Distribution of web traffic across servers

In a farm of web servers behind a proxy server, you can reasonably expect near-uniform behavior from each web server. A single server that processes traffic differently than other servers is an indication that something has gone wrong with that server or with the proxy server distributing traffic. You want to monitor your servers for these issues.

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.

   ```splunk
   tag=web |timechart span=15m count BY host useother=f
   ```

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></td>
<td>timechart span=15m count BY host useother=f</td>
</tr>
</tbody>
</table>

Next steps

An even distribution of traffic across hosts is ideal. If one of the lines in the timechart plots much differently than the
others, you might have a load balancing problem. A good next step is to understand the load balancing algorithm to help determine why traffic is not balanced. For example, a round-robin algorithm may indicate dropped connections at the network interfaces, while a least connections algorithm would suggest a server being too slow to handle its fair share of the load.

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