Application error tracing

Your application support team wants to use the Splunk platform with web access logs to see what errors occur. You need to make sure your deployment is configured correctly and create a search they can use.

Data required

Application server data

To complete this process, your deployment needs to ingest normalized data, populating the Web data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

Procedure

1. To verify you are searching for normalized web data, run the following search. You can optimize it by specifying an index and adjusting the time range.

   ```splunk
   earliest=-1d index=* tag=web
   | head 10
   ```

2. Do one of the following:

   • If you do not receive results, check that you have correctly installed and configured a web data add-on, such as Splunk Add-on for Apache Web Server or Splunk Add-on for Microsoft IIS.

   • If you receive results, run the following search:

   ```splunk
   tag=web status>=400
   | stats count BY uri_path, status
   | sort limit=20 -count
   ```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag=web</td>
<td>Search for events that are tagged as web events.</td>
</tr>
<tr>
<td>status&gt;=400</td>
<td>Search for statuses greater than or equal to 400.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats count BY uri_path, status</td>
<td>Count the number of events and group them by URI and status.</td>
</tr>
<tr>
<td>sort limit=20 -count</td>
<td>Sort the top 20 results with the largest count first.</td>
</tr>
</tbody>
</table>

**Result**

You can use this information to troubleshoot production issues for users and identify areas to improve navigation or performance.

You might want to chart key metrics related to application performance when monitoring web application performance.