Splunk .conf18
Hardware Monitoring @ workday®

Designing and Deploying a 24x7 Service

Jordan Perks

James Barnes

Soham Roy

October 2018 | Version 1.3

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.

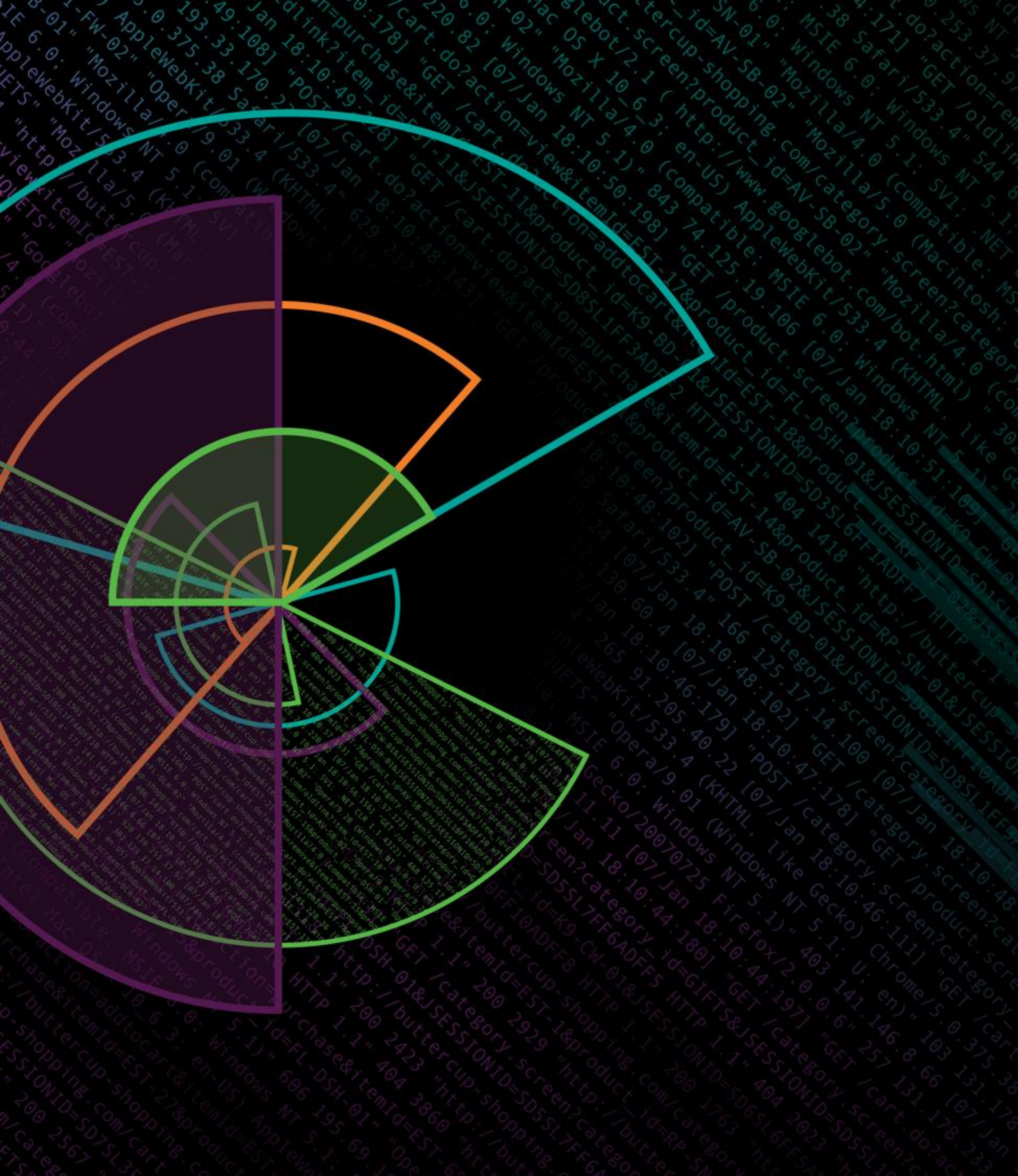
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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.

Center of Excellence

Presenter: Jordan Perks

Splunk Center of Excellence

- Architecture
  - Platform as a service
  - Design
  - Maintenance and Upgrades
- App Dev
  - Creation of apps for security team
  - Creation of Workday Add-on for Splunk
  - Enterprise Security and ITSI Administration
- Customer Support
  - Office Hours
  - User Training and Enablement
  - Encouragement of power user self-sufficiency

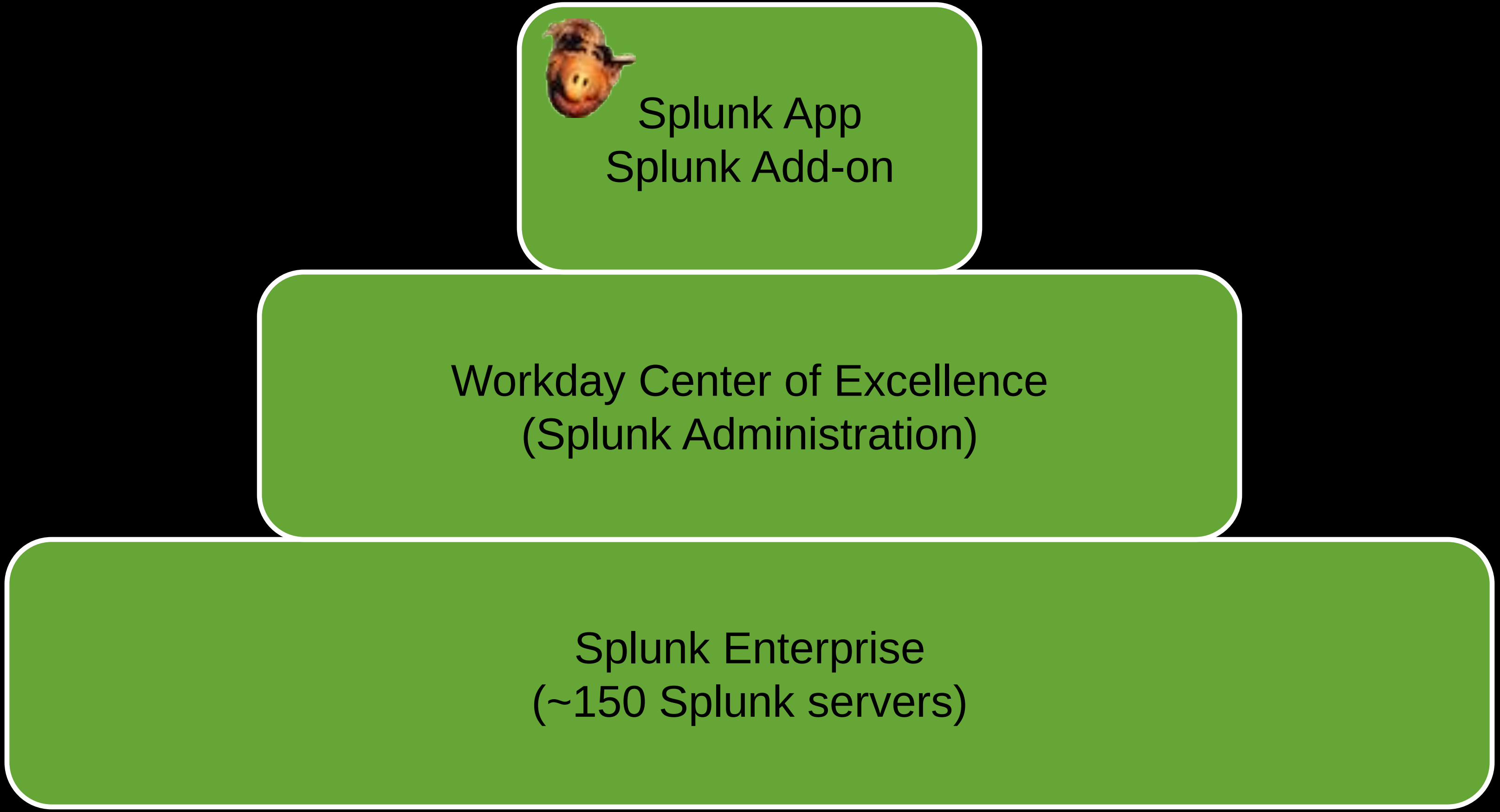


Service Overview

Presenter: James Barnes

Standing on Shoulders

Little additions can make big impacts



Splunk App
Splunk Add-on

Workday Center of Excellence
(Splunk Administration)

Splunk Enterprise
(~150 Splunk servers)

Objective

Here’s your challenge…

- Find amber lights failures for 20,000+ servers
- The existing product being sunset – be quick!
- Develop a 24x7 service
- Use limited resources (2 engineers)
- Keep data in-house (new rule)
- Integrate the service with existing tools
  - Jira
  - Slack
  - DCIM DB

Amber Lights Finder
Nickname is Alf

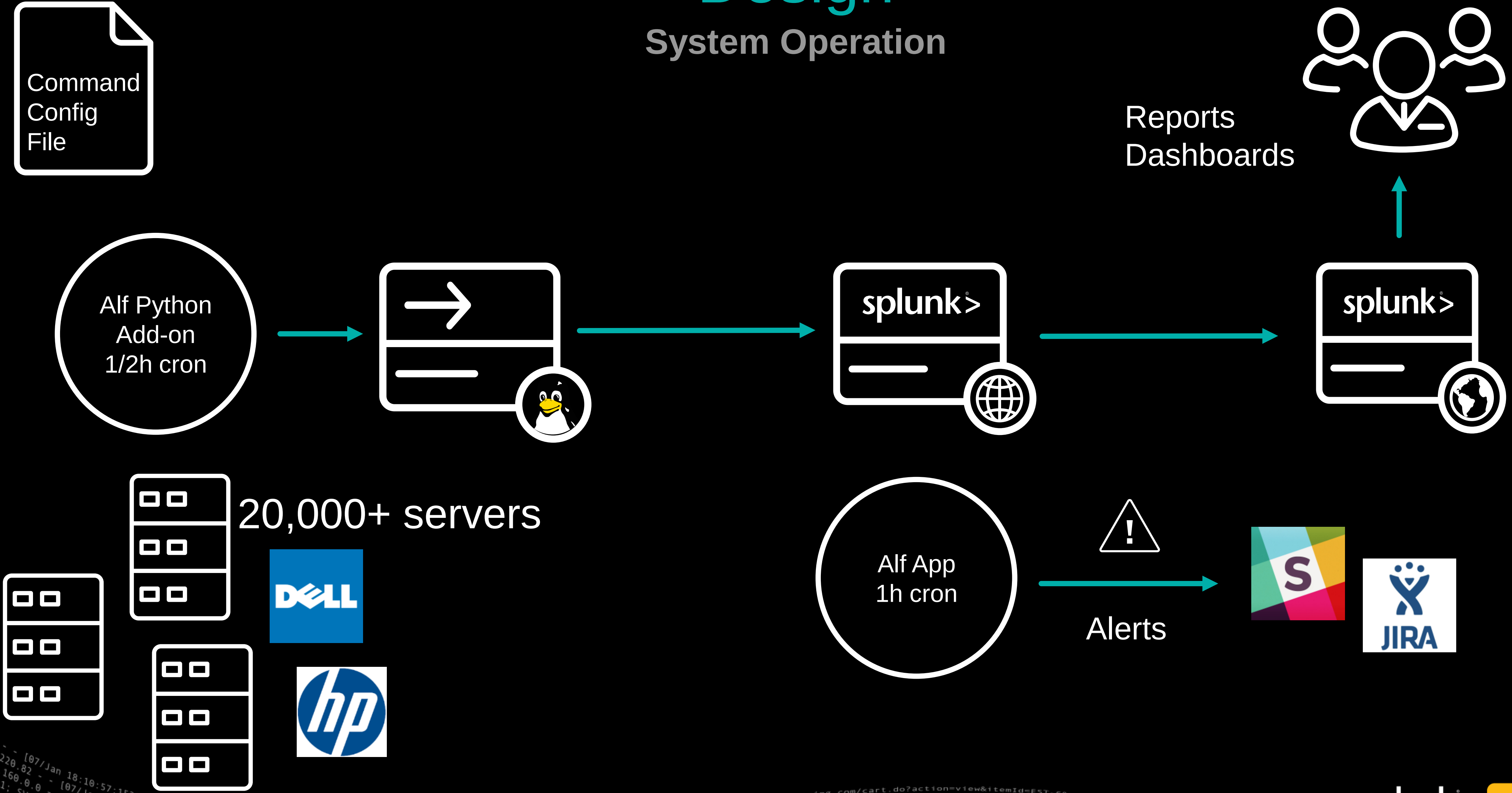
> “Alf is saving dc-ops time and money. It improves server reliability and uptime, and just plain kicks ass.”

Ken Hartman
Director of Infrastructure Data Centers

Happy Customer

Design

System Operation



Example Linux Commands

Executed every 30 minutes

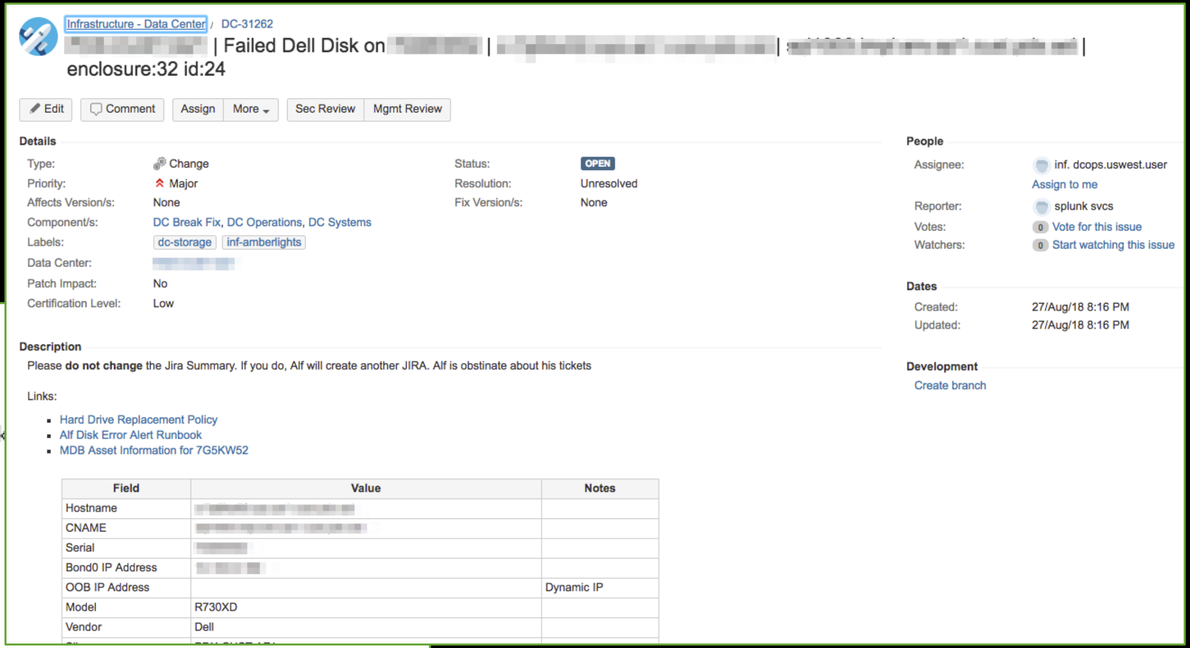
- Common
  - /usr/sbin/dmidecode -qt chassis
  - /bin/echo -n 'uptime: '; /usr/bin/uptime
  - /bin/netstat -i
- Dell (omreport)
  - /opt/dell/srvadmin/bin/omreport storage pdisk controller=0
  - /opt/dell/srvadmin/bin/omreport system esmlog
  - /opt/dell/srvadmin/bin/omreport chassis fans
- HP (hp-health)
  - /usr/sbin/hpssacli ctrl slot=0 pd {drive} show detail”
  - /sbin/hpasmcli -s 'show server’
  - /sbin/hpasmcli -s 'show dimm'

~50GB/day

Ten-Layer Alerting Pipeline

One macro per layer

- Get Current Data
- Add Category Error
- Add Category Details
- Add Targeting
- Prune for Category Errors
- Prune for Hard Errors
- Prune for Installed Status
- Prune for New Tickets
- Add Trigger Action Information
- Gatekeeper



Infrastructure - Data Center / DC-31262

[redacted] | Failed Dell Disk on [redacted] | [redacted] | [redacted] | enclosure:32 id:24

Details

Type: Change
Priority: Major
Affects Version/s: None
Component/s: DC Break Fix, DC Operations, DC Systems
Labels: dc-storage inf-amberlights
Data Center: [redacted]
Patch Impact: No
Certification Level: Low

Status: OPEN
Resolution: Unresolved
Fix Version/s: None

People

Assignee: inf. dcops.uswest.user
Assign to me
Reporter: splunk svcs
Votes: 0 Vote for this issue
Watchers: 0 Start watching this issue

Dates

Created: 27/Aug/18 8:16 PM
Updated: 27/Aug/18 8:16 PM

Development

Create branch

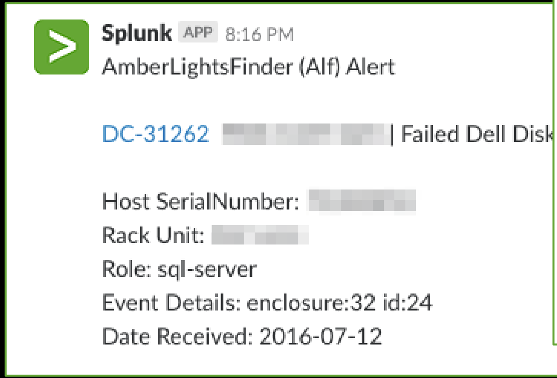
Description

Please **do not change** the Jira Summary. If you do, Alf will create another JIRA. Alf is obstinate about his tickets

Links:

- Hard Drive Replacement Policy
- Alf Disk Error Alert Runbook
- MDB Asset Information for 7G5KW52

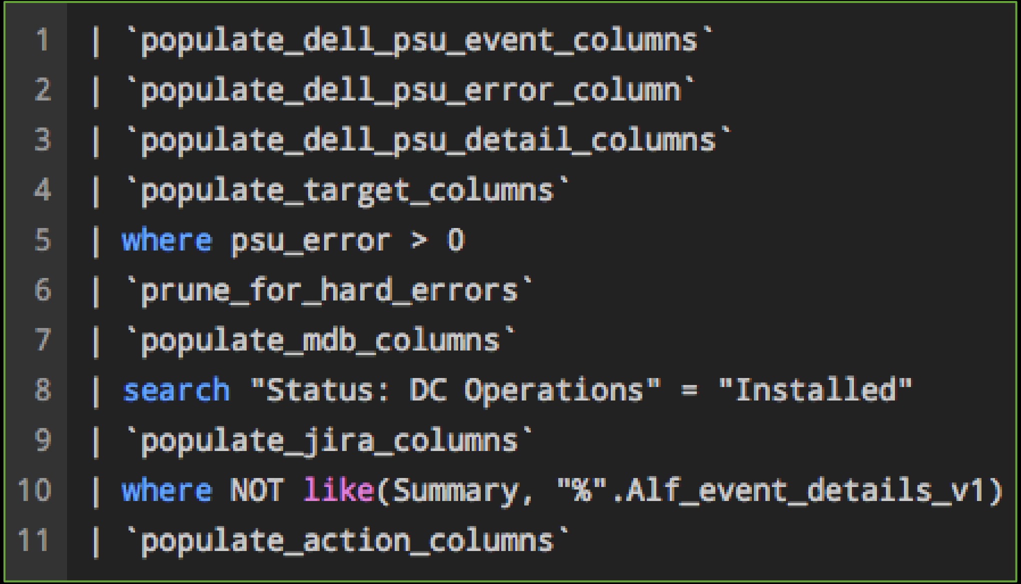
Field	Value	Notes
Hostname	[redacted]	
CNAME	[redacted]	
Serial	[redacted]	
Bond0 IP Address	[redacted]	
OOB IP Address		Dynamic IP
Model	R730XD	
Vendor	Dell	



Splunk APP 8:16 PM
AmberLightsFinder (Alf) Alert

DC-31262 [redacted] | Failed Dell Disk

Host SerialNumber: [redacted]
Rack Unit: [redacted]
Role: sql-server
Event Details: enclosure:32 id:24
Date Received: 2016-07-12



```
| `populate_dell_psu_event_columns`
| `populate_dell_psu_error_column`
| `populate_dell_psu_detail_columns`
| `populate_target_columns`
| where psu_error > 0
| `prune_for_hard_errors`
| `populate_mdb_columns`
| search "Status: DC Operations" = "Installed"
| `populate_jira_columns`
| where NOT like(Summary, "%".Alf_event_details_v1)
| `populate_action_columns`
```

Alert Statistics

First 6 months of 2018

~260 tickets/month

0 False Positives

Disks: 35%
Raid Battery: 8%

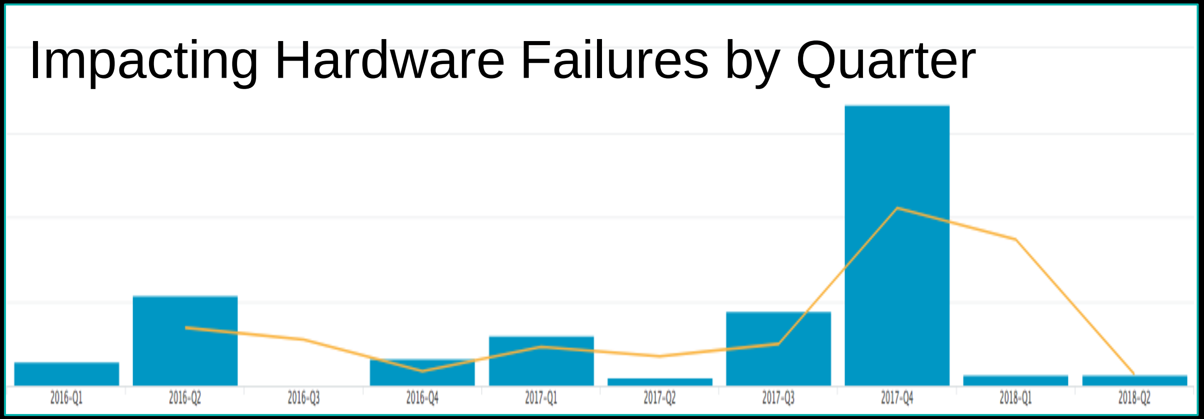
43%

1556
Automated
Tickets

Fans: 29%

Power Supplies: 16%

DIMMs: 12%



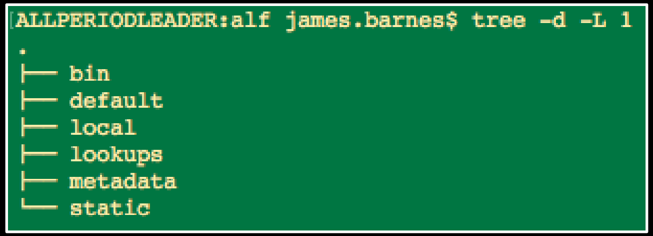
Impacting Hardware Failures by Quarter

splunk> .conf18

Lessons

If you are building a service like this…

- Keep it simple
  - With this many servers, you will see more error scenarios than you can process
- Create an app right away
  - Migrating a live service out of the search sandbox is complicated
  - Need the directory structure for source code control
  - Role-based access becomes possible



```
[ALLPERIODLEADER:alf james.barnes$ tree -d -L 1
.
├── bin
├── default
├── local
├── lookups
├── metadata
└── static
```

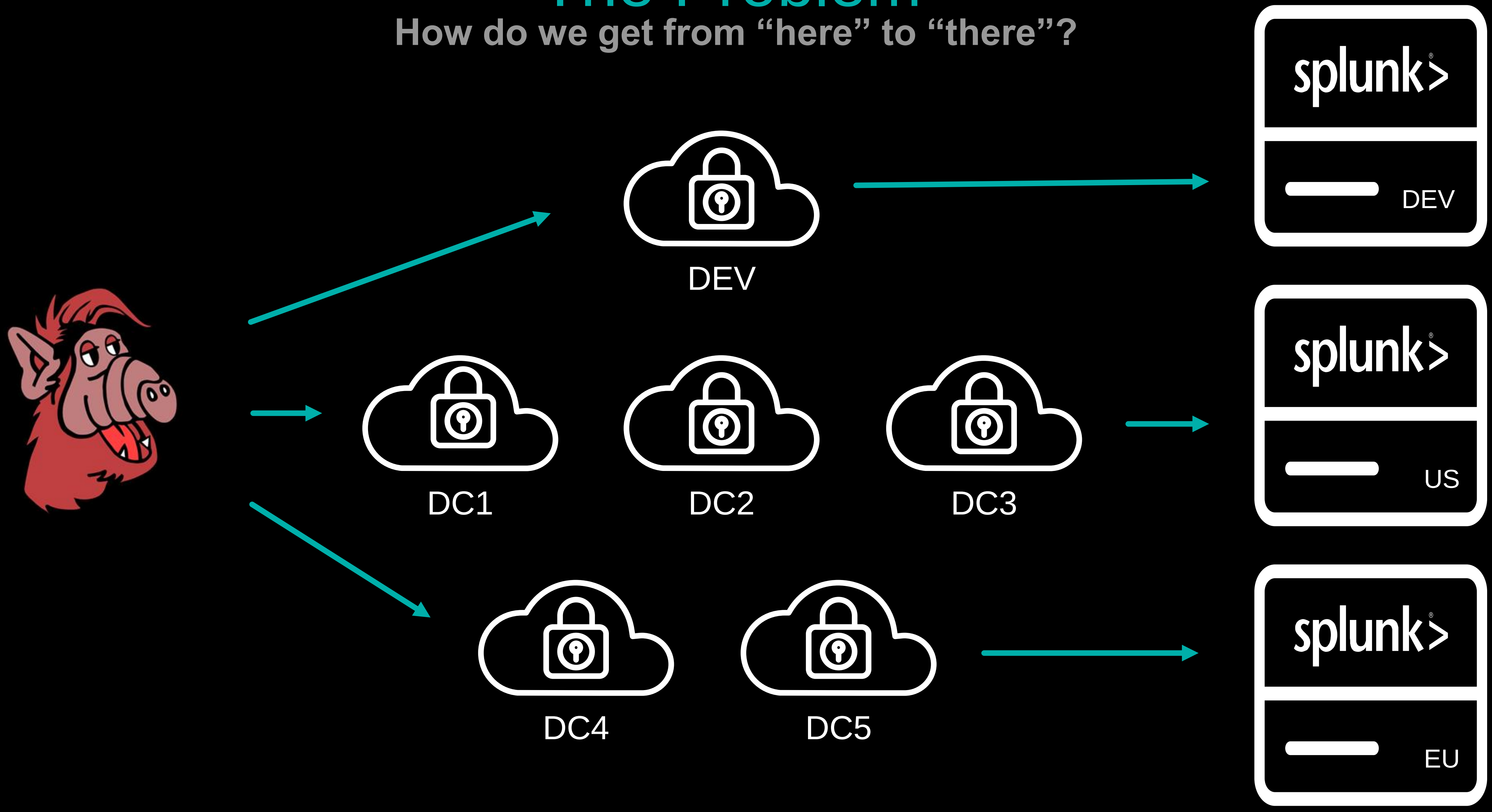
- Build an alerting pipeline
  - Define the layers and stick to them
  - New alerts are common additions
  - Use macros for code containment (DRY principle)
- Pounce on data-collection requests
  - Leads to new customers, new ingestion sources, new dashboards, new reports

Service Deployment

Presenter: Soham Roy

The Problem

How do we get from “here” to “there”?



Breaking Things Up

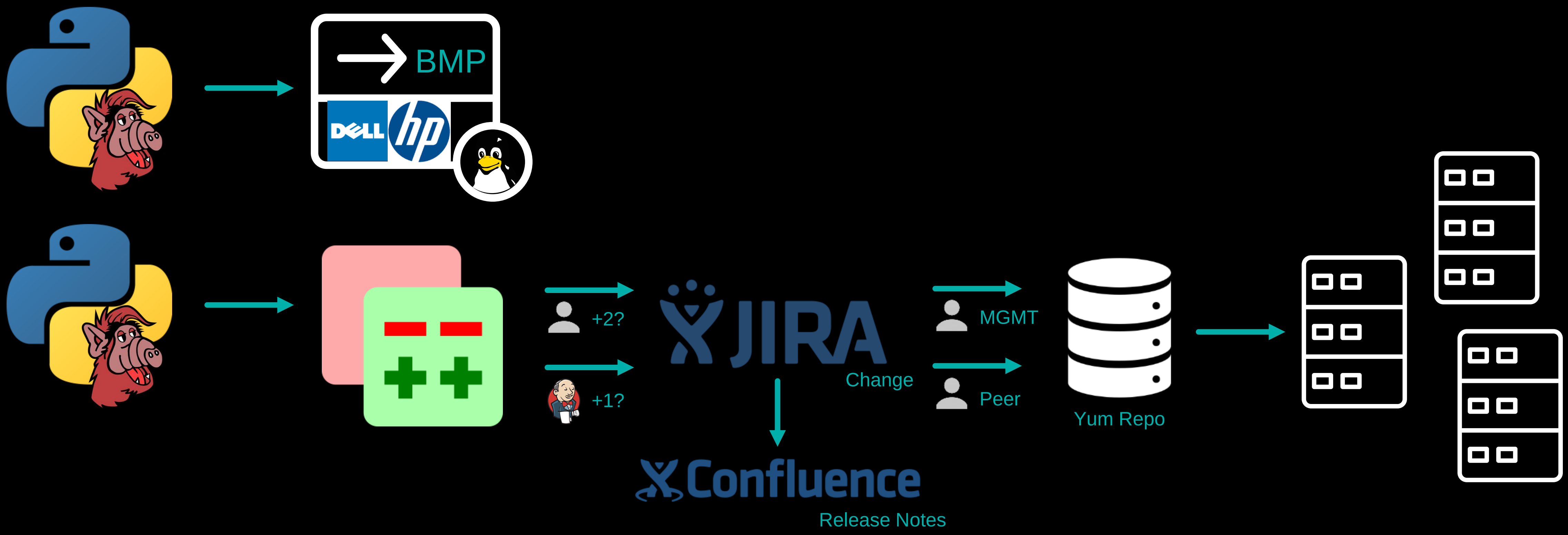
The separation of code and configuration

- Modularizing deployment
  - Code (the Alf app)
  - Configuration (Splunk TA, Splunk universal forwarder, additional files)
- Code
  - Stand-alone app
  - Install as python package
  - Future: separate from system python (platform-independent)
- Configuration
  - How does python package get installed?
  - How does data from Alf get processed/flow into Splunk?
  - Chef cookbooks + TA-Alf

20,000+
Baremetal
Servers

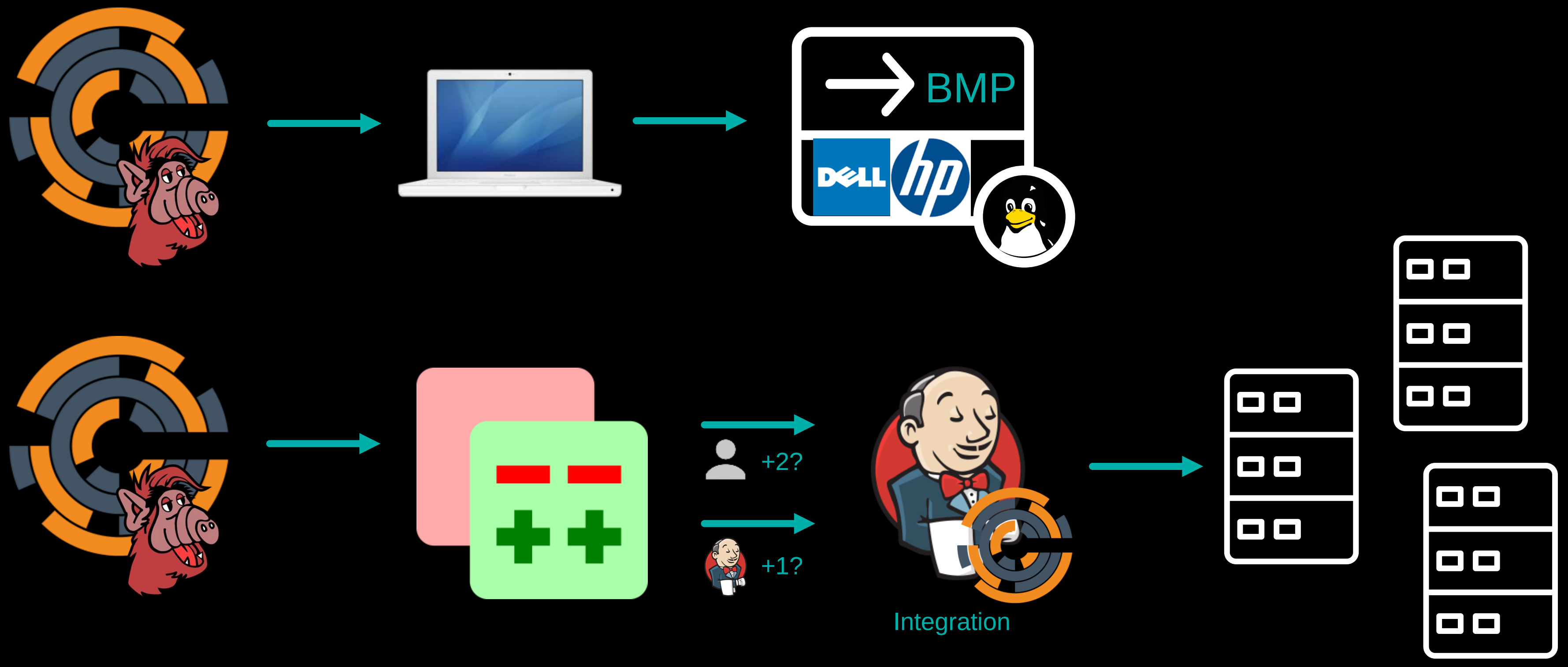
Code Pipeline

Getting Alf where it needs to go



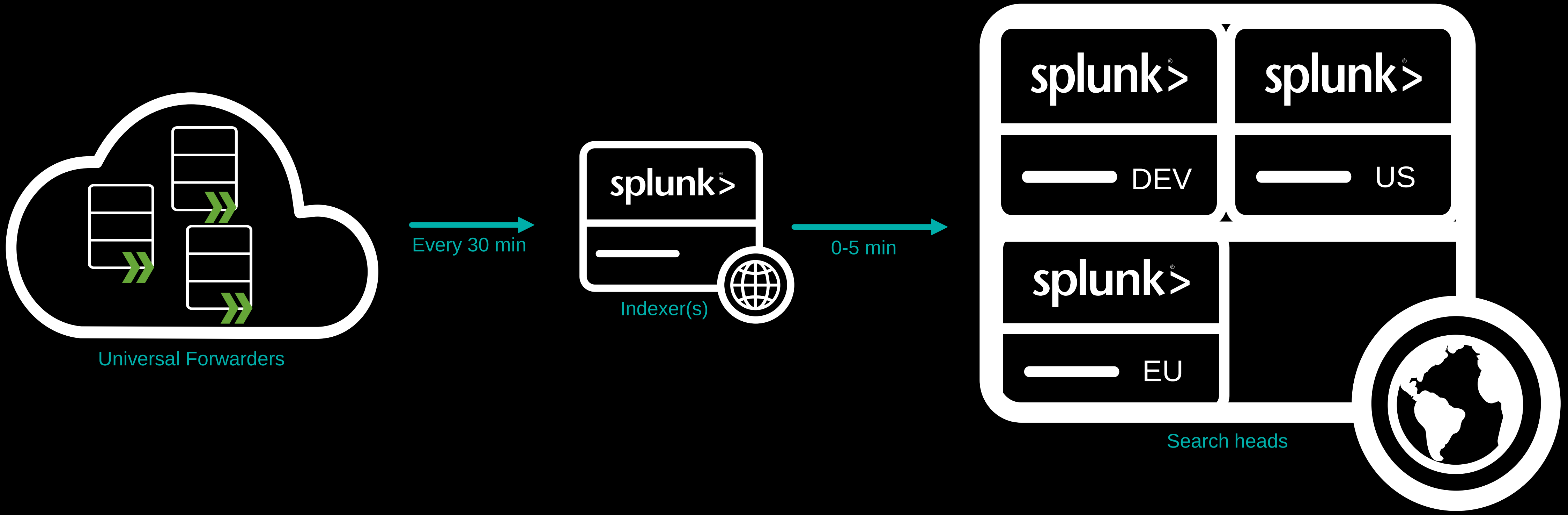
Configuration Pipeline

Making Alf feel at home



To Splunk

(And Beyond!)



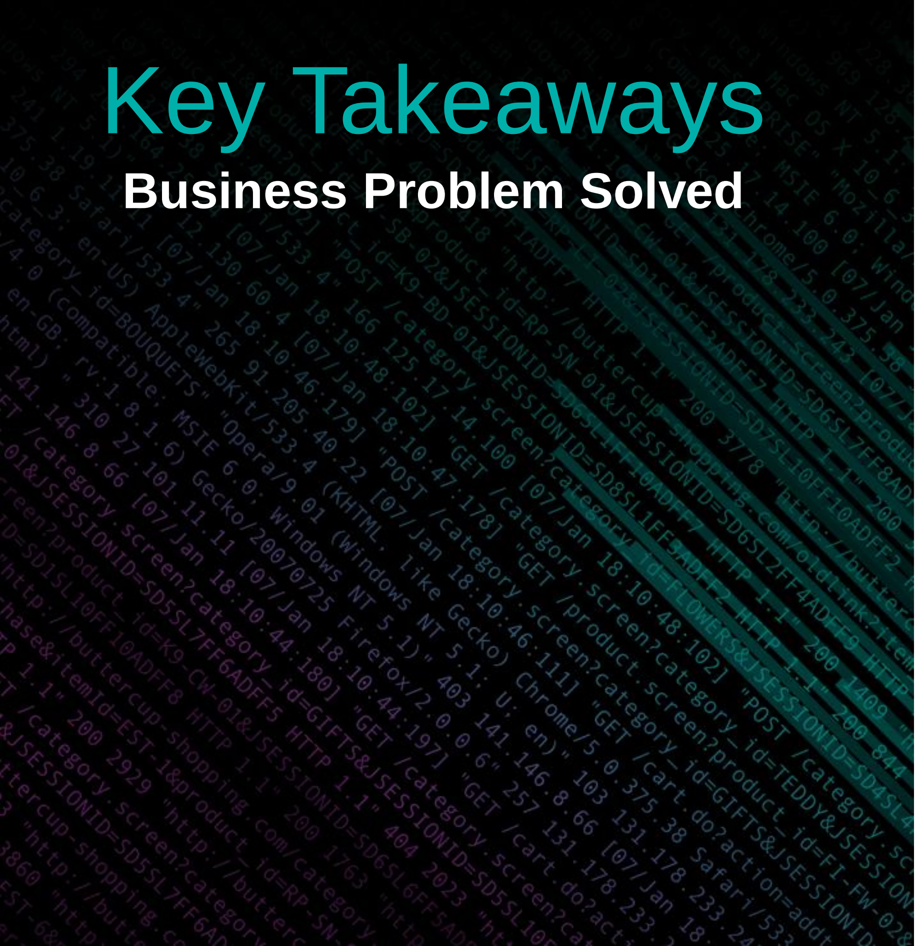
Universal Forwarders

Every 30 min

Indexer(s)

0-5 min

Search heads



Key Takeaways

Business Problem Solved

1. Expanded the business value of Splunk outside of our security organization
2. Made a simple design highly scalable
3. Delivered a complete solution in under 90 days
4. Saved money by reducing false positives and increasing customer uptime

Thank You

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

.conf18

splunk>

Q&A

Jordan Perks | Security Manager

James Barnes | DevOps Engineer

Soham Roy | DevOps Engineer