Working with Splunk Cloud

Best Practices and Things Best Known

Eric Six    | Staff Architect
Shaun Bland | Cloud Advisory Engineer

2017/09/27   | Washington, DC
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. © 2017 Splunk Inc. All rights reserved.
Just imagine..

The Adventure starts now...
Who We Are..  

Eric Six

Splunk-ing over 6 years, 4+ years as a Splunker. Before that.. A very happy customer.

Based in Japan, covering Architecture all over Asia, Australia, and New Zealand

Architecting and Deploying solutions of all sorts and sizes

▶ Favorite Command : tstats
▶ Favorite App : ITSI!
▶ Hobbies : Anything Alpine, Everything Bourbon...
▶ Active Splunk Answers : esix_splunk
Who We Are..
Shaun Bland

Splunk for 1.5 years. Asia (Japan and Hong Kong) for 15 years.

Back in Texas for the last 1.5 years. Two little splunkers at home

Background in Cloud, Servers, Data Centers

- Favorite thing to do: fix things
- Hobbies: Hike, bike, play poker with 7yr old
- Act as customer advocate for Splunk Cloud customers
Purpose and Agenda

► Splunk Cloud Architecture
  • Splunk Cloud Architecture vs On Premise Deployments

► Best Practices
  • Authentication Schemes / User Management
  • Forwarders / Aggregation Tier
  • Knowledge Object and App Management

► New Features

► Working with Support
Hybrid Search

Splunk Cloud

Splunk Enterprise

Search Head(s)

Indexer(s)

On Premises

Private Cloud

Public Cloud

On Premises

Private Cloud

Public Cloud
Splunk Cloud Deployments

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

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

*More on this later....
Managed Splunk

Splunk’s Responsibility
- Splunk is UP and Running
- Response Times
- App and KO Management
- Conf file changes

Your Responsibility
- Search and Dashboard Management
- Forwarder and Input Management
- App Creation and Validation
- Conf file creation and changes for data sources

Patching and Upgrading!
“The only true wisdom is in knowing you know nothing.”

-- Socrates
Ideal Deployment..
Authentication Methods

- Supported IDP: Ping, Okta, Azure AD, ADFS, Onelogin, Optimal, CA Siteminder
- SAML 2.0 Compliant – it should work! Confirm on Splunk Docs!
Choosing your Forwarders..

Questions....

▶ Do I need a modular input? { DBX, AWS, 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)?

* General rule of thumb.. There are always exceptions... Ask the Experts.

Yes?

Heavy Forwarder!

No?

Universal Forwarder!
Building (better) Apps.. for the Cloud

Make Apps better... faster ... stronger
Splunk Cloud and Custom Apps

▶ All apps have to be vetted, and approved, before they can be Deployed!
▶ Vetting **DOES** takes time..

Make Apps according to Best Practices...
App Vetting Process

Submit App → Pre-check → Code Review → Security Review → App Certified

*Certified Apps are pre-approved
App Certification Criteria

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

Add-on Builder is Totally Awesome!

GUI Creation of—

▶ Basic Data Inputs!
▶ FEX ! CIM Mapping
▶ Advanced Inputs { REST / HEC / Python etc}
▶ Adaptive Response Actions!
(Some) Reasons Apps Fail..

- No Compiled Executables!
- No indexes.conf!
- All outbound communication needs to be encrypted!
- All objects 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-CAAAAE2S](http://dev.splunk.com/view/app-cert/SP-CAAAAE2S)
App Management..

Production
- Use a DS
- Inspect the app yourself!
- *make them your own*

Development
- Dev environment for apps!
- TA Builder!
- Use a non-production index
- Version control
- Best Practices
Splunk Cloud Features

Splunk Cloud gets the cool stuff first!

- Metrics Store
- Search Optimization
- Dashboard Editing enhancements and Trellis Layouts
- Self-service App Installation
- And much much moooooore!
Working with Support

Its like Chemistry..

▶ Totally awesome!

▶ OR... not so much
Wrapping it up…

1. Splunk Cloud is Splunk!
2. Best Practices are the Best!
3. Splunk Cloud is Excellent!
Important Links

Informative and Useful Links for Splunk Cloud

- Splunk Cloud Latest FAQ: https://docs.splunk.com/Documentation/SplunkCloud/latest/FAQs/FAQs
- Splunk Answers: https://answers.splunk.com/topics/splunk-cloud.html
- https://splunk.box.com/v/cloudappsbestpractices
What Now?

Related breakout sessions and activities…

- Introducing Splunk Validated Architectures (Wednesday | 3:30 PM-4:15 PM)
- Digital Transformation is Here - Progress Report and Lessons Learned from Cloud-First Initiatives in the Public Sector (Wednesday | 4:35 PM-5:20 PM)
- Security Ninjutsu Part Four: Attackers Be Gone in 45 Minutes of Epic SPL (Wednesday | 2:15 PM-3:00 PM)
- Customer Success Boot at Source=*pavillion
Thank You

Don't forget to rate this session in the .conf2017 mobile app