Web hosts with HTTP error status codes

Recently, the data from your web server has shown an increase in error codes. You want to determine which hosts are generating the errors so you can resolve the problems.

Data required

Web server data

Procedure

1. Ensure you are ingesting web server data. This sample search uses the Splunk Add-on for Apache Web Server, but you can replace this source with any other web server data used in your organization. For more information, see About installing Splunk add-ons.

2. Verify you deployed a web server add-on to the search heads, so that the needed tags and fields are defined.

3. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   ```
   tag=web status>200 |stats count AS "Bad Status Codes" BY host |sort - "Bad Status Codes"
   ```

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;200</td>
<td>Search for events with a status of greater than 200.</td>
</tr>
<tr>
<td></td>
<td>stats count AS &quot;Bad Status Codes&quot; BY host</td>
</tr>
</tbody>
</table>
Splunk Search

|sort - "Bad Status Codes"

Explanation

Sort the results with the highest count of error codes first.

Next steps

Knowing which hosts generate the highest number of error codes is useful for focus troubleshooting efforts. After running this search, you can drill into each host and sort by most common error codes to further focus the troubleshooting.

You might be interested in other processes associated with the Managing web server performance use case.