Trends in web server response codes

Subtle problems introduced by regular software releases, system patching, configuration changes, and other production changes often go undetected if not monitored. You want to graph the distribution of response codes over time in order to perform long-term trending of site performance to identify problems. Additionally, you want a visualization to validate that a major production change hasn't inadvertently increased the overall number of errors or decreased the overall number of successes users experience.

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=*
|eval status_group=case(status<300, "2xx", status<400, "3xx", status<500, "4xx", status<600, "5xx", true(), unknown)
|timechart span=1h count BY status_group
```

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=*</td>
<td>Return all page requests that have an HTTP status.</td>
</tr>
</tbody>
</table>
### Splunk Search
```
|eval status_group=case(status<300, "2xx", status<400, "3xx", status<500, "4xx", status<600, "5xx", true(), unknown)
```

### Explanation
Group status codes together by 200s, 300s, 400s, and 500s.

```
|timechart span=1h count BY status_group
```

Graph the trend of status codes over time in 1-hour increments.

---

**Next steps**

If the majority of status codes are in the 2xx range, your web server is performing well. An increase in 4xx and 5xx codes, which indicate errors, would warrant further investigation.

A good next step is to search for error codes and count by server, url, or other term that could help isolate the cause of the error.

You can also use synthetics to monitor response codes and times.

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