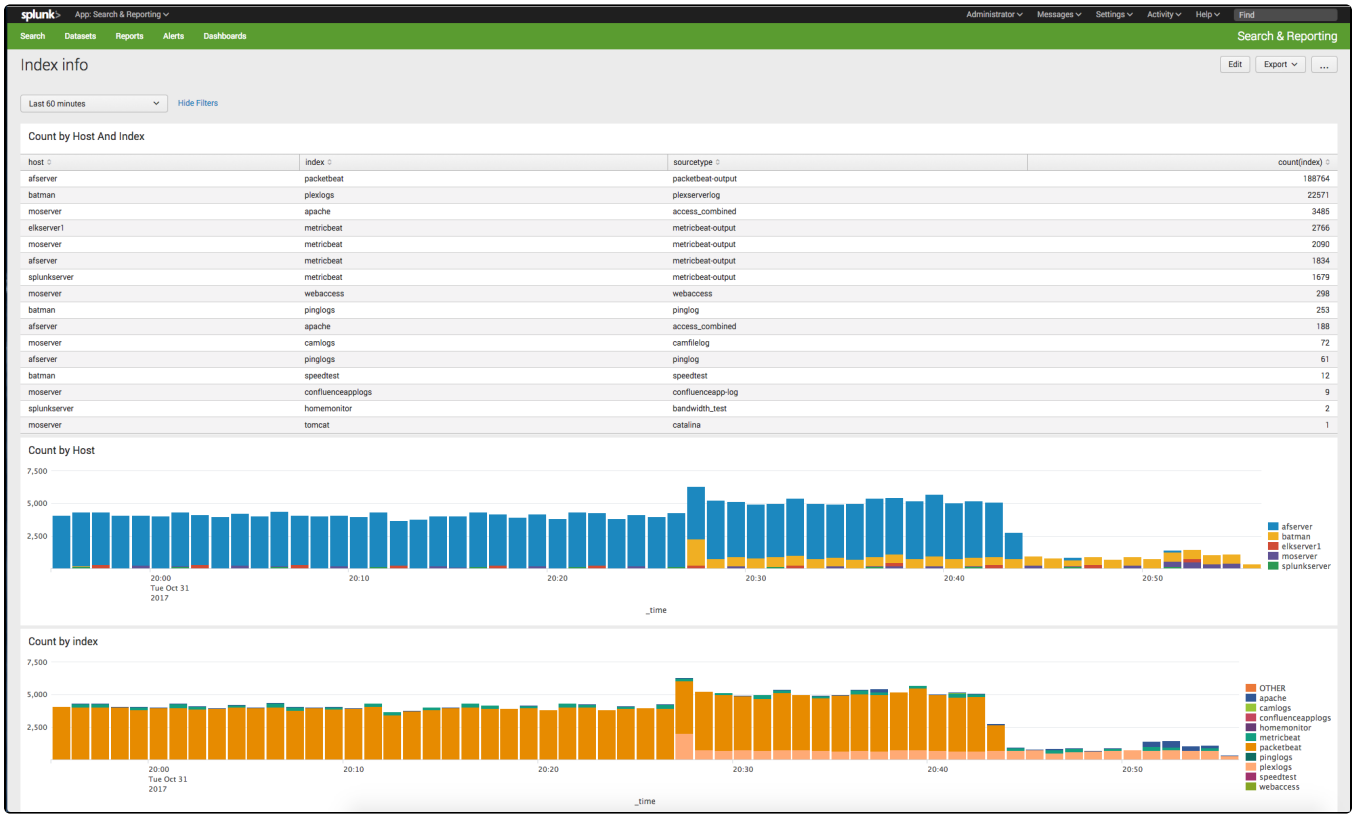
# Splunk - Index fillings

I am not impressed with the standard Splunk license info, when the filling of my indexes are more that the license allows; so I have build a simple Dashboard to find which indexes and from what server the filling is coming:




The dashboard shows the introduction of the PacketBeat from Elasticsearch and my Alfresco server (afserver), filling insane amounts into the index.

Code for the dashboard:

```
<form>
  <label>Index info</label>
  <fieldset submitButton="false">
    <input type="time" token="field1">
      <label></label>
      <default>
        <earliest>-24h@h</earliest>
        <latest>now</latest>
      </default>
    </input>
  </fieldset>
  <row>
    <panel>
      <title>Count by Host And Index</title>
      <table>
        <search>
          <query>index=* | stats count(index) by host index sourcetype| sort by -count(index)</query>
          <earliest>$field1.earliest$</earliest>
          <latest>$field1.latest$</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="count">100</option>
        <option name="dataOverlayMode">none</option>
        <option name="drilldown">none</option>
        <option name="percentagesRow">false</option>
        <option name="rowNumbers">false</option>
        <option name="totalsRow">false</option>
```

```
      <option name="wrap">true</option>
    </table>
  </panel>
</row>
<row>
  <panel>
    <title>Count by Host</title>
    <chart>
      <search>
        <query>index=* | timechart count(index) by host</query>
        <earliest>$field1.earliest$</earliest>
        <latest>$field1.latest$</latest>
        <sampleRatio>1</sampleRatio>
      </search>
      <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
      <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
      <option name="charting.axisTitleX.visibility">visible</option>
      <option name="charting.axisTitleY.visibility">visible</option>
      <option name="charting.axisTitleY2.visibility">visible</option>
      <option name="charting.axisX.scale">linear</option>
      <option name="charting.axisY.scale">linear</option>
      <option name="charting.axisY2.enabled">0</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart">column</option>
      <option name="charting.chart.bubbleMaximumSize">50</option>
      <option name="charting.chart.bubbleMinimumSize">10</option>
      <option name="charting.chart.bubbleSizeBy">area</option>
      <option name="charting.chart.nullValueMode">gaps</option>
      <option name="charting.chart.overlayFields">host</option>
      <option name="charting.chart.showDataLabels">none</option>
      <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
      <option name="charting.chart.stackMode">stacked</option>
      <option name="charting.chart.style">shiny</option>
      <option name="charting.drilldown">none</option>
      <option name="charting.layout.splitSeries">0</option>
      <option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>
      <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
      <option name="charting.legend.placement">right</option>
      <option name="trellis.enabled">0</option>
      <option name="trellis.scales.shared">1</option>
      <option name="trellis.size">medium</option>
    </chart>
  </panel>
</row>
<row>
  <panel>
    <title>Count by index</title>
    <chart>
      <search>
        <query>index=* | timechart count(index) by index</query>
        <earliest>$field1.earliest$</earliest>
        <latest>$field1.latest$</latest>
        <sampleRatio>1</sampleRatio>
      </search>
      <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
      <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
      <option name="charting.axisTitleX.visibility">visible</option>
      <option name="charting.axisTitleY.visibility">visible</option>
      <option name="charting.axisTitleY2.visibility">visible</option>
      <option name="charting.axisX.scale">linear</option>
      <option name="charting.axisY.scale">linear</option>
      <option name="charting.axisY2.enabled">0</option>
      <option name="charting.axisY2.scale">inherit</option>
      <option name="charting.chart">column</option>
      <option name="charting.chart.bubbleMaximumSize">50</option>
      <option name="charting.chart.bubbleMinimumSize">10</option>
      <option name="charting.chart.bubbleSizeBy">area</option>
      <option name="charting.chart.nullValueMode">gaps</option>
      <option name="charting.chart.overlayFields">host</option>
      <option name="charting.chart.showDataLabels">none</option>
      <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
```

```
        <option name="charting.chart.stackMode">stacked</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">none</option>
        <option name="charting.layout.splitSeries">0</option>
        <option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>
        <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
        <option name="charting.legend.placement">right</option>
        <option name="trellis.enabled">0</option>
        <option name="trellis.scales.shared">1</option>
        <option name="trellis.size">medium</option>
      </chart>
    </panel>
  </row>
</form>
```