



splunk®

App Sorcery

Building Splunk Apps With Best Practice

Matt Egin – megin@splunk.com

October 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2018 Splunk Inc. All rights reserved.

MATT EGLIN

Senior PS Consultant, EMEA  



A bit about me...

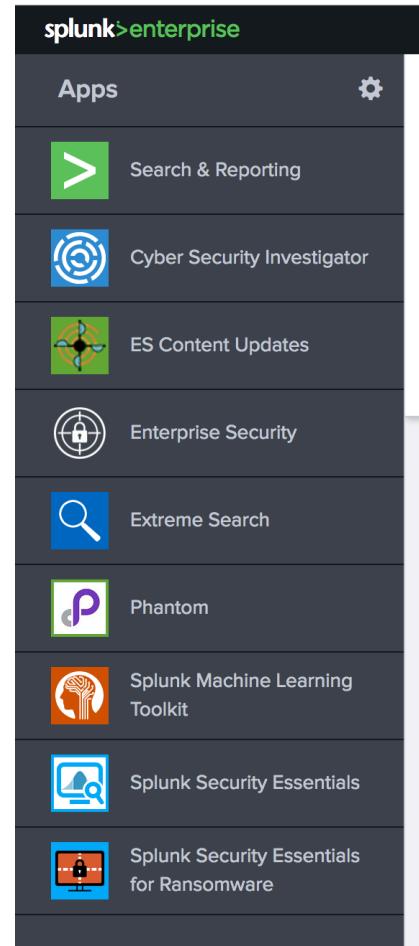
- ▶ Splunk Professional Services
 - ▶ Based out of the Splunk London Office
 - ▶ Using and working with Splunk for the past 2.5 years
 - ▶ Specialize in High Volume Splunk Enterprise and Enterprise Security
 - ▶ Enjoyer of craft beers –
 - untappd.com/user/matteglin

What the App?

Where to begin



What do we mean by “App”



- ▶ Pre-packaged Content
 - Dashboards & Searches
 - Inputs
 - Knowledge Objects
- ▶ Bundles of Associated Configuration
 - Think Configuration Management
- ▶ Integrations with third party, and associated Products
- ▶ Transformative Experiences
 - Splunk Premium Application
- ▶ Extensions of Splunk Enterprise Functionality

What do we mean by “App”

Some choice examples



Splunk Enterprise Security



Dashboard Examples



Splunk Add-on for Cisco ASA

What do we mean by “App”

So, what's the point?

- ▶ Simplify Splunk Configuration Management and Deployment
 - ▶ Package up complex content for easy deployment
 - ▶ Leverage Splunk deployment methods like Deployment Server, Cluster Master and Deployer
 - ▶ Easily reuse custom created configuration elsewhere
 - ▶ One-Click Implementation of Data Use Cases
 - ▶ Distributing your cool content to other Splunk Users ;)

Deploying Apps

You have options!



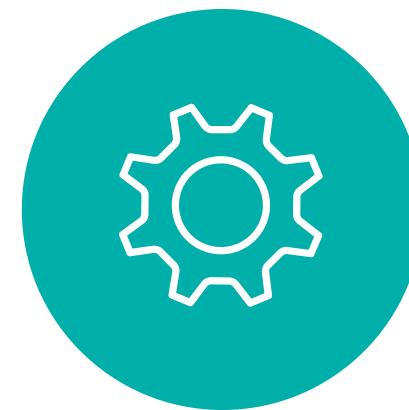
Deployment Server



Cluster Master



Deployer

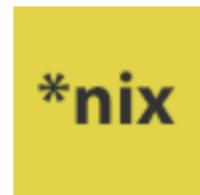


Puppet / Chef / SCCM



Manually...

Apps and TA's



Splunk Add-on for Unix and Linux

54474 Installs



Splunk App for Unix and Linux

3725 Installs



Aren't these the same thing?

Apps and TA's

Ok, but what's this “TA” thing I keep hearing about?

App

- ▶ Visible in Web UI
- ▶ Contains Dashboards and Visual Content
- ▶ Contains Search Time Knowledge Objects
- ▶ Designed for End User interaction
- ▶ Search Head Deployment

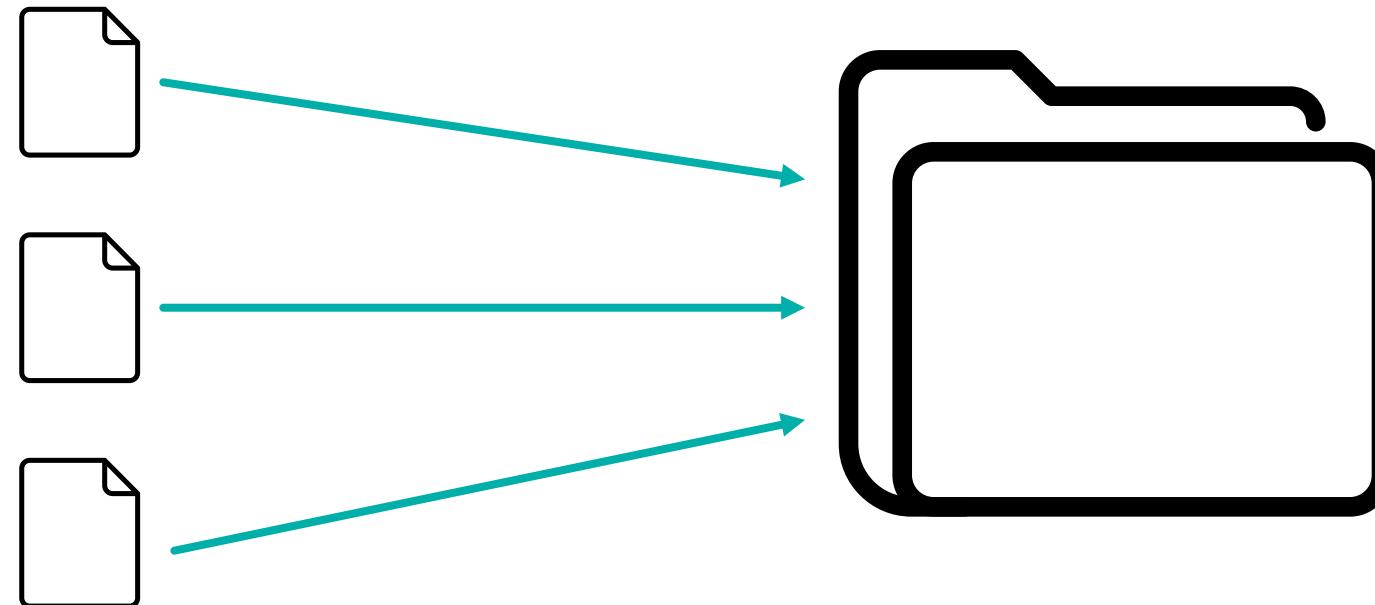
Technical Addon

- ▶ Not visible in Web UI
- ▶ Contains Search Time Knowledge objects
- ▶ Contains Index Time Knowledge Objects
- ▶ Indexer / Search Head & Forwarder Deployment

Building an App

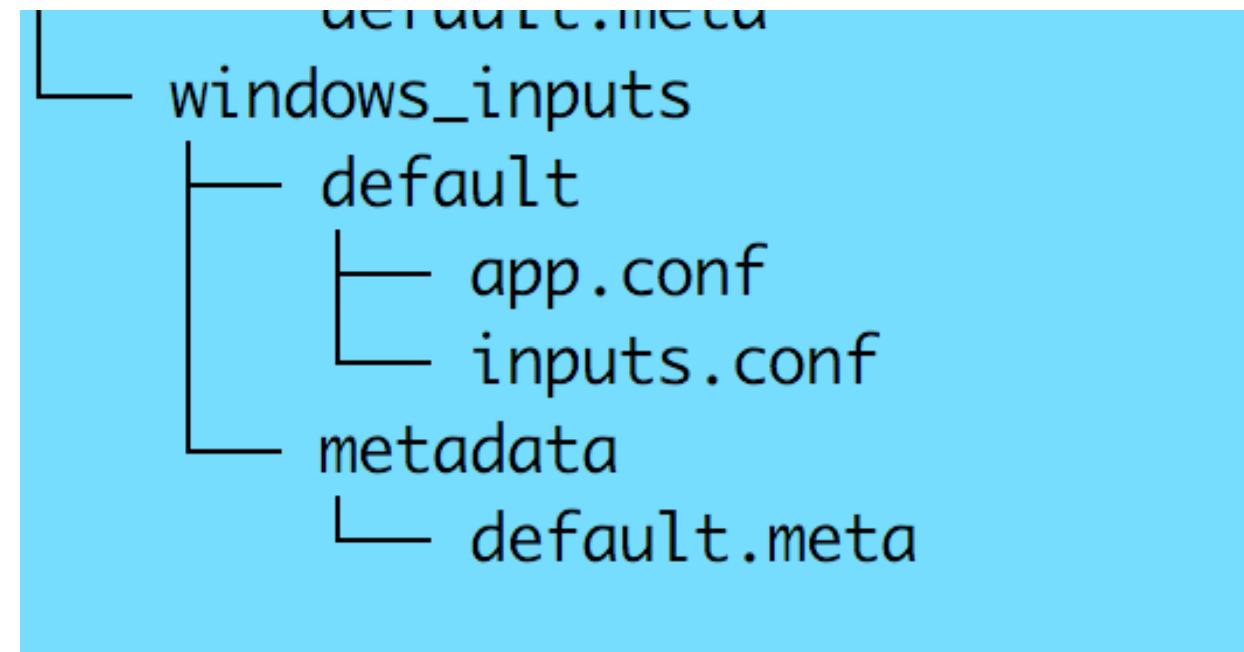
Putting it all together

The very very basics



A structured directory of related files

The very very basics



A structured directory of related files

More complex

```
  └── README.txt
  └── default
    ├── app.conf
    └── data
      └── ui
        └── panels
          ├── mcafee_graph__count_by_ids_alert_type.xml
          ├── mcafee_graph__count_by_ids_severity.xml
          ├── mcafee_graph__count_by_update_statuses.xml
          ├── mcafee_line_chart__host_severity_count.xml
          ├── mcafee_pie_chart__dat_file_versions.xml
          ├── mcafee_pie_chart__product_versions.xml
          ├── mcafee_pie_chart__top_signatures_by_severity.xml
          └── mcafee_table__top_signatures_by_severity.xml
    ├── database.conf.template
    ├── eventgen.conf
    ├── eventtypes.conf
    ├── inputs.conf.template
    ├── props.conf
    ├── tags.conf
    ├── transforms.conf
    └── web.conf
  └── license-eula.rtf
  └── license-eula.txt
  └── local
    └── app.conf
  └── lookups
    ├── epo_actions.csv
    ├── epo_severities.csv
    ├── intrushield_severities.csv
    └── mcafee_vendor_info.csv
  └── metadata
    ├── default.meta
    └── local.meta
  └── samples
    ├── hostname.sample
    ├── malicious_domains.sample
    ├── sample.mcafee_ids
    ├── sample.v4.mcafee_epo
    ├── sample.v5.mcafee_epo
    ├── sensorName.sample
    ├── username.sample
    └── windows_file_name.sample
```

- ## ► What you normally find :

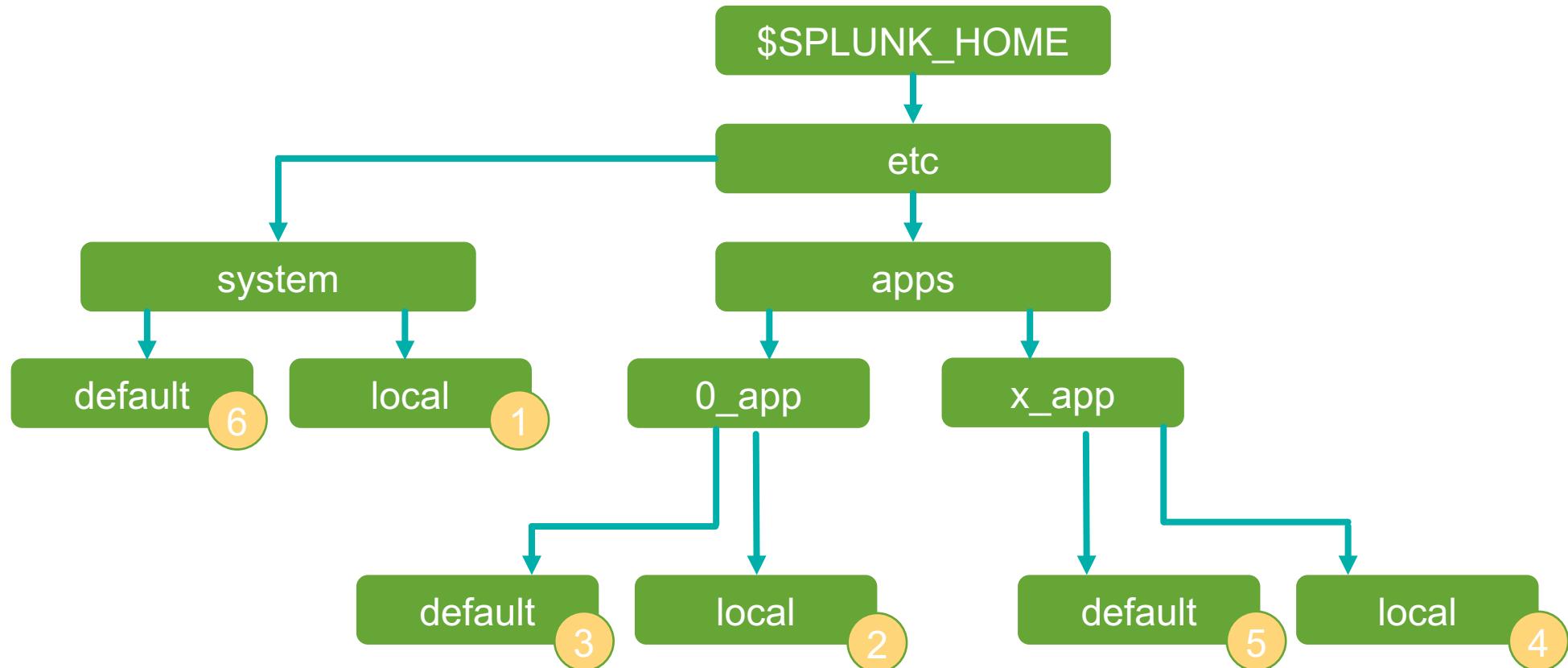
- Default Directory
 - Local Directory
 - Lookups
 - Metadata
 - Samples

- #### ► What you might also find :

- Bin directory with scripts
 - Web Static content (js / images etc.)
 - template .conf files
 - License Agreements

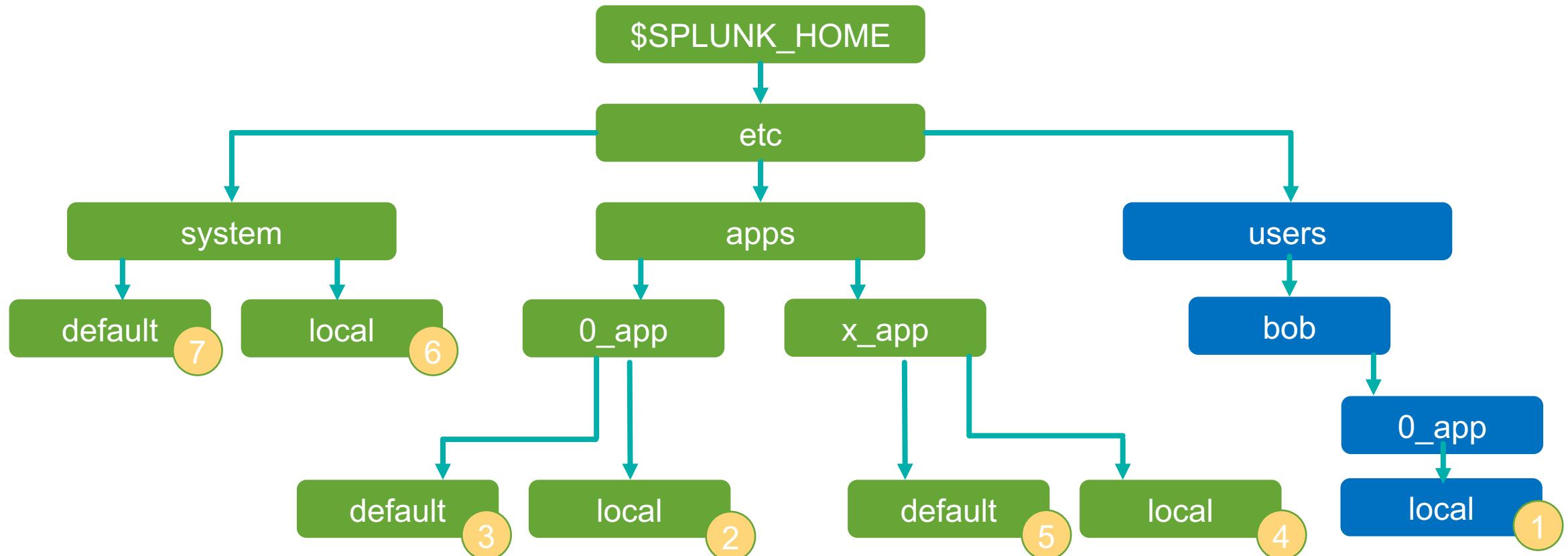
A Note on Configuration Precedence

► Index time and System level precedence



A Note on Configuration Precedence

► At Search Time



A Note on Configuration Precedence

Key Points

- ▶ local configuration will always override default
- ▶ Apps with a "higher" ASCII order name will take precedence over "lower" ASCII order named Apps
- ▶ Config in system local can override any app setting that tries to be global
- ▶ Search time configuration precedence is user centric
- ▶ When in doubt – use splunk btool to debug active config

Metadata and why it matters

- ▶ Metadata controls access and visibility to App contents
- ▶ default.meta / local.meta files
- ▶ Role based access
- ▶ Can be global or granular

```
# Application-level permissions
```



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

```
### TAGS
```

```
[tags]
export = system
```

```
### SAVED SEARCHES
```

```
[savedsearches/Errors%20in%20the%20last%204%20hours]
access = read : [ * ], write : [ admin ]
```

```
[savedsearches/Errors%20in%20the%20last%20hour]
access = read : [ * ], write : [ admin ]
```

```
[savedsearches/Messages%20by%20minute%20last%203%20hours]
access = read : [ admin ], write : [ admin ]
```

```
[savedsearches/Splunk%20errors%20last%204%20hours]
access = read : [ admin ], write : [ admin ]
```

```
### Alert Actions
```

Watch out for Configuration Spread

- ▶ Be very aware of the export level of your configuration
- ▶ Configuration can spread to, and impact other Apps
- ▶ Can be especially problematic with Splunk Enterprise Security
- ▶ If you don't need to export to 'system', then export to 'app' instead



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



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

Golden Rules

DO

- ▶ Include app.conf
- ▶ Include default.meta
- ▶ Include Documentation
- ▶ Include Example Data
- ▶ Utilise a setup.xml screen
- ▶ Test your work

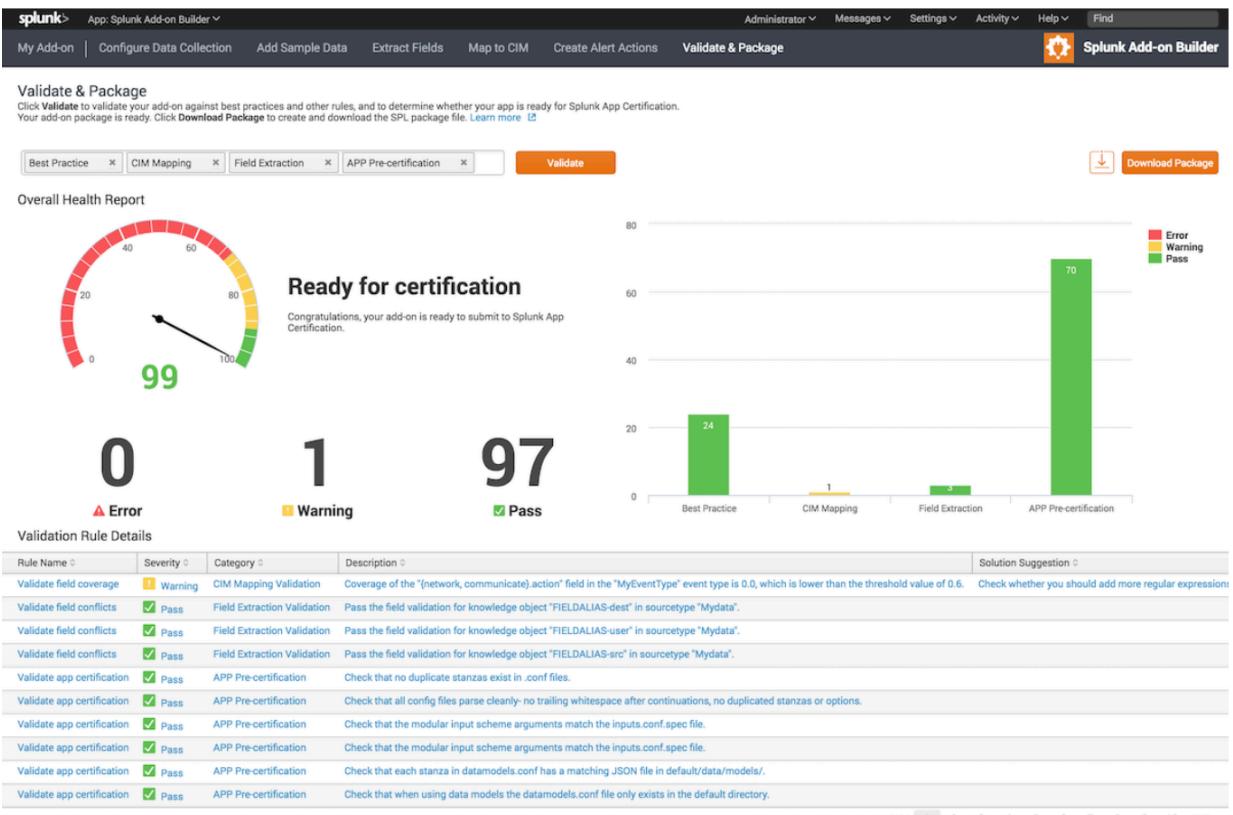
DO NOT DO

- ▶ Data Model Accelerations enabled by default
- ▶ Configuration in a /local/ directory
 - Supply a baseline of configuration in /default/
- ▶ Add excessive configuration
 - eventtypes / props / transforms etc.
- ▶ Assume index names in Searches and Dashboards
 - Consider using a macro instead

Splunk Add-on Builder

Add-ons Made Easy!

- ▶ Step by Step Process
- ▶ Save time and effort
- ▶ Easily package up Content
- ▶ Designed for making TA's
- ▶ Easy data source mapping to Splunk Common Information Model
- ▶ Prepare for Splunk Certification



Demo / Walkthrough

Let's (quickly) take a look

Something Cool

We built it!

The Report Creator App

Fix Splunk PDF Generation

- ▶ Out of the Box PDF Generation is not great
 - ▶ Aim to re-work PDF generation within Splunk
 - ▶ Integrate within existing Splunk UI
 - ▶ Completely server side solution
 - ▶ Integration with custom Python script and JavaScript Libraries (PhantomJS, CasperJS)

splunk>enterprise App: Report Capture ▾

H Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Capture Help Report Capture

Capture

Capture User: admin

Delivery Method: Download Email

Output Format: PDF PNG

Page Size: A4

Page Orientation: Landscape Portrait

Page Wait: 10 Seconds 30 Seconds 60 Seconds

[Hide Filters](#)

Available Dashboards/Reports (Click on a row to capture)

Report Type	Dashboard Author	Dashboard App	Name (Wildcard Search)	Description (Wildcard Search)
<input checked="" type="radio"/> Dashboard	All	All		
<input type="radio"/> Report				

App	Author	Name	Description
repcap	nobody	Capture	
splunk_monitoring_console	nobody	Data Quality	This dashboard helps you assess the quality of your incoming data by revealing issues that occur when the data is being indexed. These issues appear as warnings and errors in your splunkd.log.
splunk_monitoring_console	nobody	Distributed Search: Deployment	
splunk_monitoring_console	nobody	Distributed Search: Instance	
splunk_monitoring_console	nobody	Forwarders: Deployment	
splunk_monitoring_console	nobody	Forwarders: Instance	

The Report Creator App

Extending Splunk Functionality

- ▶ Custom REST API endpoint – `web.conf`
- ▶ Custom config file – `recap.conf`
- ▶ Python controller script – `repcapsvc.py`
- ▶ UI Elements
- ▶ Setup Screen – `setup.xml`

```
/Users/meglin/dev/repcap
├── README
├── repcap.conf.spec
└── web.conf.spec
├── appserver
│   └── controllers
│       └── repcapsvc.py
├── bin
├── default
│   ├── app.conf
│   ├── data
│   │   └── ui
│   │       ├── nav
│   │       │   └── default.xml
│   │       └── views
│   │           ├── capture.xml
│   │           └── help.xml
│   └── repcap.conf
├── examples
│   └── repcap_scripted.py
├── metadata
│   └── default.meta
└── static
    ├── appIcon.png
    ├── appIconAlt.png
    ├── appIconAlt_2x.png
    ├── appIcon_2x.png
    ├── html_error.htm
    ├── html_info.htm
    ├── html_test.htm
    └── screenshot.js
```

The Report Creator App

Available on Splunkbase!!

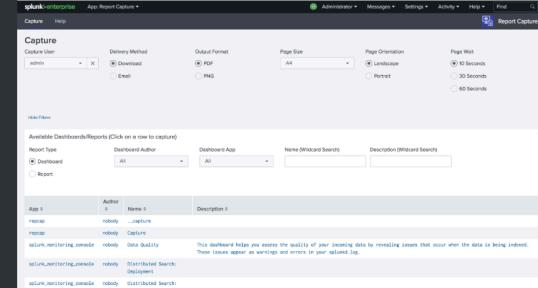
splunkbase™

Search App by keyword, technology...

My Account ▾ > My Splunk ▾ ? Support & Services ▾



Report Capture

★★★★★ 0 rating


This app is pending approval and is not yet publicly visible.

ADMINISTRATOR TOOLS: Manage App | View App | View Analytics

Overview

The Report Capture application for Splunk provides a means of screen-capturing an existing Dashboard or Report to produce a visually-accurate PDF or PNG, where the standard PDF reporting does not provide the required output. This capture can be triggered either via the application dashboard or via the REST API.

By using a combination of CasperJS/PhantomJS/ImageMagick a virtual browser is simulated which will connect to your Splunk environment and view the specified Dashboard/Report. After a defined period, a screen-capture will be taken and either returned for download or sent via email.

0
Installs
0
Downloads

[Download](#)

[Rate this App](#)

VERSION

0.8.4

splunk> .conf18

Apps On Splunkbase

Getting it out there!

splunkbase™

Search App by keyword, technology...

My Account ▾

Support & Services ▾

Platform > Splunk Built

Metrics Enhancements
Performance improvements and new SPL commands.

Updated UI Look and Feel
Modern look and feel to the Splunk Enterprise user interface.

Machine Learning Toolkit 3.1 and 3.2
Introducing new pre-processing options FieldSelector, new clustering algorithm X-Means, revamped Model and Experiment Management Framework and few other configuration options.

Splunk 7.1 Overview

Release 7.1 is the latest version of Splunk Enterprise and Splunk Cloud. We have developed an app to guide you through the powerful new features. This is not an in-depth tutorial, rather a guide to help you understand the new

< >

> Splunk 7.1 Overview

Palo Alto Networks App

Splunk ES Content Update

Splunk App for AWS

Splunk Machine Learning Toolkit

Extend the Power of Splunk with Apps and Add-ons

Splunkbase has 1000+ apps and add-ons from Splunk, our partners and our community. Find an app or add-on for most any data source and user need.

Learn More

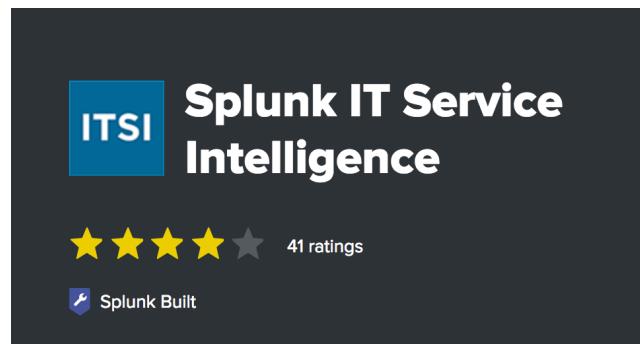
See All Apps

Browse by Category

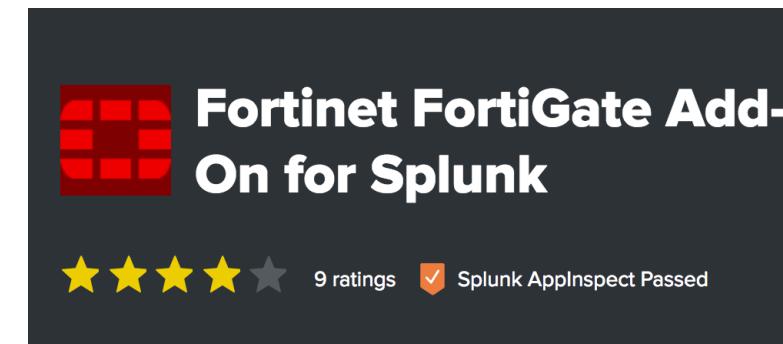
Apps on Splunkbase

Splunkbase?

- ▶ Splunk Managed repository of Apps and TA's
- ▶ One stop shop for all your Splunk needs



Splunk Built



AppInspect Passed

Apps on Splunkbase

Splunk & Third Party



Splunk Built



Splunk AppInspect Passed

- ▶ Splunk Built First Party App
 - ▶ Supported and Validated by Splunk
 - ▶ Splunk Certified Third Party Apps
 - ▶ Mark of Validation and Quality
 - ▶ Supported by the Creator

**** Not always available for Splunk Cloud ****

Validating for Splunkbase

AppInspect

- ▶ Download and install tool from Splunk Dev
 - <http://dev.splunk.com/view/appinspect/SP-CAAAE9U>
- ▶ Install pre-requisites
- ▶ Run your App through AppInspect *before* submitting to Splunkbase
 - `splunk-appinspect inspect app_path/app_filename.tgz --mode precert --included-tags splunk_appinspect`
 - Review the output and correct any Failures



```
2. bash
Check iframe elements for compliance with Splunk Cloud security policy.
SKIPPED: Skipping due to package validation issues.
Check that all XML files are well-formed.
SKIPPED: Skipping due to package validation issues.
Check any XML files that embed JavaScript via CDATA for compliance with
Splunk Cloud security policy.
SKIPPED: Skipping due to package validation issues.
Ensure that global event handlers are not used within XML files.
SKIPPED: Skipping due to package validation issues.

repcap Report Summary:
skipped: 240
success: 7
manual_check: 0
failure: 3
warning: 0
error: 0
not_applicable: 3
-----
Total: 253

(venv) meglin-mbp:~ meglins|
```

Validating for Splunkbase

- ▶ Apps will be reviewed

The screenshot shows the Report Capture app page on Splunkbase. The top header is dark with a blue icon and the text "Report Capture". To the right is a large green "DOWNLOAD" button. Below the header, a red bar contains the message "This app is pending approval and is not yet publicly visible." Underneath is a blue bar with "ADMINISTRATOR TOOLS" and links to "Manage App", "View App", and "View Analytics".

STATUS: PENDING

- Hosting
- Description
- Media
- Details
- Settings
- Leads
- Editors

VERSIONS

VERSION	DEFAULT	VISIBILITY	COMPATIBILITY	UPLOAD DATE
0.8.4	○	○	7.1, 7.0, 6.6	Aug 21, 2018

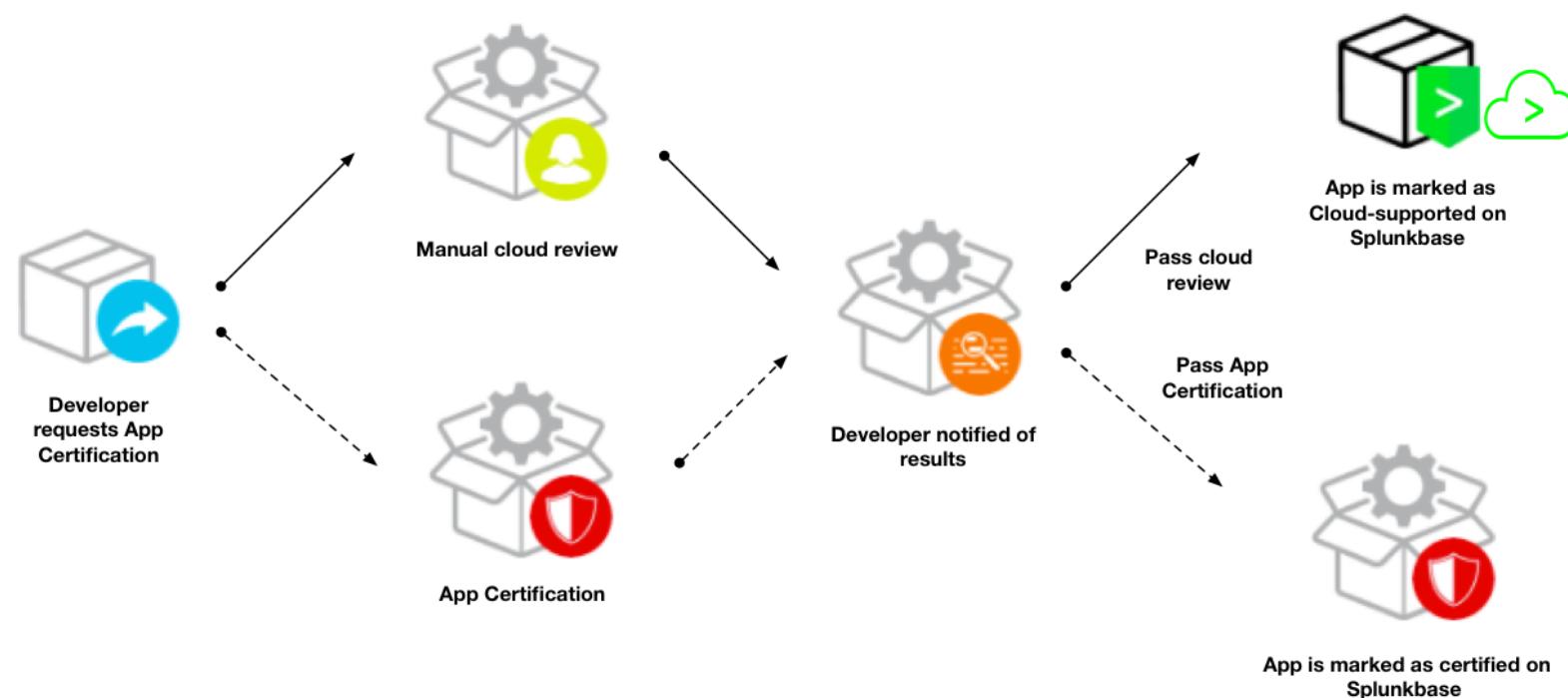
To schedule a Release Date, click [here](#).

REQUEST APP DELETION

Want to host externally or transfer ownership? [Contact Us](#)

Validating for Splunk Cloud

- ▶ Strict set of criteria required for an App to be “Cloud Certified”
- ▶ Certification Process once Submitted to Splunkbase



Validating for Splunk Cloud

AppInspect

- ▶ Download and install tool from Splunk Dev
 - <http://dev.splunk.com/view/appinspect/SP-CAAAE9U>
- ▶ Install pre-requisites
- ▶ Run your App through AppInspect *before* submitting to Splunkbase
 - `splunk-appinspect inspect app_path/app_filename.tgz --mode precert --included-tags cloud`
 - Review the output and correct any Failures



```
2.bash
Check iframe elements for compliance with Splunk Cloud security policy.
SKIPPED: Skipping due to package validation issues.
Check that all XML files are well-formed.
SKIPPED: Skipping due to package validation issues.
Check any XML files that embed JavaScript via CDATA for compliance with
Splunk Cloud security policy.
SKIPPED: Skipping due to package validation issues.
Ensure that global event handlers are not used within XML files.
SKIPPED: Skipping due to package validation issues.

repcap Report Summary:
skipped: 240
success: 7
manual_check: 0
failure: 3
warning: 0
error: 0
not_applicable: 3
-----
Total: 253

(venv) meglin-mbp:~ meglin$
```

Validating for Splunk Cloud

A quick how to

1. Register for a Splunk Developer Account
2. Run your App through Splunk AppInspect
 - Exhaustive Criteria List - <http://dev.splunk.com/view/app-cert/SP-CAAAE3H>
3. Make some Documentation!
 - Release Notes
 - Description
 - Splunk Enterprise Version Compatibility
 - CIM Compatibility
4. Decide to host on Splunkbase or Externally
5. Submit @ <https://splunkbase.splunk.com/new/>

Key Takeaways

1. Don't overload Apps / TA's with config.
Smaller, more atomic is best
2. Don't assume how Splunk has been configured
3. Always test your creations
4. Remember configuration precedence rules

Further Reading & Links

1. Releasing Apps on Splunkbase / into Splunk Cloud -
<http://dev.splunk.com/view/SP-CAAAFD8>
2. Developing Apps & Add-ons - <http://dev.splunk.com/view/SP-CAAAFD7>
3. Vetting Apps & Add-ons for Splunk Cloud - <http://dev.splunk.com/view/app-cert/SP-CAAAE85>
4. Report Creator App -
<https://splunk.box.com/s/eio1gby3hzjta5mr3rs8t0z5p5z5s9wz> **<UPDATE TO
SB LINK>**

Learn More

1. DEV1545 - Go From Dashboards to Applications With Ease: SplunkJS for Non-Developers
2. DEV1293 - Worst practices for building Splunk Apps and Add-ons and how to avoid them
3. FN1329 - I've Got Over 70,000 Servers and Two Months to Get the Universal Forwarder Installed.

Thank You

Don't forget to rate this session
in the .conf18 mobile app

