Trends in database query counts

While the number of queries executed against the database varies by hour of day and day of week, you want to monitor for growth in the overall number of calls to the database, either gradual or sudden.

Data required

Database data

Procedure

1. Verify that you have deployed Splunk Stream.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   |timechart span=1h count
   |`lineartrend(_time,count)`
   |rename newY AS lineartrend
   |fields _time count lineartrend

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><code>timechart span=1h count</code></td>
<td>Graph the count of database queries over time in 1-hour increments.</td>
</tr>
<tr>
<td>`</td>
<td><code>lineartrend(_time,count)</code></td>
</tr>
<tr>
<td>`</td>
<td>rename newY AS lineartrend`</td>
</tr>
<tr>
<td>`</td>
<td>fields _time count lineartrend`</td>
</tr>
</tbody>
</table>
Next steps

The results are displayed as a timechart where the query count is plotted over time with a second overlaid line representing the trend. This trendline is the linear regression of the count values and makes it easier to see overall trending of the counts. This is helpful with randomly distributed data or data that is bursty. In those cases, the regression line will clearly show positive, negative, or flat trends in the data.

Unanticipated growth may occur for several reasons, such as increased demand for the data, addition of new workloads, or changes to the client software due to patching or new releases. If unanticipated growth is detected, review upstream changes between the database and the client to determine if the growth is appropriate.

Another use of the trendline is to correlate query counts with other changes in the environment. For example, increasing query counts can positively affect other metrics, such as query response time or the query duration, such that response time trends up as query counts go up. You can use the steepness of the trend line to predict when query counts might affect other metrics, such as response time or transaction duration. A simple way to correlate these is to have the related metrics displayed side by side on the same dashboard.

Since trend data is used to predict the value of a metric at a future time, you can also use the `predict` command in Splunk SPL:

```
| timechart span=1h count(query) AS count
| predict count
```

By default, the predict command displays a line for the actual query counts, the predicted query counts, and bands that represent the upper and lower 95th percentile predictions. The predict command has many options including different predict algorithms and future timespan length. Note that the lineartrend macro, fields, and rename commands are not needed with the predict command.

Finally, you might also want to look at similar searches in our article [Analyzing wire data from databases](https://www.example.com).