© 2025 SPLUNK LLC

Splunk4Ninjas - Custom Commands

Hands-On Workshop

splunk> a CISCO company

© 2025 SPLUNK LLC

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

splunk> a CISCO company

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

© 2025 SPLUNK LLC

Workshop Agenda

- Recap Splunk Capability
- Search Pipeline
- Command Types
- Custom Commands Overview
- Hands-On Labs
- Tools to help
- Deployment Considerations

© 2025 SPLUNK LLC

Enroll in Today's Workshop

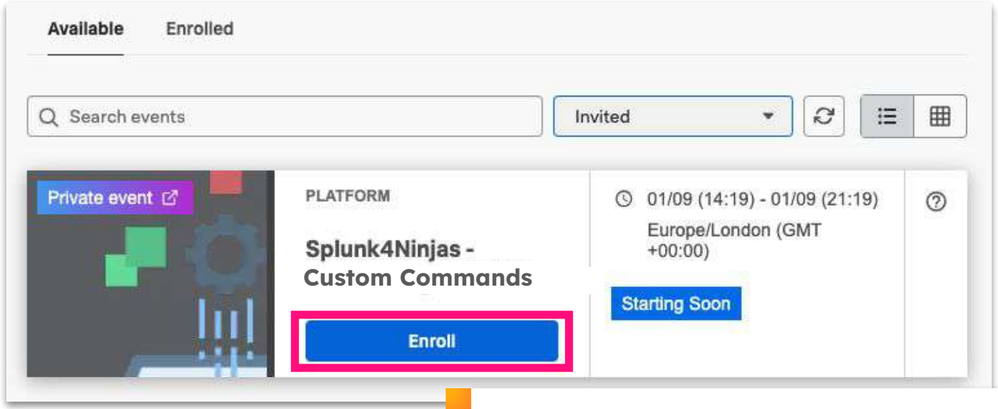
Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://splunk.show/<uniqueCode>
3. Download the hands-on lab guide:
   https://splk.it/S4N-CC-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!

1. Download a copy of today's slide deck:
   https://splk.it/S4N-CustomCommands

Goal



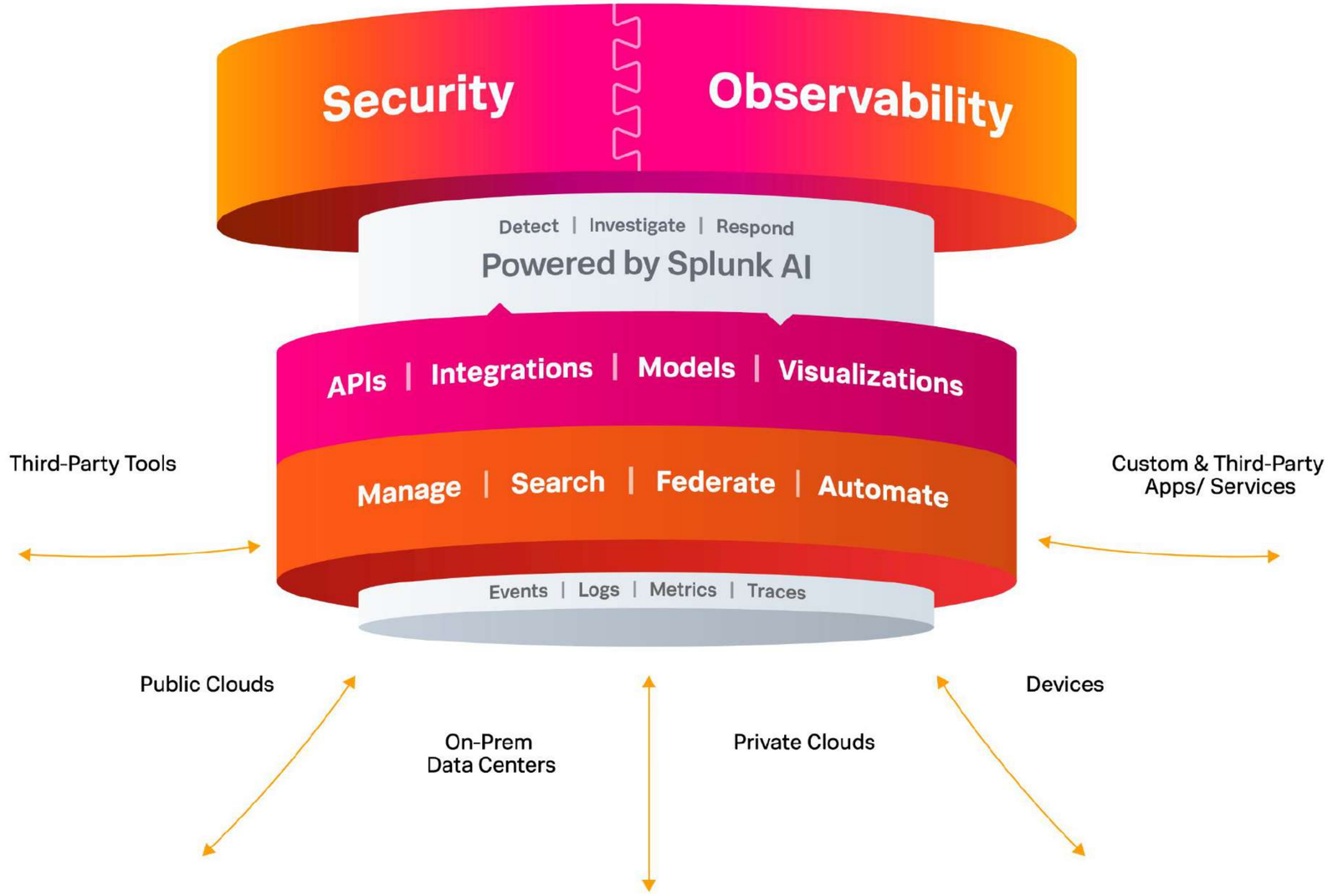
Enroll in today's event

© 2025 SPLUNK LLC

Capability and feature refresh

© 2024 SPLUNK INC.

The Unified Security and Observability Platform



© 2025 SPLUNK LLC

Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

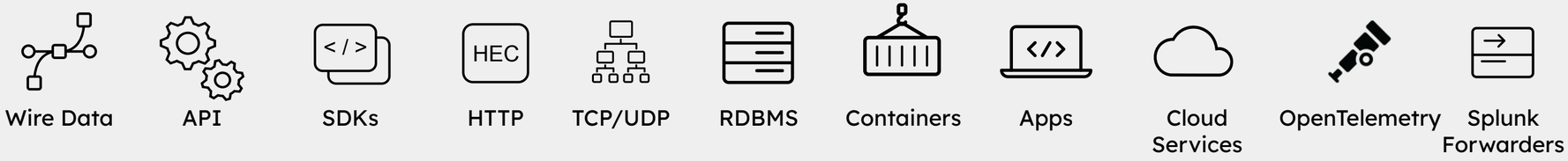
3 Simple Steps:

1. Onboard data
2. Onboard users
3. Get value from your data

splunk>cloud™

- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI DSS, HIPAA, FedRAMP Moderate, DoD IL5, IRAP
- **Encryption-in-transit** - plus optional encryption-at-rest
- **Resilient infrastructure**
- **100% uptime guarantee**
- **24/7 NOC/SOC support team**

Flexible options for data collection and forwarding

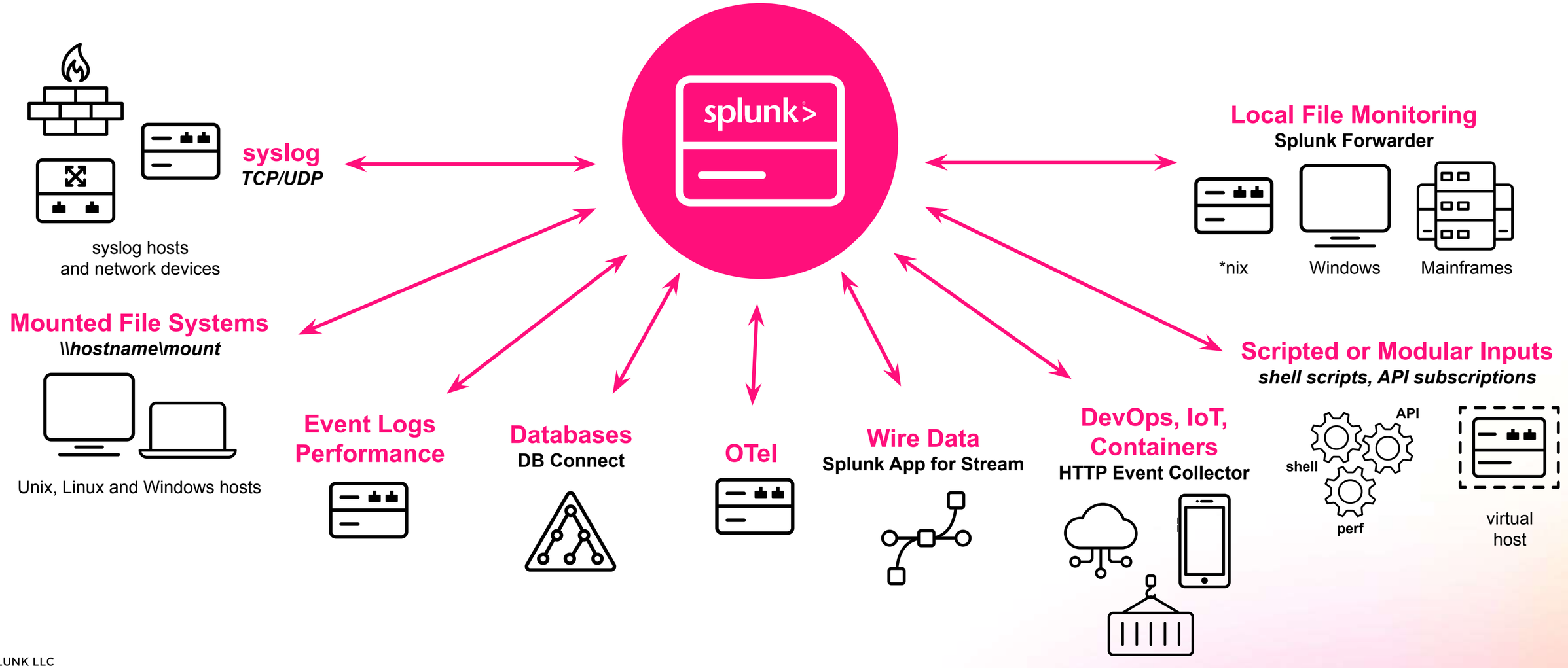


Splunk Cloud Service Description: https://splk.it/SplunkCloudServDesc

© 2025 SPLUNK LLC

Ingests Data From Heterogeneous Data Sources

Agentless and Agent Approach for Flexibility and Optimization



© 2025 SPLUNK LLC

What is a Splunk Universal Forwarder?

- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
  - Buffering / guaranteed delivery
  - Encryption
  - Compression
  - Load balancing
  - And more!
- Very small footprint
- Just forwards data – no parsing beforehand!

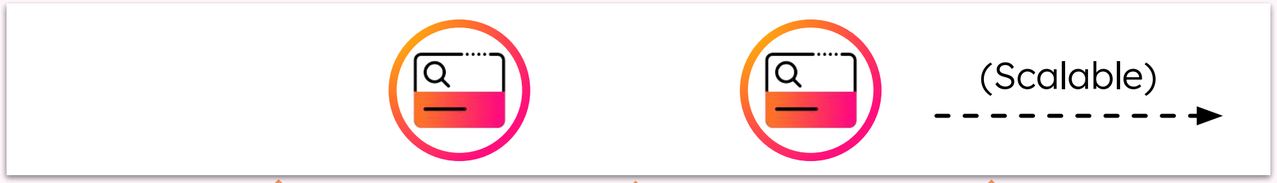
© 2025 SPLUNK LLC

Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability

splunk>cloud
Public or private cloud
On-premise

Searches are run on **Splunk Search Heads**

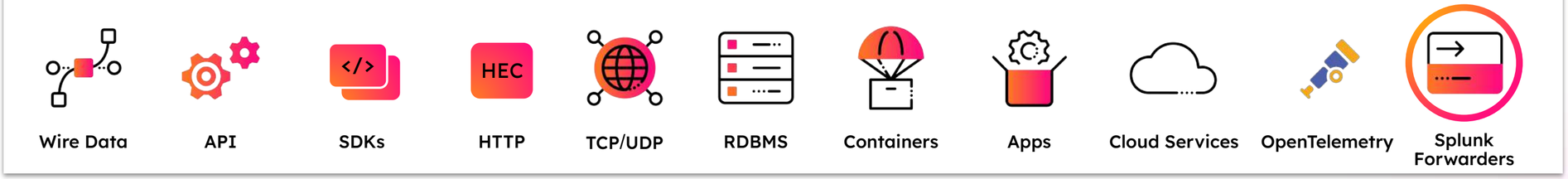


- Distribute searches to Indexers
- Can be clustered (active-active)

Data is processed on **Splunk Indexers**

- Receive and store raw data
- Data is analysed and indexed
- Can be clustered (active-active)

Collect data using a variety of data collection methods, such as **Splunk Forwarders**

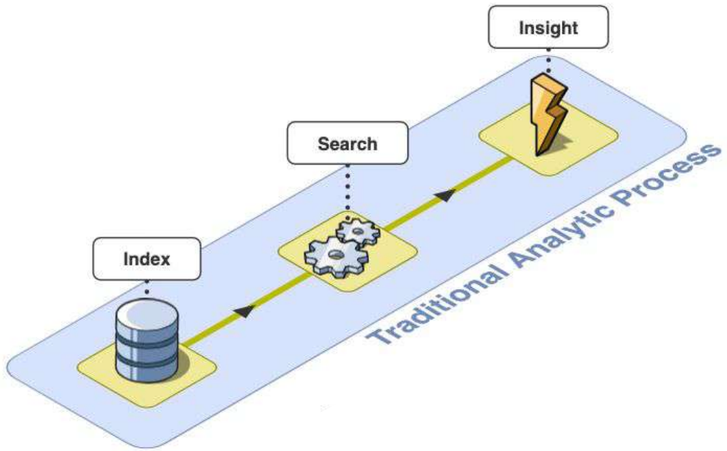


- Collect/monitor and forward data to Indexers
- Collection options for a variety of data sources

© 2025 SPLUNK LLC

Traditional Pipeline

Standard use case



First step is to decide on use case:

- Why do anything

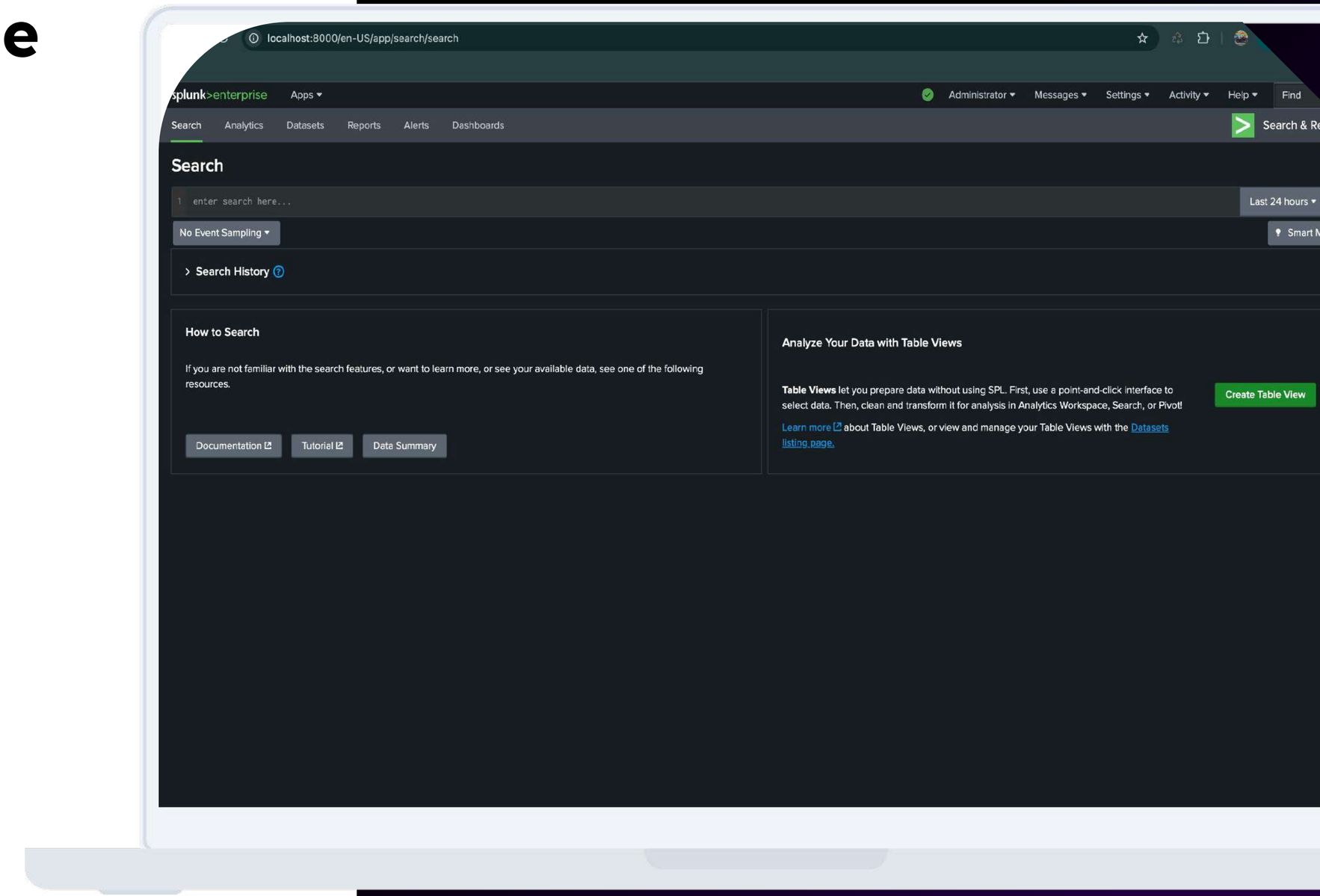
3 pipeline phases:

- Collect data
  - Clean
  - Relevant
  - Complete
- Search the data
  - Understand what's in there
  - Find Answers
- Visualise the output
  - Dashboards
  - Reports

© 2025 SPLUNK LLC

Analytic Pipeline

How a Splunk search works



© 2025 SPLUNK LLC

How a search works

Where’s Wally

Basic Search

Retrieves and filters events

SPL Commands

Evaluate, transform and evaluate events

© 2025 SPLUNK LLC

Example Search

Search Terms

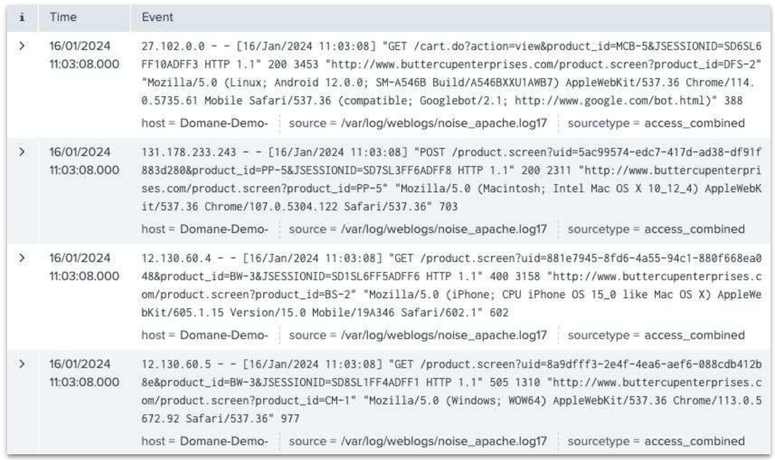
Commands

```
index=main action=purchase | stats count by status | rename count as "number of events"
```

Pipe character: Output of left is input to right

Functions

e.g. `index=main action=purchase` `| stats count by status` `| rename count as "number of events"`



i	Time	Event
>	16/01/2024 11:03:08.000	27.102.0.0 - - [16/Jan/2024 11:03:08] "GET /cart.do?action=view&product_id=MCB-5&JSESSIONID=SD6SL6FF10ADFF3 HTTP 1.1" 200 3453 "http://www.buttercupenterprises.com/product.screen?product_id=DFS-2" "Mozilla/5.0 (Linux; Android 12.0.0; SM-A546B Build/A546BXXU1AWB7) AppleWebKit/537.36 Chrome/114.0.5735.61 Mobile Safari/537.36 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 388 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	131.178.233.243 - - [16/Jan/2024 11:03:08] "POST /product.screen?uid=5ac99574-edc7-417d-ad38-df91f883d280&product_id=PP-5&JSESSIONID=SD7SL3FF6ADFF8 HTTP 1.1" 200 2311 "http://www.buttercupenterprises.com/product.screen?product_id=PP-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 Chrome/107.0.5304.122 Safari/537.36" 703 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.4 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=881e7945-8fd6-4a55-94c1-880f668ea048&product_id=BW-3&JSESSIONID=SD1SL6FF5ADFF6 HTTP 1.1" 400 3158 "http://www.buttercupenterprises.com/product.screen?product_id=BS-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 Version/15.0 Mobile/19A346 Safari/602.1" 602 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.5 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=8a9dfff3-2e4f-4ea6-aef6-088cdb412b8e&product_id=BW-3&JSESSIONID=SD8SL1FF4ADFF1 HTTP 1.1" 505 1310 "http://www.buttercupenterprises.com/product.screen?product_id=CM-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/113.0.5672.92 Safari/537.36" 977 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined

status	count
200	850
400	81
401	76
402	50
403	57

status	number of events
200	850
400	81
401	76
402	50
403	57

© 2025 SPLUNK LLC

Out-of-the-box Commands

Command	Command Type	Description
eval, fields, makemv, rename, regex, replace, strcat, typer, where	Streaming	process search results one-by-one, applying one transformation to each event that a search returns - *Hashing PII fields in real-time*
chart, timechart, stats, top, rare, addtotals	Transforming	order search results into a data table. These commands "transform" the specified cell values for each event into numerical values that Splunk software can use for statistical purposes -
dbinspect, datamodel, inputcsv, metadata, pivot, search, tstats	Generating	fetch information from one or more indexes without performing any transformations. Generating commands are either event-generating or report-generating. These commands do not require any input and appear at the beginning of a search after a leading pipe - *Pull from an API, generate test data*
sort, eventstats, and some modes of cluster, dedup, fillnull	Dataset processing	Dataset processing commands, also known as Eventing commands, require the entire dataset in place before the command can run. These commands are not transforming, not distributable, not streaming, and not orchestrating. Some of these commands fit into other command types in specific situations or when specific arguments are used

© 2025 SPLUNK LLC

Command types - simplified

Type	Needs Input Events?	Works On…	Notes
Streaming	✅ Yes	Each event (one by one)	Transforms records in-line
Transforming	✅ Yes	All events (aggregate)	Produces tables/stats
Generating	❌ No	None (starts a search)	Appears first in SPL
Dataset / Eventing	✅ Yes	Whole dataset in memory	Needs all results before output

© 2025 SPLUNK LLC

Custom Command use-cases

What They Are

- Extensions to SPL written in Python (or other languages)
- Packaged inside a Splunk app with configs + metadata
- Behave just like native SPL commands (eval, stats, etc.).

Why They’re Needed

- Add capabilities SPL doesn’t natively support
- Perform complex logic or enrichment with external data/APIs
- Improve reuse and maintainability versus long SPL hacks.

© 2025 SPLUNK LLC

Custom Command use-cases

1. Data Enrichment
- Augment events with external context (e.g., enrich IPs with GeoIP data, user IDs with HR system info).
- Lookup data from APIs or external databases at search time.

2. Advanced Data Processing
- Perform transformations not possible (or cumbersome) with SPL alone.
- Complex calculations (statistical models, custom scoring, ML feature engineering).
- String parsing/manipulation beyond SPL's built-in functions.

3. Pattern Matching & Fuzzy Logic
- Approximate string matching (names, emails, hostnames).
- Deduplication of similar records.
- Error-tolerant joins between datasets.

4. Integrations & Automation
- Call external services or trigger actions during a search.
- Send search results to ticketing systems, messaging platforms, or orchestration tools.
- Real-time decision making (e.g., block IPs via firewall API).

5. Domain-Specific Functions
- Custom parsing for niche log formats.
- Security enrichment (IOC lookups, threat scoring).
- Observability metrics derivation (SLO calculations, error budget burn rates).

6. Performance Optimization
- Move complex logic into Python for efficiency.
- Reduce SPL complexity and improve maintainability of saved searches.

© 2025 SPLUNK LLC

Custom Command vs macro

Feature	Custom Command	Macro
Purpose	Extend SPL with new capabilities in Python or external code.	Reusable SPL snippet, like a search shortcut.
Execution	Runs code during search execution. Can transform, generate, or stream data.	Expands into SPL before the search runs. No extra logic beyond SPL.
Complexity	Can perform complex logic, call APIs, use libraries, and process data.	Limited to what SPL can do. No external logic.
Use Cases	Data enrichment, custom parsing, integrations, advanced analytics.	Simplifying long/complex SPL, parameterizing common searches.
Performance Impact	May add processing time depending on code.	Same performance as the SPL it expands to.

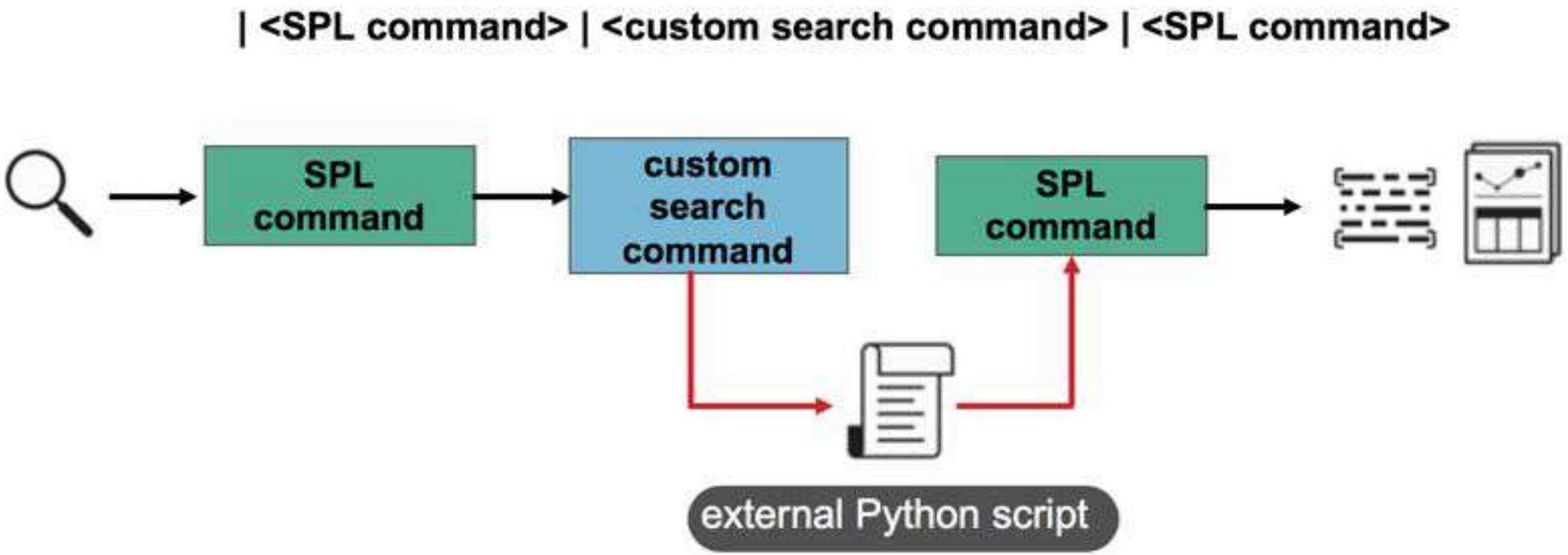
© 2025 SPLUNK LLC

Languages that can be used

Protocol	Description	formats	SDK
Custom Search Command protocol, **Version 2**	Use to create custom commands for a wide range of platforms and executable formats.	.bat, .cmd, .exe, .js, .py, .sh	Splunk SDK for Python
Custom Search Command protocol, Version 1	Use with the Splunk SDK for Python to create custom commands for Python. Use with the Intersplunk.py SDK only to support existing custom commands.	.py	Splunk SDK for Python Intersplunk.py

© 2025 SPLUNK LLC

Custom Command Pipeline



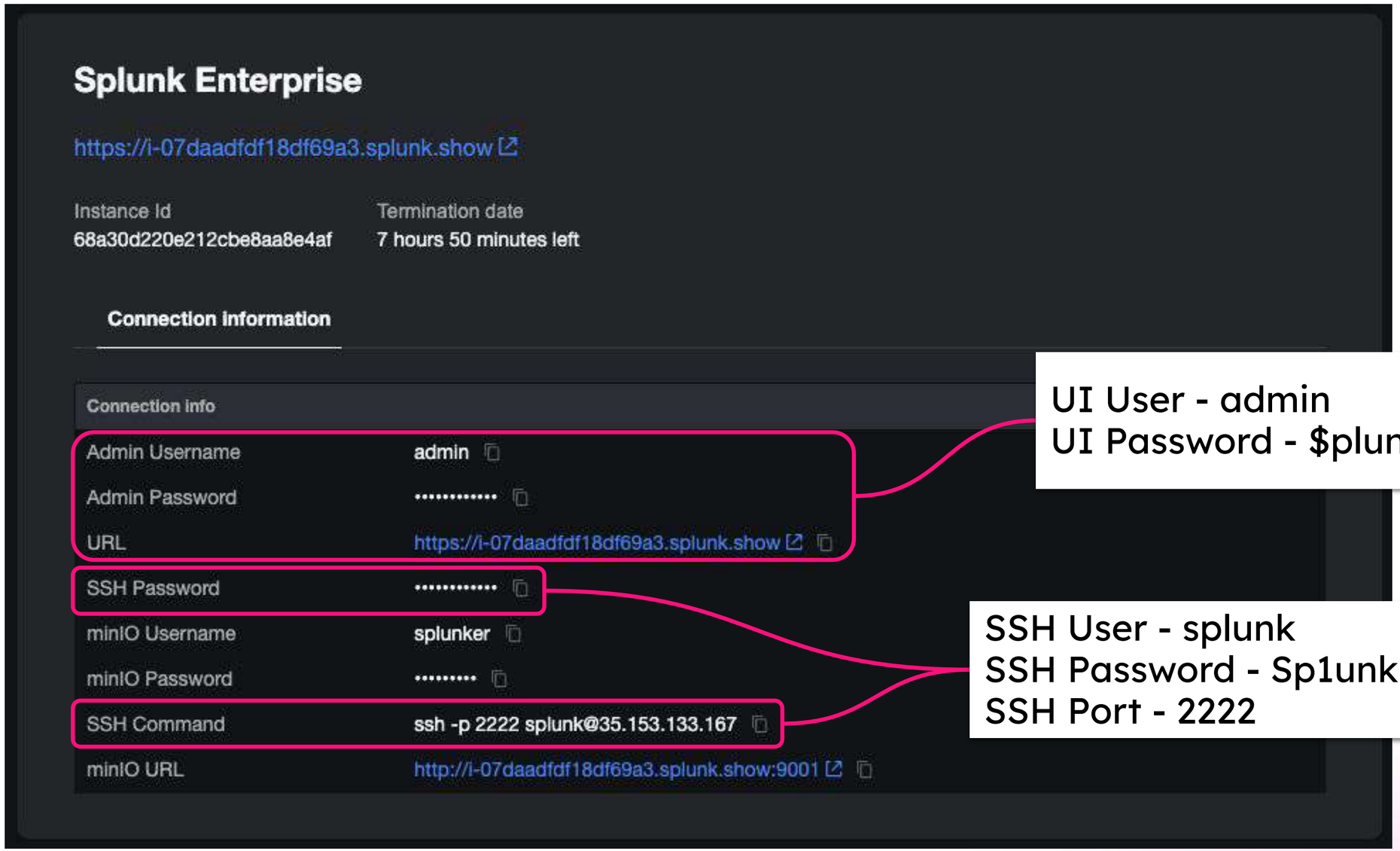
© 2025 SPLUNK LLC

Workflow for creating Custom Command

1. Create a new app in Splunk Enterprise.
2. Install Splunk SDK
3. Inside of your app, create a Python script for your search command.
4. Register the search command.
5. Enable search assistant text for the search command.
6. Package and deploy the app.
7. Modify the app and access control settings.

© 2025 SPLUNK LLC

Lab 0 - Prerequisites



© 2025 SPLUNK LLC

Lab 0 - Prerequisites

© 2025 SPLUNK LLC

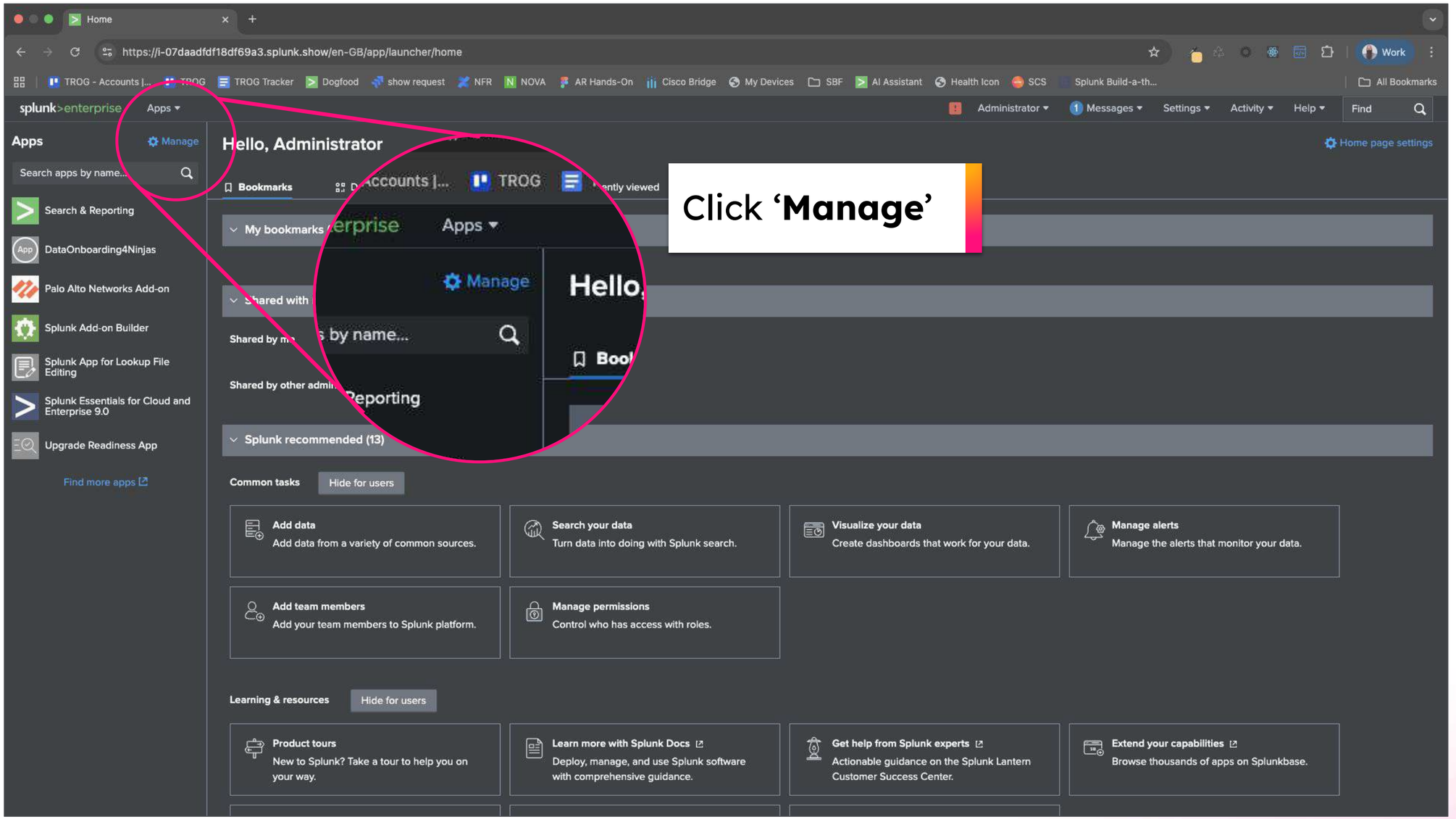
Create an app

Why we need an app

- Packaging – Apps bundle code, configs, and metadata together
- Registration – Splunk only loads commands declared in an app's commands.conf
- Permissions – Apps control visibility/export of commands via default.meta
- Portability – Apps can be installed, versioned, and shared across Splunk instances

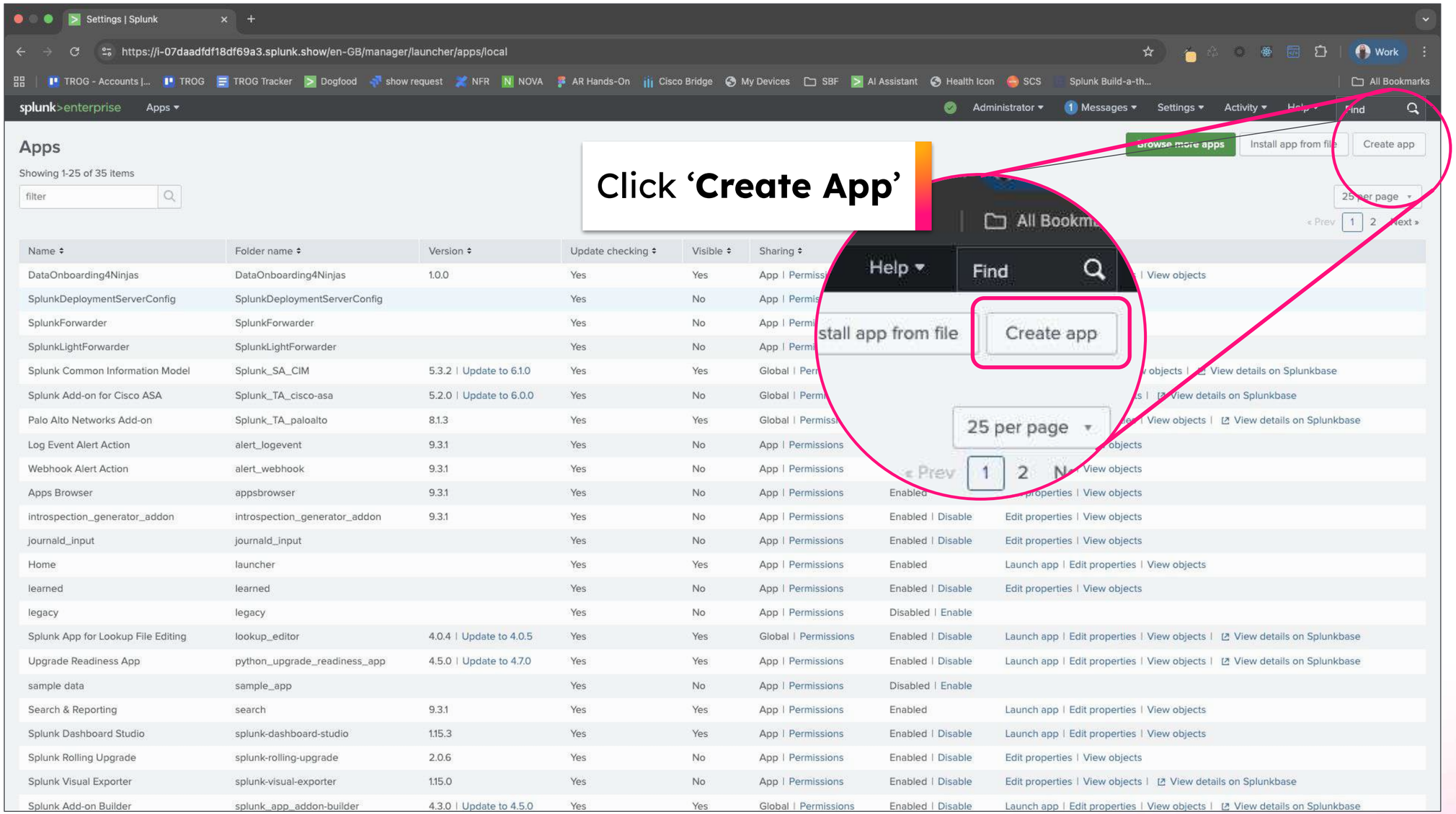
© 2025 SPLUNK LLC

Lab 1 - Create an app



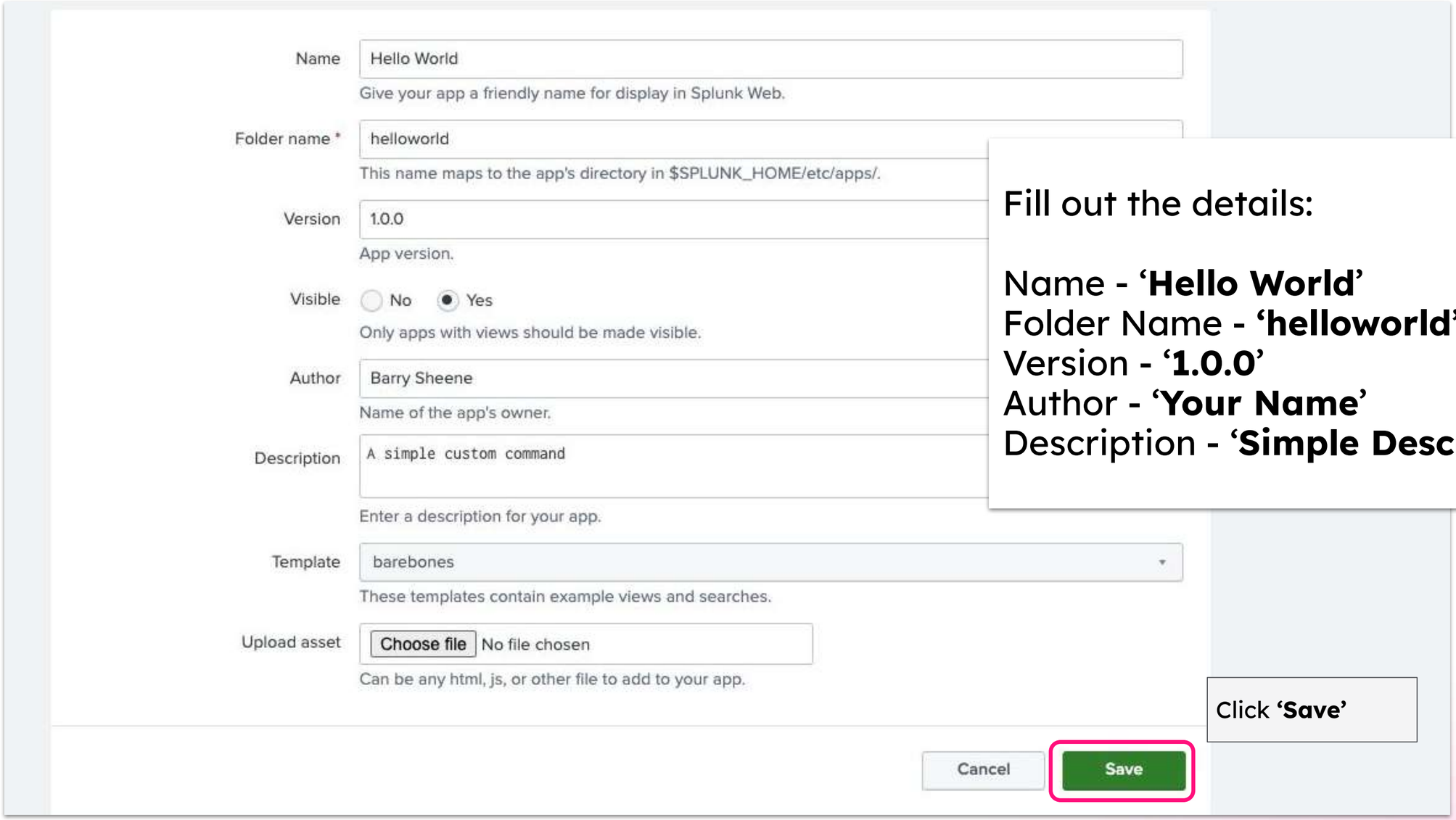
© 2025 SPLUNK LLC

Lab 1 - Create an app



© 2025 SPLUNK LLC

Lab 1 - Create an app



Fill out the details:

Name - '**Hello World**'
Folder Name - '**helloworld**'
Version - '**1.0.0**'
Author - '**Your Name**'
Description - '**Simple Description**'

Click '**Save**'

© 2025 SPLUNK LLC

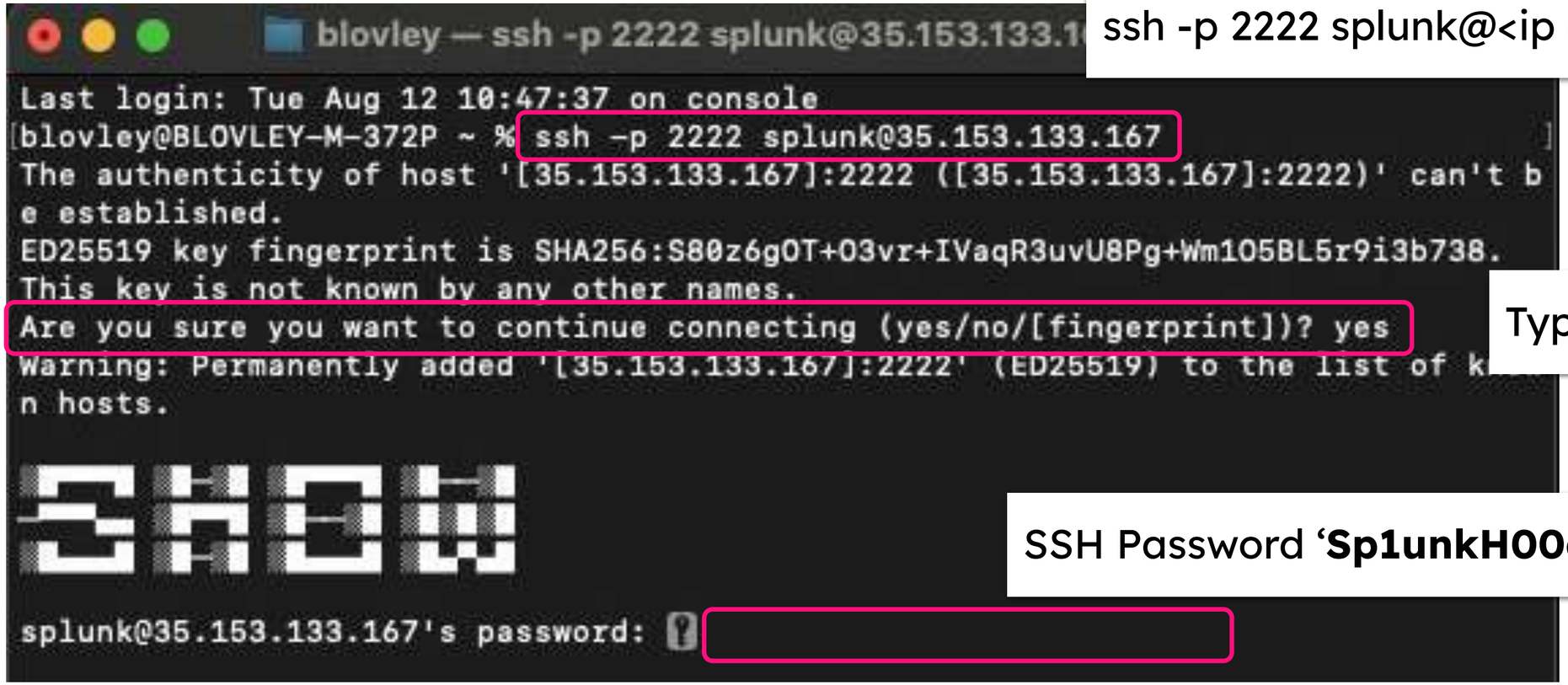
Install the SDK

What’s the SDK for

- Command Framework – Provides the splunklib.searchcommands classes (Streaming, Generating, Transforming).
- Boilerplate Handling – Manages protocol, argument parsing, and dispatch for you.
- Consistency – Ensures your command behaves like any native SPL command.
- Extensibility – Gives access to Splunk REST APIs, service objects, and utilities.

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK



ssh -p 2222 splunk@<ip address>

Type '**yes**'

SSH Password '**Sp1unkH00di3**'

Type '**pwd**'

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK

sudo chown 10777:10777 -R /opt/splunk/etc/apps/helloworld/

to confirm change:

ls -l /opt/splunk/etc/apps/

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK

```
[splunk@show-s4x-config-i-07daadfdf18df69a3:~$ sudo chmod 755 -R /opt/splunk/etc/apps/helloworld
[splunk@show-s4x-config-i-07daadfdf18df69a3:~$ ls -l /opt/splunk/etc/apps/
total 148
drwx------  5 root  root  4096 Aug 16  2023 DataOnboardi
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 SplunkDeploy
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 SplunkForwar
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 SplunkLightF
drwx------ 13 root  root  4096 Oct  1  2024 Splunk_SA_CIM
drwxr-xr-x 11 root  root  4096 Oct  1  2024 Splunk_TA_cisco-asa
drwxr-xr-x 12 root  root  4096 Oct  1  2024 Splunk_TA_paloalto
drwxr-xr-x  7 10777 10777 4096 Sep  5  2024 alert_logevent
drwxr-xr-x  8 10777 10777 4096 Sep  5  2024 alert_webhook
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 appbrowser
drwxr-xr-x  6 10777 10777 4096 Aug  7  2024 appsd
drwxr-xr-x  5 10777 10777 4096 Sep  5  2024 builtin_generat
drwxr-xr-x  4 10777 10777 4096 Oct  1  2024 dashboard
drwxr-xr-x  8 10777 10777 4096 Sep  5  2024 data_manager
drwxr-xr-x  5 10777 10777 4096 Sep  5  2024 dbinput
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 dbx3
drwx------  9 root  root  4096 Oct  1  2024 dmc
drwxr-xr-x 10 10777 10777 4096 Jul 31  2024 eadin
drwxr-xr-x  6 10777 10777 4096 Sep  5  2024 file_monitor
drwxr-xr-x 10 10777 10777 4096 Sep  5  2024 framework
drwxr-xr-x  9 10777 10777 4096 Sep  5  2024 gettingstarted
drwxr-xr-x  8 10777 10777 4096 Jul 31  2024 journal_upgrade
drwxr-xr-x  5 10777 10777 4096 Sep  5  2024 journal_exporter
drwx------ 11 root  root  4096 Oct  1  2024 kvpp_addon-builder
drwxr-xr-x  6 10777 10777 4096 Sep  5  2024 legacy_archiver
drwxr-xr-x  9 10777 10777 4096 Jun 28  2024 splunk_assist
drwxr-xr-x  7 10777 10777 4096 Jun 28  2022 splunk_essentials_9_0
drwxr-xr-x  7 10777 10777 4096 Sep  5  2024 splunk_gdi
drwxr-xr-x  5 10777 10777 4096 Sep  5  2024 splunk_httpinput
drwx------  4 root  root  4096 Apr 28  2022 splunk_ingest_actions
drwxr-xr-x  9 10777 10777 4096 May 20  2024 splunk_instrumentation
drwxr-xr-x  4 10777 10777 4096 Sep  5  2024 splunk_internal_metrics
drwxr-xr-x  8 10777 10777 4096 Sep  5  2024 splunk_metrics_workspace
drwxr-xr-x 13 10777 10777 4096 Aug  7  2024 splunk_monitoring_console
drwxr-xr-x  9 10777 10777 4096 Mar 12  2024 splunk_rapid_diag
drwxr-xr-x 11 10777 10777 4096 Aug  7  2024 splunk_secure_gateway
```

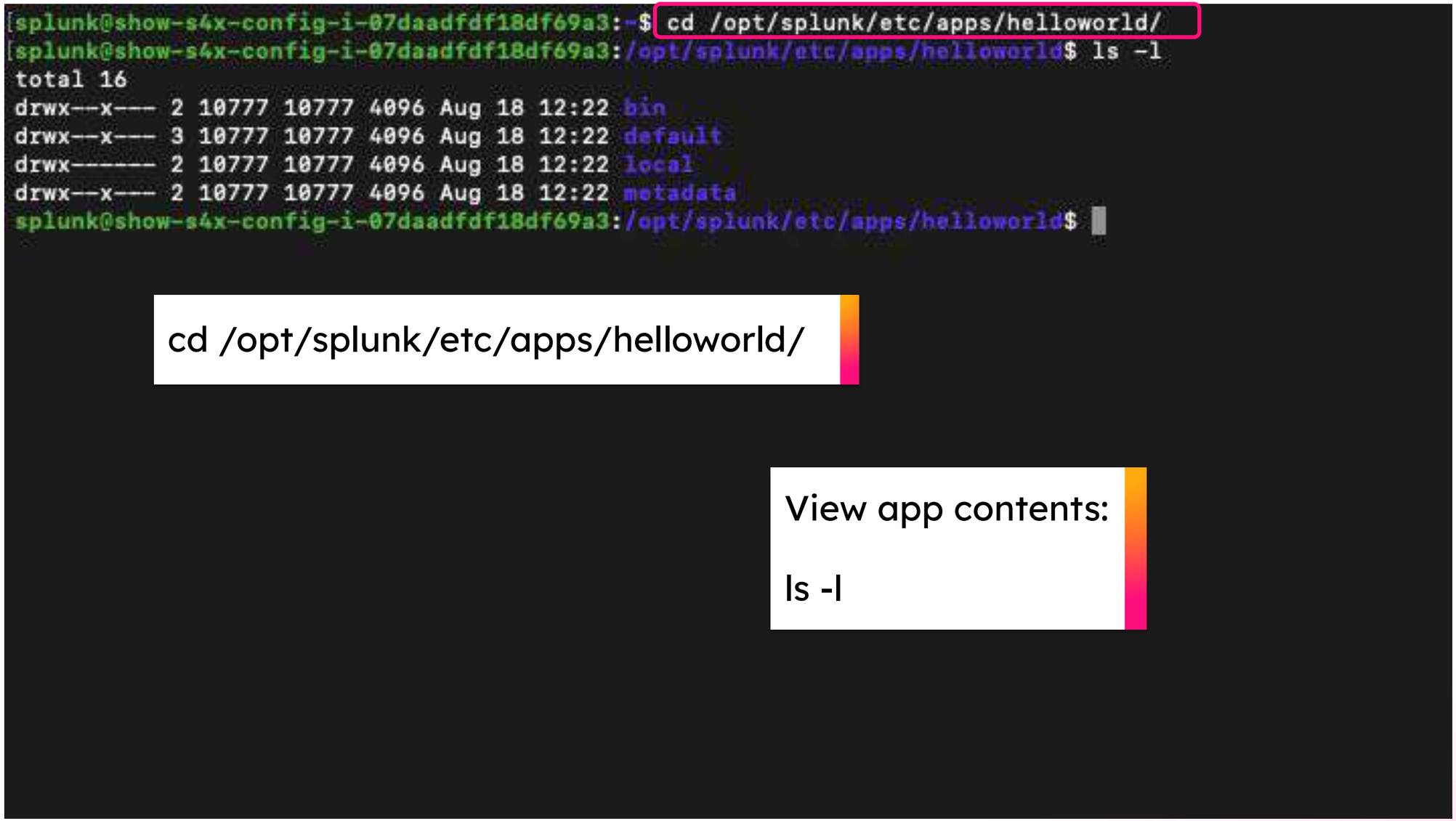
sudo chmod 755 -R /opt/splunk/etc/apps/helloworld/

to confirm change:

ls -l /opt/splunk/etc/apps/

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK



cd /opt/splunk/etc/apps/helloworld/

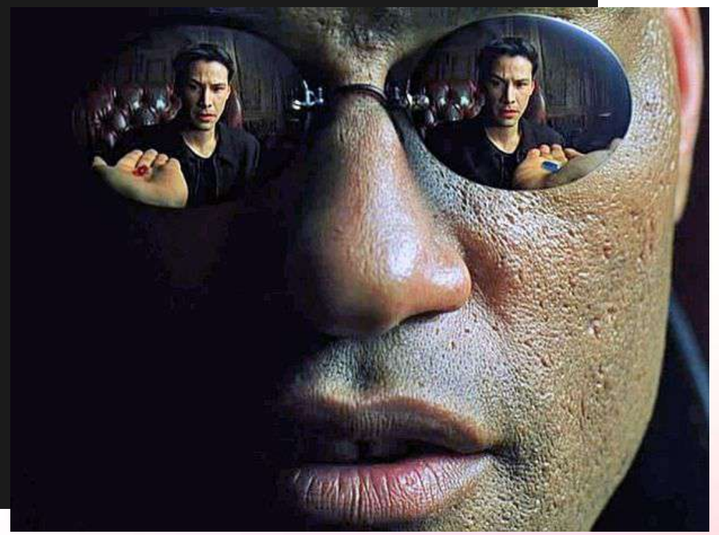
View app contents:

ls -l

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK

```
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ sudo setfacl -R -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ sudo setfacl -d -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ cd bin/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ mkdir splunklib
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ cd splunklib/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ git --version
git version 2.25.1
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ git init splunk-sdk-python
Initialized empty Git repository in /opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python/.git/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ cd splunk-sdk-python
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git remote add origin https://github.com/splunk/splunk-sdk-python.git
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git config core.sparseCheckout true
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ echo splunklib/ >> .git/info/sparse-checkout
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ git pull --depth=1 origin master || git pull --depth=1 origin main
remote: Enumerating objects: 206, done.
remote: Counting objects: 100% (206/206), done.
remote: Compressing objects: 100% (179/179), done.
remote: Total 206 (delta 24), reused 100 (delta 10), pack-reused 0 (from 0)
Receiving objects: 100% (206/206), 457.74 KiB | 8.64 MiB/s, done.
Resolving deltas: 100% (24/24), done.
From https://github.com/splunk/splunk-sdk-python
 * branch            master     -> FETCH_HEAD
 * [new branch]      master     -> origin/master
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ cp -a splunklib/* /opt/splunk/etc/apps/helloworld/bin/splunklib/
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib/splunk-sdk-python$ cd ..
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ rm -rf splunk-sdk-python
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ ls -l
total 288
-rw-r--r-- 1 splunk wheel   1304 Aug 18 13:07 __init__.py
-rw-r--r-- 1 splunk wheel  61070 Aug 18 13:07 binding.py
-rw-r--r-- 1 splunk wheel 152936 Aug 18 13:07 client.py
-rw-r--r-- 1 splunk wheel   8171 Aug 18 13:07 data.py
drwxr-xr-x 2 splunk wheel   4096 Aug 18 13:07 modularinput
-rw-r--r-- 1 splunk wheel  12801 Aug 18 13:07 results.py
drwxr-xr-x 2 splunk wheel   4096 Aug 18 13:07 searchcommands
-rw-r--r-- 1 splunk wheel  34536 Aug 18 13:07 six.py
-rw-r--r-- 1 splunk wheel   1356 Aug 18 13:07 utils.py
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$
```



© 2025 SPLUNK LLC

~~Lab 2~~ - Install Splunk SDK (The real way)

1. Use pip:

```
[sudo] pip install splunk-sdk
```

- Or, run **setup.py** on the resources you cloned from GitHub or downloaded from the Splunk dev site:

```
[sudo] python setup.py install
```

© 2025 SPLUNK LLC

Lab 2 - Install Splunk SDK

from the helloworld directory

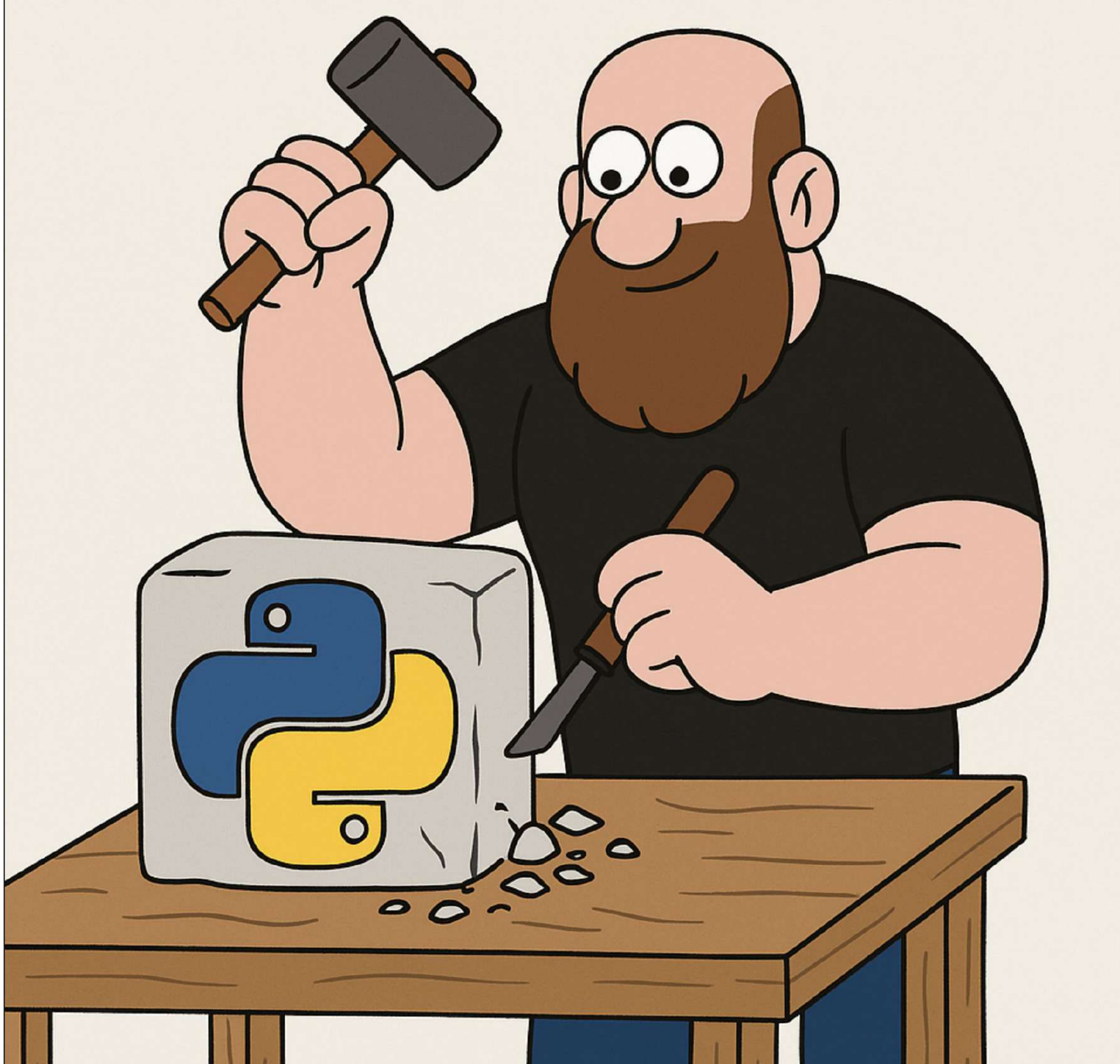
1. sudo setfacl -R -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
2. sudo setfacl -d -m u:splunk:rwx /opt/splunk/etc/apps/helloworld
3. cd bin/
4. mkdir splunklib
5. cd splunklib/
6. git --version
7. git init splunk-sdk-python
8. cd splunk-sdk-python
9. git remote add origin https://github.com/splunk/splunk-sdk-python.git
10. git config core.sparseCheckout true
11. echo splunklib/ >> .git/info/sparse-checkout
12. git pull --depth=1 origin master || git pull --depth=1 origin main
13. cp -a splunklib/* /opt/splunk/etc/apps/helloworld/bin/splunklib/
14. cd ..
15. rm -rf splunk-sdk-python

© 2025 SPLUNK LLC

Create Script

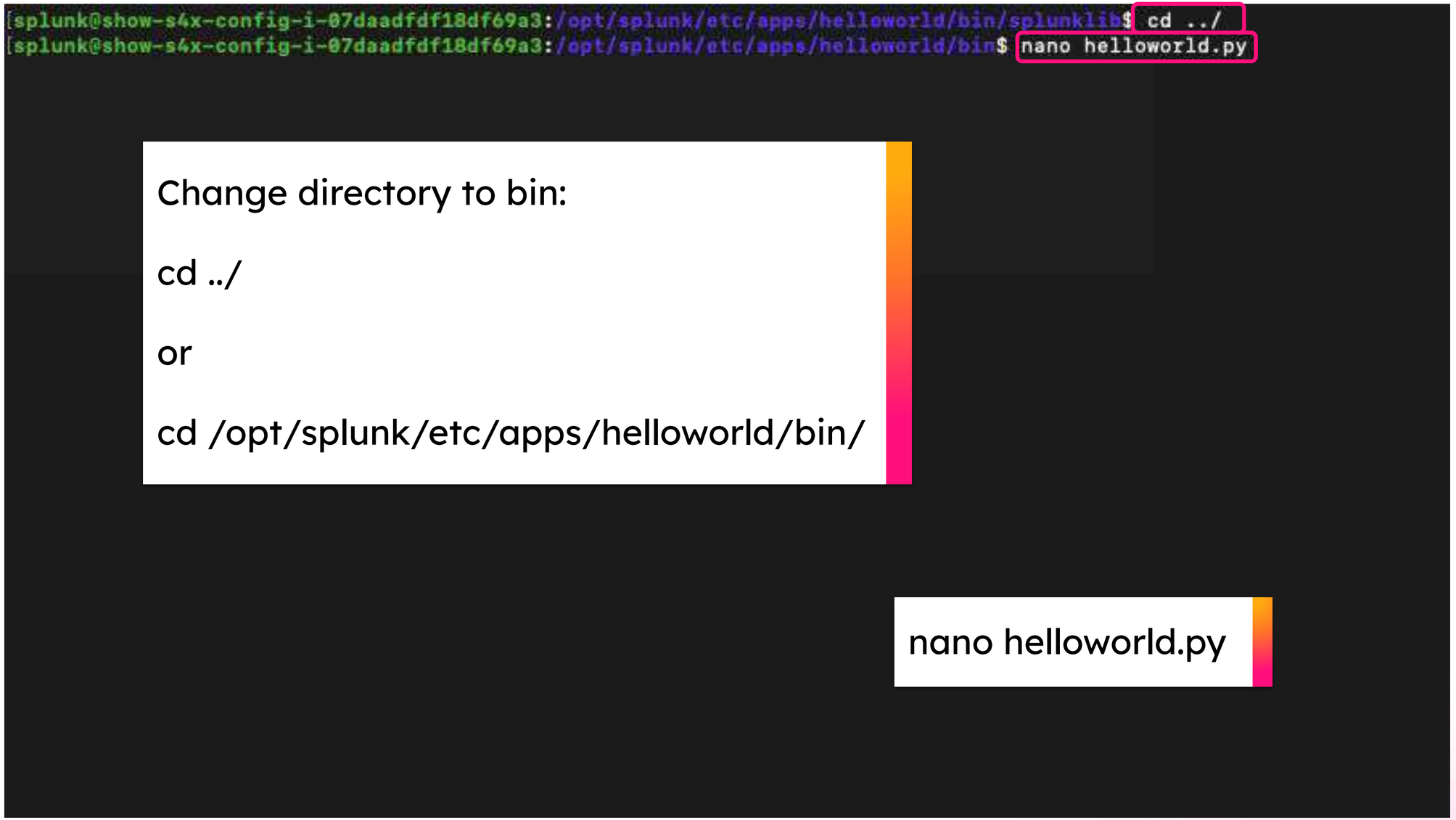
The script itself

- Executable File – A Python script inside your app’s bin/ directory
- Entrypoint – Defines the custom command’s logic (e.g., stream(), generate())
- Uses SDK – Imports splunklib.searchcommands for boilerplate + dispatch
- Integration – Splunk calls it when the command is invoked in SPL



© 2025 SPLUNK LLC

Lab 3 - Create Script



Change directory to bin:

cd ../

or

cd /opt/splunk/etc/apps/helloworld/bin/

nano helloworld.py

© 2025 SPLUNK LLC

Lab 3 - Create Script

© 2025 SPLUNK LLC

Lab 3 - Create Script

```
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin/splunklib$ cd ../
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ nano helloworld.py
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ ls -l
total 12
-rwxrwxr-x+ 1  10777 10777   63 Aug 18 12:22 README
-rw-r--r--  1 splunk wheel  559 Aug 18 13:23 helloworld.py
drwxr-xr-x  4 splunk wheel 4096 Aug 18 13:08 splunklib
splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$
```

Script now present

© 2025 SPLUNK LLC

Register the command

Why do we register it

- Discovery – Tells Splunk the command exists and what script it maps to.
- Configuration – Defines type (streaming, generating, transforming) and options.
- Visibility – Controls where the command is available (app-only or system-wide).
- Reliability – Ensures Splunk loads it correctly at startup and handles errors.

© 2025 SPLUNK LLC

Lab 4 - Register Command

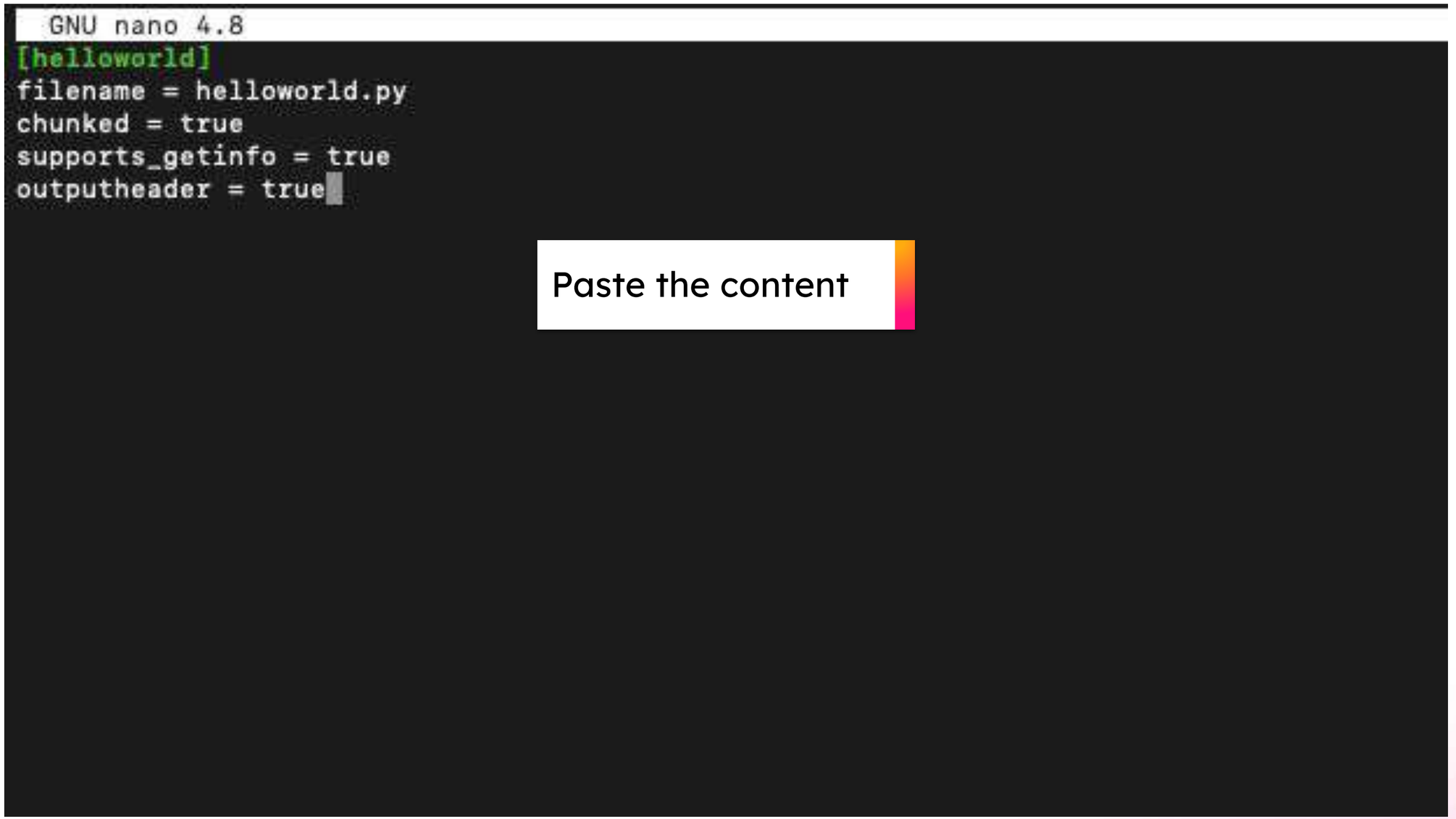
```
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ cd /opt/splunk/etc/apps/helloworld/default/
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ ls -l
total 8
-rwxrwxr-x+ 1 10777 10777  195 Aug 18 12:22 app.conf
drwxrwxr-x+ 3 10777 10777 4096 Aug 18 12:22 data
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/default$ nano commands.conf
```

navigate to the app ‘default’ directory

nano commands.conf

© 2025 SPLUNK LLC

Lab 4 - Register Command

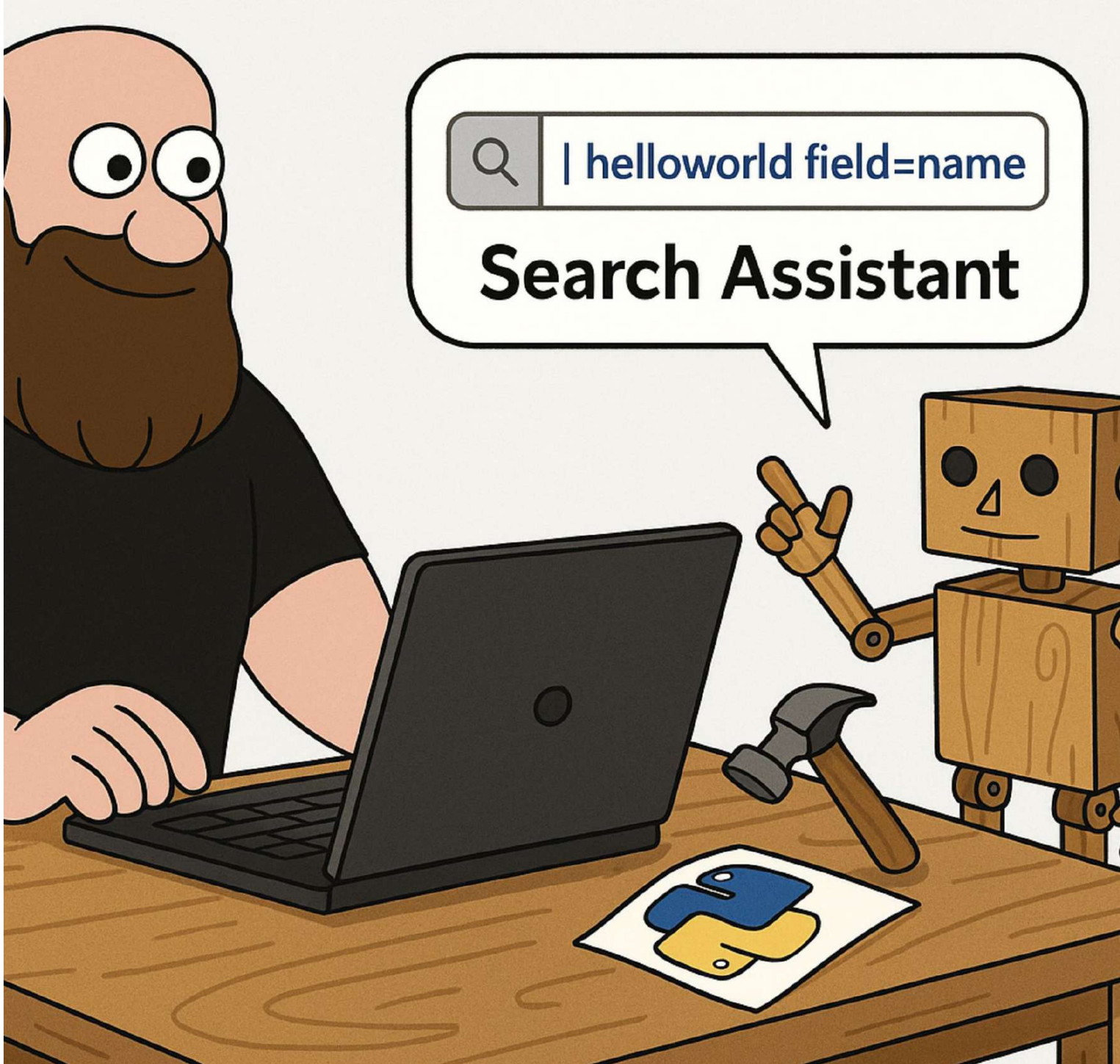


© 2025 SPLUNK LLC

Search Assistant

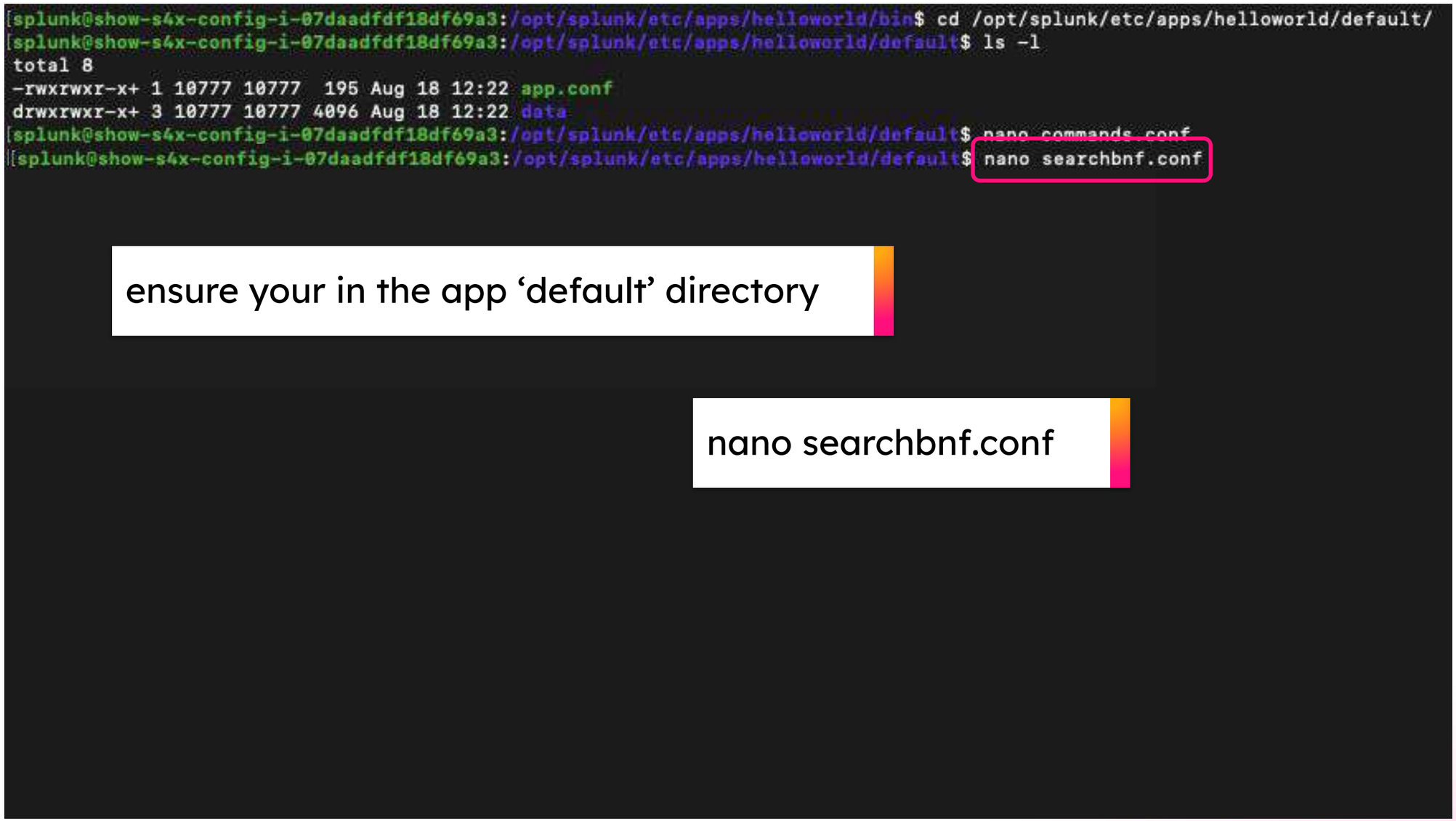
Why we need an app

- Guidance – Provides inline help so users know how to run your command
- Discoverability – Makes the command appear in SPL auto-complete menus
- Clarity – Shows syntax, arguments, and usage examples as users type
- Adoption – Reduces trial-and-error, encouraging others to actually use it



© 2025 SPLUNK LLC

Lab 5 - Enable Search Assistant



© 2025 SPLUNK LLC

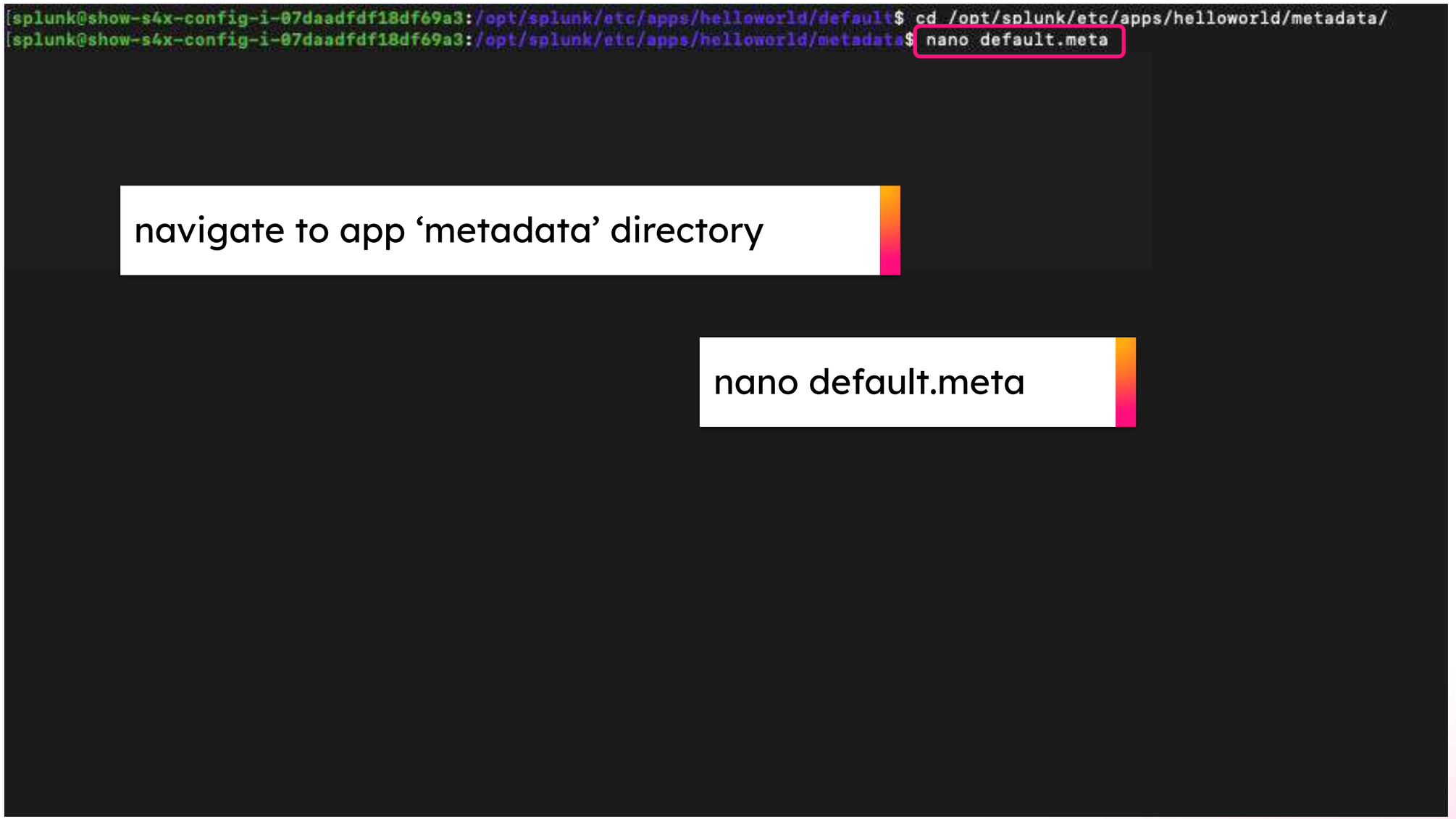
Lab 5 - Enable Search Assistant

```
  GNU nano 4.8
[helloworld-command]
syntax = HELLOWORLD FIELD=<field>
shortdesc = Returns a new field that says "hello <field value>".
description = \
    The helloworld command adds a new field called 'helloworld' that prepends 'hello ' to the value \
    of the specified field.
example1 = \
    | makeresults | eval name="Alice" | helloworld field=name
arguments.field = Required. The name of the field whose value will be prepended with "hello ".
category = streaming
usage = public
appears-in = 1.0
maintainer = you
```

Paste the content

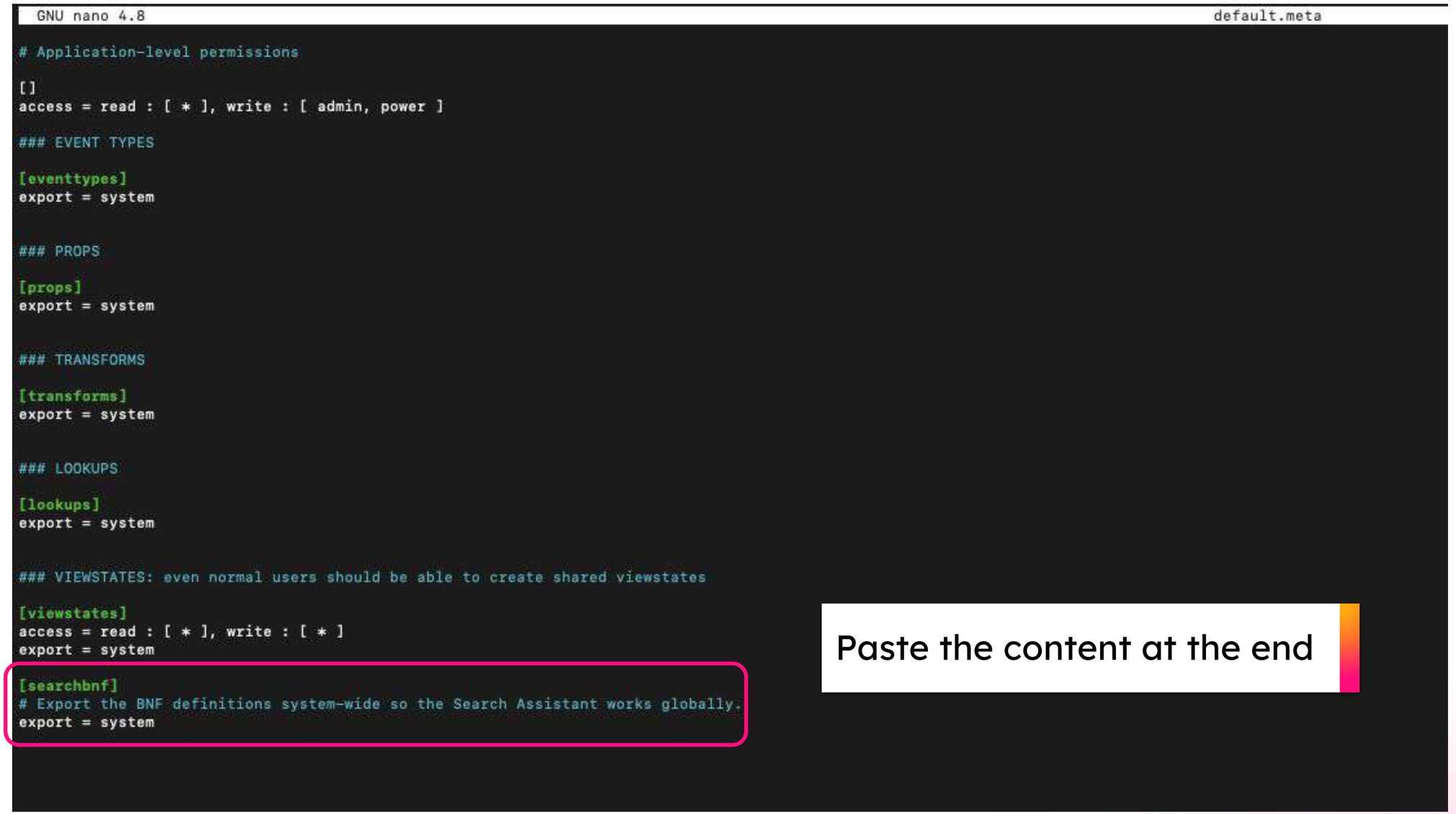
© 2025 SPLUNK LLC

Lab 5 - Enable Search Assistant



© 2025 SPLUNK LLC

Lab 5 - Enable Search Assistant



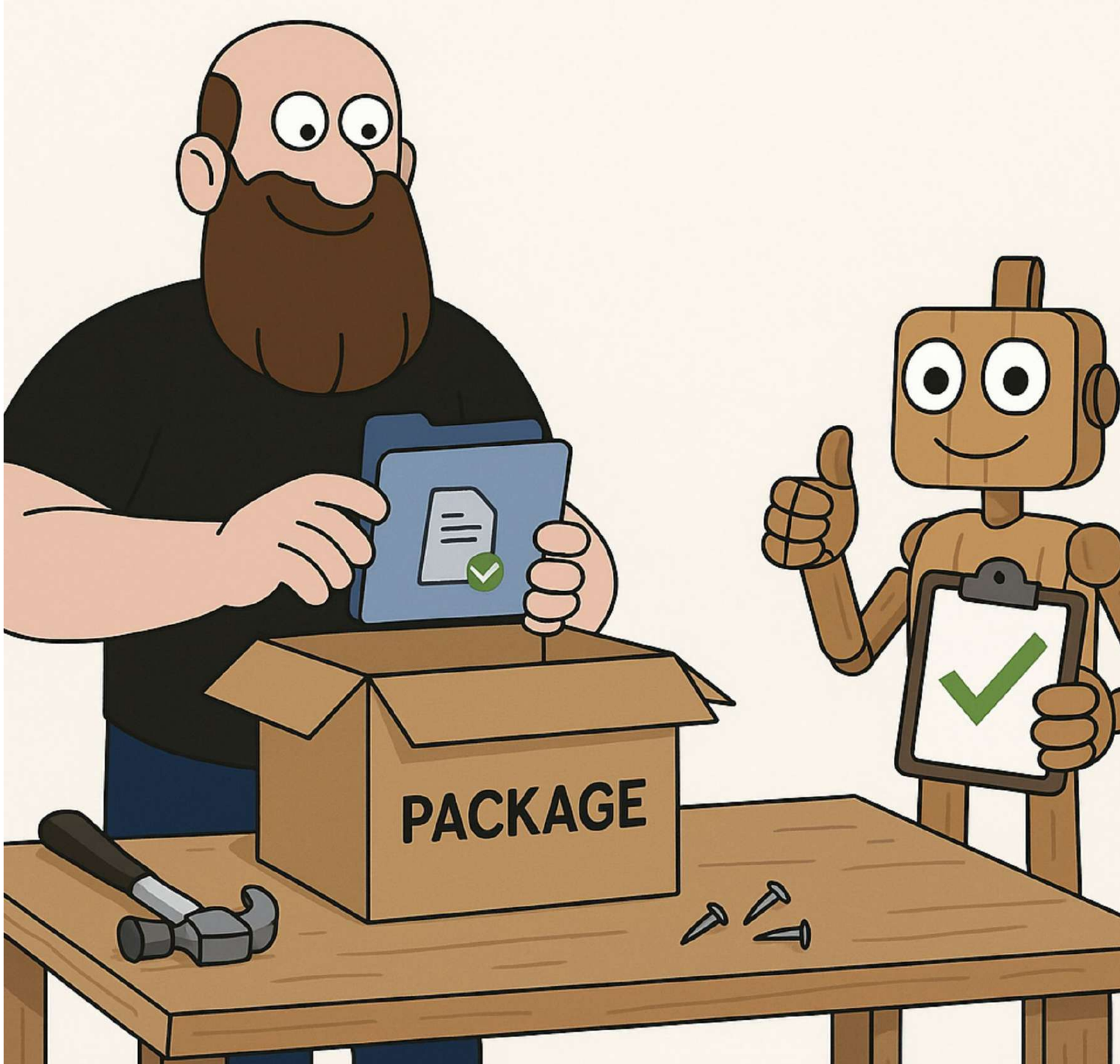
Paste the content at the end

© 2025 SPLUNK LLC

Package and test

Why we need an app

- Reload Configs – Ensures commands.conf, searchbnf.conf, and default.meta are applied
- Register Commands – Splunk discovers and loads new custom scripts
- Clear State – Resets cached settings and permissions for a clean test
- Verify Changes – Confirms your app and command are working end-to-end



© 2025 SPLUNK LLC

Lab 6 - Deploy and test

```
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld$ cd bin/
 splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ chmod 755 /opt/splunk/etc/apps/helloworld/bin/helloworld.py
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ ls -l
 total 12
 -rwxrwxr-x+ 1  10777 10777   63 Aug 18 12:22 README
 -rwxr-xr-x  1 splunk wheel  559 Aug 18 13:23 helloworld.py
 drwxr-xr-x  4 splunk wheel 4096 Aug 18 13:08 splunklib
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/bin$ sudo /opt/splunk/bin/splunk restart
```

navigate to app ‘bin’ directory

chmod 755 /op/splunk/apps/helloworld/bin/helloworld.py

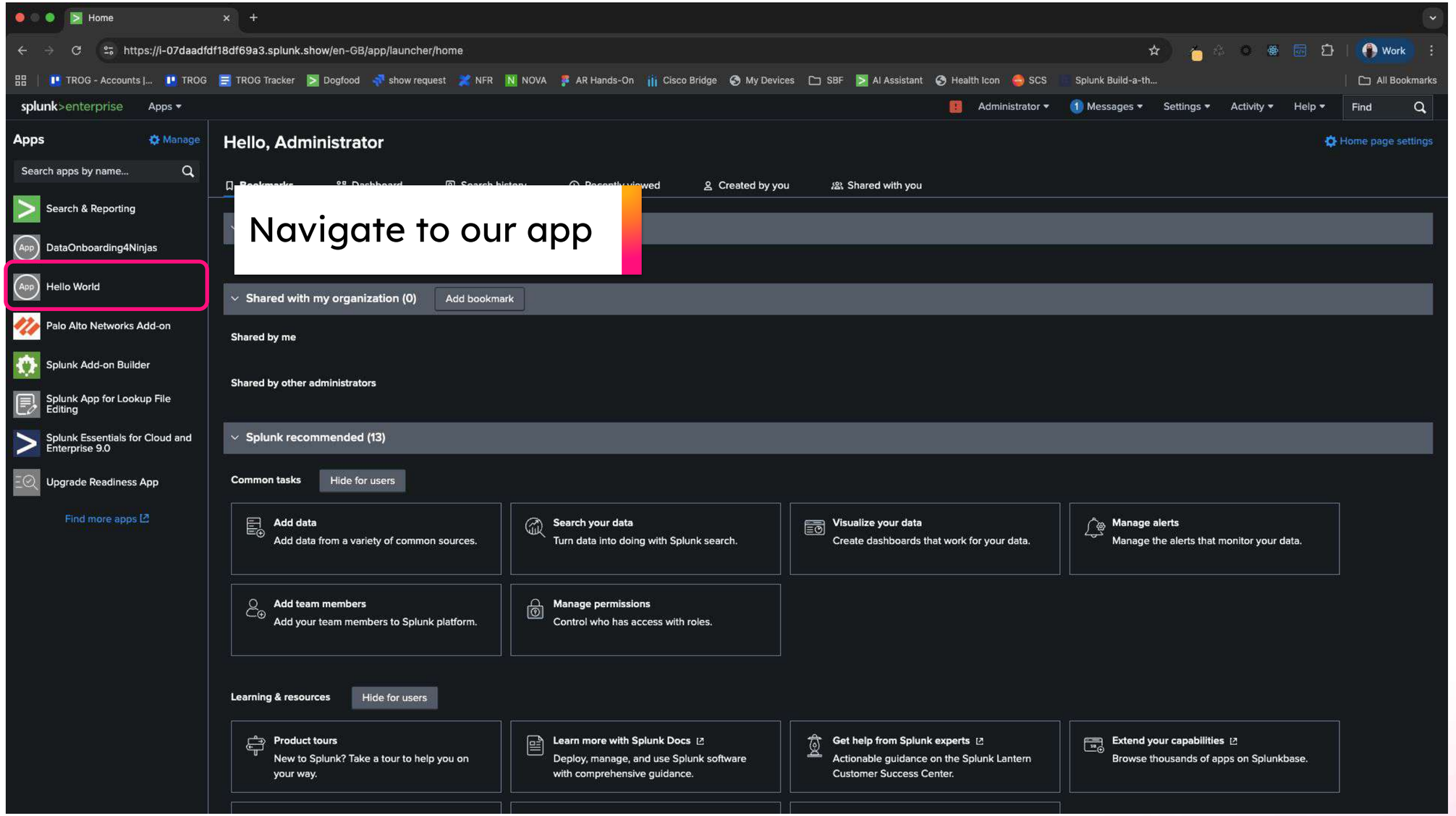
sudo /opt/splunk/bin/splunk restart

© 2025 SPLUNK LLC

Lab 6 - Deploy and test

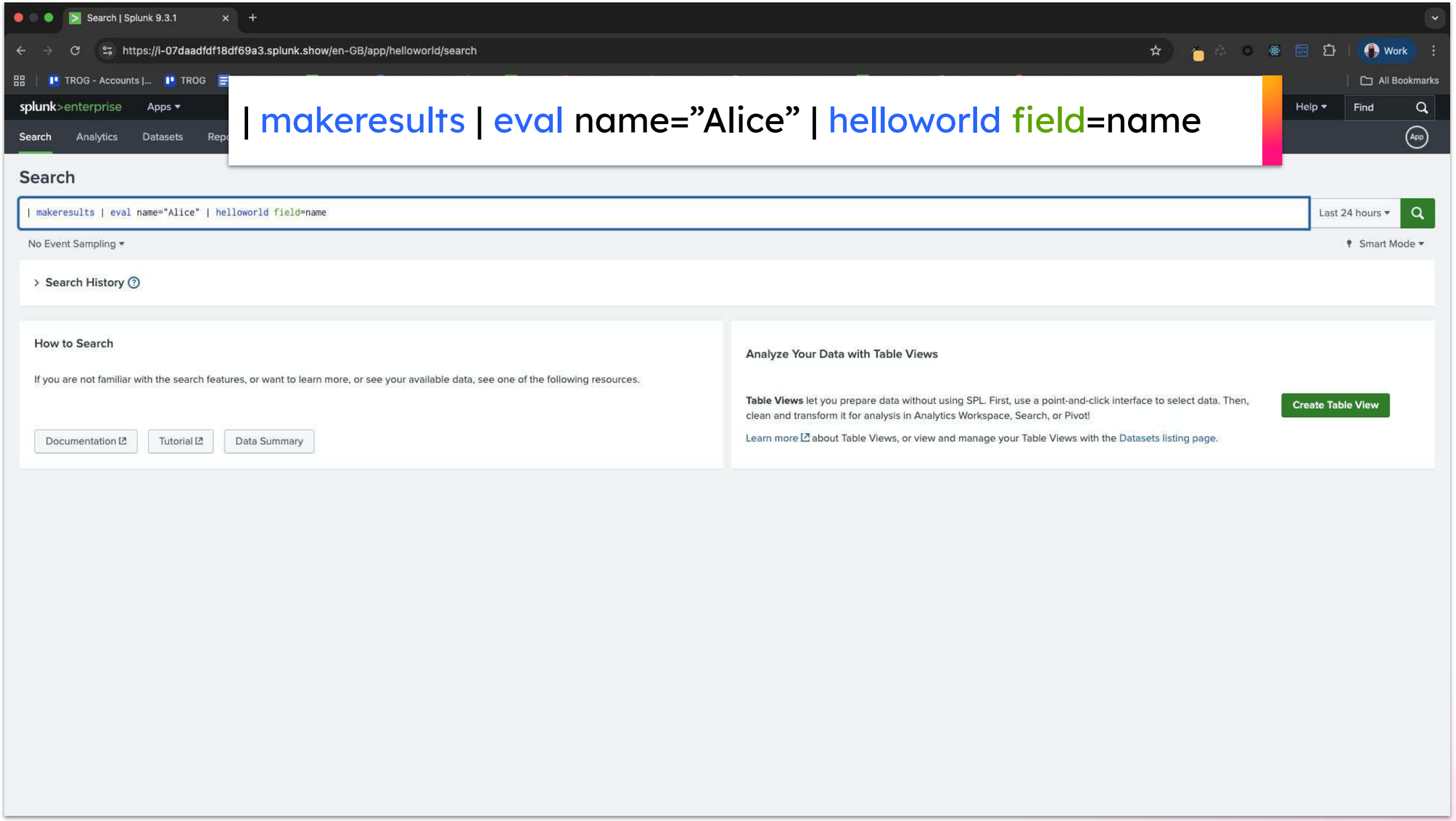
© 2025 SPLUNK LLC

Lab 6 - Deploy and test



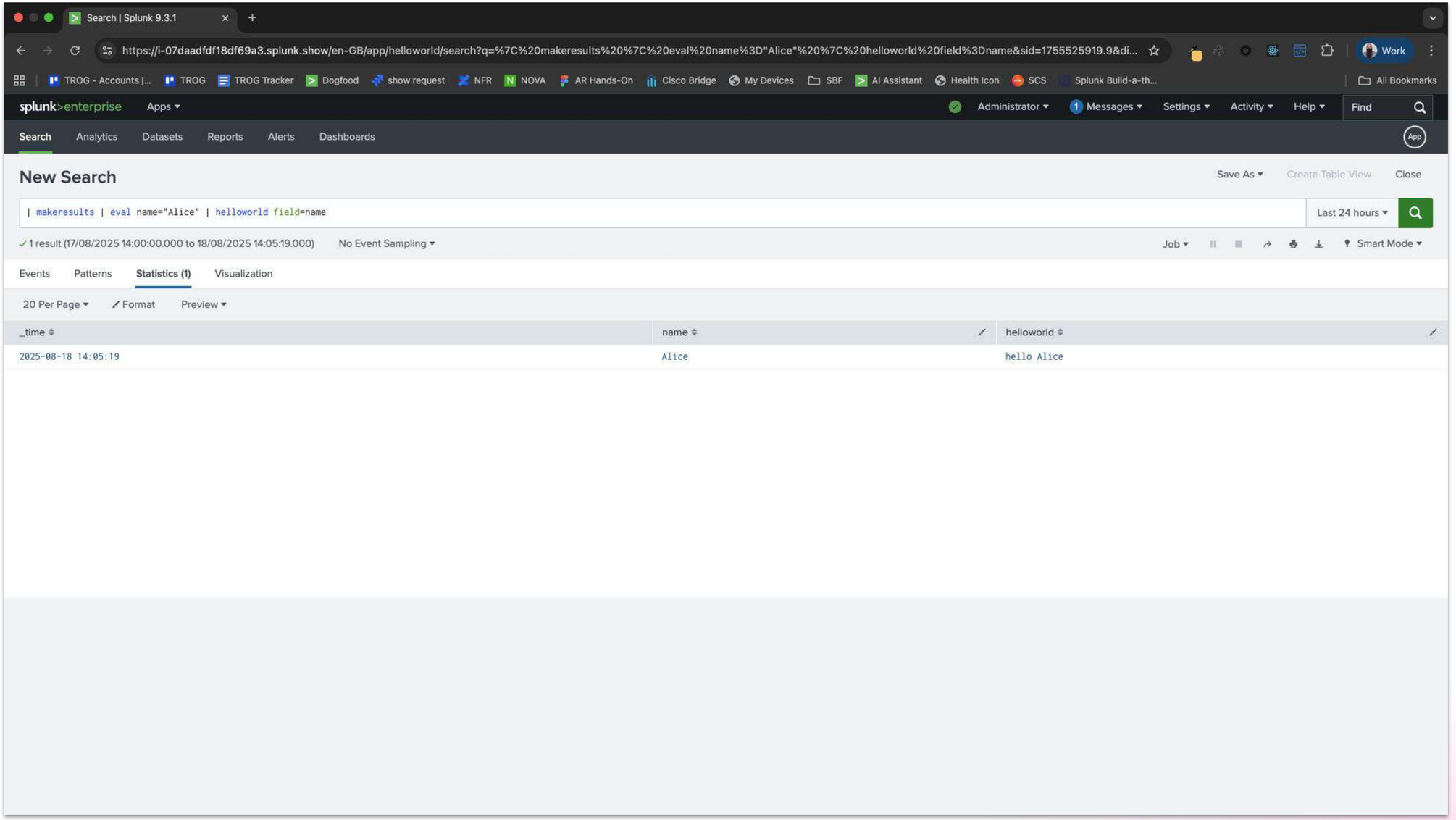
© 2025 SPLUNK LLC

Lab 6 - Deploy and test



© 2025 SPLUNK LLC

Lab 6 - Deploy and test



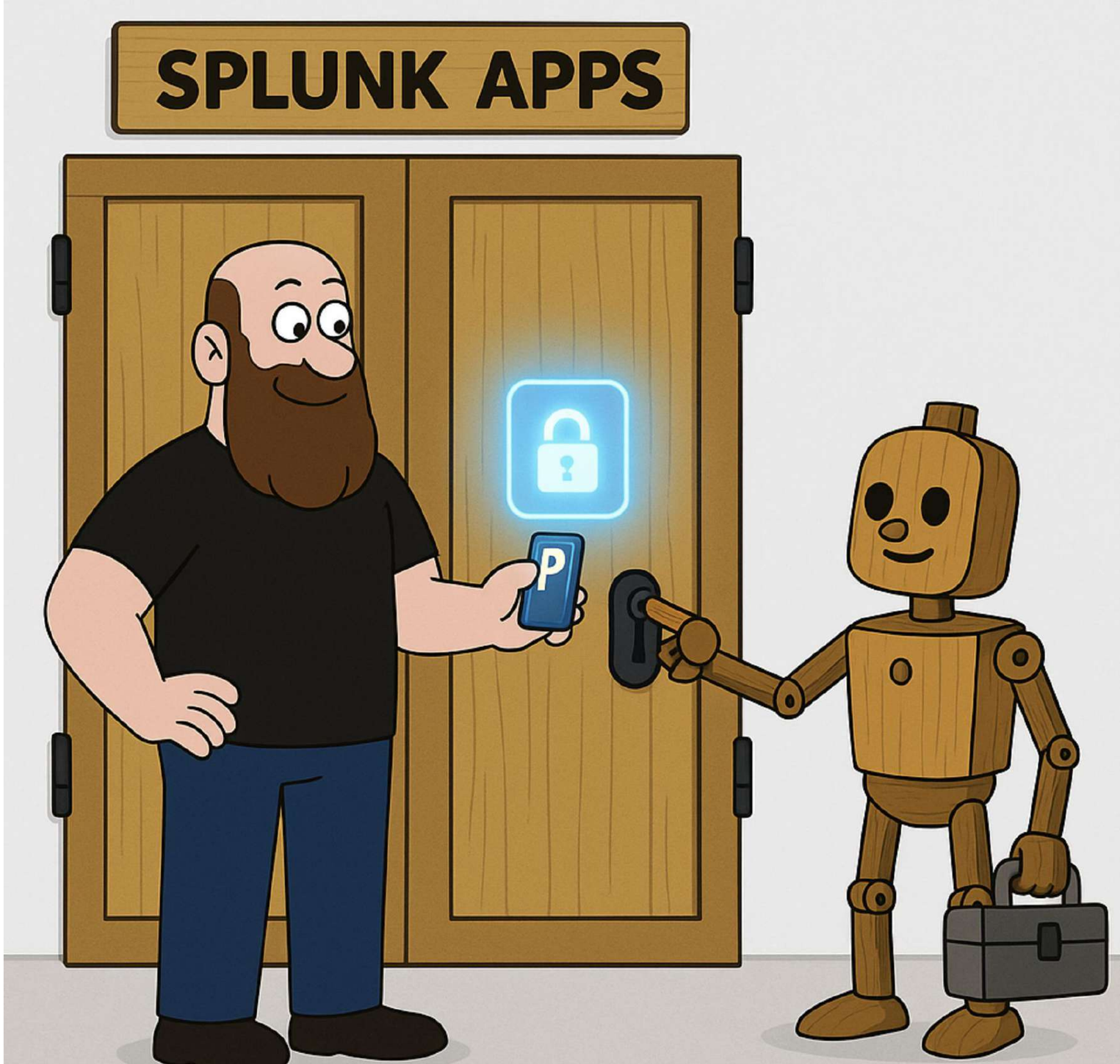
© 2025 SPLUNK LLC

Modify app access

Why we do it

- Cross-App Use – Makes the command callable from any app, not just its home app
- Collaboration – Lets all users and roles benefit without duplicating code
- Control – Manage visibility with default.meta

  (read/write and export rules)
- Consistency – Ensures one shared definition instead of scattered copies



© 2025 SPLUNK LLC

Lab 7 - Modify App access

ssh -p 2222 splunk@<ip address>

SSH Password '**Sp1unkH00di3**'

© 2025 SPLUNK LLC

Lab 7 - Modify App access

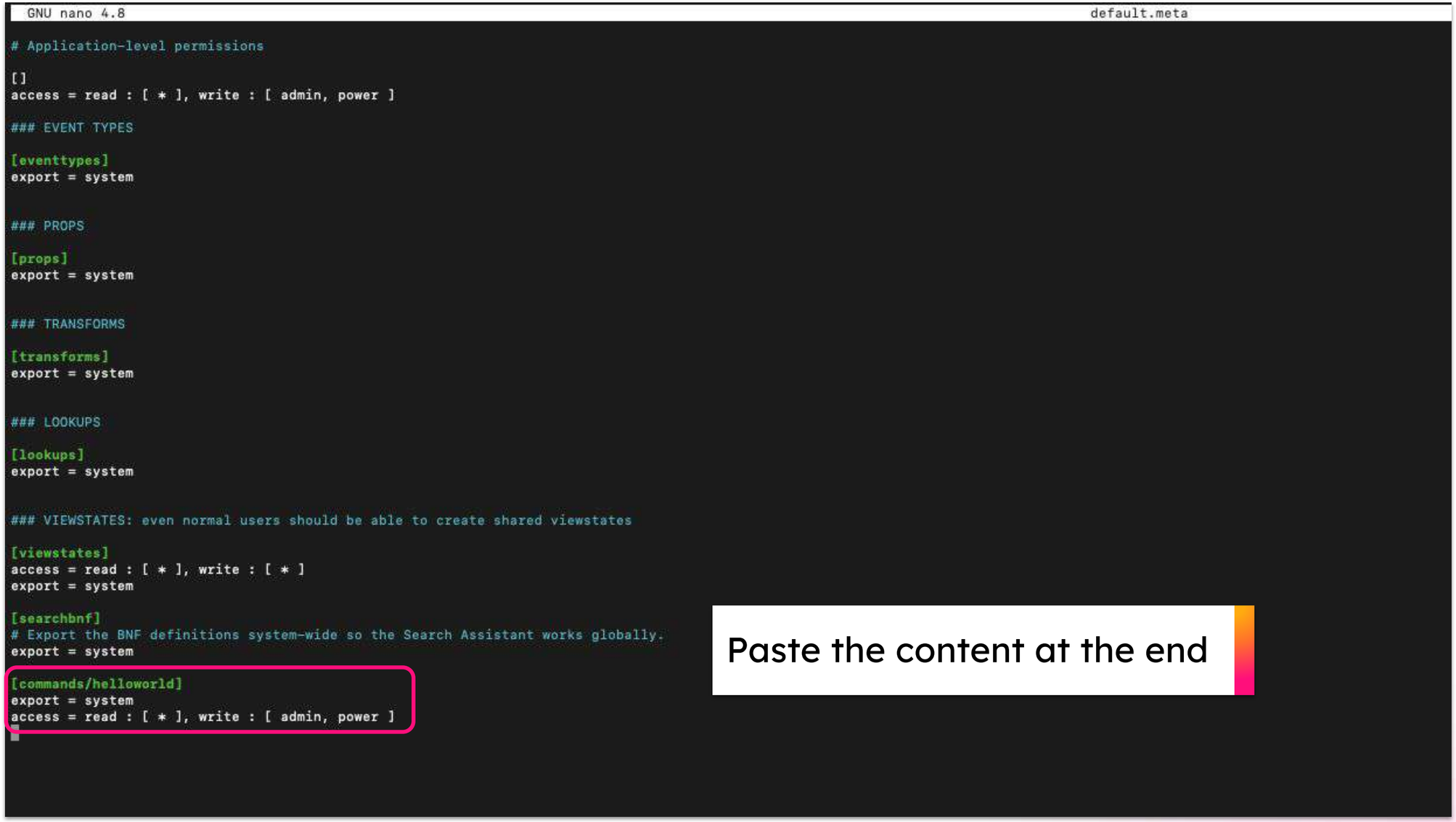
```
[splunk@show-s4x-config-i-07daadfdf18df69a3:~$ cd /opt/splunk/etc/apps/helloworld/metadata/
[splunk@show-s4x-config-i-07daadfdf18df69a3:/opt/splunk/etc/apps/helloworld/metadata$ nano default.meta
```

navigate to app ‘metadata’ directory

nano default.meta

© 2025 SPLUNK LLC

Lab 7 - Modify App access



Paste the content at the end

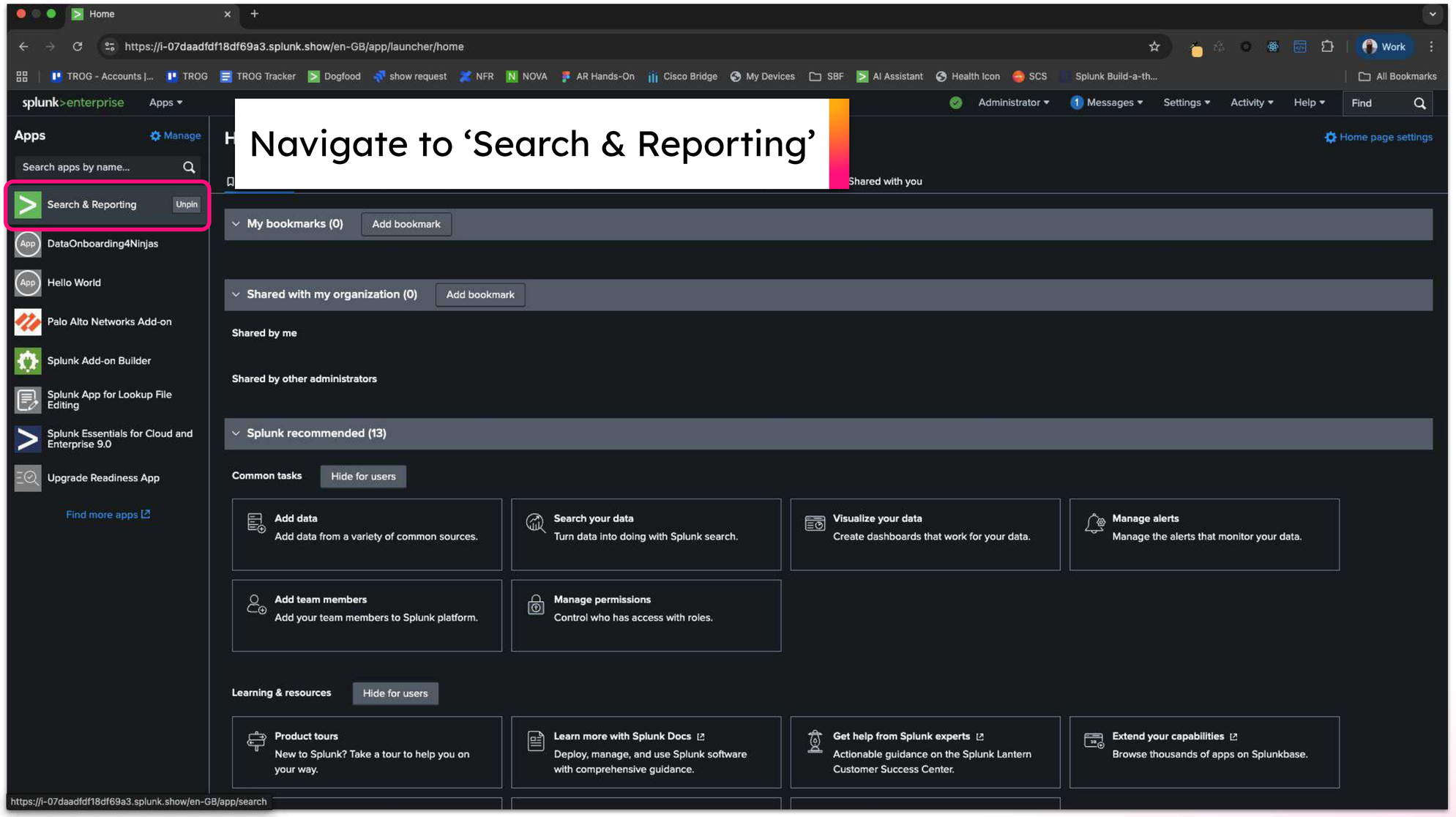
© 2025 SPLUNK LLC

Lab 7 - Modify App access

sudo /opt/splunk/bin/splunk restart

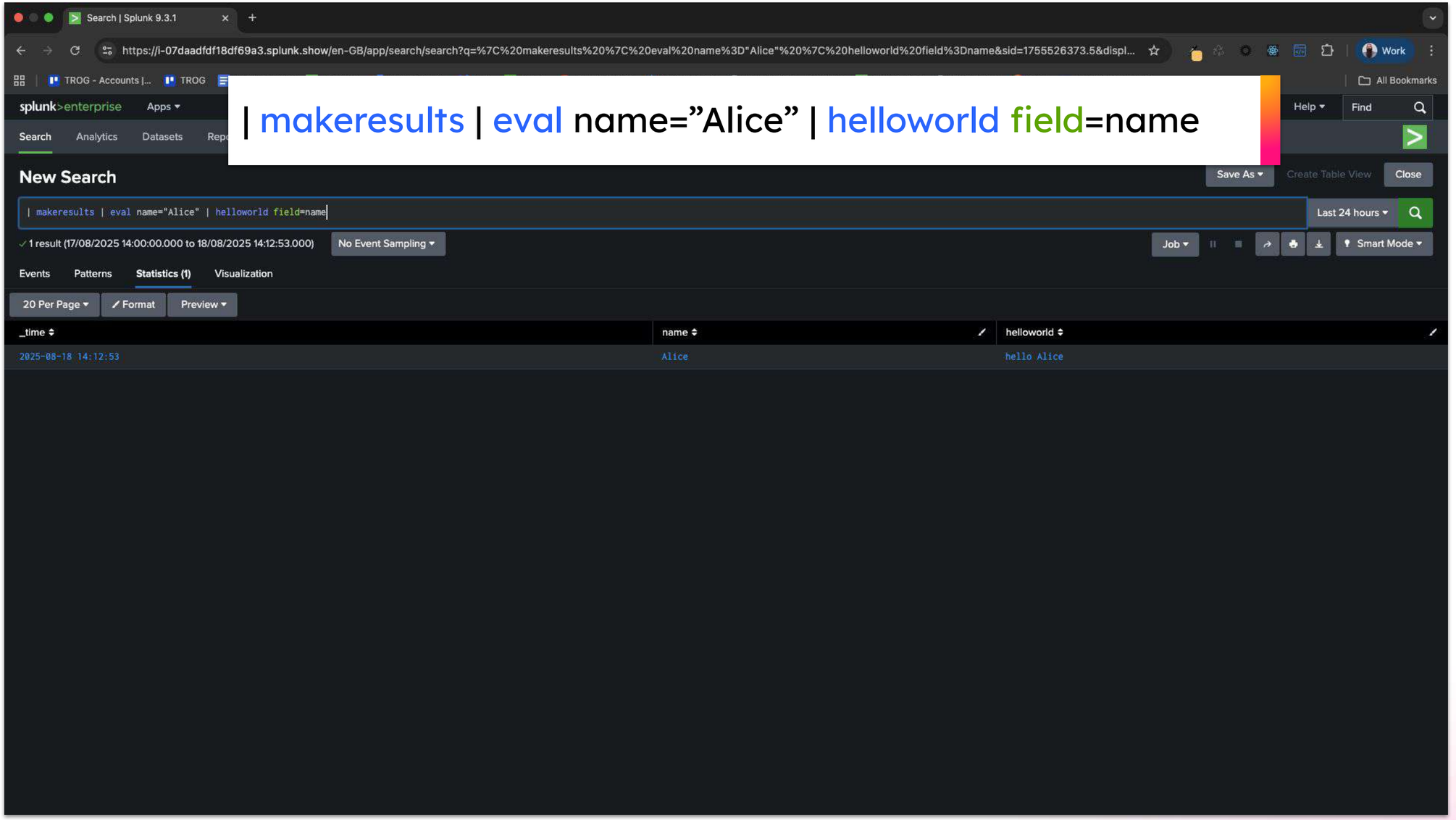
© 2025 SPLUNK LLC

Lab 7 - Modify App access



© 2025 SPLUNK LLC

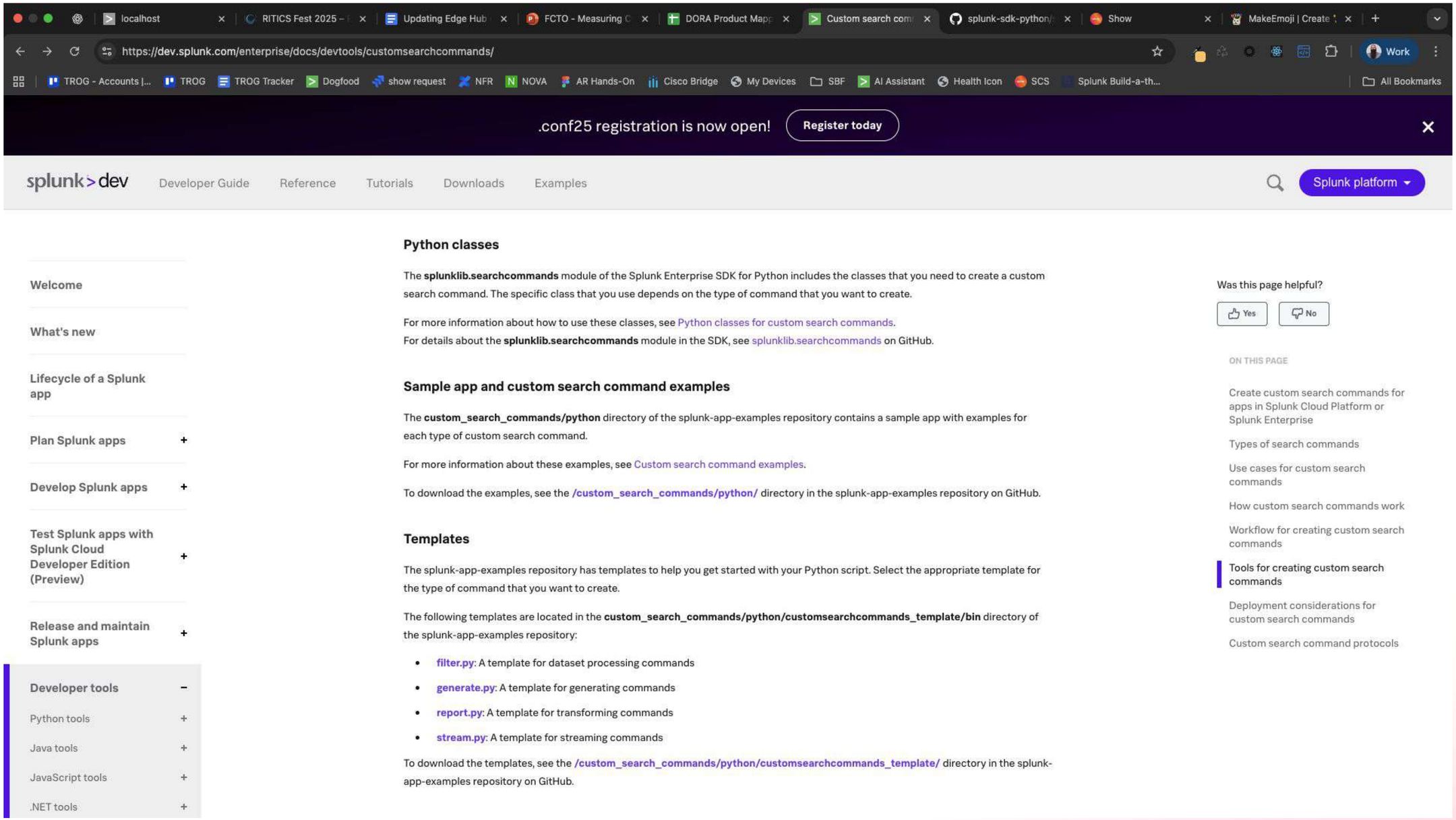
Lab 7 - Modify App access



| makeresults | eval name=”Alice” | helloworld field=name

© 2025 SPLUNK LLC

Tools for creating custom search commands



© 2025 SPLUNK LLC

Deployment considerations

In a distributed deployment, the tier that a custom search command runs on depends on the command type.

See Types of commands in the Splunk Enterprise Search Manual for more information.

If a custom search command uses the REST API to access secrets or other custom configurations in your app, the command needs to run on the search head.

If the command is a streaming command, you need to configure the command not to deploy to the indexer tier. See Deploy a streaming command on the search head for more information.

© 2025 SPLUNK LLC

Thank you

splunk> a CISCO company

© 2025 SPLUNK LLC