



从Kubernetes到谷歌容器集群管理的落地与演化

张鑫

才云科技 CEO





张鑫

CEO 创始人

- CMU博士
- 云计算和安全学术专家
- 谷歌数据中心(Borg)容器集群技术带头人
- 6次获谷歌副总裁总监奖
- 清华大学优秀毕业生
- 北京地区优秀毕业生
- 教育部优秀留学生
- Kubernetes最早贡献者



邓德源

CTO

- CMU硕士
- 谷歌资深工程师
- 开源容器集群项目顶级贡献者
- 谷歌私有云平台构筑者
- 代表中国队获得机器人人大赛金牌



唐鹏程

首席架构师

- CMU硕士
- 美国亚马逊工程师
- 开源容器集群项目贡献者
- Amazon实现容器化的技术骨干
- 精通容器技术与分布式系统



郑泽宇

首席科学家

- CMU硕士
- 谷歌资深工程师
- 大数据和机器学习专家
- 发明学习算法, 为谷歌创造千万美金营收
- 代表北大参加ACM竞赛



韩佳瑶

COO

- 匹兹堡大学博士
- 计算机、法律、历史、艺术多学位
- 美国成功连续创业者
- 创业、管理、市场经验丰富

201507 201508 201510 201511 201512 201605 201606 201608 201610 201611 201701 201701 201702 201702 201703 201703 201703

201507 才云科技CaiCloud成立

201508 获得赛伯乐数百万美金天使轮融资

201510 入选杭州市政府重点扶持计划

201511 发布容器云产品ClaaS1.0

201512 签约首个企业客户

201605 发布云产品Cargo, Kubernetes, Cyclone

201606 发布国内首个支持分布式TensorFlow的系统平台Clever

201608 正式成为美国CNCF/Linux Foundation官方合作伙伴

201610 获得第五届中国创新创业大赛总决赛第二名

201611 KubeCon主题演讲 - 美国西雅图站

201701 入选『微软加速器』

201701 入选『联想之星』

201702 发布容器云深度学习平台TaaS1.0

201702 获得经纬中国4000万A轮融资, 赛伯乐跟投

201703 发布容器云ClaaS2.0, 深度学习平台TaaS1.1

201703 KubeCon主题演讲 - 德国柏林站

201703 深度学习公有云平台发布

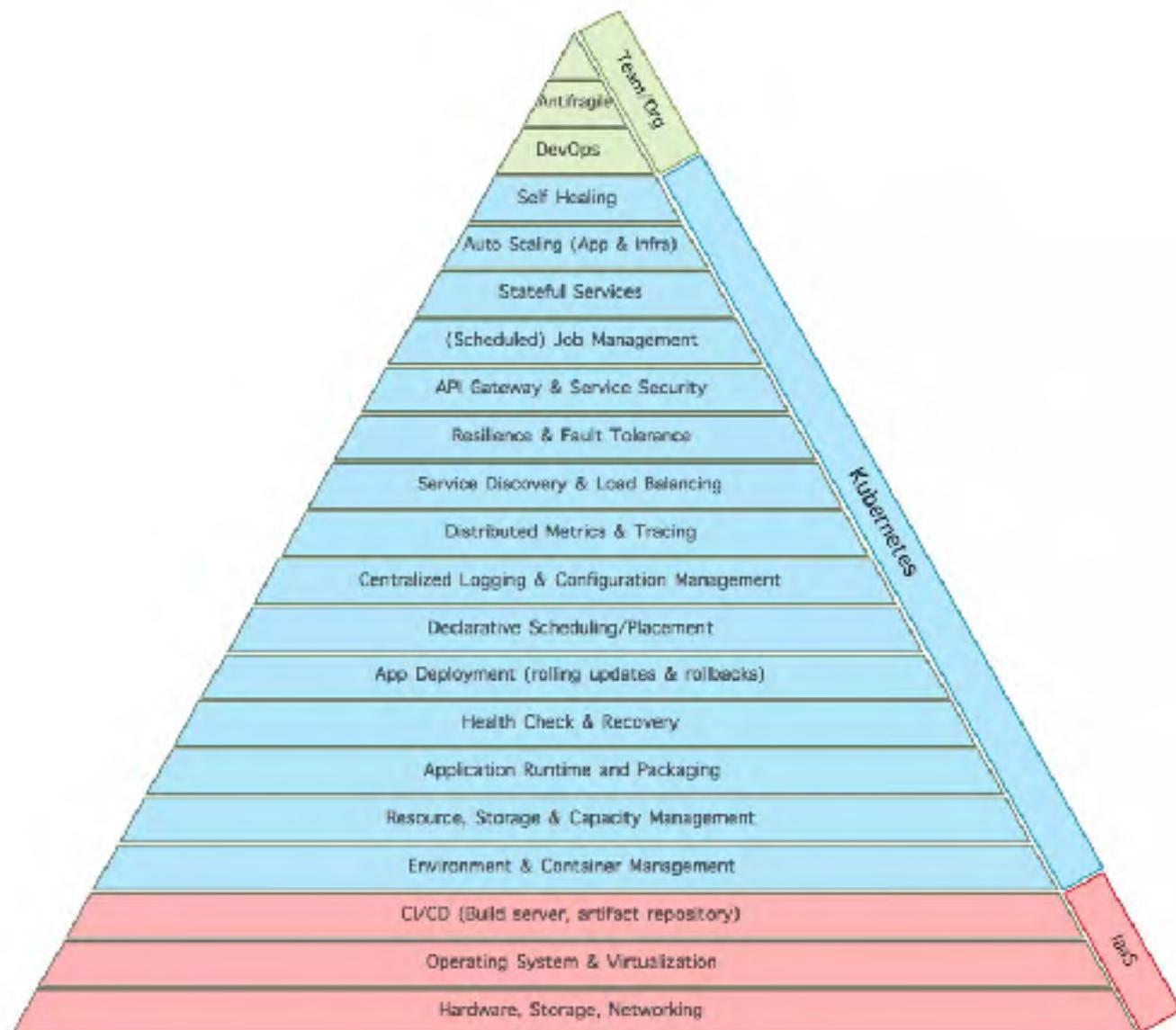
201703 Cyclone开源

What orchestrators do people use with Docker containers?



Docker usage report April 12, 2017

<https://sysdig.com/blog/sysdig-docker-usage-report-2017/>





Kubernetes vs Google Cluster Management

Kubernetes vs 传统行业

Kubernetes vs Big Data

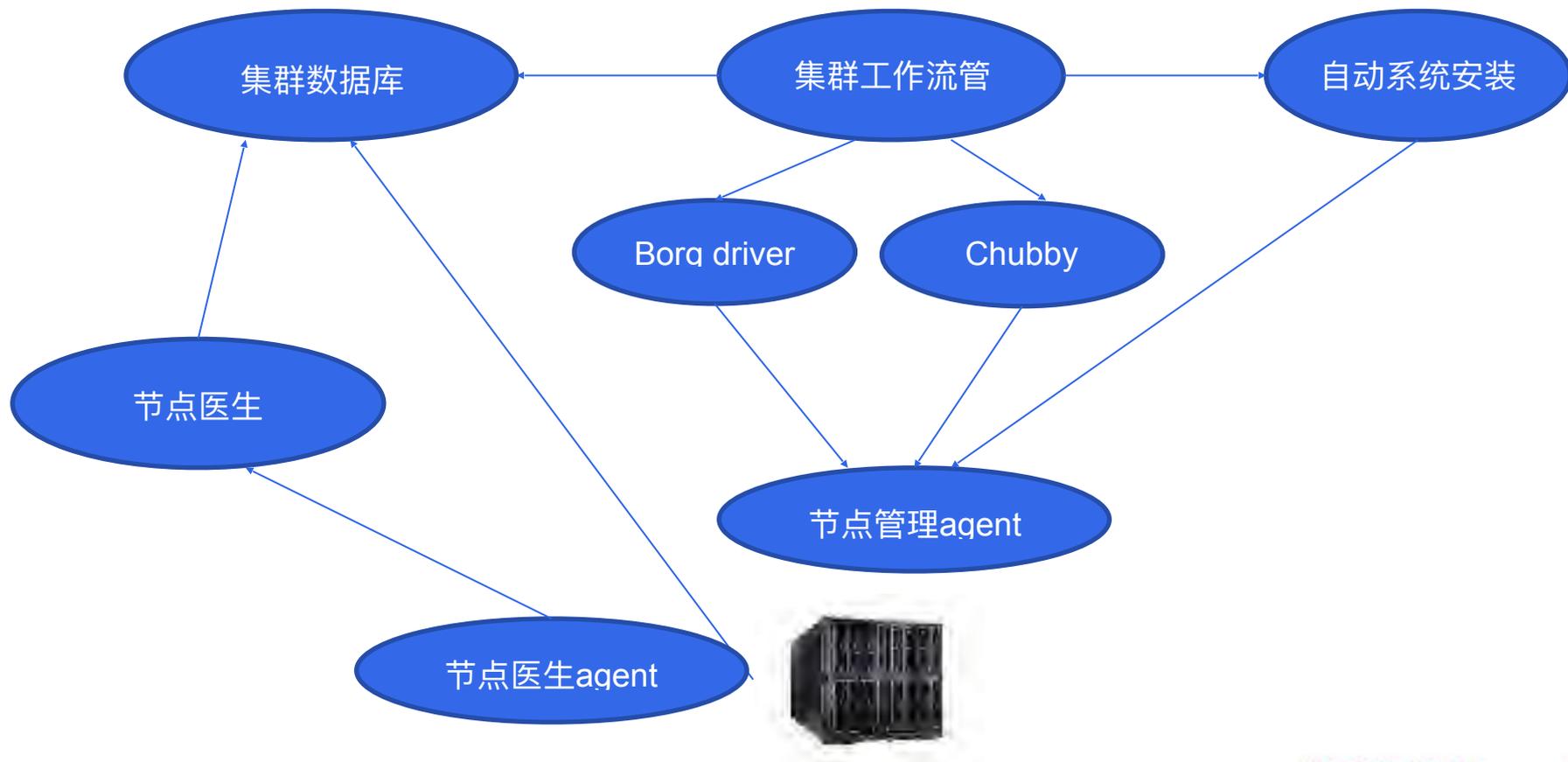


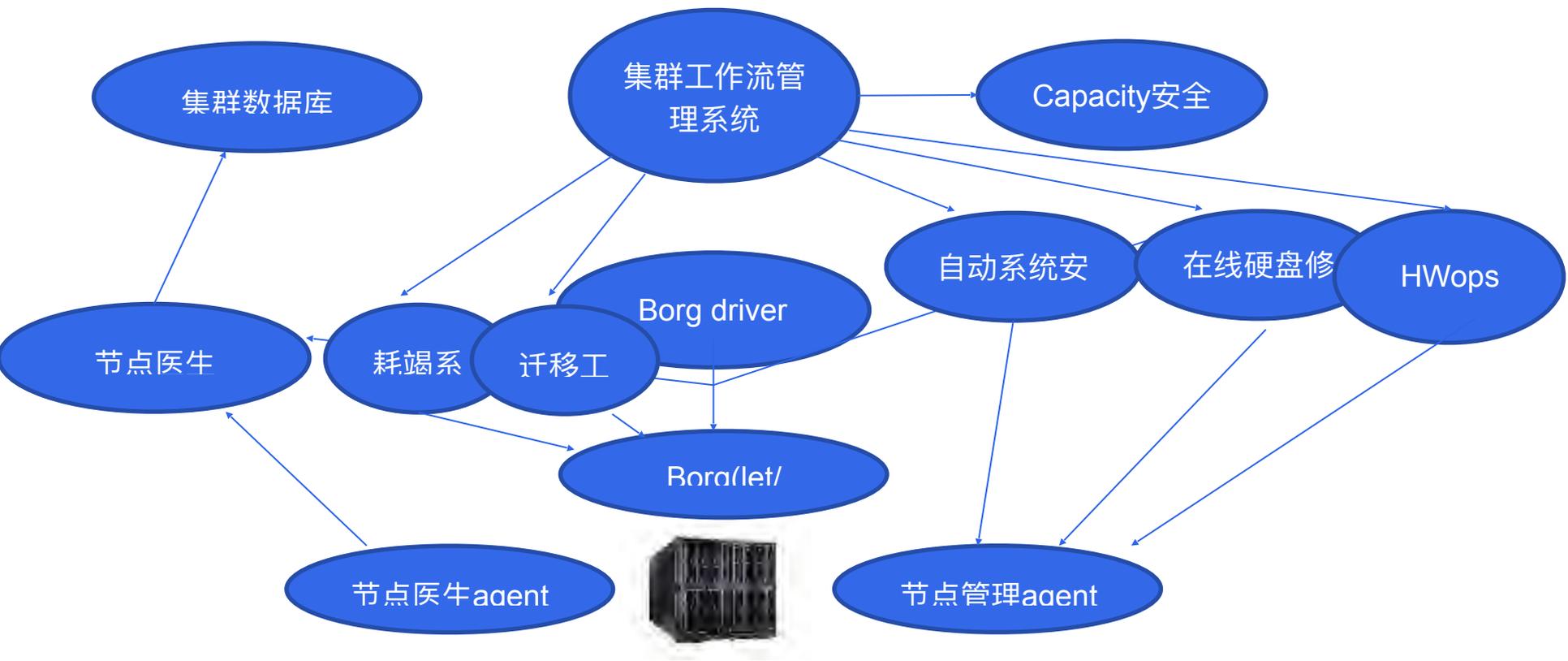


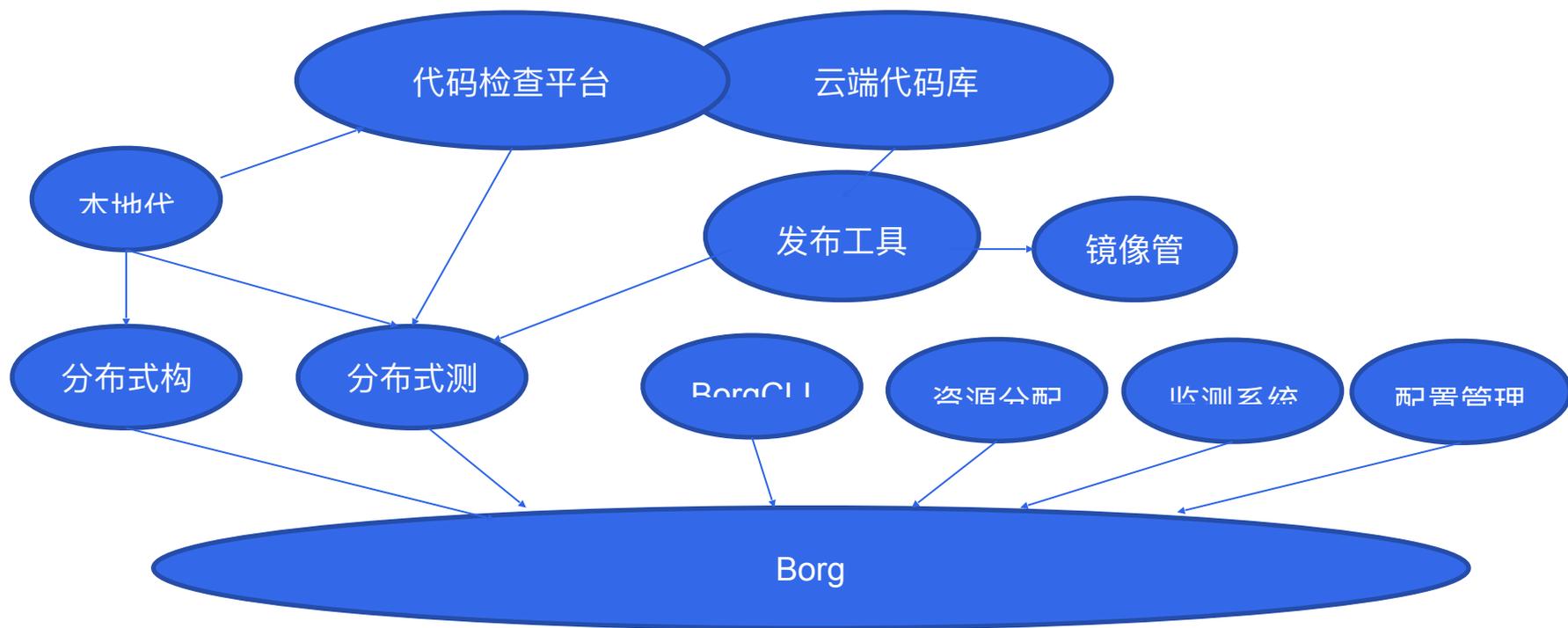
Kubernetes vs Google Cluster Management







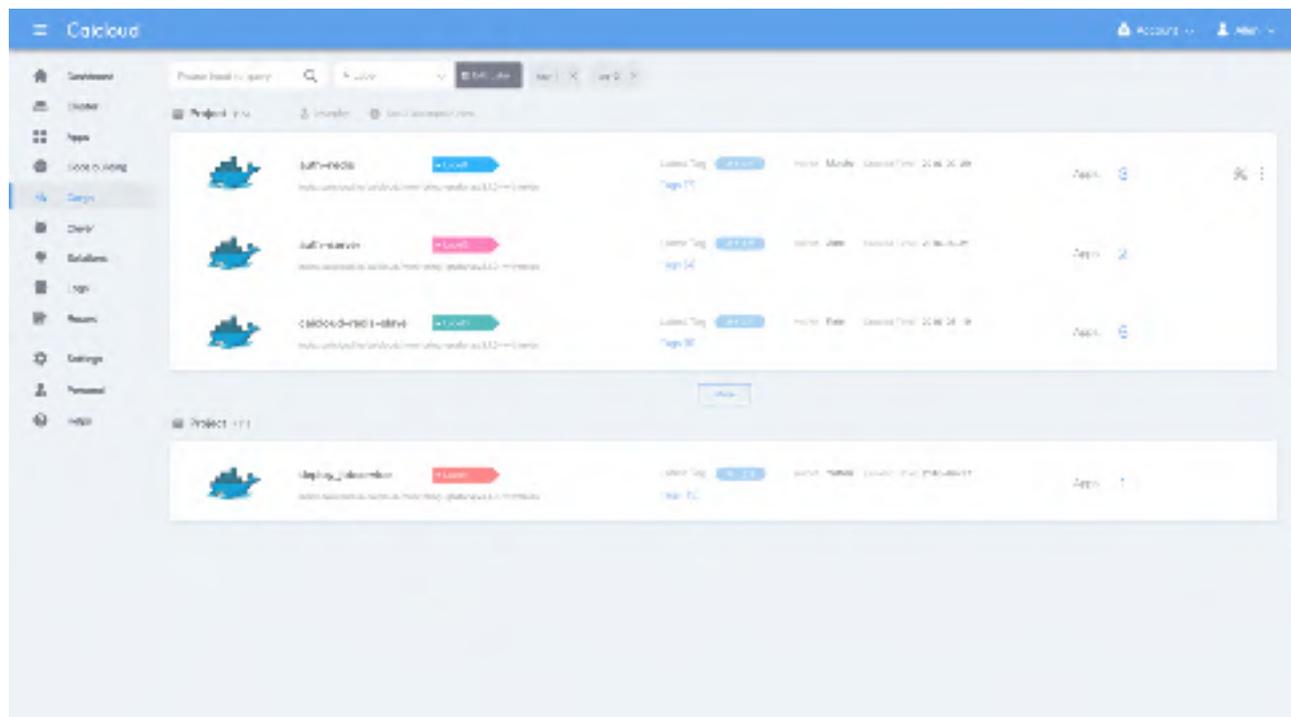




镜像管理系统 - 基于Harbor的企业级镜像仓库

github.com/vmware/harbor
github.com/caicloud/harbor

- 高可用
- 多registry镜像同步
- 镜像安全扫描
- 审计与鉴权
- 标签化灵活管理
- 可视化管理操作
- 多种存储方案





联合发布系统

github.com/caicloud/cyclone

CVE-2016-5699	Medium	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2016-0772	Medium	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.6, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-1547	Medium	Validate crypto-NAKs, AKA: nak-dos

union1 release1

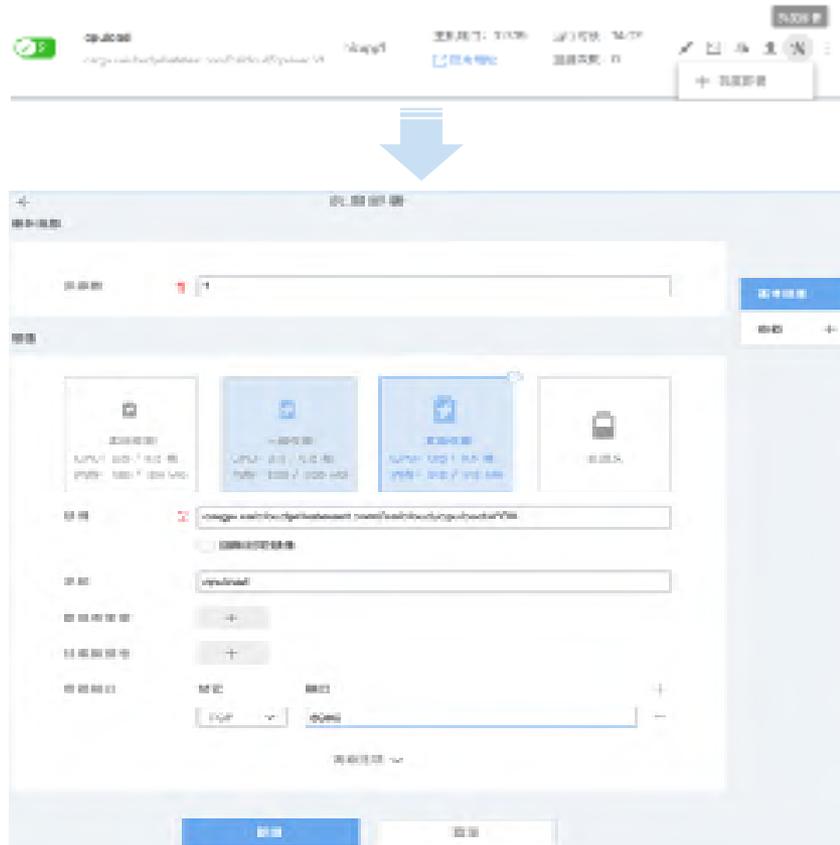
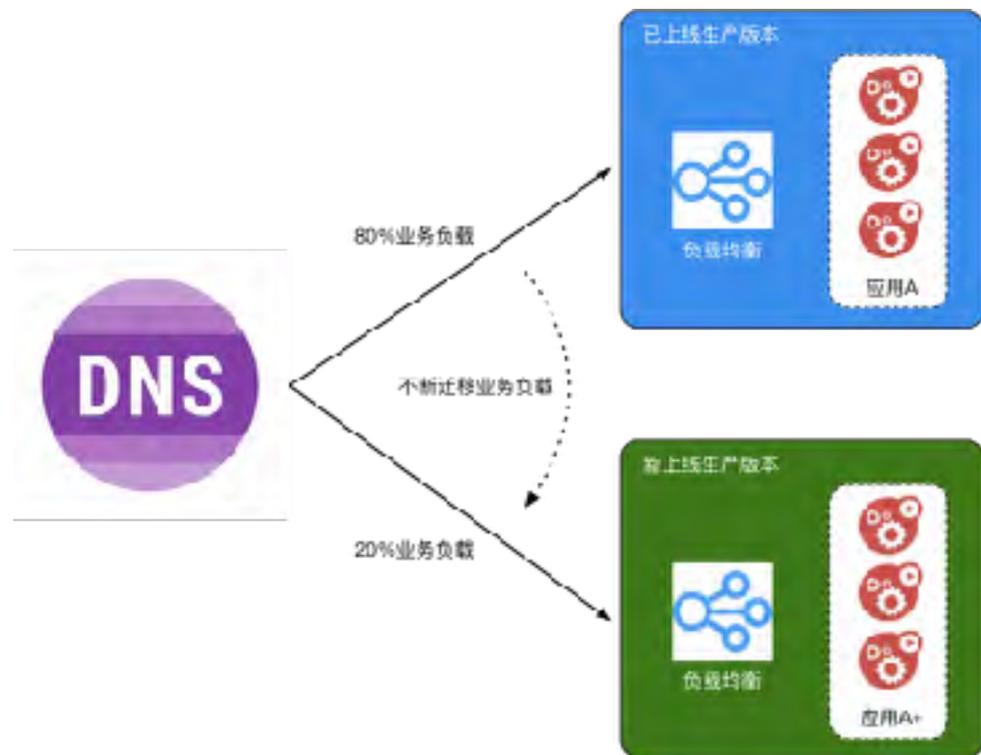
- Building
- Build succeeded
- Build failed
- Deploying
- Deploy succeeded
- Deploy failed



release1
2016-10-24 17:36:59

pointer dereference

灰度发布系统





应用编排系统

Helm

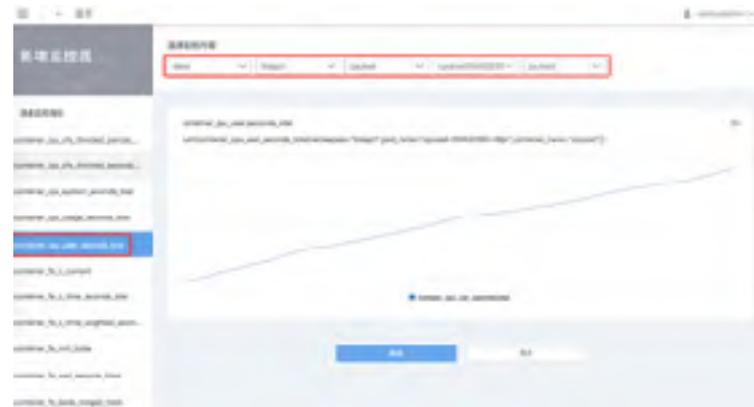
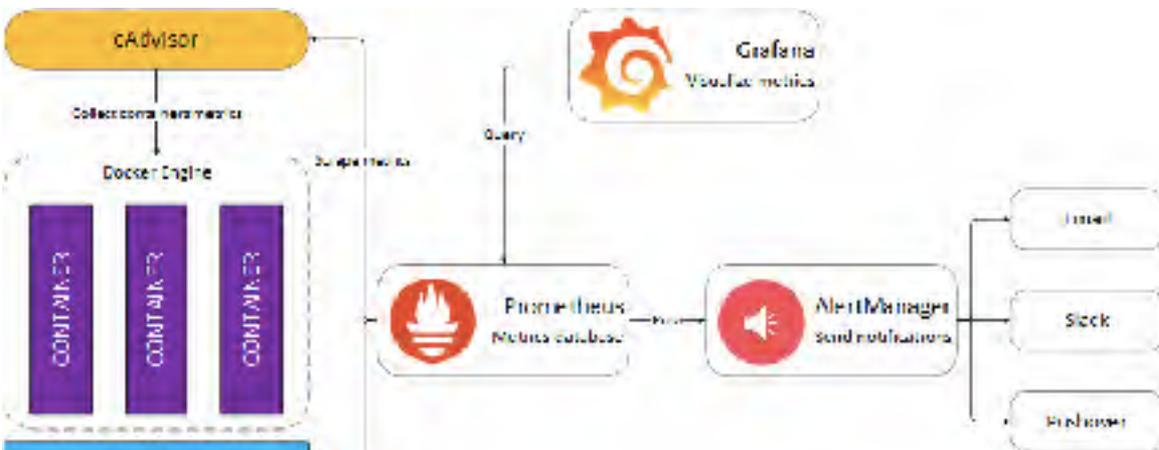
- <https://github.com/kubernetes/helm>
- 基于Kubernetes的应用编排工具
- 自带多种常用应用模版
- 快速构建、部署复合型微服务应用
- 复合应用的共享、分发、管理

Helm-registry (just open-sourced!)

- <https://github.com/caicloud/helm-registry>
- 提供持久化的、可共享的应用商店库
- 上传、存储、共享、管理应用模版
- 提供API支持工具整合
- 支持ACL等权限管理



监控报警系统

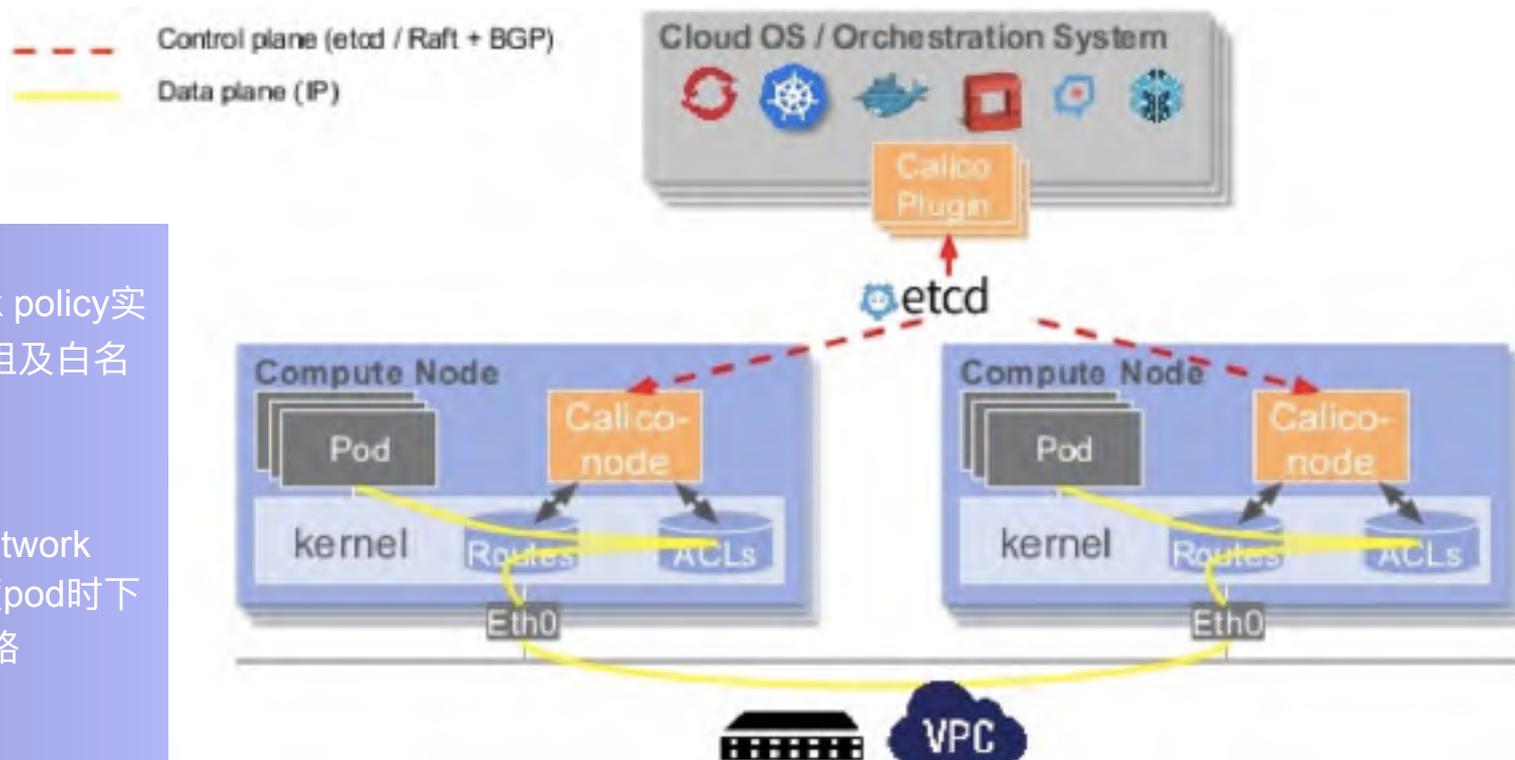


- 监控物理机、应用、容器
- CPU、内存、磁盘IO
- 网络连接数，网络请求流量
- Mysql索引数量，QPS，负载
- 告警抵制、告警策略、Webhook通知



安全策略

1. Calico network policy实现的ACL安全组及白名单，pod粒度
2. Kubernetes network policy实现调度pod时下发所需网络策略





云计算产业联盟

全球云计算峰会2017

聚焦云计算生态，构建全球产业联盟

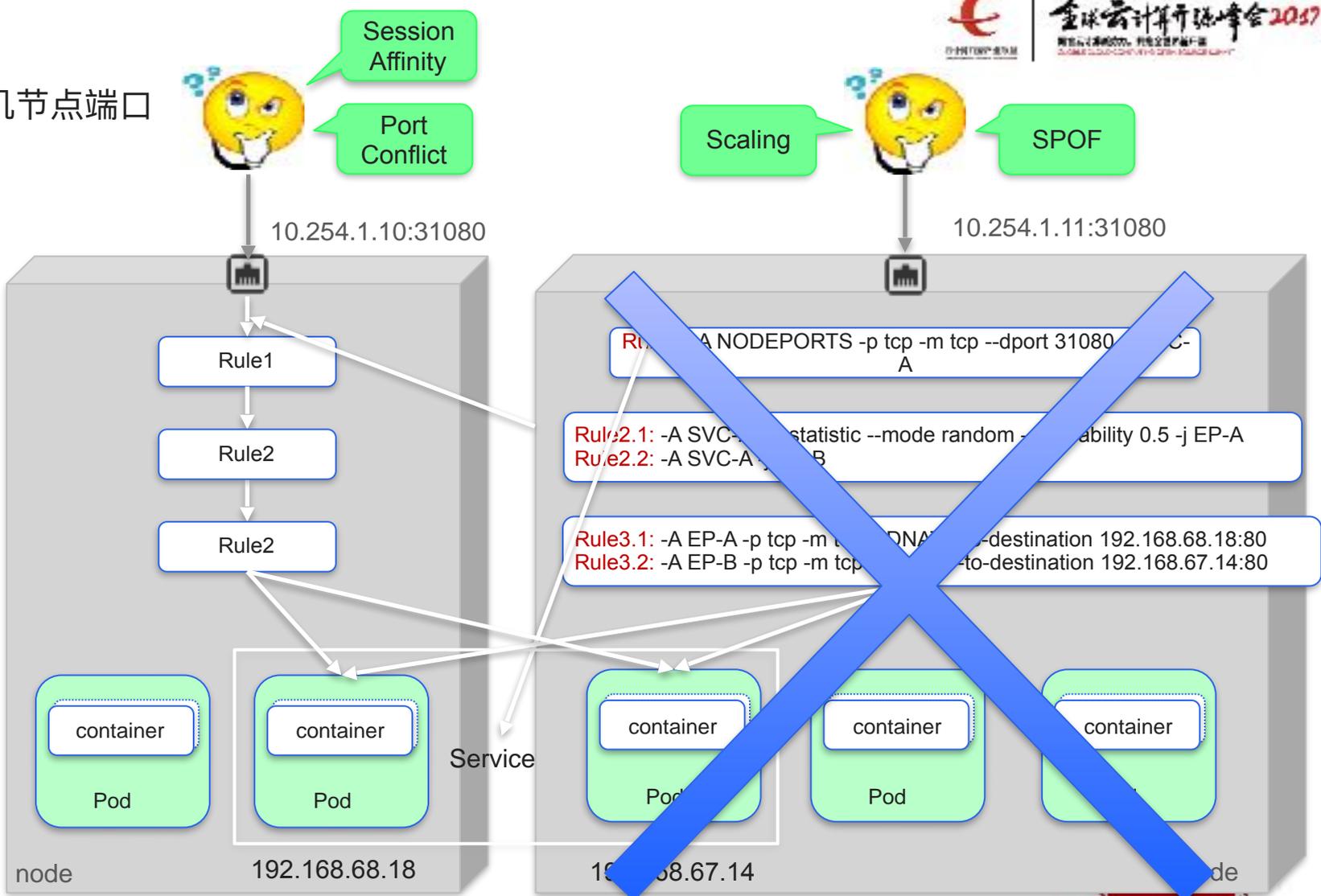
GLOBAL CLOUD COMPUTING SUMMIT 2017

Kubernetes vs 传统行业落地

- 离线部署
- 私有IaaS对接（网络、存储、负载均衡）
- 有状态、单体应用的无缝迁移
- 线上系统升级
- 多租户管理与安全把控

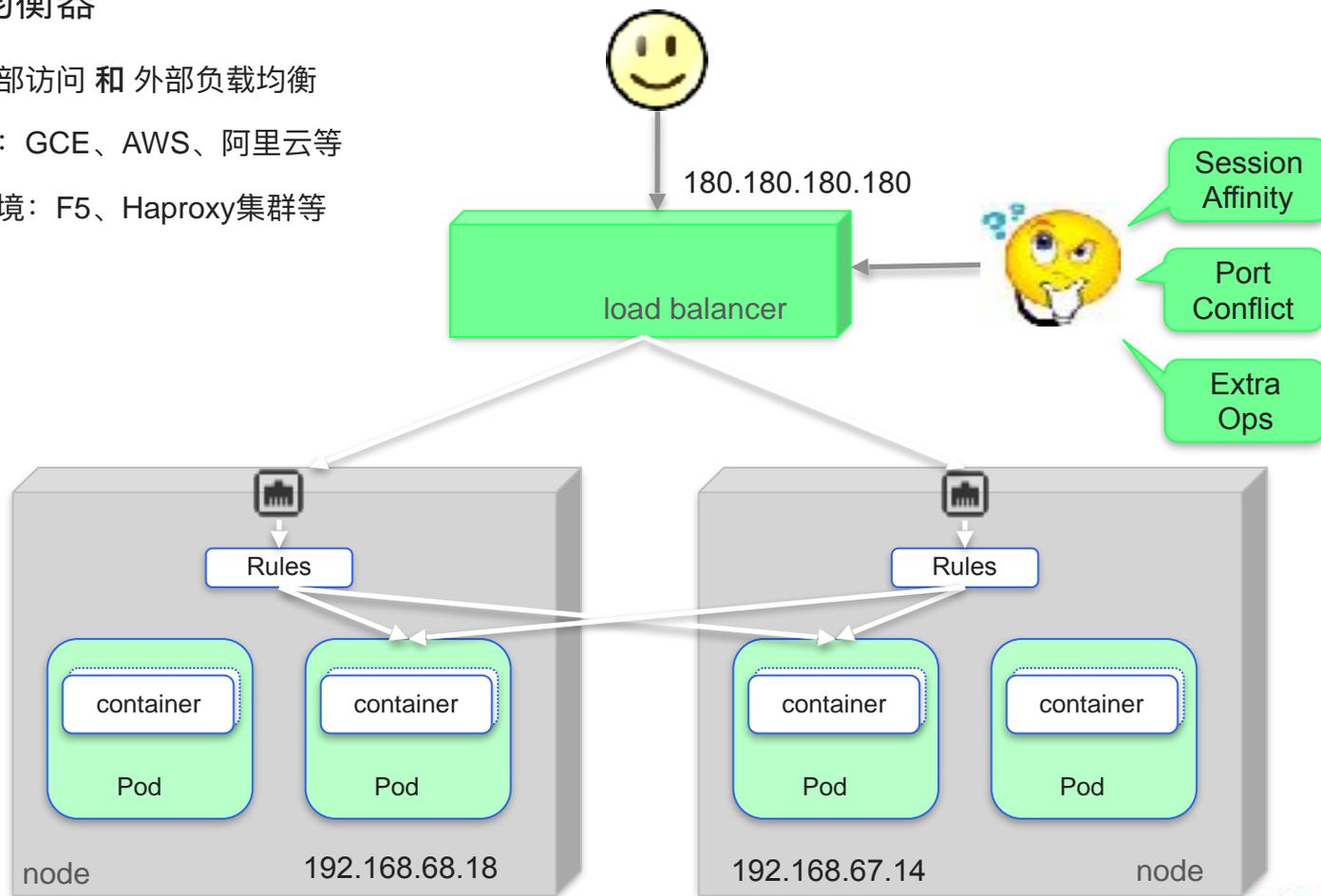


• 主机节点端口



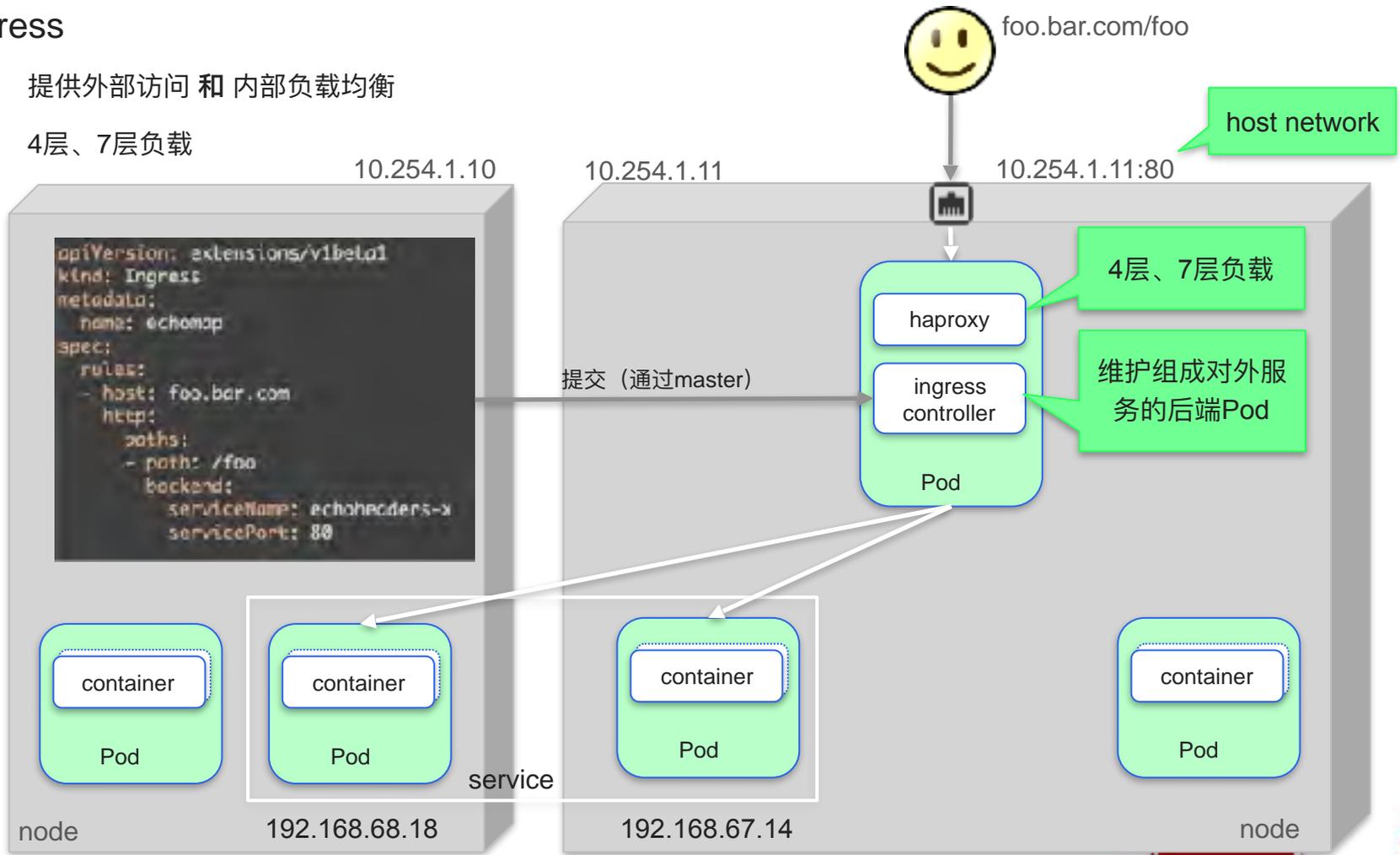
外部负载均衡器

- 提供外部访问 和 外部负载均衡
- 云环境：GCE、AWS、阿里云等
- 私有环境：F5、Haproxy集群等

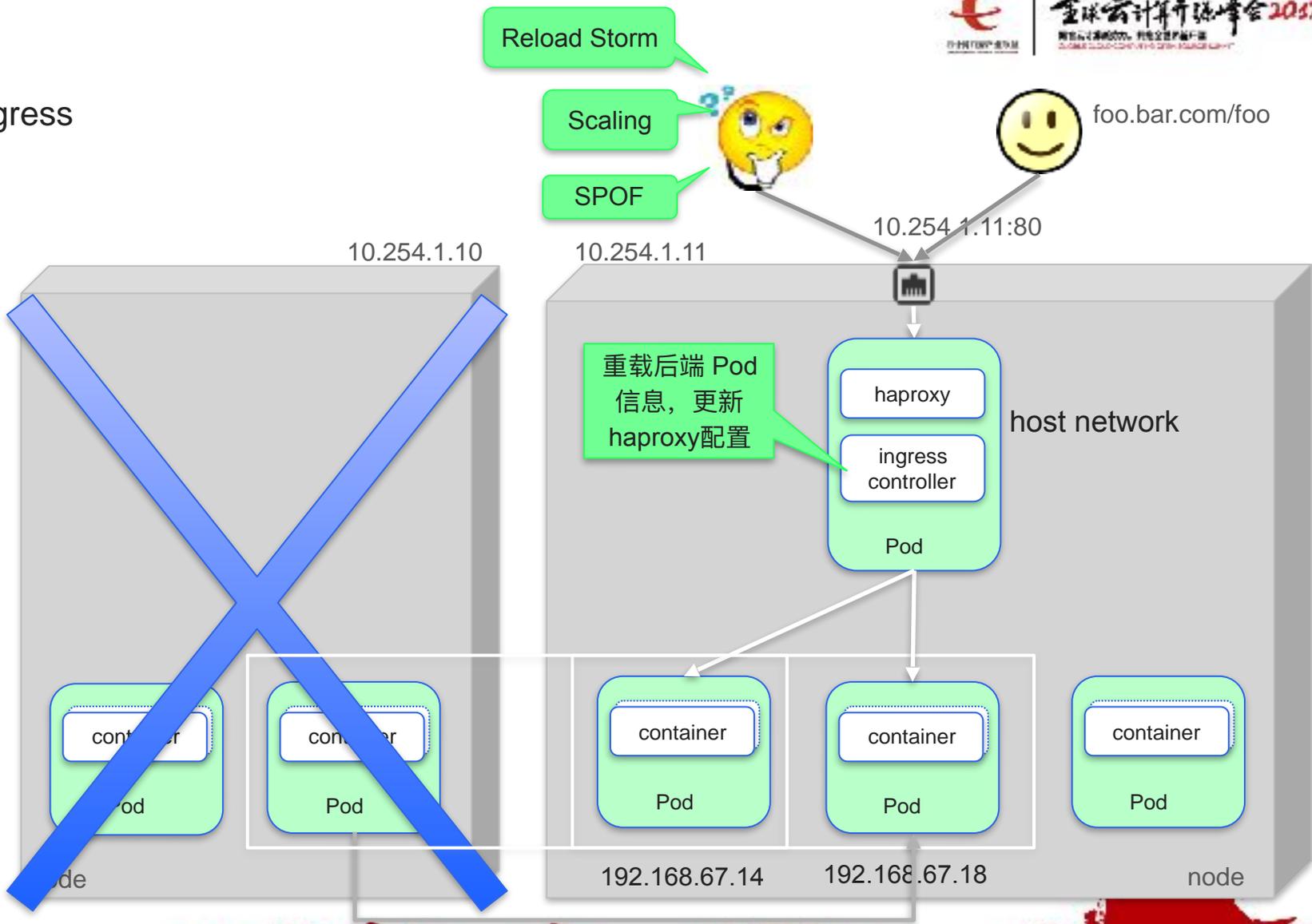


Ingress

- 提供外部访问 和 内部负载均衡
- 4层、7层负载

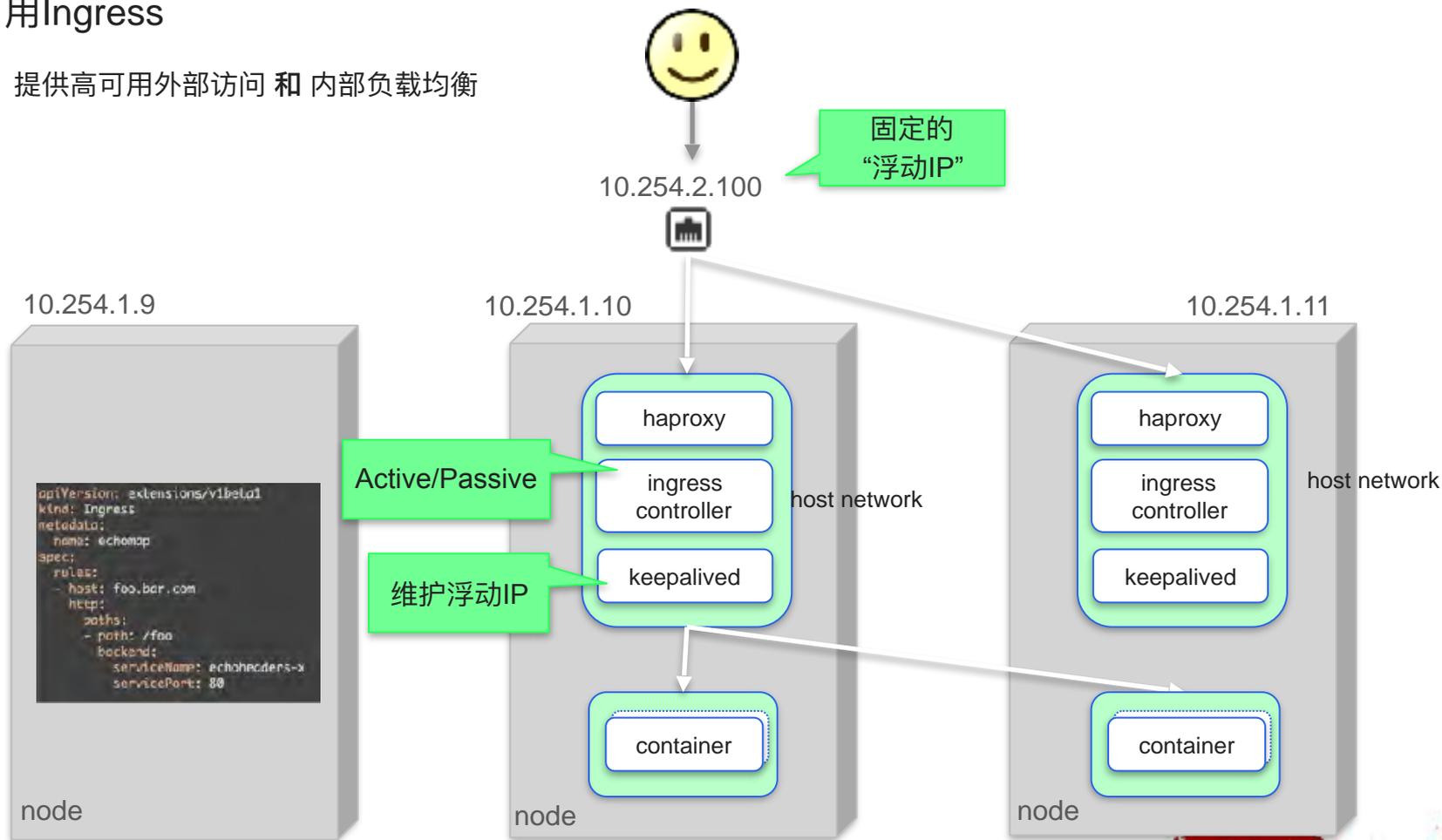


• Ingress



- 高可用Ingress

- 提供高可用外部访问 和 内部负载均衡



- 高可用Ingress

- Reload Storm
- service discovery
- Scaling



foo.bar.com/foo

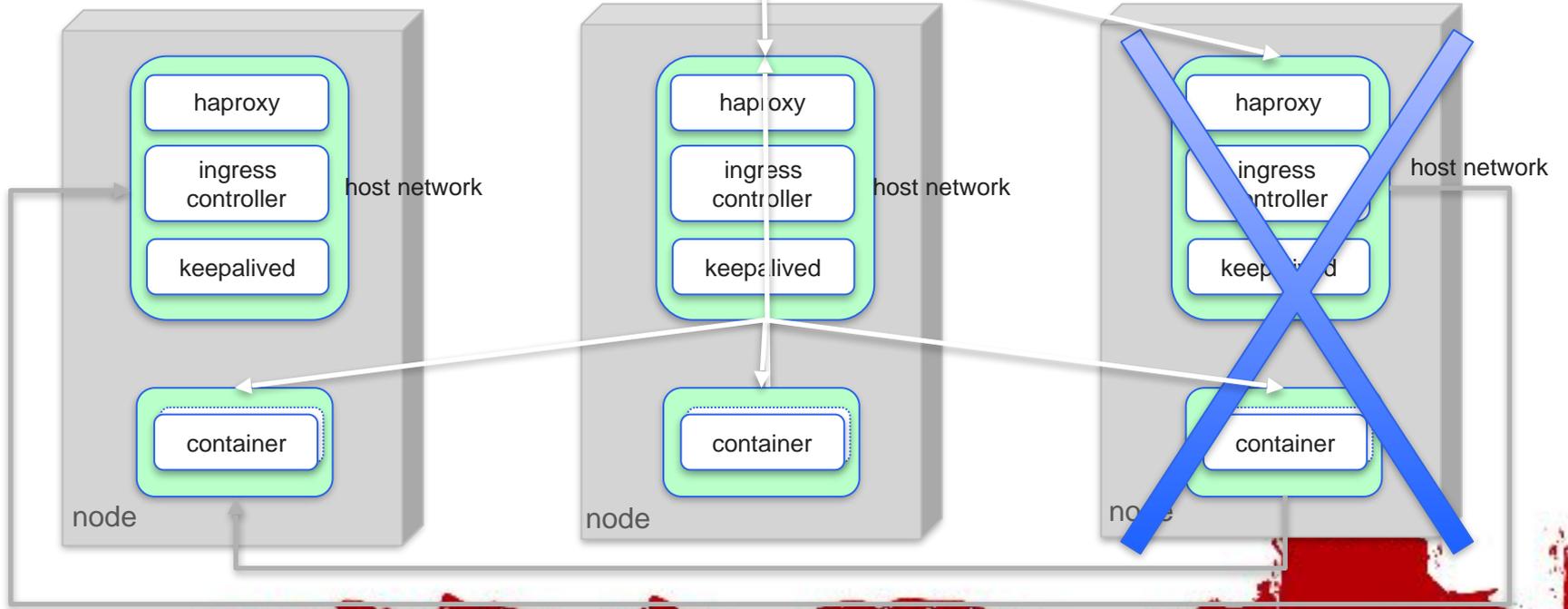
10.254.2.100



10.254.1.9

10.254.1.i0

10.254.1.11

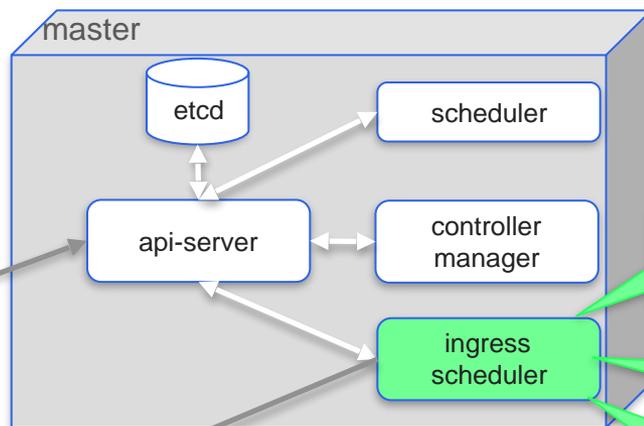


Ingress调度

- 均衡Ingress负载

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: echomap
spec:
  rules:
  - host: foo.bar.com
    http:
      paths:
      - path: /foo
        backend:
          serviceName: echoheaders-x
          servicePort: 80
```

提交



通过Policy维护Ingress池，目前支持namespace级别调度

管理可供外部访问的IP地址段

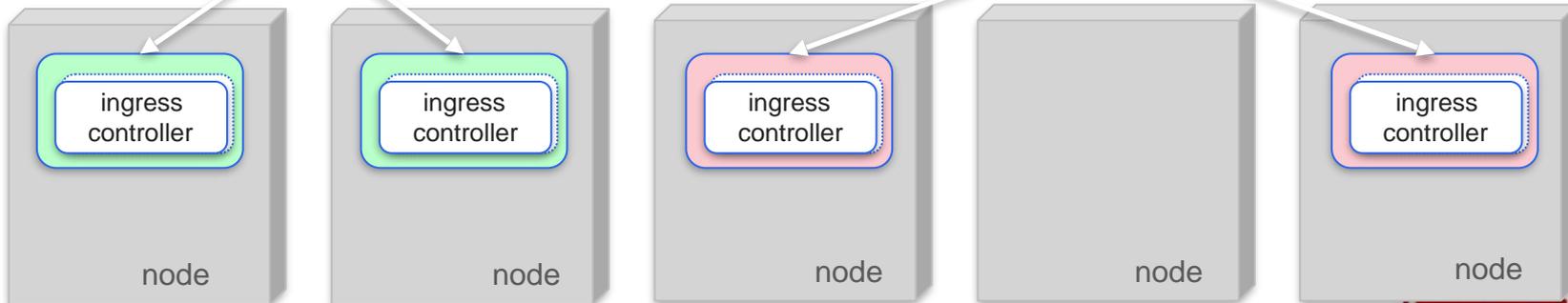
将ingress中的域名通过DNS提供给外部访问

创建

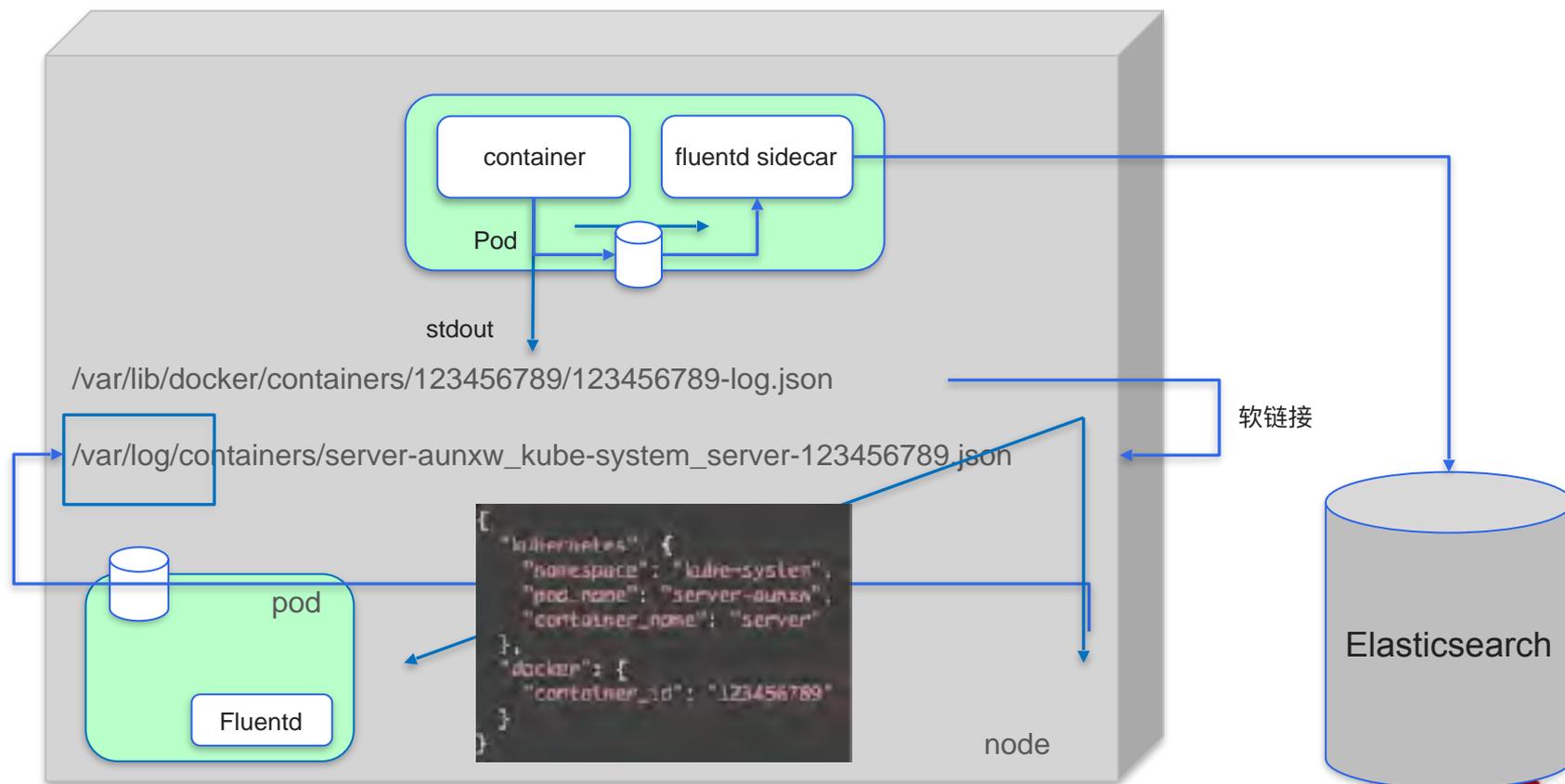
10.254.2.100



10.254.2.101

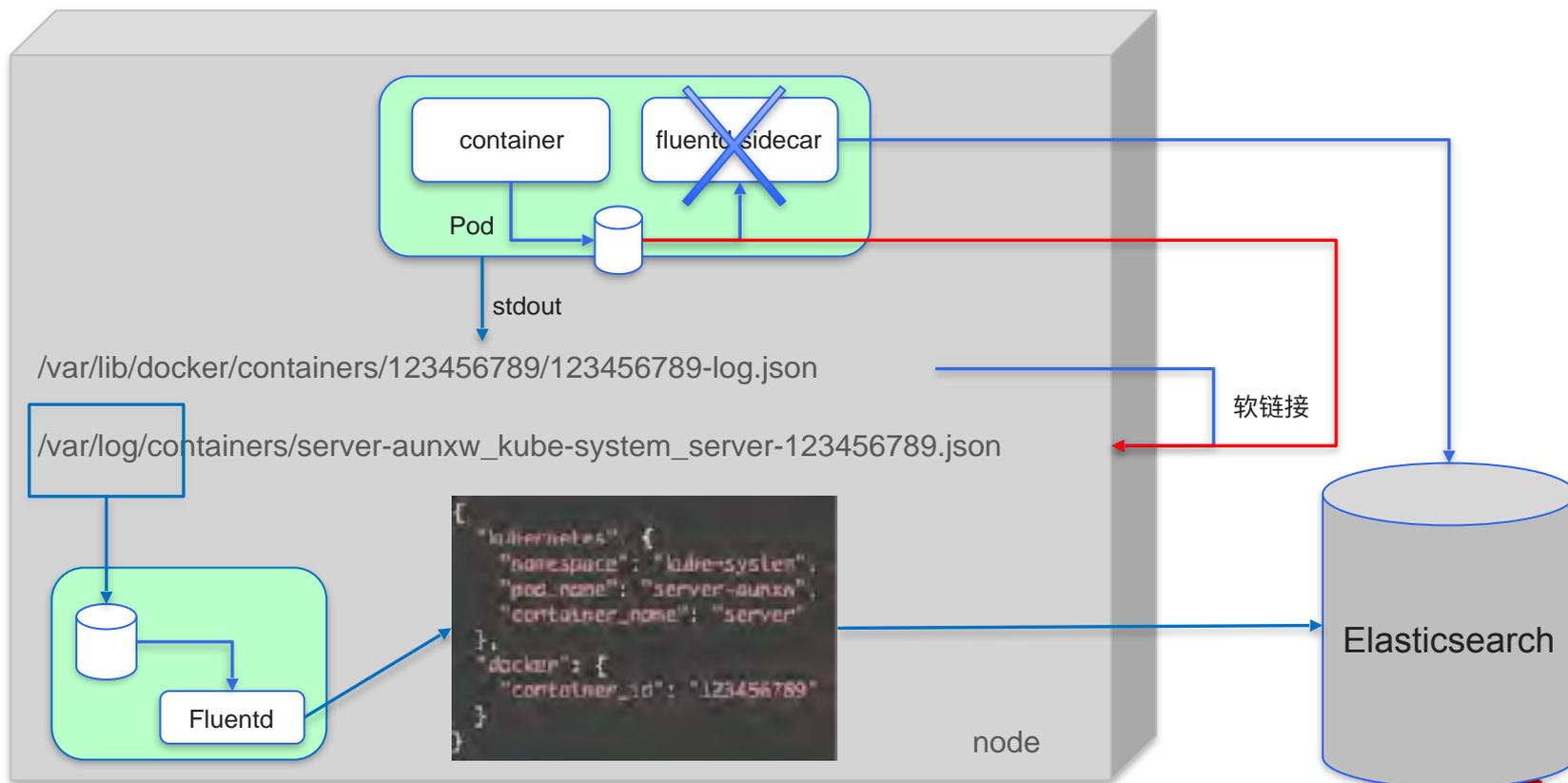


采集目录文件：采用sidecar



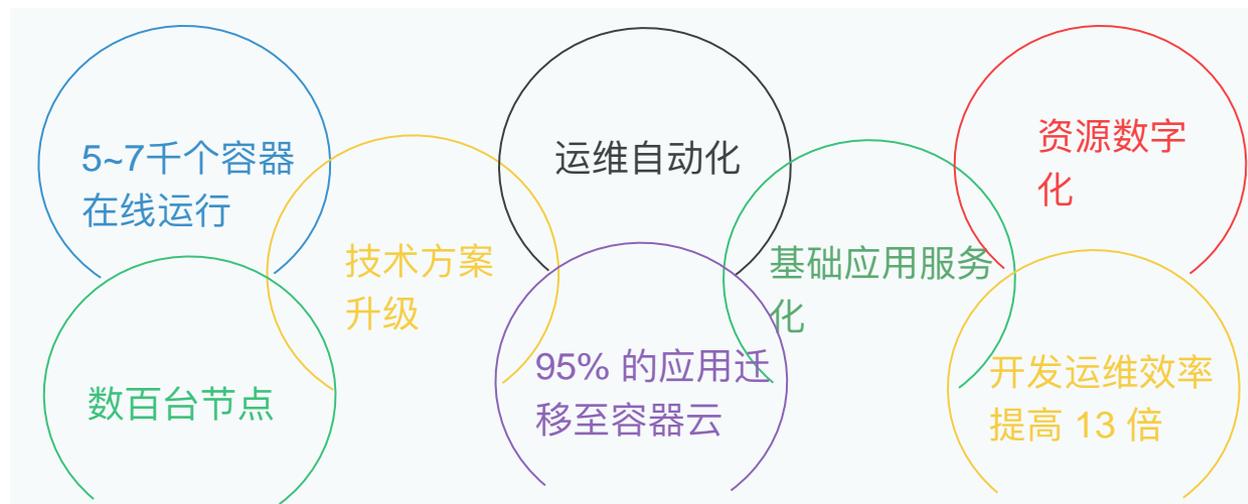
采集目录文件：logDir

- 直接扩展Pod API和系统组件，支持容器写文件



中国规模最大的综合性酒店旅游产业集团之一。截止2016年底，此酒店拥有、管理和特许经营的酒店**7000**余家，客房总数超过**70**万间，全球酒店集团排名**前5**位，亚洲**第1**位。

完成收购兼并后，集团会员规模超过1亿，线上渠道的重要性以及相关比例越来越大。线上平台还承担着内部多个BU交叉销售，海内、海外渠道交叉销售的重要角色。



银行卡联合组织。

公司通过跨行交易清算系统，实现商业银行系统间的互联互通和资源共享，保证银行卡跨行、跨地区和跨境的使用。

目前已与境内外数百家机构展开广泛合作，金融网络遍布中国城乡，并已延伸至亚洲、欧洲、美洲、大洋洲、非洲等160个国家和地区。

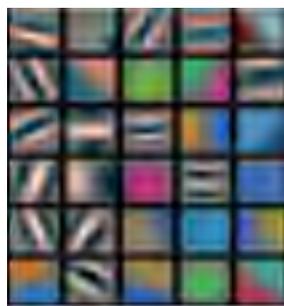
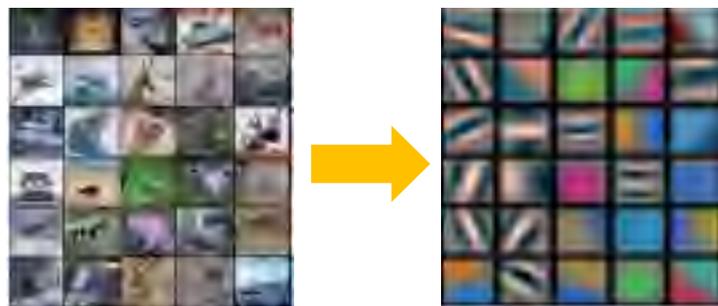




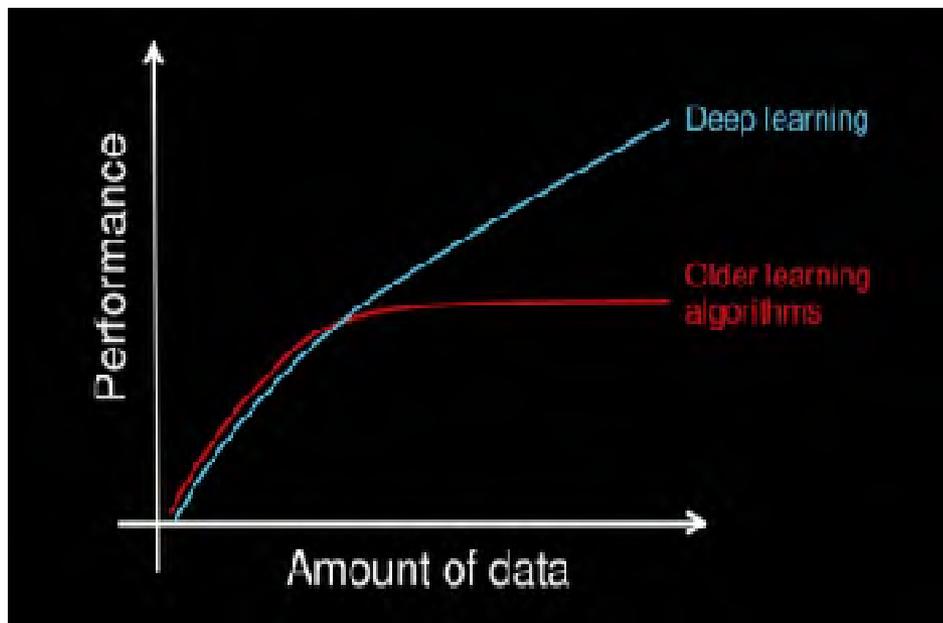
全球云计算峰会 2017
聚力云生态，构建互联网+新生态
GLOBAL CLOUD COMPUTING SUMMIT 2017

Kubernetes vs Big Data



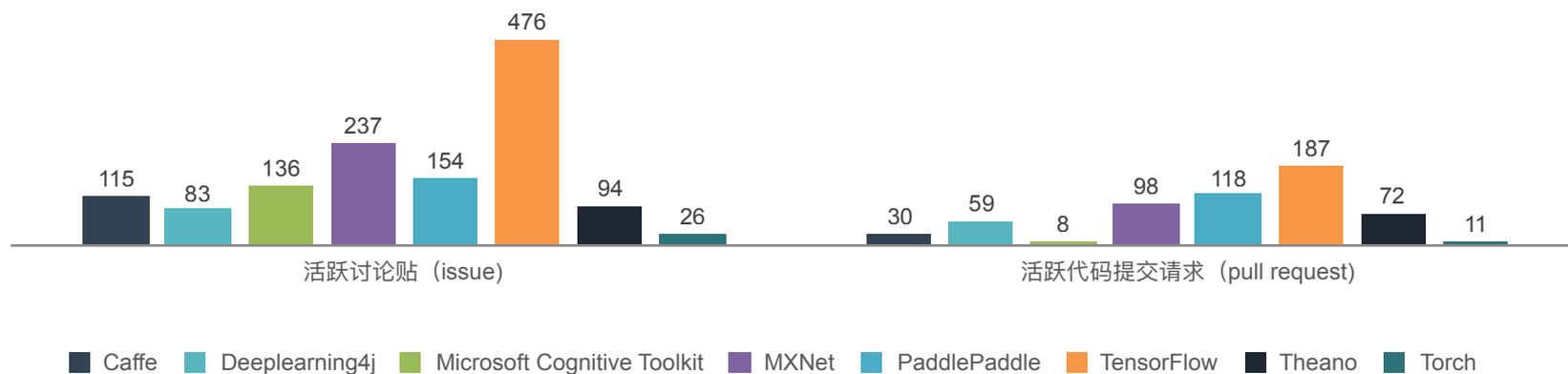
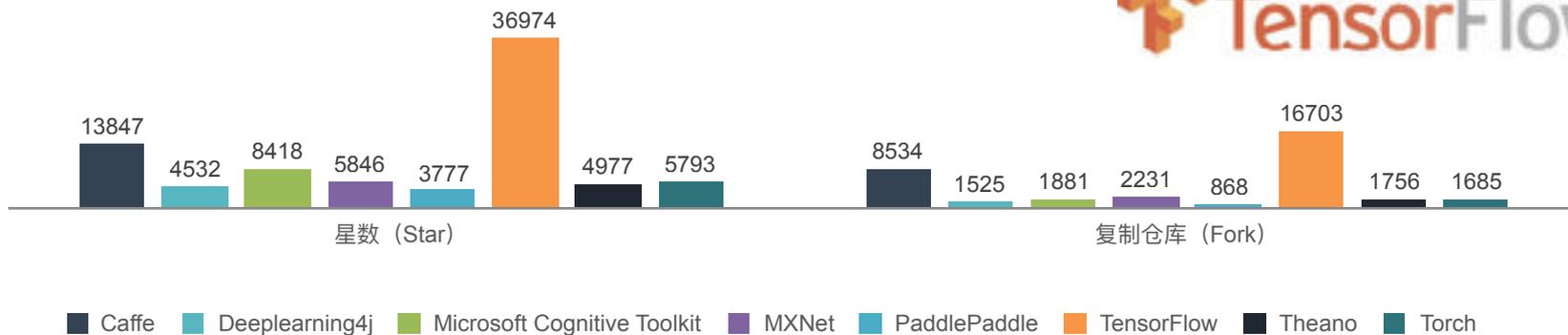


多层复杂特征提取优势

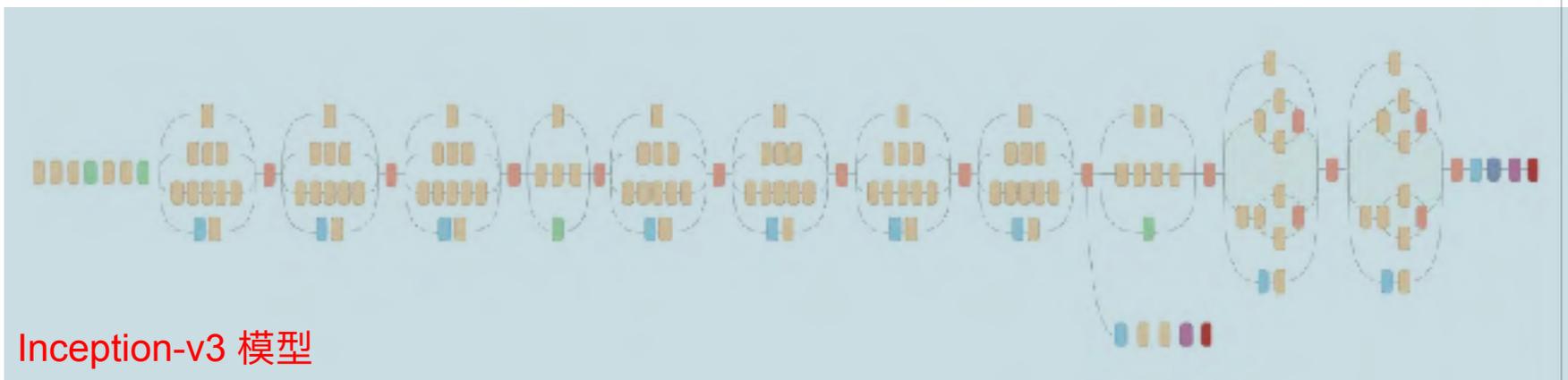


大数据量优势





IMAGENET



- ❖ Inception-v3 模型：2500万参数 & 50亿次运算/推导1张图片 ==> 78%的正确率需：6个月
- ❖ CPU计算效率较低





Google runs everything in its container clusters, including Machine Learning tasks

- scaling out
- self-management
- ease of deployment/update
- resource sharing (and isolation)



分布式Kubernetes容器集群

计算管理节点

Kubernetes Pod

Kubernetes Pod

Kubernetes Pod

深度学习计算节点

统一存储



Storage

分布式Kubernetes租户容器集群

计算管理节点

Kubernetes Pod

Kubernetes Pod

Kubernetes Pod

深度学习计算节点

Server 1

Server 2



Server 3

Server 4

Server 5



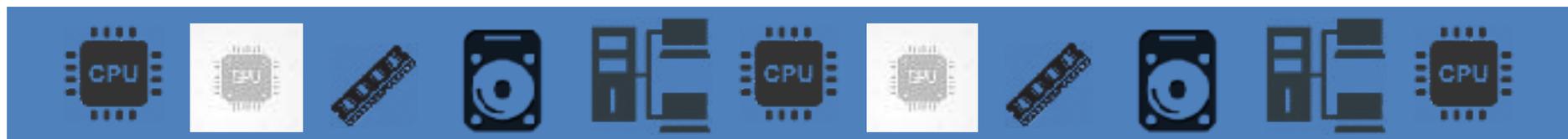
支持GPU资源调度和管理的服务器

操作	原生TensorFlow	才云科技TaaS
部署安装	Pip安装	无需安装，web界面提供服务
分布式环境	手工在多台服务器架设运行环境	无需自行搭建分布式环境，系统自动提供隔离的完整分布式环境支持
资源调度	需要考虑设备集群之间资源分配问题	基于Kubernetes高效管理计算节点集群和资源调度
模型训练	需要在多个节点上通过命令行手动设置以启动参数和计算	模板化编辑模型文件，提供上传接口，图形界面设置参数，傻瓜式操作便可启动模型训练
训练过程监控	自行启动TensorBoard，手动查看运行状态	自动启动监控平台，图形UI界面统一监控
训练过程管理	手动保存模型日志文件	自动化管理模型日志文件
在线提供服务	提供在线服务，可通过自定义方式实现	自动启动并维护在线服务；支持训练模型导出

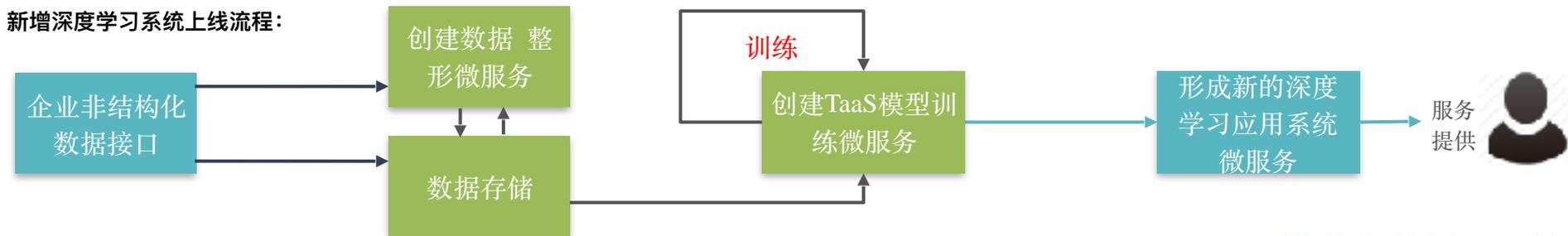




Kubernetes容器云平台



新增深度学习系统上线流程:





- ❖ 短信营销：信用卡分期客户，减少短信发送量，提高业务实现率
- ❖ 智能投顾：理财产品智能推荐，响应率和交易总金额指数级提升



- ❖ 流失预警：分析客户行为趋势，预测客户流失倾向，提升客户忠诚度
- ❖ 智能客服：电话银行菜单设置更合理，客户体验更好
- ❖ 风险控制：反欺诈，反洗钱，贷后风险管理更高准确率
- ❖ 身份认证：VTM远程开户身份验证



- ❖ 期货指标：指标预测成功率提升30%
- ❖ 基金经理：深度学习作为基金经理，无人工接触
- ❖ 金融交易：深度学习系统自动交易，秒级操作

安全入侵

- 区域入侵检测
- 翻越围墙检测
- 设备防盗检测
- 火焰智能检测



作业管理

- 安全帽检查
- 物体搬移监测
- 人员轨迹跟踪
- 遗留物品检测



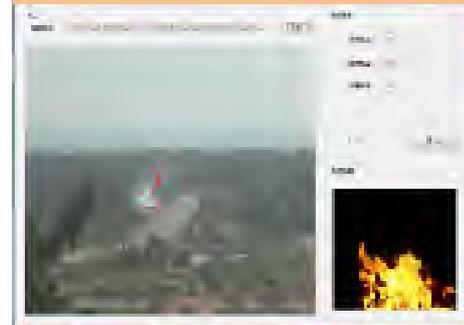
智能交通

- 空位检测
- 人车分离
- 牌号识别
- 行为分析



高危监测

- 烟雾检测
- 明火检测
- 设备故障检测
- 高危操作监测



Celecloud



点击上传图片



Hoodie, 0.529275
Jacket, 0.284865
Blouse, 0.0802139
Cardigan, 0.0126822
Blazer, 0.0221855

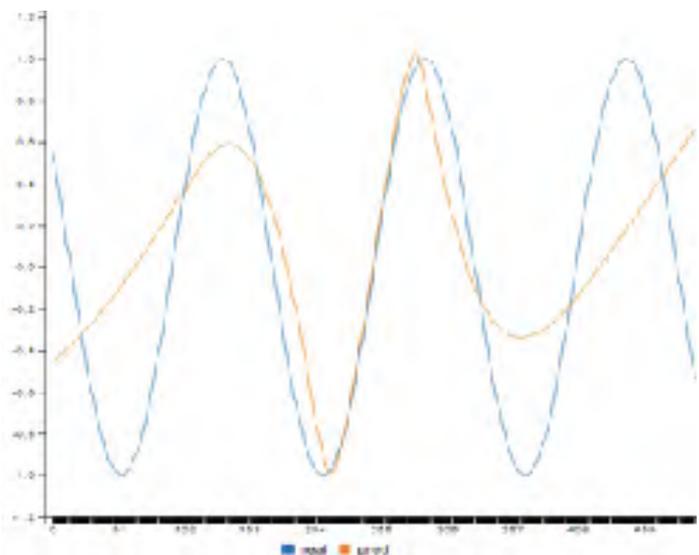


图像识别

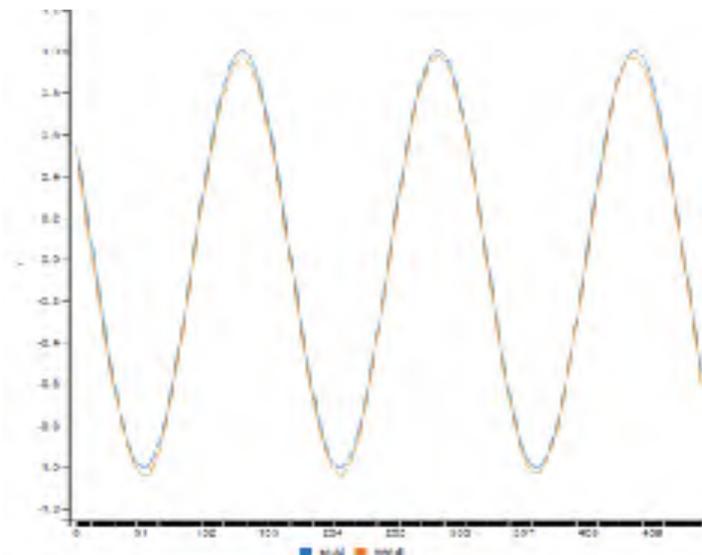




时序预测



深度学习
训练后



发电量预测

电力使用量预测

炼油量预测

水库水位预测

系统运行状况预测





全球云计算峰会 2017
聚焦云计算应用，构建生态产业链
GLOBAL CLOUD COMPUTING SUMMIT 2017



谢谢!

张鑫

才云科技 CEO