



Using Splunk to Increase Developer Confidence in the Pivotal Cloud Foundry Platform

Shubham Jain & Kirk Hanson

May 2018 | Version 1.0

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.

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. © 2018 Splunk Inc. All rights reserved.

Agenda

- ▶ Pivotal Cloud Foundry Introduction
- ▶ Pivotal Cloud Foundry Nozzle Overview and Architecture
- ▶ Pivotal Cloud Foundry health App Introduction and Overview
- ▶ Using Pivotal to make developers happier

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-01"

Splunk & Pivotal

Introduction

Overview

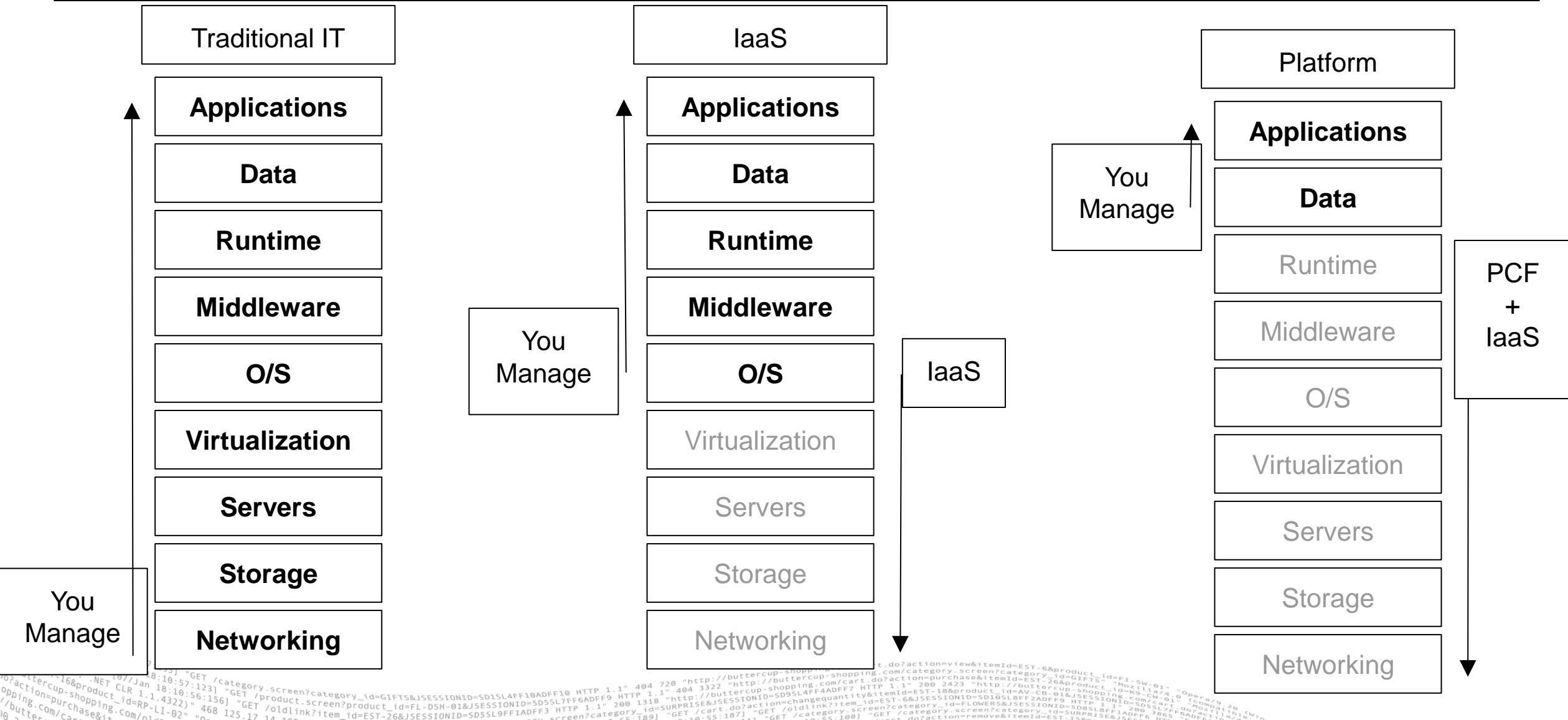
Cloud Foundry

- ▶ Open Source, multi cloud application Platform as a Service (PaaS) governed by the Cloud Foundry Foundation
- ▶ Promoted as Continuous delivery platform for full application lifecycle management
- ▶ Platform deploying and operating wide variety applications written in different languages (Java, .NET, Node.js, Python, Go etc) which can be deployed on premise or in public cloud



CLOUD **FOUNDRY**

The Power of the PCF Platform



Splunk Firehose Nozzle for PCF

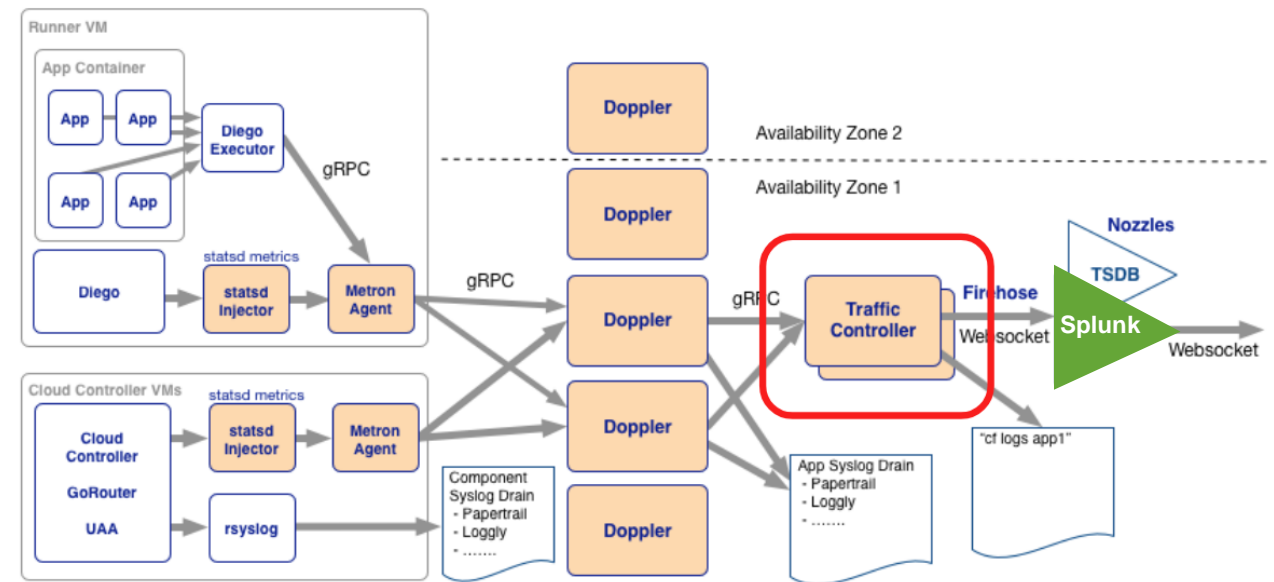
Architecture & Overview

Nozzle Overview

What is a Nozzle?

- ▶ A component dedicated to reading and processing data that streams from the Firehose Loggregator.
- ▶ Can be deployed as a managed service or an application.

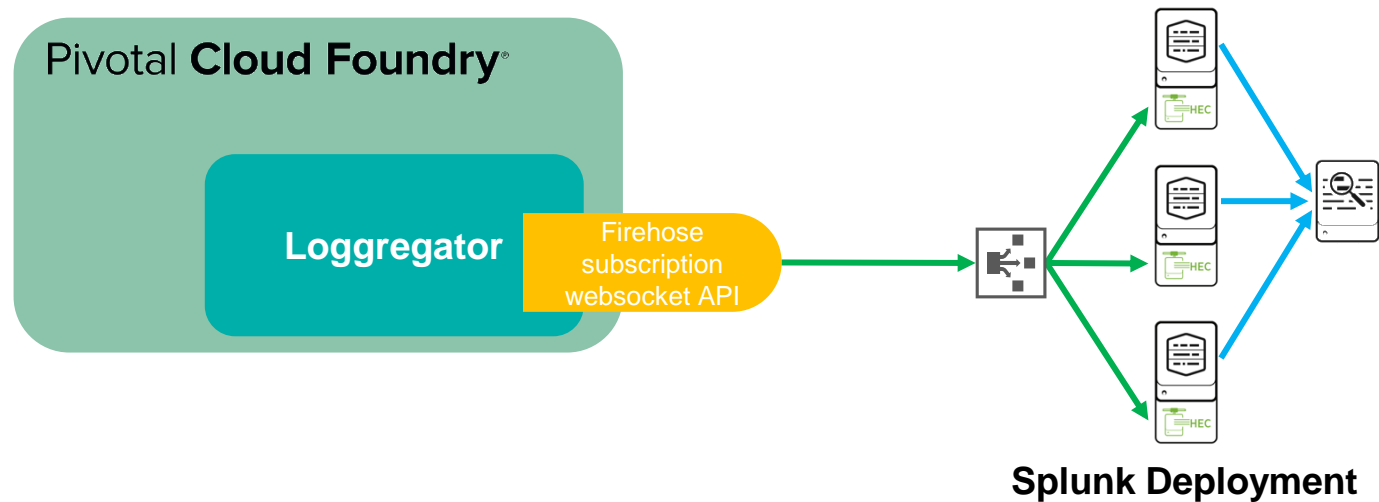
PCF Loggregator Architecture



Pivotal Cloud Foundry Integration

The Splunk Firehose Nozzle for PCF collects events from the PCF **Loggregator** endpoint and streams them to Splunk via HTTP Event Collector

- ▶ **High performance and reliability** with Nozzle's in-memory queue buffers, and parallel clients to scale out multiple ingestion channels to HEC
- ▶ **Simple deployment** natively within a PCF environment using a tile, or through CLI
- ▶ **Easy scalability** of ingest by adding more HEC data collection nodes behind a load balancer



Splunk Deployment

Splunk Firehose Nozzle for PCF Features

OOTB

Setup with out-of-the-box data parsing and enrichment for various PCF event types

HEC

Reliable event delivery by leveraging Splunk's HTTP Event Collector endpoint

SSL

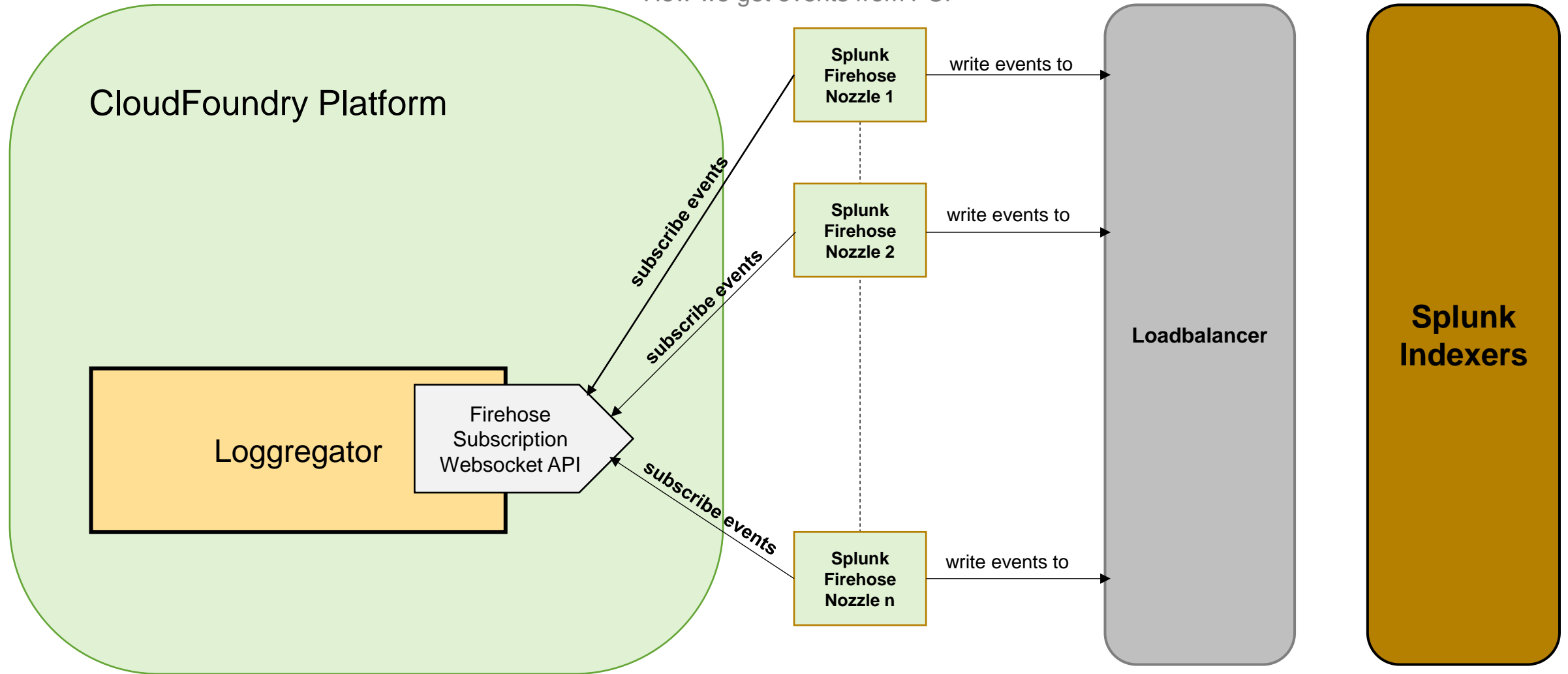
Secure forwarding from PCF into external Splunk environments using user-provided SSL certificates

Scales

Scales out to meet
increasing data
volume and number
of apps

PCF Nozzle Deployment Architecture

How we get events from PCF



[illegible]

How to install and deploy Splunk Firehose Nozzle in PCF via Tile?

- Download and install the Splunk tile from [Pivotal Network](#)
- Navigate to the Ops Manager Installation Dashboard and click **Import a Product** to upload the product file and add it to your staging area
- Configure the Tile as per requirements
- Apply changes to deploy the nozzle

Deployment Through Tile

The screenshot displays the PCF Ops Manager interface. The top navigation bar includes the PCF logo, the text "PCF Ops Manager", and a user profile dropdown labeled "admin".

The main content area is titled "Installation Dashboard". On the left, there is a sidebar with a blue button labeled "Import a Product" and a section titled "Generated Test Tile" showing a version of "0.0.83" with a trash icon and a plus sign.

The central area contains a grid of product tiles, each with a logo, name, and version:

- Google Cloud Platform (v1.11.5.0)
- Pivotal Elastic Runtime (v1.11.3)
- Spring Cloud Services (v1.4.1)
- RabbitMQ (v1.7.14)
- Redis (v1.9.0)
- Log Search (v1.0.11)
- Splunk Firehose Nozzle for PCF (v1.0.0)
- JMX Bridge (v1.9.1)
- MySQL for PCF (v1.8.10)

On the right side of the dashboard, there is a "No updates" status and a large blue button labeled "Apply changes", with a "Changelog" link below it.

At the bottom left of the sidebar, there is a link to "Download PCF compatible products at Pivotal Network" and a button labeled "Delete All Unused Products".

The footer of the interface contains the text "PCF Ops Manager v1.11.5.0; ©2013-2017 Pivotal Software, Inc; All Rights Reserved." on the left and "API Docs | End User License Agreement" on the right.

Splunk HTTP Event Collector Settings

Configure your Splunk HTTP Event Collector. See <http://docs.splunk.com/Documentation/Splunk/latest/Data/UsetheHTTPEventCollector>

Cloud Foundry Configuration

P

PCF Ops Manager

admin ▾

Installation Dashboard

Splunk Firehose Nozzle for PCF

SettingsStatusCredentialsLogs

Assign AZs and Networks

Splunk Settings

Cloud Foundry Settings

Advanced

Errands

Resource Config

Stemcell

Cloud Foundry Connection Settings

API Endpoint *

Cloud Foundry API endpoint.

API User *

API username

API Password *

Password for API user

Change

☒ Skip SSL Validation

Skip SSL certificate validation for connection to Cloud Foundry. Secure communications will not check SSL certificates against a trusted Certificate Authority. Skipping SSL validation in production environment is not recommended.

Event Types *

☒ HttpStartStop

☒ LogMessage

☒ ValueMetric

☒ CounterEvent

☒ Error

☒ ContainerMetric

Save

Advanced Configuration

PCF Ops Manager

Installation Dashboard

Splunk Firehose Nozzle for PCF

Settings Status Credentials Logs

Assign AZs and Networks

Splunk Settings

Cloud Foundry Settings

Advanced

Errands

Resource Config

Additional Nozzle Configuration

Scale Out Nozzle *

2

Firehose Subscription ID

Additional Fields

☐ Add App Information

☐ Enable Event Tracing

HEC Retries *

Configuration options:

- Scale Out Nozzle
- Firehose Subscription ID
- Additional Fields:
- Add App Information
- Enable Event Tracing
- HEC Retries
- HEC Batch Size
- HEC Workers
- Consumer Queue Size
- Flush Interval
- Missing App Cache Invalidate TTL
- App Cache Invalidate TTL
- App Limits
- Ignore Missing App



Splunk Pivotal Cloud Foundry Health App

Application design, overview and walkthrough


```
graph LR; subgraph CF_Platform [CloudFoundry Platform]; HW[Healthwatch]; LG[Loggregator]; FWSA{{Firehose Subscription Websocket API}}; HW --> LG; end; SFN1[Splunk Firehose Nozzle 1]; SFN2[Splunk Firehose Nozzle 2]; SFNn[Splunk Firehose Nozzle n]; LB[Loadbalancer]; SI[Splunk Indexers]; FWSA -- "subscribe events" --> SFN1; FWSA -- "subscribe events" --> SFN2; FWSA -- "subscribe events" --> SFNn; SFN1 -- "write events to" --> LB; SFN2 -- "write events to" --> LB; SFNn -- "write events to" --> LB; LB --> SI;
```

The diagram illustrates the architecture for sending logs from the CloudFoundry Platform to Splunk Indexers. On the left, the CloudFoundry Platform (green rounded rectangle) contains Healthwatch (orange rectangle) and Loggregator (orange rectangle). Healthwatch sends logs to Loggregator. A Firehose Subscription Websocket API (white chevron shape) is connected to Loggregator. This API subscribes to events from multiple Splunk Firehose Nozzles (Nozzle 1, Nozzle 2, and Nozzle n, all green rectangles). The nozzles write events to a central Loadbalancer (gray rounded rectangle), which then routes them to the Splunk Indexers (brown rounded rectangle).

Splunk Pivotal Cloud Foundry Health App - Walkthrough

Application design, overview and walkthrough

Getting Started

- ▶ Documentation
- ▶ Video Links
- ▶ Download Links
- ▶ Data Overview
 - Broken down by Event Type & Sourcetype

Getting Started

The Splunk PCF App was created and modeled after metrics that are collected from the PCF HealthWatch App as well as metrics that were generated by the PCF HealthWatch app. The PCF HealthWatch must be installed to receive all the metrics that it generates. In addition, the Splunk Nozzle must be installed and configured to be able to receive data into Splunk from PCF.

Below you can find a brief description of the visualizations included in this App:

The **PCF Executive View - Monitoring** is designed to give a high-level understanding of the app's health - born out of customer need to see the general health of PCF in Splunk.
 The **IT Operations Visibility** is designed around an IT ops focus - essentially one level deeper view into operations than the Executive View.
 The **PCF Ops Dropdown** is all the other visualizations you would expect to find in the PCF Healthwatch App
 The **PCF App Monitoring** is based on Application monitoring best practices

Reference Links

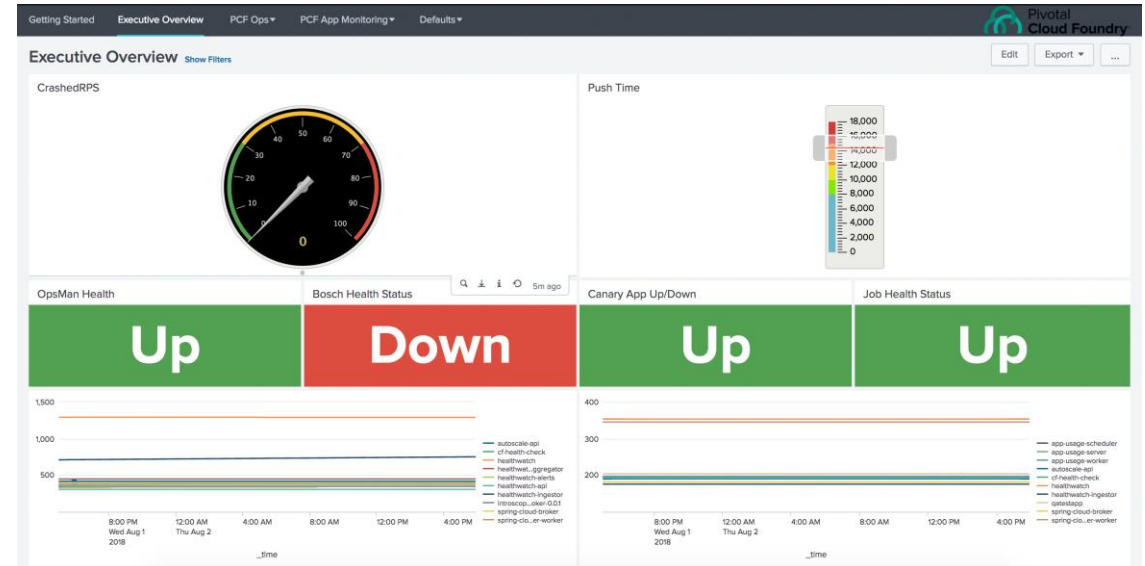
[Click Here](#) to download the PCF HealthWatch app for PCF
[Click Here](#) review the docs on using HealthWatch
[Click Here](#) review Overall PCF and Splunk Architecture
[Click Here](#) review the Splunk Blog for more information on how the Nozzle works as well as download links and instructions.
[Click Here](#) for a **video series** that details how to configure and install the Splunk PCF Nozzle, PCF Healthwatch, and the Pivotal Cloud Foundry Health Splunk app.

Data Overview

Event Type	Sourcetype Count	Status
ContainerMetric	2863	OK
CounterEvent	13646	OK
HttpStartStop	9966	OK
LogMessage	1322	OK
ValueMetric	141997	OK

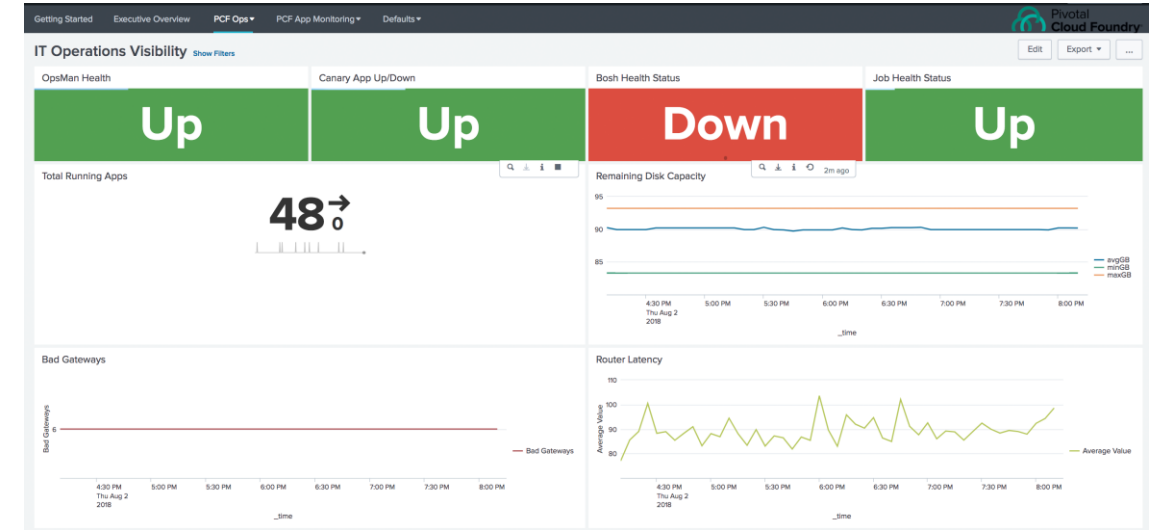
Executive Overview

- ▶ High-level metrics
- ▶ App level metrics for operators
- ▶ High-level metrics for App Developers



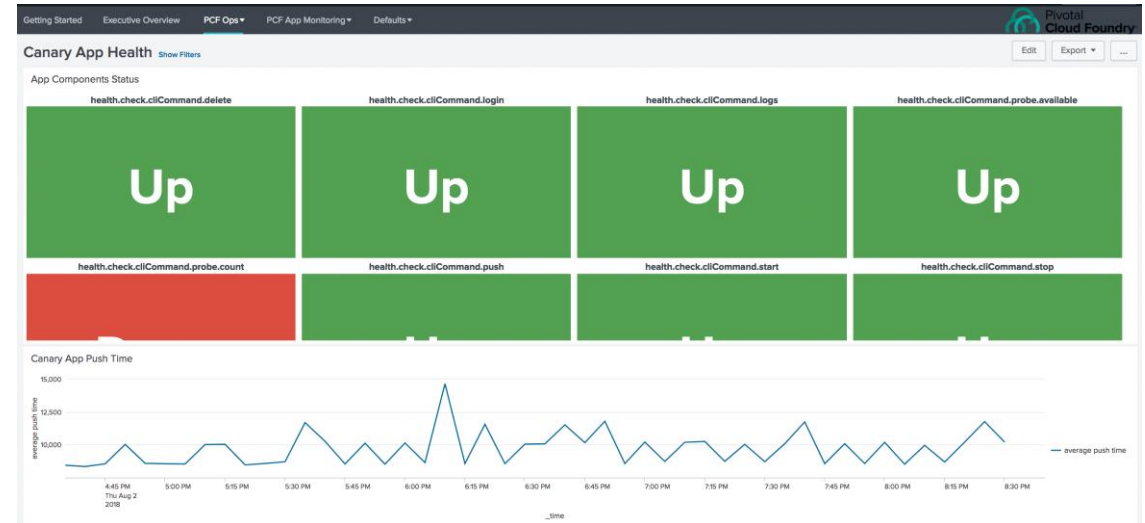
It Operations Visibility

- ▶ Same High-level metrics
- ▶ Designed to paint a picture for an Operations professional
- ▶ Consensus from customers of what matters from an IT Ops perspective



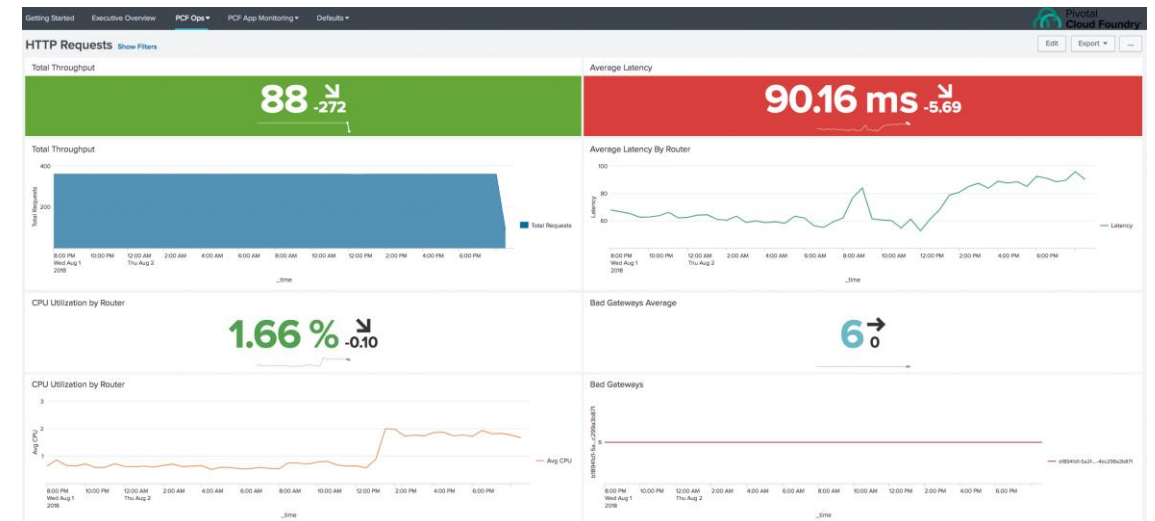
Canary App Health

- ▶ Canary Health App by component
 - Based on each component health rather than the high-level single metric
 - Detailed drill down on each metric
- ▶ Canary Push Time – average over time



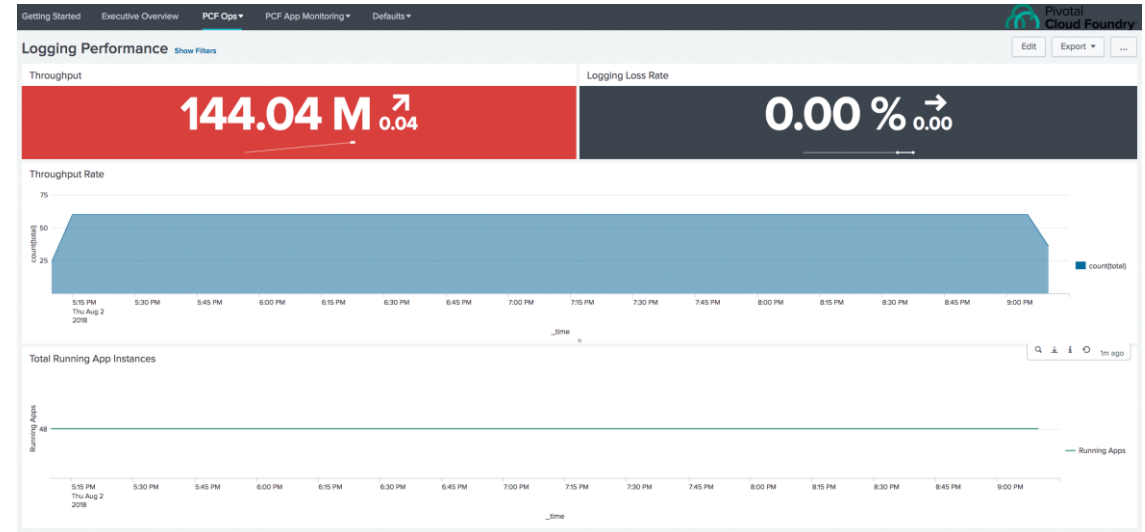
HTTP Requests

- ▶ Insights into the overall traffic flow over entire deployment
- ▶ Do you need to continue to scale the router?
- ▶ What trends are evident?
- ▶ Gorouters scale either horizontally or vertically



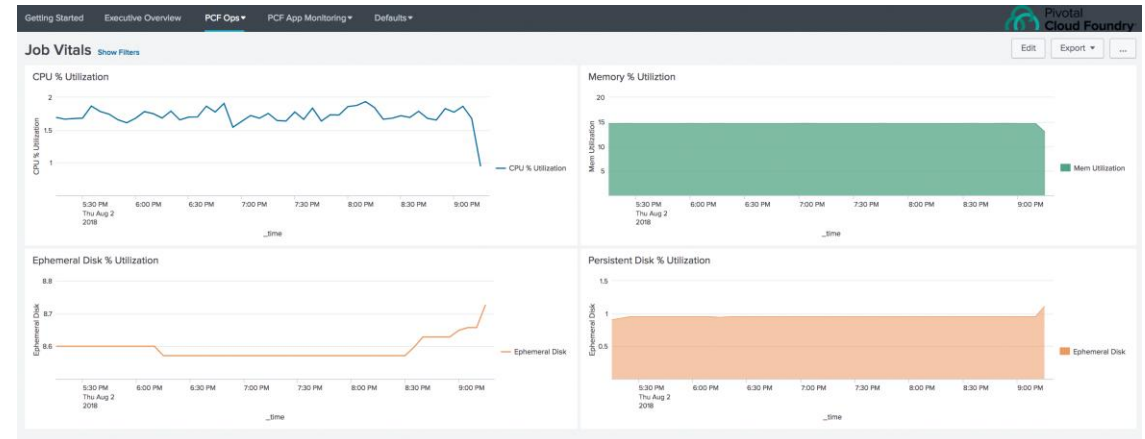
Logging Performance

- ▶ Overall Performance of Logging
- ▶ Enables you to understand the trends of your logging for example:
- ▶ Example:
 - Dropped messages can indicate that Dopplers are not processing messages fast enough and that Doppler instances need to be scaled



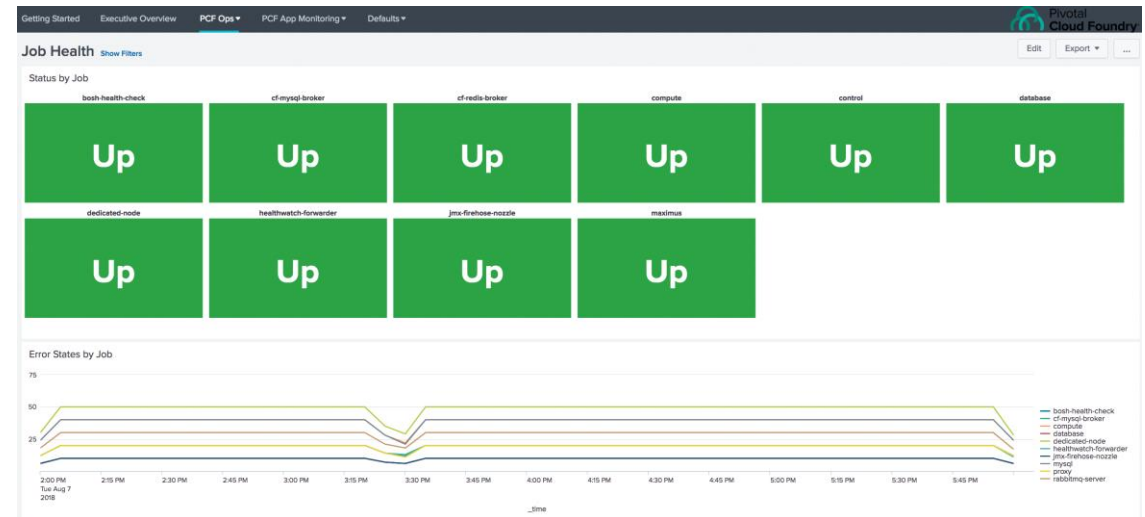
Job Vitals

- ▶ Metrics across foundation and with foundation drilldown
- ▶ High Level metrics
 - CPU, Disk Utilization, memory
- ▶ More metrics around Operational Health



Job Health

- ▶ Job Health provides you with an understanding of job health – up or down
- ▶ In addition you can find Error states by job over time and...
- ▶ Error states by deployment



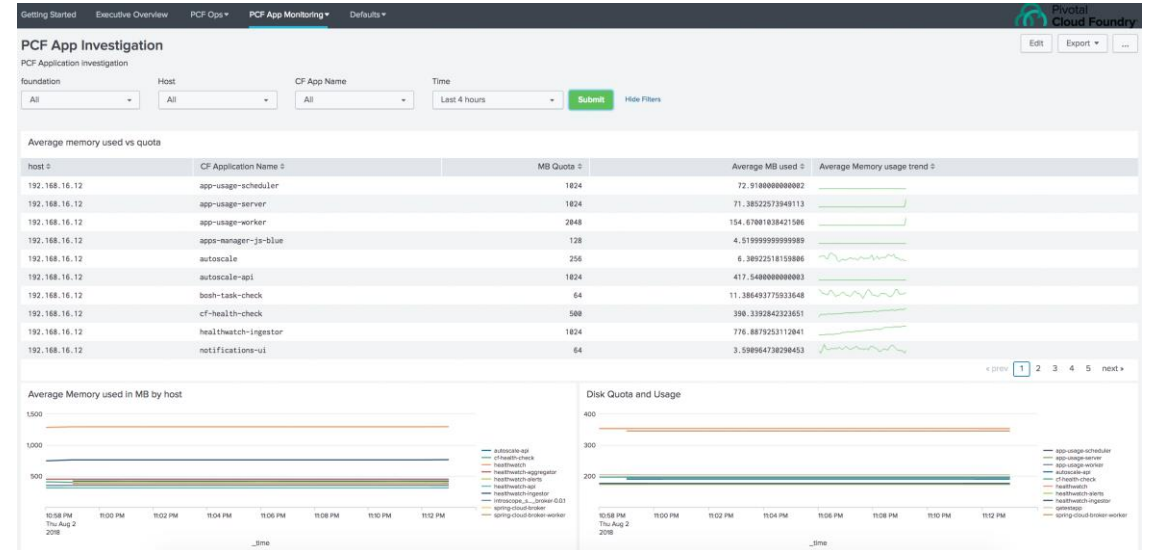
PCF App Investigation

- ▶ Interactive Dashboard designed to allow you to filter down by:

- CF App Name
- Host
- Foundation

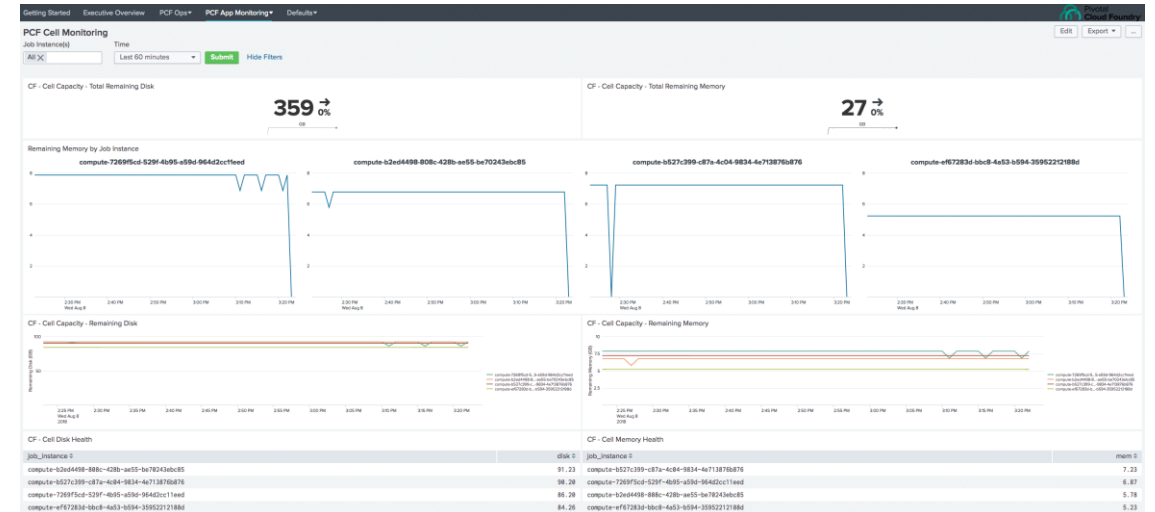
- ▶ Then provides app level metrics such as:

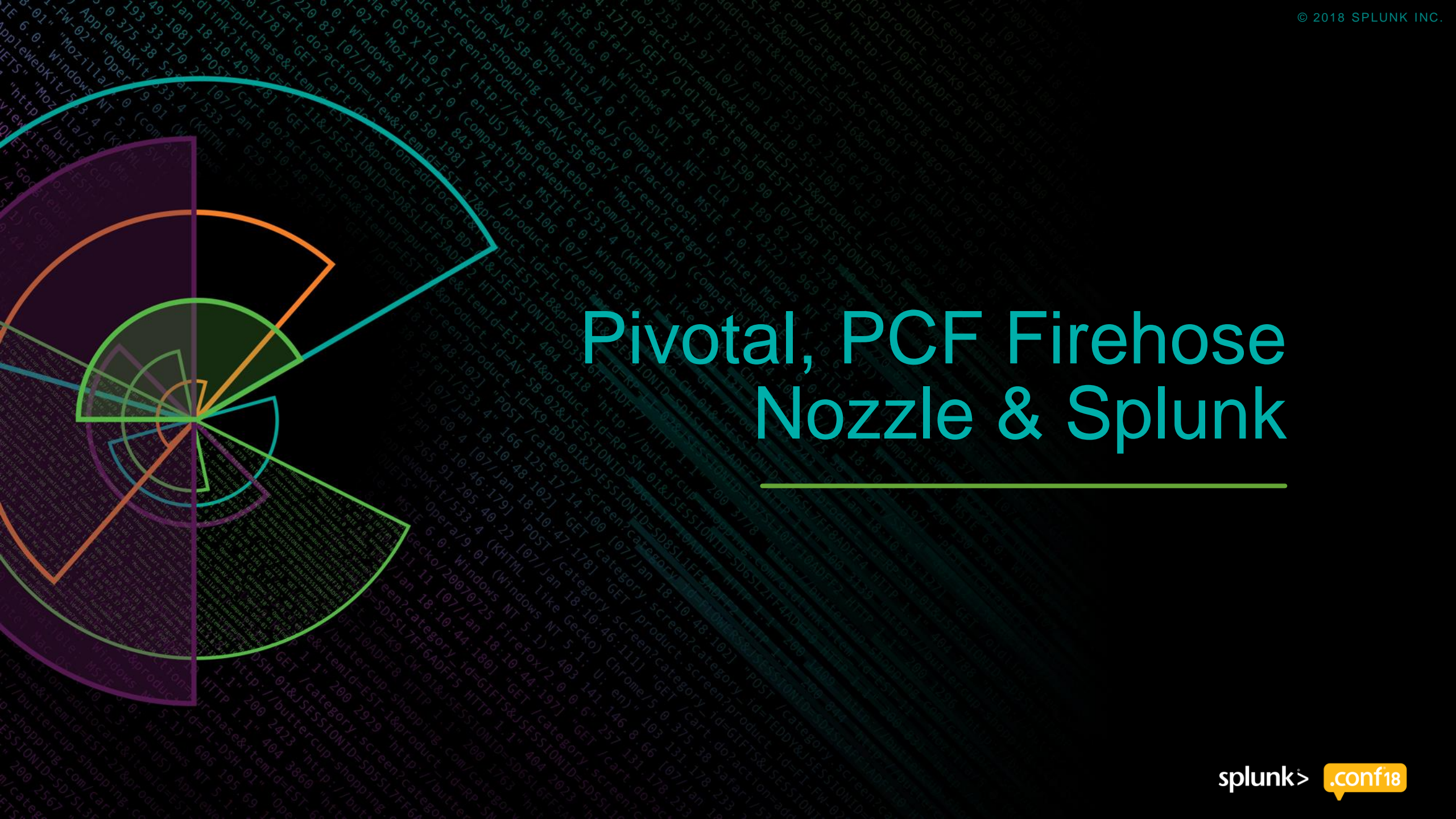
- Avg memory usage
- Disk against Quota usage
- Average Memory used by host



PCF Cell Monitoring

- ▶ CF Cell capacity
 - Total Remaining Disk
 - Total Remaining Memory
- ▶ Memory utilization by Job Instance with Job drilldowns
- ▶ Memory and disk utilization breakdowns by:
 - Disk
 - Memory





Pivotal, PCF Firehose Nozzle & Splunk

BP (Before PCF)

- ▶ Development time too long
 - Development time too high
- ▶ MTTR too high
- ▶ Two silo-ed development environments
- ▶ No way to have any insight past last 5 minutes



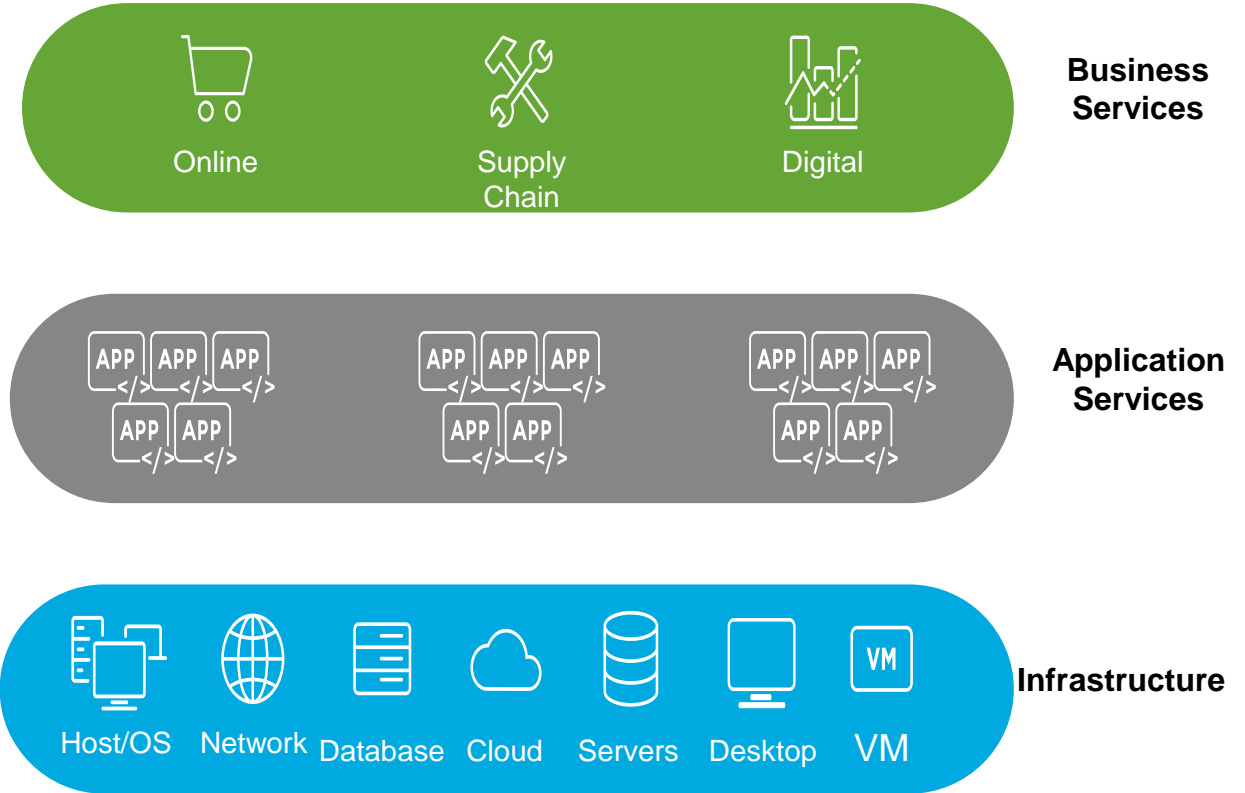
Splunk + PCF

- ▶ Splunk used for all Monitoring
- ▶ Splunk is the logical choice
- ▶ Will use to help achieve 4x9's
- ▶ PCF is the future platform for development
- ▶ App will play a critical role in that

Pivotal **Cloud Foundry**[®]

PCF + Splunk

- ▶ The main goal is a bottom up supportable process
- ▶ Not only inclusive of Infrastructure but App & Business Services
- ▶ A single source of truth both for development experience but operations as well
- ▶ A true dev-ops monitoring platform



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&SESSIONID=SD5SL7FF6ADFF9"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&SESSIONID=SD5SL7FF6ADFF9"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&SESSIONID=SD5SL7FF6ADFF9"

```

Future Plans

Where do we go from here?

ITSI integration

Service-Centric views
Notable Events

MLTK Integration

Forecast future needs for
the PCF platform

Predictive Analytics

Prevent downtime by
using predictive analytics

Thank You

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

.conf18

splunk>