

**.conf2013**

**YOUR DATA  
NO LIMITS**

# End-to-End Monitoring From Scratch

Robert Gustafson, Staff Engineer, DirectTV

#splunkconf



# Background: Me

- Staff Engineer at DIRECTV's Los Angeles Broadcast Center
- Three Things I Love
  - USC
  - Detroit Sports
  - Cycling



# Background: Project

- High Revenue
- New Venture
- Limited Monitoring
- Variety of Systems
- Lots of Blind Spots



# Why Splunk Over Other Tools?

- Give it data in any format
- Data, alarming mechanisms, UI's don't have to fit a mold
- All the heavy lifting is already done
- Finding cause faster than humans
- Developer Freedom!

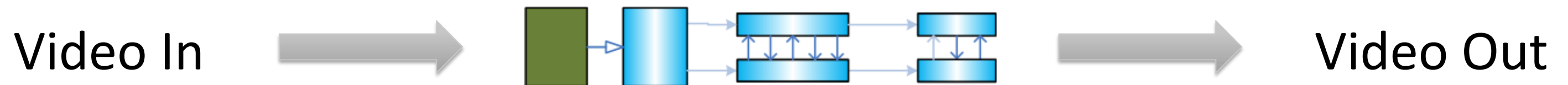


# Challenges Splunk Solved

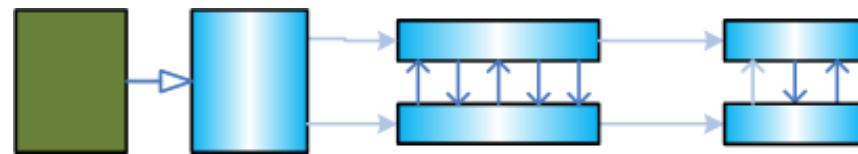
- Project scope
- Little insight into workings of platform
- Users not nerdy enough to decode log files

# Challenge: Scope

Before expansion: "The world is flat"

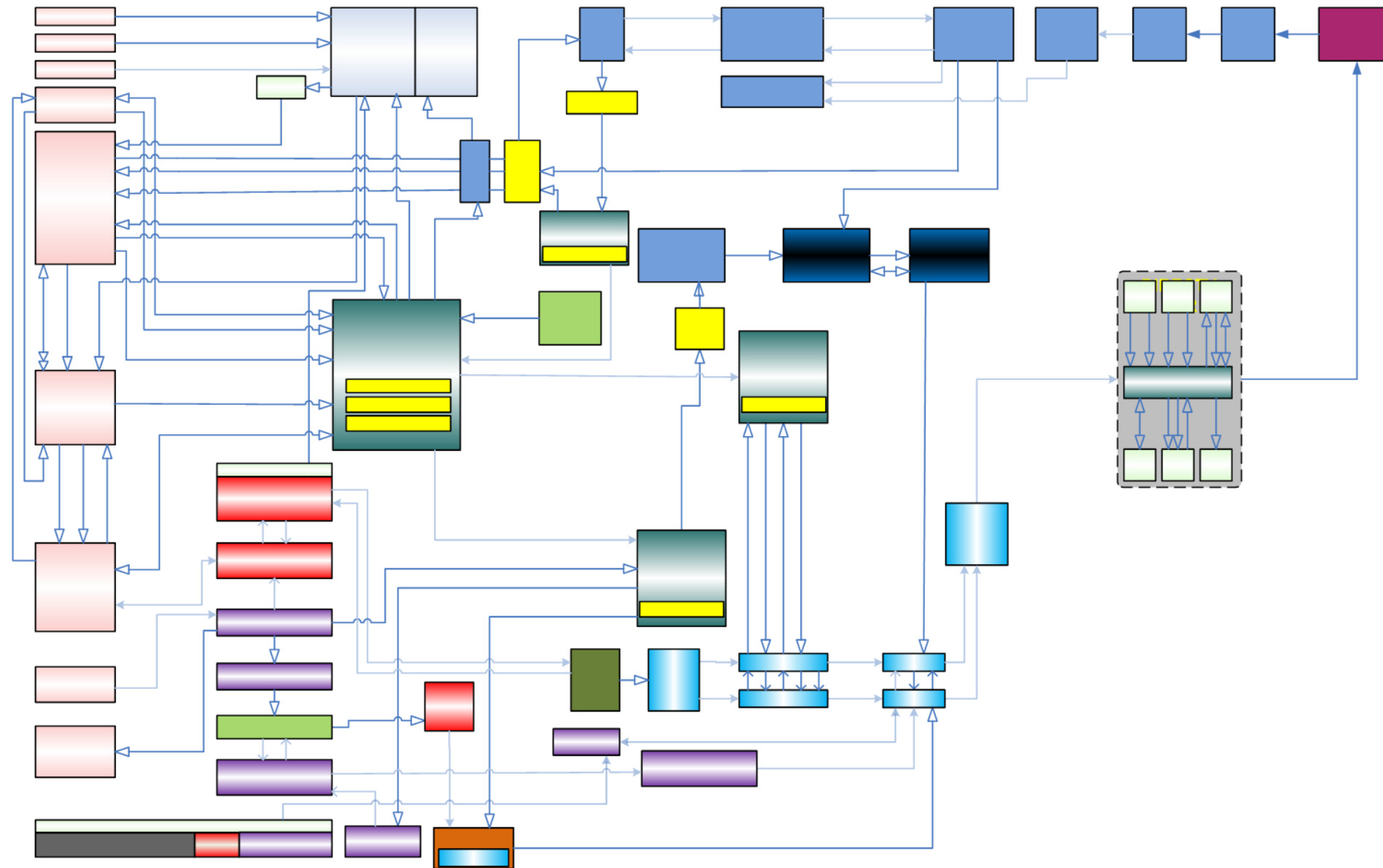


# Challenge: Scope

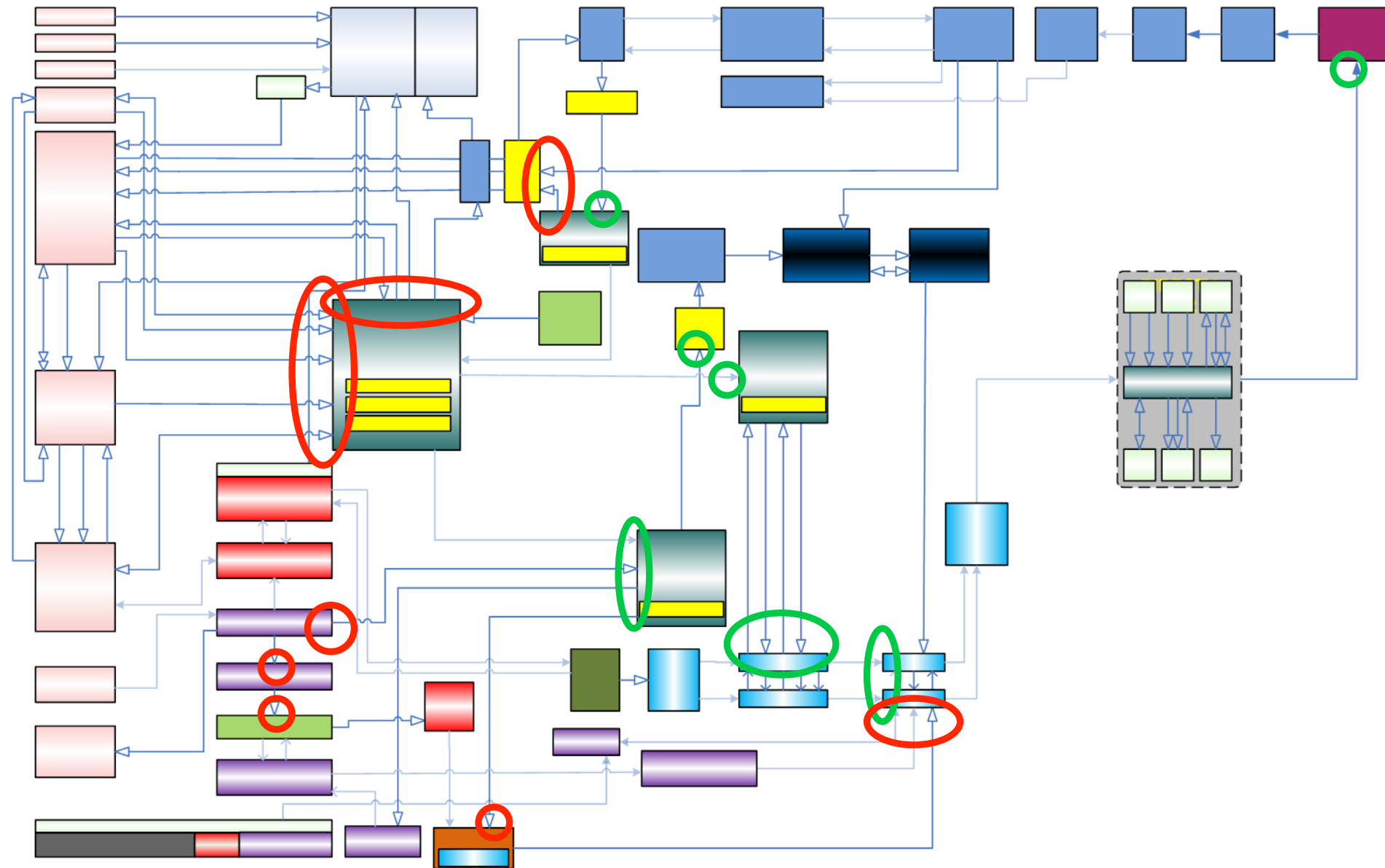


# Challenge: Scope

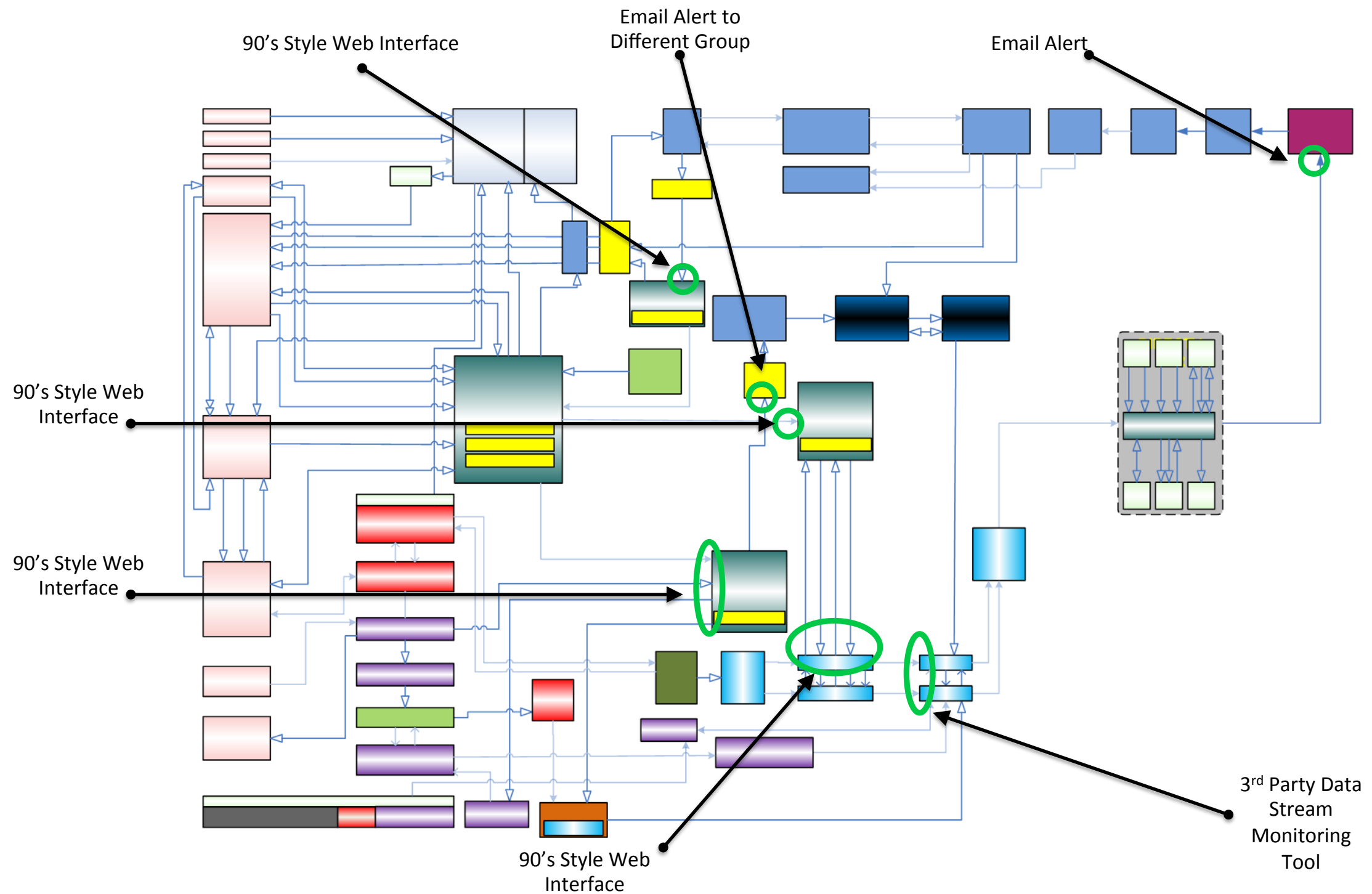
After expansion: "The world is round"



# Challenge: Scope



# Challenge: Scope



# Challenge: Scope

Is it really 2013?

Host						Status/Control	Host						Status/Control
<a href="#">prod-la-01</a>	⚠	☐	☐	🛑	☐	Active	<a href="#">prod-la-02</a>	✅	☐	☐	✅	☐	Inactive
<a href="#">prod-la-01</a>	🛑	☐	☐	☐	✅	Inactive	<a href="#">prod-la-02</a>	⚠	☐	☐	☐	🛑	Active
<a href="#">prod-la-01</a>	⚠	☐	☐	☐	☐		<a href="#">prod-la-02</a>	⚠	☐	☐	☐	☐	
<a href="#">prod-la-03</a>	⚠	🛑	⚠	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-04</a>	⚠	🛑	⚠	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-05</a>	⚠	🛑	⚠	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-06</a>	⚠	🛑	⚠	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-07</a>	⚠	🛑	⚠	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-08</a>	⚠	🛑	⚠	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-09</a>	✅	🛑	⚠	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-10</a>	✅	🛑	⚠	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-11</a>	⚠	🛑	✅	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-12</a>	⚠	🛑	✅	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-13</a>	⚠	✅	✅	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-14</a>	⚠	✅	✅	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-15</a>	✅	🛑	✅	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-16</a>	✅	🛑	✅	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-17</a>	✅	✅	⚠	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-18</a>	✅	✅	⚠	☐	☐	Offline <input type="button" value="Go Online"/>
<a href="#">prod-la-19</a>	⚠	✅	✅	☐	☐	Online <input type="button" value="Go Offline"/>	<a href="#">prod-la-20</a>	⚠	✅	✅	☐	☐	Offline <input type="button" value="Go Online"/>

# Challenge: Scope

What happens when you have no idea what you're looking for??

- Look for events that occurred while systems experienced problems
  - Narrow results using the punct field
  - “|dedup punct”
  - “|stats count by punct”



# Challenge: Scope

Search

error | dedup punct

Verbose Mode

Aug 21, 2013

≥ 89 matching events | 8,388 scanned events

Hide Zoom out Zoom to selection Deselect

Linear scale 1 bar = 1 hour

12:00 AM Wed Aug 21 2013 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM

Hide

≥ 89 events during Wednesday, August 21, 2013

Export Options

4 selected fields Edit

a host(59)

1 8/21/13 [ERROR 2013-08-22 06:59:59:991] 11:50:59.001 PM Http Error: 50x111 Content Length related error. Content Length is missing

# Ignoring the Garbage

The screenshot shows a Splunk search interface. The search bar at the top contains the query: `sourcetype="aa-bdms-jobrunner" (NOT type=Status AND NOT type=Info AND NOT type=Warning AND NOT type=DEBUG OR ("finished running") OR ("is running"))`. The search results are displayed as a list of log entries, each starting with `NOT /opt/advatar/var/log/viewsrv.log`. The interface includes a search bar, a 'Verbose Mode' dropdown, a 'Last 24 hours' time range selector, and a 'Save' button. The results are paginated, showing '50 per page'.

# Ignoring the Garbage

```
1 logfile, punct
2 viewsrv.log,"...: = ()_::: ' - ' . "
3 viewsrv.log,"...: = ()_::: "
4 viewsrv.log,"...: = ()_::: [ ] : <> : "
5 viewsrv.log,"...: = ()_::: ' - ' . "
6 viewsrv.log,"...: = ()_::: - ' ' - ' . "
7 viewsrv.log,"...: = ()_::: ' ' . "
8 viewsrv.log,"...: = ()_::: "
9 viewsrv.log,"...: = ()_::: "
10 viewsrv.log,"...: = ()_::: ; = : : , = "
11 viewsrv.log,"...: = ()_::: # : : . "
12 viewsrv.log,"...: = ()_::: # : ; = , = "
13 viewsrv.log,"...: = ()_::: , = "
14 viewsrv.log,"...: = ()_::: ; = : : , = "
15 viewsrv.log,"...: = ()_::: "
16 viewsrv.log,"...: = ()_::: - : [ ] " . : - - - - "
17 viewsrv.log,"...: = ()_::: : ; : ; : "
18 viewsrv.log,"...: = ()_::: "
19 viewsrv.log,"...: = ()_::: ' ' "
20 viewsrv.log,"...: = ()_::: "
21 viewsrv.log,"...: = ()_::: . "
22 viewsrv.log,"...: = ()_::: # : "
23 viewsrv.log,"...: = ()_::: ( ) , ( ) "
24 viewsrv.log,"...: = ()_::: ' ' ' ' , = ' ' "
25 viewsrv.log,"...: = ()_::: "
26 viewsrv.log,"...: = ()_::: ' ' ' ' , = ' ' "
27 viewsrv.log,"...: = ()_::: # : : "
28 viewsrv.log,"...: = ()_::: # : ; = , = "
29 viewsrv.log,"...: = ()_::: ' ' - ' ' "
30 viewsrv.log,"...: = ()_::: ' ' - ' ' , = ' ' "
31 viewsrv.log,"...: = ()_::: # : "
32 JobRunner.log,"<> - - - - : : + : - - : ' - ' : ( , ) . - - - - "
33 JobRunner.log,"<> - - - - : : + : - - : ( , ) . - - - - : : "
34 JobRunner.log,"<> - - - - : : + : - - : : : : ( ) "
35 JobRunner.log,"<> - - - - : : + : - - : : : : ( , , , , ) "
36 JobRunner.log,"<> - - - - : : + : - - : : : : ( , "
37 JobRunner.log,"<> - - - - : : + : - - : : : : ( "
38 JobRunner.log,"<> - - - - : : + : - - : : : : ( "
39 JobRunner.log,"<> - - - - : : + : - - : : : : ( , ) "
40 JobRunner.log,"<> - - - - : : + : - - : - - : ( , ) "
41 JobRunner.log,"<> - - - - : : + : - - : : : : ( ) : "
42 JobRunner.log,"<> - - - - : : + : - - : : : : - - - - : : : : "
43 JobRunner.log,"<> - - - - : : + : - - : : : : - - - - : : : : "
44 JobRunner.log,"<> - - - - : : + : - - : : : : "
45 JobRunner.log,"<> - - - - : : + : - - : : : : "
46 JobRunner.log,"<> - - - - : : + : - - : : : : - - - - : : : : "
47 JobRunner.log,"<> - - - - : : + : - - : : : : ( ) : "
48 JobRunner.log,"<> - - - - : : + : - - : : : : ( ) : "
49 JobRunner.log,"<> - - - - : : + : - - : - - : - - : , = , = - - : "
50 JobRunner.log,"<> - - - - : : + : - - : ' - ' : : : : - - - - "
```

Normal text file length: 2899 lines: 50 Ln: 2 Col: 1 Sel: N/A Dos\Windows ANSI INS

# Ignoring the Garbage

```
Error NOT [inputcsv ignore_errors.csv  
| search logfile="JobRunner.log" |  
rename ignore_punct AS punct | fields  
punct]
```

# Exception Based Monitoring

- What am I looking at? (High Level)
  - Does this log entry directly impact the customer experience?
  - Is it actionable?
- If yes to both: make an alert with a saved search

# Exception Based Monitoring

## Saved Search:

- Query to find error condition

```
host=splunkforwarder* ERROR no file found
```

- Secondary query to alert on

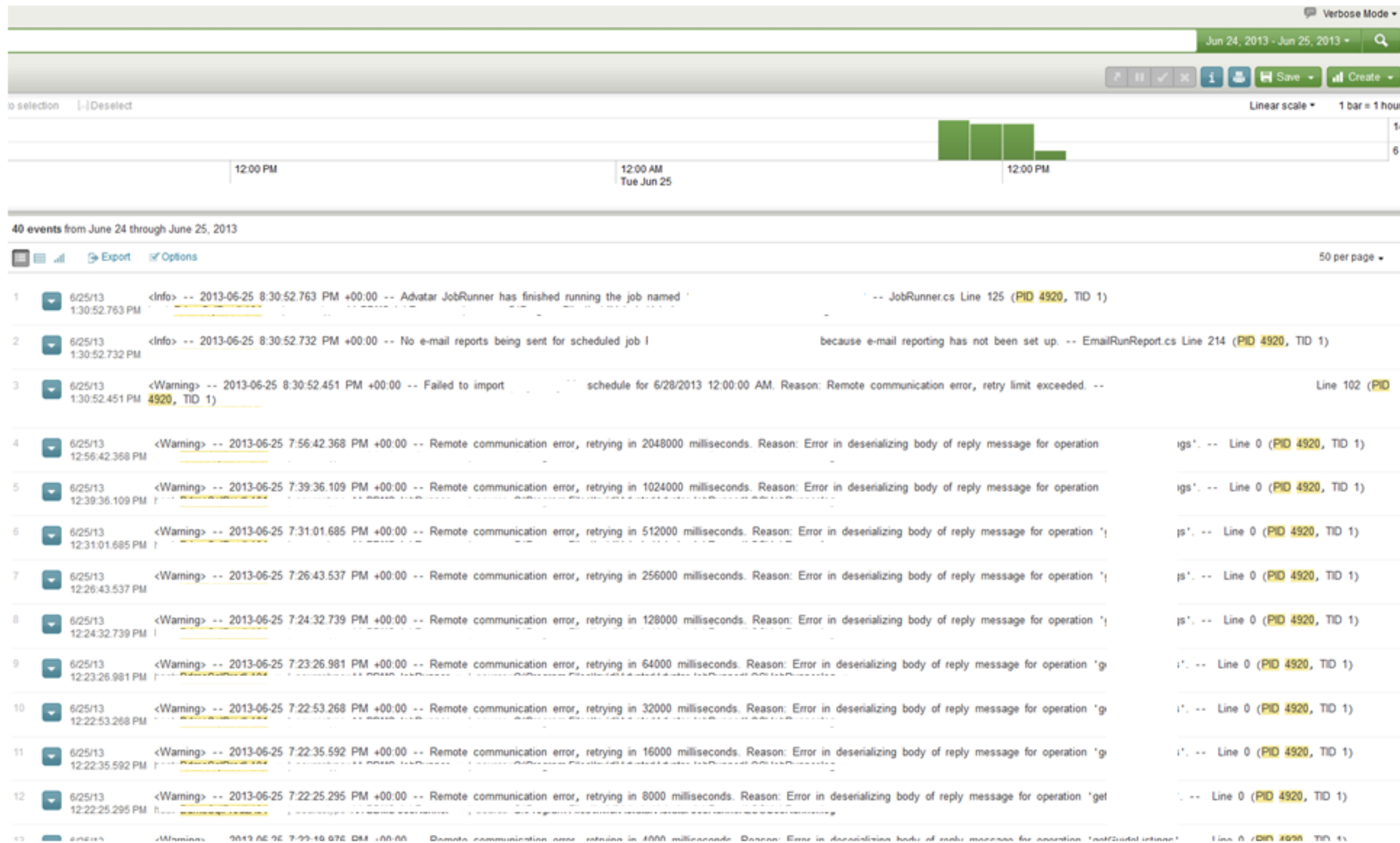
```
| stats count | where count > 1
```

- Time Ranges

# Proactive Monitoring

- What events can begin to indicate failure?
  - ex: Steady disk space increase, Repeated timeouts
- Use Splunk Enterprise to set thresholds or look for patterns

# Proactive Monitoring: Patterns



# Proactive Monitoring

- Query to find error condition

```
host=splunkforwarder* WARNING timeout
| stats count as num_errors_by_host by host
| stats sum(num_hosts_in_error) as total_errors
      count(eval(num_hosts_in_error>0)) as num_hosts_in_error
```

- Secondary query to alert on

```
| where num_hosts_in_error > 10
```

```
| where total_errors > 100
```

```
| where num_hosts_in_error > 10 AND total_errors > 100
```

- Time Ranges

# Merging Different Data Types

- Multiple servers saying the same in different ways
- Who do you listen to?

# Merging Different Data Types

- Unify the data
- Correlate the data
- Alert on the data

# Merging Different Data Types

```
<tr><td align="center"><font color="#000000">Aug 23 05:25:39.000000000</font></td>  
<td align="center"><font color="#000000">Aug 23 05:25:39.000000000</font></td>  
<td align="center"><font color="#000000">405889479</font></td>  
<td align="center"><font color="#000000">-324 ms</font></td>  
<td align="center"><font color="#000000">-prod-la-05</font></td>  
<td align="center"><font color="#000000"></font></td>  
<td align="center"><font color="#000000">110</font></td>  
<td align="center"><font color="#000000">0x100</font></td>  
<td align="center"><font color="#000000">10153</font></td>  
<td align="center"><font color="#000000">1813253</font></td>  
<td align="center"><font color="#000000">Aug 23 05:00:00</font></td>  
<td align="center"><font color="#000000">Aug 23 06:00:00</font></td>  
<td align="center"><font color="#000000">1</font></td>  
<td align="center"><font color="#000000">Successful</font></td>  
</tr>
```

2013.08.23 06:13:43 GMT (event) Successful ID= 1813253 pid=14283

57 results since 7:48:43 PM August 22, 2013

Overlay:

	<u>_time</u> ↕	<u>ID</u> ↕
1	8/22/13 10:38:09.000 PM	1813913
2	8/22/13 10:27:53.000 PM	1813323
3	8/22/13 10:25:58.000 PM	1813674
4	8/22/13 10:25:39.000 PM	1813253
5	8/22/13 10:25:35.000 PM	1813912
6	8/22/13 10:23:41.000 PM	1814096
7	8/22/13 10:22:57.000 PM	1815395
8	8/22/13 10:22:43.000 PM	1812378
9	8/22/13 10:22:29.000 PM	1814303
10	8/22/13 10:21:27.000 PM	1812538

# Correlating events

```
sourcetype="box1" | table ID |  
join type=left ID [sourcetype="box2" | eval box2ID=ID | table box2ID,ID] |  
table ID, box2ID |  
| where ID!=box2ID
```

ID	box2ID
1	1
2	
3	3
4	4
5	5
6	
7	7

# Splunk!

Exception

Proactive

**BDS** 17m ago

Missed

- HD 0
- SD 0
- Ineoquest

Successful

- HD 11 / 31
- SD 10 / 24

Server Connections

- BDMS Connections

Correlated Alert

**BDMS** 2m ago

Last log entry: Mon Jul 29 09:16:38 2013

- [redacted] - Last Success: Mon Jul 29 08:33:15 2013
- [redacted] - Last Success: Fri Jul 26 13:33:11 2013
- [redacted] - Last Success: Sun Jul 28 16:35:28 2013
- [redacted] - Last Success: Sun Jul 28 09:05:58 2013
- [redacted] - Last Success: Sun Jul 28 17:21:07 2013
- [redacted] - Last Success: Mon Jul 29 02:01:54 2013
- [redacted] - Last Success: Sun Jul 28 17:15:06 2013
- [redacted] - Last Success: Sun Jul 28 10:06:16 2013
- [redacted] - Last Success: Sun Jul 28 11:45:13 2013
- [redacted] - Last Success: Mon Jul 29 15:55:00 2013 (GMT)
- [redacted] - Last Success: Sun Jul 28 21:00:33 2013 (GMT)

**DSS** 2m ago

**CMS** **Prioritizer**

Services

- Daily ADR Request

Exception

**System Status** 2m ago

- Push Status
- Ineoquest Status
- Lost Hosts 0
- Disk Health

Proactive

# Challenge: Not So Nerdy Users

- Present data to users who don't understand the workings of the system
- Don't call it what it is

<b>What the log says</b>	<b>What user understands</b>
Timeout	Network connectivity
Forwarder agent is down	Lost Server

# Easy to Understand UI

- Start with high level... drilldown to confusion
- Incorporate workflows
- Do everything you can from same interface
- Always present in plain English, use choice words
- Colors over numbers (or colored numbers)
- Separate hardware/network alerts from application alerts

# Drilldown Example

**BDMS**  
Last log entry: Mon Jul 29 09:16:38 2013

- [redacted] - Last Success: Mon Jul 29 08:33:15 2013
- [redacted] - Last Success: Fri Jul 26 13:33:11 2013
- [redacted] - Last Success: Sun Jul 28 16:35:28 2013
- [redacted] - Last Success: Sun Jul 28 09:05:58 2013
- [redacted] - Last Success: Sun Jul 28 17:21:07 2013
- [redacted] - Last Success: Mon Jul 29 02:01:54 2013
- [redacted] - Last Success: Sun Jul 28 17:15:06 2013
- [redacted] - Last Success: Sun Jul 28 10:06:16 2013
- [redacted] - Last Success: Sun Jul 28 11:45:13 2013
- [redacted] - Last Success: Mon Jul 29 15:55:00 2013 (GMT)
- [redacted] - Last Success Sun Jul 28 21:00:33 2013 (GMT)



**Run History**  
Last 24 hours

« prev 1 2 3 next »

Start ↕	Finished ↕
09/13/13 10:15	09/13/13 10:33
09/13/13 09:15	09/13/13 09:36
09/13/13 08:15	09/13/13 08:34
09/13/13 07:15	09/13/13 07:33
09/13/13 06:15	09/13/13 06:43
09/13/13 05:15	09/13/13 05:41
09/13/13 04:15	09/13/13 04:30
09/13/13 03:15	09/13/13 03:33
09/13/13 02:15	09/13/13 02:30
09/13/13 01:15	09/13/13 01:30


Search:







« prev 1 2 3 4 5 6 next »

time ↕	type ↕	pid ↕	message ↕
09/13/13 09:36:18.558 AM	Info	6456	
09/13/13 09:36:18.543 AM	Info	6456	
09/13/13 09:36:18.527 AM	Info	6456	Import successfu
09/13/13 09:36:00.914 AM	Error	6456	IMPORT FAILED:
09/13/13 09:36:00.586 AM	Error	6456	IMPORT FAILED:
09/13/13 09:36:00.336 AM	Error	6456	IMPORT FAILED:
09/13/13 09:35:59.978 AM	Error	6456	IMPORT FAILED:
09/13/13 09:35:59.759 AM	Error	6456	IMPORT FAILED:
09/13/13 09:35:59.447 AM	Error	6456	IMPORT FAILED:
09/13/13 09:35:59.197 AM	Error	6456	IMPORT FAILED:



# Workflow Example

Cause 

<input type="text"/>		<input type="button" value="Save"/>
Undetermined Provider		<input type="button" value="Save"/>
<input type="text"/>		<input type="button" value="Save"/>
<input type="text"/>		<input type="button" value="Save"/>
<input type="text"/>		<input type="button" value="Save"/>
<input type="text"/>		<input type="button" value="Save"/>
<input type="text"/>		<input type="button" value="Save"/>

**.conf2013**

**YOUR DATA  
NO LIMITS**

**Wrap Up/Questions**

**splunk>**

# Next Steps

1

## Download the .conf2013 Mobile App

If not iPhone, iPad or Android, use the Web App

2

Take the survey & **WIN A PASS FOR .CONF2014...** Or one of these bags!



**.conf2013**

**YOUR DATA  
NO LIMITS**

**THANK YOU**

**splunk>**

