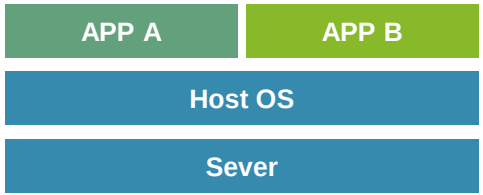
中国移动
China Mobile

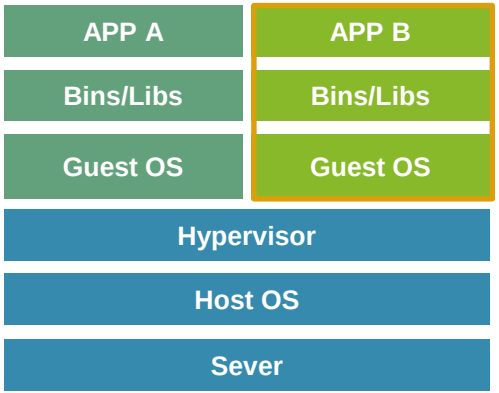
Kubernetes简介及其在雄研的实践经验

智慧城市平台研发部 2019.12

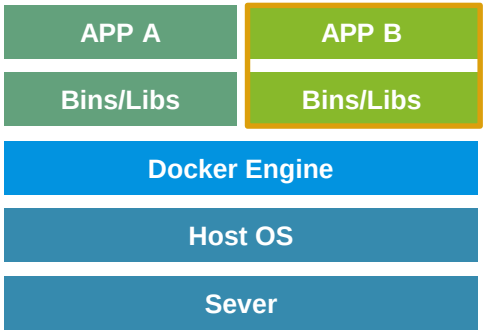
虚拟化技术变迁史



早期在物理服务器上运行应用程序， 无法为物理服务器中的应用程序定义资源边界，导致资源分配不合理。



虚拟化可以更好地利用物理服务器中的资源，并可以实现更好的可伸缩性，轻松地添加或更新应用程序，降低硬件成本。



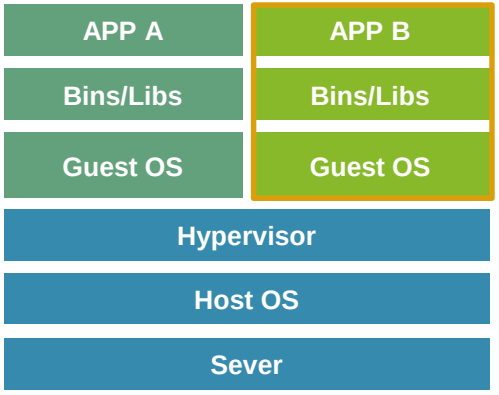
容器类似于VM，但是它们具有轻松的隔离属性，可以在应用程序之间共享操作系统（OS）。 容器与基础架构分离，可以跨云和OS分发进行移植。

高

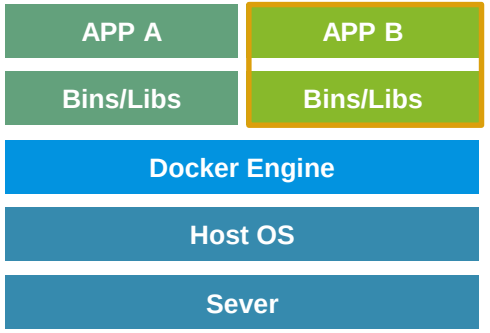
低

隔离性/安全性/性能开销

Docker介绍



VM vs Docker



Docker 是一种容器技术，它可以将应用和环境等进行打包，形成一个独立的，类似于 iOS 的 APP 形式的「应用」，这个应用可以直接被分发到任意一个支持 Docker 的环境中，通过简单的命令即可启动运行。

Kubernetes vs Openstack

中国移动 China Mobile

管理容器，是用于自动部署、扩展和管理容器化应用程序的开源系统

Kubernetes

- 业务变化快，业务量动态变化的场景
- 云化应用众多，发挥云平台的可扩展、弹性、高可用等特性
- 需要业务模块化和可伸缩性的场景
- 需要反复地创建和销毁实例的运行环境
- 微服务架构应用

面向未来

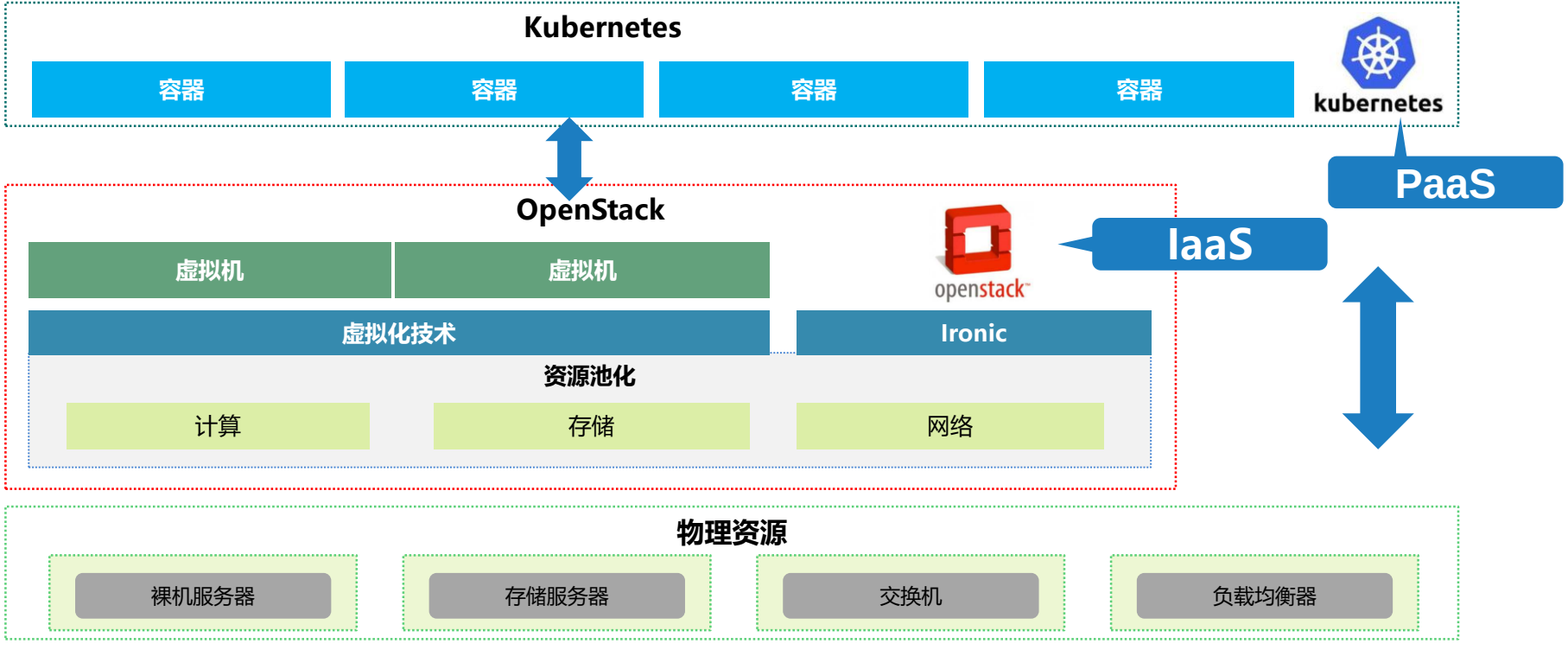
管理虚拟机，利用虚拟化技术提供可扩展，灵活，适应性强的云计算服务

Openstack

- 安全和隔离性要求高的场景
- 提供基础设施管理的场景
- 存储需求高的场景
- 不需要反复地创建和销毁实例的运行环境

兼容传统

Kubernetes和Openstack融合



根据业务需求，懂得灵活使用这两种不同风格的系统才是制胜之道

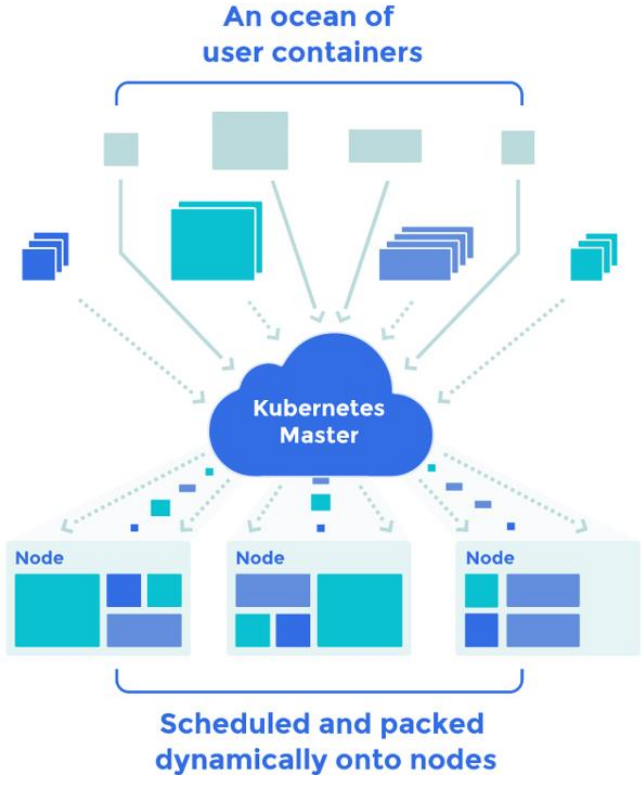
什么是Kubernetes?

定义 Kubernetes是一个可移植的，可扩展的开源平台，用于管理容器化的工作负载和服务，可促进声明式配置和自动化。 它拥有一个庞大且快速增长的生态系统，并且已经广泛应用在各种生产场景。

Kubernetes

容器集群管理器，专门为解决大规模容器集群的管理而生

- 资源调度 - Kube-Scheduler
- 生命周期 - 副本控制器
- 健康检查 - 容器组探针
- 动态伸缩 - 手动、自动伸缩
- 服务发现 - Service/DNS
- 负载均衡 - Kube-proxy

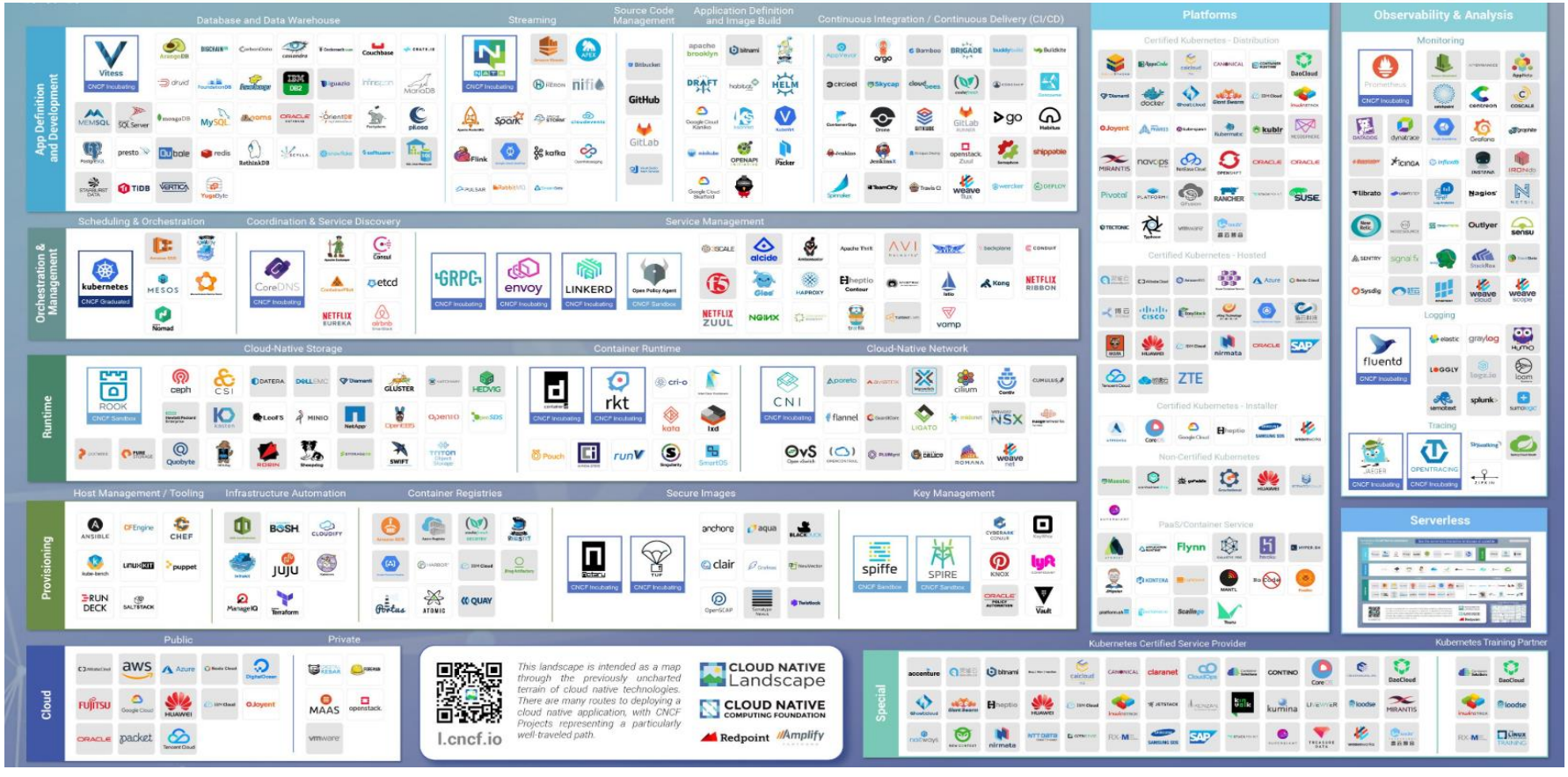


Kubernetes优势-高速发展

中国移动 China Mobile

CNCF	Stack Overflow	Gartner
生产环境的云原生应用增长超过**200%**	**容器**成为Linux之后最受欢迎的项目	到2022年，**75%**的全球企业将使用云原生的容器化应用

Kubernetes优势-庞大的生态系统支撑



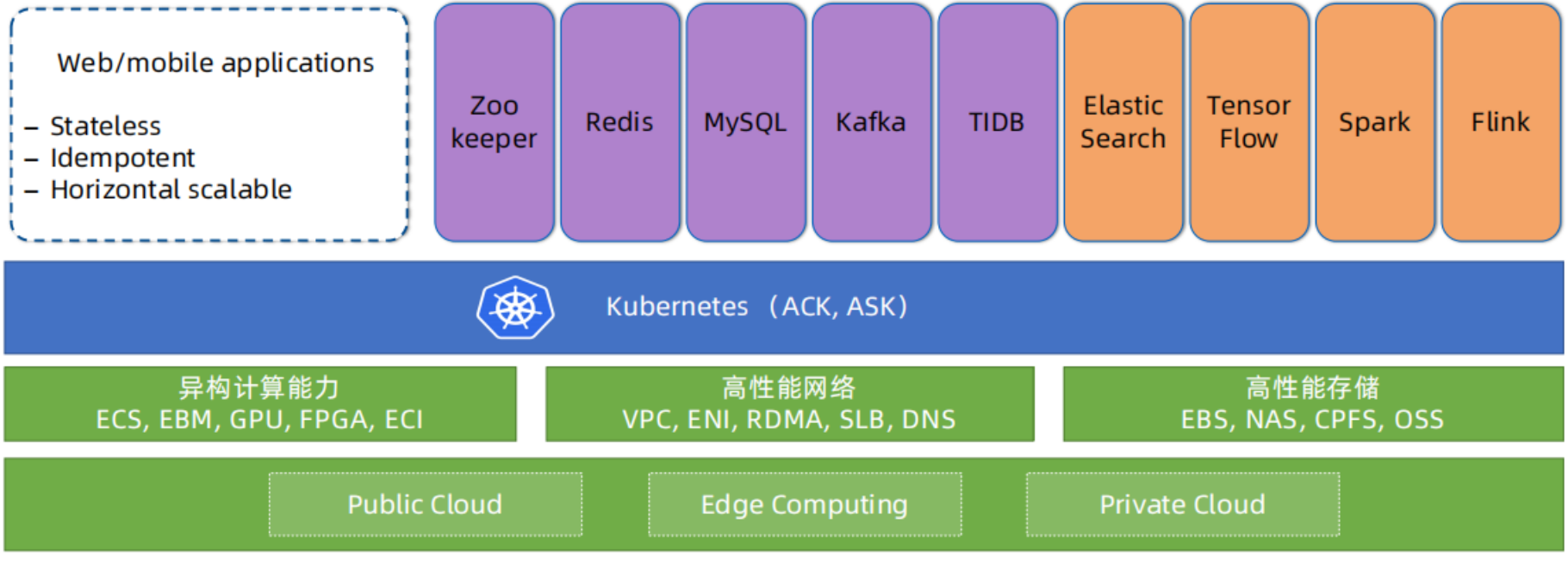
CNCF 目前托管的 20 + 正式项目共同构成了现代云计算生态的基石。其中Kubernetes 项目是全世界第四活跃的开源项目

Kubernetes优势-众多厂商支持

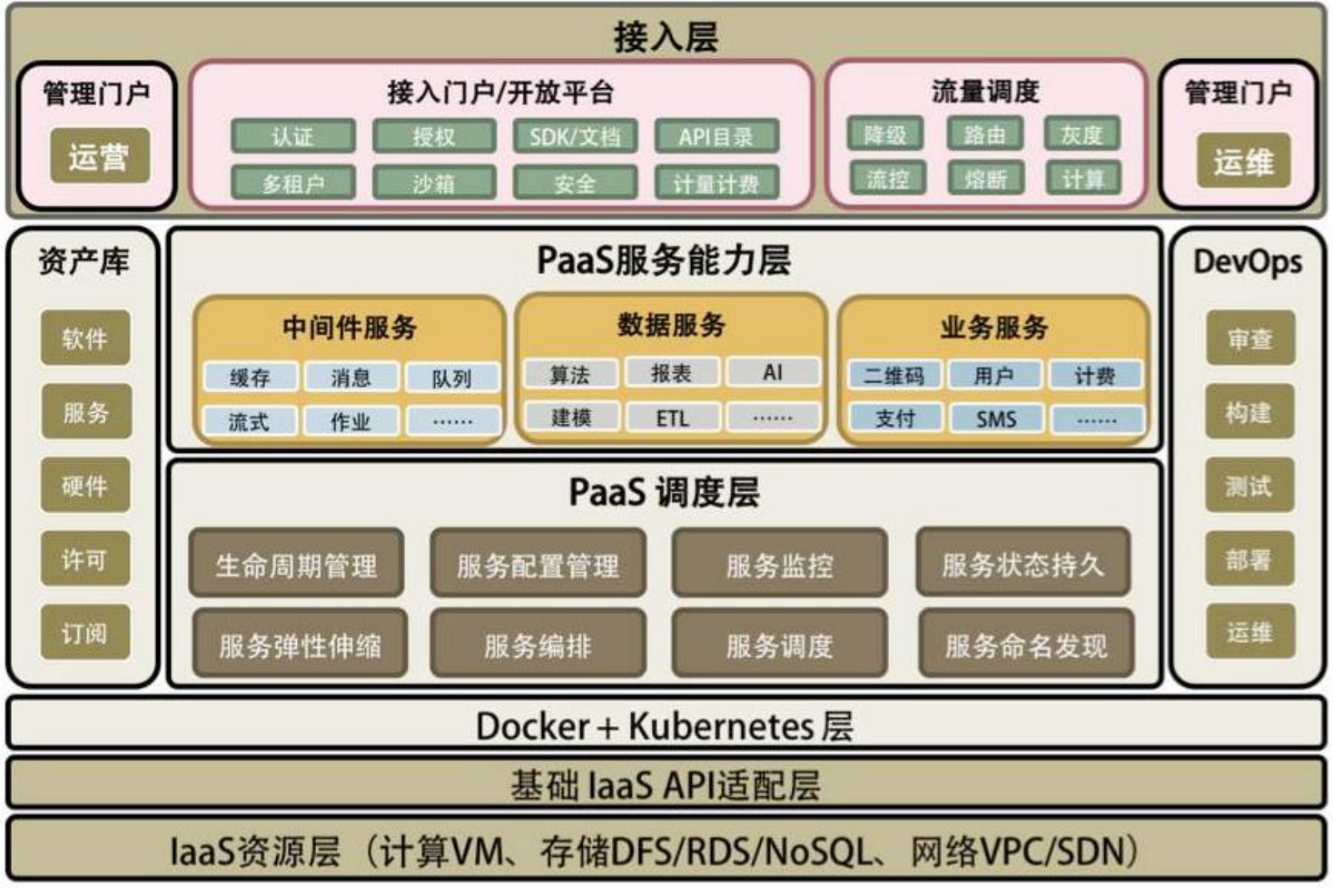
现在全球各大公有云厂商都已经支持了 Kubernetes。此外，还有 100 多家技术创业公司也在持续地进行投入，Kubernetes已经成为容器编排引擎的事实标准

Kubernetes优势-云原生时代的基础设施

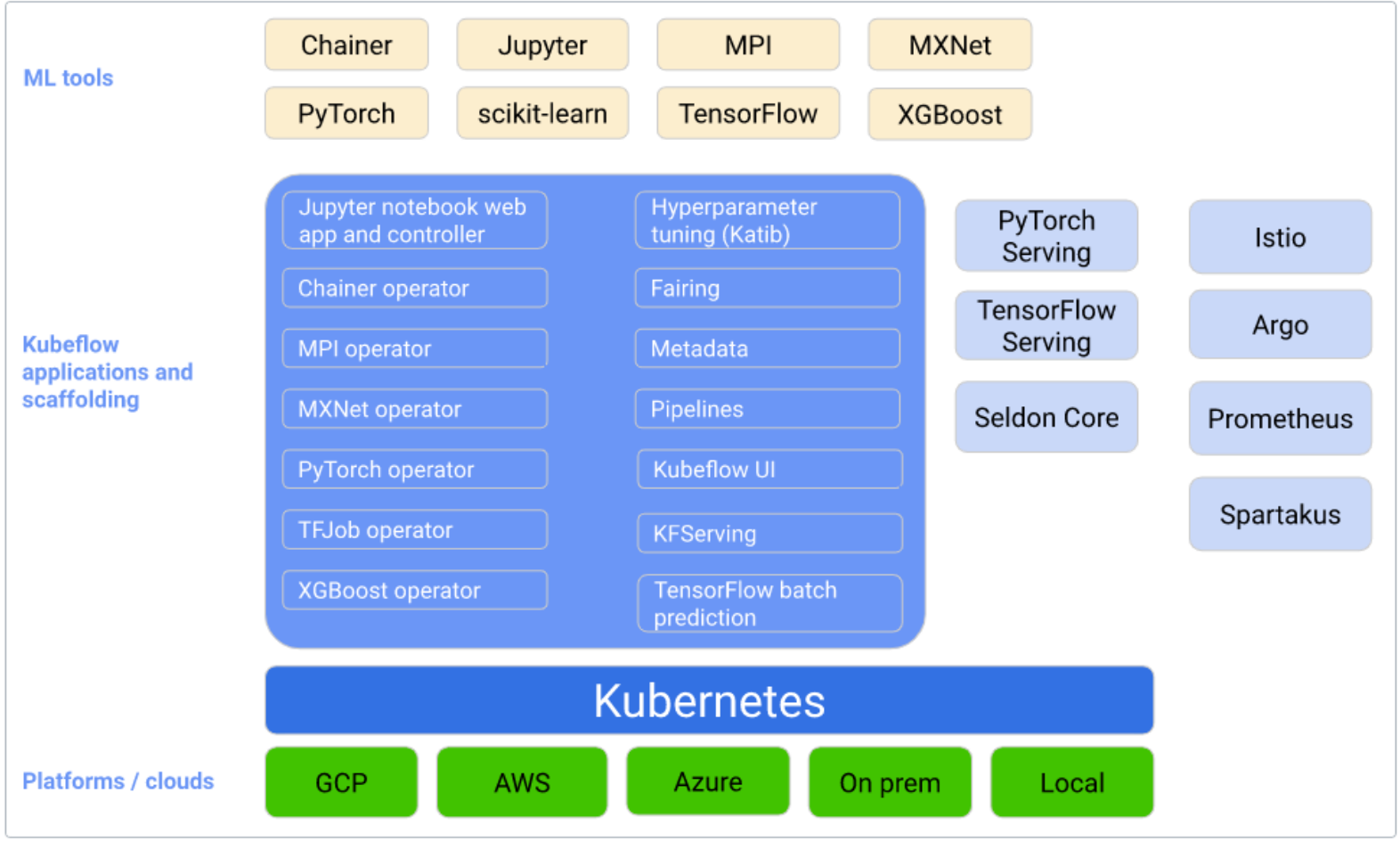
从无状态应用，到企业核心应用，到数据智能应用



Kubernetes应用场景-构建PaaS平台



Kubernetes应用场景-集成深度学习框架

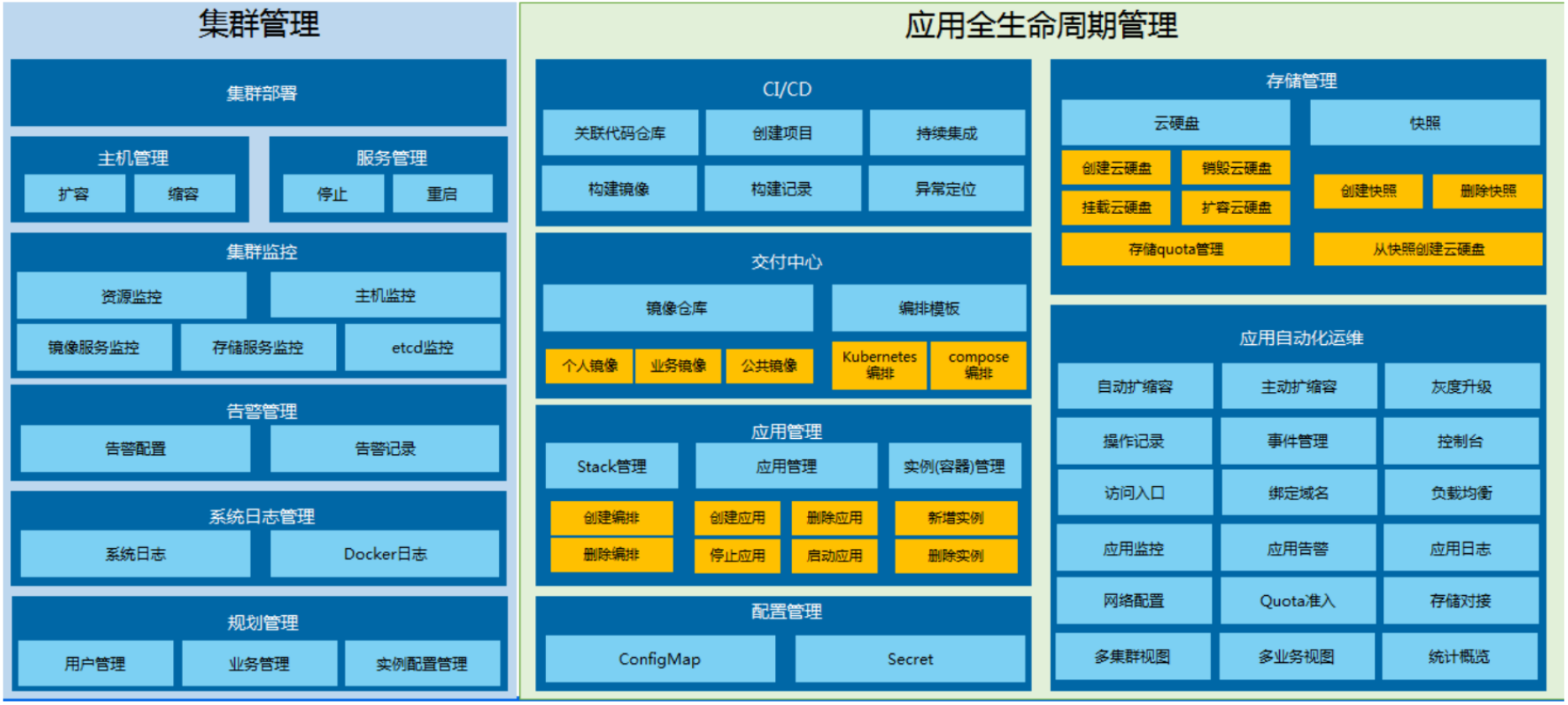


Kubernetes应用场景-集成区块链

Kubernetes使用案例

中国移动 China Mobile

腾讯基于Kubernetes的企业级容器云平台



Kubernetes使用案例

京东从 OpenStack 改用 Kubernetes

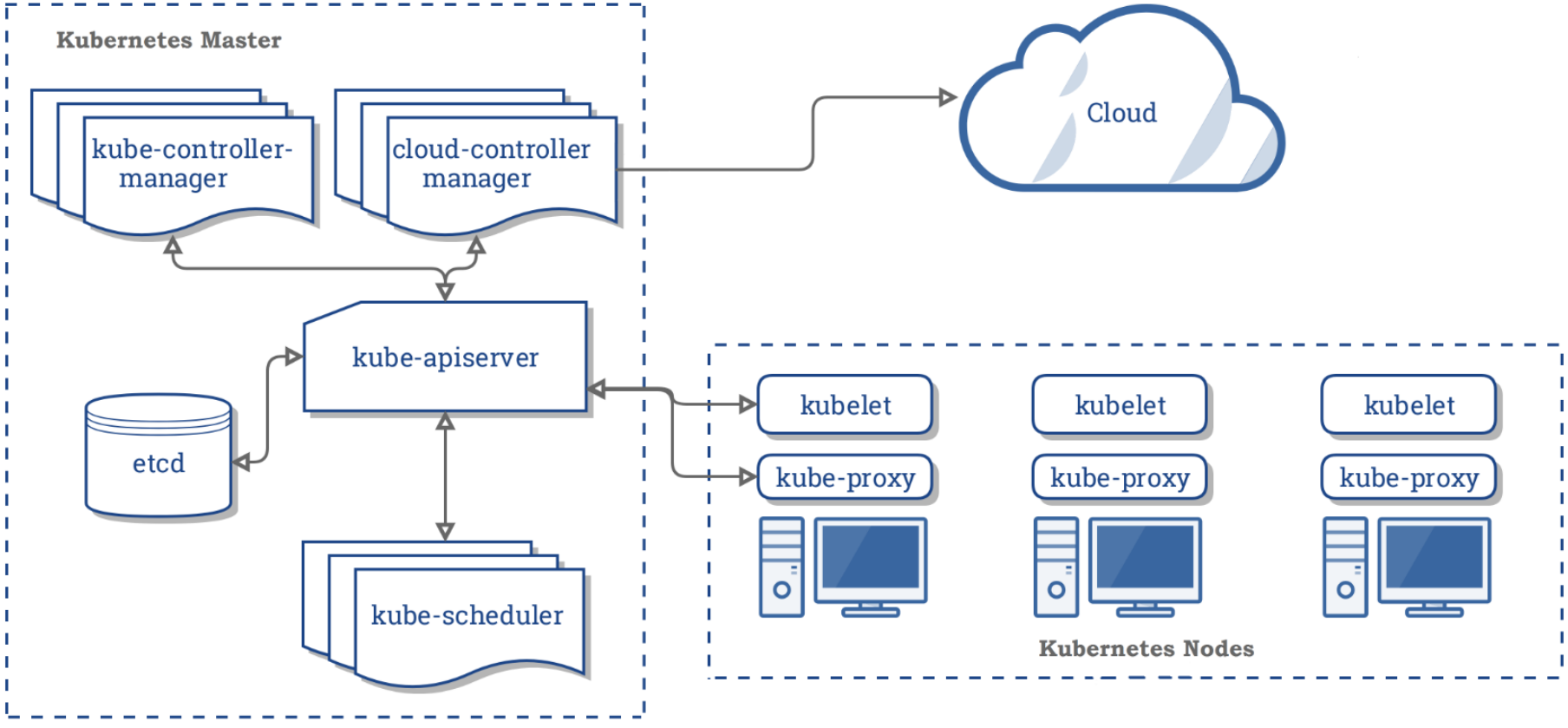
Kubernetes使用案例

DigitalOcean推出托管Kubernetes服务

Kubernetes使用案例

阿里管理上万个Kubernetes集群

Kubernetes核心组件



Kubernetes核心组件

MASTER

API Server

kubernetes系统的入口，封装了核心对象的增删改查操作

Scheduler

插件式的调度器，负责集群的资源调度，为新建的pod分配机器

Controller-Manager

负责管理各种控制器。如ReplicationController，EndPointController等

SLAVE

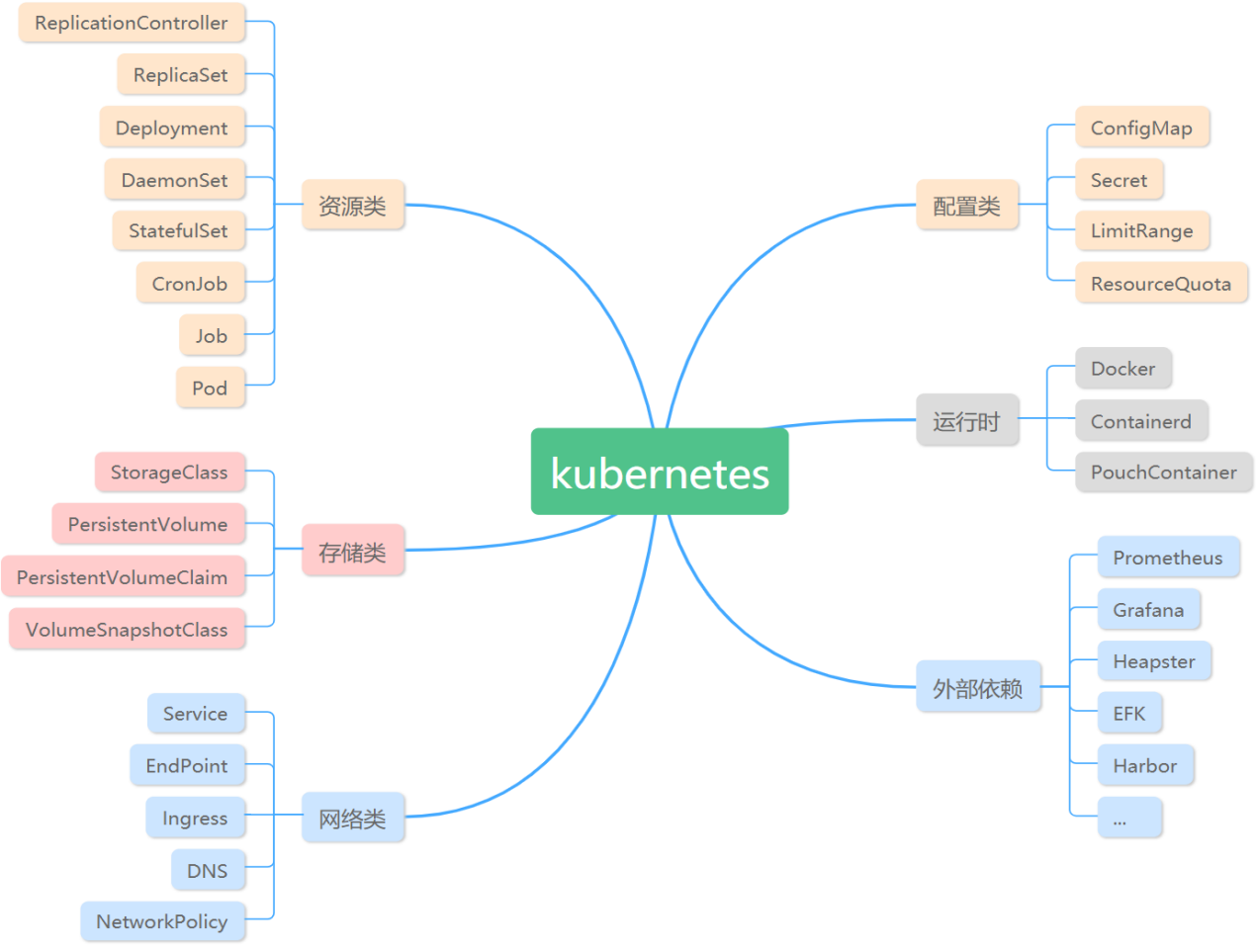
Kubelet

负责管控docker容器，如启动/停止、监控运行状态等

Kube-proxy

负责为pod提供代理。它会定期从etcd获取所有的service，并根据service信息创建代理

Kubernetes核心概念



Kubernetes核心功能

应用编排

提供丰富的原子对象，通过编写YAML文件，可以动态创建由不同对象组成的完整应用

自动恢复

持续检查应用的运行状态，对应用错误进行自动恢复，根据实例状态动态配置负载均衡策略

容器存储

容器存储系统提供容器数据的持久化存储功能，解决容器挂掉后数据丢失引发的问题，使用CSI支持多种不同类型的存储方案

容器网络

通过CNI适配不同类型的网络方案，提供平台内容器服务间的高效通信

滚动升级

应用一键升级，服务升级过程中提供可持续的不中断的服务

动态伸缩

支持容器资源动态伸缩；支持根据自定义指标对容器实例个数进行动态伸缩

Kubernetes和微服务

中国移动 China Mobile

注册中心	应用启动自动注册，调用方自动发现上线应用。服务异常自动隔离。
配置中心	多环境配置管理，支持在线管理配置信息，客户端实时生效。支持版本管理，快速回滚。
负载均衡	服务调用服务会采用一定的分发策略，一般是客户端分发策略。
降级、熔断、重试	服务或依赖服务异常时，返回保底数据。熔断，若依赖服务多次失效，则断开，不再尝试调用，直接返回降级值。重试，熔断后，定期探测依赖服务可用性，若恢复则恢复调用。
发布与回滚	红绿部署、灰度、AB Test等发布策略，可快速回滚应用。
动态伸缩	根据服务负载情况，可快速手动或自动进行节点增加和减少。
监控与告警	服务定期健康检察、指标统计、异常告警通知运维。
统一日志管理	集中收集各服务日志汇总，方便排障、问题调查、应用日志分析等。

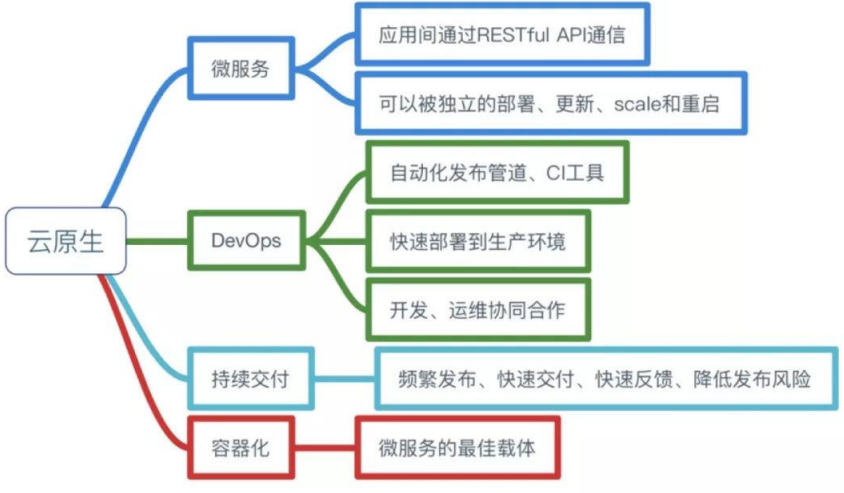
Kubernetes本身就是微服务架构

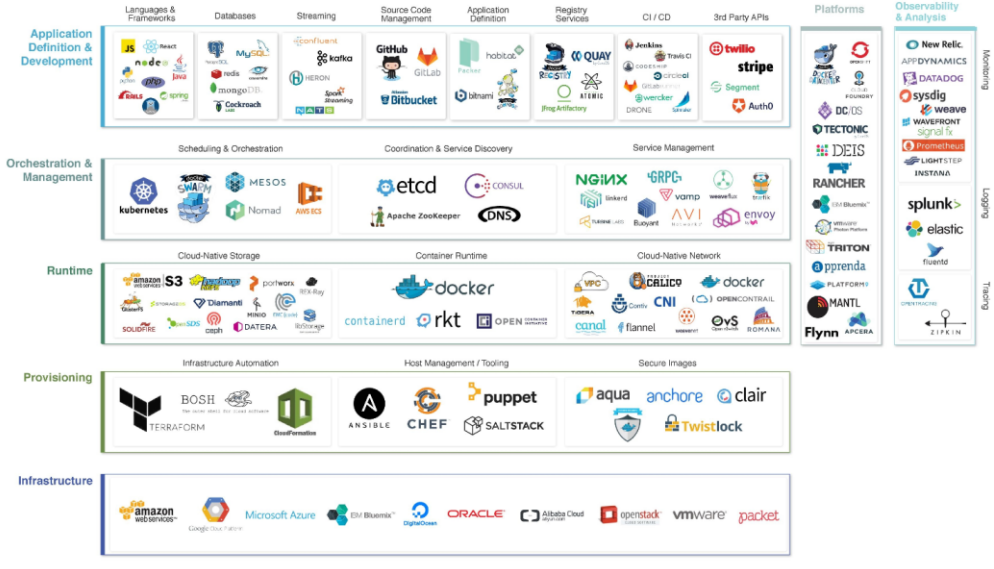
Kubernetes适合微服务应用的设计

Kubernetes和云原生

云原生

云原生是一种应用设计理念，从架构设计、开发方式到部署维护整个软件生命周期都基于云的特点设计，从而构建原生为云而设计的应用，充分利用和发挥云平台的弹性以及分布式优势





Kubernetes做了**很多**，但是还**不够**，需要其他周边方案的支持，如监控、日志、镜像、精细化路由、调用链追踪等

我们的团队

中国移动 China Mobile

01 **规模**

30人团队专攻Kubernetes和云原生相关领域

02 **学历**

95%的团队成员是研究生学历

03 **经验**

团队成员平均3年以上的Kubernetes相关领域设计开发经验

04 **背景**

社招团队成员来自腾讯、百度、华为等企业

Kubernetes的缺陷

01 **灵活但是复杂**

部署和运维起来复杂，需要有经过专业的培训才能掌握

02 **缺少应用的概念**

对于上层应用的支持不够完善，需要编写配置大量的 YAML 文件，难于管理

03 **完整的解决方案依赖大量的外部组件**

必须的镜像、监控、日志、调用链追踪、精细化路由控制都依赖外部组件

04 **缺少统一管理**

集成的开源组件众多，缺乏统一管理

01 能力开放平台简介

能力开放平台 - 简介

中国移动 China Mobile

简介

基于Kubernetes构建能力开放平台，为智慧城市行业能力提供统一的运营管理能力，完成智慧城市项目复杂场景的部署落地、统一运维以及一致交互接口

统一部署运维

提供统一的部署和运维能力，实现应用与平台环境解耦；完成服务体系的统一监控与运维；实现混合异构云部署方案

超脑平台门户

构建中心能力运营管理平台，汇聚内外能力，实现统一展示，计费运营

业务汇聚平台

提供能力，消息，数据，设备和多云集成技术方案；支撑智慧城市行业应用、数据、服务、资源等的协同

公共中间件

实现统一认证管理，消息总线，服务治理，安全防护体系，数据库中间件等

能力开放平台 - 功能架构概览

中国移动 China Mobile

安全/运维/部署

- 监控中心
- 告警中心
- 日志中心
- 安全中心
- 统一运维
- 统一部署
- 镜像管理
- 服务治理

超脑平台门户

能力上/下架	能力展示	应用体验馆
服务管理	费用中心	解决方案馆

业务汇聚平台

能力集成	消息集成
设备集成	数据集成

交互应用层

- **超脑平台门户**是超脑产品和解决方案的统一展示和体验门户网站
- **业务融合平台**通过融合原子能力，快速构建行业解决方案

API 网关

鉴权中心	消息引擎	资源管理	数据管理
租户管理	应用管理	订单管理	计费管理
应用模板代理	K8S代理	Docker代理	多云管理

公共组件层

- 汇聚支撑平台层能力，便于交互层使用；
- 提供平台公共能力，如鉴权，消息引擎，资源管理，租户管理等功能。

kubernetes　docker　Istio　HARBOR

支撑平台层

- 能力平台的支撑底座；
- 提供镜像构建管理，容器编排和服务治理功能。

裸机服务器

私有云平台

openstack.　vmware

公有云平台

阿里云　腾讯云

基础资源层

- 能力平台的基础运行环境
- 提供计算，存储，网络资源

02

统一部署运维

统一部署运维 - 统一部署

中国移动 China Mobile

统一部署

部署平台提供可视化多集群容器管理平台自动化离线部署能力，包括能力仓库，多云接入，能力管理及自动部署等能力，快速交付容器运行时环境

具备端到端服务能力的一站式发布，支持用户创建各种内部、外部能力，提供更丰富的云服务体验

以插件形式集成各种主流云平台，屏蔽底层云平台差异，保障能力跨平台运行的环境一致性

从企业业务和应用的视角来分配管理各种云的资源，优化IT资源的交付方式，轻松实现各类IT资源的全生命周期管理

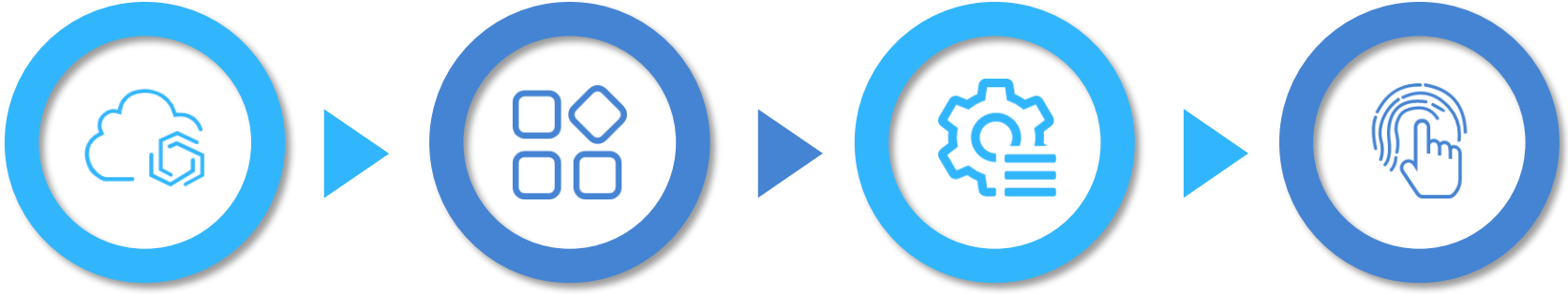
除了跨云能力的一键部署外，还可根据客户需求定制个性化实施方案

统一部署运维 - 统一部署

中国移动 China Mobile

部署使用

- 部署平台面向内部实施人员；部署平台本身只在项目初期安装一次，后续无需重复安装
- 支持超脑平台门户、业务汇聚平台，数据中台等平台或应用的一键安装部署



客户购置云服务

用户购置云服务平台，需提供相应的平台账户给与运维人员，由运维人员进行部署工作

一键部署管理平台

可选择安装运营平台、汇聚平台及其他平台应用

登录系统配置应用

选择平台或应用，进行如镜像仓库、K8S、Hadoop，Hive等平台或应用相关信息

一键部署应用

在配置完成后，点击部署按键即可进行一键部署

统一部署运维 - 统一运维

中国移动 China Mobile

统一运维

提供全面的IT资源及应用性能监控解决方案，提供故障的快速发现、通知、恢复功能，确保服务器与应用的正常健康运行，保证业务系统的性能和稳定性

集中监测

实现跨平台的7*24主动监测，包括IT资源，应用运行各类指标检测

应用全生命周期管控

从技术和管理层面共同实现面向应用的全生命周期闭环管控

统一数据管理及分析

广泛支持主流数据源和日志、流式、文本、网络等不同数据类型，构建完整的统一数据管控和分析平台；发觉数据潜在特性

告警管理

提供自动化分级告警评估、风险提示等功能，帮助运维人员快速准确定位故障

可视化

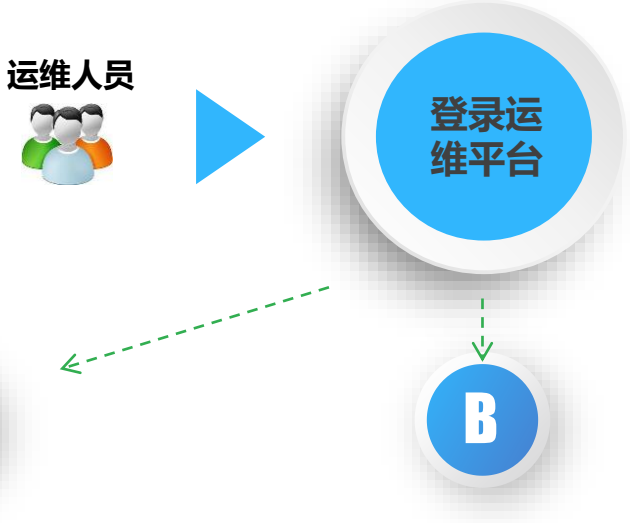
帮助运维人员直观掌握应用运维的有效信息，全面了解数字化运营状态，通过可视化管理与有效决策，提升应用管理与监控管理的效率

统一部署运维 - 统一运维

中国移动 China Mobile

运维使用

运维平台主要面向运维人员，帮助运维工程师以最低的成本和最快的速度排查服务隐患，处理服务故障；提高服务性能，优化服务成本



资源统计

运维平台首页展示系统的概要信息，包括集群维度的监控信息、实例统计等

实例管理

实例管理页面展示实例详情，包括实例的状态、历史资源使用情况、实时日志等

监控告警

监控告警页面展示告警信息、系统核心组件指标信息、不通维度的资源监控数据等

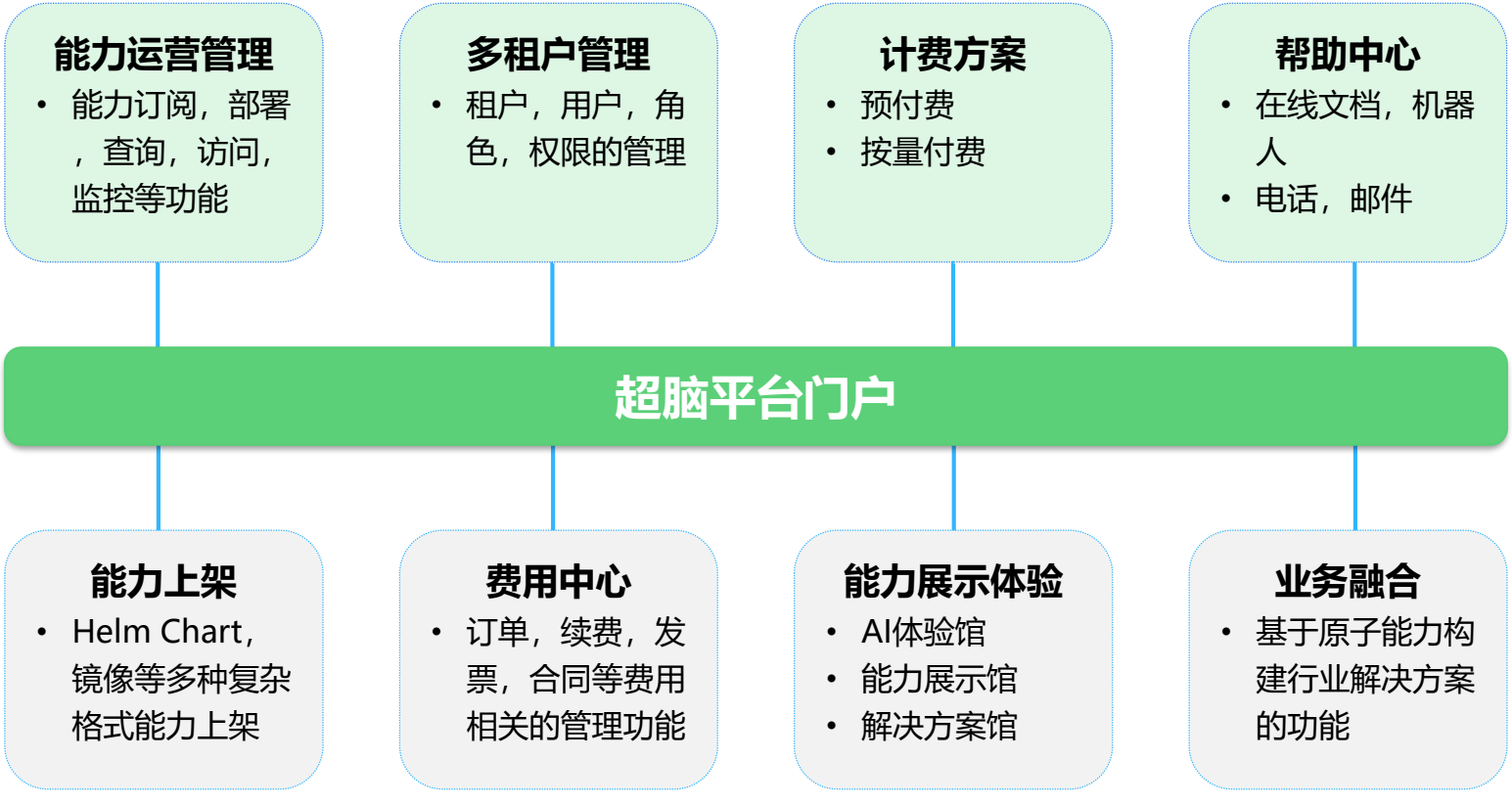
03 超脑平台门户

超脑平台门户 - 概述

中国移动 China Mobile

超脑门户

超脑平台的统一门户网站，实现面向**终端用户**的能力全生命周期的运营管理、统一计费、多租户管理、能力展示体验等功能



04 业务汇聚平台

业务汇聚平台 - 目标

五大目标

加速智慧城市平台能力的构建，实现业务融合，行业赋能，构建生态，简化集成开发和云边协同的五大目标。

业务融合

借助于标准的能力集成，数据集成和消息集成能力，实现原子能力的融合，为构建行业解决方案提供便利

行业赋能

通过标准的能力集成，数据集成，消息集成，设备集成接口，赋能于智慧城市行业内外厂商和客户

构建生态

通过赋能于智慧城市行业内外厂商和客户，进一步构建智慧城市行业相关标准，最终实现构建智慧城市行业生态的目标

简化集成开发

通过统一封装底层AI，大数据，IoT，GiS等行业原子能力，灵活调度系统资源，向上提供标准的接口，简化行业解决方案的集成开发时间，加速行业应用上线

云边协同

借助于能力集成，消息集成，数据集成和设备集成，最终通过多云集成实现云边协同能力，支持多种协同方式，融合边缘计算网络，扩展智慧城市能力边界

业务汇聚平台 - 概述

产品定义

屏蔽PaaS层原子能力的差异性，提供**统一标准的能力接口**，赋能于智慧城市行业内外厂商和客户，实现**业务融合，行业赋能，构建生态，简化集成开发和云边协同**的目标，为构建智慧城市行业解决方案提供便利，加速行业应用上线。

智慧城市行业解决方案


智慧安防


智慧城管

智慧党建


智慧消防


智慧政务


智慧环保

业务汇聚平台

能力集成 | 消息集成 | 数据集成 | 设备集成 | 多云集成

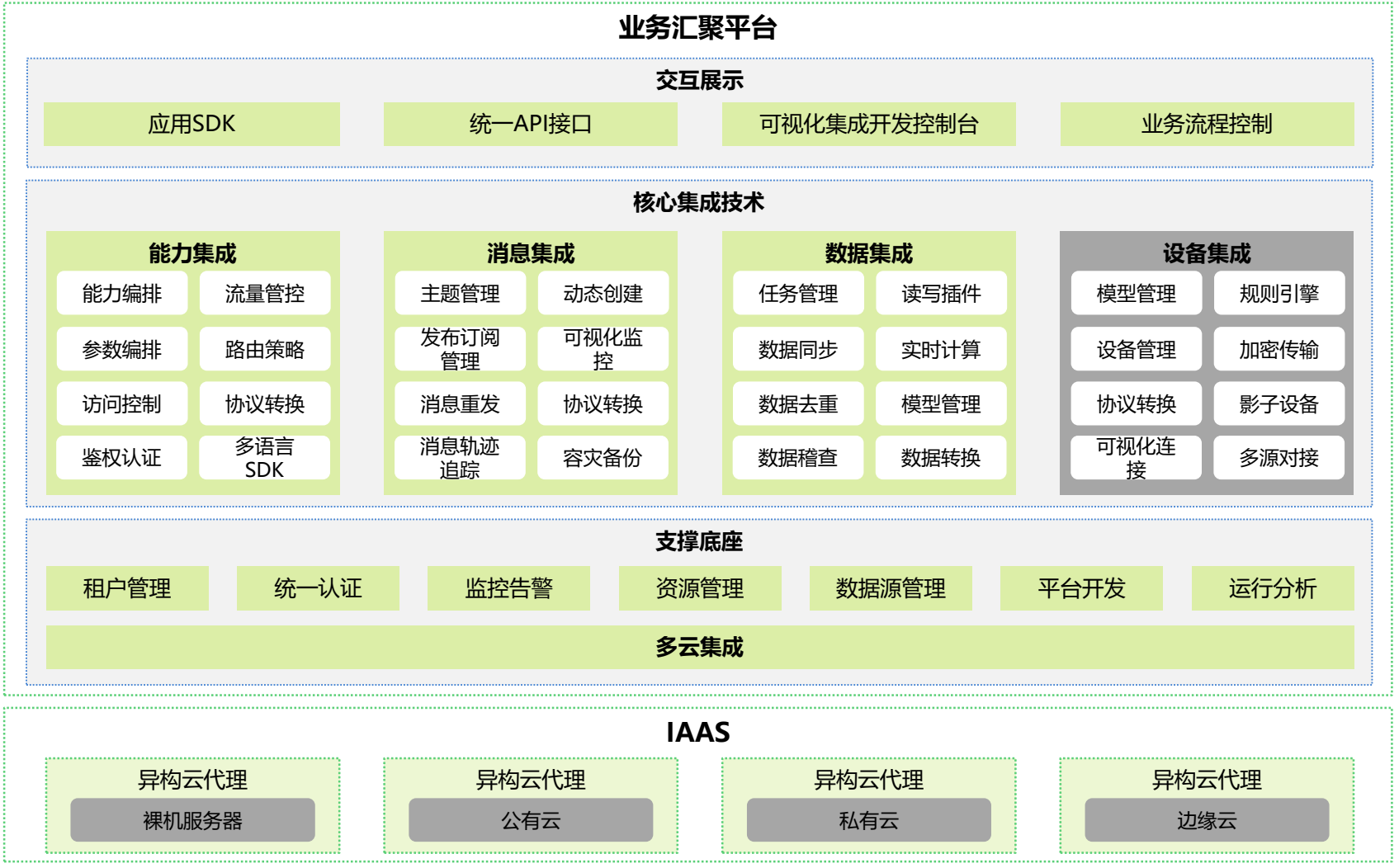
PaaS层原子能力

AI	大数据	物联网	GIS	其它
辅助决策	数据采集	设备管理	空间数据分析	统一认证
人脸识别	数据管理	设备模型	空间数据管理	权限管控
智能推理	数据应用分析	影子设备	空间数据存储	行业中间件

IAAS

裸机服务器 | 公有云 | 私有云 | 边缘云

业务汇聚平台 - 功能架构图



业务汇聚平台 - 核心功能

中国移动 China Mobile

能力集成

实现各行业原子能力和数据的集成，并以API的标准形式提供给上层行业应用，简化分享数据或提供服务的过程，降低业务融合，构建行业解决方案的成本

数据集成

支持多种数据源之间的灵活、快速、无侵入式的数据集成，可以实现跨机房、跨数据中心、跨云的数据集成方案

消息集成

实现了包括发布订阅、消息轨迹追踪、资源统计、监控告警等功能的消息队列服务，提供安全、标准化的消息通道。

设备集成

与智慧城市各类IOT，边缘网关对接，提供中心云能力，实现设备上云，统一管控

多云集成

实现异构混合云的跨云调度，统一协同，统一编排，实现多云之间能力，消息，数据和设备的快速标准化集成，帮助客户打通应用、数据、设备及合作伙伴之间的信息孤岛，实现消息和数据共享

能力开放平台--产品特性

中国移动 China Mobile

□ 与基础云计算平台的区别

	基础云计算平台	能力开放平台
业务核心	以管理资源（计算、存储、网络）为核心	以运营能力为核心
关键指标	以管理的vcpu数量、内存大小、存储大小为关键指标	以支持的能力形态数量为关键指标： • 内生能力：大数据，算法，智慧城市解决方案等 • 外部能力引入：网络开放平台，边缘计算平台等
运营内容	支持传统以计算、存储、网络为核心的能力运营	支持不同形态的能力运营，包括各种能力的上架、下架、部署、计费等
关联关系	为能力开放平台提供底层资源支撑	实现数据互通，业务互通，进一步推动云计算发展

能力开放平台内置**多云管理**组件，可以运行在各种基础云计算平台之上

Thank You