Using a Splunk sandbox

A sandbox is a stand-alone Splunk Enterprise instance used by one person as a safe place to innovate and develop new ideas. Sandboxing is the process of establishing and using a sandbox.

Everyone on your Splunk team should have their own sandbox so they feel safe to take risks and learn. With your own sandbox, you won’t be afraid to start over if you need to.

A best practice for establishing a stable and reliable production Splunk environment is to set up a workflow which includes:

- Individual sandboxes for development and innovation.
- A Splunk Lab environment for testing.
- A safe push to production once things are ready.

Encouraging a healthy sandbox culture for your Splunk team promotes learning and growth, and ensures that your innovators have the latitude to try new things without disrupting what already works, or each other.

**Audience**

- Architect
- Developer
- Engineer
- Search expert
- Knowledge manager
- User community

For more about these roles, see [Roles best practices](#).

**Options for deploying a sandbox**

A sandbox should be easy to set up and easy to tear down so you feel free to innovate. You have several options for setting up a Splunk sandbox. Whatever option you choose, use a basic Splunk setup, and keep customizations to a minimum. The more effort you put into it, the greater the fear of breaking it, and the less comfortable you will be taking risks and trying new things.

**Splunk Docker sandbox (recommended)**

Splunk has done all the thinking for you and published a Docker image so you can set up a Splunk sandbox in minutes. This is the quickest and easiest way to sandbox. See the Splunk blog [Hands on Lab: Sandboxing with Splunk (with](#)
Docker) for complete instructions. To keep it simple, set up your Splunk Docker sandbox on your localhost.

**Splunk Search Tutorial sandbox**

Setting up a Splunk sandbox using the Splunk Enterprise Search Tutorial is a great way to get familiar with installing and launching Splunk. The instructions also lead you through the basics of getting data in, searching, and creating reports and dashboards. See About the Search Tutorial for more info.

**Splunk sandbox on Cloud or VM**

You can use a public cloud (such as Amazon Web Services–AWS) or one that is private to your company. Consider any concerns your organization may have about exfiltration, or unauthorized transfer of personal or company data to a cloud-based resource.

You can also set up a virtual machine on your local instance. Oracle VM VirtualBox is a free and open-source option. Be aware that installing a virtual machine can be involved, especially if you want to replicate a distributed environment.

**Sandbox licensing**

The Splunk Enterprise trial license will revert to a free license 60 days after download, which limits its capabilities. To learn more, see Splunk Platform Comparison on the Splunk web site. For more information about Splunk licenses, see Types of Splunk software licenses in the Splunk Enterprise Admin Manual.

Splunk notifies you when your 60 day period is about to expire. Think of this notification as a reminder that your sandbox is meant for experimentation, and you should not be afraid to break it. You can also switch to a free license from within Splunk: go to Settings > Licensing and click Change license group.

For a more formal development setup, you can also get a developer license for your sandbox. See Splunk Developer License Signup on dev.splunk.com.

**Getting data into your sandbox**

You have several options for getting data into your sandbox.

**Sample data**

The most basic way to get data into your sandbox is to download sample data from Splunk. For sample data, see Upload the tutorial data in the Splunk Search Tutorial.

**_internal index**

You can also use the _internal index. It has logs about your own instance, which are often perfect for sandboxing.
Export data

If your organization's policies allow you to use production data in your sandbox, but you don't want to connect directly to a production indexer, you can use the export feature in Splunk to get a sample of raw events. Export data as raw events so you can experiment with defining the source type. You can also use a semi-structured format, such as JSON or XML. For information about exporting data, see [Export data using Splunk Web](/search-manual) in the *Splunk Search Manual*.

When you export data from the production environment, be aware of the amount of data you are requesting. If the data set is too large, Splunk could become unresponsive while transmitting the export.

Production data

Wherever your sandbox is hosted, you can point to existing indexers, including those in your production environment. You can have a many-to-many relationship between search heads and indexers (or index clusters). Before proceeding with this option, think about the purpose of your sandbox and consider the impact this will have on the environment. If you are using your sandbox for an indexer-heavy workload, connecting to production indexers may not be the best solution.

- For information about connecting to production non-clustered indexers, see [Add search peers to the search head](/distributed-search-manual) in the *Distributed Search Manual*.
- For information about connecting to production indexer clusters, see [Enable the search head](/managing-indexers) in *Managing Indexers and Clusters of Indexers*.

Tips for advanced sandboxing

- With the `| makeresults` command, you can experiment with commands by fabricating results.
- With the `|extract reload=true` command, you can apply props or transforms without having to restart Splunk.
- With the `/debug/refresh` endpoint or the `/en-US/_bump endpoint` command, you can get some config or static content reloaded.
- Using Development mode, you can add parameters to web.conf to prevent caching. For development mode settings, see [Build a custom visualization > Getting Started](/developing-views-apps) in *Developing Views and Apps for Splunk Web*. Development mode settings are especially useful when developing a new app, as you can get static content reloaded without having to `_bump` every time.

When to avoid using a sandbox

Do not use a sandbox for transaction-based work. A sandbox is not intended for transaction-based work, such as defining a new search or field extraction. Here are some other methods for experimenting in the production environment without incurring risk:

- Run your experiments on a reduced time range. This way, you can run highly complex searches without having a

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.
heavy impact on search heads, indexers, and other people using the environment. See [Select time ranges to apply to your search](#) in the *Splunk Search Manual.*

- Use the `| head` command to validate a search with 10 events by default. See [Head](#) in the *Search Reference manual.*
- Use the `| makeresults` command to generate data without worrying about the data set. See [Makeresults](#) in the *Search Reference manual.*

Do not use a sandbox for editing knowledge objects because of how long it takes to bring the data in and perform field extractions. Instead of using a sandbox, clone the knowledge object within the production environment, so you can edit the knowledge object without changing macros, saved searches, dashboards, or other settings.

- When cloning a knowledge object, set the permissions to private so only you can view it.
- Once you are done experimenting with the cloned knowledge object, copy the new configuration into the production knowledge object.
- When the updated knowledge object is transferred into production, delete the clone.