Trends in database query response times

Gradual performance degradations introduced by regular software releases, increasing database load, or under provisioned hardware often go undetected if they are not monitored. You want to use the average response time of all queries into the database to understand long term trending of database query performance and identify problems.

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.

```
| eval time_taken_sec = time_taken / 1000000
| timechart span=1h avg(time_taken_sec) AS avg_time_taken_sec
| `lineartrend(_time,avg_time_taken_sec)`
| rename newY AS lineartrend
| fields _time avg_time_taken_sec 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>eval time_taken_sec = time_taken / 1000000</code></td>
<td>Convert microseconds to seconds for readability.</td>
</tr>
<tr>
<td><code>timechart span=1h avg(time_taken_sec) AS avg_time_taken_sec</code></td>
<td>Graph the average time taken for database queries in 1-hour increments.</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td><code>lineartrend(_time,avg_time_taken_sec)</code></td>
<td>The punctuation surrounding a Splunk macro is always</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.
Next steps

The results returned are displayed as a timechart where the actual average values are plotted over time with a second straight line representing the trend. The slope of the trendline shows the linear regression and how the average time taken is trending. This is helpful when data is randomly distributed over time or 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 average response time with other changes in the environment. For example, how does average response time change with changes in concurrent users or query count? You would expect a positive relationship such that response time trends up as users trend up. The steepness of the trend line can be used to predict when future average response time will fall below an acceptable limit. That predicted time frame can be used to plan future actions.

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:

```
| eval time_taken_sec = time_taken / 1000000
| timechart span=1h avg(time_taken_sec) AS avg_time_taken_sec
| predict avg_time_taken_sec
```

By default, the predict command displays a line for the actual average time taken in second, the predicted `avg_time_taken`, 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](#).