

IBM开源技术微讲堂 Kubernetes系列第十讲

Kubernetes企业实践——某银行PaaS上云之路

2017.12.28

“Kubernetes”系列公开课

- 每周四晚8点档

1. Kubernetes 初探
2. 上手 Kubernetes
3. Kubernetes 的资源调度
4. Kubernetes 的运行时
5. Kubernetes 的网络管理
6. Kubernetes 的存储管理
7. Kubernetes 的日志与监控
8. Kubernetes 的应用部署
9. 扩展 Kubernetes 生态
10. **Kubernetes 的企业实践**

课程Wiki: <http://ibm.biz/opentech-ma>

某银行PaaS上云之路

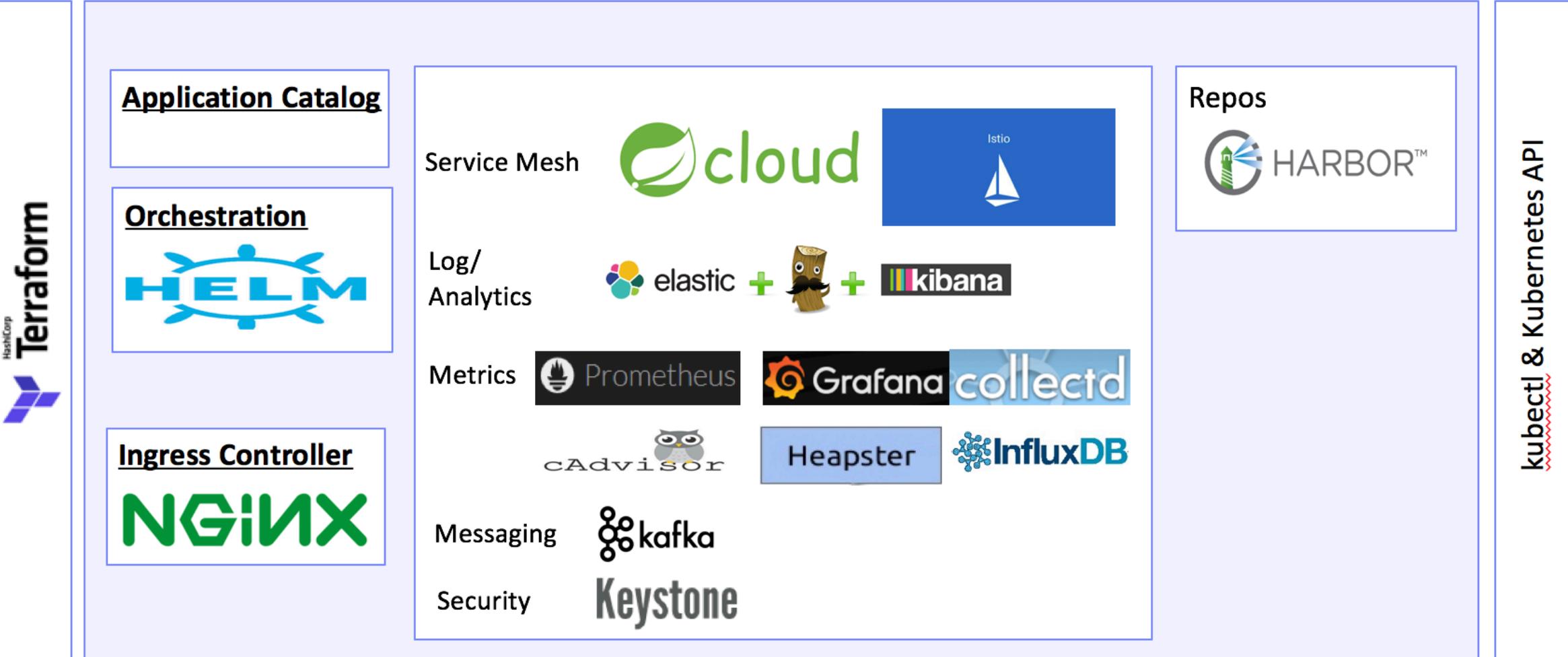
Guang Ya Liu (liugya@cn.ibm.com)

Istio Maintainer

Kubernetes Member

Mesos Committer & PMC Member

Unified User/Administration Portal



Container Management (Docker, Kubernetes, Calico)



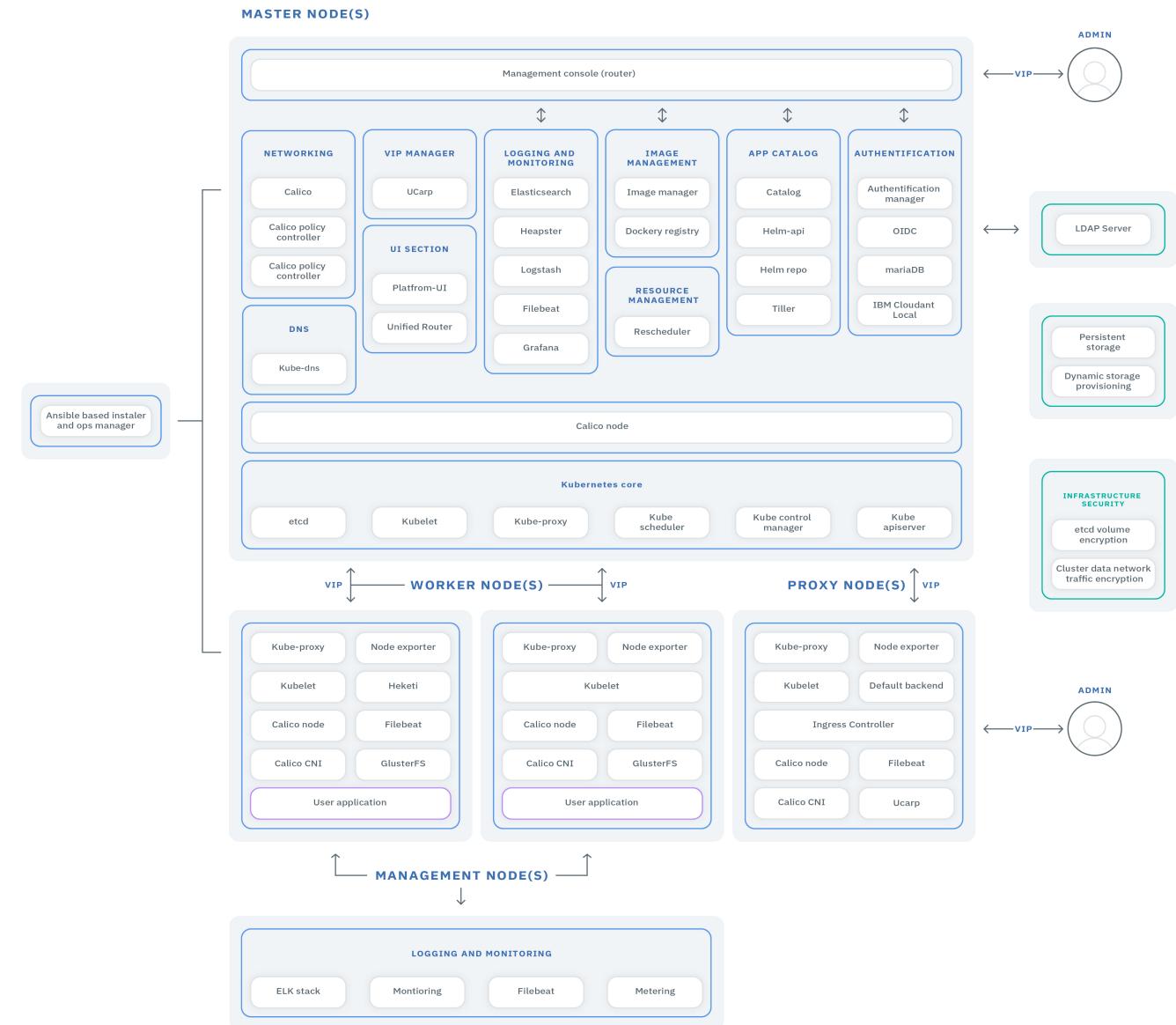
- 四种节点角色
- Master
 - Worker
 - Proxy
 - Management

```
[master]
9.21.53.13

[worker]
9.21.53.14
9.21.53.15

[proxy]
9.21.53.16

[management]
9.21.53.17
```



- 把常用的应用放在PaaS云应用商店，简化安装部署。
- 借助Terraform实现虚拟机和容器混合应用管理
- 支持胖模板和瘦模板
 - 胖模板包含镜像文件

The screenshot shows the IBM Cloud Private Catalog interface. At the top, there's a navigation bar with the text "IBM Cloud Private" and a "Catalog" section. Below the navigation bar is a search bar with a magnifying glass icon and a "Filter" button. The main area is titled "Helm charts" and contains the following application entries:

应用名称	描述
ibm-cloudant-dev	Cloudant for Linux.
ibm-db2warehouse-dev	Db2 Warehouse Developer-C for Non-Production v2.0.0
ibm-iclogging	Log storage and search management solution
ibm-lsfce-dev	IBM LSF Community Edition cluster with Application Center GUI
ibm-datapower-dev	IBM DataPower Gateway chart
ibm-dsm-dev	IBM Data Server Manager Developer-C Edition. Note that there can only be one DSM deployed per
ibm-icpmonitoring	IBM monitoring service in private cloud
ibm-microservicebuilder-fabric	Microservice Builder Fabric
ibm-db2oltp-dev	IBM Db2 Developer-C Edition 11.1.2.2
ibm-dsx-dev	IBM Data Science Experience (DSX) Developer Edition brings together best of breed open source
ibm-integration-bus-dev	IBM Integration Bus for application integration, routing and transformation
ibm-microservicebuilder-pipeline	Microservice Builder Pipeline

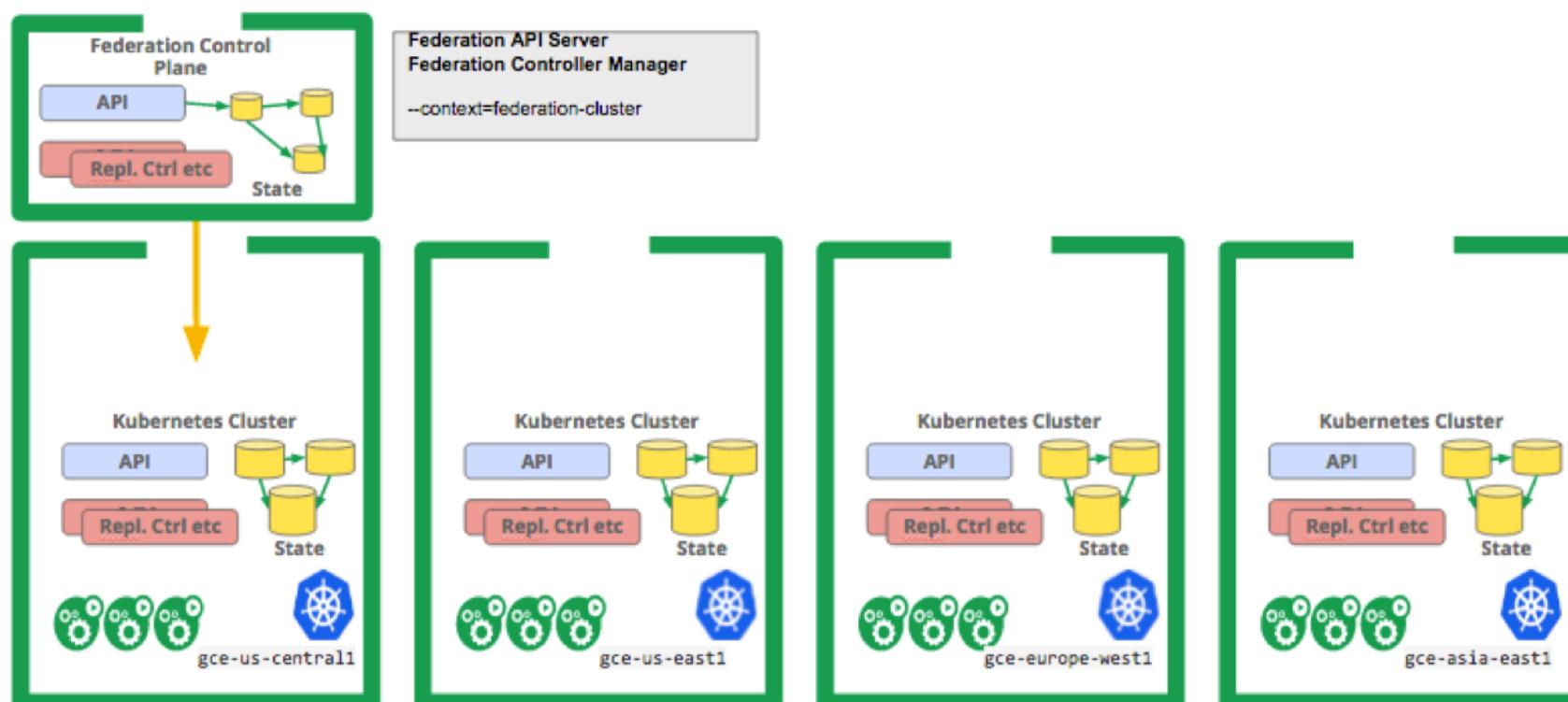
1. 基于CPU等系统核心KPI使用率弹性伸缩
 - Kubernetes原生功能
2. 基于用户自定义的KPI弹性伸缩
 - 借助第三方资源搜集系统实现
 - [kubernetes-incubator/custom-metrics-apiserver](#)
3. 基于时间弹性伸缩
 - 借助Kubernetes CronJob实现
 - 指定弹性伸缩的时间区域
 - 例如早上8: 00增加容器
 - 晚上8: 00删除容器

```
apiVersion: batch/v2alpha1
kind: CronJob
metadata:
  name: scale-up
  namespace: default
spec:
  schedule: "00 08 * * *" # Run at 8:00
  # PM every day
  jobTemplate:
    spec:
      template:
        spec:
          containers:
            - name: scale
              image: gyliu/kubectl:v1.7.3
              command:
                - kubectl.sh
                - kubectl
                - scale
                - --replicas=3
                - deployment/my-nginx
  restartPolicy: OnFailure
```

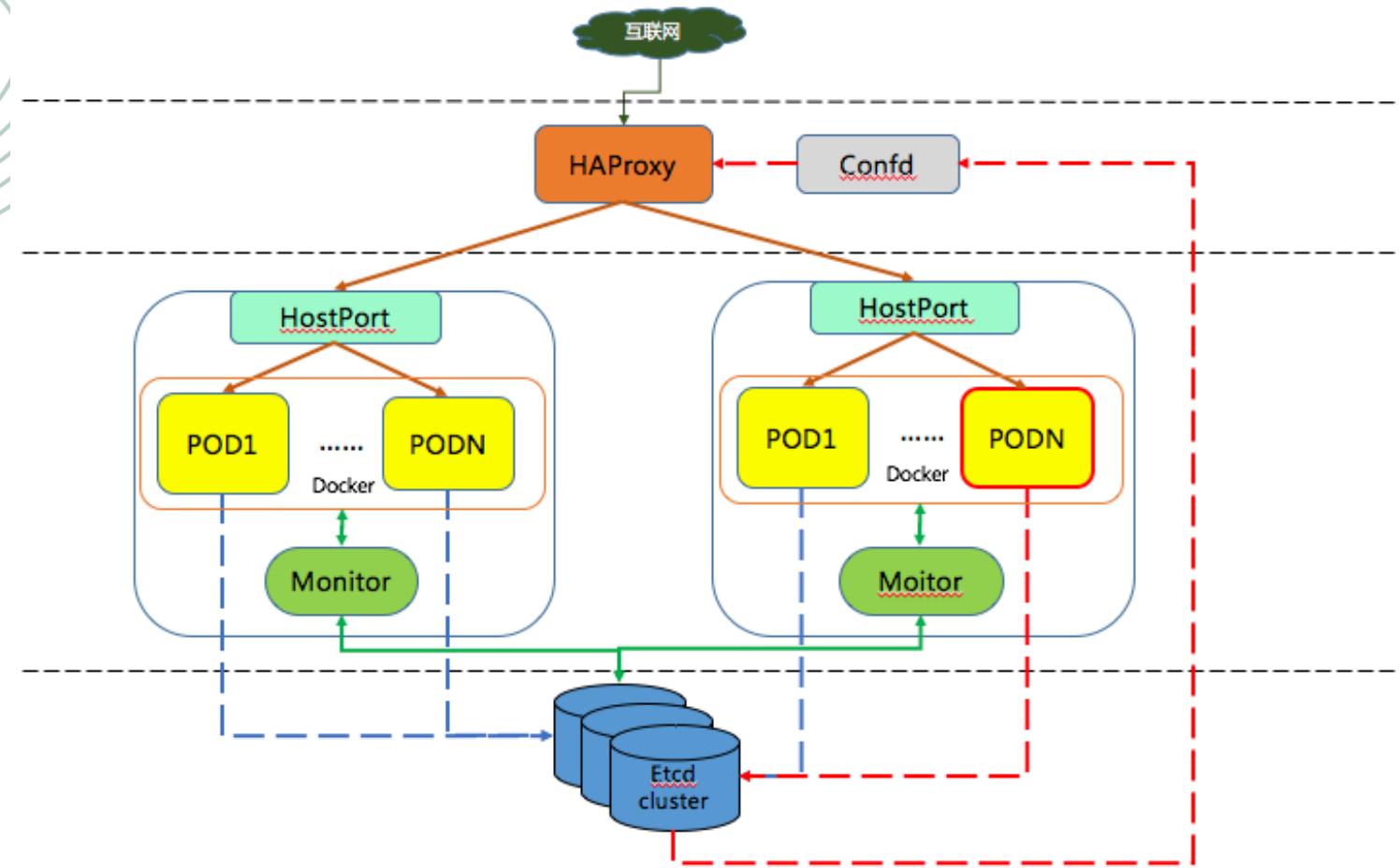
集成了Kubernetes的federation功能

- a) 跨集群部署应用
- b) 多集群负载均衡
- c) 容器跨集群漂移

➤ 当一个集群宕机后，该集群的容器会自动漂移到正常的集群。



- HAProxy动态路由至应用容器
- Confd监控etcd发现应用容器
- 容器生命周期管理
 - 容器启动时将自身信息写入etcd
 - 容器停止时将信息从etcd删除
- 注册监控模块监控并同步本机容器信息到etcd



Istio是由IBM, Google, Lyft联合研发的微服务治理新项目。

流量管理: 控制服务之间的流量和API调用的流向，使得调用更可靠，并使网络在恶劣情况下更加健壮。

可观察性: 了解服务之间的依赖关系，以及它们之间流量的本质和流向，从而提供快速识别问题的能力。

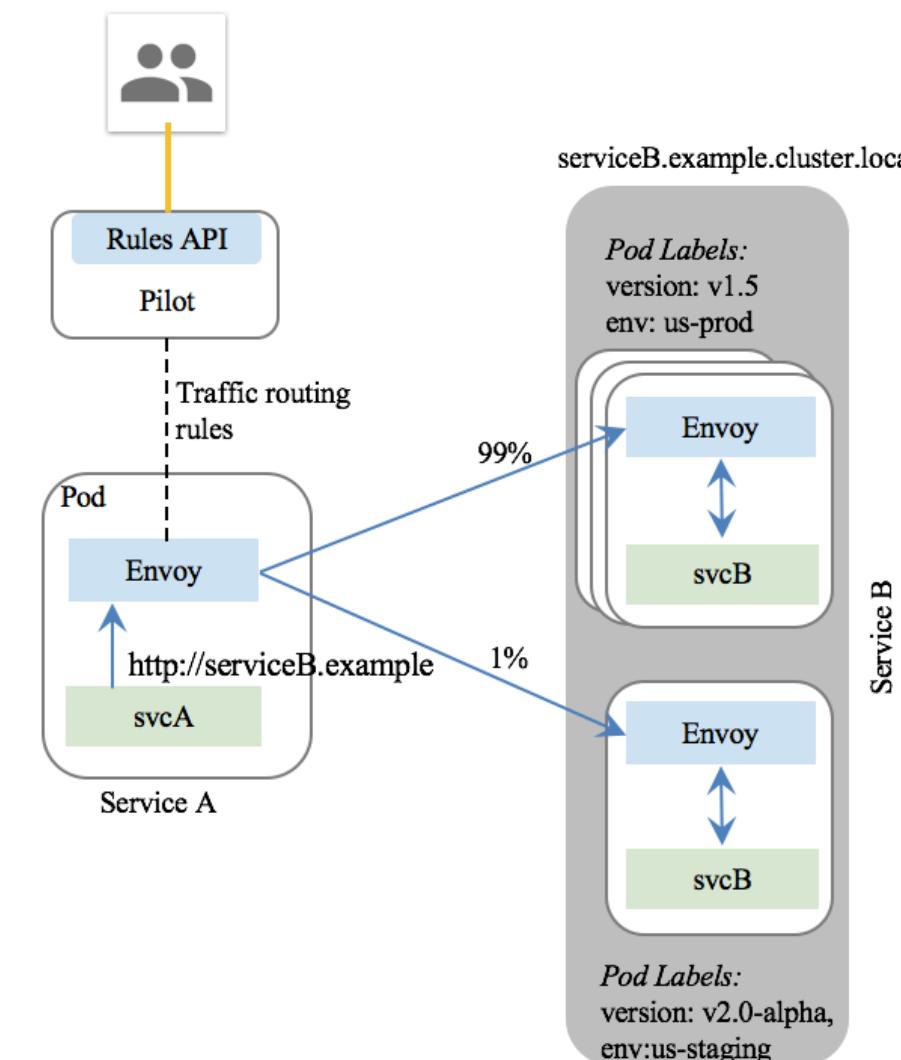
策略执行: 将组织策略应用于服务之间的互动，确保访问策略得以执行，资源在消费者之间良好分配。策略的更改是通过配置网格而不是修改应用程序代码。

服务身份和安全: 为网格中的服务提供可验证身份，并提供保护服务流量的能力，使其可以在不同可信度的网络上流转。

平台支持: Istio旨在各种环境中运行，包括跨云，预置，Kubernetes，Mesos等。目前专注于Kubernetes，但很快将支持其他环境。

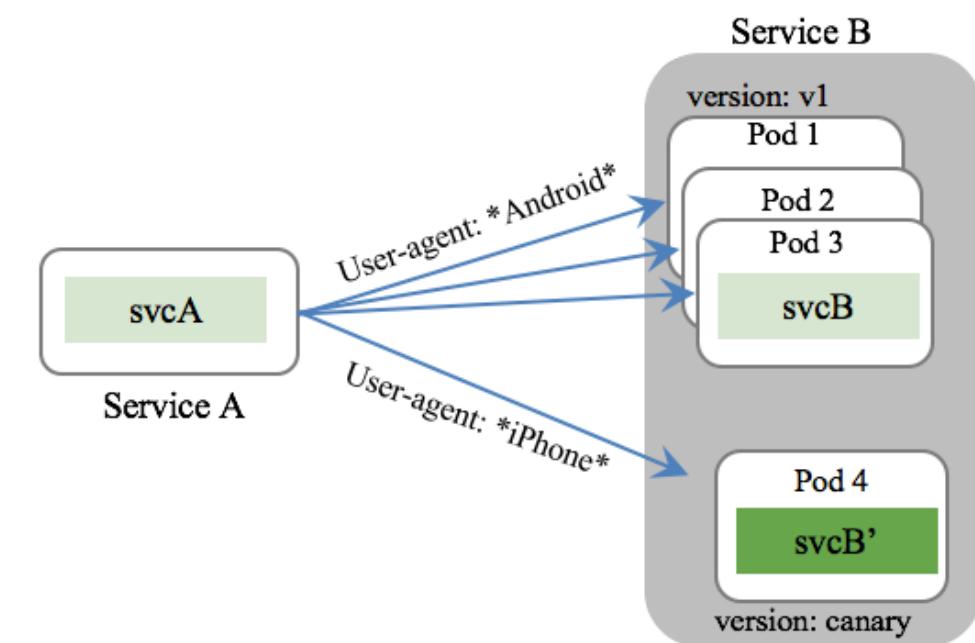
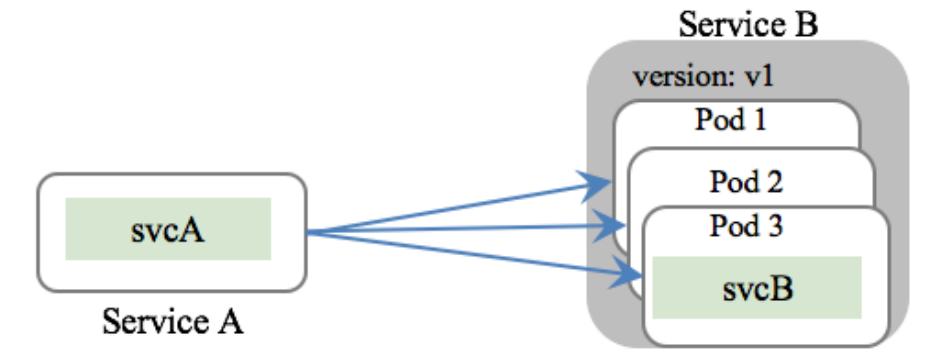
集成和定制: 策略执行组件可以扩展和定制，以便与现有的ACL，日志，监控，配额，审核等解决方案集成。

// A simple traffic splitting rule
destination: serviceB.example.cluster.local
match:
 source: serviceA.example.cluster.local
 route:
 - tags:
 version: v1.5
 env: us-prod
 weight: 99
 - tags:
 version: v2.0-alpha
 env: us-staging
 weight: 1



流量亲和性

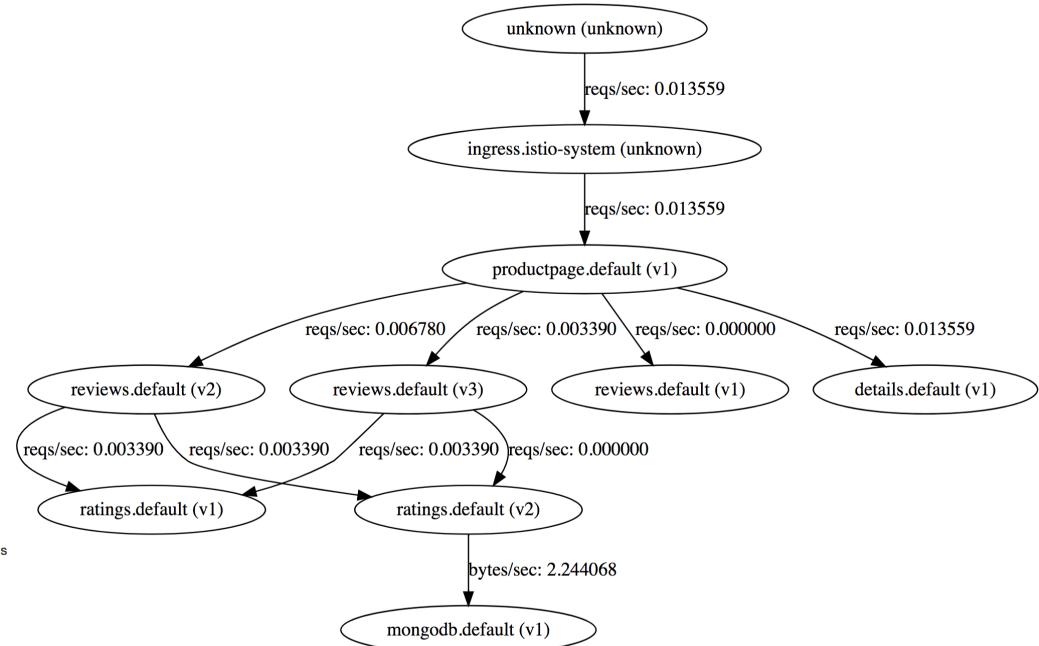
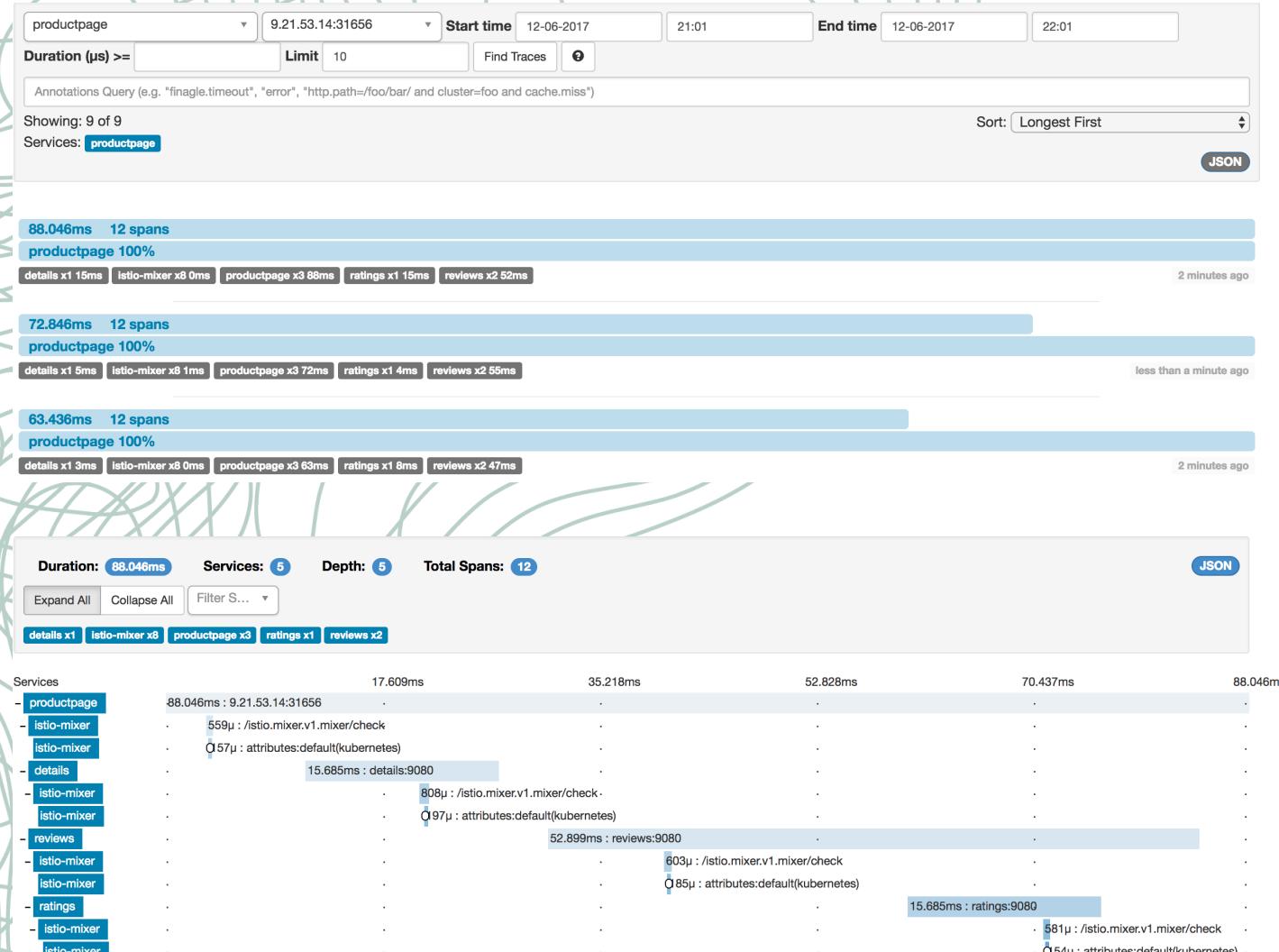
```
// Content-based traffic steering rule
destination:
  serviceB.example.cluster.local
match:
  httpHeaders:
    user-agent:
      regex: ^(.*)?(iPhone)(;.*?)$
precedence: 2
route:
- tags:
  version: canary
```



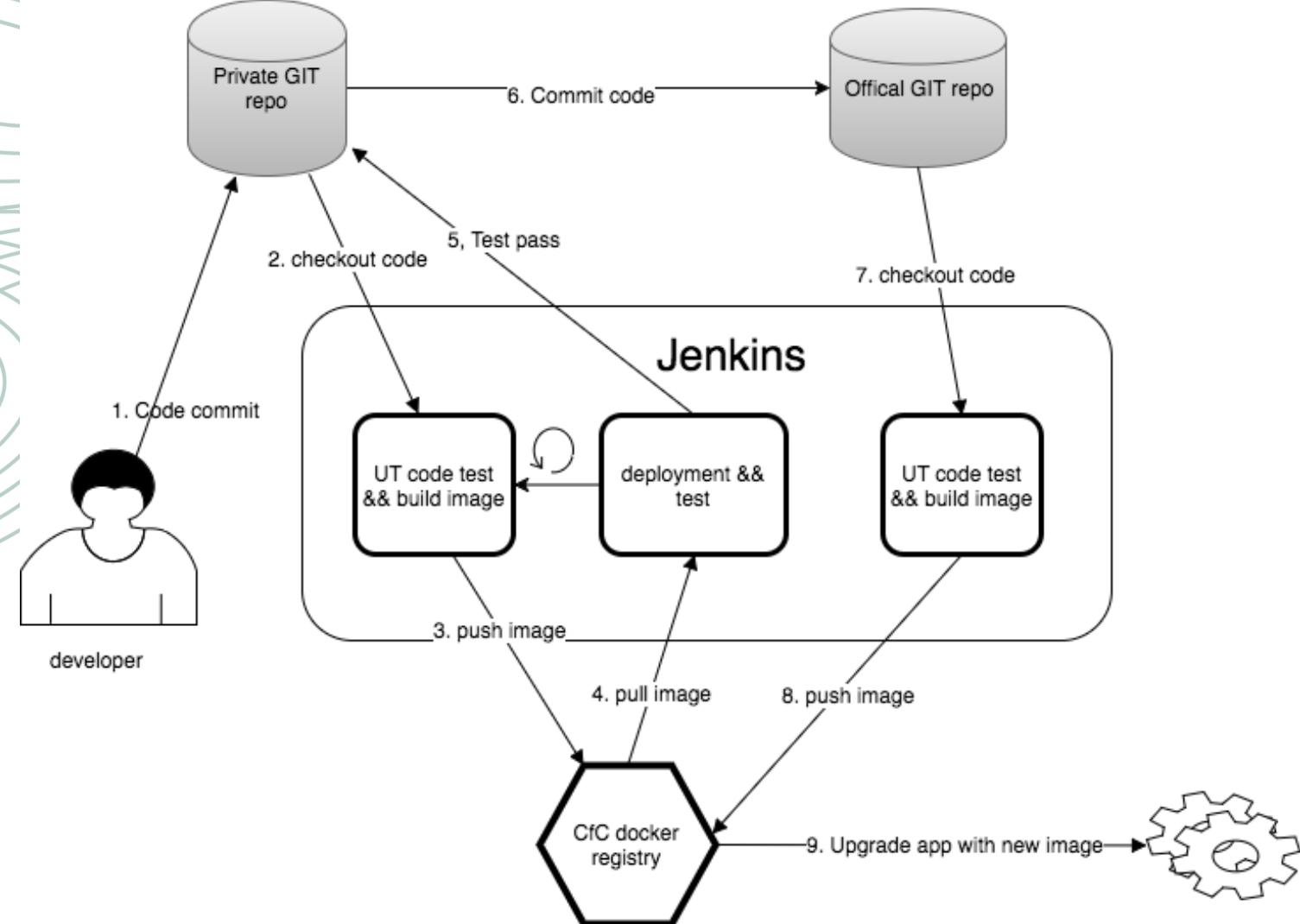
IBM PaaS云微服务治理

developer.ibm.com/code

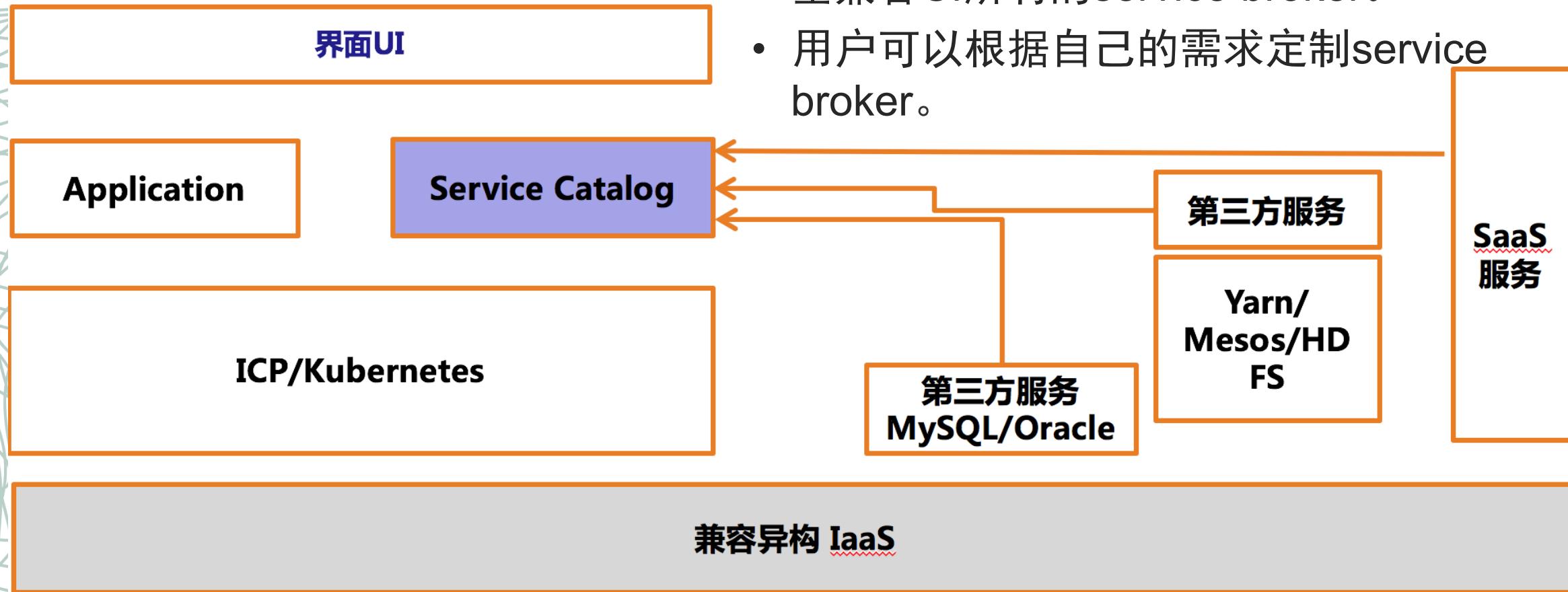
可视化服务拓扑，调用链跟踪

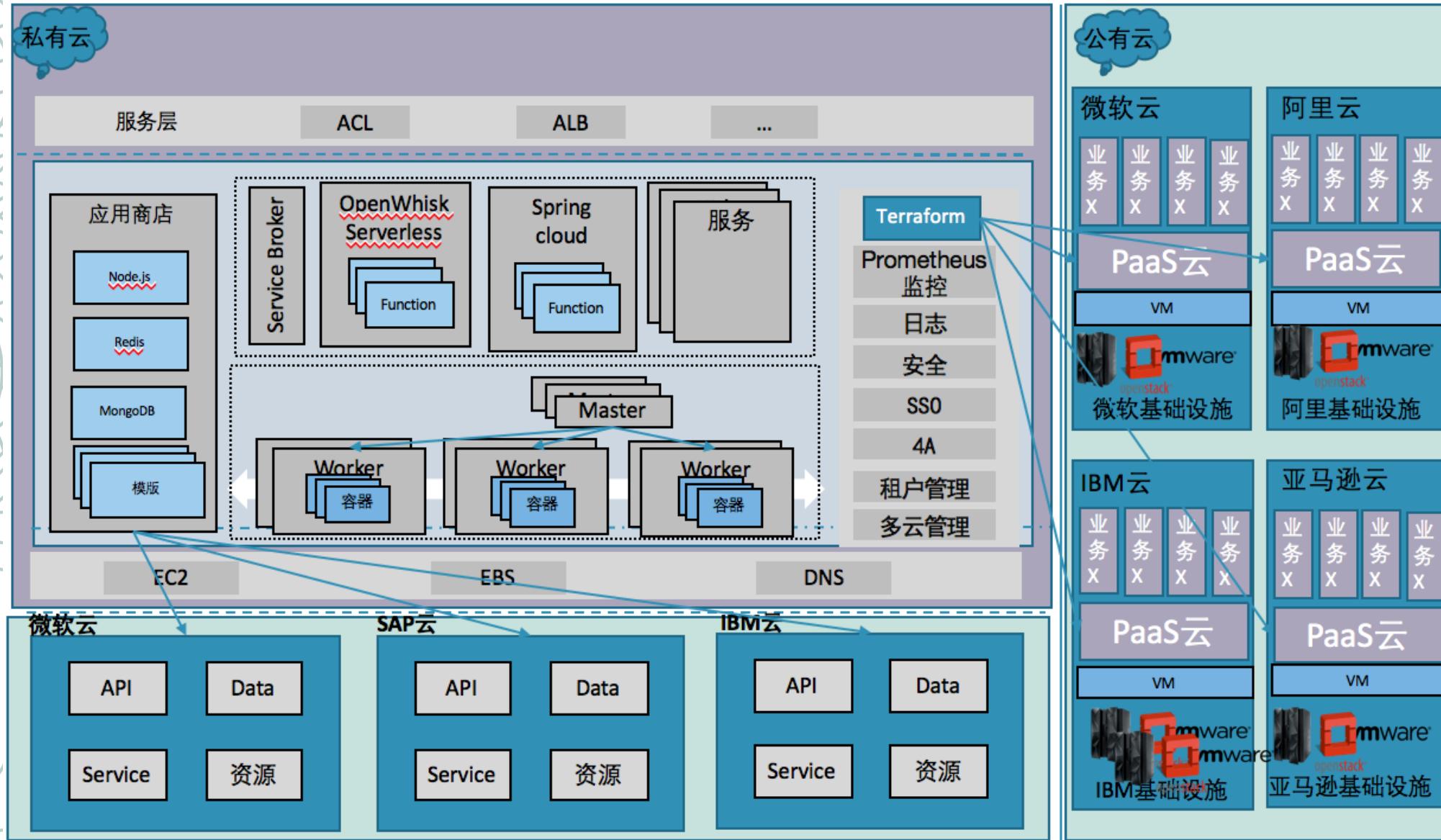


代码提交自动触发镜像构建
和应用部署



- Service Catalog是IBM在Kubernetes社区发起的外部服务集成的项目。
- 通过Service Catalog和外部服务集成，完全兼容Cf所有的service broker。
- 用户可以根据自己的需求定制service broker。





- 安装升级**: 通过容器管理所有的PaaS云系统服务，便于安装，升级
- 弹性伸缩**: 基于时间
- 多集群管理**: 可以实现多集群应用部署和跨集群负载均衡。
- DevOps**: 通过集成Jenkins实现了DevOps的功能，包括代码托管，镜像自动编译，应用自动部署，自动产生DevOps分析报告的功能。
- 微服务治理**: 通过Istio实现了微服务治理的功能，主要包括分流，限流，熔断，服务发现，服务跟踪，服务拓扑结构展示等功能。
- 外部服务集成**: 通过service catalog实现了和外部应用对接的能力。例如ICP可以通过service catalog对接外部的一些数据库服务，第三方PaaS平台上的一些服务等等。
- 多云集成**: 通过集成Terraform实现了对不同云平台的集成。

IBM Cloud Private

developer.ibm.com/code

Application Development,
Integration, Operations &
Management



IBM DevOps



Microservices



Hybrid Cloud Management

Next Generation
Middleware, Data,
Integration & Analytics



IBM MQ



Apache
Open Whisk

IBM Cloud private Platform

Kubernetes-based Platform

Multiple open compute models
IaaS Automation, Containers, PaaS & Functions

Software & Policy driven Network & Storage

Autoscaling & Automatic Application Recovery

Multi-site HA/DR features



kubernetes



Enterprise
Infrastructure



z Systems



Solution Architectures & Best Practices

Integration Content

Middleware, Data, management & Analytics Content

Continuous
Delivery

Image
Registry

Continuous
Integration

App
Catalog

App
Health

App Log
Analysis

API
Mgmt

Continuous
Availability

Monitoring

Log
Analysis

Audting

Alerting

Metering

Continuous
Security

Authentication

RBAC

Certificate
Store

Key Store
Image
Vulnerability

Cluster

kubernetes
apiserver

kubernetes
scheduler

kubernetes
proxy

kubelet

etcd

Highly
Available

Masters
Virtual IP

Proxies
Virtual IP

Workers

Persistent
Storage

Network Mesh with Support for Tenant Isolation



Thanks