Pivotal

Cloud Native Operations
With PKS (Kubernetes)

Paul Czarkowski

@pczarkowski
pczarkowski@pivotal.io

© Copyright 2018 Pivotal Software, Inc. All rights Reserved.

Pivotal

Cloud Native Operations
With PKS (Kubernetes)

Paul Czarkowski

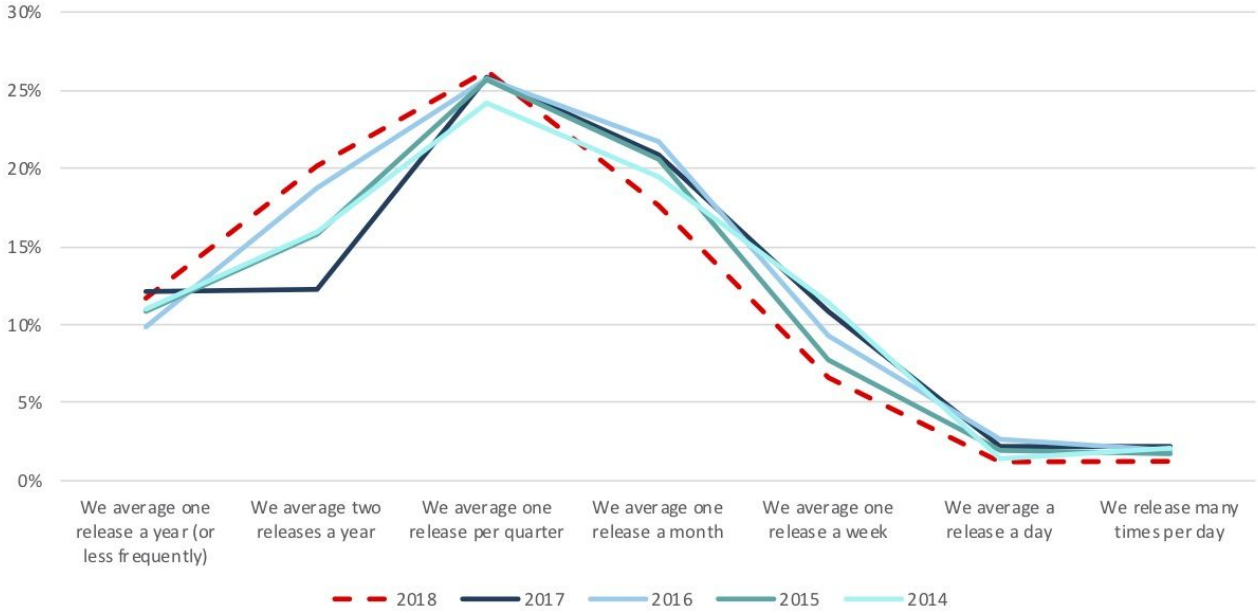
@pczarkowski
pczarkowski@pivotal.io

© Copyright 2018 Pivotal Software, Inc. All rights Reserved.

Operations is the Secret sauce

Operations as a Competitive Advantage

Just not Traditional Operations.

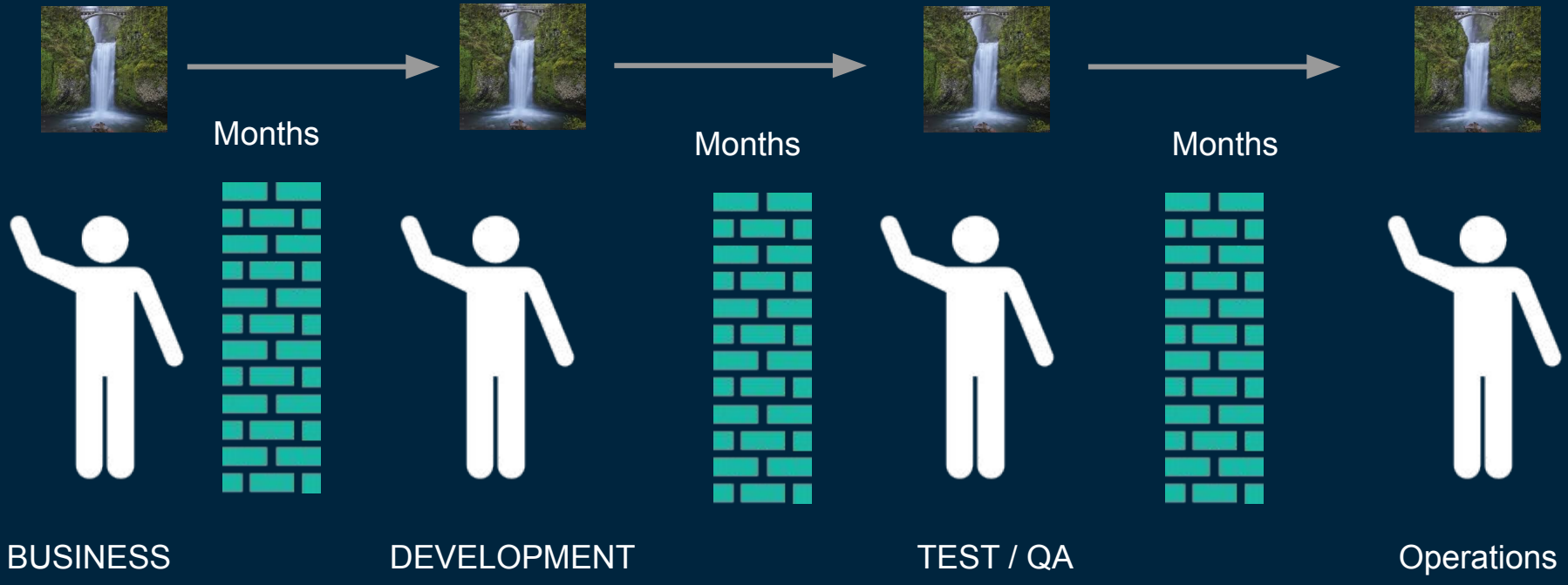


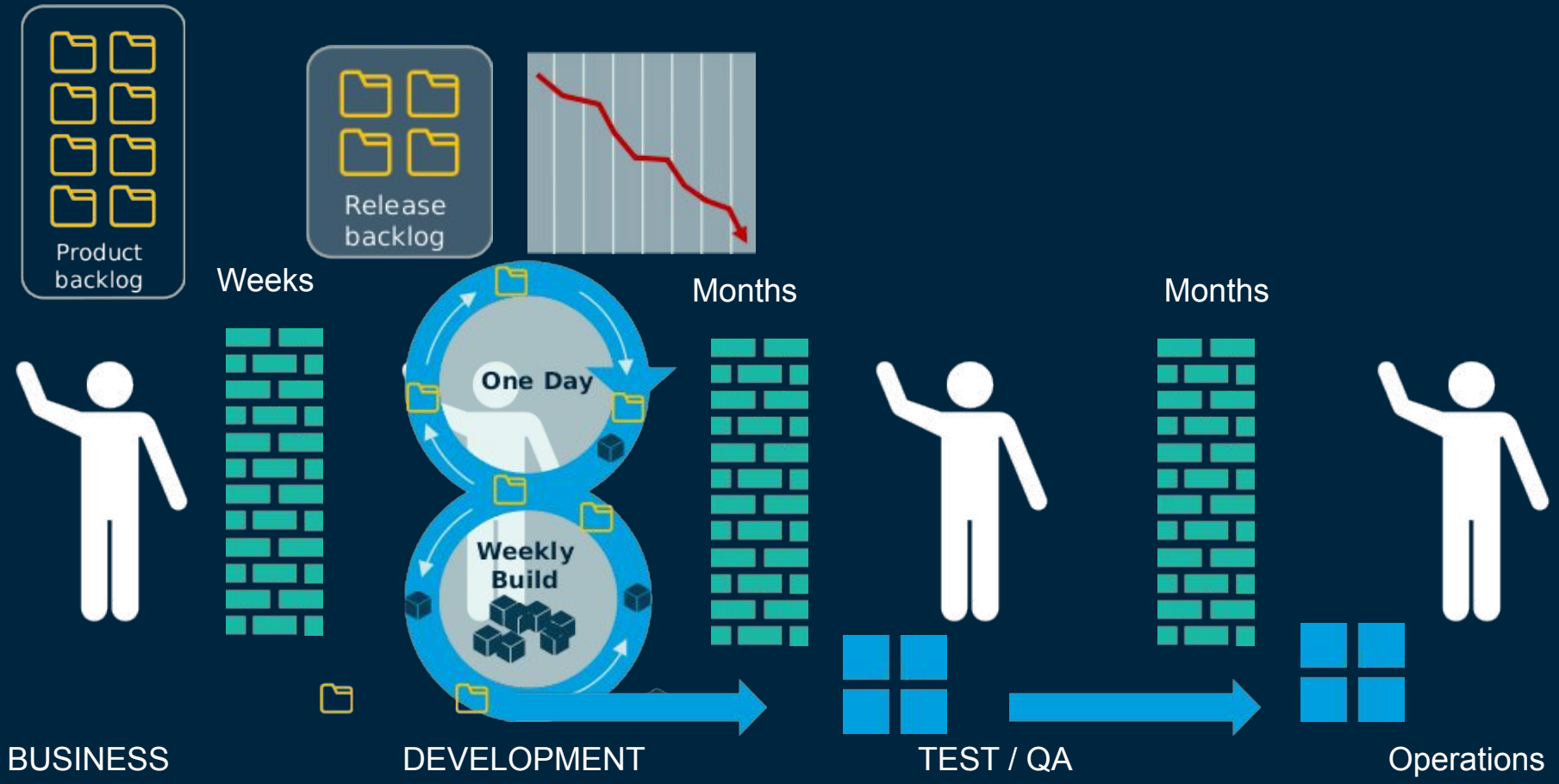
Base (2018): 3,228 Developers
Base: 546-719 Developers who work for a software company, for internal IT, or in technology services
Source: Forrester Business Technographics Developer Survey, 2014-2018.

https://go.forrester.com/blogs/ceos-and-software/

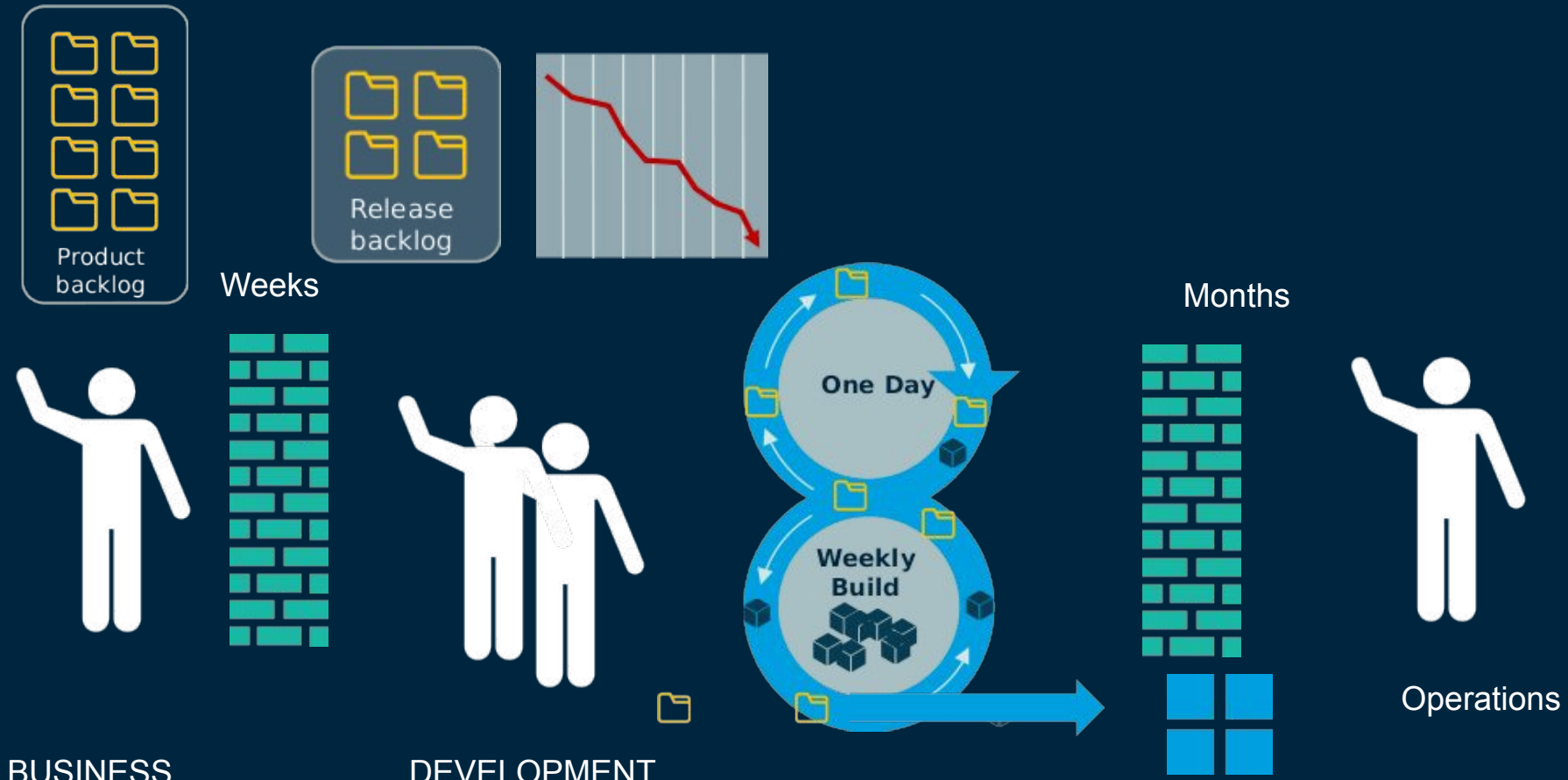
The Agile/DevOps Journey

Pivotal

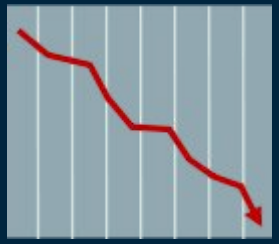

Months
Months
Months
BUSINESS
DEVELOPMENT
TEST / QA
Operations


Product backlog
Release backlog
Weeks
Months
Months
One Day
Weekly Build
BUSINESS
DEVELOPMENT
TEST / QA
Operations

Pivotal

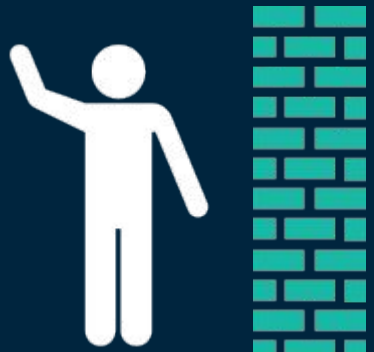

Product backlog
Release backlog
Weeks
Months
One Day
Weekly Build
BUSINESS
DEVELOPMENT
TEST / QA
Operations

Pivotal



Weeks

Months



BUSINESS

DEVELOPMENT

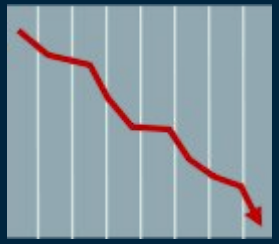
TEST / QA

Operations

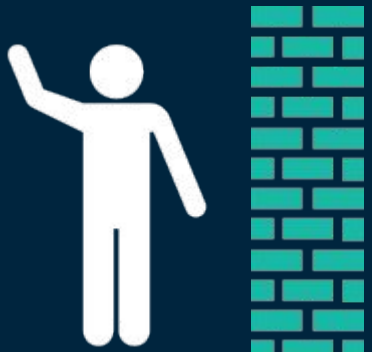
Pivotal

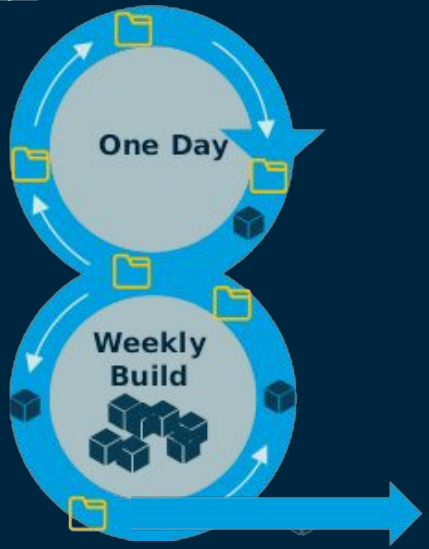
```
apiVersion: v1
kind: Service
metadata:
  name: mysql
spec:
  ports:
    - port: 3306
      protocol: TCP
  selector:
    app: mysql

apiVersion:
extensions/v1beta1
kind: ReplicaSet
metadata:
  name: mysql
  labels:
    app: mysql
spec:
  replicas: 1
  selector:
    matchLabels:
      app: mysql
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - name: database
        image: mysql:5.6
        resources:
          requests:
            cpu: 1
            memory: 1Gi
        livenessProbe:
          tcpSocket:
            port: 3306
        ports:
        - containerPort: 3306
        env:
          - name: MYSQL_ROOT_PASSWORD
            valueFrom:
              secretKeyRef:
                name: mysqlsecret
                key: database.password
          - name: MYSQL_USER
            valueFrom:
              secretKeyRef:
                name: mysqlsecret
                key: database.username
          - name: MYSQL_PASSWORD
            valueFrom:
              secretKeyRef:
                name: mysqlsecret
                key: database.password
          - name: MYSQL_DATABASE
            valueFrom:
              secretKeyRef:
                name: mysqlsecret
                key: database.name
        volumeMounts:
          -  name: database
             mountPath: /var/lib/mysql
      volumes:
        -  name: database
           persistentVolumeClaim:
             claimName: database

apiVersion: v1
kind: PersistentVolume
metadata:
  name: database
  labels:
    volume: mysqlvolume
spec:
  accessModes:
    - ReadWriteMany
  capacity:
    storage: 1Gi
  hostPath:
    path: /data/pv0002/
```

Source: Ben Wilcock's Musical Kubernetes Cluster.



Weeks





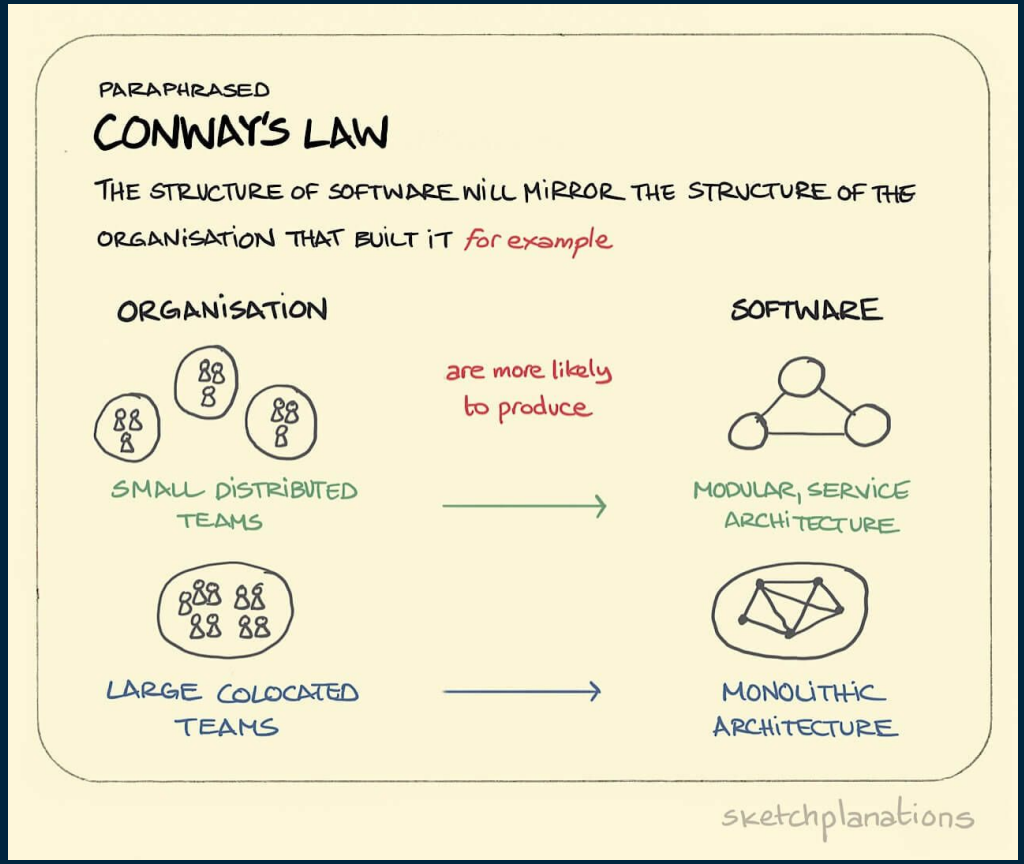
BUSINESS

DEVELOPMENT

TEST / QA

Operations

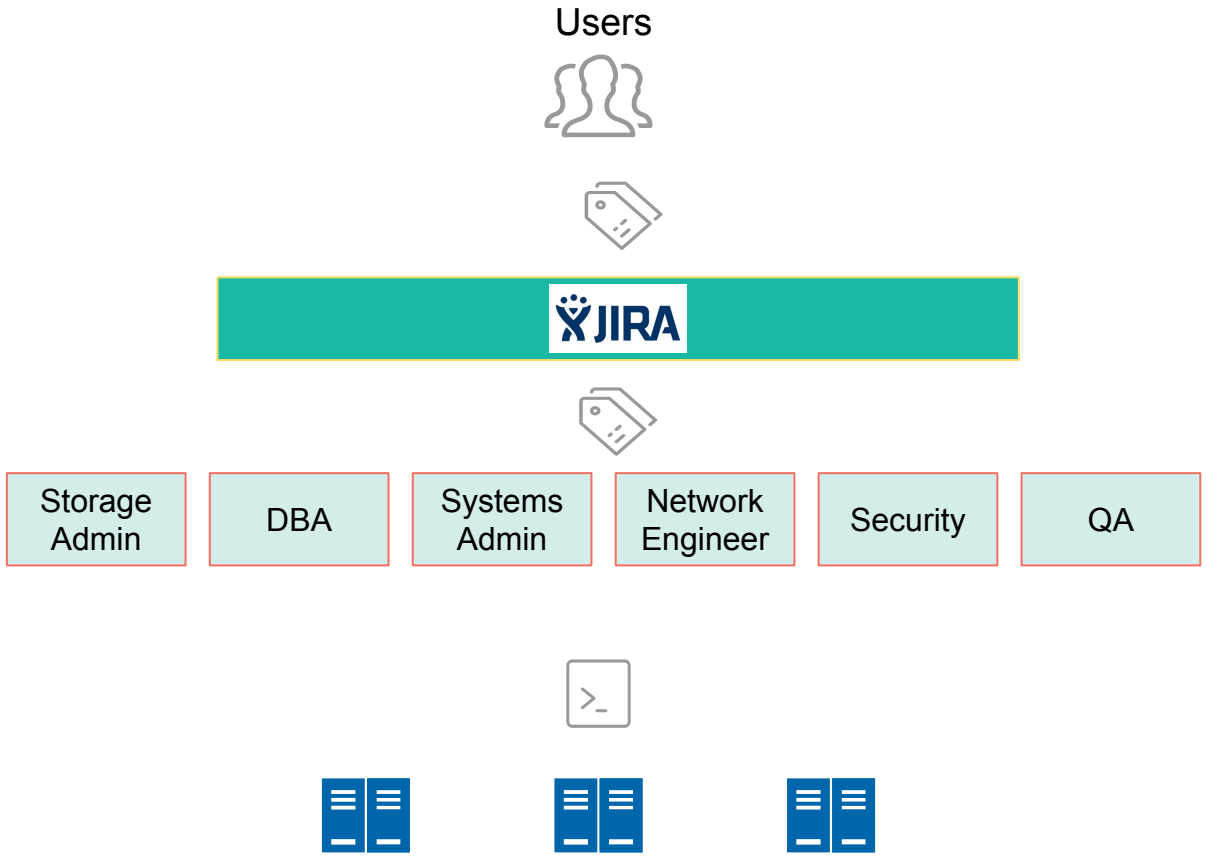
Pivotal



https://www.sketchplanations.com/post/175174474143/conways-law-im-paraphrasing-here-but-the-gist

Pivotal

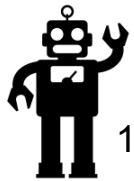
Pivotal


Users
JIRA
Storage Admin
DBA
Systems Admin
Network Engineer
Security
QA

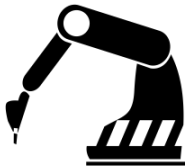
Users

API

Artifacts | Database | Storage | Compute | Network | Access



1



2

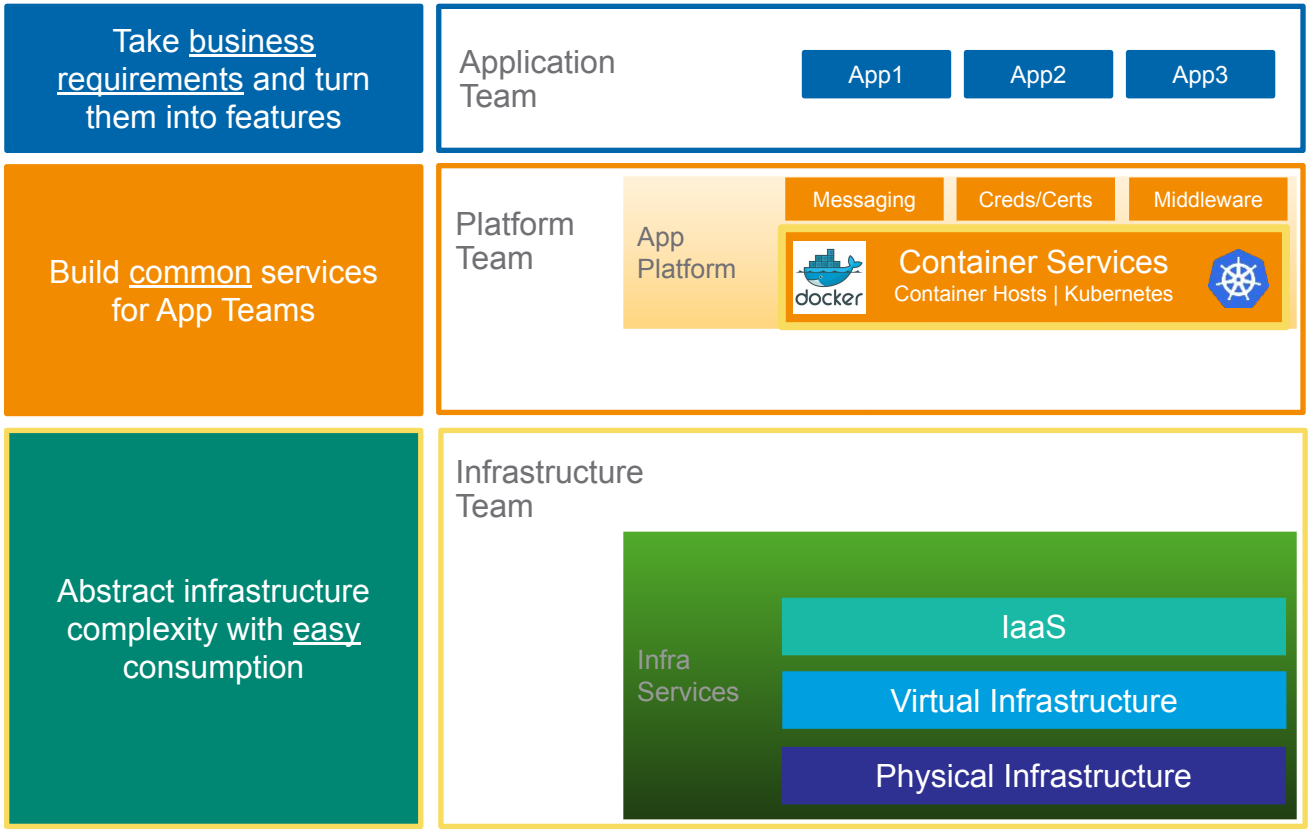
Pivotal

Creative Commons
[1] Jon Trillana
[2] Simon Child

Czarcloudski
@pczarkowski
Enterprise DevOps
JIRA
Security
Sys Eng
Network Eng
DBAs
Release Manager
11:16 AM - 11 Jun 2018
1,217 Retweets 2,307 Likes

Operations as a Platform

Platform as a Product


Take business requirements and turn them into features
Application Team
App1
App2
App3
Build common services for App Teams
Platform Team
App Platform
Messaging
Creds/Certs
Middleware
docker
Container Services
Container Hosts | Kubernetes
Abstract infrastructure complexity with easy consumption
Infrastructure Team
Infra Services
IaaS
Virtual Infrastructure
Physical Infrastructure

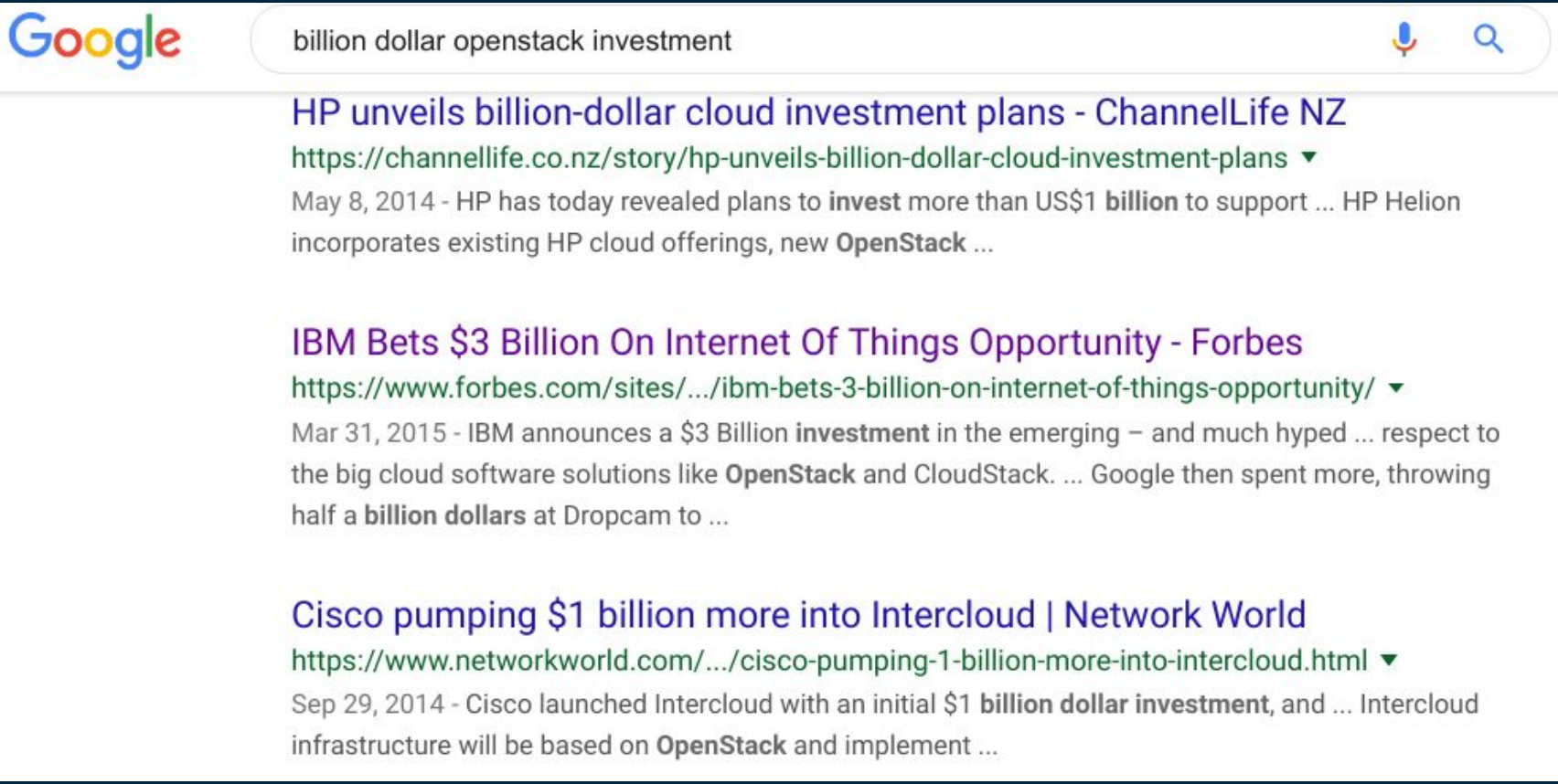
Orchestration
and scheduling

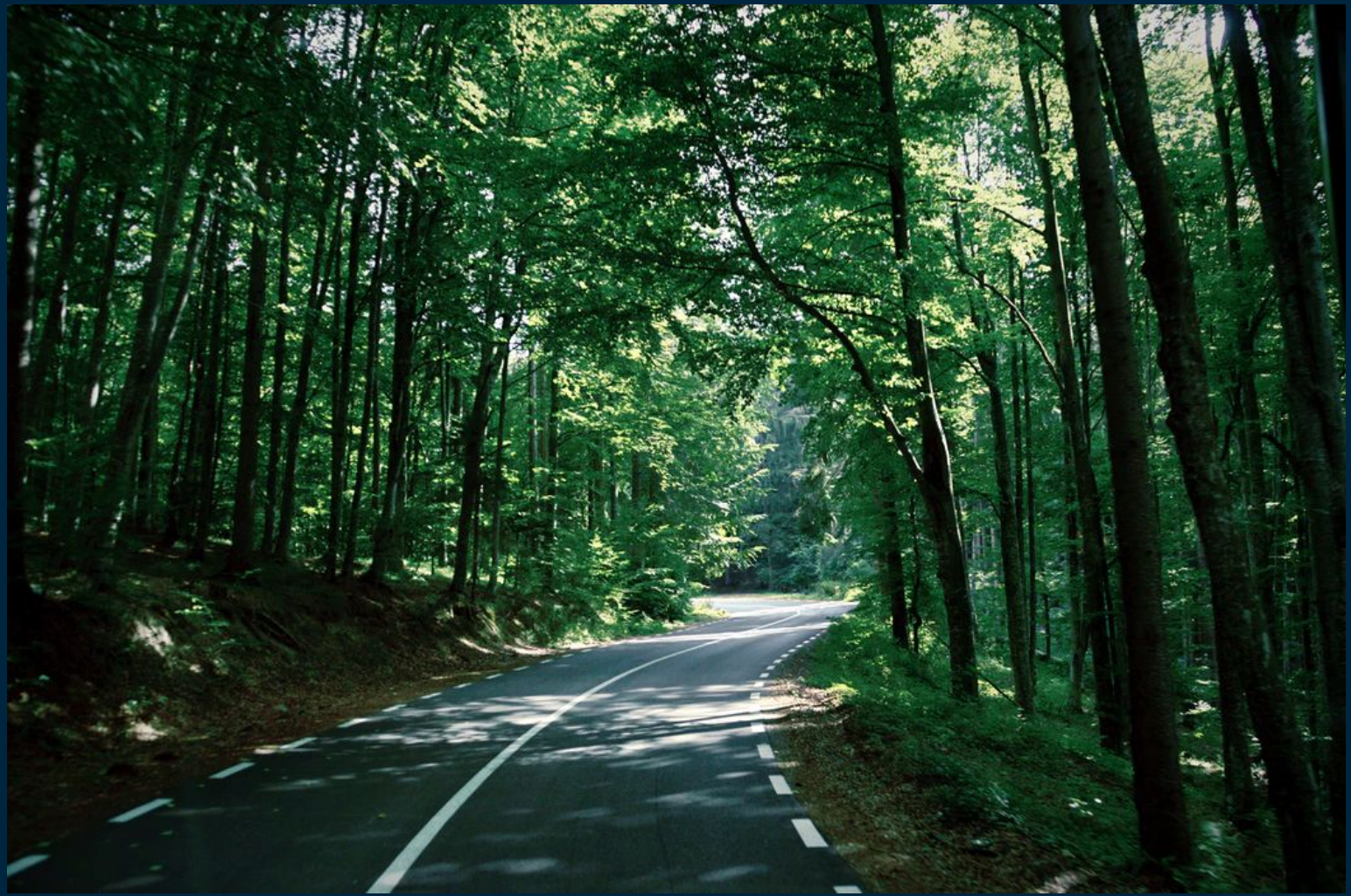
Observability

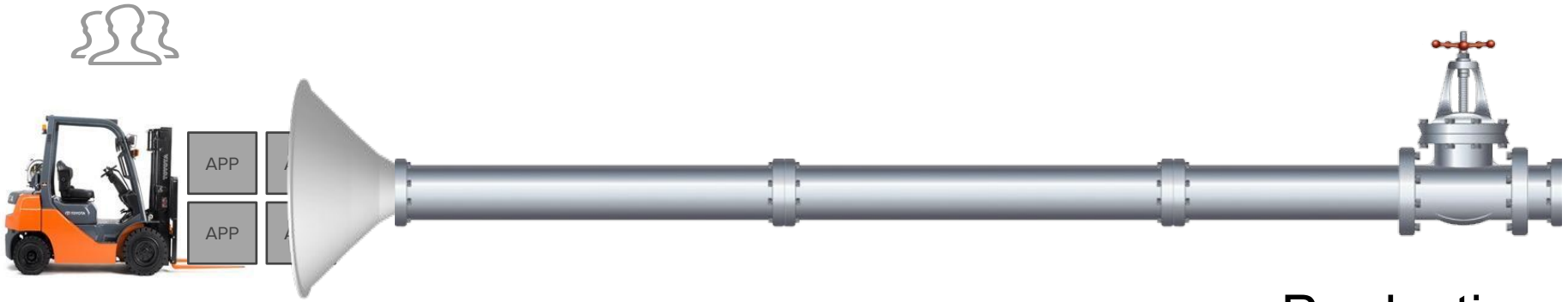
CI / CD

Access
Control

Pivotal


Google
billion dollar openstack investment
HP unveils billion-dollar cloud investment plans - ChannelLife NZ
https://channellife.co.nz/story/hp-unveils-billion-dollar-cloud-investment-plans
May 8, 2014 - HP has today revealed plans to invest more than US$1 billion to support ... HP Helion incorporates existing HP cloud offerings, new OpenStack ...
IBM Bets $3 Billion On Internet Of Things Opportunity - Forbes
https://www.forbes.com/sites/.../ibm-bets-3-billion-on-internet-of-things-opportunity/
Mar 31, 2015 - IBM announces a $3 Billion investment in the emerging – and much hyped ... respect to the big cloud software solutions like OpenStack and CloudStack. ... Google then spent more, throwing half a billion dollars at Dropcam to ...
Cisco pumping $1 billion more into Intercloud | Network World
https://www.networkworld.com/.../cisco-pumping-1-billion-more-into-intercloud.html
Sep 29, 2014 - Cisco launched Intercloud with an initial $1 billion dollar investment, and ... Intercloud infrastructure will be based on OpenStack and implement ...

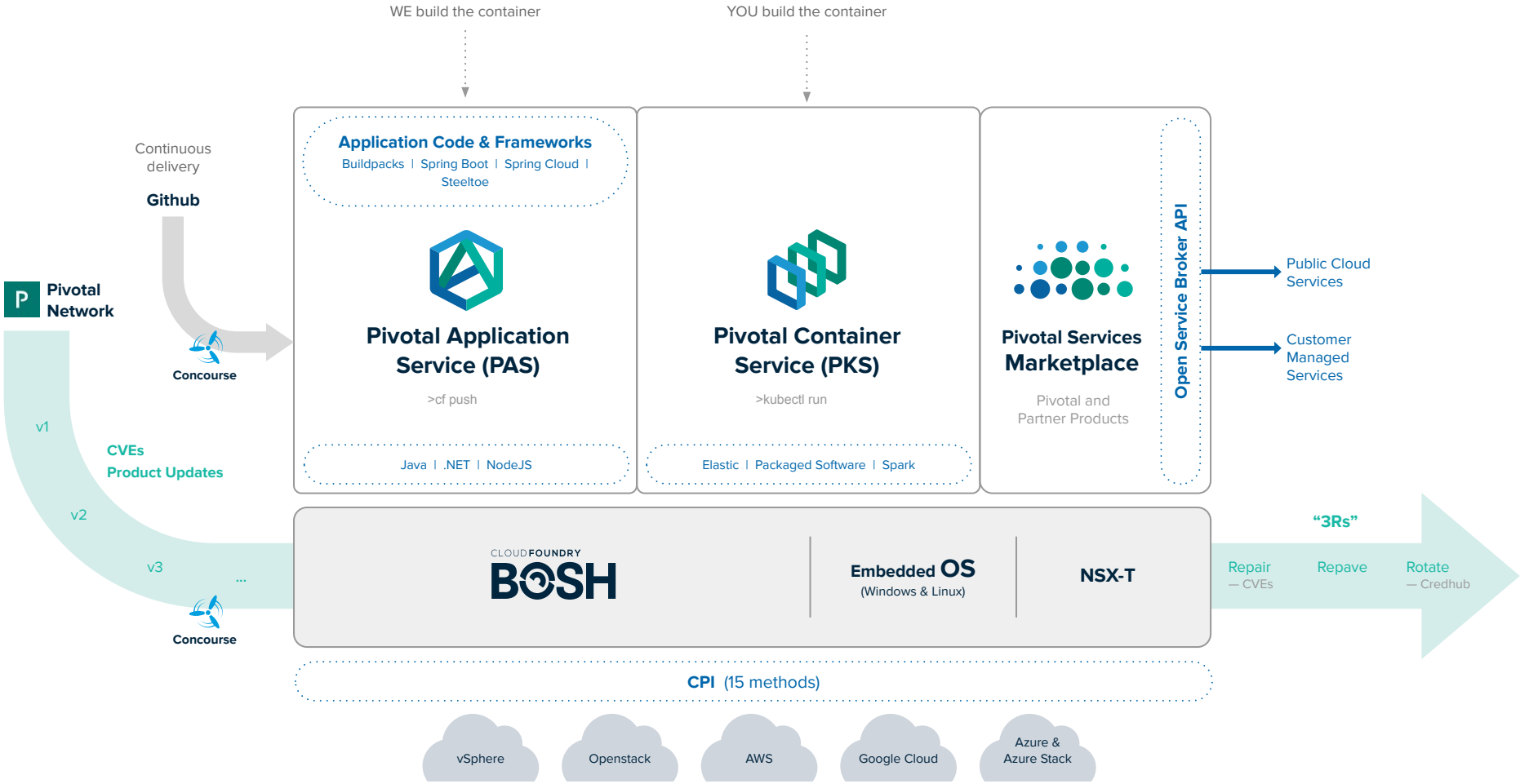




Production

This is Cloud Native Operations

Pivotal is a Platform Company


WE build the container
YOU build the container
Continuous delivery
Github
Application Code & Frameworks
Buildpacks | Spring Boot | Spring Cloud | Steeltoe
Pivotal Network
Pivotal Application Service (PAS)
>cf push
Pivotal Container Service (PKS)
>kubectl run
Pivotal Services Marketplace
Pivotal and Partner Products
Open Service Broker API
Public Cloud Services
Customer Managed Services
Concourse
v1
CVEs
Product Updates
v2
v3
...
Concourse
Java | .NET | NodeJS
Elastic | Packaged Software | Spark
CLOUDFOUNDRY BOSH
Embedded OS (Windows & Linux)
NSX-T
"3Rs"
Repair — CVEs
Repave
Rotate — Credhub
CPI (15 methods)
vSphere
Openstack
AWS
Google Cloud
Azure & Azure Stack

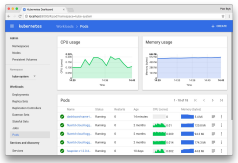
Pivotal

Kubernetes is a Runtime for Containerized Workloads

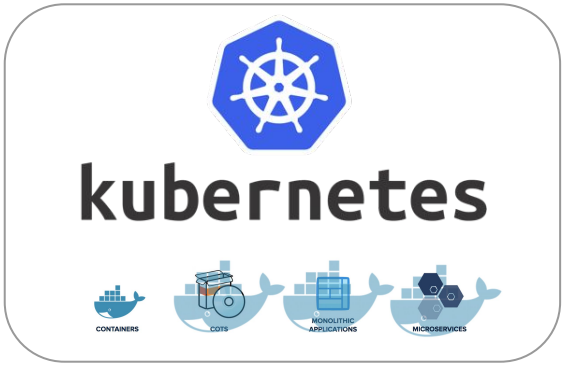
App User

Dev / Apps

```
> kubectl
```



Kubernetes Dashboard



IT / Ops

Compute

Storage

Networking

Pivotal

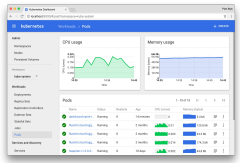
...but Kubernetes alone is not enough for enterprises

App User

Load Balancing / Routing

Dev / Apps

```
> kubectl
```



Kubernetes Dashboard

Container Image Registry

App Monitoring

App Logging

kubernetes

CONTAINERS

COTS

MONOLITHIC APPLICATIONS

MICROSERVICES

External Data Services

Cluster Provisioning

IT / Ops

Command Line / API

Management GUI

Monitoring GUI

OS Updates

K8S Updates

Log & Monitor

Backup & Restore

OS Images

K8S Images

Recover & Restart

Provision & Scale

Compute

Storage

Networking

Pivotal

Pivotal Container Service (PKS) provides what's missing

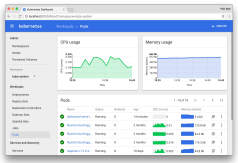
Pivotal
vmware
Google

App User

vmware NSX

Dev / Apps

```
> kubectl
```



Kubernetes Dashboard

HARBOR™

WAVEFRONT

App Logging

kubernetes

CONTAINERS COTS MONOLITHIC APPLICATIONS MICROSERVICES

GCP Service Broker

PKS Control Plane

IT / Ops

```
> pks
```

Operations Manager

vRealize Operations*

CLOUDFOUNDRY BOSH™

Compute

Storage

vmware NSX

*integration

Pivotal

on any Cloud

Pivotal

vmware

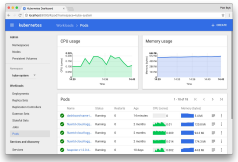
Google

App User

vmware NSX

Dev / Apps

```
> kubectl
```



Kubernetes Dashboard

HARBOR™

WAVEFRONT

App Logging

kubernetes

CONTAINERS COTS MONOLITHIC APPLICATIONS MICROSERVICES

GCP Service Broker

PKS Control Plane

IT / Ops

```
> pks
```

Operations Manager

vRealize Operations*

CLOUD FOUNDRY BOSH™

vmware NSX

vmware vSphere

Azure

Google Cloud Platform

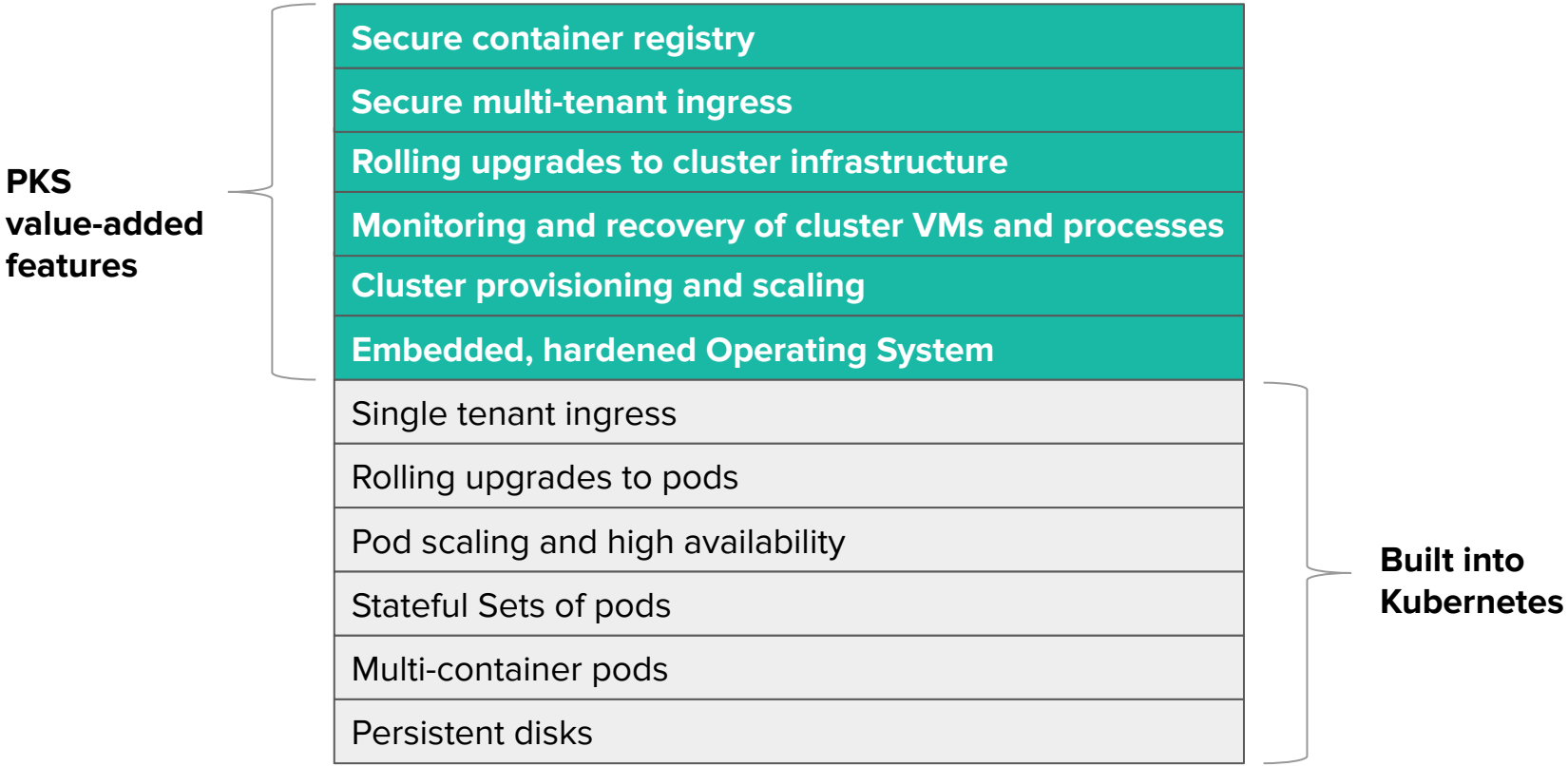
aws

openstack.

Pivotal

*integration

What PKS adds to Kubernetes



PKS Vision

*To provide enterprise customers with the ability to **safely** and **efficiently** deliver container services on their **preferred infrastructure** so that they can excel in their market with a cloud native platform*

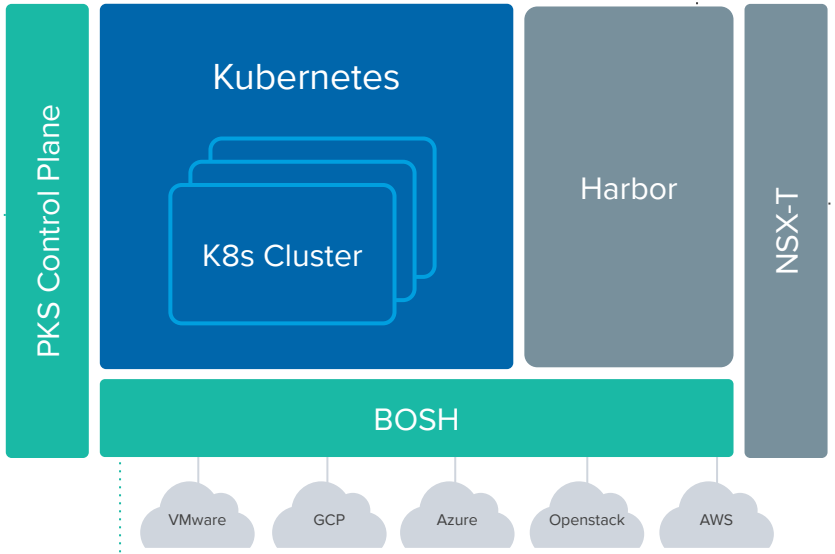
PKS does for your Kubernetes
what
Kubernetes does for your apps
Pivotal

Pivotal Container Service™

Enterprise-Grade Kubernetes

Built with open-source Kubernetes
Constant compatibility with the latest stable release of Google Kubernetes Engine—no proprietary extensions.

PKS Control Plane
Use the PKS CLI and API to create, operate, and scale your clusters.



Harbor
An enterprise-class container registry. Includes vulnerability scanning, identity management, and more.

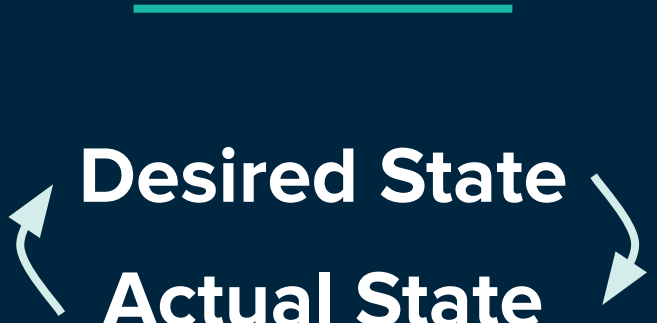
NSX-T
Network management, security, and load balancing out-of-the-box with VMware NSX-T. Multi-cloud, multi-hypervisor.

BOSH
Reliable and consistent operational experience for any cloud.

Pivotal

Pivotal

Controllers make Kubernetes great.


Desired State
Actual State

Unix Philosophy:

Do one thing. Do it well.

A Kubernetes pod is fragile.

The **ReplicaSet** Controller

Adds resiliency to your **Pods**.

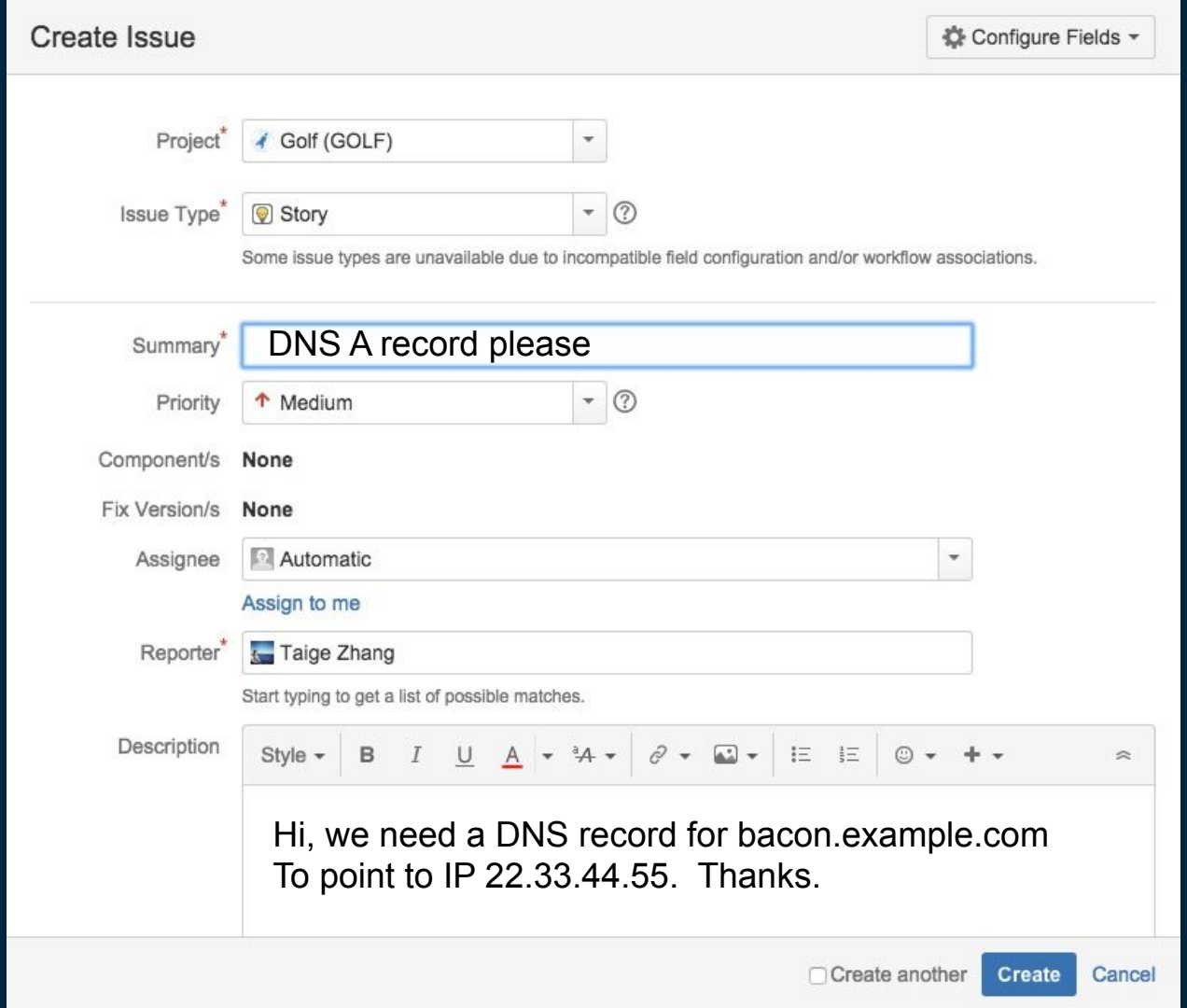
The **Deployment** Controller

Adds upgradability to your **ReplicaSets**.

You can write custom controllers very easily.

Kubernetes is an API

for Operations


Create Issue
Configure Fields
Project*
Golf (GOLF)
Issue Type*
Story
Some issue types are unavailable due to incompatible field configuration and/or workflow associations.
Summary*
DNS A record please
Priority
Medium
Component/s
None
Fix Version/s
None
Assignee
Automatic
Assign to me
Reporter*
Taige Zhang
Start typing to get a list of possible matches.
Description
Style
Hi, we need a DNS record for bacon.example.com
To point to IP 22.33.44.55. Thanks.
Create another
Create
Cancel

Pivotal

external-dns controller

https://github.com/kubernetes-incubator/external-dns

outage due to certificate expiry

All News Images Videos Shopping More Settings Tools

About 278,000 results (0.45 seconds)

Ericsson Outage: Expired Certificate knocks millions of UK mobile ...

https://www.thesslstore.com/blog/expired-certificate-ericsson-o2/

★★★★★ Rating: 5 - 3 votes

Dec 8, 2018 - **Thanks** to an **expired** digital **certificate** in a version of Ericsson's ... The **outage** has inspired no shortage of vitriol, which isn't exactly going to be ...

People also ask

- What happens when certificate expires?
- Why do SSL certificates expire?
- How do you renew security certificate that expired?
- Has my SSL certificate expired?

Feedback

Pivotal

cert-manager controller

(/operator)

https://github.com/jetstack/cert-manager

Operators extend Kubernetes

to support custom resources

https://github.com/operator-framework/awesome-operators

Controllers and Operators turn Kubernetes Into an API for Operations

Let’s run Kubernetes

Kelsey Hightower ✓

@kelseyhightower

Follow

Kubernetes is a platform for building platforms. It's a better place to start; not the endgame.

1:04 PM - 27 Nov 2017

“Let somebody else
Do the hard stuff” - Me
Pivotal

One Big Cluster or Many Smaller Clusters

One [or two] Big Cluster[s]

- All teams co-located on cluster, “namespaces” separate them.
- Higher chance of noisy neighbor, other multi-tenancy issues.
- Better utilization of resources (less servers, higher bin-packing)
- Cluster Upgrades affect everyone.
- Large Blast radius during cluster issues / outages.
- Monolithic approach to infrastructure

Many Smaller Clusters

- Each “team” or “business unit” gets its own cluster.
- Dedicated resources to each cluster reduces noisy neighbor etc.
- Resources can be customized at the cluster for the specific use cases.
- Cluster Upgrades only affect one team, easier to coordinate.
- Cluster issues/outages restricted to one team.
- Microservices approach to Infrastructure

One Big Cluster or Many Smaller Clusters

One [or two] Big Cluster[s]

- *Pivotal Container Service - Essentials*
- Kops
- Some Kubernetes distro from another vendor
- Kubespray
- DIY chef/puppet/ansible

Many Smaller Clusters

- **Pivotal Container Service - Enterprise**
- *Pivotal Container Service - Cloud*
- Google Container Engine
- Elastic Container Service
- Azure Container Service

https://k8s.af

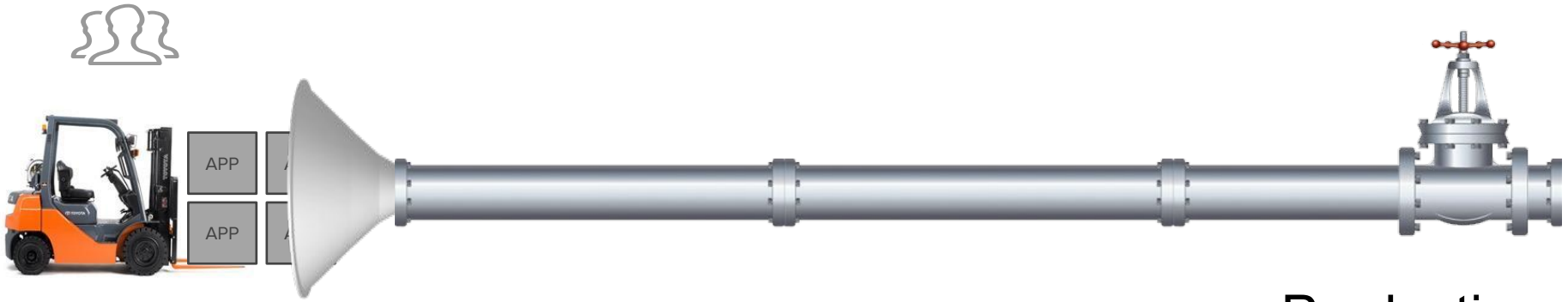
Start with the idea of doing

many smaller clusters.

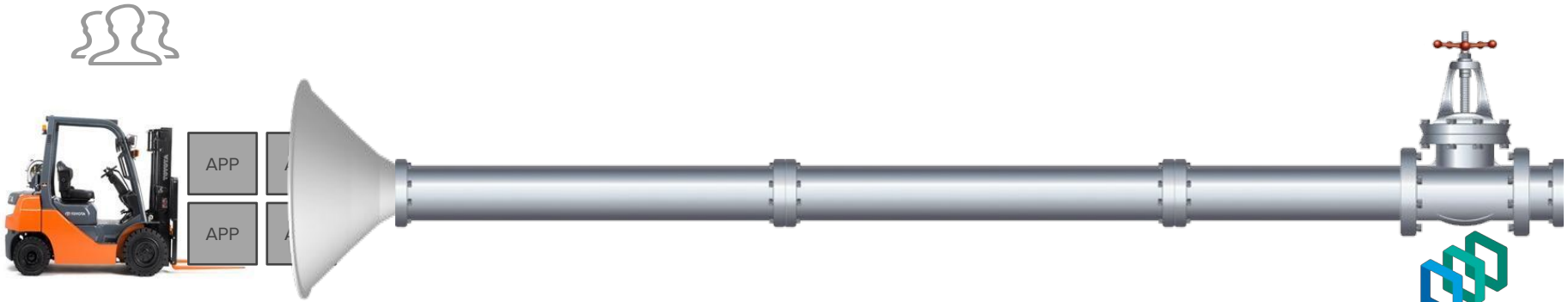
One Big Cluster or Many Smaller Clusters

One [or two] Big Cluster[s]

Many Smaller Clusters



Production



Pivotal Container Service™

Pivotal

vmware

Google Cloud

Azure

HARBOR™

Pivotal Container Service™

vmware

Google Cloud

Azure

Pivotal

HARBOR™

Pivotal Container Service™

vmware

Google Cloud

Azure

Pivotal

Gitlab

HARBOR™

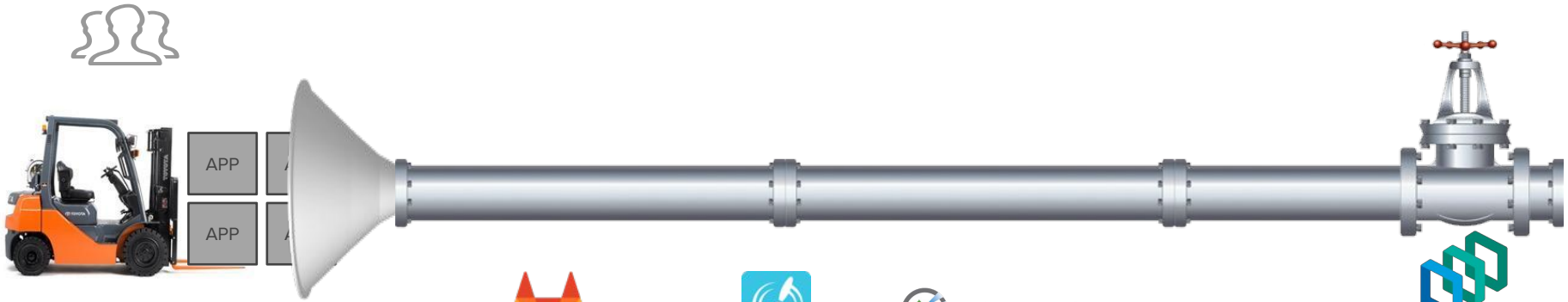
Pivotal
Container
Service™

vmware

Google Cloud

Azure

Pivotal



Gitlab

Concourse

HARBOR™

Pivotal
Container
Service™

vmware

Google Cloud

Azure

Pivotal

vmware

Google Cloud

Azure

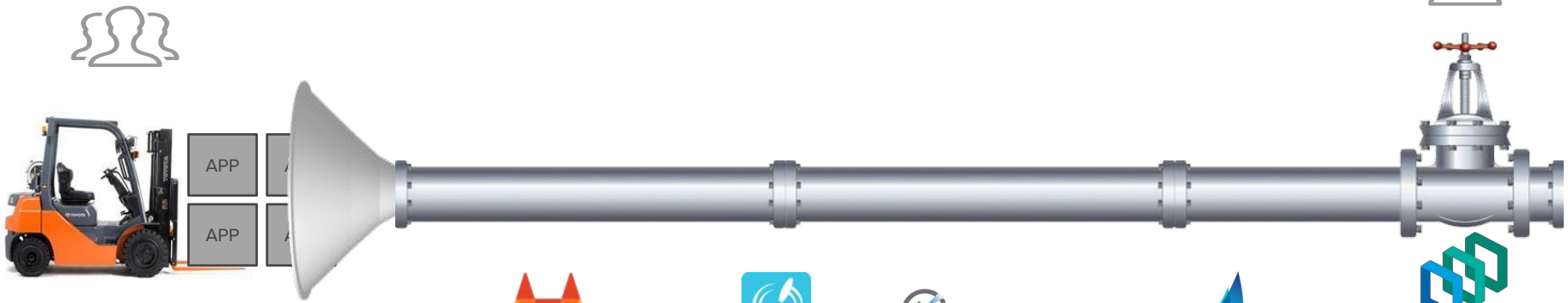
Pivotal

vmware

Google Cloud

Azure

Pivotal



Prometheus

Grafana

elastic

Gitlab

Concourse

HARBOR™

Spinnaker

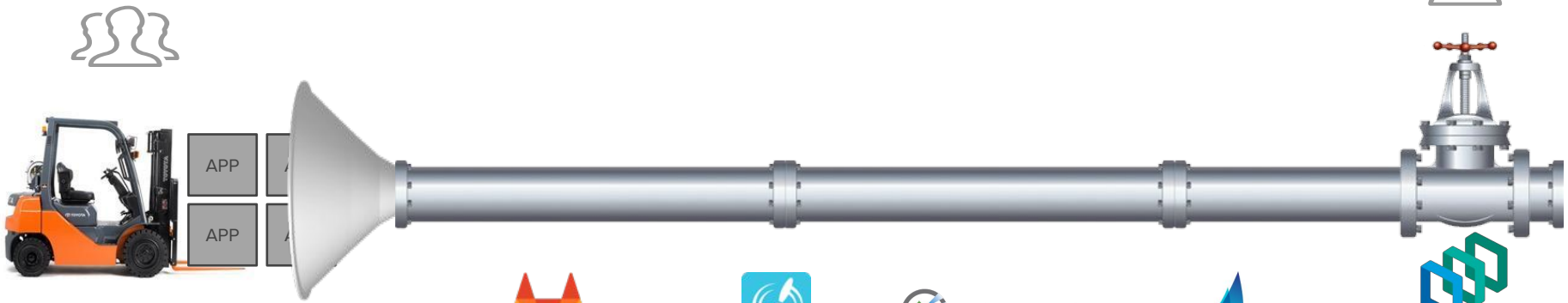
Pivotal Container Service™

vmware

Google Cloud

Azure

Pivotal



Prometheus

Grafana

elastic

Gitlab

Concourse

HARBOR™

Spinnaker

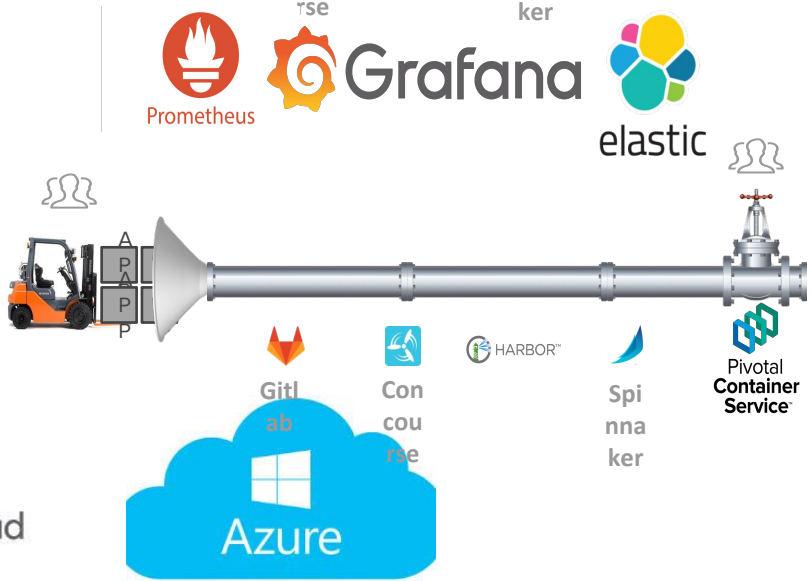
Pivotal Container Service™

vmware

Google Cloud

Azure

Pivotal



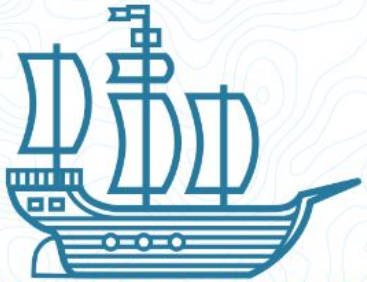
Google Cloud

Pivotal

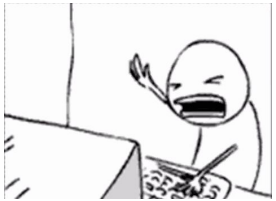
We've spent 10 years figuring

out how to do agile operations

HELM



Platform Operations



Kube Env #2 Repo

Helm Chart Repo

Kube Env #1 Repo

HELM

Prometheus

Grafana

elastic

Gitlab

Concourse

HARBOR

Spinnaker

Pivotal Container Service

Prometheus

Grafana

elastic

Gitlab

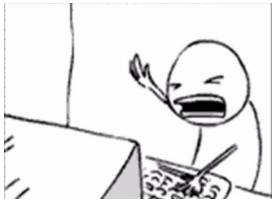
Concourse

HARBOR

Spinnaker

Pivotal Container Service

Developer Workflow



App Env Repo #1

App Source Code

App Env Repo #2

Concourse

HARBOR™

Spinnaker

Pivotal Container Service™

DEMO TIME

Transforming How The World Builds Software

© Copyright 2019 Pivotal Software, Inc. All rights Reserved.