Splunk Gone Wild! – Innovating A Large Splunk Solution At The Speed Of Management

Kevin Dalian

kdalian@ford.com

Glen Upreti

Glen.Upreti@Sierra-Cedar.com

.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.

Introductions

Kevin Dalian
Team Lead Server Hosting Tools
Ford Motor Company
Nothing Interesting About Kevin, he’s a boring work-aholic.

Glen Upreti
Director Enterprise and Cloud Technologies
Sierra-Cedar
Terrible at Jenga

Agenda

- Where We Came From
- Where We Planned to Go
- Where We Ended Up
- Installation
- On Boarding Data
- What We’re up to Now
- Q & A

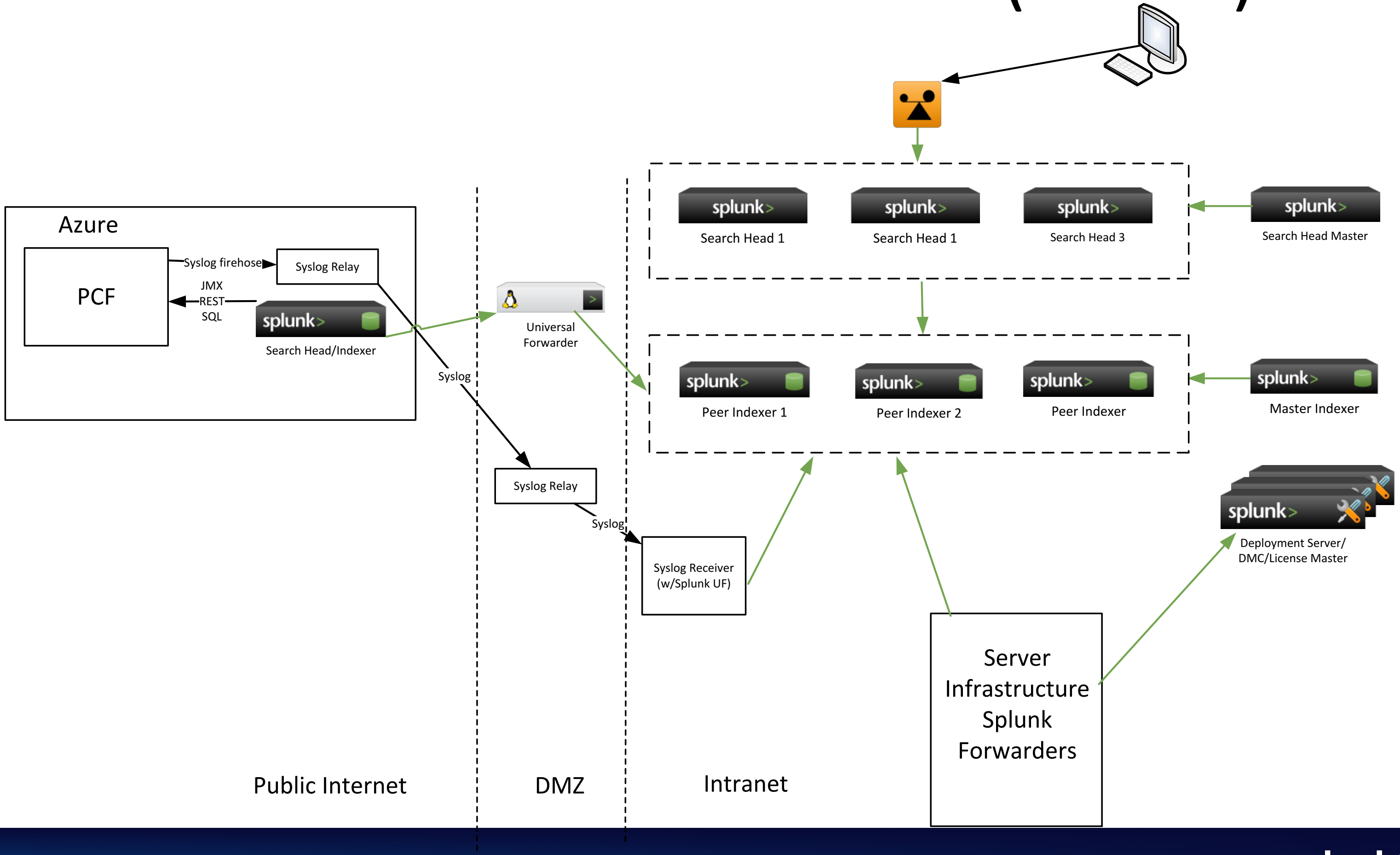
Where We Started

- 2 Splunk Environments – Network and Server Operations
- Server Ops
  - 4 Standalone Search Head / Indexers
  - 3 Deployment Servers
  - 20 Gb license
  - +11,500 Universal Forwarders

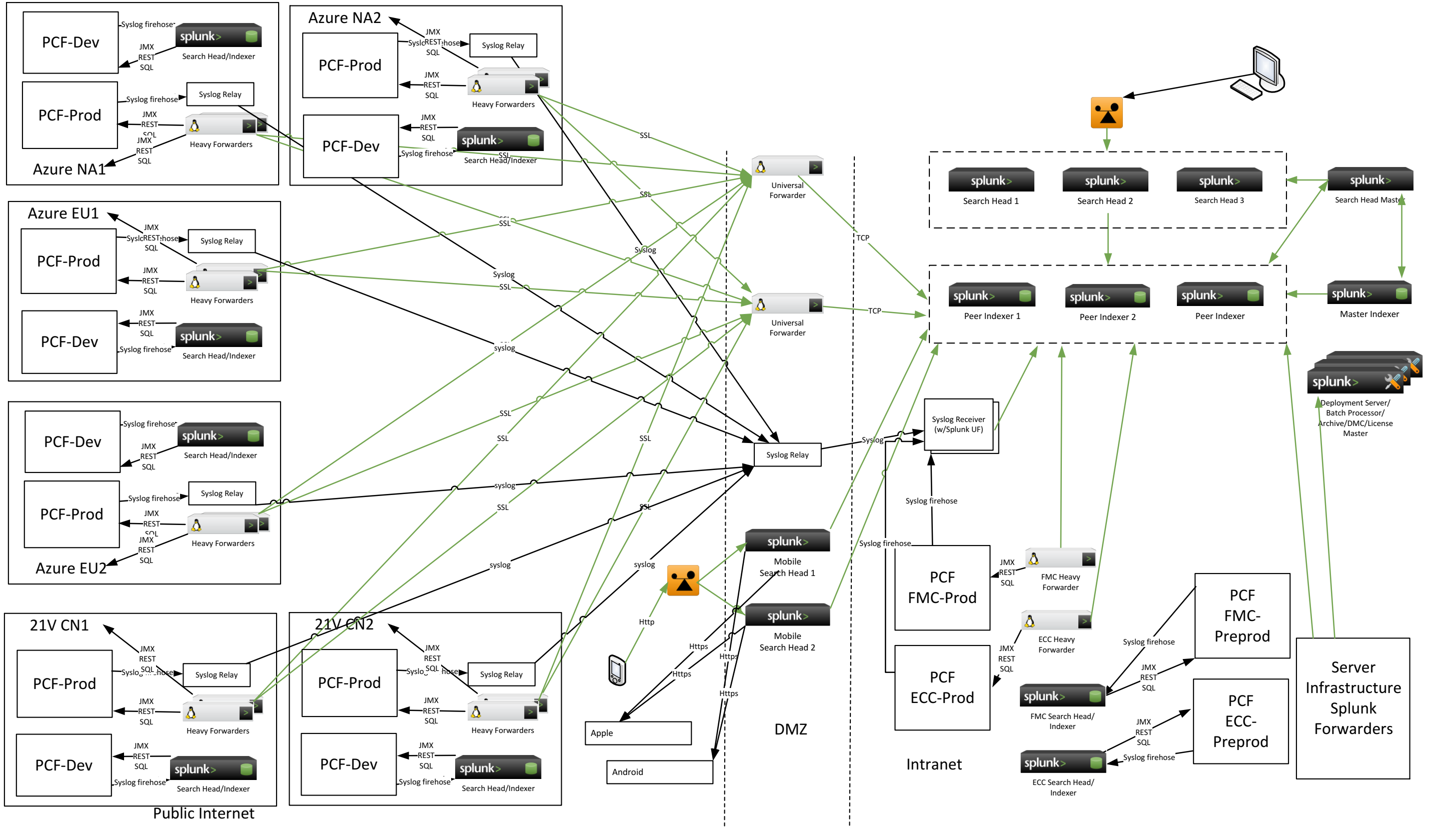
Where We Planned to Go

- Major new Ford Initiative – FordPass/Connected-X
  - PCF – Pivotal Cloud Foundry
  - Microsoft Azure Cloud
  - Mixture of internal and external applications and data
  - 100Gb/day

Where We Planned to Go (cont'd)



Where We Ended Up



Installing

- Glen and Kevin meet and plan for installation tasks
- Have a POC environment in Azure
- Azure to on-premise, HOW???
- Started with temporary stand alone instance

Installing (Surprises)

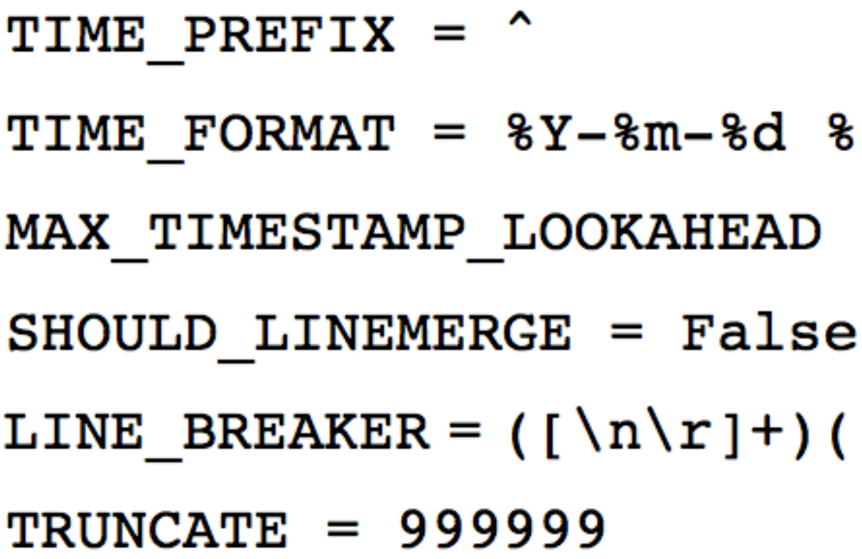
- Hardware shows up & everything falls apart
  - Hardware arrived piece meal
  - Not enough CPUs
  - Azure VMs, we were the first template install
  - Servers in ‘Public’ DMZ weren’t publicly accessible
- Even with issues SH Cluster and IDX Cluster all installed within days!

On Boarding Data

- On boarded data from
  - Pivotal Cloud Foundry
  - Microsoft Azure PAAS via DB Connect
  - Third party and custom developed inputs

Onboarding Data

- When onboarding always set
  - TIME_PREFIX
  - TIME_FORMAT
  - MAX_TIMESTAMP_LOOKAHEAD
  - SHOULD_LINEMERGE
  - LINE_BREAKER
  - TRUNCATE



```
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %
MAX_TIMESTAMP_LOOKAHEAD
SHOULD_LINEMERGE = False
LINE_BREAKER = ([\n\r]+)(
TRUNCATE = 999999
```

Onboarding Data (Surprises)

- ‘Oh by the way …’
  - New inputs
  - New regions
  - New environments (pre-production)
  - New teams
  - New Splunk License
  - Sensitive Data - Need for obfuscation

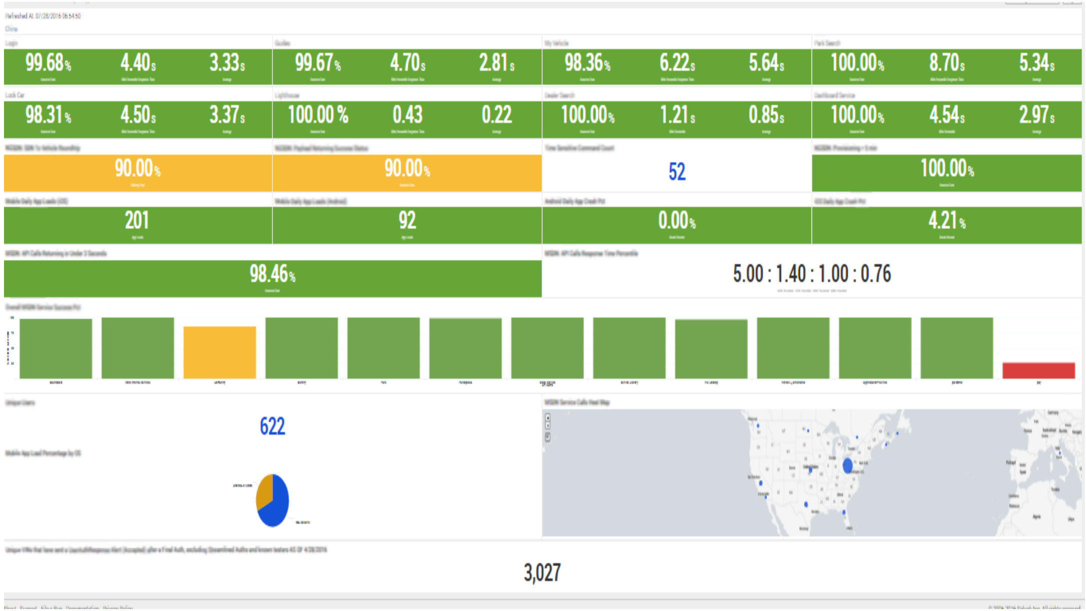
Got Data, Now What?

- Prototyped Dashboard wrap up quick.
- What Does This Mean?
  - Engage developers and user communities
- Keep Creating
  - Always be moving forward
- Alerts
  - Alerting is an iterative process
  - Be prepared for a lot of noise at first
  - Refine, refine, refine

Got Data, Now What? (Surprises)

- Surprises:
  - Massive Dashboards
  - New Users and Roles
  - Data Security
  - Retention Times

Oh yeah, and mobile …



Refreshed At: 07/28/2016 06:54:50

China

Login: 99.68% 4.40s 3.33s

Guides: 99.67% 4.70s 2.81s

My Vehicle: 98.36% 6.22s 5.64s

100.00% 8.70s 5.34s

Lock Car: 98.31% 4.50s 3.37s

Lighthouse: 100.00 % 0.43 0.22

Dealer Search: 100.00% 1.21s 0.85s

100.00% 4.54s 2.97s

90.00%

90.00%

52

100.00%

201

92

0.00%

4.21%

98.46%

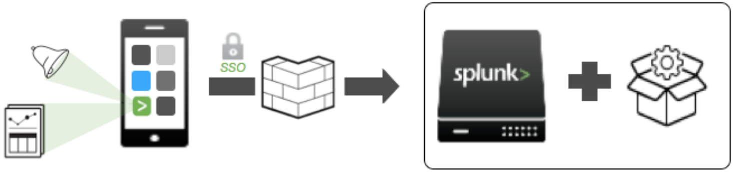
5.00 : 1.40 : 1.00 : 0.76

622

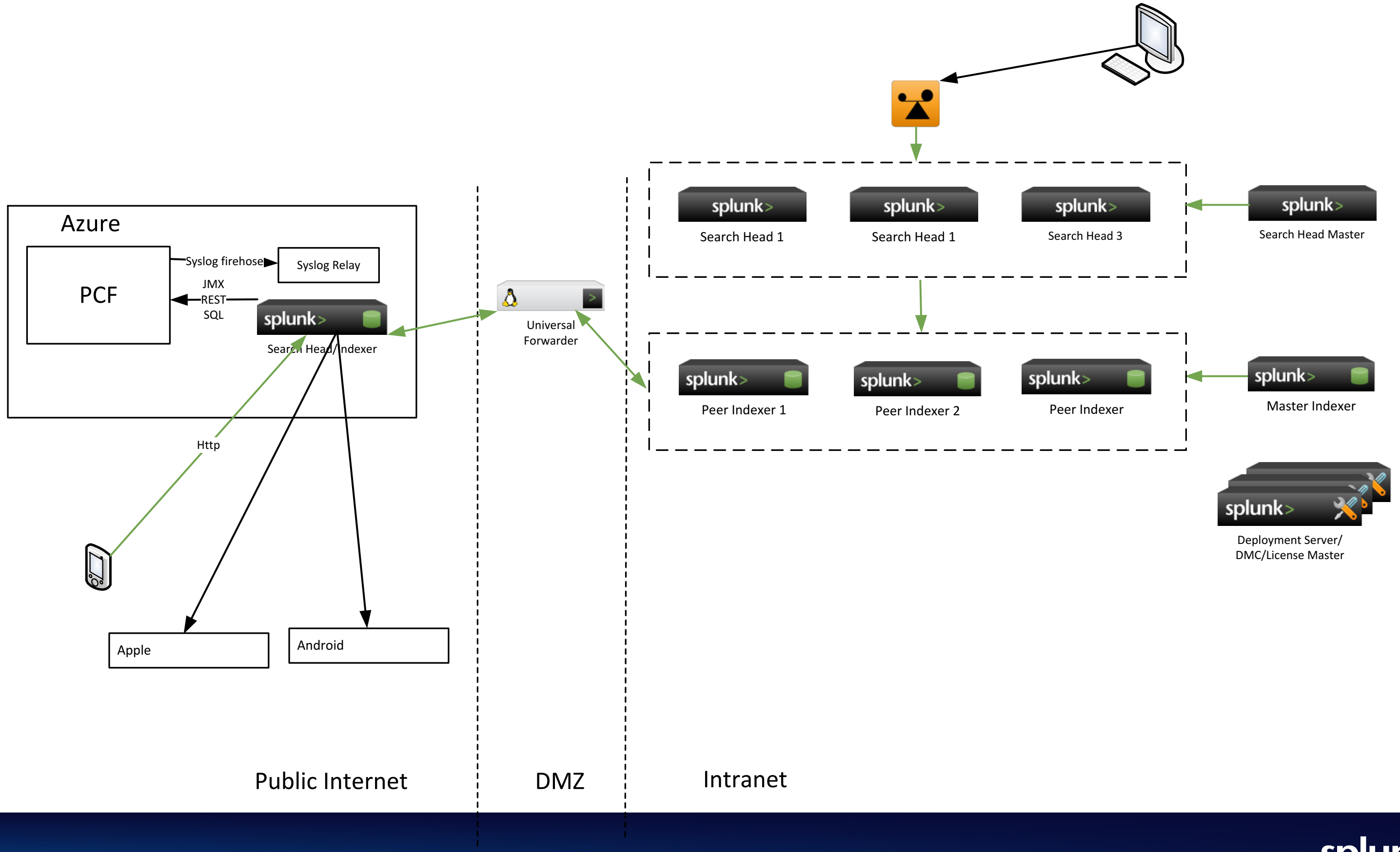
3,027

Mobile Madness

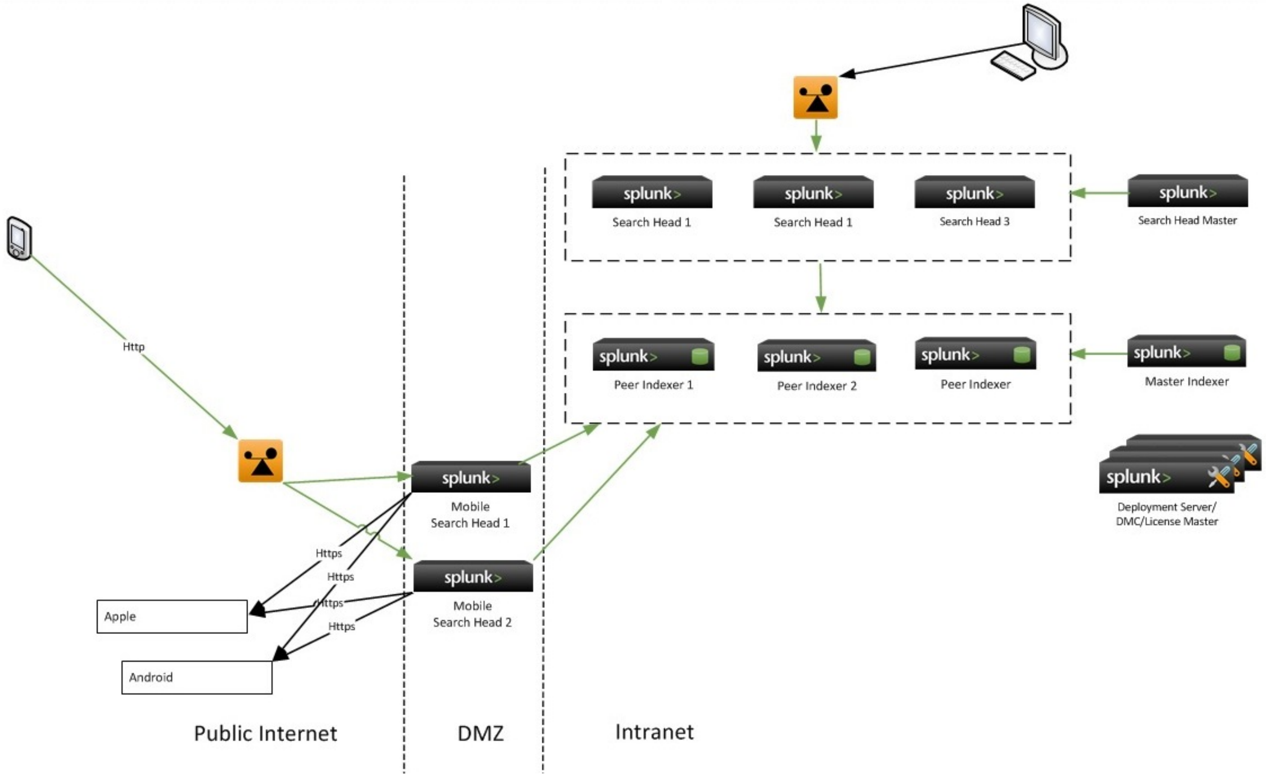
- Splunk Add-on for Mobile Access
  - Crazy Easy!
- Initial POC in Azure worked like a champ
- Planned, prepared and moved to DMZ
- Notifications don’t work
  - New management surprise … the kind you don’t want
- Back to the drawing board



Mobile Madness (Temp Solution)



Mobile Madness (Eventually)



Where Are We Now?

- Planning for the Future/Scaling
- Refining and documenting
- Migrating data/apps from original environment
- Expanding the customer base
- Still refining dashboards
- Re-sourcetyping
- Preparing for more management shenanigans

Advice Moving Forward

1. Insist non-production environment
2. Work with the customer to further understanding of data
3. Define/Document all Customer requirements and get sign off
4. Avoid the data graveyard
5. Splunk is very flexible, keep an open mind and stay calm!

And Remember …

“Fall seven times and stand up eight.”

- *Japanese Proverb*

Q & A

Questions?

THANK YOU

.conf2016

splunk>