Faster Splunk App Certification with Splunk AppInspect

Andy Nortrup

Product Manager, Splunk

Grigori Melnik

Director, Product Management, Splunk

Disclaimer

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 the 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.

Agenda

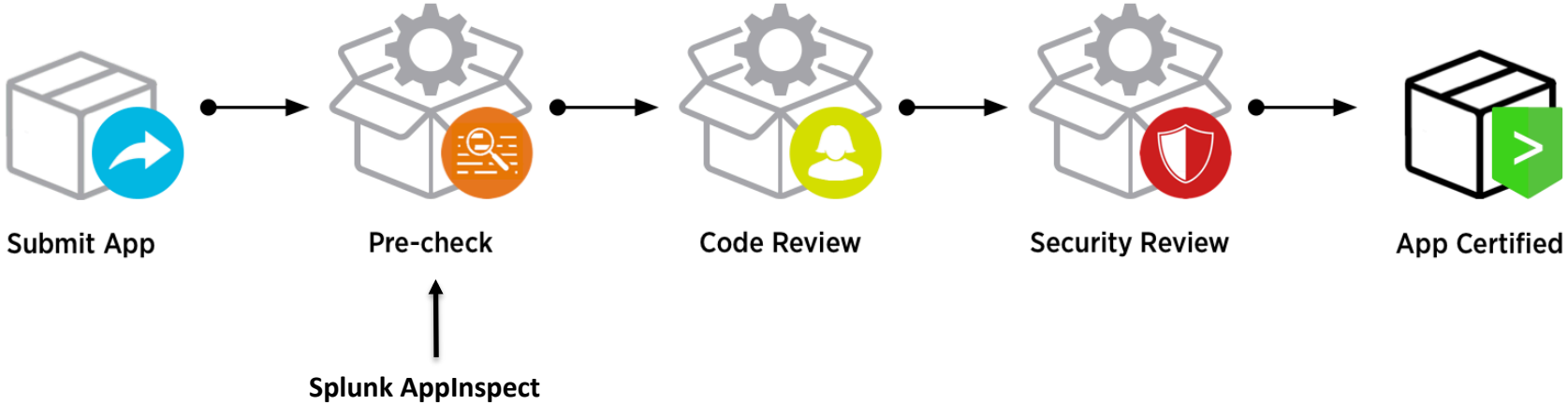
- What is Splunk AppInspect
  - Standalone package
  - Web Service
- Demos
  - Custom REST endpoint
  - Modular Input
  - Add-on building
- Questions

Splunk App Certification Program – Benefits

- For app **devs**
  - Obtain sales leads
  - Earn premium listing on Splunkbase
  - Find bugs in your code
  - Get additional insights into your code & your technical debt.
  - Ensure conformance to coding guidelines, proven, and recommended practices.
  - Check for cloud readiness

- For app **users**
  - Gain confidence in app quality
  - Better level of app support

Splunk App Certification – Process



What is Splunk AppInspect

- Standalone tool
  - `pip install splunk_appinspect`
  - Static analysis checks
- Web service
  - REST endpoints
  - Static and dynamic analysis

- Full Documentation: <Documentation Reference Addr / Link>

Well-formedness Checks

- Similar to *Lint*, *FindBugs*, *PMD*, *FxCop*

- 141 checks covering:
  - Modular Inputs
  - Custom Alert Actions
  - Custom Search Commands
  - Custom Workflow Actions
  - Custom REST Endpoints
  - Custom Visualizations
  - btool (web service only)

Sample checks:

Mod inputs:

Check that a valid `inputs.conf.spec` file exists at `README/inputs.conf.spec` .
Check that at least one stanza/mod input exists when using a modular input.
Check the scheme arguments match the `inputs.conf.spec` file when using a modular input.
Check a valid scheme is returned via the scripts via the scheme command when using a modular input.
Check that a script exists for each stanza when using a modular input.
Check that arguments are specified when using a modular input.
Check that arguments are not duplicated within a stanza when using a modular input.
Check that stanzas are not duplicated when using a modular input.
Check lines breaks are included in configuration when using a modular input.

Custom alert actions:

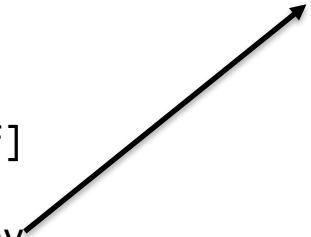
Check that a valid `alert_actions.conf` file exists at default/alert_actions.conf.
Check that a valid executable exists when using a custom alert action.
Check that a valid alert icon exists at `appserver/static/{alert name}.png` when using a custom alert action.
Check that a valid app icon exists at `appserver/static/appIcon.png` when using a custom alert action.
Check that when any executable args are specified when using a custom alert action.
Check that the payload format is set to a valid value of `xml` or `json` when using a custom alert action.
Check that a setup.xml file exists when using a custom alert action.
Check that a html file exists for use when creating a custom alert action.

Splunk AppInspect – Standalone Demo

Well-formedness Checks – Custom REST endpoint

default/restmap.conf

```
[admin_external:do_stuff]
handlertype = python
handlerfile = do_stuff.py
handlerpersistentmode=false
handleractions=create
```



bin/do_stuff.py

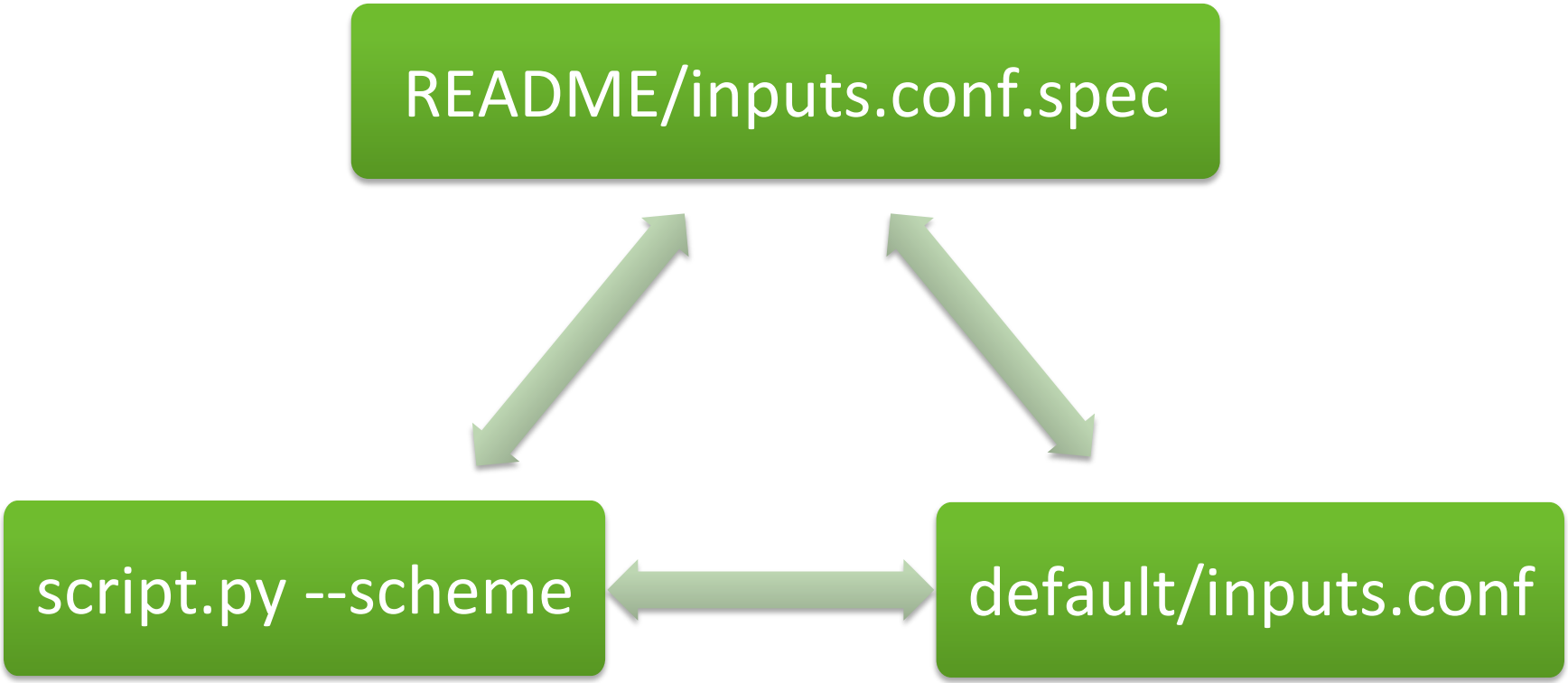
```
import splunk.admin as admin import
splunk.entity as en

class ConfigApp(admin.MConfigHandler):
      ...
```

Splunk AppInspect – Web Service Demo

REST Endpoints

- Validate – Submit and app for validation
  - http -f POST appinsepct.splunk.com/v1/app/validate app.tgz
- Status – Get the status of the validation
  - http GET appinsepct.splunk.com/v1/app/status/{report-id}
- Report – Get the results of the validation
  - http GET appinsepct.splunk.com/v1/app/report/{report-id}
- Groups – Get a list of check groups
  - http GET appinsepct.splunk.com/v1/group
- Checks – Get a list of checks
  - http GET appinsepct.splunk.com/v1/check

Well-formedness Checks Example – Modular Input



Integration with Add-on Builder

- <placeholder> if this is done in time for .conf
- Also, refer attendees to a related talk on Add-on Builder

Accelerate Your App Certification

- Follow proven and recommended practices.
  - **splk.it/appcert**
  - **splk.it/cloud-apps**
- Pre-certify your apps with AppInspect
- Make sure your Splunkbase listing has a valid email
- Provide release notes and installation instructions. Test them!
- Provide test data / eventgen
- Provide testing API keys
- Provide functional test suite or test cases
- Respond to code and security review feedback promptly
- Perform regression testing

Call to Action!

- Download AppInspect (<link placeholder>)
- Pre-certify your app be for publishing
- Apply for certification
  - Lead generation
  - Better visibility on Splunkbase
  - Approved for Splunk Cloud installation
- Provide feedback to us (AppCertAdmin@splunk.com)
  - Success stories
  - Pain points
  - Bugs
  - Suggestions for additional checks
  - Suggestions for fine tuning of pattern analysis to reduce false positives
- Spread the word #AppInspect

Questions?

THANK YOU

splunk>