Splunk Infrastructure Monitoring

Implementation reference guide

This resource is designed to provide implementation guidance to customers just getting started with Splunk® Infrastructure Monitoring. Think of this as an easy to digest guide for implementations, training and services, and best practices.

Work through this entire guide at your own pace, applying these learnings to your infrastructure monitoring environment as you go.

Concepts and Value Proposition

To make the most of your investment in Splunk Infrastructure Monitoring, it's important that you understand some core concepts and the value this product/technology aims to deliver.

What is Splunk Infrastructure Monitoring?

Splunk Infrastructure Monitoring is a real-time, analytics-driven multicloud monitoring solution. Create robust visualizations, and alert on your organization's infrastructure metrics.

What problems does Splunk Infrastructure Monitoring help solve?

Splunk Infrastructure Monitoring helps organizations stay on top of the health and performance of their technology infrastructure. Splunk IM's streaming architecture will detect issues in real time, allowing for faster recovery and minimized impact on end user experience.

What are some business initiatives Infrastructure Monitoring ties into?

- Make the most of the benefits of cloud adoption.
- Meet elevated SLAs for availability and uptime, including real-time alerts.
- Real-time visibility fosters innovation.

How does it work?

Through integrations with cloud providers, and the deployment of an OpenTelemetry agent, Splunk IM collects infrastructure data/metrics. The streaming analytics engine processes and analyzes the data for visualizations and alerting.

What does adoption of Infrastructure Monitoring look like?

Infrastructure Monitoring alerts customers, in real time, of any issues that may be occurring in their infrastructure. Splunk IM helps customers answer the question "Do I have a problem?" and then alerts customers of the problem in real time via Splunk IM's detectors, which are powered by streaming analytics. For customers to adopt this product and gain value they must: send data into Splunk IM via integrations/agents with cloud providers/services, create dashboards and visualizations to make sense of all their data, and then create detectors in order to be alerted on this data at the desired thresholds important to the customer's use case(s).

What are some outcomes we can expect from implementing Splunk Infrastructure Monitoring?

- Case Study: Mark43 Depends on Splunk to Keep Its Law Enforcement Technology Always Available
- Case Study: Acquia Transforms Customer Experience With Real-Time Problem Resolution

Where can I go to get more help? — See Support Section of this document

- Open a Support Case — signalfx-support@splunk.com or within the Support Portal (which can be found in settings in-app)
- In-App Chat
- Documentation + More (Use sidebar and search to navigate) and Splunk Lantern

Implementation

Infrastructure Monitoring implementations consist of four high-level phases: Getting Data In + Training, Visualizations, Alerting and Administration. Customers must start with Getting Data In + Training…

Getting Data In + Training

To begin, let's start with Getting Data In (GDI).

In order to start sending data in, you will need to:

- Connect Cloud Services — Connect Splunk Observability Cloud to your cloud service provider to collect data from supported cloud services in AWS, GCP or Azure. If you don't use cloud services or don't want Splunk Observability Cloud to collect data from them, skip to the next step. You don't have to connect to cloud services to monitor hosts or Kubernetes clusters that run in cloud services, but connecting your cloud account is the only way to collect cloud metadata.
  - To connect to a cloud service, select **Navigation menu > Data setup** and search for the cloud service you want to connect to.
    - For detailed steps on connecting cloud services to Splunk Observability Cloud, see these pages: Connect to AWS, Connect to GCP and Connect to Azure
- Collect infrastructure data with an OpenTelemetry Collector — Splunk Observability Cloud supports integrations for Kubernetes, Linux and Windows. Integrations for these data sources help you deploy a Splunk OpenTelemetry Collector to export metrics from hosts and containers to Splunk Observability Cloud.
  - Using the Splunk OpenTelemetry Collector is optional; however, you get higher-resolution data using the collector than from cloud integrations.
    - See these pages for more information about sending host or container metrics to Splunk Observability Cloud: Collect Kubernetes data, Collect Linux host data and Collect Windows host data

Need extra help with Getting Data In?

There is an OnDemand Services task you can request to help unblock you:

- OTel Collector Configuration Guidance
- Smart Agent for Single Integration Configuration Guidance

Additionally … here is a list of ALL supported data sources, and how to integrate them, for your reference.

Once you have completed the setup for Getting Data In, you can verify by leveraging the built-in content found in-app. To view the Infrastructure Overview, select **Navigation menu > Infrastructure**. If your data has populated there, you have successfully completed this step.

Don't forget about training, so you can make the most out of Infrastructure Monitoring. Start with this FREE self-paced eLearning.

Visualizations

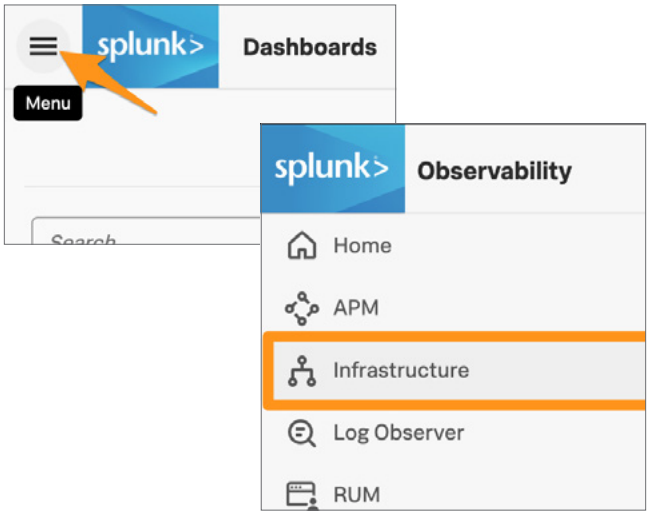
Now that we have our data being sent in, let's focus on visualizations — charts and dashboards — to make sense of this data. Out of the box, there's a bunch of great built-in content to make use of, but let's also create custom visualizations.

Built-in content

If you followed the previous steps with Getting Data In (GDI), you should have already used the built-in content to verify successful setup of GDI. 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.

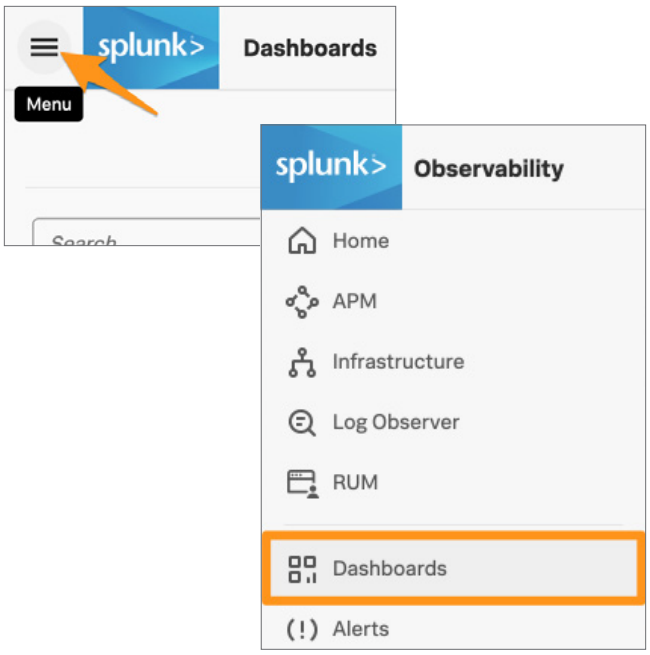
Infrastructure navigator:
Navigation menu > Infrastructure

Each of the "navigators" — Public Clouds, Containers and My Data Center — will provide you with a high-level overview of the related infrastructure entities. From there, you can drill down into each entity's specific dashboard for deeper investigation. Use these to aid in your troubleshooting workflows as well as to get inspiration for more custom visualizations.



Built-in dashboard groups:
Navigation menu > Dashboards

Infrastructure Monitoring provides built-in dashboards for a wide variety of technologies and services. These dashboards give you immediate visibility into the technologies and services 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.



Custom charts and dashboards

Charts enable you to visualize the metrics you are sending into 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.

Dashboards are logically grouped collections of charts. You'll want to create dashboards that help you answer a question at a glance. Before we get into dashboards, let's focus on charts and creating them…

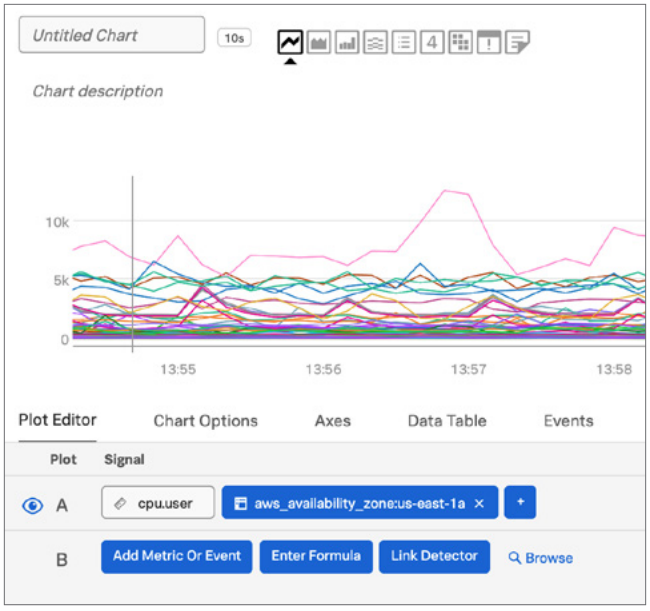
Planning a chart

Before creating a chart, you should first think about what metrics you want to track. Also, consider ways in which you might want to customize some default settings. From there, think about how you can create this chart: Can you work from an existing template, copy an already existing chart and modify or create from scratch? To search for Metrics select **Navigation Menu > Metrics > Metric Finder** and search.

Creating a chart

Use Chart Builder to create a chart from scratch.

- To create a new chart, locate the + sign (create button) in the top right corner of the UI and select "Chart."
- Within the Chart Builder you can set parameters like:
  - **Name of Chart and Description** — Give it something useful and intuitive.
  - **Metrics** — Within the "Plot Builder" you can search for and select which metrics to plot.
    - **Filters** — Apply filters like environment or cluster to zero in on the desired metric and dimensions.
    - **Analytics** — Apply analytics to further fine tune how the selected metric is plotted.
    - **Formulas** — Craft a formula using multiple metrics.
- Furthermore, additional options can be found under "Chart Options:"
  - **Visualization Type** — What is the best way to visually represent the metrics and their context? Maybe a heatmap, single value, list, histogram, line or even area chart and others.
  - **Advanced Options** — Configure Max Delay and Minimal Resolution.
- Leverage all of these options to fine tune your chart and make it exactly what you need.



Need extra help with Visualizations?

There is an OnDemand Services task you can request to help unblock you:

- Assist with Building a Simple Dashboard or Charts
- Assist with Building an Advanced Dashboard or Charts
- Chart or Dashboard Optimization

Copying a chart

To copy a chart, locate the chart you wish to copy, then select the "three dots" button in the top right corner of the chart, then select "Copy."

Copying a chart can help speed up the new chart creation process and can serve as a way of templating certain charts.

Dashboards

Dashboards are groupings of charts and visualizations of metrics. Well-designed dashboards can provide useful and actionable insight into your system at a glance. To view all dashboard groups — Built-In, Custom and User — and their associated dashboards, go to **Navigation menu > Dashboards**.

- Built-In Dashboards — we've touched on these already. They cannot be modified and automatically populated 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 will be dashboard groups organized for each user account in your instance. User created dashboards will be found in their specific user dashboard group.

Alerting

At this point, we have data flowing in, and our built-in and custom visualizations are populating and providing insights to us at a glance. Now, let's focus on what will notify us of issues and anomalies …

Detectors

Detectors are the configurable resources in-app that monitor metrics on a plot line, or on a chart, and trigger alert events and clear events based on conditions you define in rules.

Creating detectors

You have a number of starting points when creating a detector — you can: clone an existing detector, create a detector from a chart, create from the API or simply create a detector from scratch in the UI.

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 a chart you just created, create the detector by navigating to that chart, select the "Bell" icon, and select "Create Detector from Chart."

Let's also focus on creating your first detector from scratch, just so you get a feel for all the parameters involved.

So, what can you configure within a detector? Detectors contain rules that specify:

- 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

To create a new detector from scratch, you can either click the New Detector button on the Alerts or Detectors tab on the Alerts page, or select Detector from the Create menu (plus sign) on the navigation bar.

From there, begin setting up your detector parameters:

- **Type** — Choose what type of detector to create: APM Metric or Infrastructure/Custom Metric.
- **Alert Signal** — What metric are you trying to alert on? You'll find this interface to be similar to the Chart Builder interface. You'll be able to 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. You can also link to helpful documentation to be delivered with the alert.
- **Alert Recipients** — Define who will receive the alert and the delivery method — email, Splunk On-Call, Slack, PagerDuty, Webhook, etc.

Alerts

The Alerts page will give you a holistic view into active alerts. You can also filter alerts to zero-in on the most critical active issues.

Alert details

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.

Filtering 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.

Notifications

To get the most out of the real-time streaming nature of Splunk Infrastructure Monitoring you'll likely want to integrate it with another service for notification, like Splunk On-Call, PagerDuty or Slack. Doing so will help you respond more efficiently.

You can find all of the instructions on integrating with notification services here.

Administration

Now that we have the core components all squared away, let's focus on administration. It's important for you to know how to best manage the tool in order to optimize usage throughout your organization.

You can find all of the documentation for administration-related activities here, but let's touch on a few important ones to be aware of as you get started:

- Create and manage users — Add users to the instance and begin onboarding their data.
- Create and manage access tokens — Use authentication tokens to authenticate Splunk Infrastructure Monitoring API requests, track API usage and control your use of resources.
- System Limits for Infrastructure Monitoring — System limits help ensure good performance, stability and reliability. It is important to simply be aware of these.
- Manage permissions for detectors, dashboard groups and dashboards.

Training

Splunk offers a number of EDU training courses to help you get up to speed on how to make the most of Infrastructure Monitoring. Completion of these courses is an essential building block to success. If you'd like to explore education options here, please get in touch with us via this contact form or get in touch with your account manager.

Infrastructure Monitoring Course Offerings

Course	Duration	SREs and DevOps	Developers
Introduction to Splunk Observability	Free eLearning	✔	✔
Introduction to Splunk Infrastructure Monitoring	Free eLearning	✔	✔
Splunk Infrastructure Monitoring Fundamentals	4.5 hours	✔	✔
Visualizing and Alerting in Splunk Infrastructure Monitoring	4.5 hours	✔	
Automation Using the REST and SignalFlow API	9 hours	✔	
Using the Splunk IM Terraform Provider	9 hours	✔	
Kubernetes Monitoring with Splunk Infrastructure Monitoring	4.5 hours	✔	
Ingesting Application Metrics in Splunk Infrastructure Monitoring	4.5 hours		✔

Infrastructure Monitoring Course Offerings and Prices

Course	Individual		Dedicated Virtual Class		Dedicated Onsite Class	
Introduction to Splunk Observability	Free eLearning	N/A	N/A	N/A	N/A	N/A
Introduction to Splunk Infrastructure Monitoring	Free eLearning	N/A	N/A	N/A	N/A	N/A
Splunk Infrastructure Monitoring Fundamentals	$500	1 Credit	$3,000	6 Credits	$4,000	8 Credits
Visualizing and Alerting in Splunk Infrastructure Monitoring	$500	1 Credit	$3,000	6 Credits	$4,000	8 Credits
Automation Using the REST and SignalFlow API	$1,000	2 Credits	$6,000	12 Credits	$8,000	16 Credits
Using the Splunk IM Terraform Provider	$1,000	2 Credits	$6,000	12 Credits	$8,000	16 Credits

Helpful links:

- Courses for Splunk Observability Customers
- Introduction to Splunk Infrastructure Monitoring (free eLearning)

Professional Services

Splunk's experts are here to help achieve the outcomes that are important to your organization. There are several ways to access our experts: through OnDemand subscription services or traditional project-based services. We make it easy to get you the help you need in whatever way works for you.

OnDemand Services

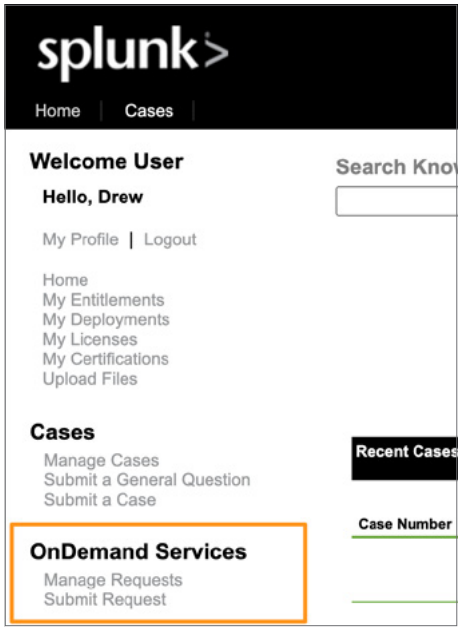
OnDemand Services (ODS) provides proactive technical adoption, implementation and optimization assistance for Splunk deployments, using a pool of remote technical consultants. ODS credits are required in order to consume ODS and the scope of ODS activities/tasks are predetermined. ODS can be requested within the Splunk Support Portal.

OnDemand Services Catalog for Observability:

Tasks: Observability Cloud, Infrastructure Monitoring (IM), APM, Log Observer (LO)			
All Products: • Use Case Advisory Discussion • Architecture Diagram Creation **APM/IM/Cloud:** • Cloud Migration Assessment	**APM/IM/Cloud:** • Post Implementation Review • Smart Agent for Single Integration Configuration Guidance • OTel Collector Configuration Guidance **Log Observer:** • FluentD Configuration • Log Processing Rule Configuration • Metricization Rule Configuration • Infinite Logging Configuration	**APM/IM/Cloud:** • Create a Simple Detector • Create an Advanced Detector • Assist with Building a Simple Dashboard or Charts • Assist with Building an Advanced Dashboard or Charts **Cloud:** • Getting Started with Splunk Observability Cloud **IM:** • Getting Started with Splunk Infrastructure Monitoring • Assist with Exporting Data • Assist with a Supported Cloud Integration • Assist with a Supported Library Configuration • Assist with the Configuration of prometheus-exporter **APM:** • Create Custom Span Tags • Assist with Auto-instrumentation	**APM/IM/Cloud:** • Usage Assessment • Dashboard Administration Assistance • Chart or Dashboard Optimization • Detector Optimization

How to request OnDemand Services:

- Ensure your organization has ODS credits to use — if you do not, please get in touch with your Splunk point of contact to discuss how to purchase.
- Log in to the Splunk Support Portal.
- Use the navigation on the left to locate the OnDemand Services section and proceed with submitting your request.



Helpful Links:

OnDemand Services Overview Video

Project-Based Services

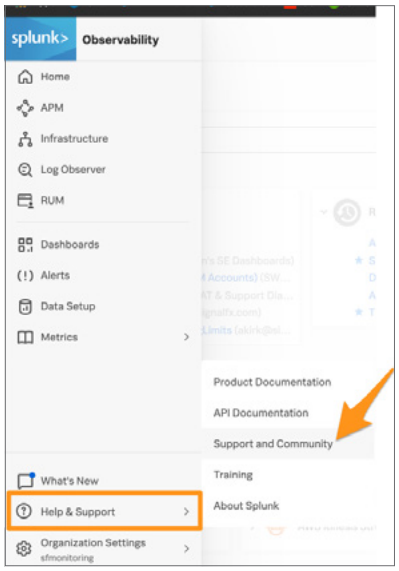
Project-Based Services are much more involved, typically larger scale, services engagements compared to ODS. With these, you will work with a Splunk Engagement Manager to determine and finalize the scope of the project. Once everything is signed off on, we will work with you in lockstep to deliver on the agreed-upon project. If you'd like to explore options here, please get in touch with us via this contact form or get in touch with your account manager.

Support

Even the most savvy customer will need a little help. Whether it's error messages, unexplained or unexpected behaviors, or incidents and outages, Technical Support is the first line of defense for all of your post-sales issues. Our Splunk Support Engineers will partner with you to ensure your environment is optimized to drive your journey with a focus on long-term technical health, so you can realize your ROI as soon as possible.

How to open a Support Case:

- Support Portal: This can be accessed from the application UI. To navigate to, bring up the navigation menu, direct your attention to the bottom of the side-bar, select "Help & Support" and then select "Support and Community." From there you will be able to open a Support Case.



- Email: Please email signalfx-support@splunk.com to open a support case.
- In-App Chat (only available for customers with Premium Support entitlement by purchasing the Observability Cloud): A drawer or icon in the bottom right corner of the application is where you will find in-app chat. Engage there to be connected with a Support Engineer.

Get started with Splunk Observability Cloud and reach out to us for on-demand expert help and implementation services.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-19894-Splunk-Splunk Infrastructure Monitoring-SG-102