Splunk Cloud: Who is Responsible for What?

"WHAT YOU NEED TO KNOW" SERIES

Table of Contents

Introduction

This Roles & Responsibilities Guide is for organizations considering Splunk's cloud-based Saas solution, known as Splunk Cloud. Splunk's SaaS-based offering is an increasingly-popular alternative to deploying Splunk on-prem or in your own Cloud environment.

This is because Splunk Cloud:

- ✓ Removes the necessity of purchasing and administering the infrastructure Splunk sits on
- ✓ Eliminates a significant portion - but not all - of the administrative overhead tied to Splunk software
- ✓ Reduces the need to hire full-time Splunk Administrators (which are difficult to find and expensive), or allows existing staff to focus less time on platform administration.

You may think incorporating Splunk Cloud will relieve you of all platform administrative duties. However, that's not the case.

It's critical that your organization understands which responsibilities Splunk's Cloud Operations removes from your team, and what your organization will still be responsible for, in order to be successful with Splunk.

Here's what you need to know.

Splunk Administration, Defined

There are three broad activities within Splunk:

- ✓ Data collection
- ✓ Back end Splunk administration (platform administration, i.e., engineering)
- ✓ Front end Splunk administration (sometimes referred to as "Splunk development" or "content development")

Data Collection

Splunk starts with the collection of data from a variety of disparate data sources. This data collection is accomplished in a number of different ways outlined later in this document. Data collection is engineering-focused work.

Platform Administration

Back end administration includes the deployment and maintenance of the various Splunk instances, or components. This is engineering-focused work. Splunk's software has many components but the two major ones are:

- ✓ **Indexers –** The data store
- ✓ **Search Heads –** Where queries, searches and alerts are processed

Front end Splunk - Analytics Development

Front end includes the building of reports, dashboards, queries and alerts within Splunk. This is sometimes referred to as **content creation**.

In some organizations, these front-end Splunk duties are carried out by Splunk end users, including the security analysts, systems administrators, developers, business analytics team members, or others that use Splunk on a day-to-day basis. In these environments, these duties do not fall on the shoulders of the Splunk Administrator.

In other organizations, end users open tickets with requests for reports, queries and alerts that are the responsibility of that organization's Splunk Admin, because that administrator possesses the Splunk expertise the end users rely on.

This structure of Analytics development varies from organization to organization. It depends on how well-versed the end user community is with Splunk.

What **Does** Splunk Cloud Alleviate?

Splunk's Saas model shifts the administrative burden of **one of the three** components identified on the previous page, managing Splunk search head(s) and indexers in Splunk's secure cloud.

This, in turn, alleviates the following:

- ✓ Cost and overhead tied to administering and regularly refreshing (procuring) the technology infrastructure that Splunk sits on (servers, software, storage, and security).
- ✓ Tool/platform administration. You no longer need to perform Splunk upgrades, OS upgrades, or firewall changes for anything related to a Splunk search head or indexer.

Splunk Cloud also minimizes organizational risk. Your organization will no longer face:

- ✓ The responsibility of Splunk (search head/indexer) administration being in the hands of one or two individuals who, if they were to leave an organization, would create a significant administration void.
  - This void is not easily nor immediately remediated, given the niche nature of Splunk, the expertise required to administer the platform, and the ramp time for newly-assigned FTEs to master Splunk.
- ✓ Splunk being administered by someone without subject matter expertise.
  - An improper configuration of Splunk will result in difficulty around scalability as new users are added, or new components of the Splunk stack are added over time. It will also lead to poor system performance, including queries that are slow or time out; or data not being ingested into Splunk and log data missing, among other issues.

What Responsibilities are **Not** Alleviated by Splunk Cloud?

- Data Collection
- Analytics Development
- Domain Advisement / Maturity Roadmaps

Data collection

Data collection infrastructure is still the responsibility of the client. Even when migrating to Splunk Cloud, the data collection portion of the *Splunk stack must be maintained and administered by the client.*

Your organization will still manage:

- ✓ Splunk Universal Forwarders, (UF) on client endpoints (normally Linux and Windows servers)
- ✓ Splunk's Deployment Server, to manage Splunk UF instances
- ✓ Syslog servers that collect data from infrastructure systems (firewalls, IDS, UPS, or any other syslog generating device)
- ✓ Splunk Heavy Forwarders, which can collect and parse information from various databases or third-party systems
- ✓ Splunk HTTP event collector, to obtain data from custom applications (Java, .net, JavaScript, or other web apps), and
- ✓ Splunk Stream, to capture wire data and output raw or statistical information about the data

These elements of the Splunk stack - let's collectively call them the data collection and parsing components - can't be managed by the Splunk Cloud operations team. Why? Because the source systems Splunk is ingesting log data from reside in your own organization's environment.

The knowledge required to maintain the data collection infrastructure can be significant — especially when things don't go according to plan.

What Responsibilities are **Not** Alleviated by Splunk Cloud? *continued*

Analytics Development

Splunk Cloud operations does not perform content creation.

Your organization will still need to develop the capabilities to develop queries in Splunk to create reports, dashboards and alerts.

You will also be responsible for *tuning* queries, in order to reduce false-positive alerts and the plague of wasting time responding to those alerts.

This is critical to understand, given that the typical Splunk User is woefully under-trained, with insufficient levels of skill with the software.

It's not the set-up and maintenance of Splunk that is the key value driver for any organization. Front-end content creation – alerts, reports, dashboards, and queries – is the real driver of attaining up to the 90% reduction in incident investigation time or troubleshooting time Splunk is capable of.

Professional Services Survey

We asked our Splunk SMEs who have collectively delivered over "500 Professional Services projects the following:

On a 1 to 10 scale with 10 being the highest, please assess the overall Splunk capabilities of your typical customer's Splunk User.

Answer: 3.5

There is a "hump" that users need to get over, with regards to Splunk's query language. Even the easiest of commands can be daunting to the first-time user. To get to a level of proficiency the solution is a function of:

- ✓ Knowledge Transfer and assistance from others (an advanced Power User, third party Services firms, or others)
- ✓ Time (experience) with the product
- ✓ Formal EDU on the product and/or a commitment to learning on any user's part

Domain Advisement & Maturity Roadmaps

Another aspect of Splunk that Splunk Cloud doesn't address is the maturation of security detection, enterprise monitoring or other analytics within your organization.

Improvement in those areas accelerates when your business engages a team of domain experts who understand what you want to achieve; and can show you how to achieve those goals faster and better with Splunk.

Understanding business drivers allows for the quick creation of new ways to search for data, visualize data, enrich data, selecting and assisting with the onboarding of key data sources, alerting and troubleshooting missing log sources, and interactively training users.

In Summary

A transition from on-prem to Splunk Cloud does remove the burden of managing several components of the Splunk stack (search head/ indexer/Add-Ons). However, other responsibilities remain with the organization leveraging Splunk's Saas model.

For this reason, it's in your best interests to partner with competent Splunk SMEs who can:

- ✓ Manage, scale and troubleshoot log collection (forwarder) infrastructure
- ✓ Assist with the creation of critical queries, reports, dashboards and alerts Optimize queries to reduce false-positive alerts
- ✓ Provide domain expertise tied to use case recommendations and prioritization of those use cases In doing so, your organization will derive the most value from this incredibly powerful tool.

SP6 Can Help

If your organization doesn't have Splunk certified team members or could benefit from additional Splunk expertise, our cybersecurity and information technology observability specialists can help ensure your systems are both protected and highly performant. Contact us today to learn more about SP6 Managed Services options and schedule a complimentary consultation.

Request a Conversation

For more information, visit **www.SP6.io**

or contact us at **Service@SP6.io**

Components of Splunk and Who Owns Responsibility

SP6