Extracting insights from InfraMon

Visualizations

• Leverage built-in content. Built-in content provides you with immediate visibility and value right out of the box. All you need to do is send your data in.
  ◦ The Infrastructure Navigator (found in Navigation menu > Infrastructure) provides a high-level overview of the related infrastructure entities: Public Clouds, Containers, and My Data Center. From there, you are able to drill down into each entity’s specific dashboard to aide in your deeper investigation. All of this is provided right out of the box. Use these to aide in your troubleshooting workflows as well as to get inspiration for more custom visualizations.
  ◦ Built-In dashboard groups (found in Navigation menu > Dashboards) are applicable to a wide variety of technologies and services. These dashboards give you immediate visibility into the technologies and services being used in your environment. Built-in dashboards, and the charts they contain, are read-only. They are automatically created in your organization if you deploy any of the integrations listed on the Data Setup page. When trying to modify a built-in dashboard, first copy and save it as a new dashboard, then you will be able to modify the copy.

• Create custom charts and dashboards.
  ◦ Charts enable you to visualize the metrics you are sending in to Splunk Infrastructure Monitoring. A metric is anything that is measurable (you can assign a numerical value to it) and variable (changes over time). Charts can range from extremely simple (monitor a single metric for a single host in real time) to very sophisticated (apply advanced analytic formulas across several dimensions, compare values for different time periods, configure advanced display settings, and more). You can find a chart terminology quick reference here. Consider the following when creating a chart.
    ▪ What metrics do you want to track?
    ▪ How might you want to customize some default settings?
    ▪ How you can create this chart -- is there an existing template you can work from, or copy an already existing chart and then modify, or create from scratch?
  ◦ Dashboards are logically grouped collections of charts. Well-designed dashboards can provide useful and actionable insight into your system at a glance. There are three kinds:
    ▪ Built-in dashboards. We’ve touched on these already. These cannot be modified and automatically populate with data once data is flowing in.
    ▪ Custom dashboards. Tailored/custom dashboards grouped together logically or for a specific purpose. Remember that dashboards are meant to provide you insight at a glance so keep this in mind when creating dashboards and organizing them into groups.
    ▪ User dashboards. These are dashboard groups organized each user account in your instance. Their created dashboards will be found in their specific user dashboard group.
Alerts

• Create detectors. Detectors are the configurable resources in-app that monitor metrics on a plot line, trigger alert events, and clear events based on conditions you define in rules. You have a number of starting points when creating a detector -- you can: clone an existing detector, create a detector from a chart, or create from the API. An important concept with detectors is that you are essentially creating a chart for the analytics engine to analyze and monitor, so keep that in mind when creating these. If you want to alert off an important chart you just created, create the detector from that chart. You can also create a detector from scratch in the UI. When doing so, you must establish:
  ◦ Detector rules.
    ▪ When the detector will be triggered, based on conditions related to the detector’s signal/metric
    ▪ The severity of the alert to be generated by the detector
    ▪ Where notifications should be sent
    ▪ Type. Choose what type of detector to create: APM Metric or Infrastructure/Custom Metric.
    ▪ Alert Signal. Decide what metric are you trying to alert on and apply filters, analytics, and formulas.
    ▪ Alert Condition. Define the conditions of the signal/metric in which you would like to be alerted on. A straightforward example is ‘Static Threshold’ or ‘Heartbeat check’ and a more complex example is ‘Custom Threshold’ where you can compound conditions using AND or OR logic.
    ▪ Alert Settings. These settings will depend on which condition is selected and will be configured at this step.
    ▪ Alert Message. Define the severity of the alert and customize the message of it. Can also link to helpful documentation to be delivered with the alert.
  • View alerts. The Alerts page gives you a holistic view into active alerts. You can also filter alerts to zero-in on the most critical active issues. Click any item in the list to view details about the alert. In the details popup, you can click Resolve to set the alert’s status to “Resolved,” click View in detector to open the detector that triggered the alert (see Viewing active alerts for a specified detector), or click Close to return to the alerts list.
  • Filter alerts. You can click on any of the five large alert counters to drill down into alerts of that single severity level; a filter for severity level is added. You can also use the Filter field to show only alerts that are relevant to particular tags or dimensions.

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.