Trends in application errors over time

Most applications are coded to emit errors, warnings, and other problems to log files as they occur. It’s not uncommon for applications to continuously emit a steady stream of errors. However, sudden increases in the volume of errors or a rise in error volumes over time might be a sign of a problem with the application. You want to monitor for spikes.

Data required

Application server data

Procedure

1. Check that you have correctly installed and configured an application performance monitoring add-on.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   host = <host to look at>
   (error OR fail* OR warn)
   | timechart span=5m count

Search explanation

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>host=&lt;host to look at&gt;</td>
<td>Search a specific host.</td>
</tr>
<tr>
<td>(error OR fail* OR warn)</td>
<td>Find any application log events containing words such as “error”, “fail*”, or “warn”.</td>
</tr>
<tr>
<td></td>
<td>timechart span=5m count</td>
</tr>
</tbody>
</table>

Next steps

The result of this search is a bar chart that shows the frequency of errors over time. This is useful to see if errors occur more frequently at certain times. If so, look for a correlation with load or release dates of new code or patches.

Additionally, you might need to detect trends in application errors over time when using stack traces to detect application errors.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.