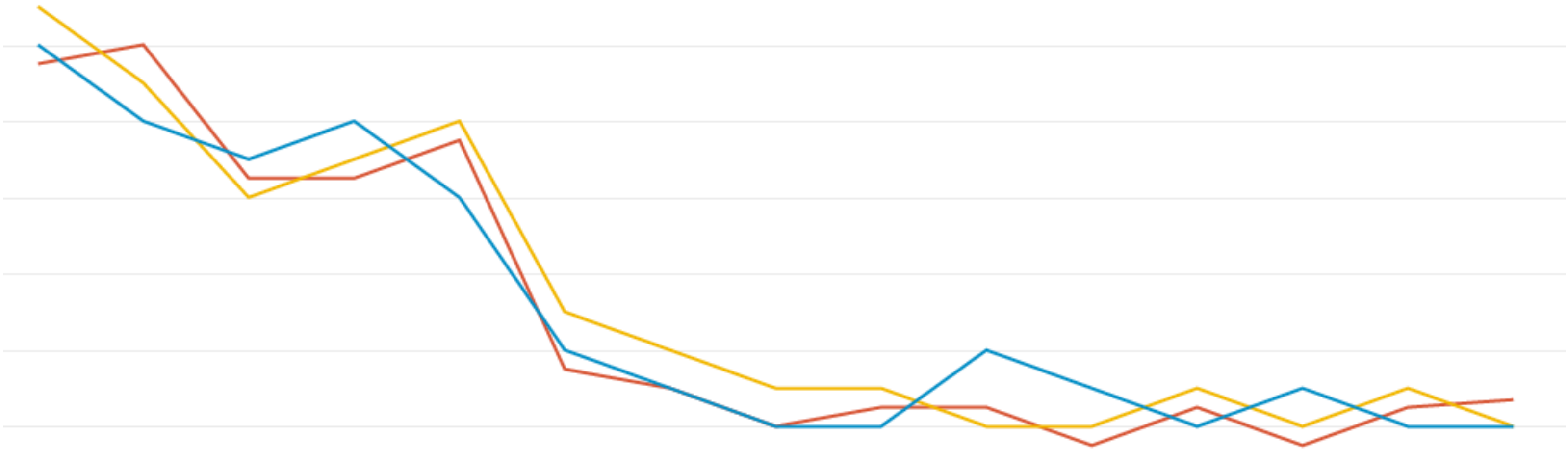
Why Visualization Matters

Humans are excellent at seeing visual patterns



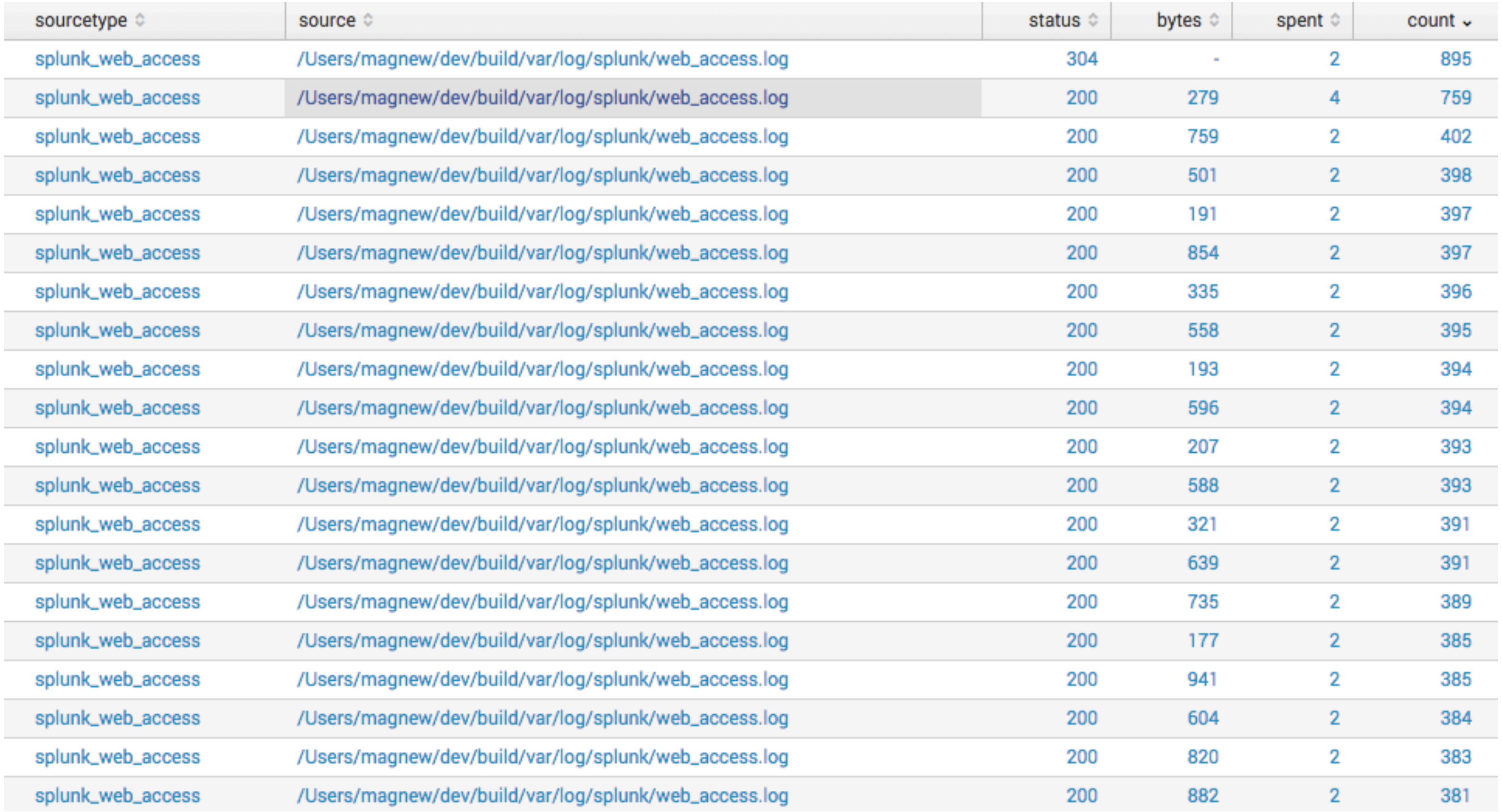
Why Visualization Matters

Visualization bridges the gap



Basic visualization

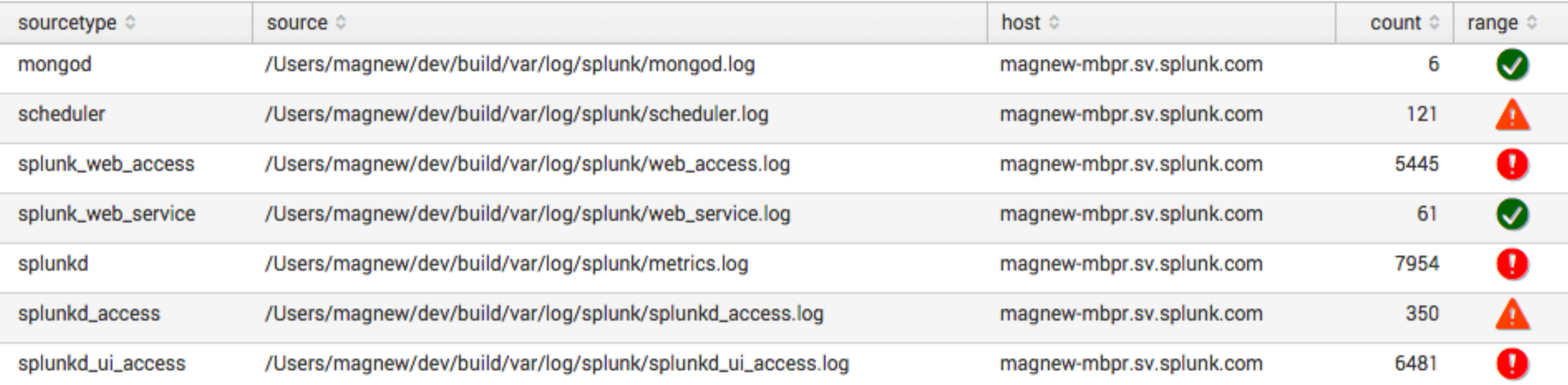
- Filter
- Format
- Sort
- Transform



sourcetype	source	status	bytes	spent	count
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	304	-	2	895
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	279	4	759
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	759	2	402
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	501	2	398
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	191	2	397
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	854	2	397
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	335	2	396
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	558	2	395
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	193	2	394
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	596	2	394
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	207	2	393
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	588	2	393
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	321	2	391
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	639	2	391
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	735	2	389
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	177	2	385
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	941	2	385
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	604	2	384
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	820	2	383
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	200	882	2	381

Doing Better

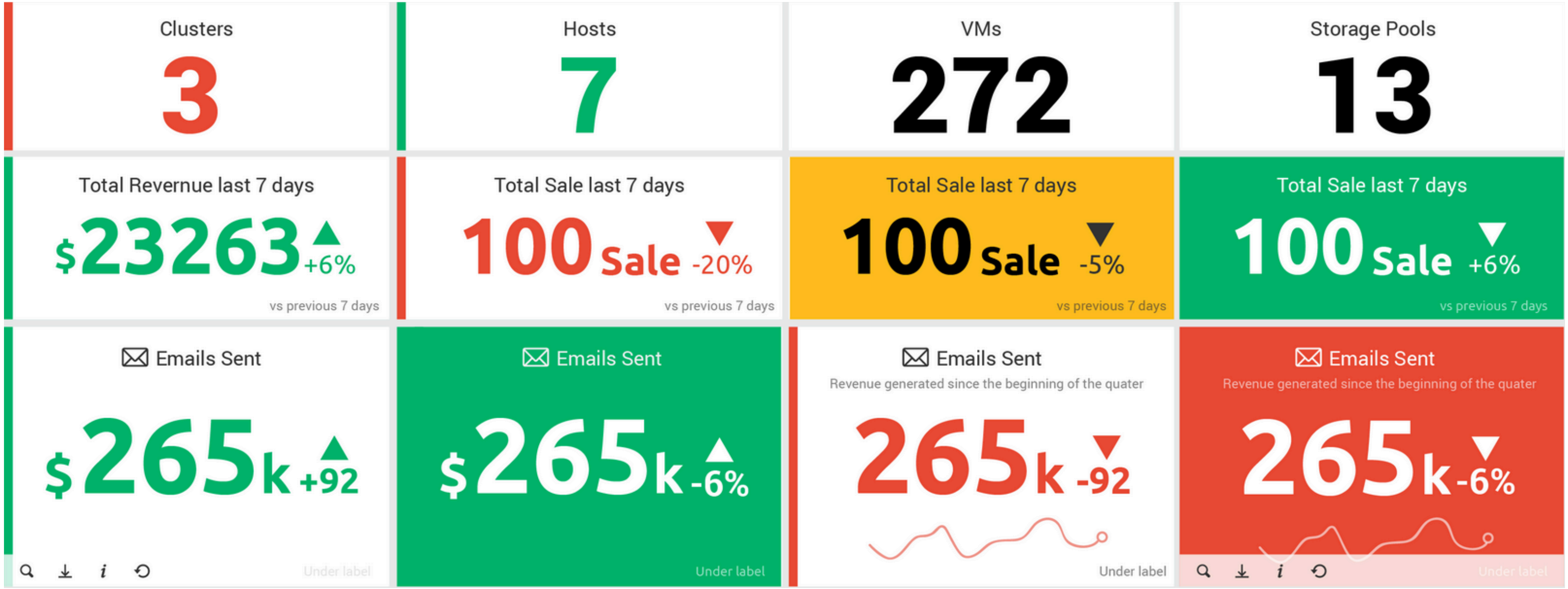
- Color
- Shape
- Size
- Knowledge



sourcetype	source	host	count	range
mongod	/Users/magnew/dev/build/var/log/splunk/mongod.log	magnew-mbpr.sv.splunk.com	6	✓
scheduler	/Users/magnew/dev/build/var/log/splunk/scheduler.log	magnew-mbpr.sv.splunk.com	121	⚠
splunk_web_access	/Users/magnew/dev/build/var/log/splunk/web_access.log	magnew-mbpr.sv.splunk.com	5445	❗
splunk_web_service	/Users/magnew/dev/build/var/log/splunk/web_service.log	magnew-mbpr.sv.splunk.com	61	✓
splunkd	/Users/magnew/dev/build/var/log/splunk/metrics.log	magnew-mbpr.sv.splunk.com	7954	❗
splunkd_access	/Users/magnew/dev/build/var/log/splunk/splunkd_access.log	magnew-mbpr.sv.splunk.com	350	⚠
splunkd_ui_access	/Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log	magnew-mbpr.sv.splunk.com	6481	❗

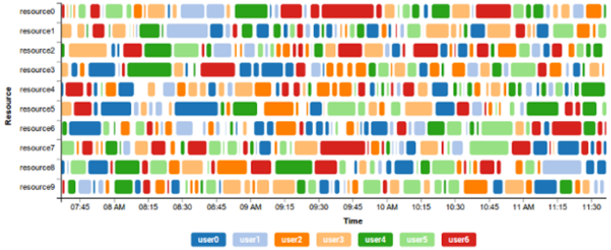
Doing Better

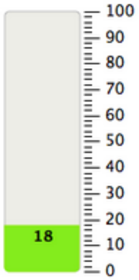
- Color
- Shape
- Size
- Knowledge



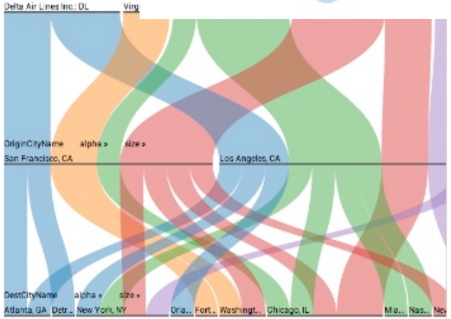
And Better

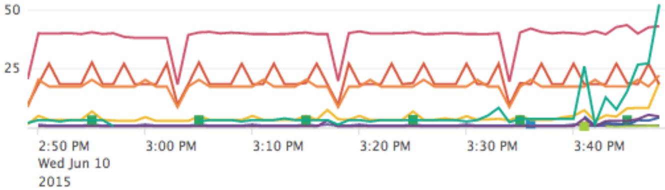
- More Knowledge
- Complexity
- Interaction

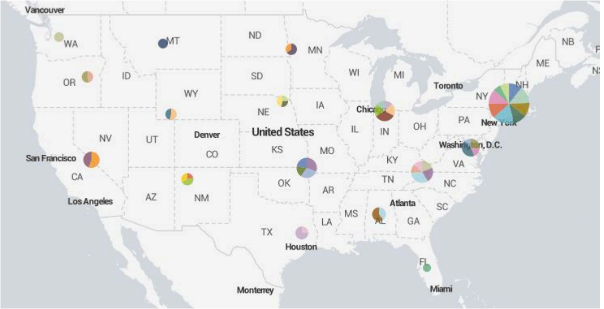




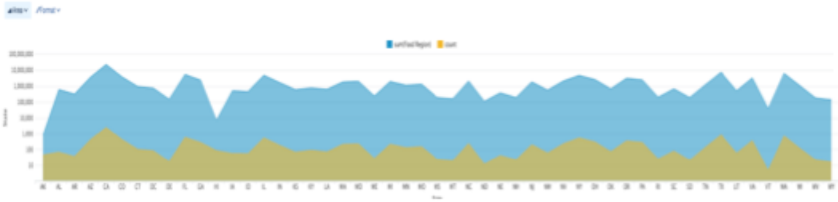
900
800
1000
2000
500
800
400
400
4000
3000
200
200
400
1000
800
500
300
100





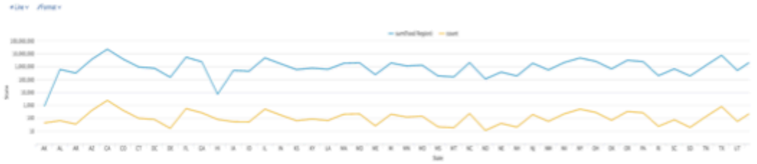


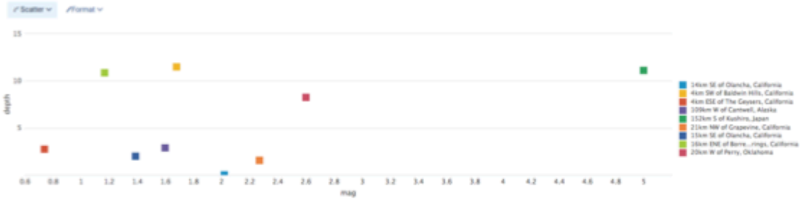
10
20
30
40
50
60
70
80
90
100
0
18

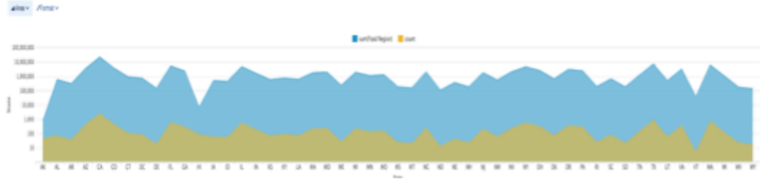


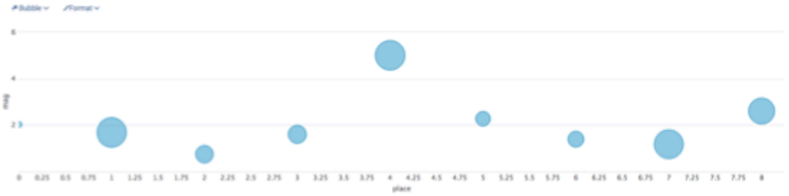
Splunk Built-in Visualizations

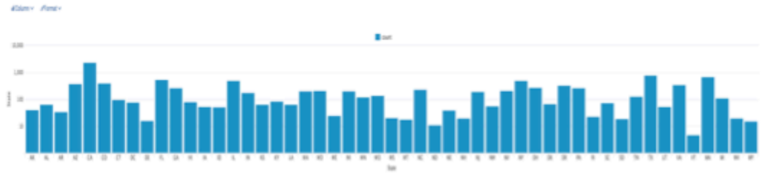
Axis charts: Line, Area, Column, Scatter, Bubble, Bar

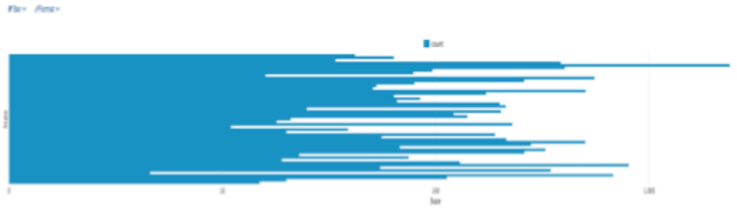



Scatter
Format
15
10
5
depth
0.6
0.8
1
1.2
1.4
1.6
1.8
2
2.2
2.4
2.6
2.8
3
3.2
3.4
3.6
3.8
4
4.2
4.4
4.6
4.8
5
mag
14km SE of Olancha, California
4km SW of Baldwin Hills, California
4km ESE of The Geysers, California
109km W of Cantwell, Alaska
152km S of Kushiro, Japan
21km NW of Grapevine, California
15km SE of Olancha, California
16km ENE of Borre...rings, California
20km W of Perry, Oklahoma



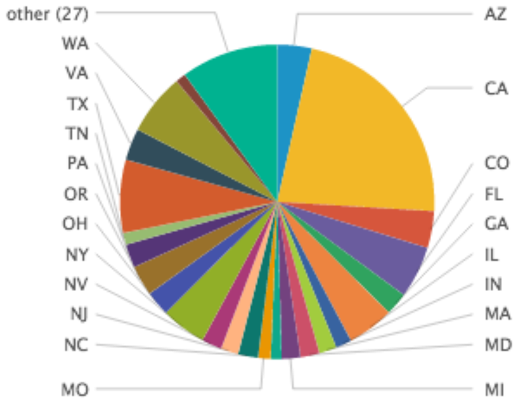


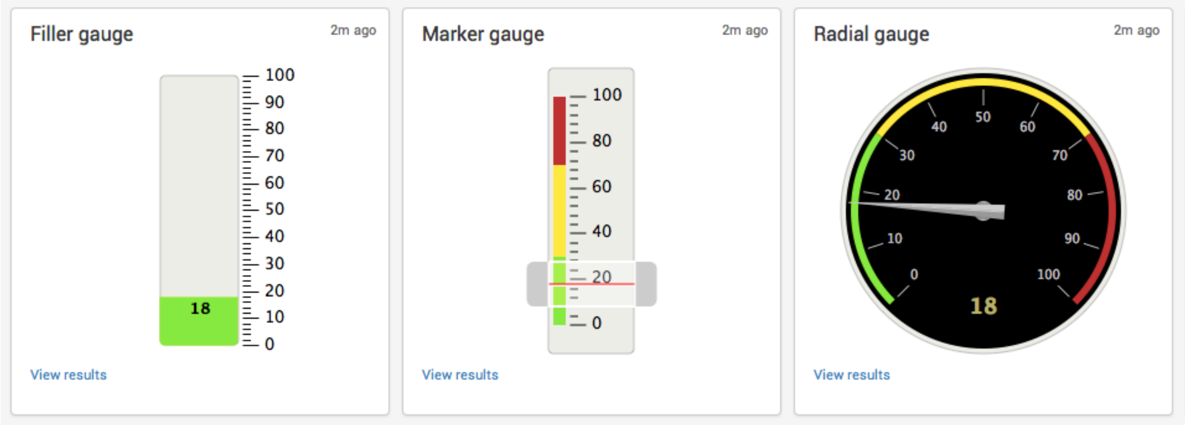




Splunk Built-in Visualizations

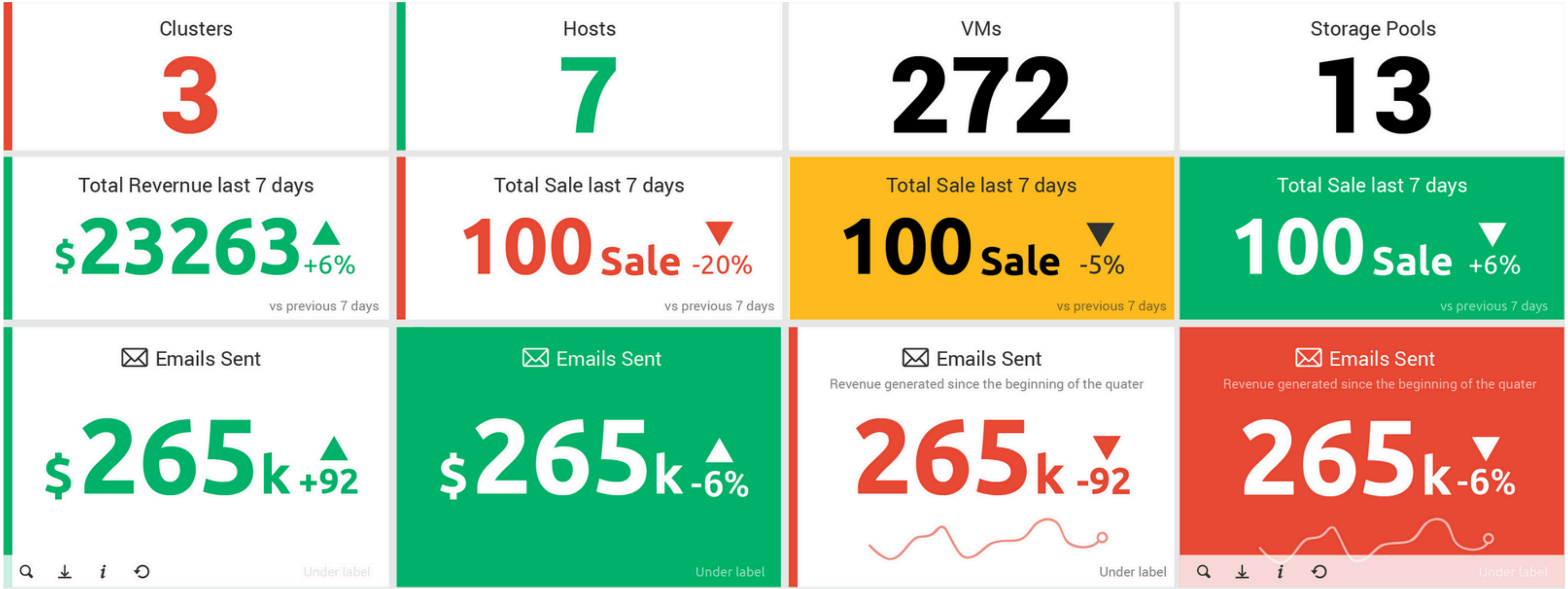
Counting: Pie, Filler Gauge, Marker Gauge, Radial Gauge, Single Value (now counting++)





Splunk Built-in Visualizations

Counting: Pie, Filler Gauge, Marker Gauge, Radial Gauge, Single Value (now counting++)



Clusters 3

Hosts 7

VMs 272

Storage Pools 13

Total Revenue last 7 days $23263 ▲ +6% vs previous 7 days

Total Sale last 7 days 100 Sale ▼ -20% vs previous 7 days

Total Sale last 7 days 100 Sale ▼ -5% vs previous 7 days

Total Sale last 7 days 100 Sale ▼ +6% vs previous 7 days

✉ Emails Sent $265k ▲ +92 Under label

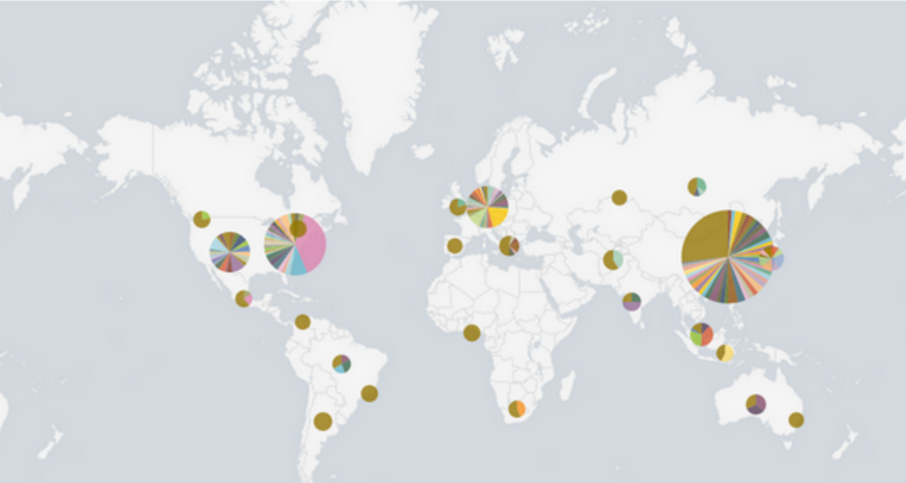
✉ Emails Sent $265k ▲ -6% Under label

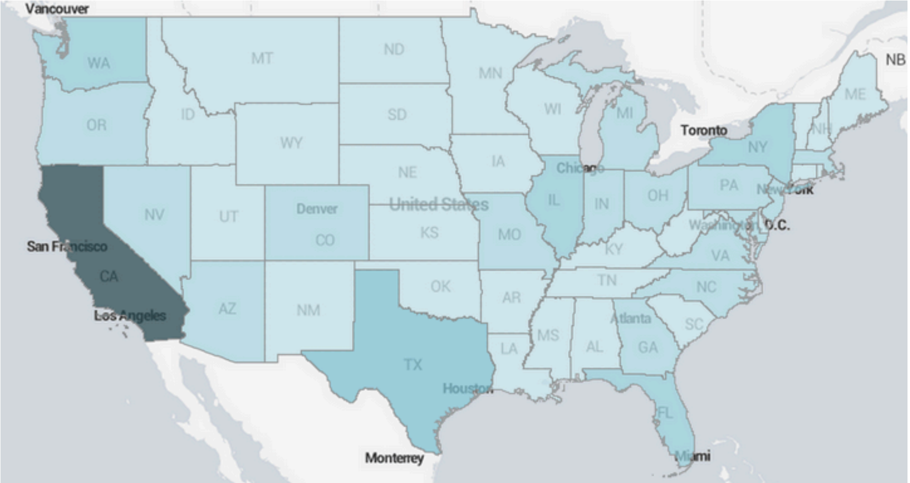
✉ Emails Sent Revenue generated since the beginning of the quater 265k ▼ -92 Under label

✉ Emails Sent Revenue generated since the beginning of the quater 265k ▼ -6% Under label

Splunk Built-in Visualizations

Maps: Marker Map, Choropleth Map

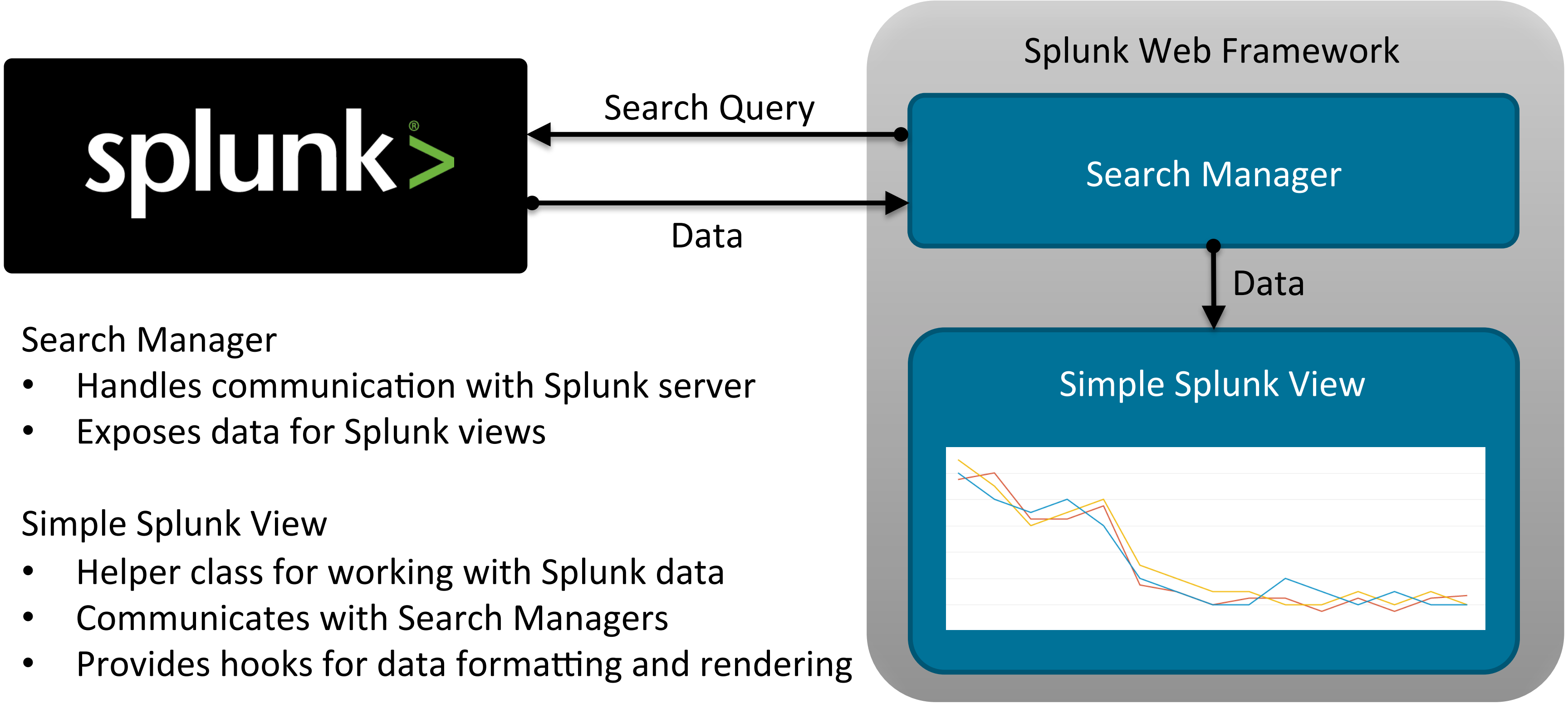




Extending Splunk's Capabilities

- Splunk Web Framework and JavaScript
- Splunk Dashboard Extensions, Standalone Views, or Standalone Splunk apps
- All share the same basic concepts

Overview



Search Manager

- Handles communication with Splunk server
- Exposes data for Splunk views

Simple Splunk View

- Helper class for working with Splunk data
- Communicates with Search Managers
- Provides hooks for data formatting and rendering

Coding Demo

Concepts Review

- Loading JavaScript
- Search Managers
- SimpleSplunkView
- Data Formatting
- Rendering
- Token Binding

Learning More

Other Sessions...

- Accelerating your Solution Development with Splunk Reference Apps – Grigori Melnik
- Enhancing Dashboards with JavaScript! – Satoshi Kawasaki
- Advanced Interactions Using SimpleXML – Mathew Elting and Siegfried Puchbauer

Learning More

- Developer guide: http://dev.splunk.com/view/dev-guide/SP-CAAAE2R
- Developer reference app: https://splunkbase.splunk.com/app/1934/
- Dashboard examples app: https://splunkbase.splunk.com/app/1603/
- Splunk Web Framework reference: http://dev.splunk.com/webframework
- Splunk Web Framework Toolkit: https://splunkbase.splunk.com/app/1613/

.conf2015

THANK YOU

splunk>