PCF 2.0和CFCR进阶

鲍亭方 bbao@pivotal.io

主要内容

- PaaS的价值
- Cloud Foundry介绍
- BOSH工具链
- PCF 2.0 (PAS PKS PFS)
- Cloud Foundry Container Runtime （CFCR）
- 思考

Pivotal

用户应该关注什么？专业的人做专业的事儿！

Traditional IT

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

IaaS

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

PaaS

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Pivotal

IaaS和PaaS各自解决了什么问题?

IaaS

硬件的自动化管理，人与机器的解耦合，获得效率/提高资源利用率

PaaS

应用的自动化管理，应用与OS的解耦合，获得弹性/简化运维，以及更高的资源利用率

PaaS的业务价值

解耦上层应用与底层基础设施

数据即服务

应用微服务化

一切自动化

Cloud Foundry是什么？ 一个开放的PaaS平台

Keep It Simple:

开发者专注于业务代码实现，其他的事情交给Cloud Foundry平台

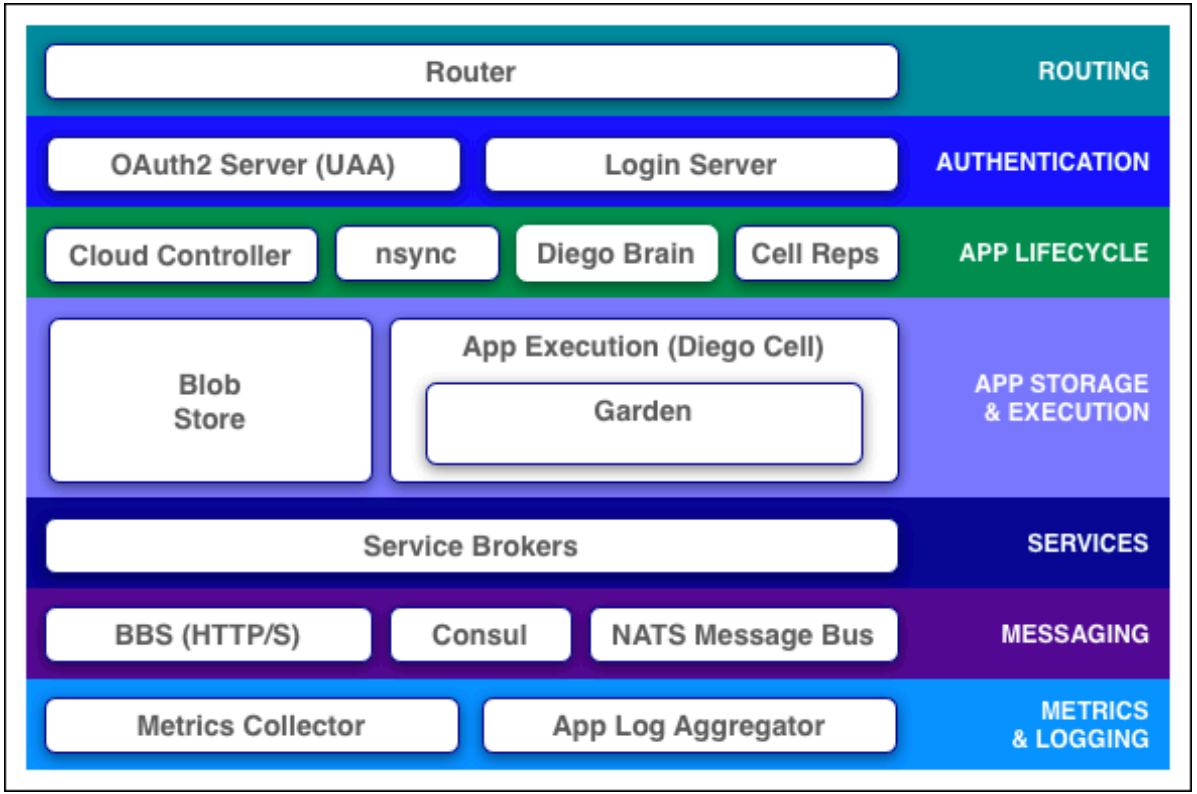
Open Source:

开源，并且支持各大主流云平台：AWS, GCP, Azure, OpenStack。

哪里运行App，用户说了算！

Pivotal

Cloud Foundry 分层设计



接收入口流量, 之后路由到合适的组件

为CF提供身份认证和权限管理

对app生命周期管理

数据存储及APP执行引擎

为CF提供各种第三方服务

CF消息总线

CF基础监控指标和日志收集系统

Pivotal

PCF工具链

BOSH：

- stemcell： 提供底层的操作系统镜像
- release： 打包软件包和各种服务
- manifest： 描述部署过程
- bosh-cli： 用户接口

OpsManager: 为bosh提供了Web访问方式

Concourse: CI/CD工具,可以实现自动集成测试和自动部署工作

CF-CLI: 用户与Cloud Foundry的主要交互工具

BOSH

—— 针对大规模分布式服务提供的一种发布， 部署和生命周期管理的开源工具链

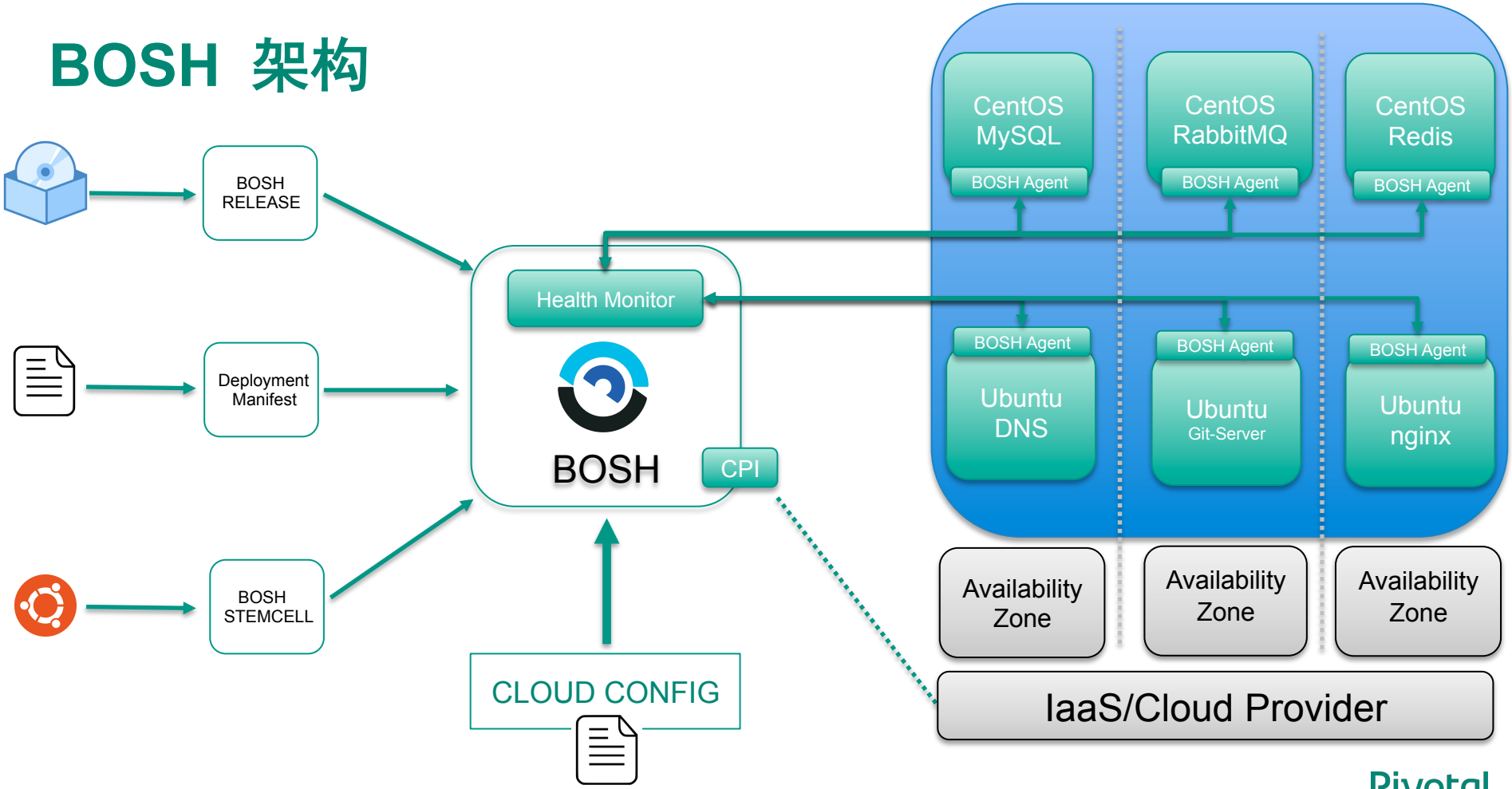
BOSH可以做什么？

封装操作系统， 保证以一致的方式（Stemcell）为各种服务提供**操作系统支持**
通过BOSH CPI接口， 屏蔽不同IaaS平台的差异， 统一抽象底层**虚拟机管理**
提供统一的软件**打包规范**（Release）， 实现在集群上稳定可靠部署软件服务
开箱即用的**健康检查**功能， 支持服务器健康检查以及服务进程健康检查，服务进程状态监控
支持服务**自愈特性**以及服务器**自动重建特性**
支持**存储管理**， 包括本地的NFS，也支持远程的对象存储， 比如： S3
检测式的滚动升级， 保证升级的可靠性 （canary test）

一句话：PCF的生态环境中，离不开BOSH，它不仅仅是一个部署工具，更是整个PCF系统的**基础支持组件**。

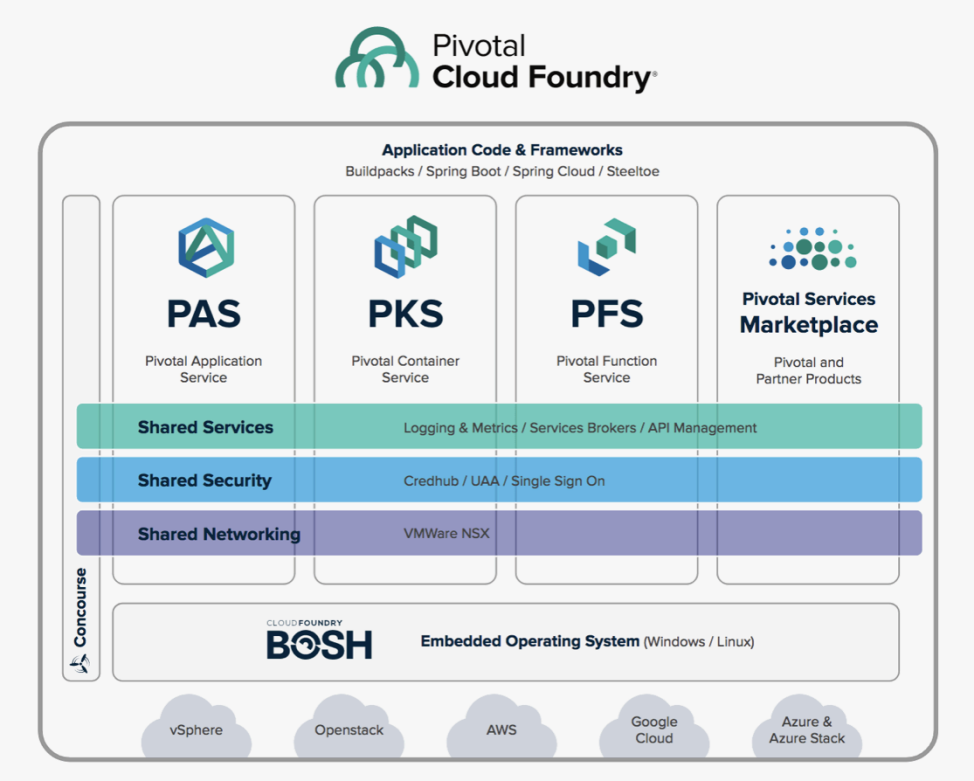
Pivotal

BOSH 架构



Pivotal

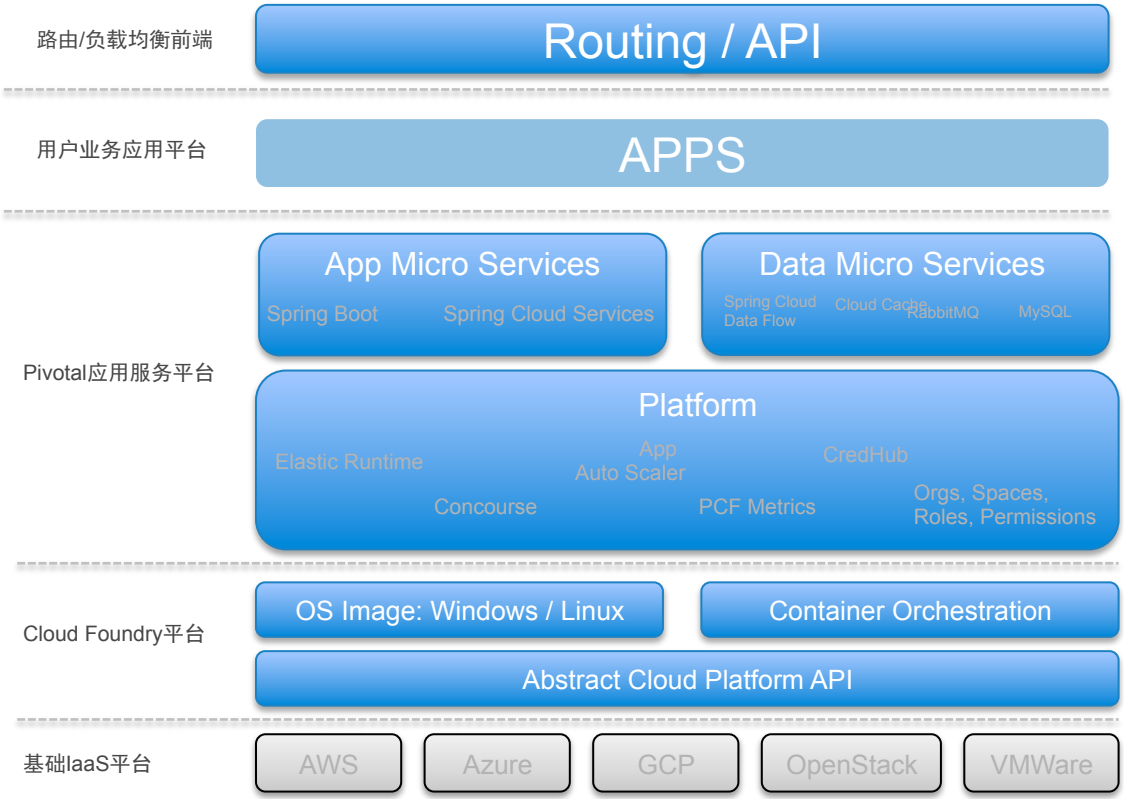
PCF 2.0改进



- BOSH屏蔽了不同IaaS平台的差异
- PAS PKS PFS共享基础服务
- PAS 提供了企业版的Cloud Foundry支持
- PKS 提供了企业版的K8s支持
- PFS 提供了企业版的Server Less支持
- Marketplace支持第三方产品的集成
- Concourse提供CI/CD支持

Pivotal

PAS 体系结构



Pivotal

PAS 安全特性

HAProxy与Gorouter之间的所有流量启用TLS（支持自定义CA证书）

HAProxy与APP之间可以通过X-Forwarded-Client-Cert Header进行认证

服务实例的认证信息， 经过加密后保存在Credhub中

Ops Manager提供了更多的角色，拥有更细的控制粒度

PAS 运维效率提升

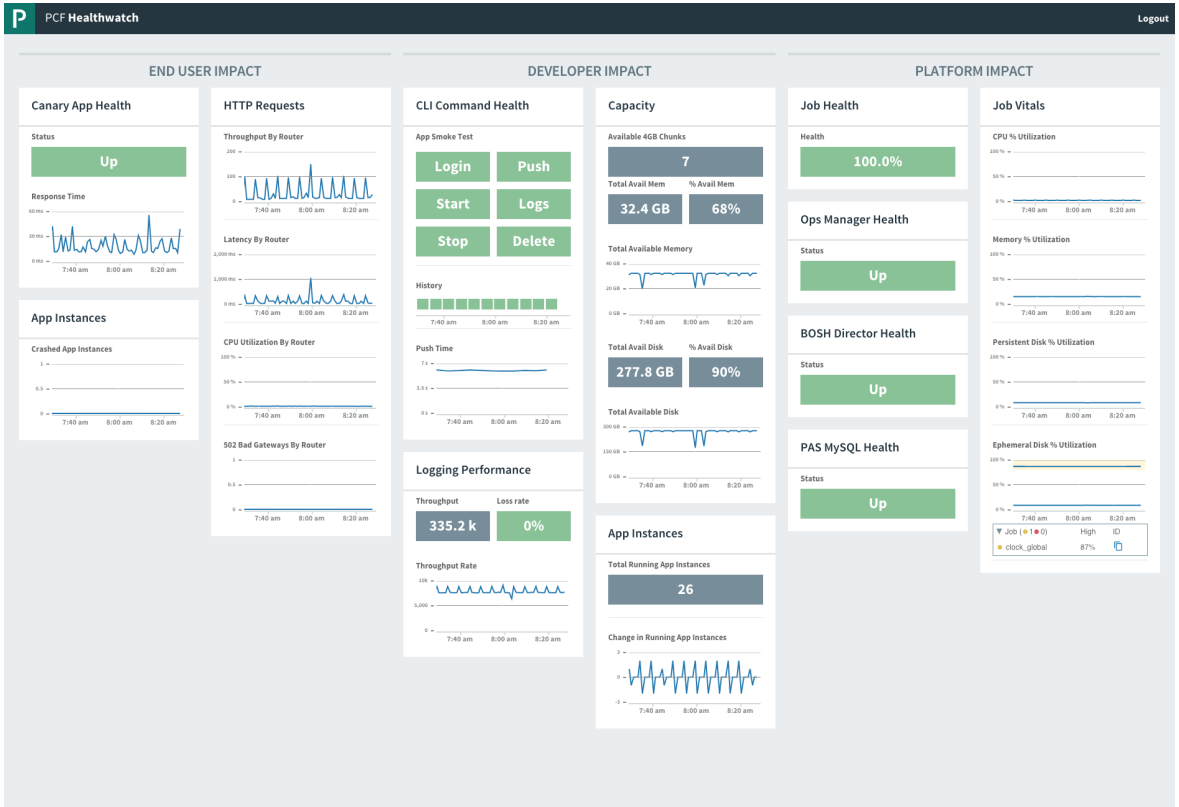
C2C网络支持 NSX-T，NSX-T 通过CNI接口集成到Cloud Foundry,容器可以通过NSX-T托管网络获取IP地址

Apps Manager集成计划任务，可以非常容易创建计划任务

Apps Manager中可以查看app的mapping actuator，便于错误跟踪和调试

PCF Healthwatch PCF提供的dashboard，可以查看关键KPI和监控指标

PAS Healthwatch



Pivotal

Pivotal Container Service (PKS)

—— 在各种云平台上， 为K8S集群提供一致高效管理方式，包括集群的创建， 集群的自动化运维管理， 以及K8S集群的各种资源管理。

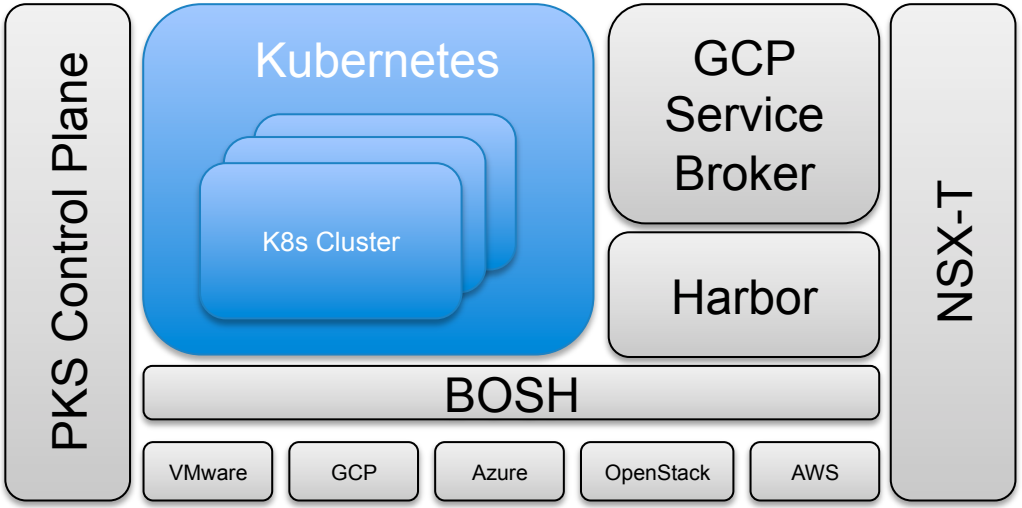
PKS优点：

节点的健康管理； 自动收集节点的性能指标和日志； 快速扩容； 持久化接口

Control Plane功能：

快速创建K8S集群； 定制K8S集群大小； 操作系统自动升级； 负载均衡； 网络； 多租户管理

PKS 架构



- 跨平台：BOSH屏蔽底层IaaS差异
- 平面网络：NSX-T支持容器网络的跨主机访问
- 高效部署：Harbor提供企业级内部镜像管理
- 服务集成：通过Service Broker接口实现第三方集成
- 容器运行时环境支持：完全支持K8s最新特性，支持升级
- 集群管理：PKS CP让K8S集群的扩容更简单高效

Pivotal

PKS 特性

完全兼容最新版K8S，支持K8S的版本升级

企业级支持：为APP提供了高可用的运行环境：无单点， 支持健康检查，
支持集群扩容， 服务组件自愈以及滚动升级

MultiCloud支持：BOSH屏蔽了各平台的差异，支持跨平台部署。

网络支持：集成了VMware的NSX-T技术，实现容器的跨主机访问。

GCP原生支持： 允许APP透明访问Google的各项服务

自动化运维支持： 完全自动化运维部署， 扩容， 升级， 无宕机操作

Pivotal

Pivotal Function Service (PFS)

—— PFS是Cloud Foundry上的一种服务。可以针对某一事件作出响应，执行用户之前定义好的某个函数

PFS特点：

开源; 原生支持Kubernetes; 支持多个云平台; 通知多种语言; 基于事件流模型; Pivotal官方支持

PFS使用场景：

Web Events； 基于事件的处理逻辑；流式处理

Repo： https://github.com/projectriff/riff

Pivotal

Cloud Foundry Container Runtime （CFCR）

2016年Pivotal发布支持Google公有云GCP的PCF,随后，Pivotal开发测试环境在GCP上部署

2016年,Google为PCF配套开发了8项主要的Service Broker,以接入PCF应用

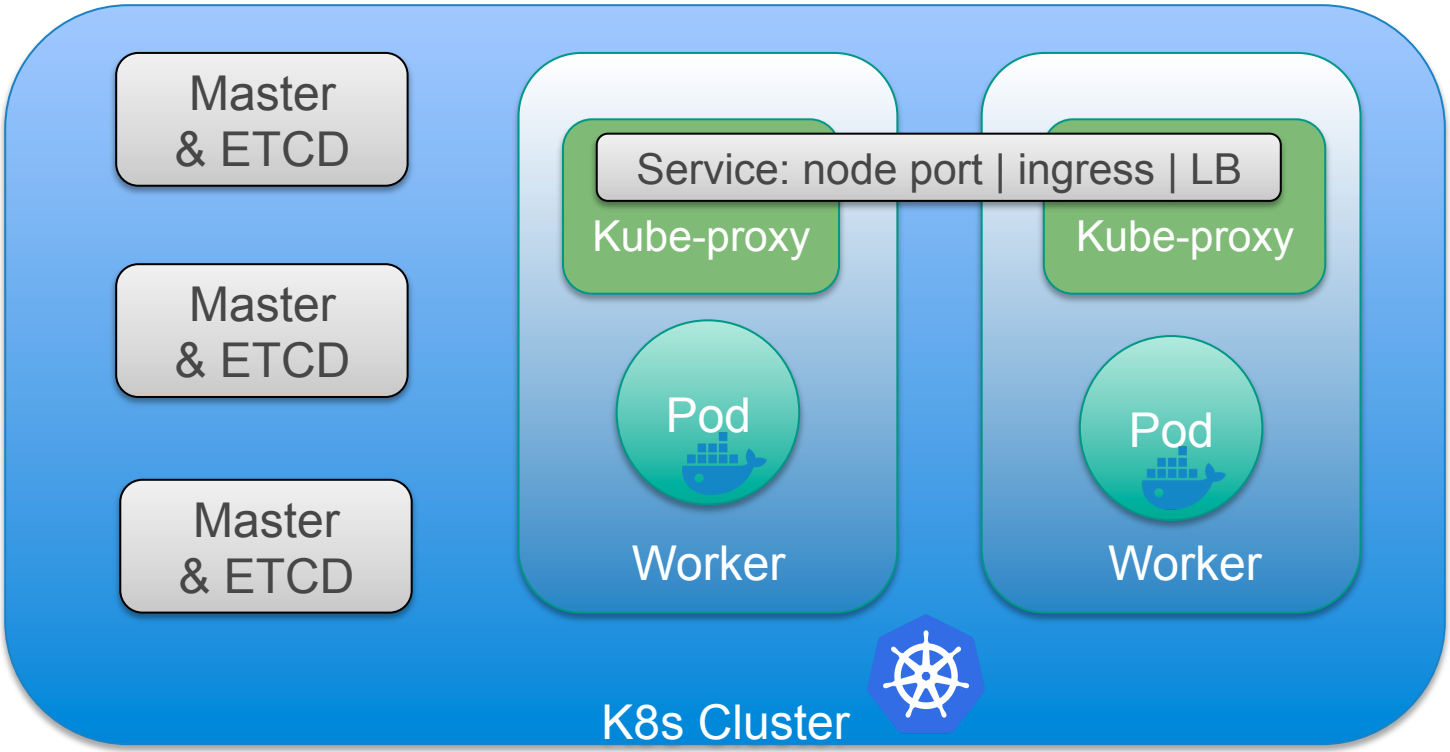
2016年12月Google加入Cloud Foundry基金会黄金会员

2017年3月，Google和Pivotal共同发布**Kubo开源版**，Google工程师和Pivotal工程师共同分析K8s和PCF各自有优缺点，形成**融合方案**

2017年3月，Pivotal的云运维部门正式组建SRE团队，开始在PWS上推行SRE，形成工具，然后推广到PCF的运维工具上去

Pivotal

Kubernetes： 用好，真不容易



对K8S集群的思考

- 集群的高可用性： 组件冗余就是高可用吗？
- 集群的伸缩性：有定义集群状态的工具或方法吗？
- 集群的自愈性：如何保证集群本身的故障自动恢复？
- 集群的平滑升级：不要让自己脱离社区最新发展。
- 集群的安全性：如何安全高效地为系统打补丁

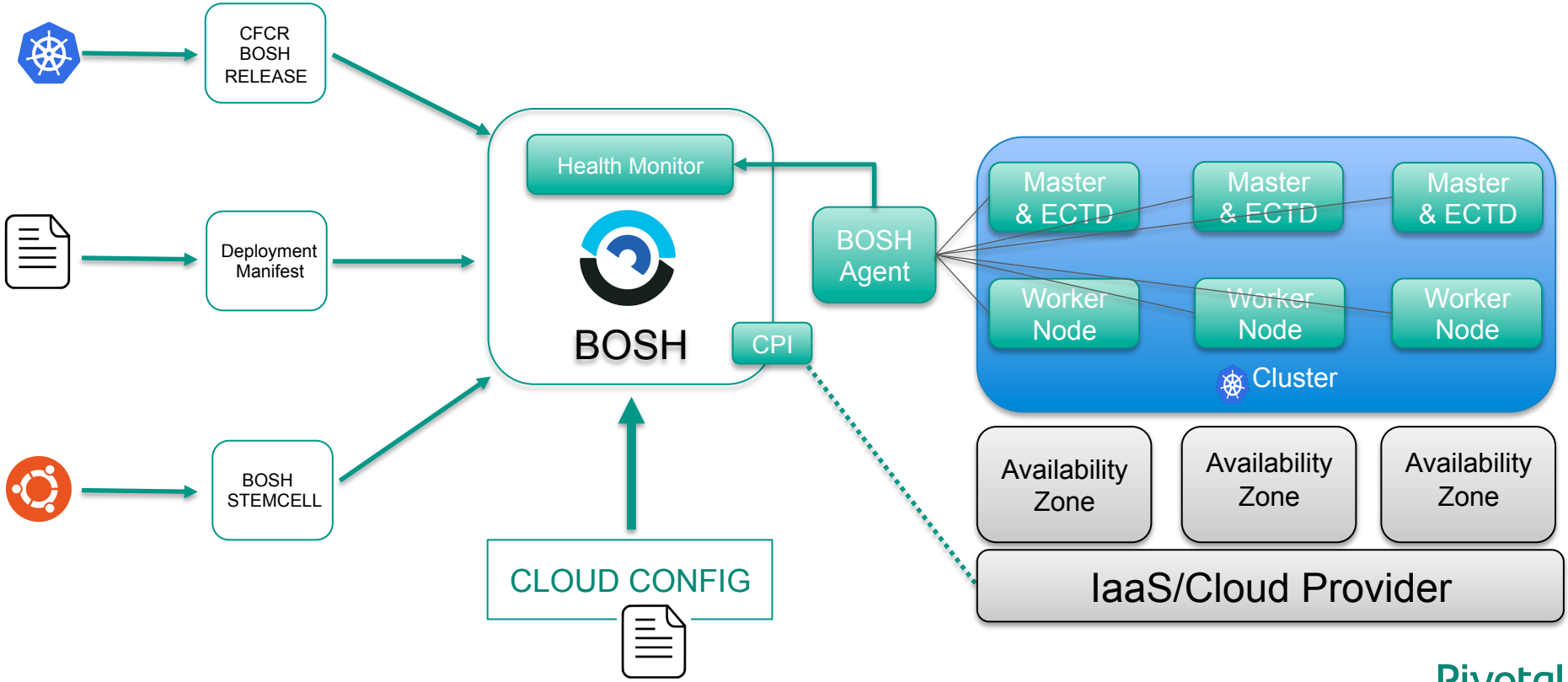
CFCR到底是什么？

—— 一套使用Bosh部署和管理kubernetes集群的解决方案.

CFCR = IaaS + BOSH + K8S

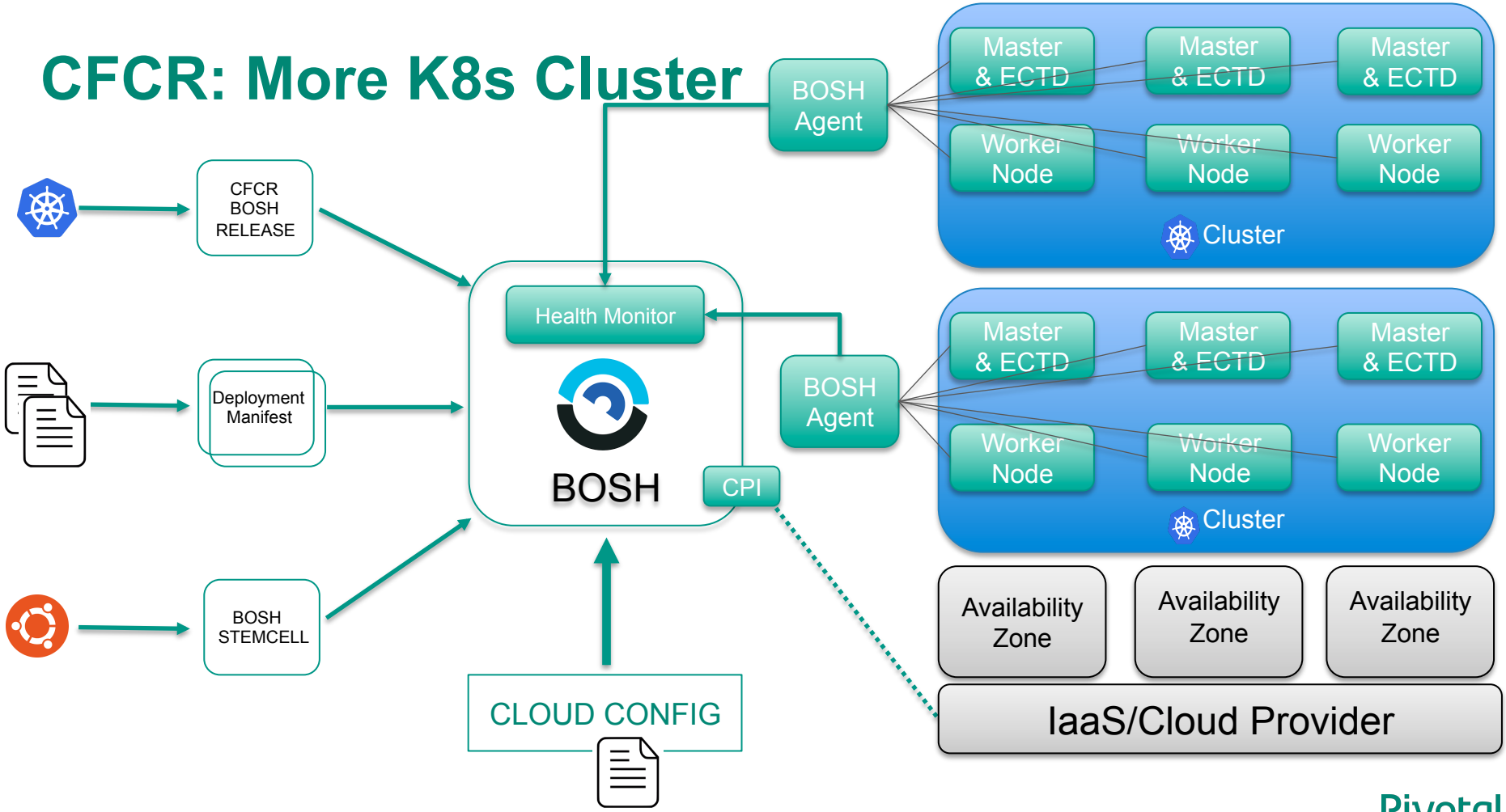
K8S让app实现了可伸缩性和自愈特性，BOSH让K8S实现可伸缩性和自愈特性

CFCR Provision: Create one K8s Cluster



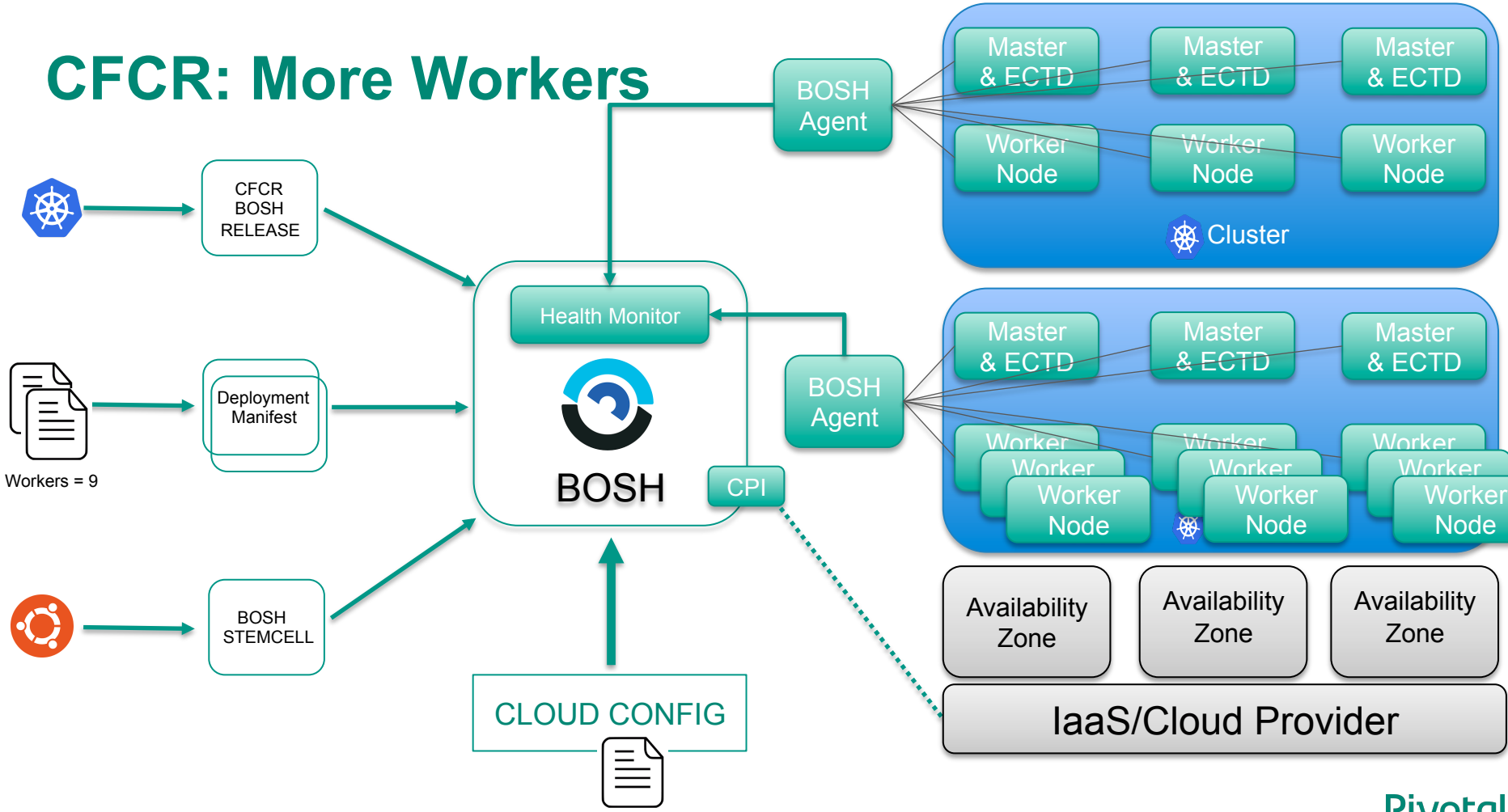
Pivotal

CFCR: More K8s Cluster



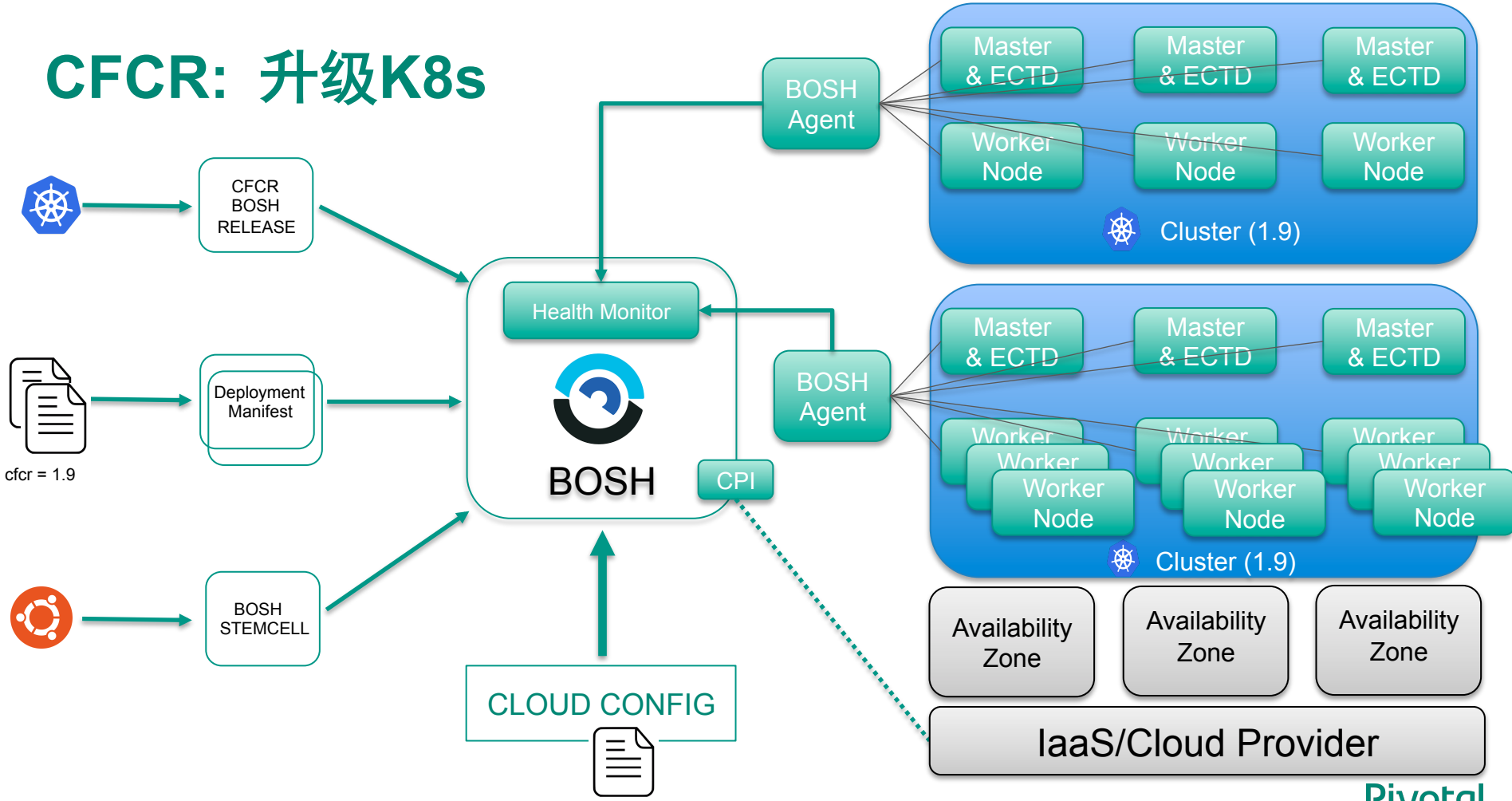
Pivotal

CFCR: More Workers



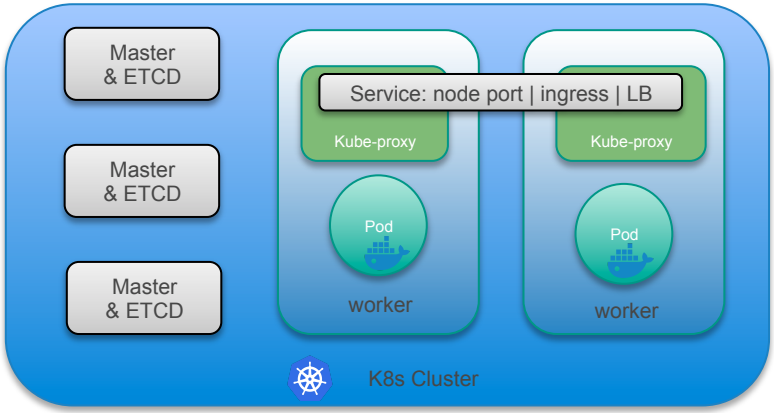
Pivotal

CFCR: 升级K8s



Pivotal

CFCR: 系统风险来源



开发人员负责 由容器image引入的漏洞风险 （APP）

运维人员负责 由虚拟机image引入的漏洞风险 （Worker）

IaaS 平台

Pivotal

CFCR带来了什么？

高可用性：

对master节点， worker节点以及ectd节点的冗余管理

灵活的扩展能力：

可以对master， worker， etcd节点数进行扩展， 用户需要做的就是修改参数值

健康检查以及自愈能力：

CFCR持续对各组件的健康状态进行监控，并且会自动保持集群的运行状态

生命周期管理：

支持滚动升级， 无宕机升级方式。支持平台级的安全漏洞修复能力

Pivotal

问题与思考

- BOSH如何与企业内部已有基础设施集成？
- CFCR出现的时间点？
- Pivotal Cloud Foundry与K8S的关系？

Pivotal


Pivotal®
Transforming How The World Builds Software