Establishing an operating framework

An operating framework provides structure for how you set up and manage your Splunk implementation.

Choose an operating model

You can organize your Splunk implementation a number of ways, depending on how you want to manage your resources. This topic outlines three possible approaches: centralized, federated, and a hybrid of both.

Federated model

With a federated model, teams operate their own independent Splunk deployments and projects. Program management provides best practice guidance and a forum for meetings to keep them coordinated. Each team can manage its own deployment architecture and operations.

You can store event data on separate indexers.

<table>
<thead>
<tr>
<th>Federated model advantages</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Teams can manage their infrastructure independently under a common set of standards</td>
<td>• Requires more coordination from the program manager</td>
</tr>
<tr>
<td>• Scaling is more modular, and easier to plan and execute</td>
<td>• More complex to set up and manage</td>
</tr>
<tr>
<td>• Good for large organizations</td>
<td>• Managing deployment-wide search concurrency is more complex</td>
</tr>
<tr>
<td>• Isolates “noisy neighbors”</td>
<td>• Changes by one team have less risk of impacting other teams</td>
</tr>
<tr>
<td>• Flexible infrastructure deployment options</td>
<td>•</td>
</tr>
</tbody>
</table>

Centralized model

A centralized model concentrates Splunk engineering (hardware and people) into a central team with a single Splunk deployment. A majority or the entirety of event data is stored on a common set of indexers, and users access a common search head or search head cluster.

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.
Centralized model advantages

- Good for small deployments
- Data is easily accessible and shared
- Faster to get started and simple to set up
- Allows for quick growth
- Easier to manage deployment-wide search concurrency
- Requires the least hardware

Challenges

- Requires effort to scale as more groups adopt Splunk and the number of use cases/number of users grows
- "Noisy neighbors" can slow the system down

Hybrid model

A hybrid model is a mix of both centralized and federated, where a critical mass of the Splunk activity is within a central team. Satellite deployments can exist outside of the central team. You can set up dedicated indexers and search head(s) for a use case or department, and the search heads may have the ability to search other deployments.

Hybrid model advantages

- Less complex to manage
- A centralized team can still manage smaller groups or business units
- A centralized operations team can provide Splunk as a Service
- Federated customer teams can meet scale demands

Challenges

- Requires coordination for federated resources
- The Operations team must be prepared to operate a large Splunk deployment
- Requires the most hardware

Identify the program manager

It is important to identify someone who is responsible to fulfill the program manager role, someone who has clear authority to manage operations for your entire Splunk implementation. The program manager role performs one of the most crucial functions on your team.

Program managers fulfill the following responsibilities:

- Drive decision-making
- Manage inter-dependencies between Success Framework pillars
- Ensure the Splunk implementation plan aligns with business objectives
- Oversee Splunk success measurements
• Is accountable for return on investment
• Promotes and facilitates program-wide communication
• Supports initiatives for knowledge sharing and collaboration
• Ensures executive alignment

For more information, see Setting Roles & Responsibilities.

---

**Post a service catalog**

If you are providing Splunk as a service, you can post a catalog of Splunk-related services and processes for your user community. A service catalog communicates to your community the services you offer, and indicates how they can engage with your team. Post your service catalog in a publicly accessible space, such as your team wiki, community, or internal web site.

---

**Define service level objectives and agreements**

Service level definitions include service-level objectives (SLOs), service-level agreements (SLAs), and case priorities. For more about creating service-level agreements, see Service-level best practices.