Table of Contents

Best Practices Index

How to use the Splunk platform best practices index

Best practices to start your journey with the Splunk platform

Best practices to deploy and administer the Splunk platform

Best practices to search and manage data

Best practices to manage your Splunk program

Best practices to empower the people who use Splunk software
Best Practices Index

How to use the Splunk platform best practices index

Use the Splunk platform best practices index to discover best practices that help you deploy, administer, and get more value from the Splunk platform. All best practices indexed here are gathered from Splunk customers, partners, and employees.

The best practices linked in this index are validated best practices hosted on the Splunk community question-and-answer forum Splunk Answers, Splunk Docs, and Splunk Blogs.

To find validated best practices on Splunk Answers, see the validated_best-practice page. To follow the [validated_best-practice] tag and receive notifications when new validated best practices are posted, log in using your Splunk.com credentials. While logged in, you can also make a comment, post an answer, or ask a new question. For more information, see Splunk Answers in Get Started with Splunk Community.

For more information about how you can participate in developing Splunk best practices, see the blog post How Crowdsourcing is Shaping the Future of Splunk Best Practices.

The following table lists what the best practices in the Splunk Platform Best Practices index can help you do.

<table>
<thead>
<tr>
<th>Task</th>
<th>What best practices can help you do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start your journey with Splunk software</td>
<td>Use the Splunk platform to achieve value and insights as quickly as possible.</td>
</tr>
<tr>
<td>Deploy and administer the Splunk platform</td>
<td>Deploy, monitor, maintain, upgrade, and scale the Splunk platform.</td>
</tr>
<tr>
<td>Search and manage data</td>
<td>Optimize searches and manage data, from getting data in to optimizing logs.</td>
</tr>
<tr>
<td>Manage your Splunk program</td>
<td>Plan, scope, and drive engagement with a well-organized Splunk program based on best practices.</td>
</tr>
<tr>
<td>Empower the people</td>
<td>Empower users and teams using learning incentives</td>
</tr>
</tbody>
</table>
who use Splunk software and role-based access controls with user-management best practices.

Best practices to start your journey with the Splunk platform

The best practices to start your journey with the Splunk platform help you start using the Splunk platform to achieve value and insights as quickly as possible. Each step in the journey includes a link to validated best practices on Splunk Answers. The best practices define concepts and provide context to understand the intricacies of the software. Each validated best practice topic includes a Things to do section to allow you to put those concepts into practice immediately.

Since the topics and corresponding best practices are listed in sequence, work through each topic in the order presented to expedite your learning.

A lot of the product information and best practices apply to both platforms. In cases where the information is different, either Splunk Enterprise or Splunk Cloud is specified in the reference.

Get started with the Splunk platform

When you begin using Splunk Enterprise or Splunk Cloud, start with understanding the key concepts and components of the Splunk platform. After your comfortable with the basics, use that base knowledge to create searches and dashboards.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of the Splunk Platform</td>
<td>See Splunk overview, introduction, and getting started resources? on Splunk Answers.</td>
</tr>
<tr>
<td>Key concepts</td>
<td>See How do I get new users acquainted with the basic anatomy of how Splunk Enterprise works? on Splunk Answers.</td>
</tr>
<tr>
<td>Getting data in</td>
<td>For Splunk Enterprise, see Where to find resources about getting data into Splunk? on Splunk Answers.</td>
</tr>
<tr>
<td></td>
<td>For Splunk Cloud, see Overview of data and getting data into Splunk Cloud? on Splunk Answers.</td>
</tr>
<tr>
<td>Searching</td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Best practices</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Knowledge Objects</td>
<td>See What are knowledge objects, and what do I need to know about them? on Splunk Answers.</td>
</tr>
<tr>
<td>Searches and dashboards</td>
<td>See Can I have an overview of how Splunk reports and dashboards work? on Splunk Answers.</td>
</tr>
</tbody>
</table>
| Configuration files | For Splunk Enterprise, see Can I use configuration files to extend the power of Splunk Enterprise? on Splunk Answers.  
For Splunk Cloud, see Can I use field extractions and lookups to extend the power of Splunk Cloud? on Splunk Answers. |

**Learn and implement best practices**

This section builds on the basics with in-depth information about concepts and components and how to use them. Use the following best practices to broaden your user base, monitor your system, build a sandbox for development teams, and learn best practices to optimize your system.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best practices</th>
</tr>
</thead>
</table>
| Configuration files and deployment server | For Splunk Enterprise, see Can I use a deployment server to scale my Splunk Enterprise deployment? on Splunk Answers.  
For Splunk Cloud, see Can I use forwarders to scale my Splunk Cloud deployment? on Splunk Answers. |
| Roles and governance | See Can I get an overview of how Splunk permissions work? on Splunk Answers. |
| Index management and archive storage | For Splunk Enterprise, see How many indexers do I need in my Splunk deployment? on Splunk Answers.  
For Splunk Cloud, see Can I archive data in Splunk Cloud? on Splunk Answers. |
| Monitoring system health | For Splunk Enterprise, see How do I get started monitoring system health on Splunk Enterprise? on Splunk Answers. |
Expand and scale your Splunk platform deployment

This section covers material to expand and scale the use of Splunk Enterprise and Splunk Cloud. Use the following best practices to troubleshoot and maintain your environment, plan for the future, and start building Splunk apps.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Best practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity planning, troubleshooting, and health</td>
<td>For Splunk Enterprise, see Capacity planning best practices for Splunk Enterprise? on Splunk Answers.</td>
</tr>
<tr>
<td></td>
<td>For Splunk Cloud, see How do I get started monitoring system health on Splunk Cloud? on Splunk Answers.</td>
</tr>
<tr>
<td>Search optimization</td>
<td>For Splunk Enterprise, see Best practices for search optimization for Splunk Enterprise? on Splunk Answers.</td>
</tr>
<tr>
<td></td>
<td>For Splunk Cloud, see Best practices for search optimization for Splunk Cloud? on Splunk Answers.</td>
</tr>
</tbody>
</table>

**Best practices to deploy and administer the Splunk platform**

The best practices to deploy and administer the Splunk platform make your Splunk deployment more available, scalable, and maintainable. These best practices optimize your Splunk platform architecture and facilitate continuity
planning, capacity planning, and incident management.

**Best practices for upgrading Splunk Enterprise**

The best practices for upgrading Splunk Enterprise help you plan, execute, and verify a successful Splunk Enterprise upgrade.

**Splunk product version compatibility matrix**

The tables in the version compatibility matrix list versions of Splunk Enterprise and their compatible versions of Splunk premium apps for customer-deployed environments.


**Splunk Enterprise upgrade considerations**

Before you upgrade, consider changes in behavior to Splunk Enterprise and the Splunk Universal Forwarder when you upgrade to the latest version. This topic is a must-read before you embark on a Splunk Enterprise upgrade.

See About upgrading Splunk Enterprise READ THIS FIRST in the Splunk Enterprise *Installation Manual.*

**Upgrade best practices on Splunk Answers**

Find upgrade best practices with the tags [validated_best-practice] and [upgrade] on Splunk Answers.

**Best practices to configure Splunk Enterprise using configuration files**

Best practices to configure Splunk Enterprise using configuration files help you fine-tune Splunk platform behavior and performance.

Find platform configuration best practices with the tags [validated_best-practice] and [configuration] on Splunk Answers.
Best practices to search and manage data

Best practices to search and manage data help you manage and structure your data efficiently, and design effective use cases.

**IT operations analytics use cases**

IT operations analytics (ITOA) is the practice of interpreting machine data from your IT operations infrastructure to guide decisions and predict potential issues.

The ITOA use cases suggest how to get data in, search for insights, and fine-tune results from data across your entire operations infrastructure on a single diagnostic platform. Better performance and greater efficiency can reduce overall costs, increase revenue, and improve the user experience.

See IT operations analytics use cases in the *IT Operations Analytics Use Cases* manual.

**Security use cases**

Use the Splunk platform to centralize essential security data and build a strong security operations center (SOC).

Each example security use case provides guidance about the apps, source types, implementation prerequisites, and searches to help increase your security posture. The use cases are sourced from Splunk Enterprise Security (ES) and Splunk Security Essentials (SSE).

See About security use cases in the *Security Use Cases* manual.

**Best practices to manage and monitor Splunk Enterprise on Windows**

Find best practices to manage and monitor Splunk Enterprise on Windows systems with the tags [validated_best-practice] and [windows] on Splunk Answers.

**Best practices to manage and monitor Splunk Enterprise on *nix**
Find best practices to manage and monitor Splunk Enterprise on *nix systems with the tags [validated_best-practice] and [unix] on Splunk Answers.

**Best practices for using Amazon Web Services**

Find best practices for using Amazon Web Services with the tags [validated_best-practice] and [amazon] on Splunk Answers.

**Best practices to define source types**

Find best practices to define source types with the tags [validated_best-practice] and [sourcetype] on Splunk Answers.

**Best practices to manage your Splunk program**

The best practices to manage your Splunk program can help you drive engagement with your Splunk deployment, and improve business alignment, collaboration, and operations. A program manager generally drives these activities and manages interdependencies among the stakeholders.

**Best practices to drive engagement with Splunk software**

Use the best practices in this section to drive engagement with Splunk software among your user community.

**Best practices to engage new and existing Splunk software users**

This article provides recommendations for how to engage new and existing users to get more out of Splunk software.

See How can I jumpstart my stalled Splunk user community and engage more users? on Splunk Answers.

**Best practices to revitalize a Splunk deployment**

This article provides guidance for how to evaluate and revitalize a Splunk deployment that hasn't been touched in a while to make sure you're getting the best value out of Splunk software. Find suggestions for how to get data in more efficiently, make your data more effective, and make it easier to distribute apps and manage configuration and content updates using a deployment server.
See Do you have any guidance about how to revitalize a Splunk Enterprise/Splunk Cloud deployment that's stuck on autopilot? on Splunk Answers.

**Best practices to empower the people who use Splunk software**

Best practices to empower the people who use Splunk software focus on learning incentives and role-based access to features and data. These best practices encourage Splunk platform users to earn access to more capabilities as they advance their knowledge and experience with Splunk software. They also establish organized workspaces where users can collaborate and experiment with new ideas.

**Best practices to enable users**

Best practices to enable users can help motivate people to learn and grow their Splunk platform skills. An environment of incentive-driven access encourages users to explore and develop good habits, which results in better use cases and adds value to the whole user community.

See User enablement best practices for a Splunk deployment in the *Splunk Success Framework Handbook*.

**Best practices to define roles for a Splunk implementation team**

A Splunk implementation team requires different strengths and skills to help your organization get the most out of its data. Define roles and responsibilities to build an effective Splunk implementation team.

See Roles best practices for a Splunk deployment in the *Splunk Success Framework Handbook*.

**Best practices to manage data using roles**

Role-based data management best practices use role separation and data governance to provide modular, fine-tuned access to data and product features.

**Best practices to create a welcome page**

Use a welcome page as a default dashboard to present specific users with the resources and workflows they need to get started using the Splunk platform.


**Best practices to create a workspace**

Use a workspace app tailored to a specific role or user group for users to search, explore, and create solutions without distractions from other teams and users.