Adding Depth to Dashboards

Pierre Brunel
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.

Agenda

- Introduction
- Static vs Dynamic Dashboards
- Demo
- Step-by-Step Implementation
- Q&A

Introduction

- Splunker since 2014

- Previously worked in operations for large SaaS company
  - 5 years in escalation support before Splunk
  - 2 years using Splunk

I liked the product so much I joined the company!

A Quick Poll

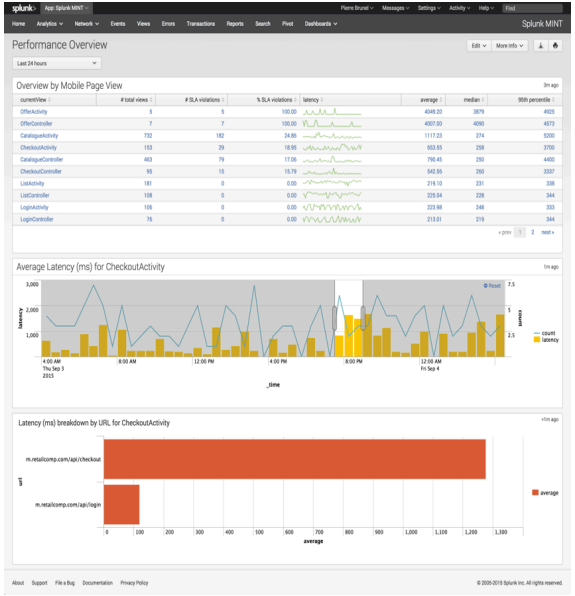
- New to Splunk?
- Experience w/ Simple XML?
- Experience w/ Advanced XML?

Perspective is Key

Perspective is Key

Static vs Dynamic Dashboards

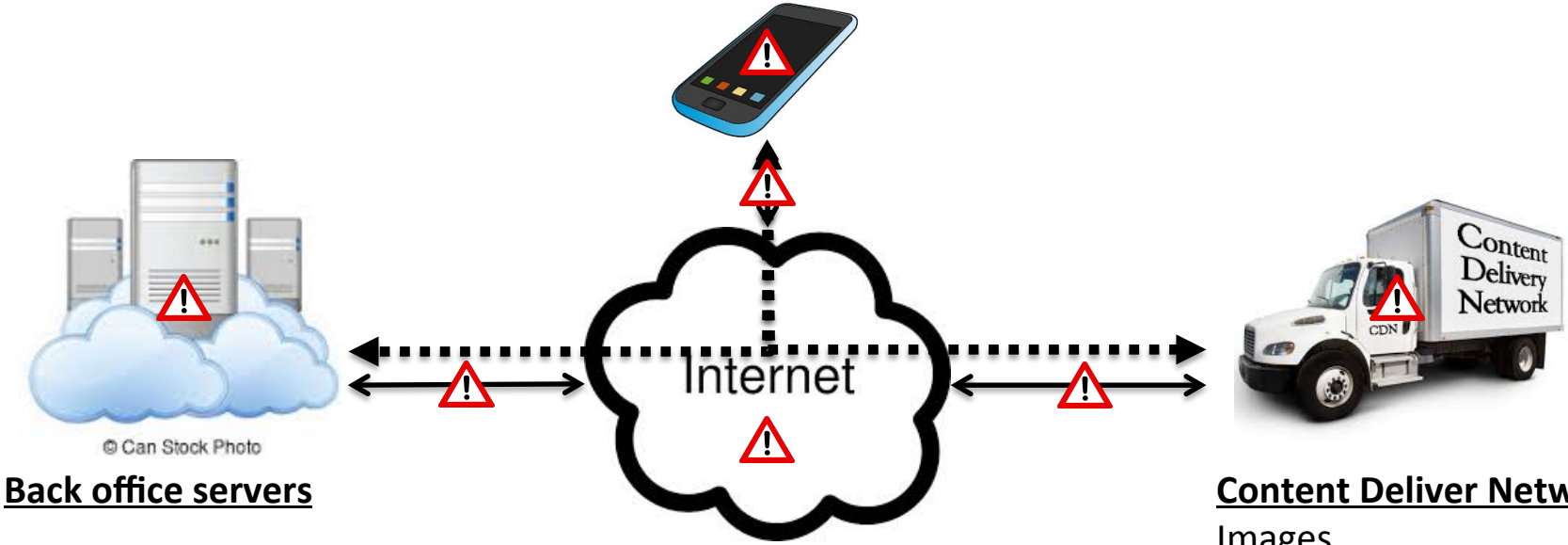
- Static Dashboards
  - Provides executive summaries
  - Answers specific questions
    - “What are my top … ?”
    - “What’s the timeline of activity for … ?”
- Dynamic Dashboards
  - Same as above…and more
  - Pivot and answer subsequent questions
    - “Given my selection here, tell me more about …”
  - View the same dataset from multiple angles



Use Case – Mobile Applications

splunk>

One Page Load = Many Network Calls



Back office servers

Content Deliver Networks
Images
videos

Slow page loads = unhappy customer

Use Case - Introduction

- Page load times are critical
- One page load may involve retrieving information from multiple sources
- Problem could exist in mobile app, network, or back-office
- Operational SLAs

Disclaimers

- Not all visual capabilities will be discussed
- SimpleXML only
- Searches are out of scope
- Limited implementation

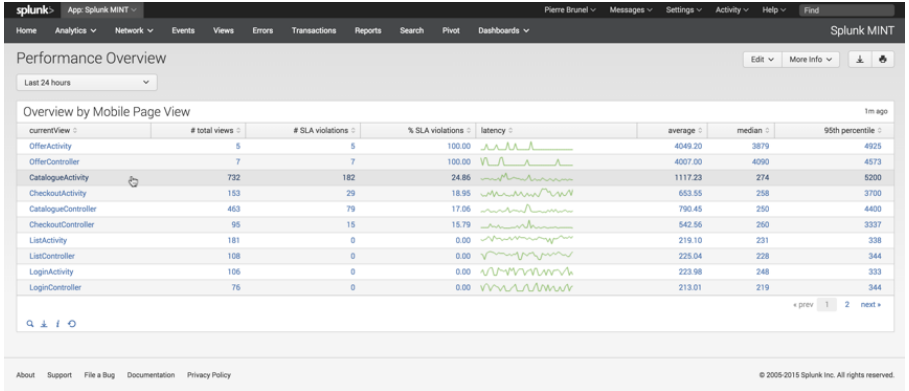
Demo

splunk>

How it Works

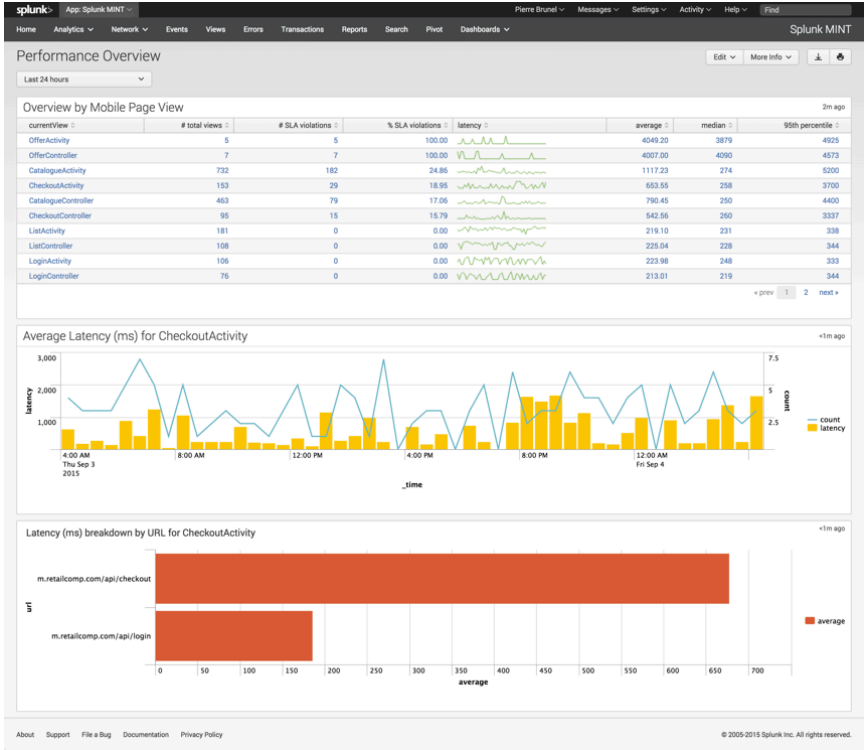
splunk>

Select a Row

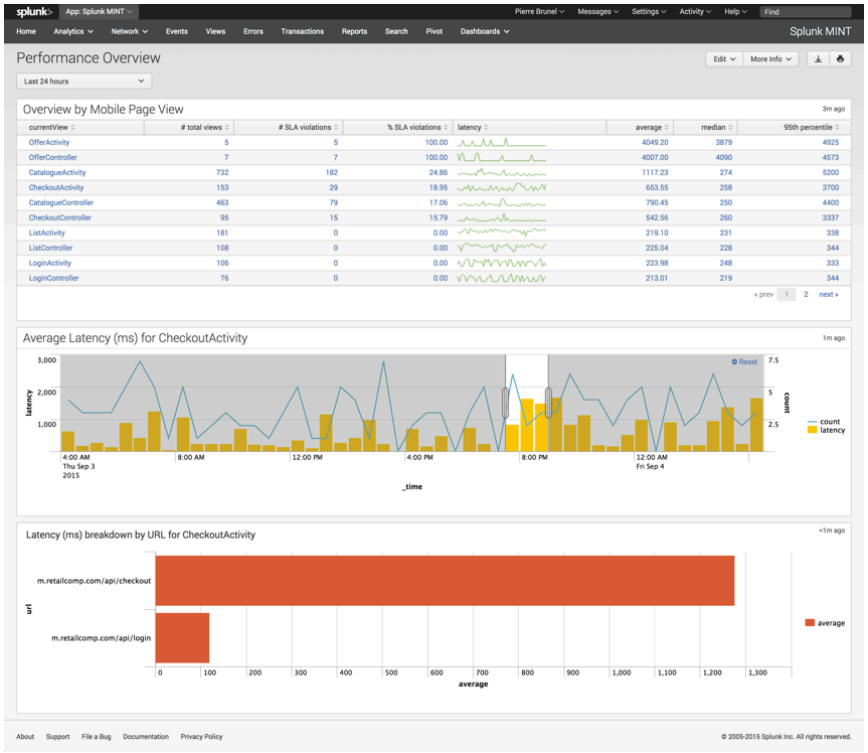


Other panels are hidden

Show Details for Selected View



Select a Subset of Timerange



Tokens – A Primer

- Variables that dynamically pass information within & between dashboards
  - Action on one panel can drive behavior in another panel
  - Tokens can be used to pass information into another URL
    - Another Splunk dashboard
    - Page outside Splunk altogether

Set the token:

```
<drilldown>
    <set token="my_new_token">$row.this_field$</set>
</drilldown>
```

Use the token:

```
<search>
    <query>sourcetype=mysourcetype this_field=$my_new_token$
</search>
```

Tokens

Tokens Set

currentView

selection.earliest
selection.latest

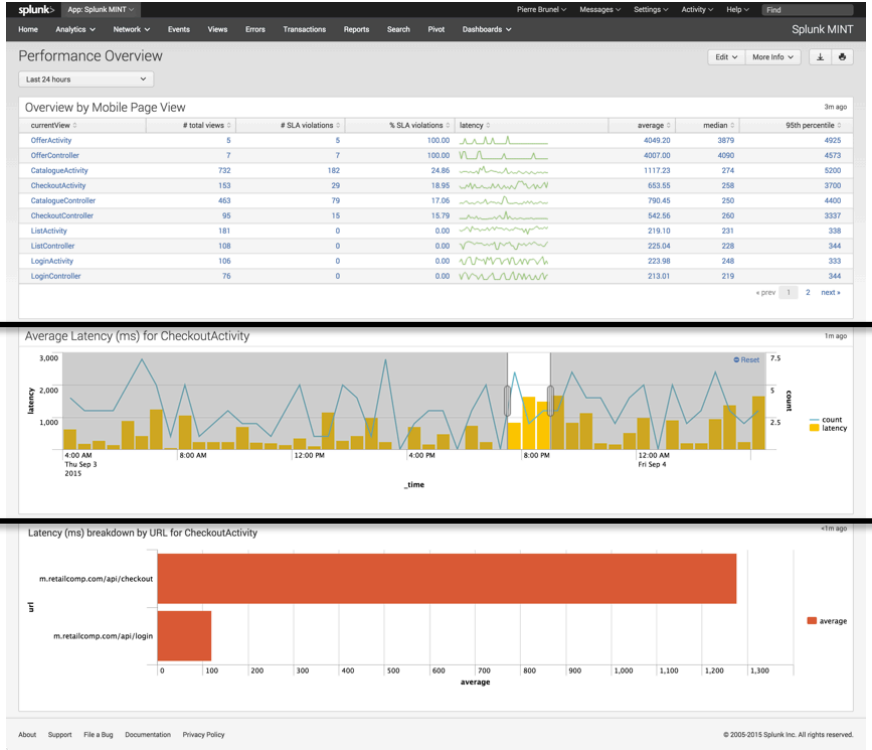
Tokens Utilized

currentView

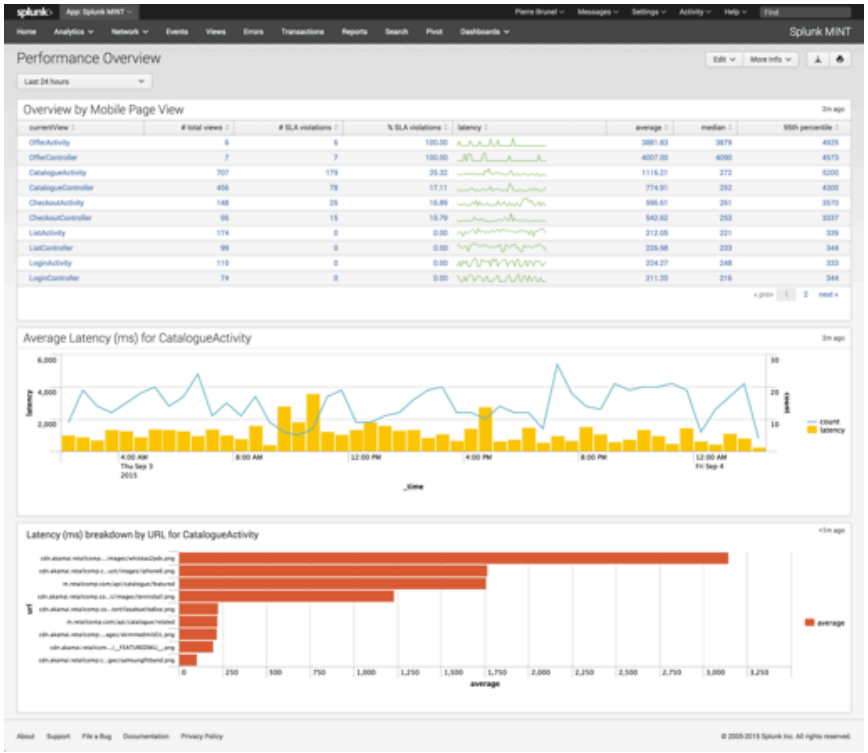
currentView

currentView

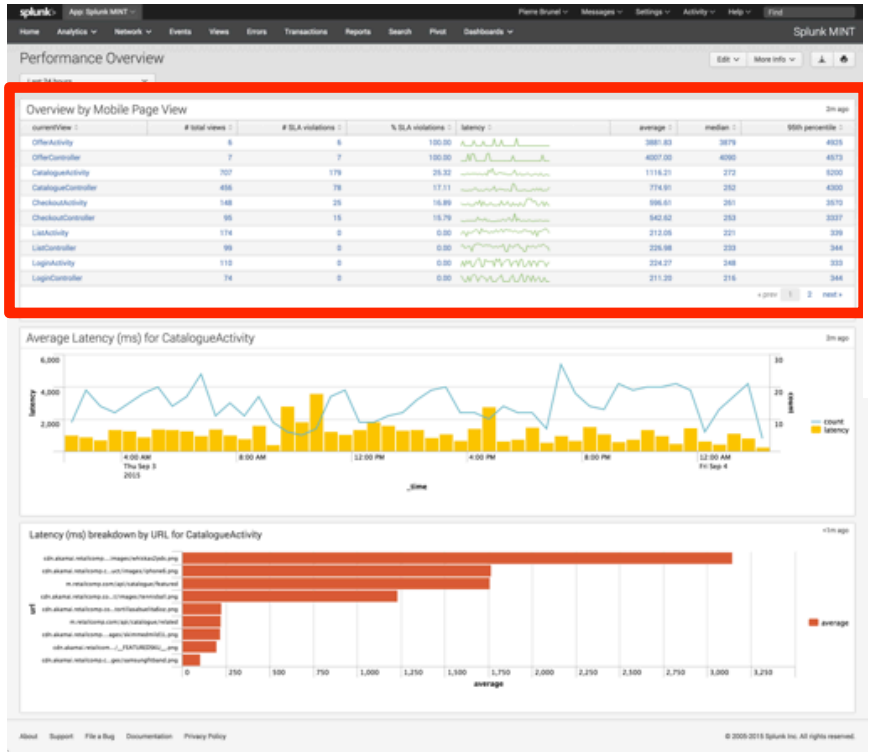
selection.earliest
selection.latest



Walkthrough



Select Row, Set Token




```
<row>
  <panel>
    <title>Overview by Mobile Page View</title>
    <table>
      <search>
        <query>sourcetype=mint:network
          | eval sla=1000
          | stats count count(eval(latency &gt; sla)) as sla_violations sparkline(avg(latency)) as latency
        avg(latency) as average median(latency) as median perc95(latency) as "95th percentile" by currentView
          | eval average=round(average,2)
          | eval "% SLA violations"=round((sla_violations/count)*100,2)
          | rename count as "# total views"
          | rename sla_violations as "# SLA violations"
          | fields currentView "# total views" "# SLA violations" "% SLA violations" latency average median
        "95th percentile"
          | sort -"% SLA violations"</query>
        <earliest>$global_time.earliest$</earliest>
        <latest>$global_time.latest$</latest>
      </search>
      <option name="drilldown">row</option>
      <drilldown>
        <set token="currentView">$row.currentView$</set>
      </drilldown>
      <option name="wrap">true</option>
      <option name="rowNumbers">false</option>
      <option name="dataOverlayMode">none</option>
      <option name="count">10</option>
    </table>
  </panel>
</row>
```

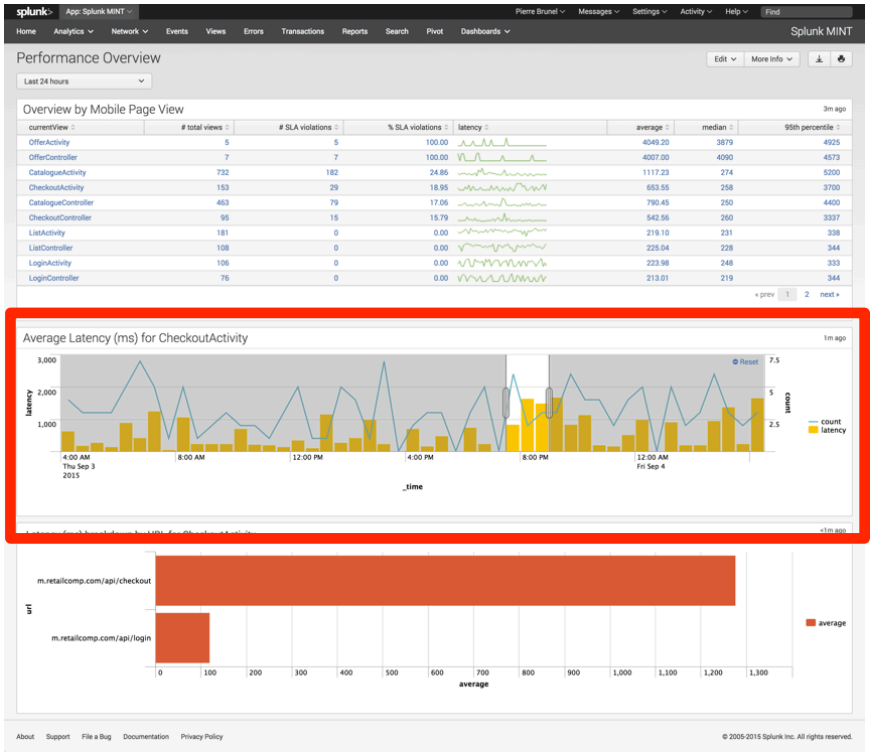
Select Row, Set Token

```
<row>
  <panel>
    <title>Overview by Mobile Page View</title>
    <table>
      <search>
        <query>sourcetype=mint:network
          | eval sla=1000
          | stats count count(eval(latency &gt; sla)) as sla_violations sparkline(avg(latency)) as latency
          avg(latency) as average median(latency) as median perc95(latency) as "95th percentile" by currentView
          | eval average=round(average,2)
          | eval "% SLA violations"=round((sla_violations/count)*100,2)
          | rename count as "# total views"
          | rename sla_violations as "# SLA violations"
          | fields currentView "# total views" "# SLA violations" "% SLA violations" latency average median
          "95th percentile"
          | sort -"% SLA violations"</query>
        <earliest>$global_time.earliest$</earliest>
        <latest>$global_time.latest$</latest>
      </search>
      <option name="drilldown">row</option>
      <drilldown>
        <set token="currentView">$row.currentView$</set>
      </drilldown>
      <option name="wrap">true</option>
      <option name="rowNumbers">false</option>
      <option name="dataOverlayMode">none</option>
      <option name="count">10</option>
    </table>
  </panel>
</row>
```

Select Row, Set Token

```
<option name="drilldown">row</option>
<drilldown>
  <set token="currentView">$row.currentView$</set>
</drilldown>
```

Select Subset of Timerange

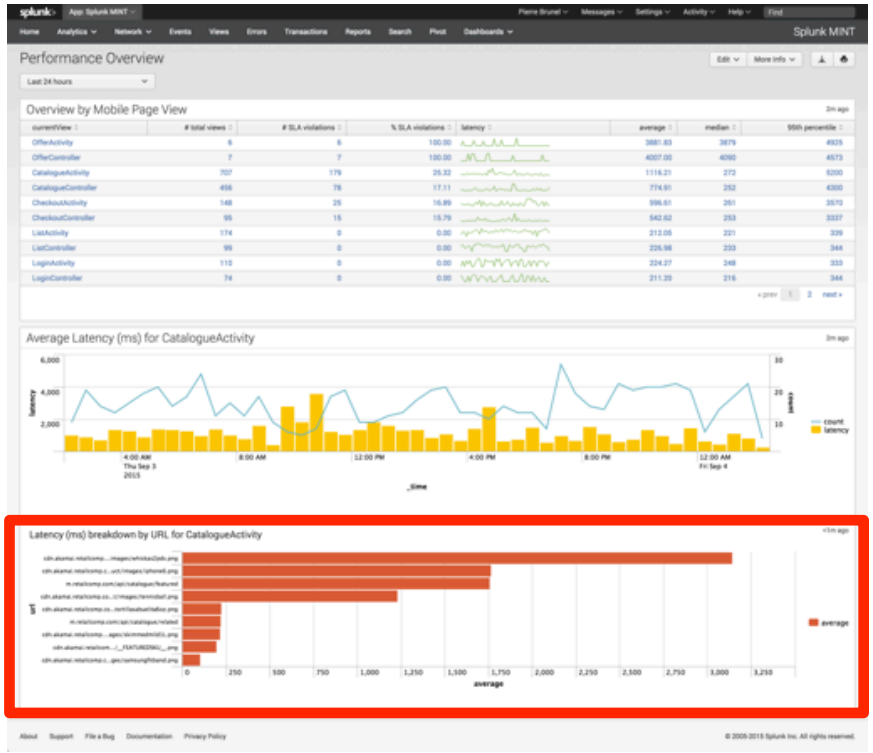



```
<row>
  <panel depends="$currentView$">
    <title>Average Latency (ms) for $currentView$</title>
    <chart>
      <search>
        <query>sourcetype=mint:network currentView=$currentView$
          | timechart count avg(latency) as latency</query>
        <earliest>$global_time.earliest$</earliest>
        <latest>$global_time.latest$</latest>
      </search>
      <option name="charting.axisY2.enabled">1</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart.overlayFields">count</option>
      <option name="charting.chart">column</option>
      <option name="charting.drilldown">all</option>
      <option name="charting.layout.splitSeries">0</option>
      <option name="charting.legend.placement">right</option>
      <selection>
        <set token="selection.earliest">$start$</set>
        <set token="selection.latest">$end$</set>
      </selection>
    </chart>
  </panel>
</row>
```

Select Subset of Timerange

```
<row>
  <panel depends="$currentView$">
    <title>Average Latency (ms) for $currentView$</title>
    <chart>
      <search>
        <query>sourcetype=mint:network currentView=$currentView$
          || timechart count avg(latency) as latency</query>
        <earliest>$global_time.earliest$</earliest>
        <latest>$global_time.latest$</latest>
      </search>
      <option name="charting.axisY2.enabled">1</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart.overlayFields">count</option>
      <option name="charting.chart">column</option>
      <option name="charting.drilldown">all</option>
      <option name="charting.layout.splitSeries">0</option>
      <option name="charting.legend.placement">right</option>
      <selection>
        <set token="selection.earliest">$start$</set>
        <set token="selection.latest">$end$</set>
      </selection>
    </chart>
  </panel>
</row>
```

Use Selected Timerange




```
<row>
  <panel depends="$currentView$">
    <chart>
      <title>Latency (ms) breakdown by URL for $currentView$</title>
      <search>
        <query>sourcetype=mint:network currentView=$currentView$
          | chart eval(round(avg(latency),1)) as average by url
          | sort -average</query>
        <earliest>$selection.earliest$</earliest>
        <latest>$selection.latest$</latest>
      </search>
      <option name="charting.axisY2.enabled">1</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart">bar</option>
      <option name="charting.chart.overlayFields">count</option>
      <option name="charting.drilldown">all</option>
      <option name="charting.layout.splitSeries">0</option>
    </chart>
  </panel>
</row>
```

Use Selected Timerange

```
<row>
  <panel depends="$currentView$">
    <chart>
      <title>Latency (ms) breakdown by URL for $currentView$</title>
      <search>
        <query>sourcetype=mint:network currentView=$currentView$
          | chart eval(round(avg(latency),1)) as average by url
          | sort -average</query>
        <earliest>$selection.earliest$</earliest>
        <latest>$selection.latest$</latest>
      </search>
      <option name="charting.axisY2.enabled">1</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart">bar</option>
      <option name="charting.chart.overlayFields">count</option>
      <option name="charting.drilldown">all</option>
      <option name="charting.layout.splitSeries">0</option>
    </chart>
  </panel>
</row>
```

Conclusion

- Greater depth in dashboards -> greater insight
- SimpleXML: powerful capabilities for the non-UI expert
- Work with your users
  - Which questions would they ask next?

Additional Reading

- Get the code
  - https://github.com/sirmonkey/conf2015
- Splunk Docs
  - http://docs.splunk.com/Documentation/Splunk/6.2.5/Viz/Visualizationreference
- Dashboard examples app
  - https://splunkbase.splunk.com/app/1603/
- Level up: Satoshi's conf talk "Enhancing Dashboards with Javascript!"
  - Wed 12:15 -> 1pm (Breakout 9)

Questions?

splunk>

THANK YOU

splunk>