Number of current users on a website

Active users provide a real-time measurement of load on the system, which can be helpful in multiple circumstances. If active users are low, for example during the early morning hours, it may be appropriate to proceed with a maintenance activity that could result in downtime or user disruption. Similarly, tracking active users during known peak times helps to gain an appreciation for the use of the system and the impact unexpected degradations can have on the user base. For these reasons, you need a search that can provide active user counts.

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. If you’re using The Splunk Add-on for Apache Web Server, make sure to configure log formatting on the Apache Web Server as described in the following link. This step will make sure you have all the required fields present in apache_access.log and especially the response time value needed for this procedure. For detailed configuration steps, see Configure log formatting on the Apache Web Server using httpd.conf.

3. Verify you deployed a web server add-on to the search heads, so that the needed tags and fields are defined. For more information, see About installing Splunk add-ons.

4. Choose a critical page on your site to filter on.

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

```
tag=web
site=<URL of critical page>
|eval unique_user_info = src_ip.http_user_agent
|timechart span=15m aligntime=now dc(unique_user_info)
```

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>
</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>site=&lt;URL of critical page&gt;</td>
<td>Search only the site you want to see the number of users on. For example, site=www.mysite.com.</td>
</tr>
<tr>
<td></td>
<td>eval unique_user_info = src_ip.http_user_agent</td>
</tr>
<tr>
<td></td>
<td>timechart span=15m aligntime=now dc(unique_user_info)</td>
</tr>
</tbody>
</table>

**Result**

The search produces a line chart that shows unique users, as described above. It gives a visual of concurrent users over time and visualizes peaks and valleys over time. The timeframe should be selected according to organizational needs. It can be limited to only working hours, business days, or weekends. Concurrent usage is often useful for capacity planning or measuring interest in the content the site presents.