Managing your Splunk Cloud Platform deployment

The information in this article will help you discover methods for deploying, administering and extracting more value from your data with Splunk Cloud Platform. The best practices indexed here are gathered from Splunk customers, partners and employees.

Monitoring system health

To help you monitor Splunk Cloud Platform deployment health, use this quick reference list that highlights how Splunk administrators can use the Cloud Monitoring Console to gain insight into system health, including indexing and search performance, OS resource usage, and license usage.

• Set up the Splunk Cloud Platform monitoring console. Review your data retention capacity and configure Splunk Cloud Platform to generate an alert when the value exceeds your usage license.

• Locate the Splunk Cloud monitoring console and get familiar with the dashboards and the information they show. From the Overview dashboard, check the CPU usage of your indexer(s). Is it in the green (0-59%), orange (60-79%), or red (80% or more) status range? Are there any triggered alerts? From the Topology view under Indexers, toggle to show the indexing rate per second.

• As a best practice, incorporate the monitoring console dashboards into a regular schedule of health maintenance checks. For example, you can monitor search efficiency on a weekly interval, and monitor overall deployment health every month. You can also configure the priority of the scheduled reports.

• Ensure you have healthy searches for optimal performance of your entire Splunk Cloud Platform environment. Check for skipped searches, review searches by user, and review long-running searches. Check for and resolve data quality issues, such as line or event breaking issues.

• Search Splunk Answers for answers, or ask a question of your own. If you're still not sure, contact Splunk support by submitting a case on the Splunk Support and Services portal! Don't forget to generate a diagnostic file to give Support insight into your configuration and performance history.

Managing configurations

This quick reference list highlights how customers can best manage configurations in Splunk Cloud Platform. Splunk Cloud customers do not have the ability to directly edit .conf files, but that doesn't mean they can't extend base capabilities to get more insights into their data.

• Find an especially important source type and resolve data quality issues to make sure it's set up for success.

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.
• Review at the timestamps in your data. Configure timestamp recognition to make sure Splunk doesn't waste time trying to figure out the right date-time stamp to use.

• Define and tune event breaks. You almost certainly have some multi-line events. Figuring out what's multi-line can be taxing on the indexers. Set the segmentation for event data to optimize your source types with what you've learned about .conf files.

• Create a source type using the Source types management page.

• Watch the Splunk Cloud Tutorial to see how to set up Splunk Cloud and get data in using a Universal Forwarder.

• Build field extractions with the field extractor to build search-time field extractions. After you run a search, fields extracted for that search are listed in the fields sidebar. You can create custom field extractions to define which fields are extracted and when Splunk software extracts fields.

• Leverage the power of lookups. Lookups make it easy to add context and create correlations with your data. For example, you can use a geospatial lookup to turn a series of IP addresses into geographical locations. Learn more about lookups and how they can enhance your search experience.

---

**Additional resources**

- .Conf Talk: Understanding the Monitoring Console
- Community: Scale your deployment
- Community: How do access control and permissions work?
- Blog: Access the Cloud Monitoring Console from anywhere