Staffing a Splunk deployment

The size of the staff you need to operate your Splunk implementation depends on how you set up your Splunk business model and the needs of your organization, not on how much data you ingest.

A Splunk team is composed of a series of roles. A role is not a person or job description, a role is a collection of responsibilities delegated to existing staff member(s). Think about roles and responsibilities before you think about the individual members on your team. When you approach staffing by role rather than by individual, you can better estimate your staffing needs.

Follow these guidelines for setting up a staffing model and planning your staff needs.

Audience

- Executive sponsor
- Program manager
- Project manager

For more about these roles, see Roles best practices.

Guidelines for creating a staffing model

Create a resource that identifies who is on your Splunk team and the roles they fulfill. Post it in a place where stakeholders and team members can access it easily. Include contact information, such as an email link and a picture, so people know who to look for and where they are located. Consider this as information you share on your communication portal. For more information about a communication plan, see Communicating with your user community.

As you complete the staffing model, keep in mind that any team member can be assigned to multiple roles. Multiple team members can also fulfill the same role.

Example:
Staffing model template

<table>
<thead>
<tr>
<th>Team member</th>
<th>Program manager</th>
<th>Developer</th>
<th>Engineer</th>
<th>Executiv e sponsor</th>
<th>Search expert</th>
<th>Knowledge manager</th>
<th>Architect</th>
<th>Project manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Smith</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Sally Brown</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>John Doe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommendations for staff sizing

One person can usually manage a single instance of Splunk, a deployment server, and several forwarders. However, as your Splunk implementation grows and you add some advanced features to meet your data analysis needs, you may need more staff. The larger, more distributed, and service-oriented your implementation, the more people you will need to keep it running smoothly.

Technical drivers that influence staffing decisions

Increased complexity and mitigating risk are the two main drivers for increasing Splunk staff. Here is a closer look at some situations that can increase the demands on your team. For each of these advanced features, consider adding at least half a person’s time. The skills needed to address that demand fall within the roles of architect and engineer. For details about these roles and skills needed, see Setting Roles & Responsibilities.

Distributed deployment

If an implementation shifts to a more distributed deployment model that separates indexers from the search head, you may want to add an architect or engineer to help manage the expanded deployment. Another team member can provide peer review and help optimize and maintain a distributed deployment.

Indexer clustering

If you implement indexer clustering, your staff should have the necessary data management skills to maintain data fidelity between data sources and the indexer cluster nodes. You should also have sufficient staff to ensure timely response in case a problem arises—if you have high availability requirements for data or search, you also need high availability for people.

Search head clustering

If you implement search head clustering, your staff should have the necessary capacity tuning and optimization...
skills to maintain and optimize search head performance.

Data collection tier

If you establish a data collection tier, modular inputs and third-party data forwarding can add administrative complexity. Your staff should have the expertise with the systems your Splunk deployment integrates with.

Complex utility tier

Utility Splunk instances, such as Splunk deployers, masters, and deployment servers, are usually managed easily within normal operations. However, if you deploy complex redundancies, such as a pool of deployment servers, this can increase the team workload.

---

**Operational drivers that influence staffing decisions**

How you set up your operational model can also influence your staffing needs. Here are some considerations for how you set up Splunk in your organization, and how that can influence staffing decisions. The skills required for staff that interact with your customers and their use cases are filled by the developer, search expert, and user community roles.

Closed platform approach

In a closed platform setup, Splunk staff are responsible for managing and creating all knowledge objects. This model is more resource intensive. In an environment where Splunk is a service or a strategy, the Splunk staff are rarely the subject matter experts for a given use case's technical domain. That means your staff will need to spend more consultation time to understand what aspects of the data are important and worth getting insights into. If this is your model, make sure you have enough staff to devote the necessary time to to explore the data and be inspired with other questions.

Open platform approach

In an open platform setup, end users are empowered and entitled to implement their own use cases. This enables them to provide their own subject matter expertise, and is generally less resource intensive. The focus of your team shifts from consultation to education, empowerment and community management.

Whether you adopt a closed or open platform approach, Splunk usage often grows virally as the user community begins to use it, experiments using their own SPL, and eventually becomes proficient enough to create their own knowledge objects. As one person learns, they share their knowledge with another. As this happens, you should have enough staff to support the more consultative skills of the closed platform approach, and the education, empowerment, and community management skills of the open platform approach.