



DevOps Day

企业级容器服务架构： VIC、PKS和PCF

Architecting Enterprise Container Services: VIC, PKS and PCF

张海宁, VMware中国研发先进技术中心技术总监

周 晖, Pivotal云计算首席架构师

张 鑫, 才云科技创始人兼 CEO



#vForum

vFORUM 2017

议程

1

容器的应用场景和挑战

2

vSphere Integrated Containers

3

VMware Pivotal Container Service

4

Pivotal Cloud Foundry

5

案例分享

容器的应用场景和挑战

企业中容器应用的场景

新应用

新封装

新架构

容器化应用面临的挑战

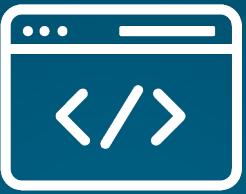
容器技术
日新月异

无法满足生产
系统的要求

缺少
运维工具

人员技能
缺失

开发运维一体化



开发人员

提高效率

减少开销



运维人员

提高服务水平

降低成本

选择正确的工具



vFORUM



vSphere Integrated
Containers



Pivotal
Container Service



Pivotal
Cloud Foundry®

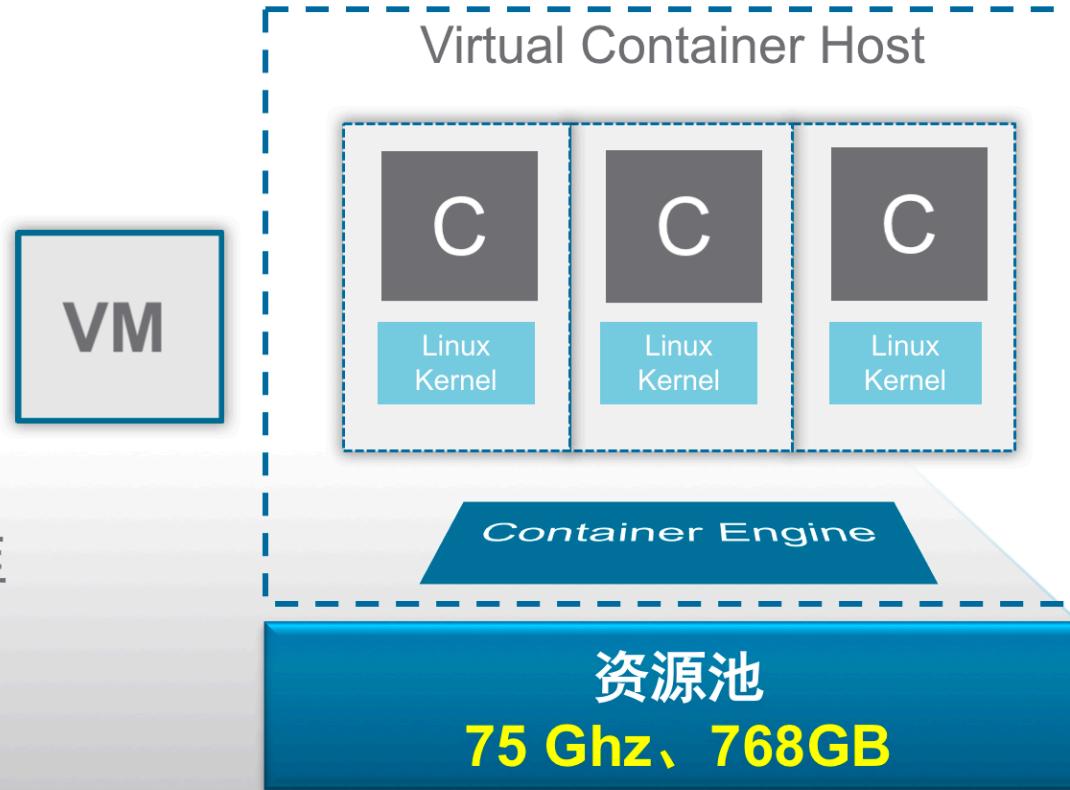
vSphere Integrated Containers

vmware®



虚拟机即容器：vSphere Integrated Containers 原理

- 不共享操作系统
- 高效利用资源
- 弹性伸缩
- 系统管理员可见性
- 使用现有的经验和工具
- 融合的架构简化部署、运维和支持



vSphere Integrated Containers 运维模式



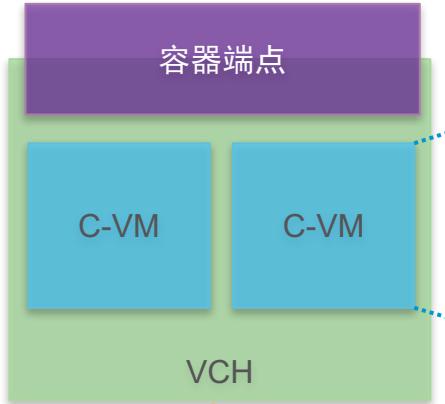
Jason : Cloud Admin
Setup and automate cloud infra



Scott : Developer
Write & deploy code

vic-machine-linux create

docker run -d -p 80:80 nginx



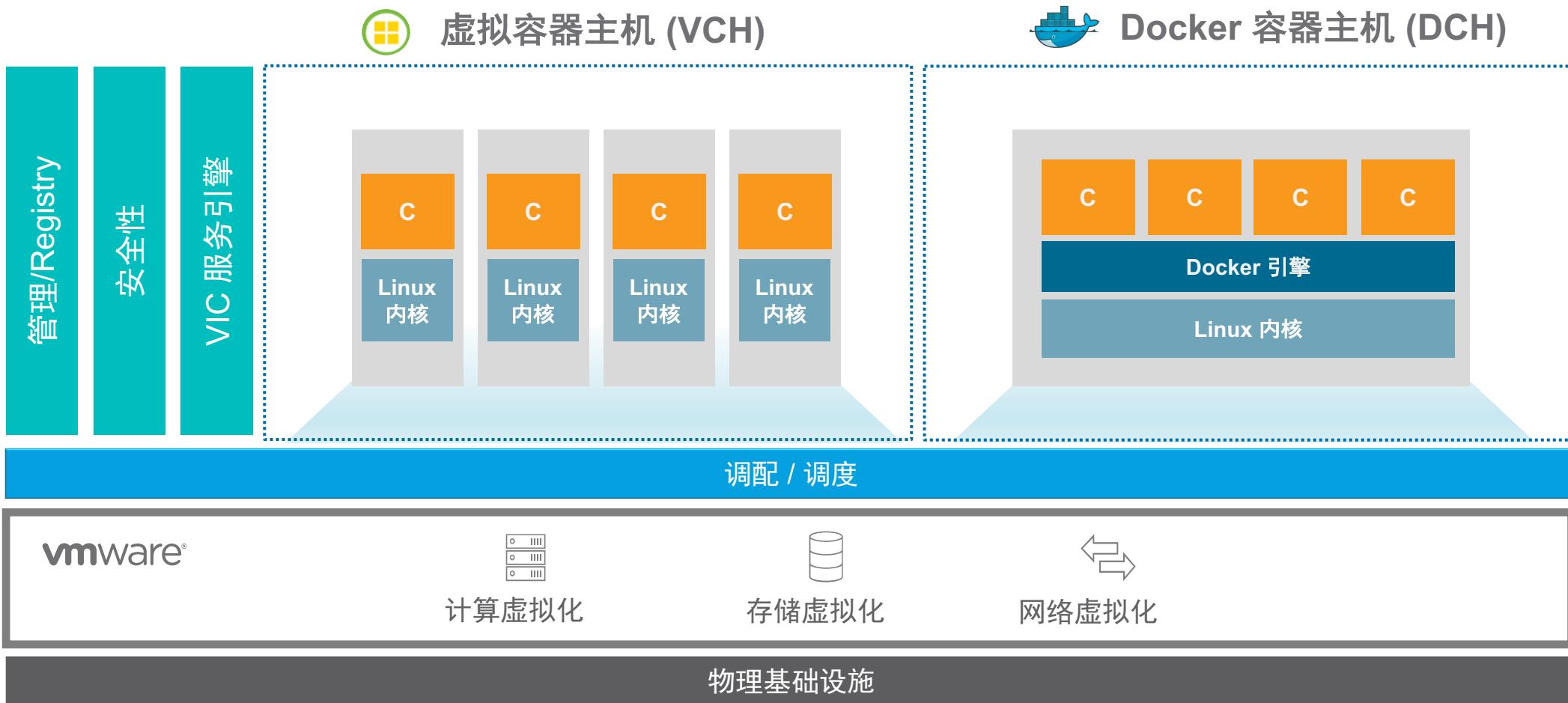
vSphere 集群



vSAN

NSX

两种容器主机： VCH 和 DCH



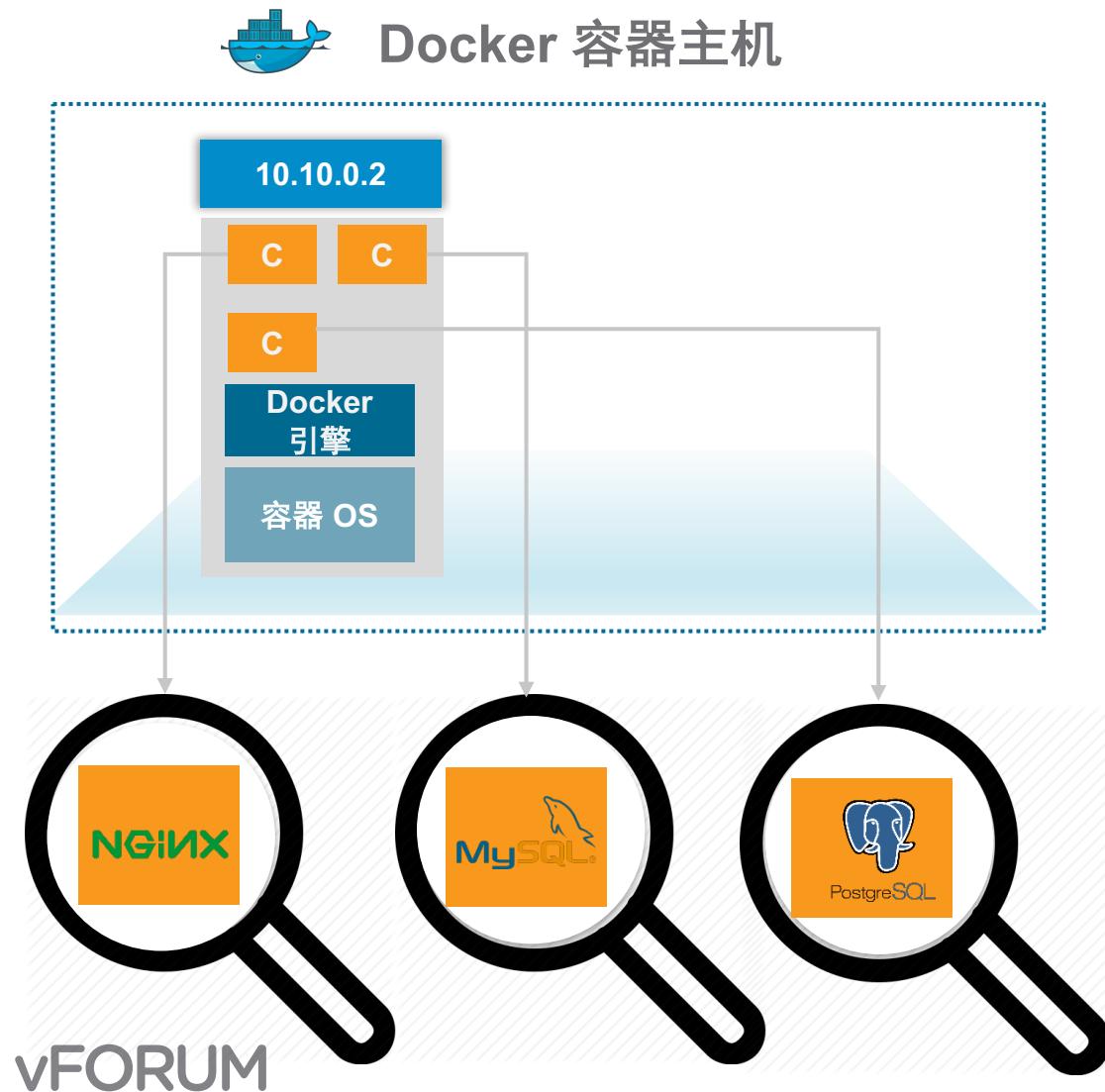
虚拟容器主机的工作方式



使用原生 Docker 命令

- 1 docker run nginx
- 2 docker run mysql
- 3 docker run postgres

支持原生 Docker 主机,作为开发沙箱



- 1 docker run vmware/dch-photon:17.06
- 2 export DOCKER_HOST=10.10.0.2
- 3 docker run nginx
- 4 docker run mysql
- 5 docker run postgres

VIC内置Harbor提供镜像漏洞扫描、内容信任



名称 标签数

- library/logstash 1
- library/mariadb 1
- library/nginx/1.11.5 1

标签 大小 Pull命令 漏洞

latest	69.48MB	docker pull 10.112.122.204/library/nginx/1...		×	NGINX Docker Maintainers "docker-maint@nginx.com"	2016/11/9 上午6:41
--------	---------	---	--	----------------	---	------------------

1 - 1 共计 1 条记录

! 漏洞严重度: 严重
96个组件中的29个含有漏洞.

- ! 13 严重
- ! 10 中等
- △ 4 一般
- ? 2 未知
- ✓ 67 无

扫描完成时间: 10月/19日/2017年 17时:07:17

Harbor 开源企业级容器镜像仓库: <https://github.com/vmware/harbor>

VIC内置Harbor提供镜像漏洞扫描、内容信任

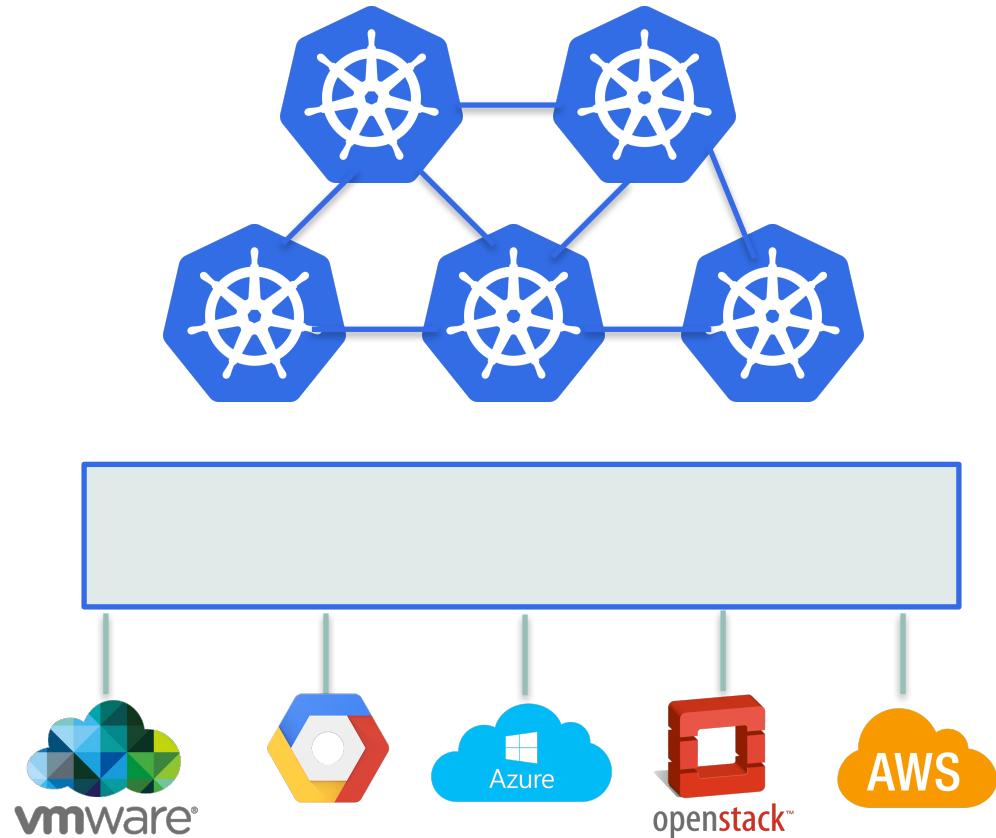


缺陷码	严重度	组件	当前版本	修复版本
> CVE-2016-9843	严重	zlib	1:1.2.8.dfsg-2	
> CVE-2016-9841	严重	zlib	1:1.2.8.dfsg-2	
> CVE-2016-9842	中等	zlib	1:1.2.8.dfsg-2	
> CVE-2016-9840	中等	zlib	1:1.2.8.dfsg-2	
> CVE-2017-2616	可忽略	util-linux	2.25.2-6	
> CVE-2016-5011	中等	util-linux	2.25.2-6	
> CVE-2015-5224	可忽略	util-linux	2.25.2-6	
> CVE-2015-5218	可忽略	util-linux	2.25.2-6	
> CVE-2016-2779	严重	util-linux	2.25.2-6	

Harbor 开源企业级容器镜像仓库: <https://github.com/vmware/harbor>

VMware Pivotal Container Service (PKS)

Kubernetes 运维面临的挑战



高可用性. 集群节点本身不具备开箱即用的可用性，(masters, workers and etcd nodes)。

伸展性. Kubernetes集群处理节点上的pod / 服务，但没有提供扩展的机制给Workers, Masters 和 etcd 虚机。

健康检查和治愈. Kubernetes集群只对运行在节点上的工作负载的健康进行常规的健康检查。

升级. 在大型集群上进行滚动升级是很困难的。谁管理它运行的系统？

BOSH 可弥补 Kubernetes 运维的不足



BOSH是用于发布工程、部署、生命周期管理和分布式系统监控的开源工具。

- 包装有嵌入式的 OS
- 服务器可部署在多种IaaS上
- 跨可用区的软件部署
- 健康监控 (服务器和进程)
- 带复活功能的自修复
- 存储管理
- 金丝雀滚动升级
- 集群易于伸缩

Kubo 开源项目的诞生

在任何云上，用统一的方法来实例化、部署和管理高可用的Kubernetes集群。

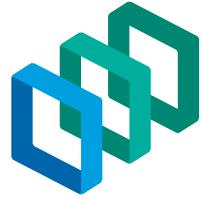
2017年2月由Pivotal 和 Google 联合推出，于2017年6月贡献给Cloud Foundry基金。

“Day 1” 构建

- Deploy Kubernetes cluster via BOSH

“Day 2” 运维

- 可自愈虚机，通过BOSH监控
- 弹性扩展的集群
- 滚动升级到最新的Kubernetes版本
- 高可用性和多AZ支持



Pivotal Container Service

提供用于部署和管理Kubo
版本的控制平面

由Pivotal、VMware和谷歌
联合开发

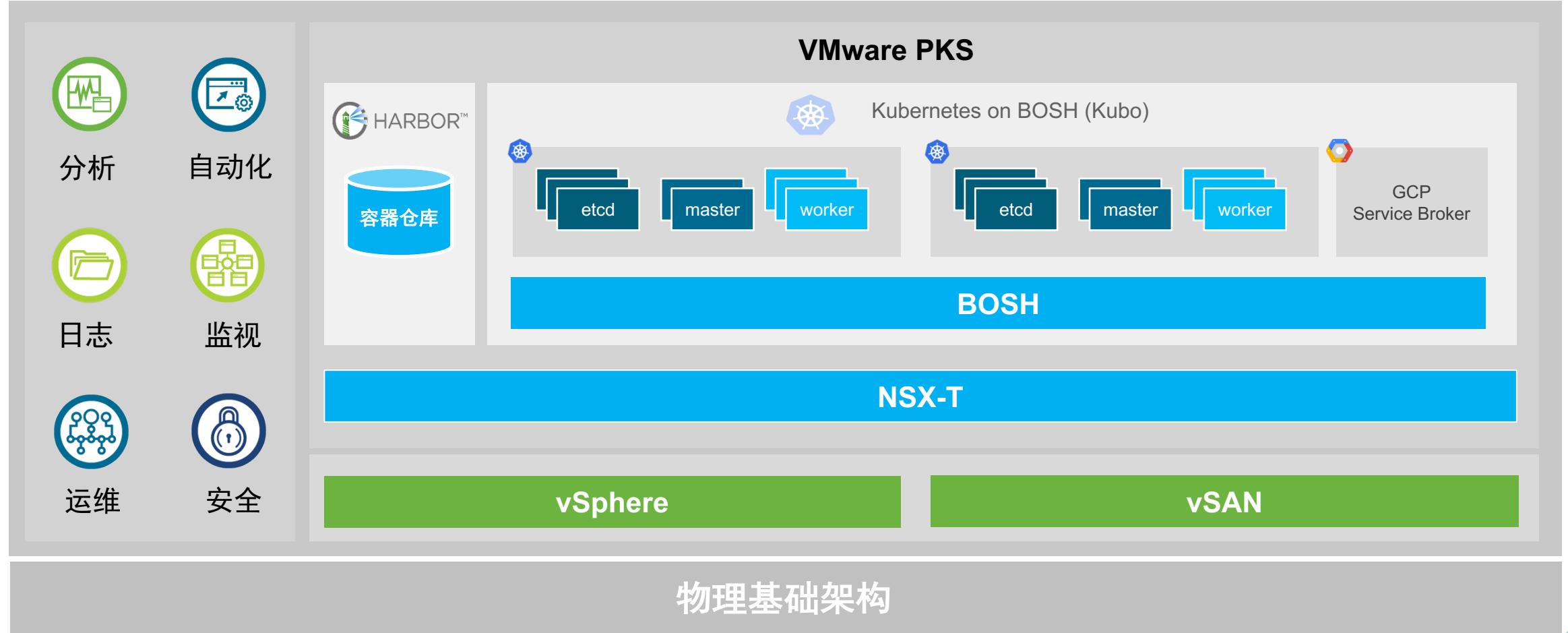
Kubernetes Dial Tone:

- 健康管理
- 聚合指标和日志记录
- 自动扩展
- 一致性接口

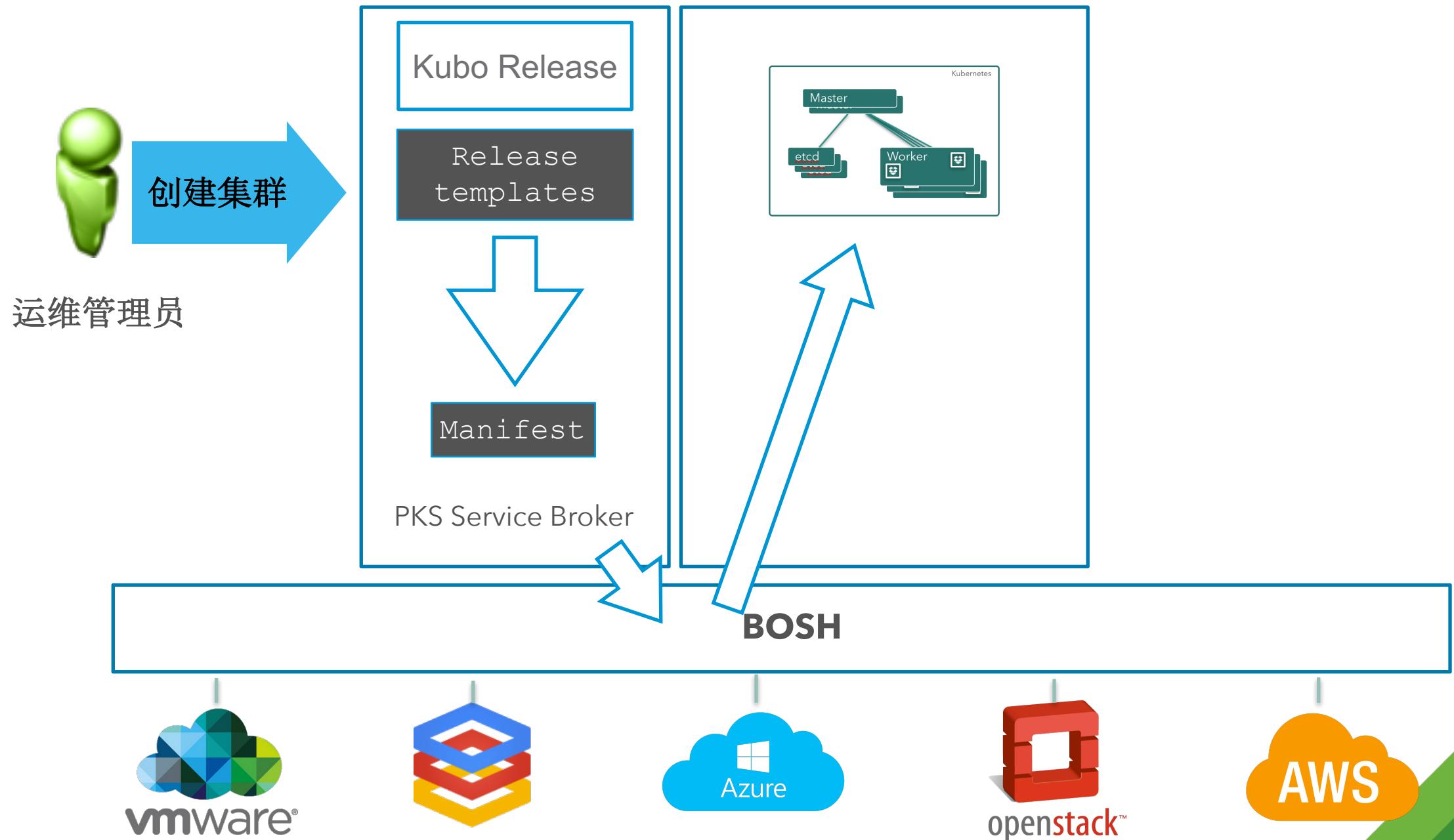
Control Plane:

- 部署引擎
- 自服务集群
- 软件更新自动化
- 负载均衡
- 网络
- 多租户

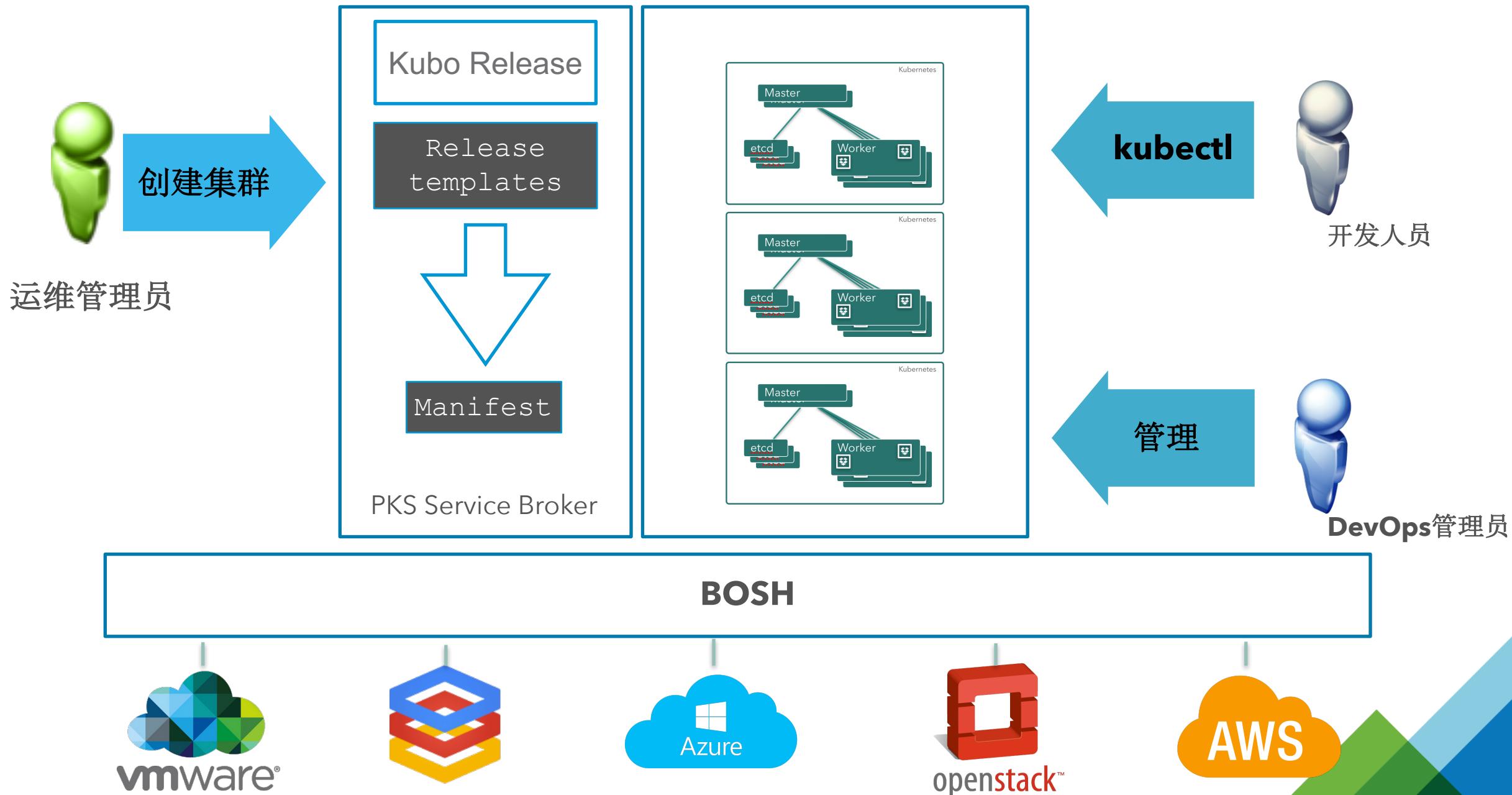
企业级的Kubernetes – Pivotal Container Service (PKS)



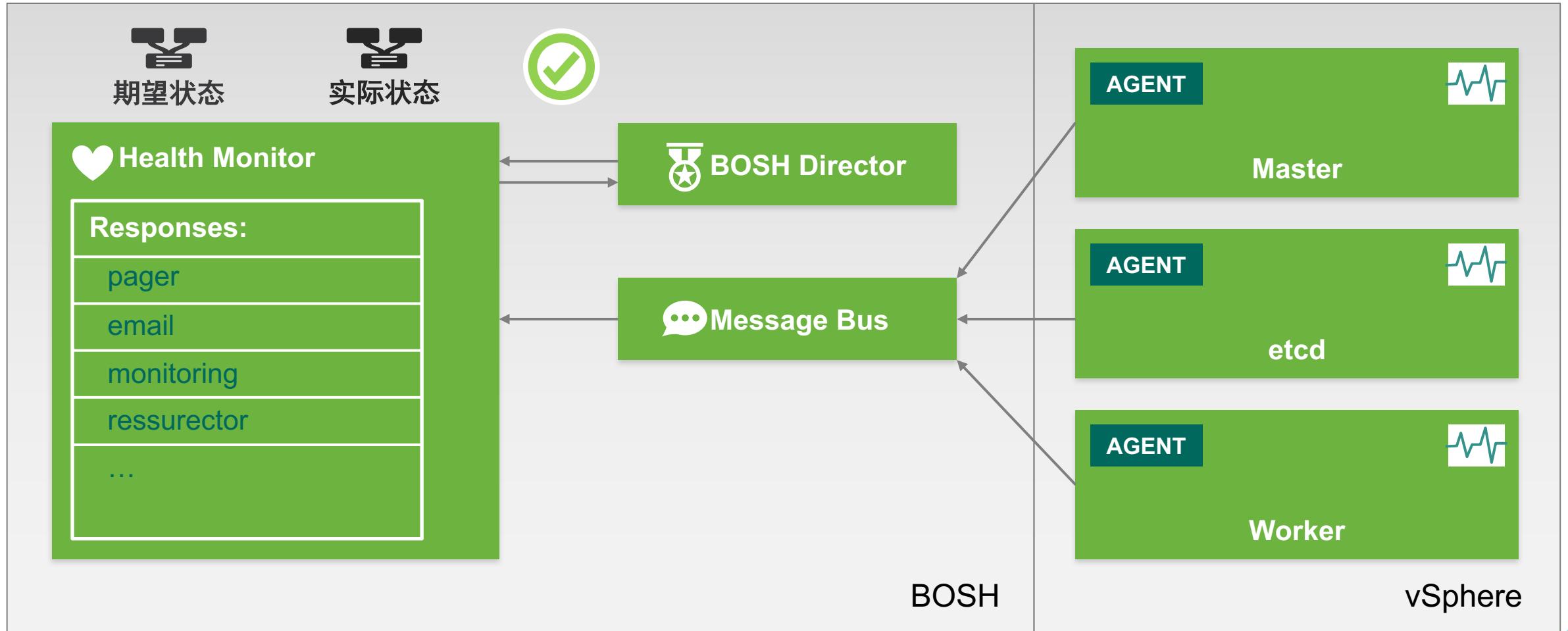
BOSH部署Kubernetes的方式



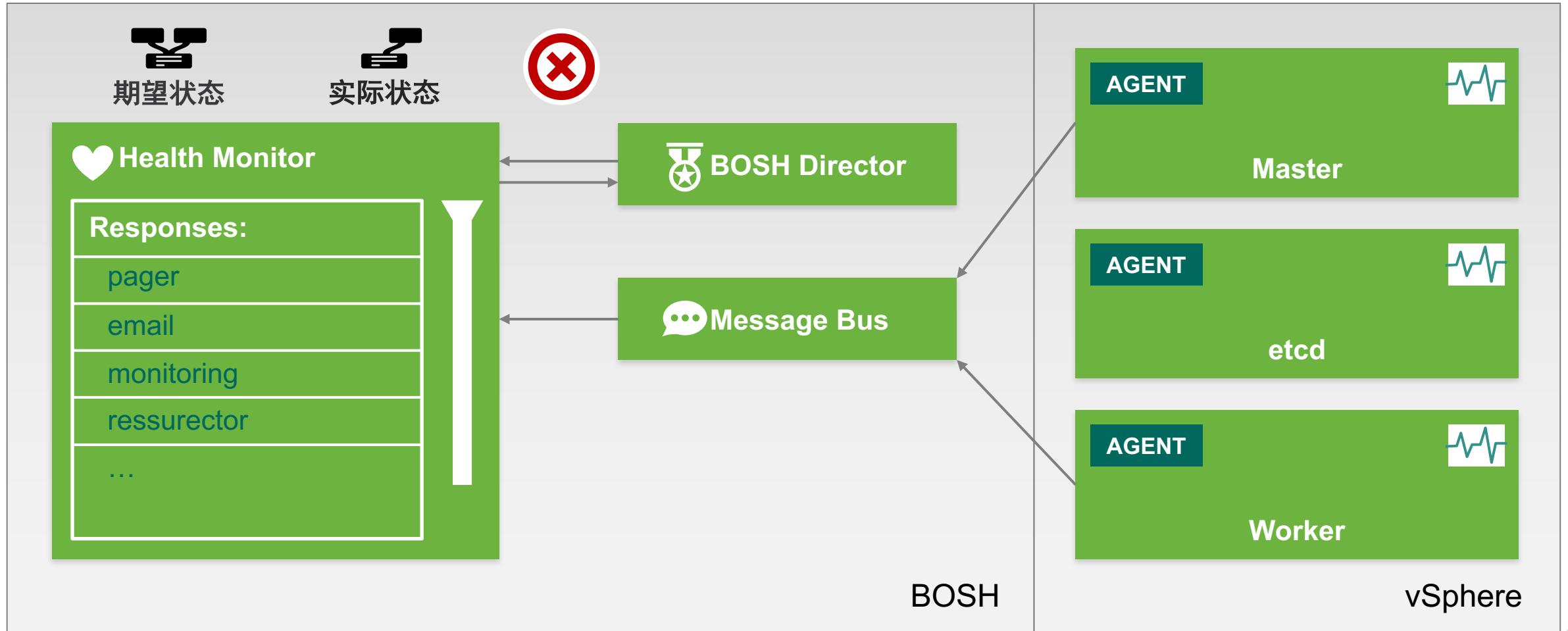
BOSH部署Kubernetes的方式



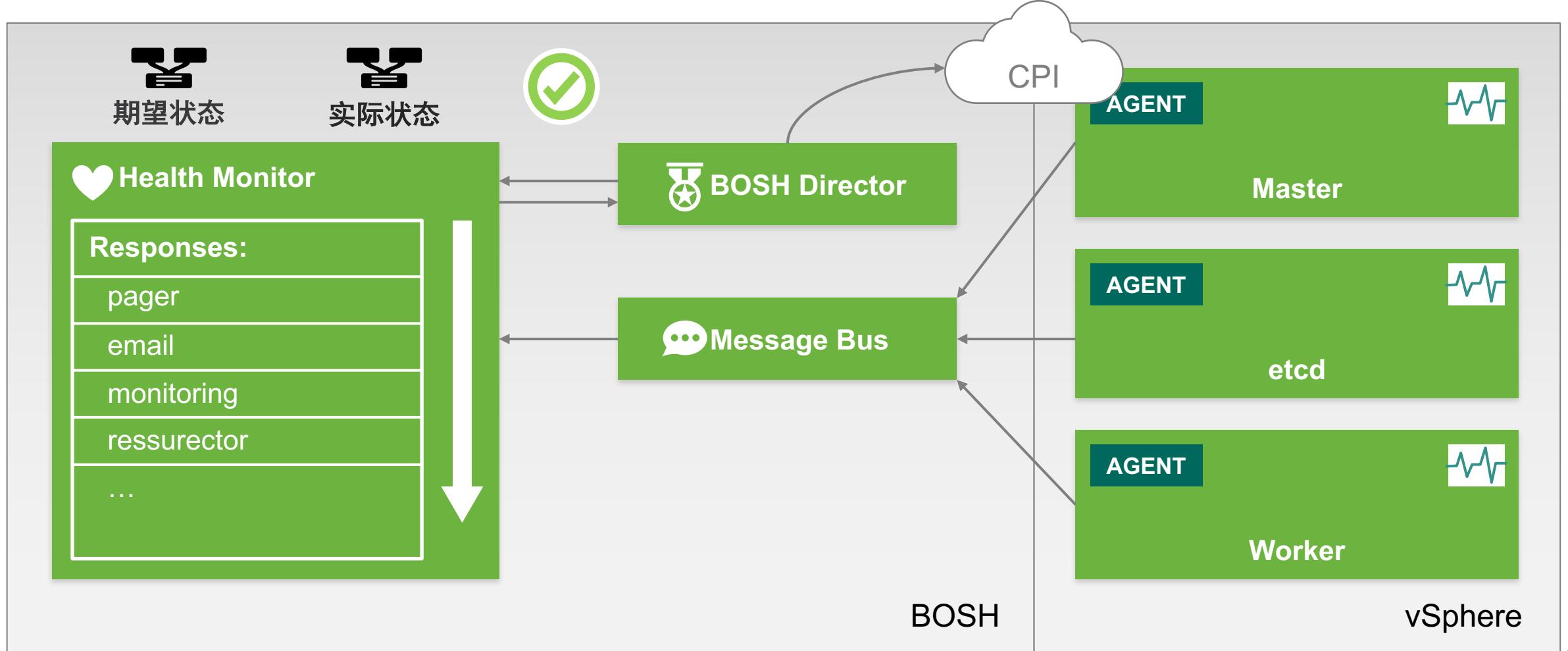
K8s 集群健康: 进程、虚机的监控



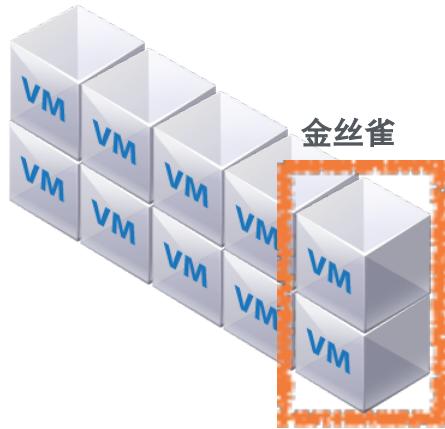
K8s 集群健康: 虚机和监控



K8s 集群健康: 虚机和监控



BOSH使K8s 集群可滚动升级: 金丝雀部署

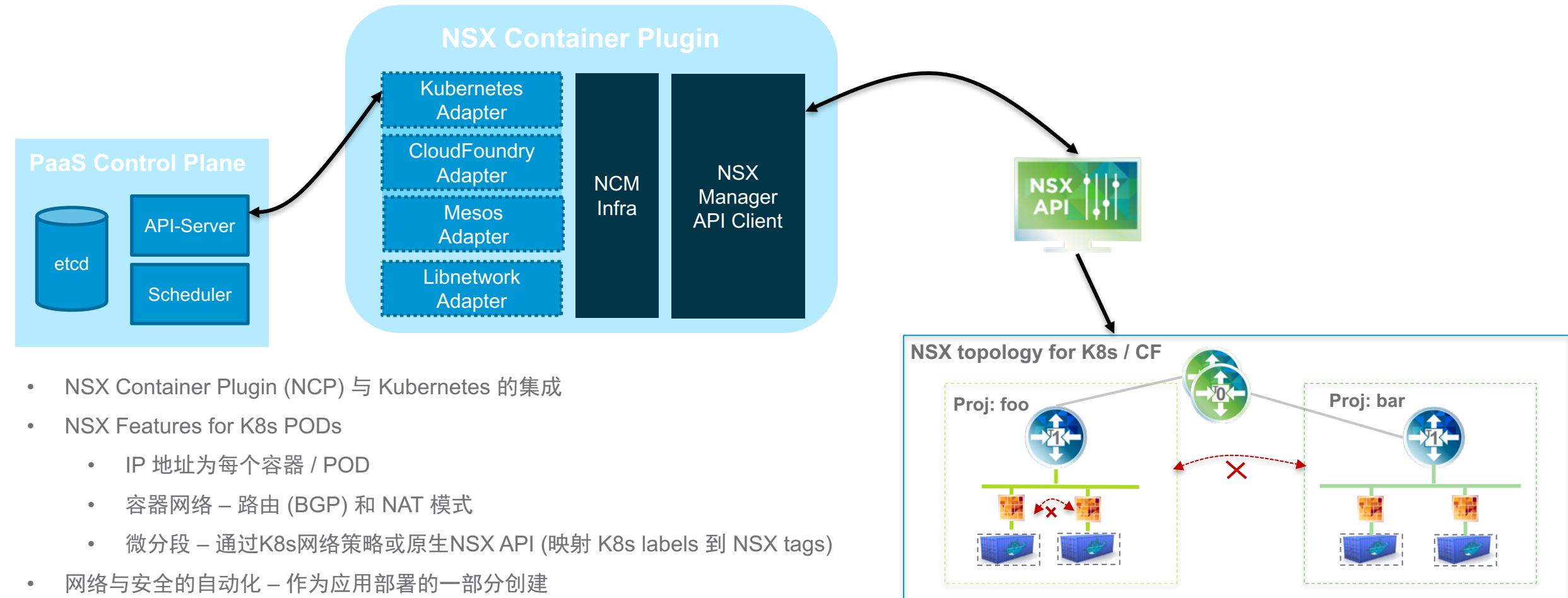


v1.0



v1.1

NSX-T 集成



Pivotal Cloud Foundry

周晖，Pivotal云计算首席架构师

PCF V2.0的逻辑架构

开发者交付

平台功能

PCF的三大应用平台

PCF的共享服务

vFORUM



PKS
(Pivotal Container Service)

PAS
(Pivotal Application Service)

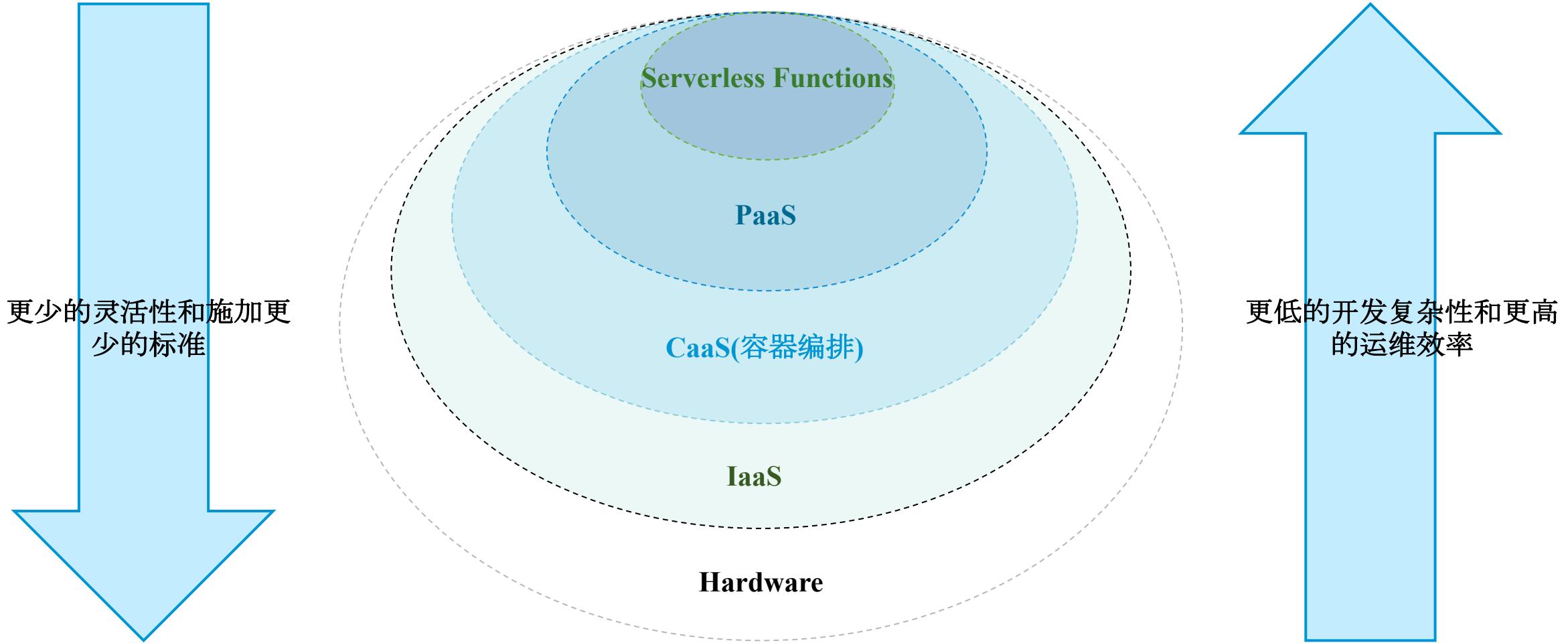
PFS
(Pivotal Function As A Service)

共享的服务

共享的安全性机制

共享的网络环境和策略

PCF V2



战略目标: 根据技术可行性，把各种工作负载放在不同的平台层

Pivotal Cloud Foundry 覆盖 CaaS/PaaS/FaaS

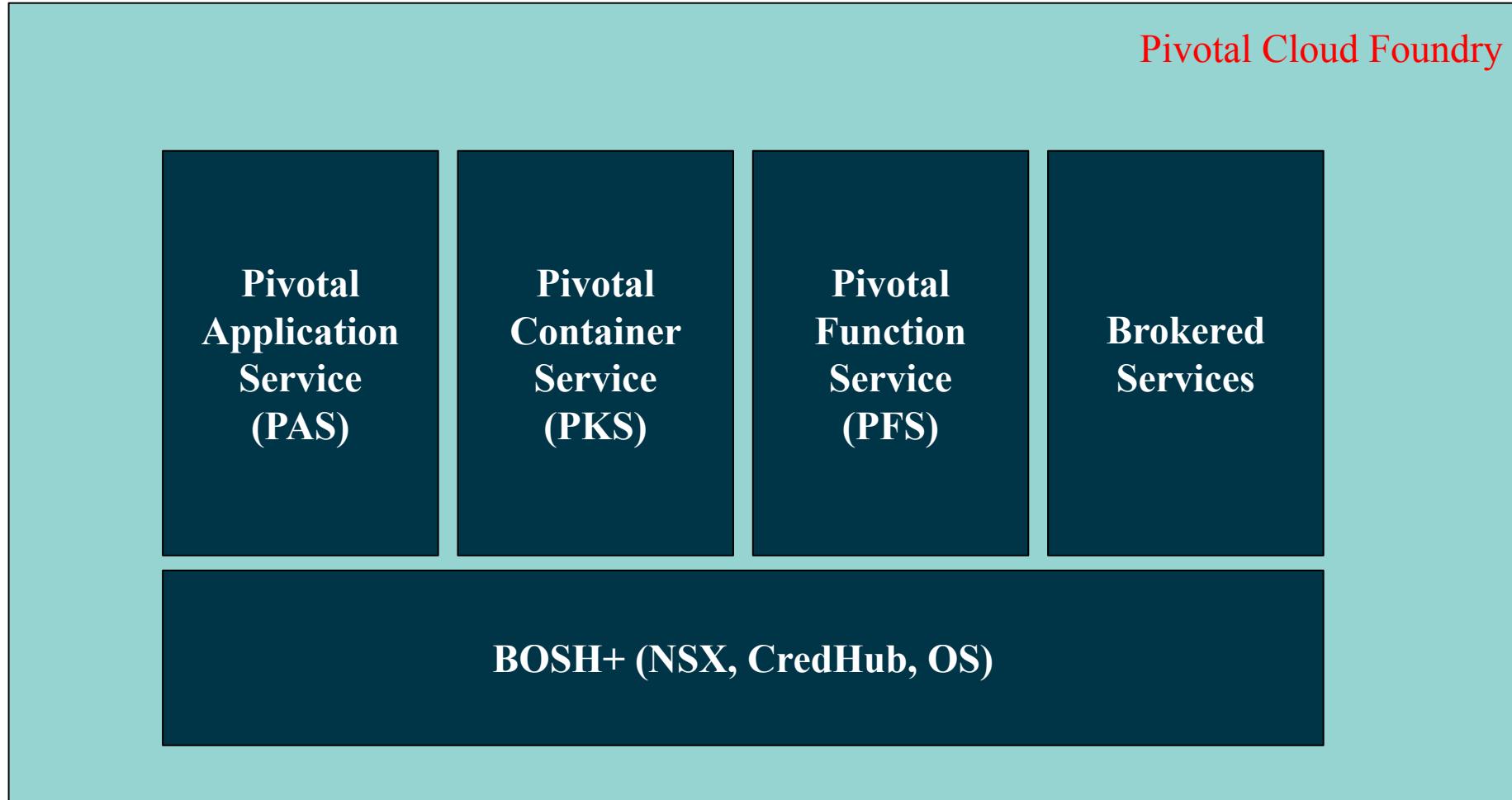
PCF 1.X

ERT

Services

BOSH

PCF 2.0 架构



Pivotal Application Service 2.0

Selected Highlights

- 深度NSX-T集成 (container networking, security groups, isolation segments, vSphere CPI)
- 提供路由服务，定制路由策略
- PCF调度器，支撑任务
- PCF Healthwatch: Dashboards + KPIs to monitor platform health
- Apps Manager:更细颗粒度控制应用
- BOSH DNS
- Azure Stack [beta]

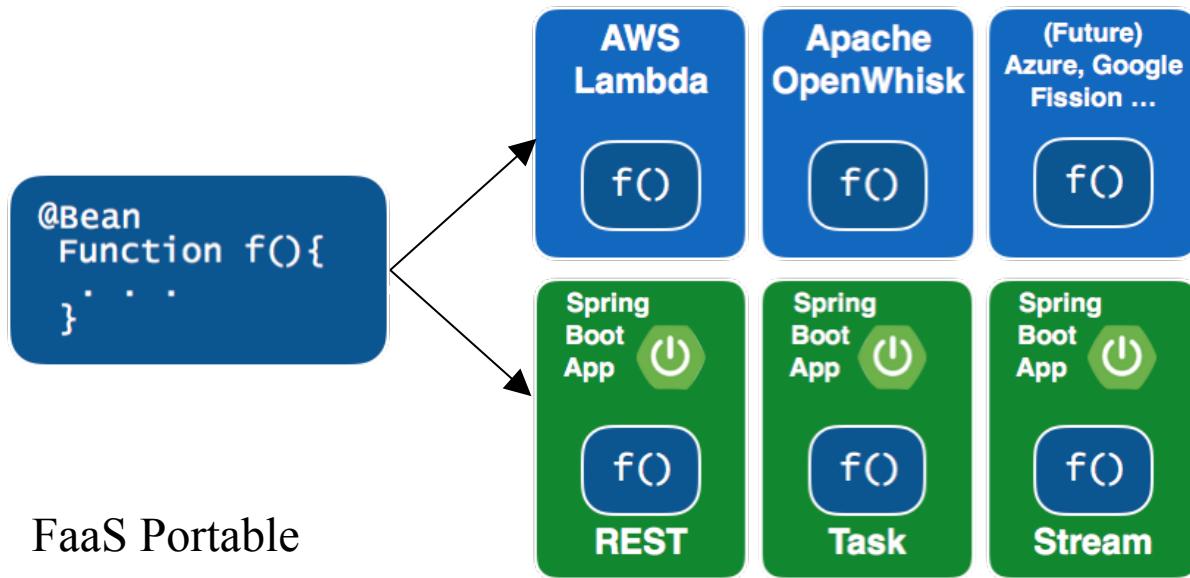
PAS for Windows

Includes Windows Server Containers
offered on Windows Server 2016

- Windows 2016运行时安装包
- 支持Windows Server的虚机模板
- 把PCF和容器技术引入Windows环境: CPU + network隔离, 基于CPU的弹性伸缩, CredHub encrypted service creds, Diego SSH (i.e. cf ssh)
- 提供安装包, 使得应用OS可以平滑的从Windows 2012R2升级到2012R2 to 2016

Pivotal Function Service (PFS—Pivotal函数服务)

A service for running Functions



FaaS Portable
And run in Spring Boot
REST, Tasks, or Streams

功能

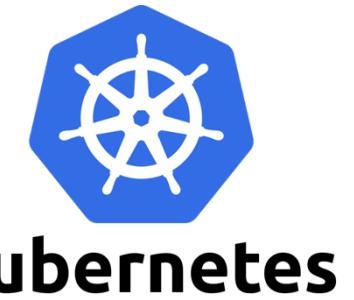
- 原生支持Kubernetes
- 支持多种语言 - Shell, Node.js, Spring/Java, Python
- 基于Spring开源—Spring Function
- 工作负载动态的装入暖容器
- 事件流- 支持分区、窗口化
- 可以插拔的消息机制 - Kafka, AWS Kinesis, Google Pub/Sub, RabbitMQ

VMware 用户在 Kubernetes 上的案例分享

张鑫，才云科技创始人兼 CEO

VMware 与 Kubernetes 容器平台的共生与互补

- 资源管理 + 服务管理
 - VMware 提供计算、网络、存储解决方案
 - Kubernetes 提供应用、开发流程、业务运维流程的管理
 - Harbor 提供稳定的镜像存储与安全把控
- 细粒度物理资源划分支持多集群统一管理
 - 多集群顺应企业的组织架构划分与多租户强隔离
- 更强的风险控制
 - 降低操作风险
 - 更强的业务隔离



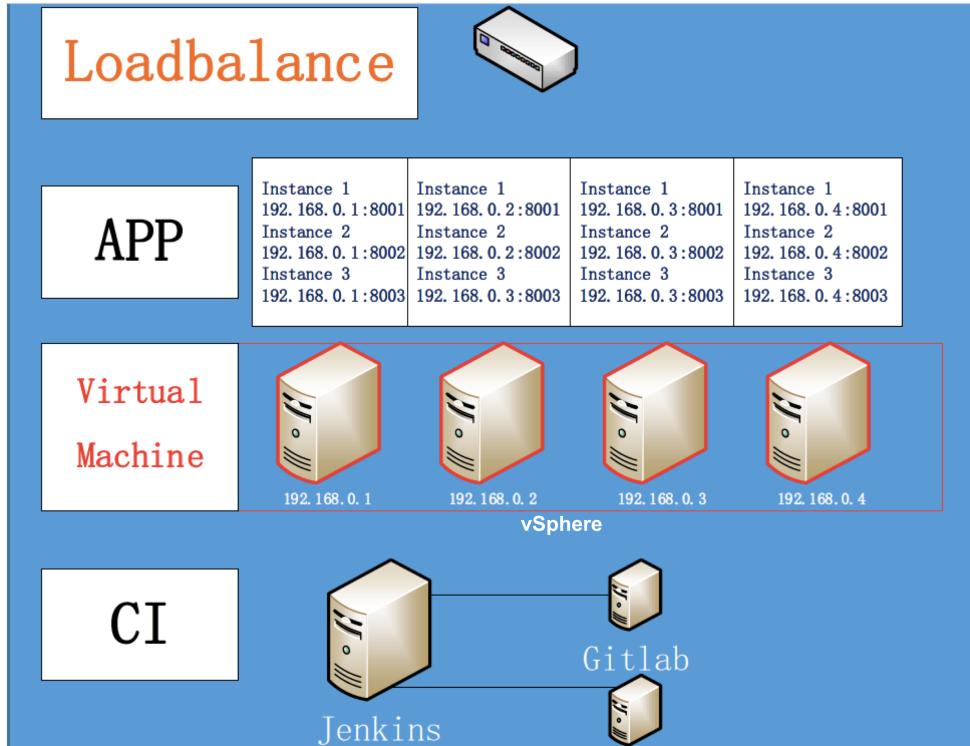
VMware 与 Kubernetes 的案例 - 某大型酒店、旅游管理集团

用户痛点：

- 系统架构缺乏弹性
- 开发、部署、发布缓慢、易错
- 服务稳定需要大量人工保障

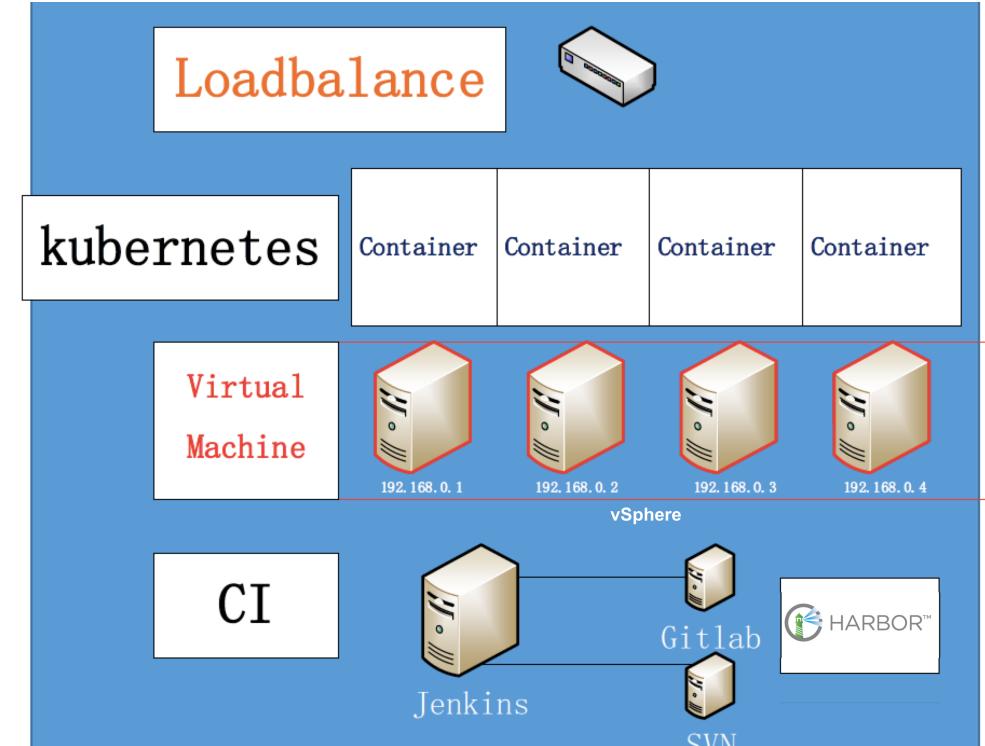
解决方案：

- 业务快速部署、销毁、重建
- 自动化应用运维
- 应用高可用、可扩展
- IaaS + PaaS = 集群管理一体化



vFORUM

Before



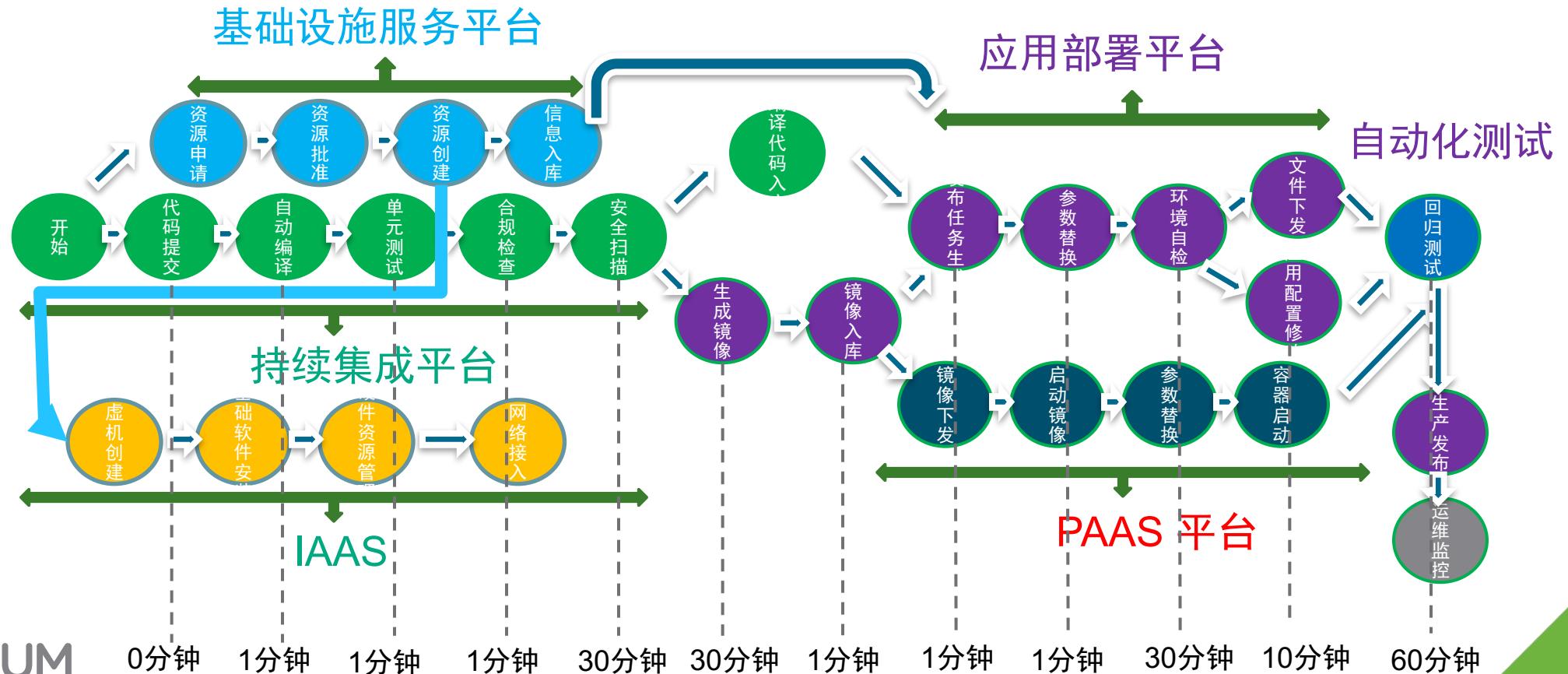
After

VMware 与 Kubernetes 的案例 - 汽车行业某龙头厂商

用户痛点：

- 业务系统笨重、应用上线慢、开发运维缺乏联动

解决方案：

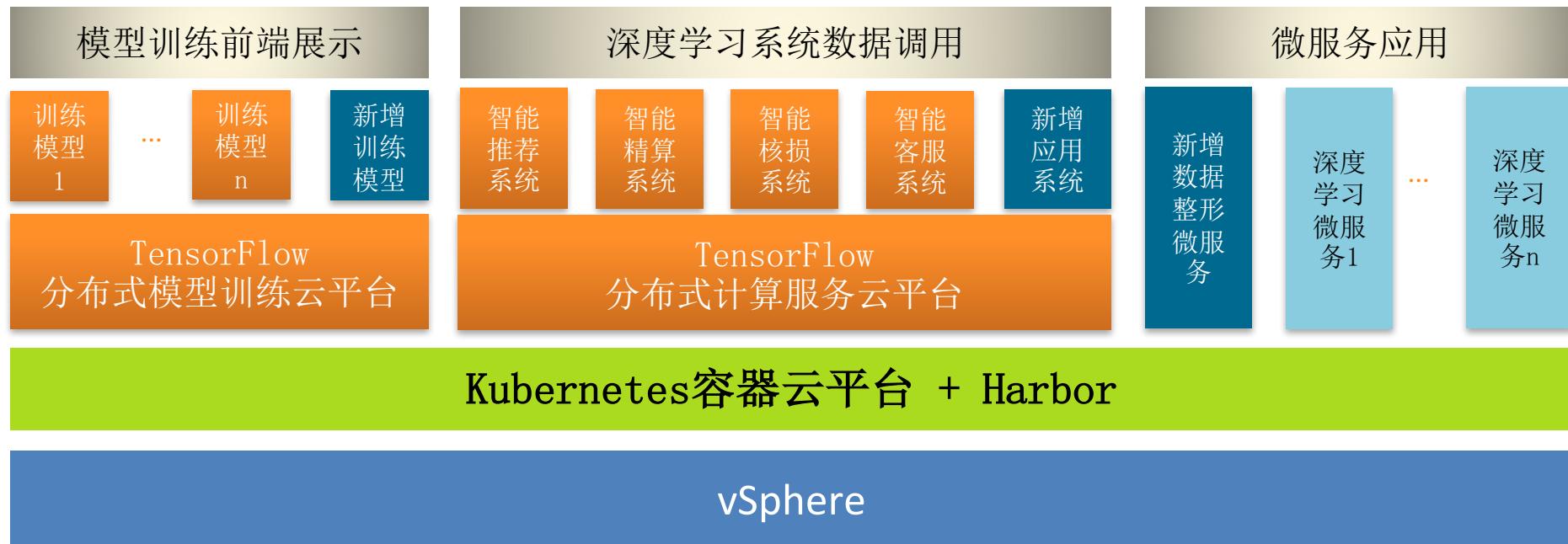


VMware 与 Kubernetes 的案例 - 金融行业某大型国企

用户痛点：

- 数据量大、异构明显，难以挖掘数据价值，缺乏算法与算力
- 线上生产业务系统与数据分析业务分别管理，运维复杂，资源利用率低

解决方案：



Thank You

vFORUM
2017

vmware®