

Splunk4Admins

Apps

<Customer Name>

<TSE/TAM Name>



splunk>
a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see 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 reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about 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. We undertake no 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.

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

© 2024 Splunk Inc. All rights reserved.





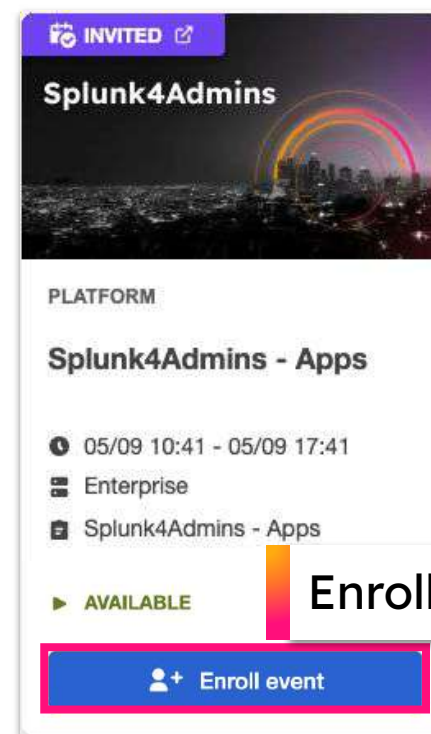
Enroll in Today's Workshop

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://show.splunk.com/event/<eventID>>
3. Download the hands-on lab guide:
<https://splk.it/S4A-Apps-Lab-Guide>

Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
<https://splk.it/S4A-Apps-Attendee>

Goal



Enroll in today's event

Please introduce yourself!

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



Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunkbase
 - Splunk Cloud
 - Upload to Cloud via GUI - Lab 4
 - AppInspect vetting
- Summary

Audience

Who is this Workshop for?

- Those who are interested in how to observe and detect issues within Splunk ...
 - Splunk Admins
 - “Required”: Power User Certified
 - “Preferred”: Splunk Admin enabled (at least started ...), Certified

Expectations for Workshop

Apps and Technology Add-Ons - hereinafter “apps” or “TAs”

- Last roughly 60-75 minutes
- Understand what makes up an app or TA, including files
- Experience how to install a complete app or TA in Enterprise OnPremise
- Experience how install a complete app or TA in Splunk Cloud
- Unable to provide examples of all of the ways to build and install, representative samples

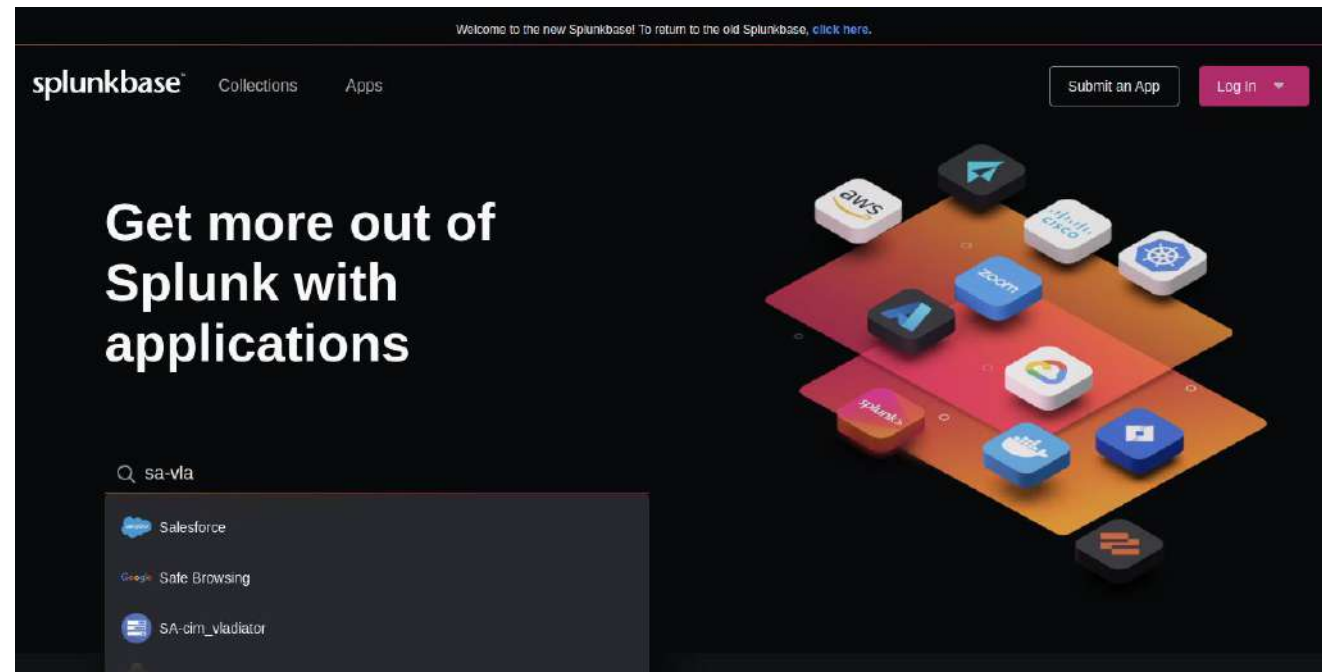
What is an “app” or “TA” or “SA”?

- Apps are ways to define solutions for Splunk - can include:
 - Dashboards
 - Ingest configurations - including sourcetypes, fields, ...
 - Modular inputs/scripts/REST interactions
 - Any set of configurations, can be partitioned off with permissions and role access
 - And any other settings ...
- TA = Technology Add-on (**TA-corelight**)
 - Limited-scope, potentially reusable code/configuration extension, typically associated with an App, will frequently have custom commands included specific to a correlated app
- SA = Supporting Add-on (**SA-cim_vladiator**)
 - Sets of configurations that can be used with other apps, frequently include custom commands, but not as tightly correlated to other apps

What are Splunk Apps and Add-Ons ?	https://www.splunk.com/en_us/blog/tips-and-tricks/what-are-splunk-apps-and-add-ons.html
What is a Splunk app?	https://dev.splunk.com/enterprise/docs/welcome/#What-is-a-Splunk-app
Developing Views and Apps for Splunk Web	https://docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/Whatsinthismanual
Apps and add-ons	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp

Splunkbase?

- Thousands of apps/TAs/SAs have been created
- Many supported by Splunk
- Many NOT supported by Splunk
- Available from <https://splunkbase.splunk.com> with login auth: splunk.com
- Provides official access to apps, includes checksum validation
- Splunk-supported, developer-supported, unsupported
 - Developer-supported - meeting a specific need
 - Many created by other corporations - for example - Palo Alto



Not Splunkbase?

- Private app/TAs/SAs
- Made to specific requirements for each customer
- Entirely customizable to customer needs
- Supported by the customer

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunkbase
 - Splunk Cloud
 - Upload to Cloud via GUI - Lab 4
 - AppInspect vetting
- Summary

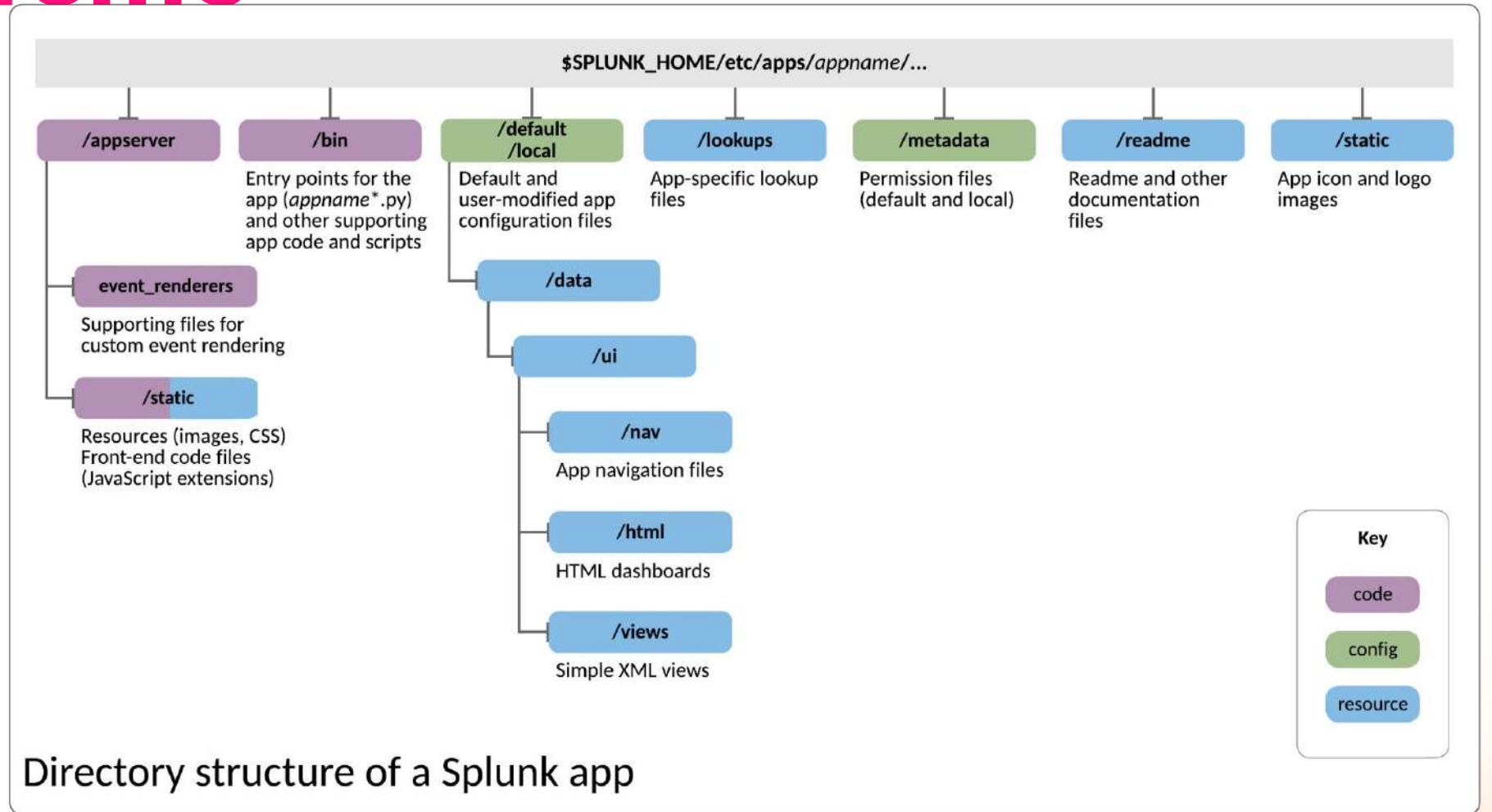
What makes an app?

- Files, files, files ...
 - .conf - many, many .conf files
 - inputs.conf, macros.conf, savedsearches.conf ...
 - \$SPLUNK_HOME/etc/apps/App_name/default, .../local, .../metadata, .../lookups, .../bin, .../appserver
- Binaries/scripts for the relevant OS to accomplish specific tasks
- REST call definitions to other compute resources
- Database calls to database environments
- Schedules
- Dashboard definitions in either JSON or XML

What is a Splunk app?	https://dev.splunk.com/enterprise/docs/welcome/#What-is-a-Splunk-app
Developing Views and Apps for Splunk Web	https://docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/Whatsinthismanual
Getting Data In	https://docs.splunk.com/Documentation/Splunk/latest/Data/Usingapps
Developing a Private App for Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/DevApp/Overview

App contents

- Based on location of files in the hierarchy under `$SPLUNK_HOME/etc/apps` (or `peer-apps`, `shcluster/apps` ...)



Understand file precedence in apps for Splunk Cloud Platform or Splunk Enterprise

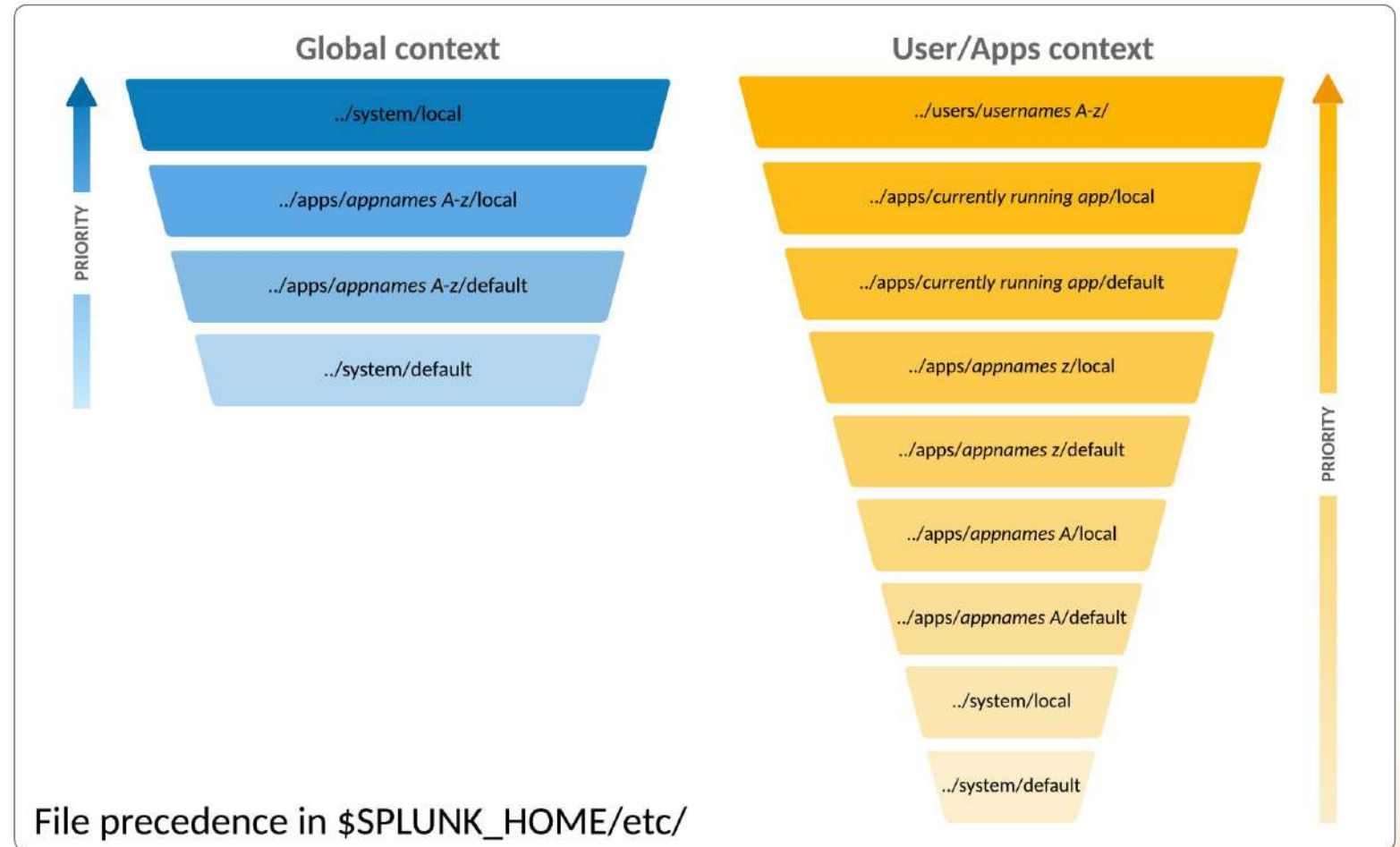
<https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/fileprecedence/>

Configuration file precedence

<https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles>

App context - Precedence

- How are apps “layered”
- Based on location of files in the hierarchy under \$SPLUNK_HOME/etc

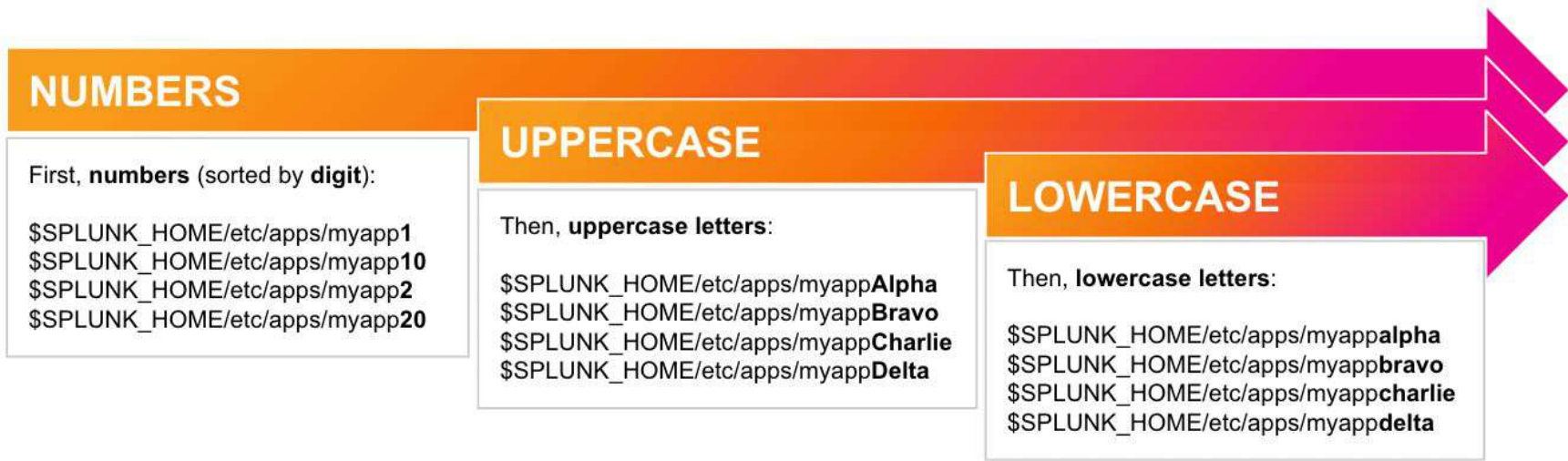


Understand file precedence in apps for Splunk Cloud Platform or Splunk Enterprise
Configuration file precedence

<https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/fileprecedence/>
<https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles>

App context - Precedence and Naming

- How are apps “layered”
- Based on location of files in the hierarchy under \$SPLUNK_HOME/etc
- And the name of the app ...



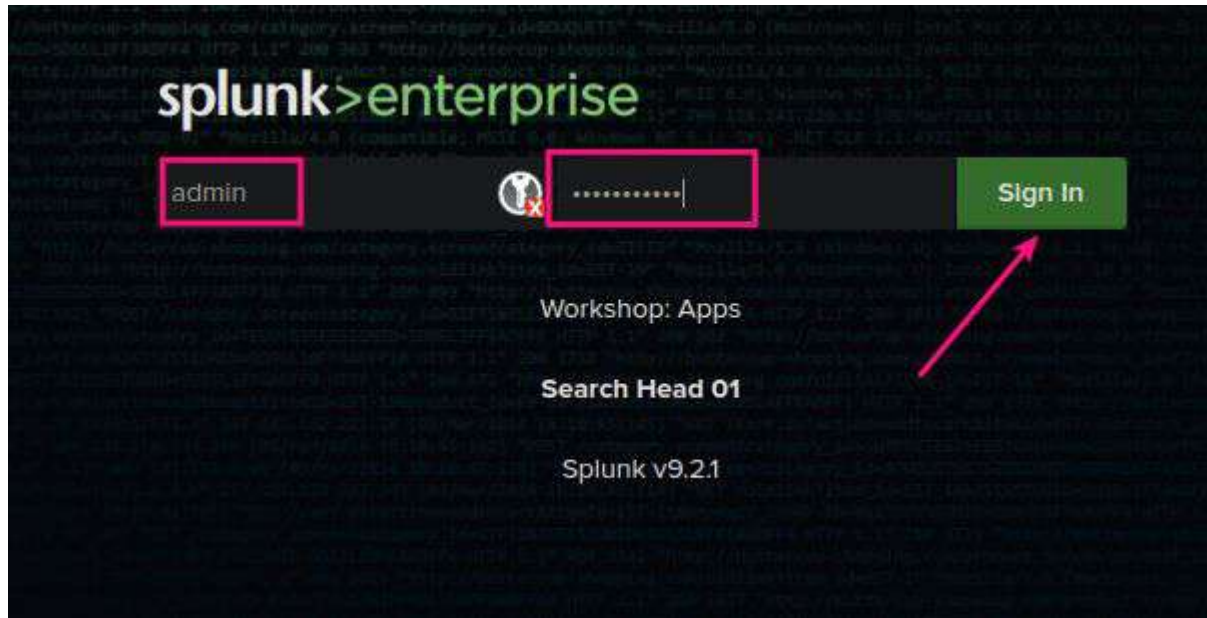
- Suggestion for naming convention
 - <company|department_name>_<purpose>_<(app|add-on|function)>

Naming conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Understand file precedence in apps for Splunk Cloud Platform or Splunk Enterprise	https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/fileprecedence/
Configuration file precedence	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles

App context - Demonstration



- See a field description in global vs. app context



App context - Demonstration



- See a field description in global vs. app context

Original (correct)

Search & Reporting

New Search

1 index=_internal sourcetype=splunkd_ui_access
2 | stats count by method

✓ 459 events (8/9/24 4:05:34.000 PM to 8/9/24 4:20:34.000 PM) No Event Sampling Job

Events Patterns Statistics (2) Visualization

100 Per Page Format Preview

method	count
GET	459
POST	0

Global (broken)

Search & Reporting

New Search

1 index=_internal sourcetype=splunkd_ui_access
2 | stats count by method

✓ 872 events (8/9/24 4:12:13.000 PM to 8/9/24 4:27:13.000 PM) No Event Sampling Job

Events Patterns Statistics (5) Visualization

100 Per Page Format Preview

method	count
en-US+200	833
en-US+201	17
en-US+303	17
en-US+304	4
en-US+404	1

In app (broken)

Search & Reporting

New Search

1 index=_internal sourcetype=splunkd_ui_access
2 | stats count by method

✓ 552 events (8/9/24 4:06:27.000 PM to 8/9/24 4:21:27.000 PM) No Event Sampling Job

Events Patterns Statistics (5) Visualization

20 Per Page Format Preview

method	count
en-US+200	535
en-US+201	4
en-US+303	10
en-US+304	2
en-US+404	1

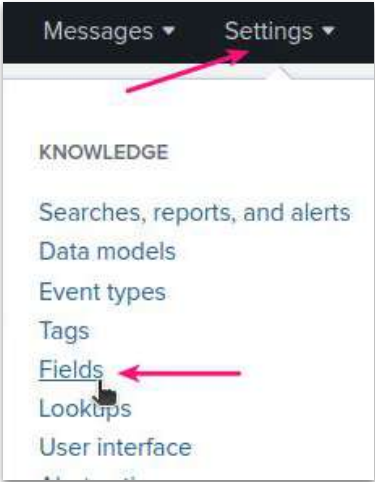
default.meta.conf

<https://docs.splunk.com/Documentation/Splunk/latest/Admin/Defaultmetaconf>

App context - Demonstration



- See a field description in global vs. app context



Name	Field name	Eval expression	Owner	App	Sharing	Status	Actions
splunkd_ui_access : EVAL-method	method	root.*.*.status	admin	001_field_exploration	Global Permissions	Enabled	Clone Move Delete

Calculated fields

Fields > Calculated fields

Showing 1-1 of 1 item

App: 001_field_exploration ... Configuration Source: Visible in the App Owner: Any filter 100 per page

Name	Field name	Eval expression	Owner	App	Sharing	Status	Actions
splunkd_ui_access : EVAL-method	method	root.*.*.status	admin	001_field_exploration	App Permissions	Enabled	Clone Move Delete

Permissions

Fields > Calculated fields > splunkd_ui_access : EVAL-method > Permissions

Object should appear in

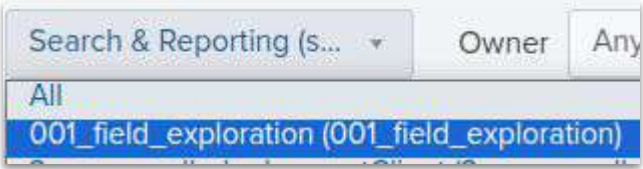
☐ Keep private

☒ This app only (001_field_exploration)

☐ All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>



Manage knowledge object permissions	https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/Manageknowledgeobjectpermissions
Manage app permissions in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/9.2.2403/Config/ManageAppPermissions
default.meta.conf	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Defaultmetaconf

App context - btool



- Btool is your friend ... but only for Enterprise OnPremise

*nix example

```
./splunk btool inputs list --debug | grep splunktcp
```

Windows example

```
splunk btool inputs list --debug | findstr splunktcp
```

```
splunk@3spruces-mc-01:~$ splunk cmd btool props list -app=001_field_exploration --debug
/opt/splunk/etc/apps/001_field_exploration/default/props.conf [splunkd_ui_access]
/opt/splunk/etc/apps/001_field_exploration/default/props.conf EVAL-method = root."+".status
splunk@3spruces-mc-01:~$ splunk cmd btool props list --debug |grep -E method
/opt/splunk/etc/apps/001_field_exploration/default/props.conf EVAL-method = root."+".status
```

Use btool to troubleshoot configurations	https://docs.splunk.com/Documentation/Splunk/9.3.0/Troubleshooting/Usebtooltotroubleshootconfigurations
Configuration file precedence	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles
Administrative CLI commands	Link
Admins Little Helper for Splunk	https://splunkbase.splunk.com/app/6368

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - **Methods and Locations**
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunk Cloud
 - Upload to Cloud via GUI
 - AppInspect vetting - Lab 4
- Summary

Create an App

Methods and Locations...

- GUI create (Enterprise & Splunk Cloud)
- Add on Builder (Enterprise & Splunk Cloud)
- GUI upload (Enterprise & Splunk Cloud)
- CLI / REST upload (Enterprise only)
- Copy into location and restart (Enterprise only)
- ACS install - API install via upload and for Splunkbase (Splunk Cloud only)

Locations

- Stand-alone search head or indexer, Monitoring Console or Cluster Manager -
`$SPLUNK_HOME/etc/apps`
- Cluster Manager (for apps to be pushed to indexers) - `$SPLUNK_HOME/etc/manager-apps`
- Deployment Server (for apps to be pushed to forwarders) -
`$SPLUNK_HOME/etc/deployment-apps`
- Search head Deployer (for apps to be pushed to the search head cluster members) -
`$SPLUNK_HOME/etc/shcluster/apps`

Naming conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Configuration file directories	https://docs.splunk.com/Documentation/Splunk/Admin/Configurationfiledirectories

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunk Cloud
 - Upload to Cloud via GUI - Lab 4
 - AppInspect vetting
- Summary

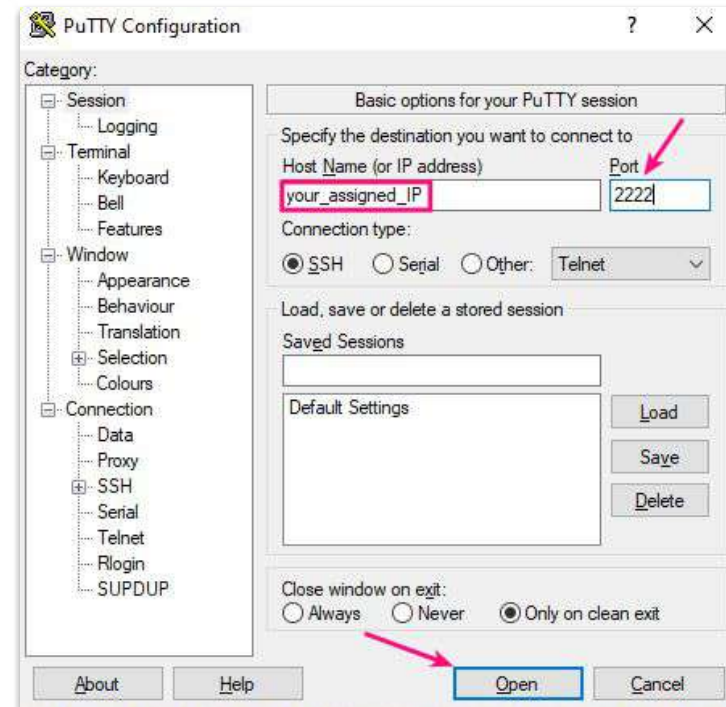
Create an App



Access the node assigned via ssh

- Linux and macOS - note the lowercase “p”
 - `ssh -p 2222 splunk@<your_assigned_IP|hostname>`
- Remember - change the `<your_assigned_IP>` to the IP you were assigned from Splunk Show...

- Windows - you don't have to care about CLI parameters ...



What is SSH (Secure Shell)?

<https://www.ssh.com/academy/ssh>

Download PuTTY: latest release

<https://putty.org/>

Create an App



Upload via CLI ... sequence and review what happened

```
splunk@s4a-a-aio01:/opt$ /opt/showlab/s4a-a-aio01/splunk/bin/splunk install app /tmp/fin_user_viz.tgz -auth admin:5p1unk.conf
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
App '/tmp/fin_user_viz.tgz' installed
```

```
default metadata README static
splunk@s4a-a-aio01:/opt/showlab/s4a-a-aio01/splunk/etc/apps/fin_user_viz$ find -ls
1581890      4 drwxr-xr-x   5 splunk  splunk      4096 Aug 13 20:03 .
1581892      4 drwxr-xr-x   2 splunk  splunk      4096 Aug 13 20:03 ./metadata
1581275      4 -rw-----   1 splunk  splunk        85 Aug 13 20:03 ./metadata/local.meta
1581897      4 -rw-r--r--   1 splunk  splunk       101 Aug 13 20:03 ./metadata/default.meta
1581898      4 drwxr-xr-x   3 splunk  splunk      4096 Aug 13 20:03 ./default
1581900      4 drwxr-xr-x   3 splunk  splunk      4096 Aug 13 20:03 ./default/data
1581902      4 drwxr-xr-x   4 splunk  splunk      4096 Aug 13 20:03 ./default/data/ui
1581903      4 drwxr-xr-x   2 splunk  splunk      4096 Aug 13 20:03 ./default/data/ui/views
1581904      4 -rw-r--r--   1 splunk  splunk     1361 Aug 13 20:03 ./default/data/ui/views/splunk_ps__users_and_roles.xml
1581905      4 drwxr-xr-x   2 splunk  splunk      4096 Aug 13 20:03 ./default/data/ui/nav
1581906      4 -rw-r--r--   1 splunk  splunk       233 Aug 13 20:03 ./default/data/ui/nav/default.xml
1581265      4 -rw-----   1 splunk  splunk       382 Aug 13 20:03 ./default/app.conf
1581912      4 -rw-r--r--   1 splunk  splunk       139 Aug 13 20:03 ./README
1581913      4 drwxr-xr-x   2 splunk  splunk      4096 Aug 13 20:03 ./static
1581914      4 -rw-----   1 splunk  splunk     1902 Aug 13 20:03 ./static/appIcon_2x.png
1581915      4 -rw-----   1 splunk  splunk       639 Aug 13 20:03 ./static/appIcon.png
splunk@s4a-a-aio01:/opt/showlab/s4a-a-aio01/splunk/etc/apps/fin_user_viz$
```

Create an App



Upload via CLI ... review file contents

```
splunk@show-no-config-1-01e760ef443ed0e19:/opt/splunk/etc/apps$ more /opt/splunk/etc/apps/fin_user_viz/metadata/default.meta
# Application-level permissions

[]
access = read : [ fin_monitoring_admin admin ], write : [ fin_monitoring_admin admin, sc_admin ]
owner = fin_monitoring_admin
```

```
splunk@show-no-config-1-0f8fa34e686e76c6d:/opt/splunk/etc/apps/fin_user_viz$ more /opt/splunk/etc/apps/fin_user_viz/default/app.conf
[package]
id = fin_user_viz
check_for_updates = false

[install]
state = enabled
build = 1
install_source_checksum = 97fea7989bcd5cd5e7384ba0

[launcher]
author = splunkadmin@buttercup.com
description = dashboards for finance user setup visualizations
version = 1.0.0

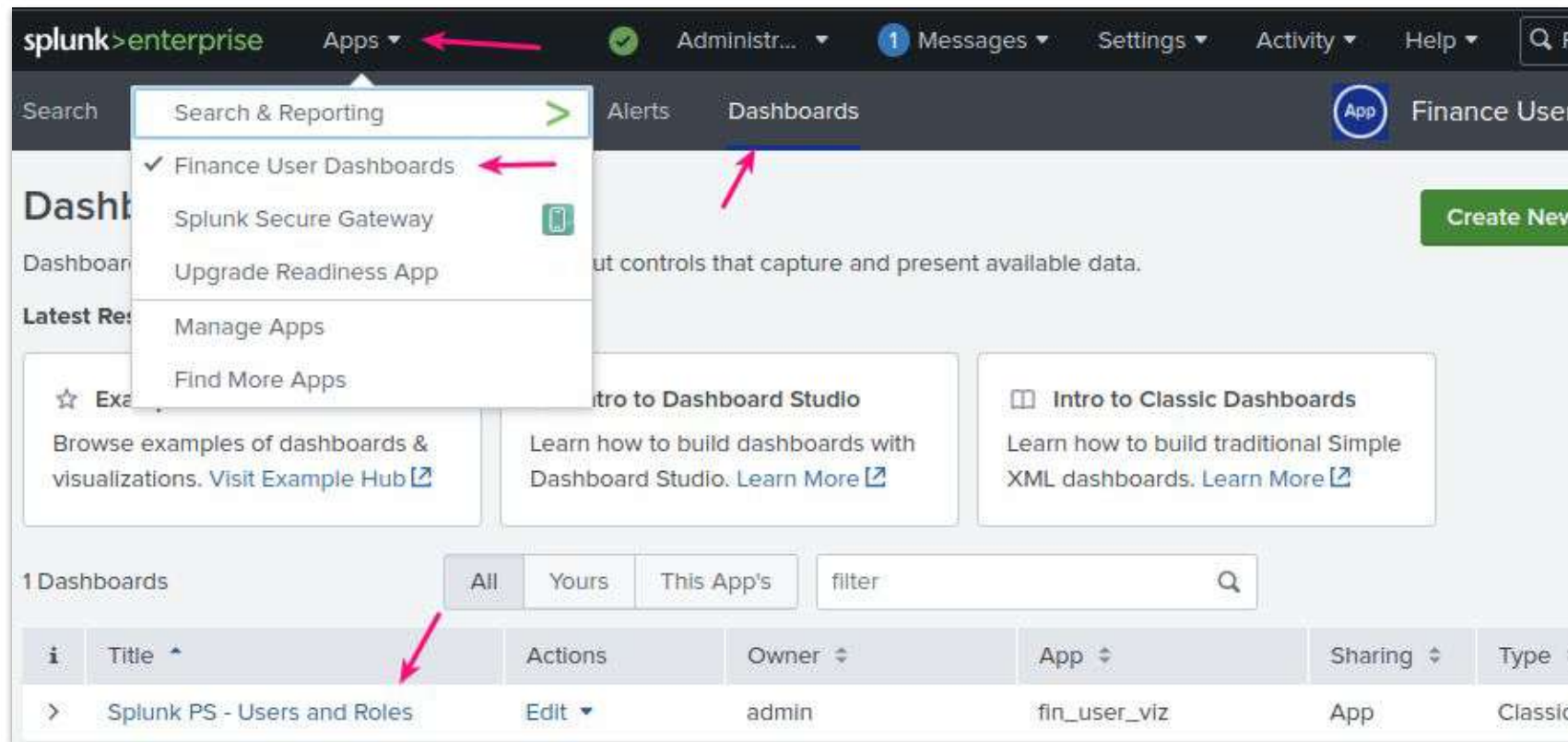
[ui]
is_visible = true
label = Finance User Dashboards

[id]
version = 1.0.0
name = fin_user_viz
```

Create an App



Upload via CLI ... validate the new app and dashboard



Administer Splunk Enterprise with the command line interface (CLI)

<https://docs.splunk.com/Documentation/Splunk/latest/Admin/AbouttheCLI>

Create an App



Copy into location ... sequence of events

1. `splunk@s4a-a-aio01:/opt/showlab$ cp -rp /opt/showlab/APPS-s4a-apps/fin_weblogs_indexes/ /opt/showlab/s4a-a-aio01/splunk/etc/apps/`

2. `splunk@s4a-a-aio01:/opt/showlab$ more /opt/showlab/s4a-a-aio01/splunk/etc/apps/fin_weblogs_indexes/default/app.conf`

```
[package]
id = fin_weblog_indexes
check_for_updates = false

[install]
state = enabled
build = 1

[launcher]
author = splunkadmin@buttercup.com
description = index for weblogs
version = 1.0.0

[ui]
is_visible = false
label = Finance Index Definitions

[id]
version = 1.0.0
name = fin_weblog_indexes
```

3. `splunk@s4a-a-aio01:/opt/showlab$ more /opt/showlab/s4a-a-aio01/splunk/etc/apps/fin_weblogs_indexes/default/indexes.conf`

```
[volume:hot-warm]
path = /opt/splunk/var/lib/splunk
maxVolumeDataSizeMB = 80000

[volume:cold-thawed]
path = /opt/splunk/var/lib/cold_thawed
maxVolumeDataSizeMB = 1000
```

```
[weblogs]
homePath = volume:hot-warm/$_index_name/db
coldPath = volume:hot-warm/$_index_name/coldddb
thawedPath = $SPLUNK_DB/$_index_name/thaweddb
summaryHomePath = volume:hot-warm/$_index_name/summary
tstatsHomePath = volume:hot-warm/$_index_name/datamodel_summary
maxDataSize = auto
maxTotalDataSizeMB = 5000
frozenTimePeriodInSecs = 43200
```

4. `splunk@s4a-a-aio01:/opt/showlab$ more /opt/showlab/s4a-a-aio01/splunk/etc/apps/fin_weblogs_indexes/metadata/local.meta`

```
[ ]
access = read : [ * ], write : [ admin ]
export = system
```

5. `splunk@s4a-a-aio01:/opt$ /opt/showlab/s4a-a-aio01/splunk/bin/splunk restart`

```
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
...
Stopping splunk helpers...
```

Configuration file directories

<https://docs.splunk.com/Documentation/Splunk/Admin/Configurationfiledirectories>

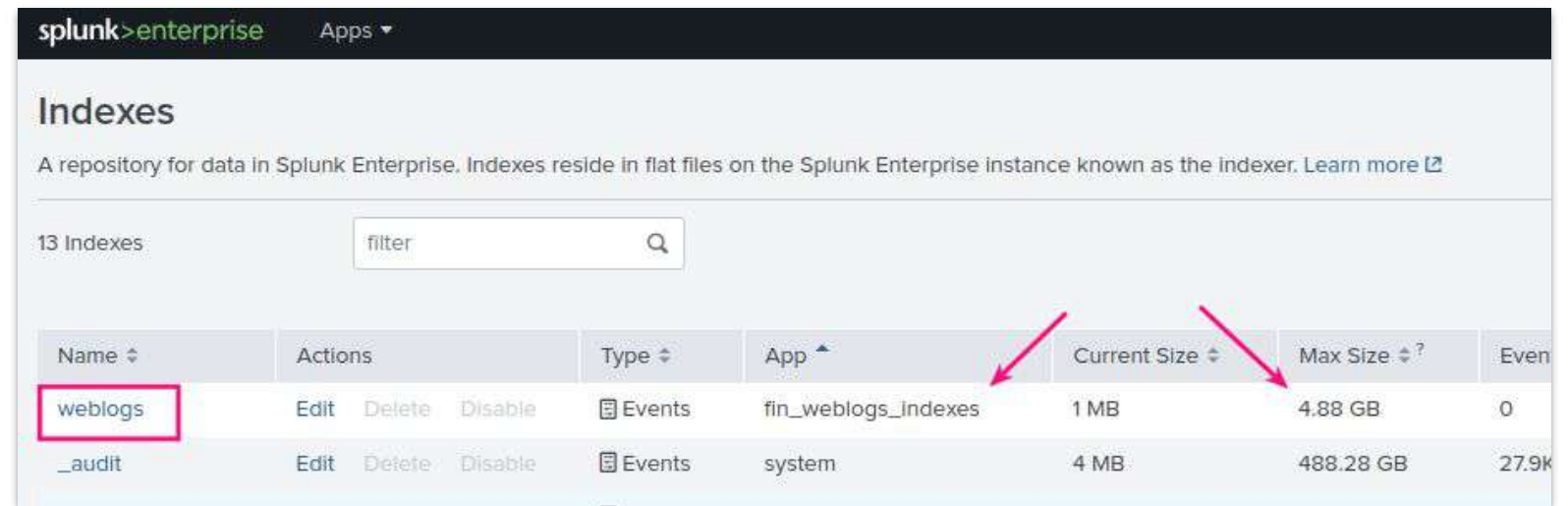
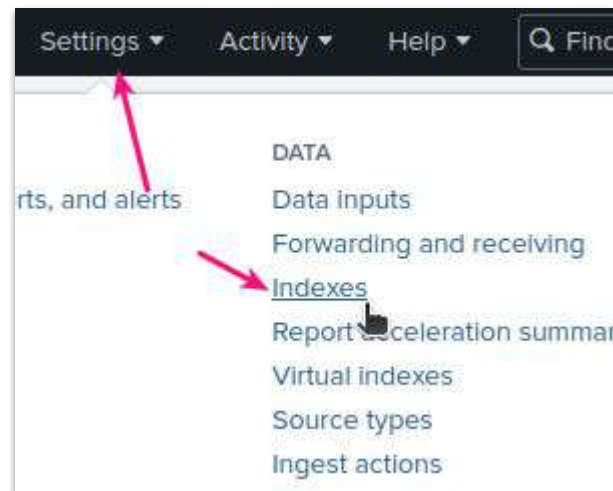
Edit the configuration file settings directly

[Link](#)

Create an App



Copy into location ... validate



Configuration file directories	https://docs.splunk.com/Documentation/Splunk/Admin/Configurationfiledirectories
Edit the configuration file settings directly	Link

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - **Splunk Cloud**
 - Upload to Cloud via GUI - Lab 4
 - AppInspect vetting
- Summary

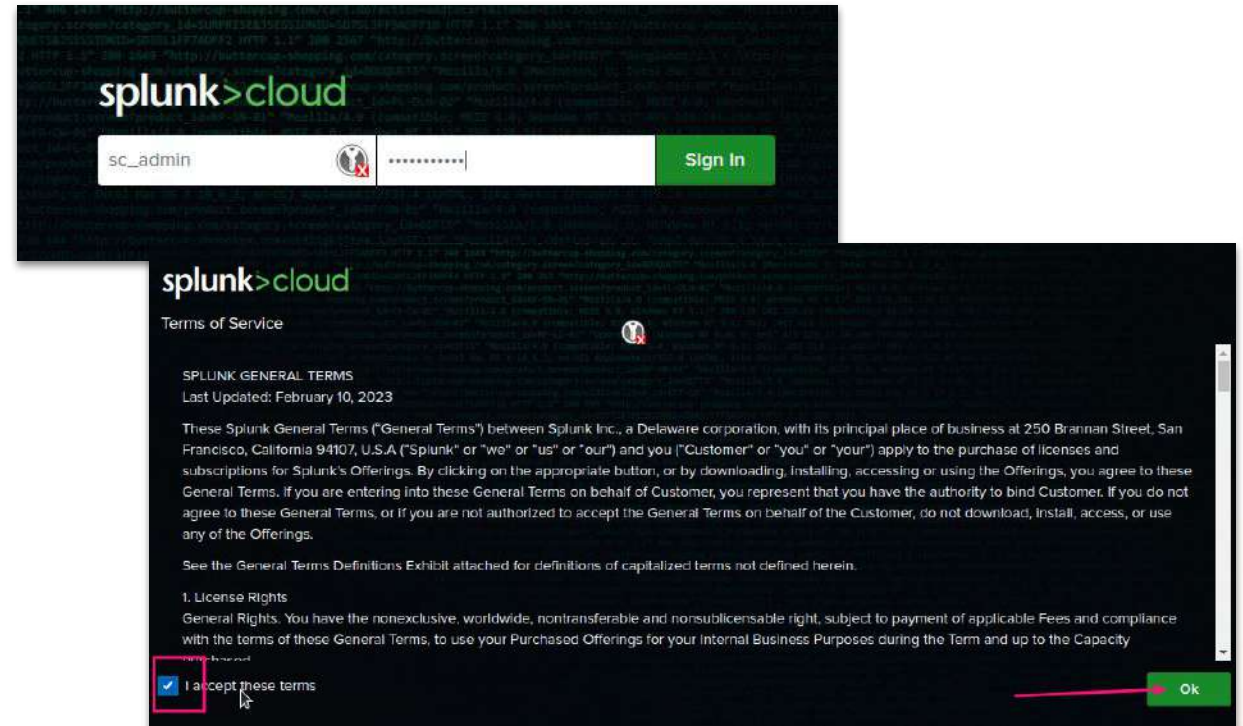
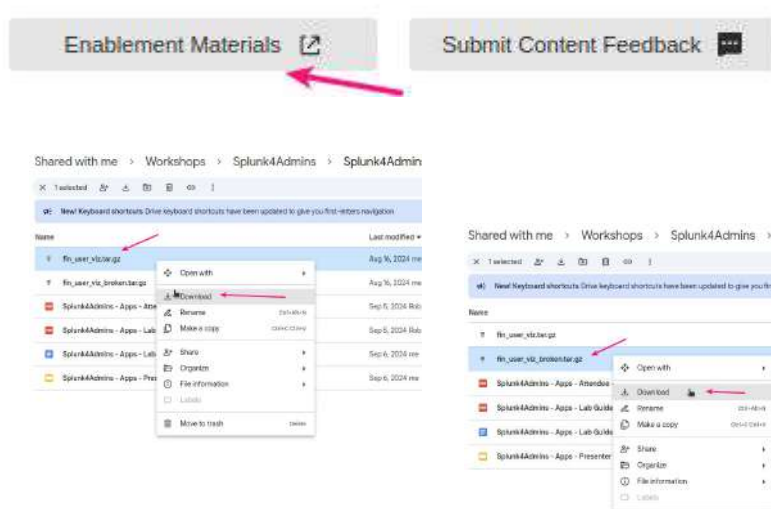
Create an App



Upload to cloud

Login ...

Download ...



Overview of developing a private Splunk Cloud Platform app	https://docs.splunk.com/Documentation/SplunkCloud/latest/DevApp/Overview
Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Install a private app on Victoria Experience	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps#:~:text=Platform%20Experience.-,Install%20a%20private%20app%20on%20Victoria%20Experience.-,If%20your%20Splunk

Create an App



Upload to cloud

-
-
-
-
-
-

Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	Link

Create an App



Upload to cloud

6. Upload App

Supported app package file formats are .spl, .tar, .tar.gz or .tgz file.

Drop your file here or browse...

fin_user_viz_broken.tar.gz

Close

Upload

App Validation in Progress

fin_user_viz.tar.gz uploaded successfully! Automated private app validation is now checking for issues, which can take a few minutes.

App Vetting Complete

2 Issues found.

You must fix these issues before you can install your app. for details, see the [report](#). For help, see the [Splunk Developer Docs](#).

Close

View Report

Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	Link

Create an App



AppInspect

splunk>

[MISSING 'default/app.conf']

[MISSING 'default/app.conf']

Author

[MISSING 'default/app.conf']

Tags

advanced_xml_alert_actions_conf, appapproval, cloud, custom_search_commands, custom_search_commands_v2, custom_visualizations, custom_workflow_actions, deprecated_features, developer_guidance, dingo_bindings, future, health_conf, jquery_manual, kubernetes, multi_tenancy, observability_packaging_standards, phish_app, removed_features, restapi_conf, savedsearches, security, self-service, splunk_appinspect

Version

[MISSING 'default/app.conf']

Hash

15064634a3086f220e00030d05d

Appinspect Request ID

8ab01ae-0894-48c1-902a-12c890a38

Run Time

2024-08-10T12:40:04.001Z

Execution Time

0

Run parameters:

Field	Value
Appinspect Version	3.7.0

Analizers:

Name	Version	In Latest
static-checks	3.7.0	True
dynamic-checks	1.34.0	True
refine-js	1.0.2	True

Compatibility totals:

Status	Count
Successes	0
Failures	2
Errors	0
Warnings	0
Manual Checks	0
Not Applicable	2
Skipped	335

Compatibility totals:

Status	Count
Successes	0
Failures	2
Errors	0
Warnings	0
Manual Checks	0
Not Applicable	2
Skipped	335

[Failure Summary]

Failures will block the Cloud Vetting. They must be fixed.

❶ check_that_extracted_splunk_app_contains_default_app_conf_file

Splunk App packages should contain a default/app.conf file. No default/app.conf was found in 'appinspect'.

❷ check_that_splunk_app_package_does_not_contain_files_outside_of_app

A file or folder was found outside of the app within the overall package. Or the file or folder does not have expected permission. Please remove this file or folder or modify the permission: 'fin_user_viz_broken'

```
r91395fg 08/21/24 > find fin_user_viz_broken -ls
14983184 4 drwxr-xr-x 5 splunk splunk 4096 Aug 16 12:41 fin_user_viz_broken
14983185 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/static
14983149 4 -rw-r--r-- 1 splunk splunk 1902 Aug 13 13:01 fin_user_viz_broken/static/appIcon_2x.png
14981357 4 -rw-r--r-- 1 splunk splunk 639 Aug 13 13:01 fin_user_viz_broken/static/appIcon.png
14983186 4 drwxr-xr-x 3 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/local
14983187 4 drwxr-xr-x 3 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/local/data
14983188 4 drwxr-xr-x 4 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/local/data/ui
14983189 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/local/data/ui/nav
14981358 4 -rw-r--r-- 1 splunk splunk 233 Aug 13 13:01 fin_user_viz_broken/local/data/ui/nav/default.xml
14983190 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:04 fin_user_viz_broken/local/data/ui/views
14981359 4 -rw-r--r-- 1 splunk splunk 1361 Aug 13 13:01 fin_user_viz_broken/local/data/ui/views/splunk_ps_users_and_roles.xml
14981360 4 -rw-r--r-- 1 splunk splunk 315 Aug 13 13:06 fin_user_viz_broken/local/app.conf
14983191 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz_broken/metadata
14981361 4 -rw-r--r-- 1 splunk splunk 101 Aug 13 13:01 fin_user_viz_broken/metadata/default.meta
14981362 4 -rw-r--r-- 1 splunk splunk 139 Aug 13 13:03 fin_user_viz_broken/README
```

Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	Link

Create an App



Upload to cloud... a correctly built app

6.

Upload App

Supported app package file formats are .spl, .tar, .tar.gz or .tgz file.

Drop your file here or browse...

fin_user_viz.tar.gz

Close

Upload

```
91395fg 08/21/24 > find fin_user_viz -ls
14983170 4 drwxr-xr-x 5 splunk splunk 4096 Aug 13 13:03 fin_user_viz
14983177 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz/static
14981394 4 -rw-r--r-- 1 splunk splunk 1982 Aug 13 13:01 fin_user_viz/static/appIcon_2x.png
14981393 4 -rw-r--r-- 1 splunk splunk 639 Aug 13 13:01 fin_user_viz/static/appIcon.png
14983171 4 drwxr-xr-x 3 splunk splunk 4096 Aug 13 13:01 fin_user_viz/default
14983172 4 drwxr-xr-x 3 splunk splunk 4096 Aug 13 13:01 fin_user_viz/default/csta
14983173 4 drwxr-xr-x 4 splunk splunk 4096 Aug 13 13:01 fin_user_viz/default/csta/ui
14983174 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz/default/csta/ui/nav
14981348 4 -rw-r--r-- 1 splunk splunk 233 Aug 13 13:01 fin_user_viz/default/csta/ui/nav/default.xml
14983175 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:04 fin_user_viz/default/csta/ui/views
14981384 4 -rw-r--r-- 1 splunk splunk 1361 Aug 13 13:01 fin_user_viz/default/csta/ui/views/splunk_ps_users_and_roles.xml
14981347 4 -rw-r--r-- 1 splunk splunk 315 Aug 13 13:06 fin_user_viz/default/app.conf
14983176 4 drwxr-xr-x 2 splunk splunk 4096 Aug 13 13:01 fin_user_viz/metadata
14981392 4 -rw-r--r-- 1 splunk splunk 101 Aug 13 13:01 fin_user_viz/metadata/default.meta
14948065 4 -rw-r--r-- 1 splunk splunk 139 Aug 13 13:03 fin_user_viz/README
```

App Validation in Progress

fin_user_viz.tar.gz uploaded successfully! Automated private app validation is now checking for issues, which can take a few minutes.

7.

Acknowledge and Install

I acknowledge that Splunk is not responsible for the installation or use of any application that is not a supported Splunk application and Splunk specifically disclaims the accuracy, integrity, quality, legality, usefulness or security of such application or its use. Installation and use of an application that is not a supported Splunk application can introduce risks, including security risks, and is at your own risk. Please note that if data leaves Splunk Cloud as a result of installing or using such application, Splunk's security attestations do not apply to data outside Splunk Cloud. Learn more about installing private apps.

Cancel

Acknowledge and Install

Install - In Progress

Splunk cloud is installing **Finance User Dashboards**. App installation can take several minutes and might cause Splunk Cloud to restart. Do not navigate away from this page until app installation is complete.

Install - Success

Finance User Dashboards has been successfully installed.

Manage private apps on your Splunk Cloud Platform deployment

<https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps>

Deploy and manage private apps in Splunk Cloud Platform

<https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/>

Install a private app on Victoria Experience

[Link](#)

Create an App



AppInspect Vetting - Common issues

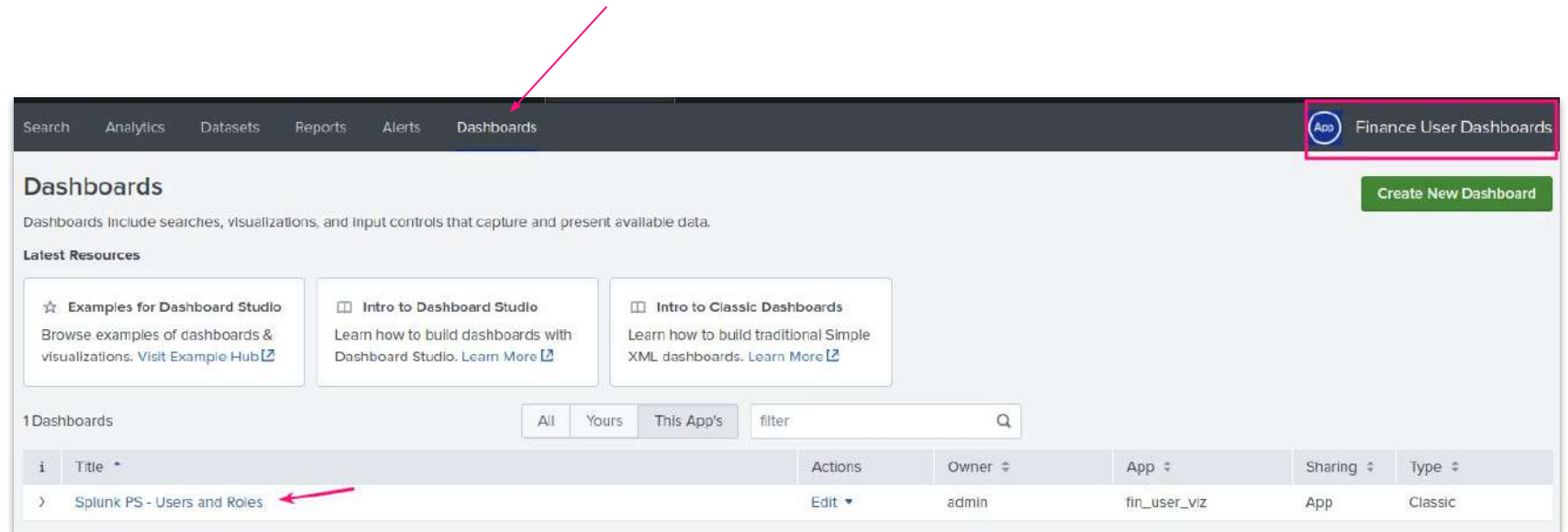
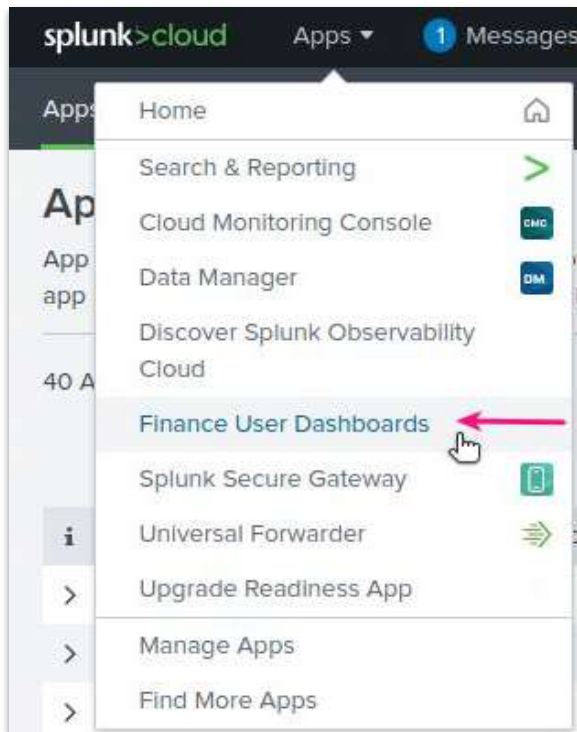
- 'local' vs. 'default'
 - Files in a 'local' directory, should be only in 'default'
- default/app.local
 - Required file, name must match and unique version
- metadata/default.meta
 - Permissions file - write for specific teams only, reasonable no-write in Splunk Cloud Production
- Modular inputs/scripts detected
 - Automated acceptance of scripts not permitted, manual process
- Files in non-standard locations
 - default, appserver, bin, lookups, metadata, static permitted - as well as README

Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	Link
Validate Splunk Apps in Enterprise and Spunk Cloud	https://dev.splunk.com/enterprise/docs/developapps/testvalidate/appinspect/

Create an App



Upload to cloud... a correctly build app



Validate the quality of Splunk apps and add-ons for Splunk Cloud Platform or Splunk Enterprise using Splunk AppInspect

<https://dev.splunk.com/enterprise/docs/developapps/testvalidate/appinspect/>

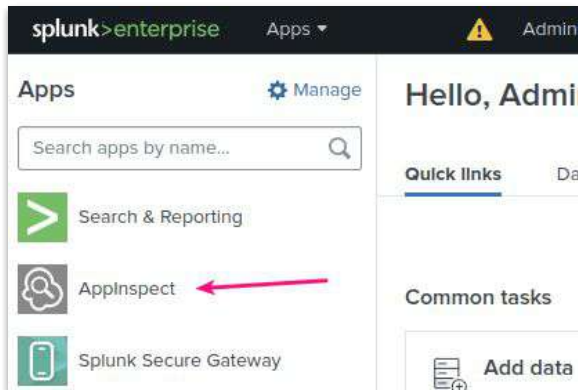
Manage private apps on your Splunk Cloud Platform deployment

<https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps>

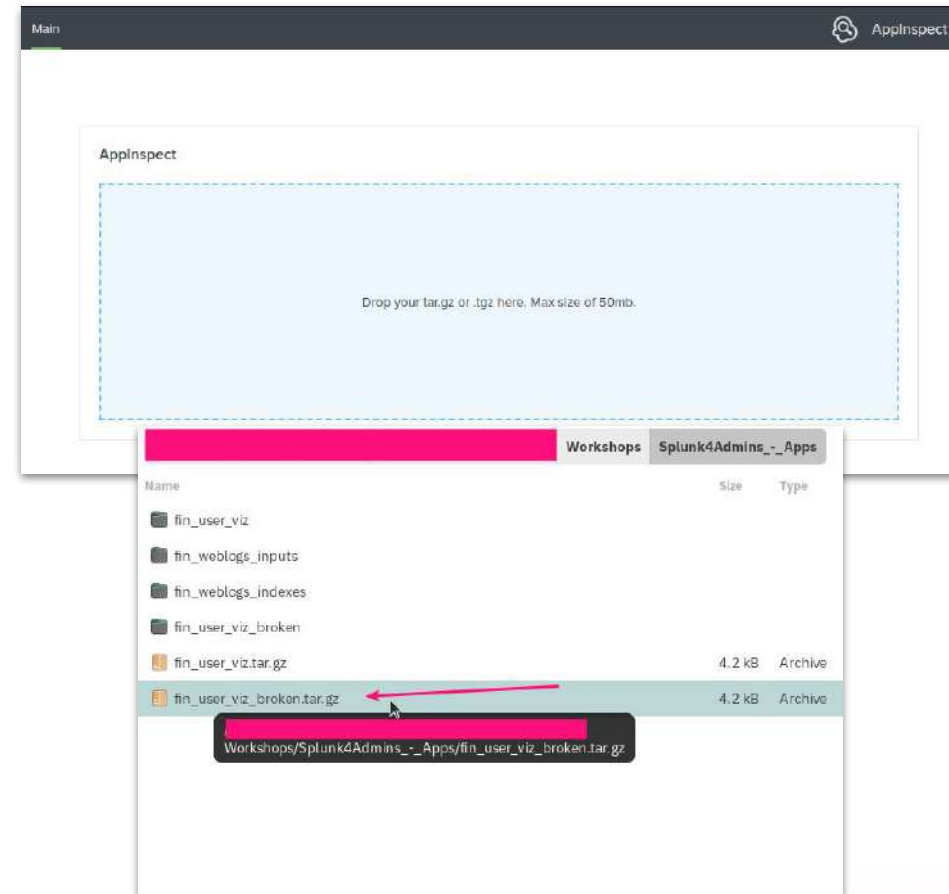
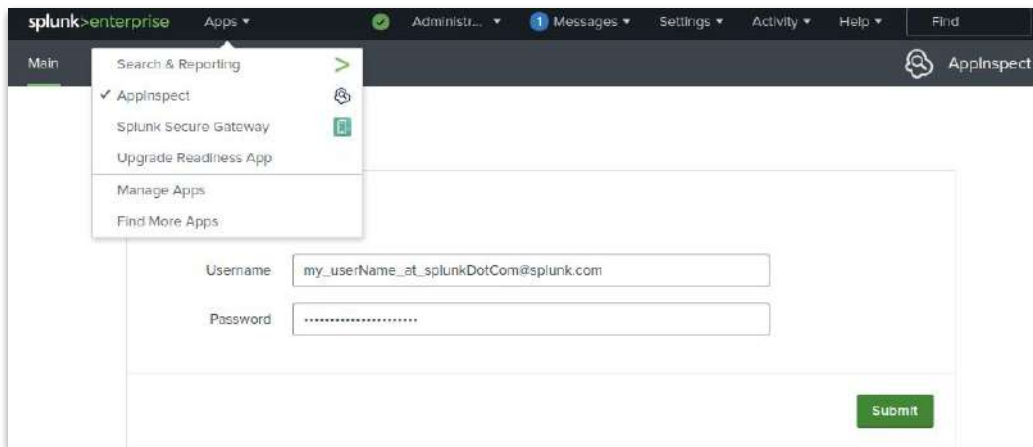
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunkbase
 - Splunk Cloud
 - Upload to Cloud via GUI - Lab 4
 - AppInspect vetting
- Summary

Create an App



The on-premise app
AppInspect is NOT
Splunk supported,
and not available in
Splunk Cloud



AppInspect App for Splunk

<https://splunkbase.splunk.com/app/3956>

Create an App

AppInspect - Enterprise

- Ensure consistency
- Ensure function
- Provide off-Cloud development (if needed)
- Ensure that apps developed can be migrated with ease

Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	Link
Validate Splunk Apps in Enterprise and Spunk Cloud	https://dev.splunk.com/enterprise/docs/developapps/testvalidate/appinspect/

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an app, TA, or SA?
- What makes an app?
- App contents and precedence - Lab 1
- Create apps
 - Methods and Locations
 - Enterprise
 - Upload an app via CLI - Lab 2
 - Copy to directory - Lab 3
 - Splunkbase
 - Splunk Cloud
 - Upload to Cloud - Lab 4
 - AppInspect vetting
- Summary

Summary

Splunk Apps

- What makes an app?
- App precedence
- How to create an app
 - Locations
 - In Enterprise
 - In Splunk Cloud
- AppInspect

Links

What are Splunk Apps and Add-Ons ?	https://www.splunk.com/en_us/blog/tips-and-tricks/what-are-splunk-apps-and-add-ons.html
What is a Splunk app?	https://dev.splunk.com/enterprise/docs/welcome/#What-is-a-Splunk-app
Developing Views and Apps for Splunk Web	https://docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/Whatsinthismanual
Apps and add-ons	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp
Getting Data In	https://docs.splunk.com/Documentation/Splunk/latest/Data/Usingapps
Manage knowledge object permissions	https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/Manageknowledgeobjectpermissions
Manage app permissions in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/9.2.2403/Config/ManageAppPermissions
Developing a Private App for Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/DevApp/Overview
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Splunk Add-on Builder	https://splunkbase.splunk.com/app/2962
Splunk Cloud Platform Admin Manual	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/SelfServiceAppInstall
Splunkbase Home	https://splunkbase.splunk.com/
Understand file precedence in apps for Splunk Cloud Platform or Splunk Enterprise	https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/fileprecedence/
Configuration file precedence	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles
Use btool to troubleshoot configurations	https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations
Admins Little Helper for Splunk	https://splunkbase.splunk.com/app/6368
Administrative CLI commands	https://docs.splunk.com/Documentation/Splunk/latest/Admin/CLladmincommands#:~:text=poll%20bologna%3A1234-.show.-config%2C%20cluster%2Dbundle

Naming conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Install App via Command Line	https://docs.splunk.com/Documentation/Splunk/latest/Admin/CLladmincommands#:~:text=tmp/export.dat-.install.-app
Admin Config Service Manual	https://docs.splunk.com/Documentation/SplunkCloud//Config/ACSIntro
default.meta.conf	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Defaultmetaconf
app.conf	https://docs.splunk.com/Documentation/Splunk/latest/Admin/appconf
App deployment overview	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Deployappsandadd-ons
Administer Splunk Enterprise with the command line interface (CLI)	https://docs.splunk.com/Documentation/Splunk/latest/Admin/AbouttheCLI
Configuration file directories	https://docs.splunk.com/Documentation/Splunk//Admin/Configurationfiledirectories
Edit the configuration file settings directly	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles#:~:text=system/default-.Edit%20the%20configuration%20file%20settings%20directly.-While%20you%20can
Use the deployer to distribute apps and configuration updates	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/PropagateSHCconfigurationchanges
Update common peer configurations and app	https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Updatepeerconfigurations
Administer Splunk Enterprise with configuration files	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
Overview of developing a private Splunk Cloud Platform app	https://docs.splunk.com/Documentation/SplunkCloud/latest/DevApp/Overview
Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps
Deploy and manage private apps in Splunk Cloud Platform	https://dev.splunk.com/enterprise/docs/releaseapps/manageprivatecloud/
Install a private app on Victoria Experience	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps#:~:text=Platform%20Experience-.Install%20a%20private%20app%20on%20Victoria%20Experience.-If%20your%20Splunk
Validate the quality of Splunk apps and add-ons for Splunk Cloud Platform or Splunk Enterprise using Splunk AppInspect	https://dev.splunk.com/enterprise/docs/developapps/testvalidate/appinspect/
AppInspect App for Splunk	https://splunkbase.splunk.com/app/3956
What is SSH (Secure Shell)?	https://www.ssh.com/academy/ssh
Download PuTTY: latest release	https://putty.org/

Thank you