Troubleshoot service problems using ITSI Service Analyzer

When a service is non-responsive or not running as intended, it’s essential to be able to quickly identify the root cause of the problem. The Service Analyzer within Splunk ITSI lets you do that by showing metrics for your services that you can drill down into to access different levels of detail. These metrics are:

- **The Service Health Score (SHS).** This is an overall score for each service based on the health scores of all of its KPIs, and ranges from 0-100 (0 being critical and 100 being normal.) Within Splunk ITSI, services are color-coded using a traffic-light system according to their SHS. The health of a service is affected by the health of a child service.

- **KPIs.** KPIs are searchable performance metrics, such as CPU load percentage, and any valid business metrics like revenue. Individual services can have multiple KPIs - for example, Database KPIs could include % Memory Used, % CPU Used, % Disk Space Used or Database Queries.

1. Open the Splunk ITSI app. By default, this app opens on the Service Analyzer Tree View. If you're in Tile View, access the Tree View by clicking the Tree button.

2. You can now see a hierarchy of all of your services. You can use the zoom tool as well as click and drag to focus on specific parts of the hierarchy.

3. Change the search timeframe at the top-right of the screen to choose what time period you want Service Analyzer to display. The timeframe you choose impacts the values of the KPI and SHS metrics shown.
4. Services here are color-coded to help you identify services that are performing outside of their SHS values. Hover over a service to highlight its dependencies, then click on the service to see more detail.

5. You can see the service's metrics on the right-hand side of the screen:
   - The SHS is in the header of this area, along with a sparkline view, giving you an idea of how it has changed over time.
   - Individual KPIs for the service are shown below this. You can see a current value plus a sparkline view for each KPI.

View entities of a KPI

KPIs can be split by field into entities. These can help you troubleshoot service problems by providing more context and detail in your investigations. Some common entity splits you might see include:

<table>
<thead>
<tr>
<th>Split</th>
<th>Helps to determine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>A specific server has become unhealthy.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The problem is limited to how users are connecting.</td>
</tr>
<tr>
<td>Region</td>
<td>A data center, ISP, or regional dependency is unhealthy.</td>
</tr>
<tr>
<td>Client</td>
<td>An important customer or client is affected.</td>
</tr>
<tr>
<td>Version</td>
<td>A recent software change or patch is to blame.</td>
</tr>
<tr>
<td>URI</td>
<td>The problem is limited to a certain API, webpage, or endpoint.</td>
</tr>
</tbody>
</table>
When viewing a service, click the KPI to access its entities and their values.

Deep dive into service KPIs

Deep diving into service KPIs means you can gather more information about how they have changed over a period of time. The deep dive view also lets you correlate KPIs from different services.

1. From the service view, click **Open all in Deep Dive**.

2. Mouse over swim lanes to access the vertical timeline.

At this point, you may want to search for and add the most appropriate KPI from another service into your deep dive to determine if changes in each are correlated.

1. From the Deep Dive view, using the Bulk Actions menu at the top-left of the screen, delete any KPIs you want to remove from the view.
2. Click **Add Lane**, then click **Add KPI Lane**.
3. Select the service you want to correlate, then select its KPI, and click **Create Lane**.

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.
Deep dive views can be saved so you can refer back to a deep dive that you’ve previously created or customized. Select the **Save As** button at the top of the deep dive view to do this. Access saved deep dives from the Deep Dive menu within the Service Analyzer toolbar.

**Next steps**

These additional Splunk resources might help you understand and implement these recommendations:

- Splunk Docs: [Overview of the Service Analyzer in ITSI](#)