Setting up a lab environment

An essential enterprise software best practice is to set up a lab environment that simulates your production environment so you can test product features.

A lab is different from setting up an individual sandbox, which is intended to be a lightweight, high-volatility environment for individual development and experimentation. A lab is similar to your production environment, and should be stable and persistent, so you can effectively test and develop product features before implementing them in your production environment.

Audience

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

For more about these roles, see Roles best practices.

Guidelines for establishing a lab

A lab environment should mirror your production topology to the extent possible, in functionality, if not in scale. You can host your lab a number of ways:

On-prem lab

You can host your lab on premises using dedicated hardware. This hardware should be managed and maintained under the same policy as your production environment to ensure stability, security, and up-time.

Cloud or VM lab

You can use a public cloud (such as Amazon Web Services) 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.
Access control

Access control in your lab environment should mirror your production environment. See About configuring role-based user access in Securing Splunk Enterprise for details. See Role-based data management best practices for tips on how to fine tune your user access model.

Getting data into your lab

A lab is where you test product features and custom solutions on production-simulated data before pushing them to production, so ideally, you want the data in your lab to mirror production as closely as possible.

When you first set up your lab, you can start with sample data from Splunk. For sample data, see Upload the tutorial data in the Splunk Search Tutorial. You can also use the _internal index, which has logs about your own instance. Once you have your lab set up, however, use one of the other methods listed below so you can test your product features on data that closer simulates reality.

Export data

If 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 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

You can point to existing indexers, including those in your production environment. It is possible to have a many-to-many relationship between search heads and indexers (or index clusters). For information about connecting to production non-clustered indexers, see Add search peers to the search head in the Distributed Search Manual. For information about connecting to production indexer clusters, see Enable the search head in Managing Indexers and Clusters of Indexers. Before proceeding with this option, consider the impact this will have on the environment.

If you are using your lab for an indexer-heavy workload, connecting to production indexers may not be the best solution.

License management

Configure a license master and set up a license slave for your lab. This will ensure that your lab is stable and persistent, and has all the functionality available to it that is available in production. See Configure a license slave in the Splunk Enterprise Admin Manual.

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.