Working With Splunk Cloud – Best Practices

Dennis Bourg

Customer Success, Splunk

Eric Six

Customer Success, Splunk

.conf2016

splunk>


splunk>cloud™
.conf2016
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.

Who We Are…

Eric Six

Splunk-ing over 5 years, 3+ years as a Splunker. Before that.. A very happy customer.

Home in Tokyo, Japan, but frequently with Customers in Europe, America, China, Australia, and Singapore…

Architecting and Deploying simple to very complex deployments…

All about Splunk Cloud!

Favorite Command : **| *tstats***

Favorite App : **Enterprise Security**

Hobbies : **Trad Climbing, Back Country Snowboarding, Bourbon…**

Love 80s movies..

No relation!

Who We Are…

Dennis Bourg

4 years at Splunk, Business Development, Sales Engineer, now… Cloud!

16 years in Operations and IT

Likes: Long walks on the beach, picking things up and putting them down, gator wrestling

Dislikes: Onions, help from Rhonda, bad mic drops

Purpose

The Splunk Cloud Adoption Team works with customers and resources to assist customers in fully utilizing Splunk to meet their needs.

This talk will outline various points to Splunk Cloud and the recommended best practices for using Splunk Cloud and working with Splunk Support.

splunk>cloud™

Agenda

- **General Architecture**
  Cloud Architecture **vs** On Premise Deployments **vs** Hybrid Deployments

- **Best Practices**
  - SSO / LDAP / Authentication Schemes / User Management
  - On Premise Forwarders
  - TA Management and App Deployment

- **Working with Support**
- **Questions .. AND .. Answers!**

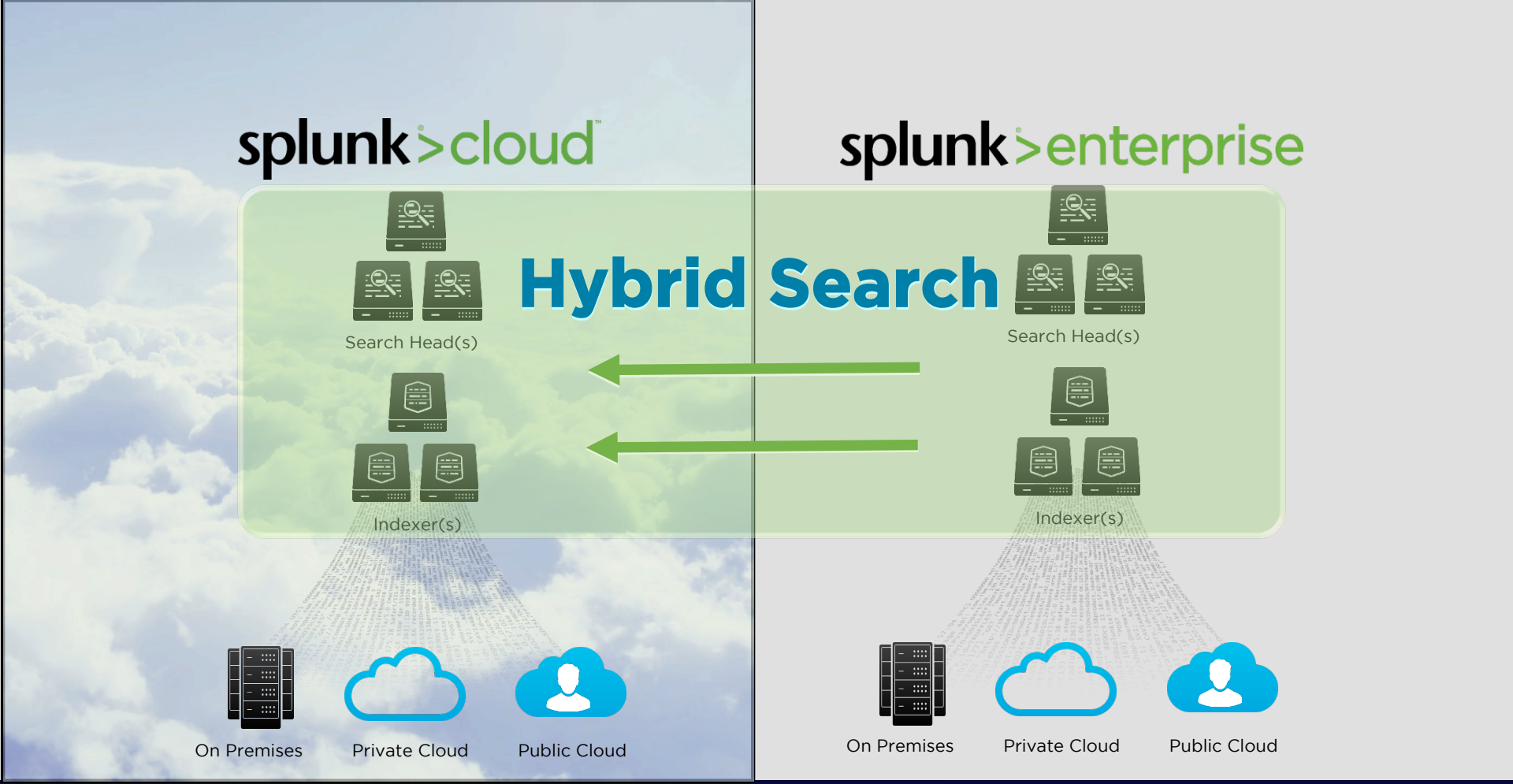
This talk is…..

A high-level Overview of what you get, and can do, with Splunk Cloud. This includes best practices and recommendations on how to work effectively with Splunk Support.

This talk is NOT…..

This talk is not a *deep dive session*.

We won't teach you how to configure or deploy the Splunk! You should already have an general understanding of Splunk Cloud. On Premise components such as a Search Head, Indexer, Indexer Cluster, Heavy / Universal Forwarders, and Apps will be mentioned, but it is not necessary to understand this to gain from the presentation


splunk>cloud
splunk>enterprise
Hybrid Search
Search Head(s)
Search Head(s)
Indexer(s)
Indexer(s)
On Premises
Private Cloud
Public Cloud
On Premises
Private Cloud
Public Cloud

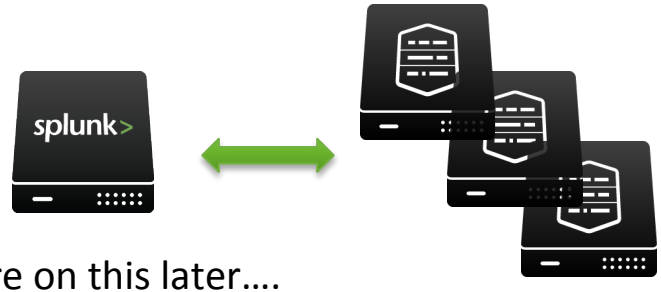
Splunk Cloud Offerings

Self-Service Splunk

- Click through to purchase!
- Up to 25gb a Day
- Single Instance!
- ***https://prd-*.cloud.splunk.com***

Managed Splunk

- Full Index Cluster
- Up to **N** tb+ a Day
- Encryption at Rest (As an option!)
- https://*.splunkcloud.com
- Have to contact sales..



*More on this later….

Managed

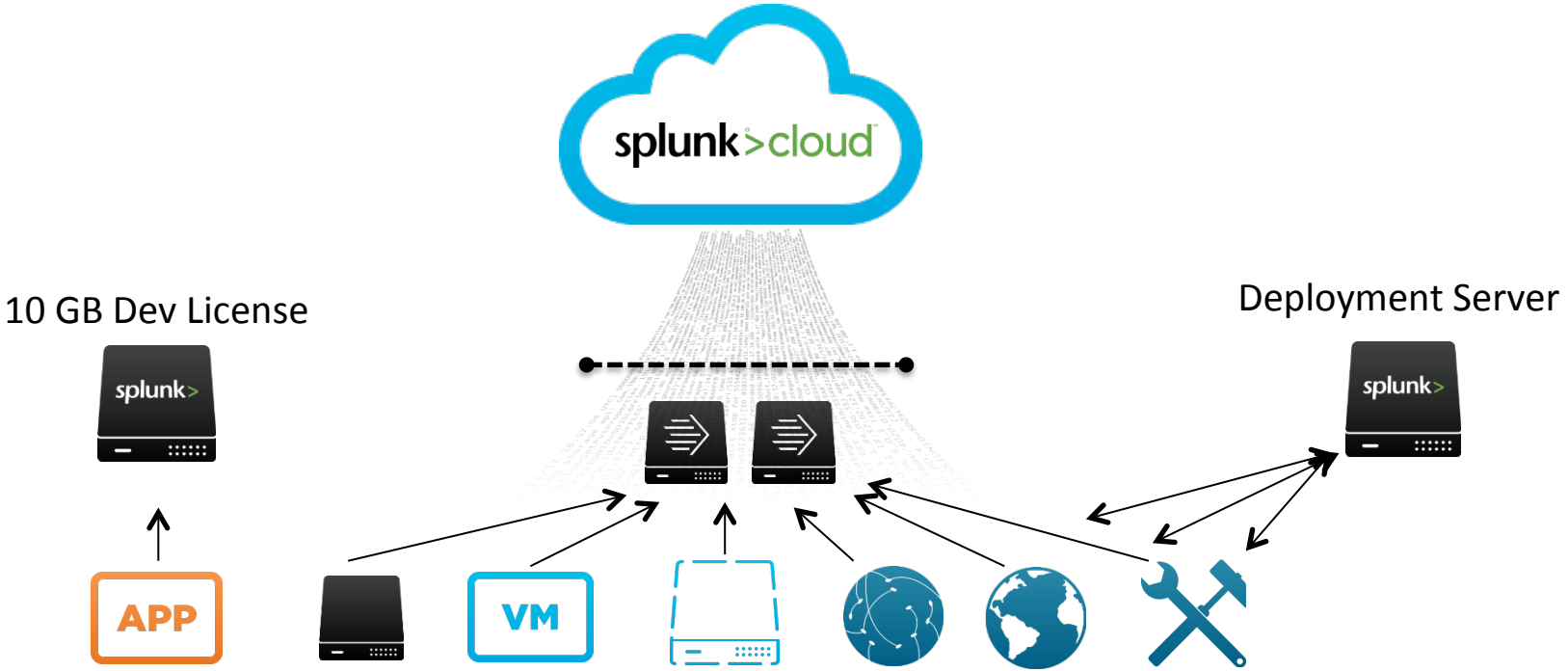
Splunk's Responsibility

- Splunk is running
- Reasonable response times
- App management
- Configuration management

Your Responsibility

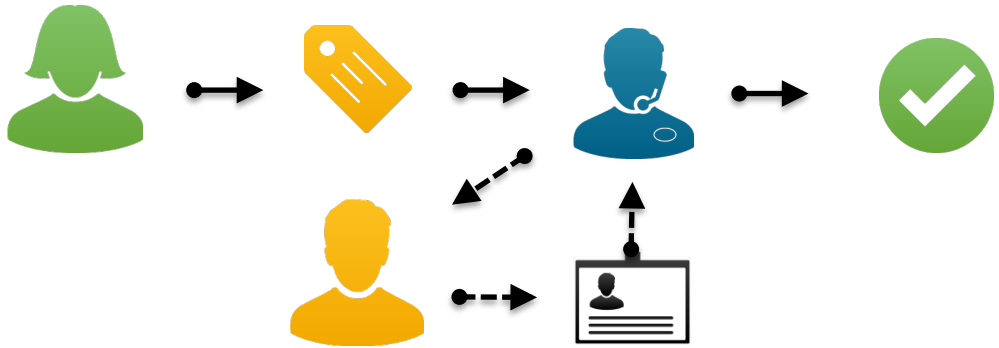
- Search and Dashboard development
- Forwarder & input management
- App creation
- Edits/Additions to .conf files

The Ideal Splunk Cloud Deployment..



SSO / LDAP / Auth

- Supported IDP: Azure, ADFS, Ping Federate, Okta
- SAML 2.0 Compliant – it works, but not supported



Choosing Your Forwarders..

Questions....

- Do I need a modular input? { DBX, EPO, OpsecLEA etc }
- Do I need to be able to Filter / Mask Data before it goes to the Cloud?
- Do I need a Deployment Server (DS) or a local License Master (LM)?

Yes?

Heavy Forwarder!

No?

Universal Forwarder!

* General rule of thumb.. There are always exceptions..

Helpful Searches

- License Usage

  index=_internal sourcetype=splunkd source="/opt/splunk/var/log/splunk/license_usage.log" type="RolloverSummary"| bucket _time span=1d | stats sum(b) as DailyVolume by _time | eval DailyVolume=round(DailyVolume/1024/1024/2014,2) | eval license="2000"

- Storage remaining

  …

- Volume by sourcetype

  …

All searches & more can be found under ‘Cloud’ on blogs.splunk.com

Article: BITTP https://blogs.splunk.com/cloud/bittp

Building (better) Apps.. (not only) for the Cloud

Make Apps better… faster... sexier

Splunk Cloud And Custom Apps

- All apps have to be vetted, and approved, before they can be Deployed!
- Vetting Process in going through a Major Process improvement
- Vetting *DOES* takes time..

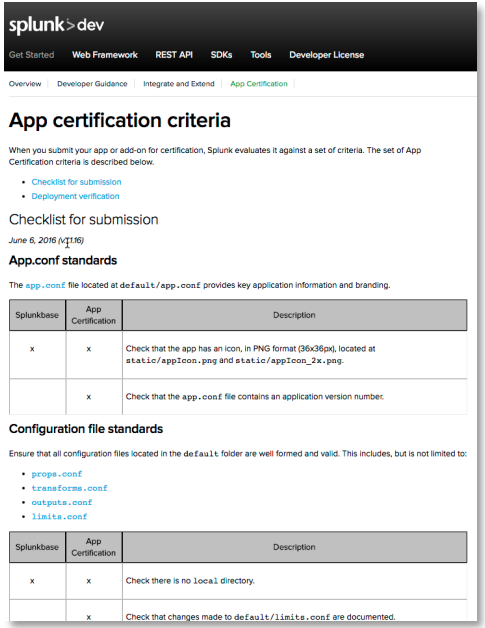
Splunk App Vetting

App Vetting is process for ensuring Apps submitted by customers meet guidelines for Splunk Cloud

App Vetting and App Certification have unified criteria on:

- ☑ Security
- ☑ Quality
- ☐ Good Form

New



splunk>dev

Get Started | Web Framework | REST API | SDKs | Tools | Developer License

Overview | Developer Guidance | Integrate and Extend | App Certification

App certification criteria

When you submit your app or add-on for certification, Splunk evaluates it against a set of criteria. The set of App Certification criteria is described below.

- Checklist for submission
- Deployment verification

Checklist for submission

June 6, 2016 (V116)

App.conf standards

The `app.conf` file located at `default/app.conf` provides key application information and branding.

Splunkbase	App Certification	Description
x	x	Check that the app has an icon, in PNG format (36x36px), located at `static/appIcon.png` and `static/appIcon_2x.png`.
	x	Check that the `app.conf` file contains an application version number.

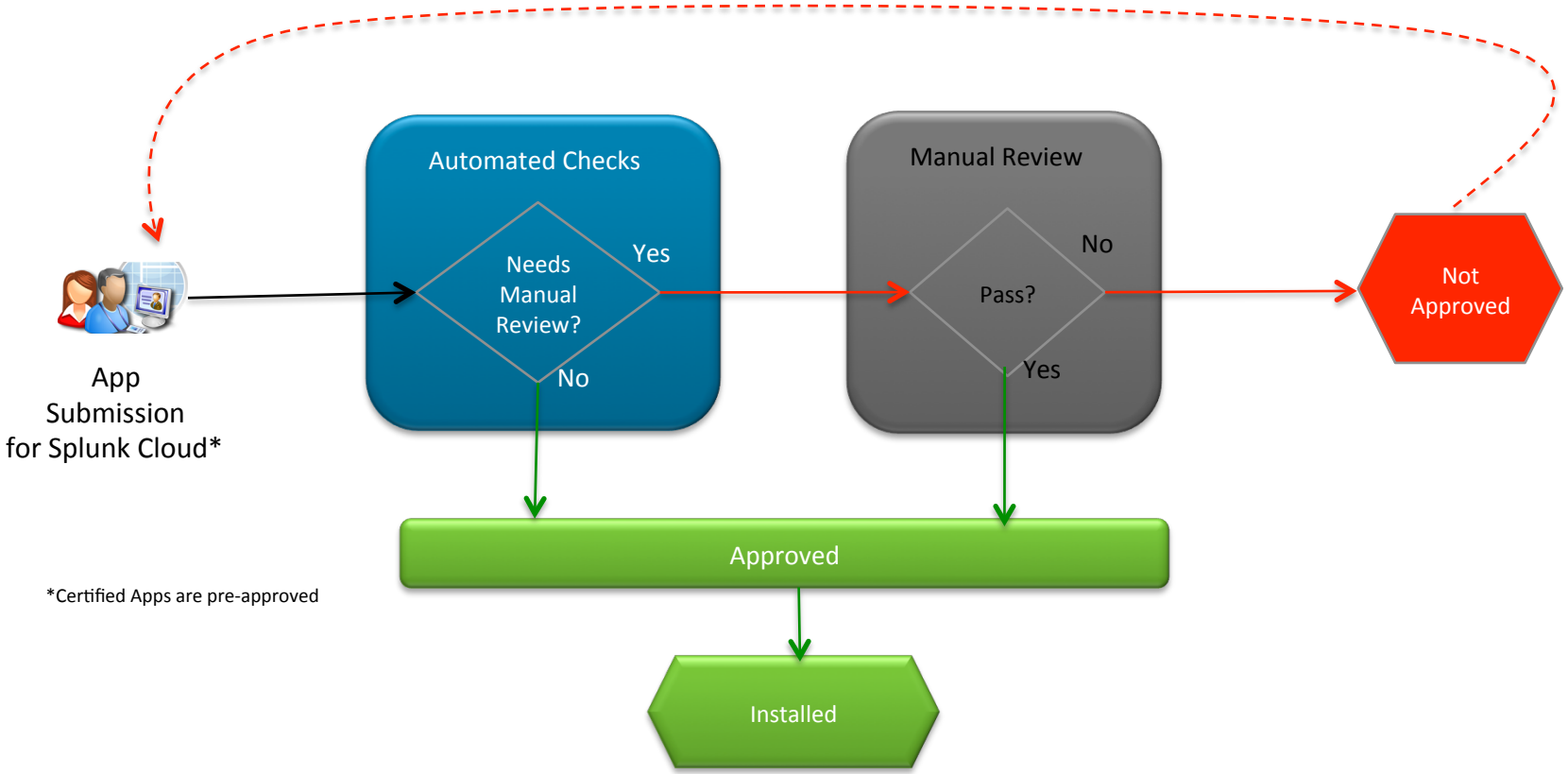
Configuration file standards

Ensure that all configuration files located in the `default` folder are well formed and valid. This includes, but is not limited to:

- `props.conf`
- `transforms.conf`
- `outputs.conf`
- `limits.conf`

Splunkbase	App Certification	Description
x	x	Check there is no `local` directory.
	x	Check that changes made to `default/limits.conf` are documented.

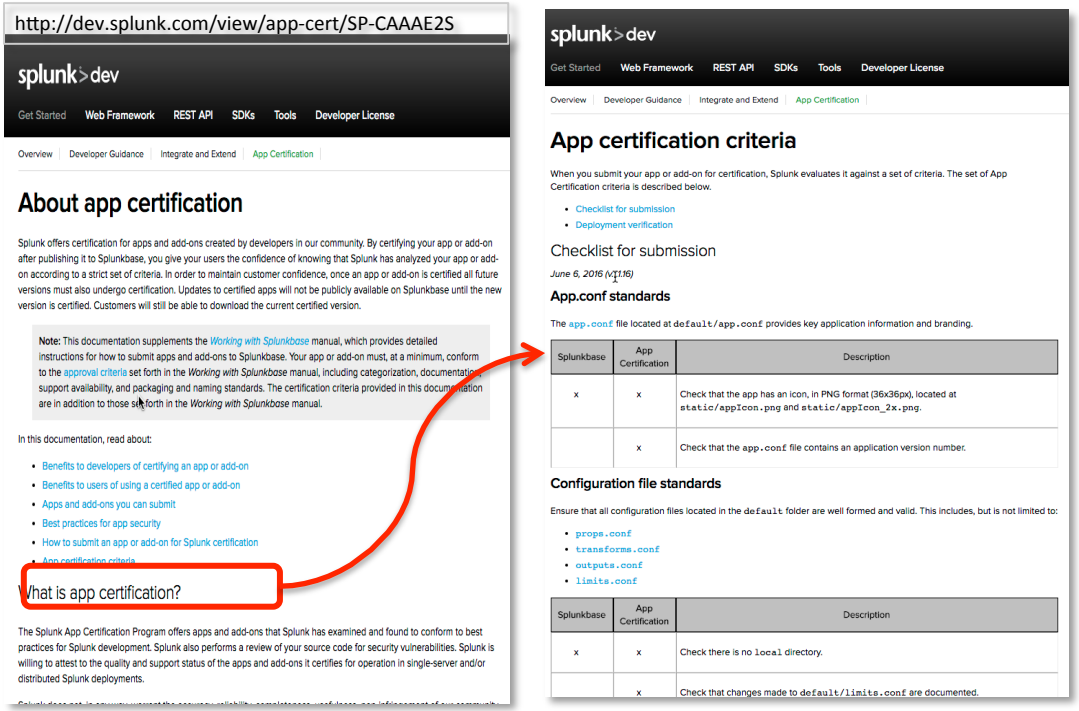
App Vetting Process



*Certified Apps are pre-approved

Splunk App Certification

- For 3rd party developers
- Revised set of guidelines
  - 141 specific best-practice guidelines
- Guidelines focus on:
  - Security
  - Quality
  - Good Form
- Certified App displayed with a certification mark on Splunkbase



(Some) Reasons Apps Fail...

- No Compiled Executables!
- All outbound communication needs to be *encrypted*! E.g. https
- All content must be within the App Context!
- Custom scripts must be limited to Splunk's internal python!
- Credentials **MUST** be *encrypted*!
- No file system / process manipulation is allows (Only lookups/KV Store)

*Full list is available at : http://dev.splunk.com/view/app-cert/SP-CAAAE2S

App Management...

Production

- Use a DS
- Inspect the app yourself!
- Make them your own!

Development

- Wut? A dev environment for apps?
- Use a new index
- Version control
- Follow Best Practices

Working With Support

It’s not working!

Its slow!

How do I do…..

My extractions aren’t working..

Can’t see my data!

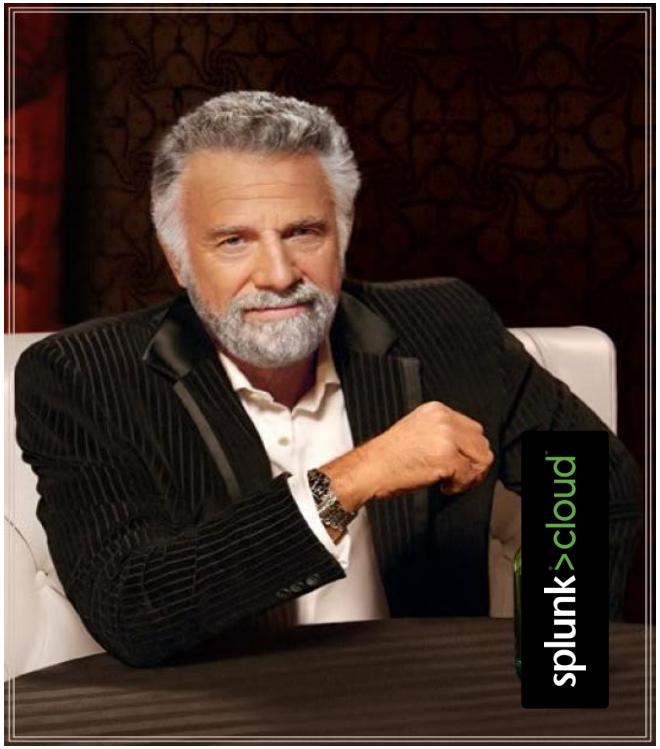
Important Links

Informative and Useful Links for Splunk Cloud

Splunk Answers – https://answers.splunk.com
Splunk IRC!

- Splunk Cloud Latest FAQ : https://docs.splunk.com/Documentation/SplunkCloud/latest/FAQs/FAQs
- Splunk Cloud Docs : https://docs.splunk.com/Documentation/SplunkCloud/latest/User/WelcometoSplunkCloud
- Splunk Answers : https://answers.splunk.com/topics/splunk-cloud.html
- Splunk Cloud TOS : http://www.splunk.com/en_us/legal/terms/splunk-cloud-terms-of-service.html
- Splunk Cloud Service Schedule : http://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html
- Splunk Cloud Maintenance Policies : http://www.splunk.com/view/SP-CAAAMTU
- App Certification : http://dev.splunk.com/view/app-cert/SP-CAAAE2S
- Splunk AddOn Builder : http://dev.splunk.com/view/SP-CAAAE9F

Q & A



"I may not normally answer questions when on stage, but with Splunk > Cloud, I do. And I do it real time. "

What Now?

Related breakout sessions and activities…

THANK YOU

splunk>