云原生产业大会 2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

联通数科云原生时代探索与实践

联通数字科技有限公司-张宇

CAICT 中国信通院

介绍

关于联通数字科技有限公司

整合组建

以联通系统集成公司为主体组建数科公司，所有联通产业互联网有限公司股权相应转入数科公司运营公司以云数据、大数据、物联网、安全等4家子公司和部分合资公司股权增资数科公司。

- 联通系统集成有限公司
- 联通智慧安全科技有限公司
- 联通物联网有限责任公司
- 联通大数据有限公司
- 联通云数据有限公司

联通数字科技有限公司

“组建联通数科公司，既是主动适应数字经济“跨域整合”新生产力的变化，重构“融合创新”的新生产关系，也是紧跟数字经济需求侧的新变化推动的供给侧结构性改革，是中国联通打造独特创新竞争优势、实现创新赛道差异化突围的重大战略布局。” - 王晓初董事长

关于团队

2017年组建而成，100余人团队近4年时间专注打造云原生能力与基座，助力内外部客户数字化转型。2020年获得了中国信通院颁发的《可信云最佳服务实践-PaaS服务》奖项。

关于我

联通云原生能力与平台项目核心成员，参与联通信息化云原生改造全过程，对云计算及云原生技术有着深刻的理解和丰富的实践经验。
2020年中国电子信息行业联合会举办的《第四届全球程序员节》之上，荣获《全国年度十佳新锐程序员》奖项。

内容大纲

1. 企业数字化转型面临的挑战
2. 联通IT基础设施演进历程与成果
3. 未来探索与展望

当前，多变的内外环境正在塑造企业，同时对IT提出了更高要求

内部挑战

1、业务流程调整，系统如何快速变更?

- 松耦合、组件化、服务化的系统架构，支撑业务流程的快速变更；

2、企业的经营状况，如何快速掌握?

- 实时数据监控采集，集中数据管理，实现交易数据需要前后贯通，决策数据集中实时展示，决策信息移动端展示；

3、新业务的出现，信息化系统如何能快速支撑?

- 敏捷的开发管理体系，支持支撑能力的快速构建；底层资源和技术能力快速支撑；
- 平台化的能力管理体系，支持通过服务编排的方式实现快速的业务支撑；

外部挑战

4、新技术的出现，如何快速赋能业务的发展?

- 组件化、服务化的能力管理方式和系统构建方式，支持新技术的快速引入；
- 平台化的能力管理体系，让新技术以服务的方式进行构建并对应用提供支撑，实现业务赋能

5、内外部的优秀资源，如何实现开放和共享，实现产业链协同?

- 能力开放平台，提供外部能力纳管、内部能力开发的能力；实现外部用户访问权限和配额管理

IT能力新要求

低成本	动态实时	图形可视
随时可见	松耦合	组件化
服务化	能力沉淀	高效支撑
能力开放	内外打通	……

新的IT能力要求，对于基础设施带来了新的挑战

- IT能力要求的提升，对于基础设施也带来了更多的诉求与挑战
- 需要构建新的企业数字化转型基础设施，并以此构建企业新型IT架构，助力企业数字化转型
- 通过企业数字化转型基础设施，来实现提升企业资源利用率、适应市场需求的快速变化、提高生产效率等

联通数字化转型的挑战与需求

- 2017年联通开始进行混改，公司加速数字化、互联网化转型
- 联通拥有丰富的基础设施资源，但数字化转型过程中如何实现资源智能调度、最大化利用、能力共享，进一步赋能内部以及各类合作伙伴应用创新，实现高质量发展，是一个痛点问题

痛点

- **计算/存储资源使用不均衡，弹性调度不足**
- **技术组件支撑不全，重复建设成本居高不下**
- **应用架构设计落后，迭代周期长**
- **迫切需要一站式云平台支撑业务创新**

智能化基础设施

- **算力及存储资源一站式供给**
- **PaaS能力免运维快速提供**
- **应用开发部署及代码上云，提升交付效率**
- **业务数据上云、大数据平台上云，数据价值深挖**

通过持续研究和探索，需要打造智能化基础设施，解决痛点问题

内容大纲

1. 企业数字化转型面临的挑战
2. 联通IT基础设施演进历程与成果
3. 未来探索与展望

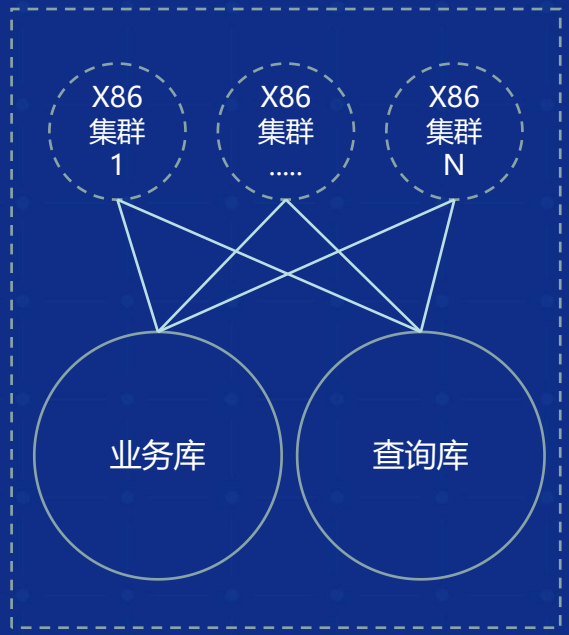
历程回顾

早期

高端硬件系统

2013年

X86化、虚拟化、减负分流



历程回顾

2016年

Mesos、分布式、容器化

2018年

云原生、Kubernetes

基础设施与技术演进的创新成果-沃云集成平台

- 沃云集成平台纳管跨数据中心的海量资源，基于K8s与Docker构建智能化基础设施，通过统一服务集成框架，提供云原生（容器、 DevOps、微服务）、大数据、物联网、人工智能与安全相关能力，并以多租户的方式向用户在线开放，实现分钟级交付和弹性扩缩容，赋能用户一线生产经营，助力企业实现数字化转型。

先进的容器化技术　**丰富的组件服务**　**统一的服务集成框架**　**互联网化的运营模式**

内部应用　数据应用　管理应用　政企应用　公众应用　…

外部应用　智慧城市　数字政府　工业互联网　…

统一服务集成框架

中间件数据库	大数据	人工智能	安全	物联网	DevOps	微服务开发
Redis, MySQL, MyCat, Kafka, MongoDB	Hadoop, Spark, Hbase, Hive, Impala, Storm	TensorFlow, Caffe, PyTorch	区块链, 数据脱敏, 镜像安全扫描, 漏洞检测	Serverless 云函数, 时序数据库	CI/CD, Jira 项目管理, 镜像仓库 Harbor	Istio, Spring Cloud, Dubbo

容器管理平台（Kubernetes+Docker）

资源管理　资源调度　资源隔离　弹性伸缩　安全管控　负载均衡

基础设施　CPU资源　GPU资源　内存资源　存储资源　网络资源

统一运营门户
一点接入，一站服务

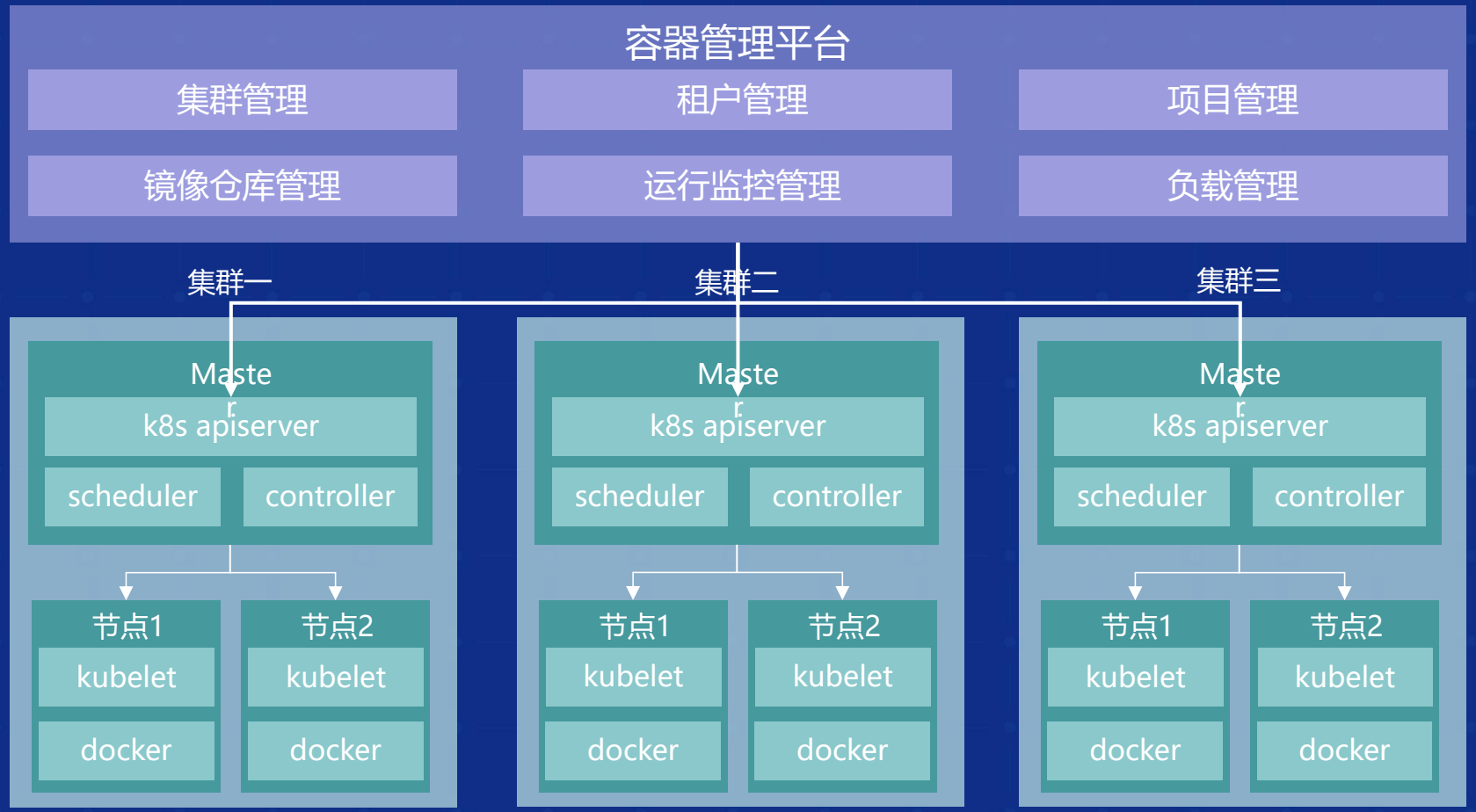
统一资源调度
异构资源，统一调度

统一监控平台
集群组件，一点看全

统一产品交付
分钟交付，弹性伸缩

平台能力-容器管理能力

- 构建容器管理平台，对于K8S与Docker的统一管理。基于传统基础设施可快速构建K8S集群，并且以多租户形式对多K8S集群进行统一纳管，降低K8S与容器使用门槛，提高企业云原生基础设施使用与运维效率。



特性：

- 多k8s集群多版本管理
- 多租户、多项目管理
- 项目配额管理
- 网络负载管理
- 应用部署可视化界面
- 与DevOps模块的结合

平台能力-丰富的PaaS能力

中间件数据库（11）

Redis　MySQL　MyCat

MongoDB　Kafka　ES

大数据（15）

Hadoop　Spark　Hbase

Hive　Impala　Storm

安全（4）

区块链　数据脱敏

镜像安全扫描　漏洞检测

人工智能（4）

Tensor Flow

PyTorch

物联网（3）

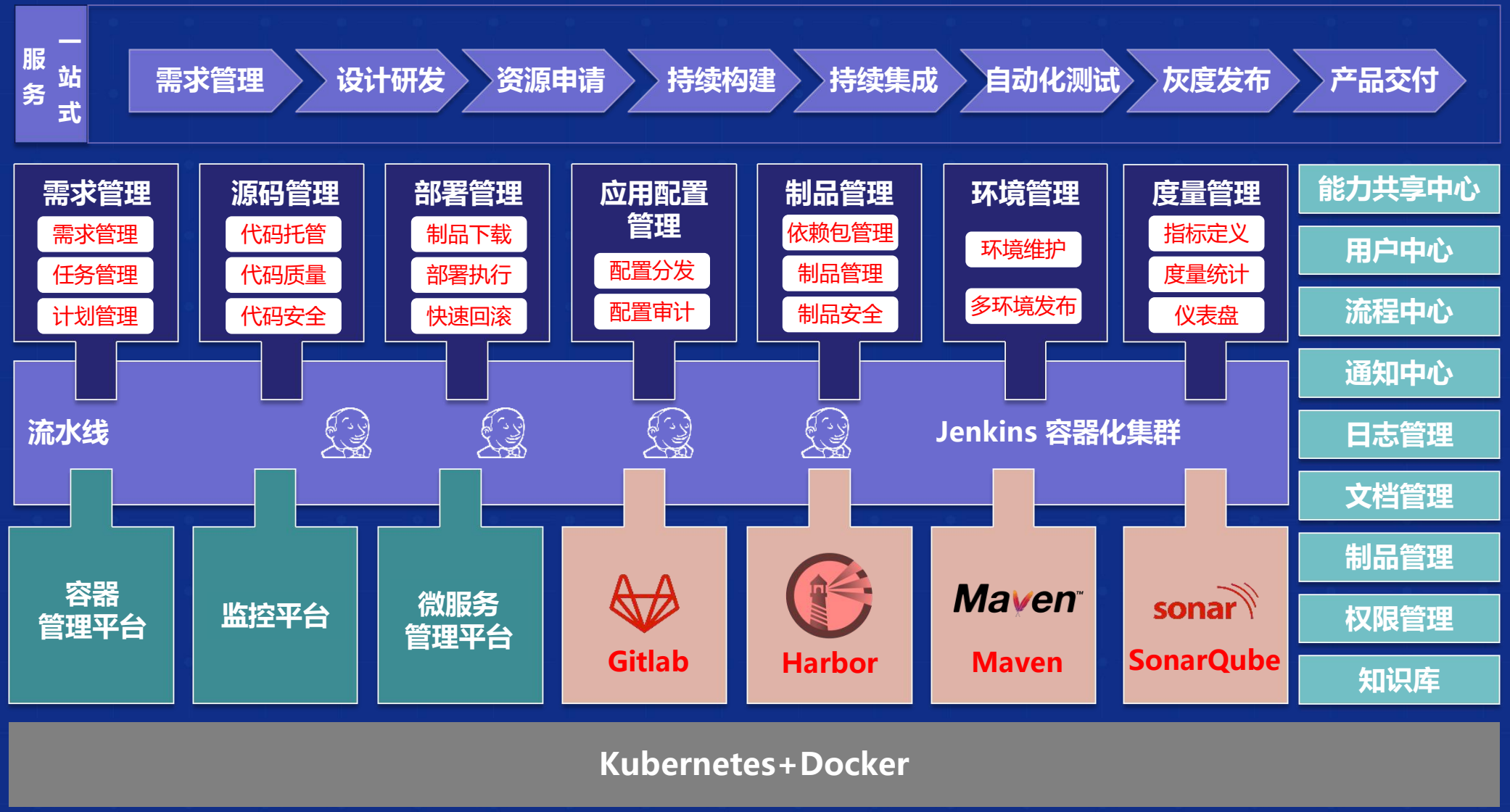
时序数据库

时空数据库

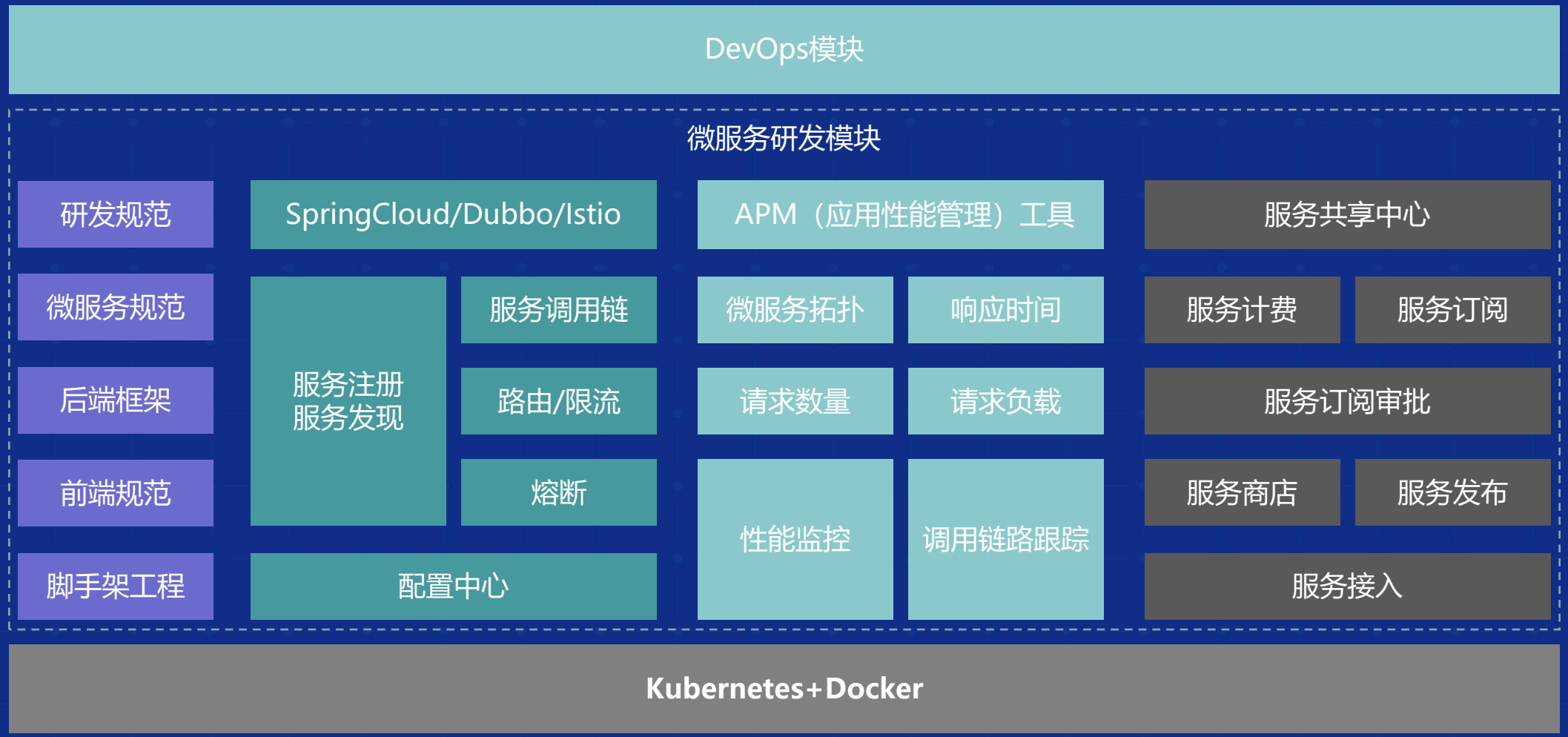
中间件封装与编排

- 根据联通多年组件能力生产实践与使用经验，对中间件**进行了配置与参数的优化**，保障了组件能力的性能；
- 围绕开源组件能力，将开源组件能力相关的监控、日志、备份、可视化参数设定、Dashboard等**运维功能进行封装与编排**，组件拉起是同时获得相关运维功能；
- 使用了Helm与Ansible-Playbook**两种编排与封装方式**，可分别在容器化与虚拟化的环境中快速拉起，满足用户多种需求；

平台能力-DevOps能力



平台能力-微服务开发能力



技术创新点-多样化能力组件集成

- 自研统一服务集成框架，定义了一套标准化的服务集成接口，涵盖服务的全生命周期管理（查询、开通、变更、退订等），快速对接各类能力组件，实现异构能力组件的统一纳管、自助拉起、弹性伸缩和在线开放，形成了能力众筹的技术生态，为租户充分赋能。

问题：作为联通的数字化底座，接入的能力组件由多个能力供应商提供，如何接入多样化的异构能力？

解决方案：

- 通过自研的统一服务集成框架，制定了一套标准化的接口，快速进行能力对接。
- 能力供应商提供服务代理，实现能力查询、能力开通、能力变更、能力退订等服务接口。
- 平台通过标准化产品控制台，和各服务代理对接，适配多租户体系，并进行资源隔离，实现从服务开通到退订的全生命周期管理。

成效：

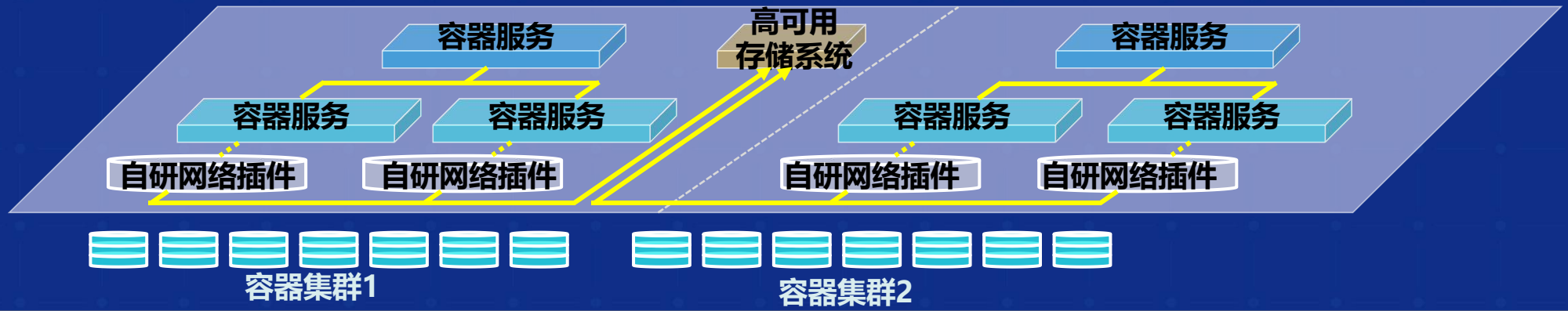
1. 统一服务集成框架给平台带来极强的扩展性；
2. 简单有效的标准化接口提升了能力对接效率30%以上。

技术创新点-容器集群间网络互通

- 平台纳管的异构资源分散在4大数据中心，相应的能力组件也部署在不同数据中心的不同集群中，通过联通自研的网络插件，实现了多集群共用一套网络，解决了数据中心内部不同集群间以及跨数据中心的不同集群间网络的互通问题。

难点

在部署原生Flannel的K8S集群中，容器网络环境下每个容器有独立虚拟IP地址，并且此地址无法与外部物理IP直接互联。受限于此，多K8S间容器互访一直是业内技术难题。国内外通常采用业务拆分的方案避免单业务链跨多个K8S集群，但是这种方案会给集群管理和业务管理带来诸多不便。



解决方案：

平台创新性的提出**多容器集群共享一个高可用存储系统**的技术方案，通过自研网络插件，基于vxlan实现跨集群overlay容器网络，实现了在多个容器集群间进行**统一的子网划分、容器IP管理、网络策略管理等功能**，完美解决了多集群间容器互访的难题。

成效

1. 此方案支持数据中心内部不同集群互访，也支持跨数据中心的不通集群间的网络互访，总集群规模可达**5000节点**
2. Route、ARP、FDB以及Iptables规则的增加对服务器CPU负载影响**小于1%**。

平台应用效果

传统基础设施

VS

沃云集成平台

传统基础设施		沃云集成平台
利用率10%	资源利用率	利用率60%
至少2天	扩展集群	分钟级
1小时以上	应用部署	一键发布、秒级启动
至少1天	应用扩展	动态扩容、秒级启动
一个月左右	发布周期	1周左右
中断业务、分钟级	升级/回滚	不中断业务、秒级回滚

1. **提高资源利用率**
   容器化、资源池化
2. **业务快速开发上线、敏捷迭代**
   业务逻辑+积木式PaaS组件，拿来即用
3. **支持大规模互联网化业务**
   大流量、高并发、高可靠
4. **实现系统的高扩展、高弹性**
   分布式、微服务架构
5. **实现智能运营**
   快速响应、安全隔离、故障自愈
6. **降低运营成本**
   长期投入边际效应递减

底座能力全面升级，可赋能内外部转型创新

- 对内，提供智能化数据基础设施，驱动数据价值释放，打造行业样板示范。
- 对外，输出新基建相关产品及技术能力，助力行业客户打造行业应用中心、大数据中心、智能计算中心，赋能行业客户进行数字转型、智能升级、融合创新。

内部
数字化底座

- 算力及存储资源一站式供给
- PaaS能力快速免运维提供
- 应用开发部署及代码上云，提升交付效率
- 大数据平台上云，AI训练上云，数据价值深挖

- 行业智能基础设施构建
- 云、大、物、智、安能力平台化输出
- 开拓数字经济场景化应用

外部
行业新基建

对内
数字化使能
激发应用创新

线上申请
统一运营门户

即时开通
分钟交付
弹性伸缩

自助使用
免安装运维
自监控使用

应用开发上云

数据上云

AI上云

沃云集成平台

全栈容器化
异构算力 弹性调度

PaaS能力众筹
云、大、物、智、安

统一研发体系
敏捷开发 持续交付

对外
赋能行业客户打造平台型、生态化企业

内外部整体应用情况

对内：数字化底座

- 打造智能化数据基础设施，弹性调度跨数据中心异构资源，承载企业内部IT系统集约化建设，保持行业领先优势。
- 实现省公司应用上云、数据平台上云，AI训练上云，管理信息系统集约，激发数据价值创造活力，重塑数字化管理能力。

纳管异构资源（跨4大数据中心）

- 节点数 2000+
- 容器规模 2.3万+
- GPU卡显存 2000G+
- CPU核数 5.5万+
- 内存 350TB+
- 存储 47PB+

使能业务

- 大数据处理类 100+
- 省分大数据平台 10+
- 微服务类 350+
- AI训练类 70+
- 区块链应用类 8+

对外：行业新基建

- 云、大、物、智、安等46种能力组件无缝集成至公有云平台（沃云），极大丰富产品类型，繁荣应用生态。
- 面向数字政府、智慧城市、工业互联网等16个行业领域输出整体解决方案及新基建能力，赋能客户高质量发展。

行业应用开发

- 入驻研发人员 1700+
- 管理源代码 800万+
- 项目数 500+
- 研发效率提升 50%以上

行业云赋能

- 覆盖行业/领域 16+
- 平台订单数 5+
- 产品数 150+
- 产品订单数 300+

电子商城 | 用户中心 | 智慧门户 | 人力系统

AI训练 | 大数据生产 | 经营分析 | 精准营销

工业互联网 | 智慧教育 | 医疗健康 | 智慧交通

智慧城市 | 数字政府 | 文化旅游 | 生态环保

沃云集成平台

内容大纲

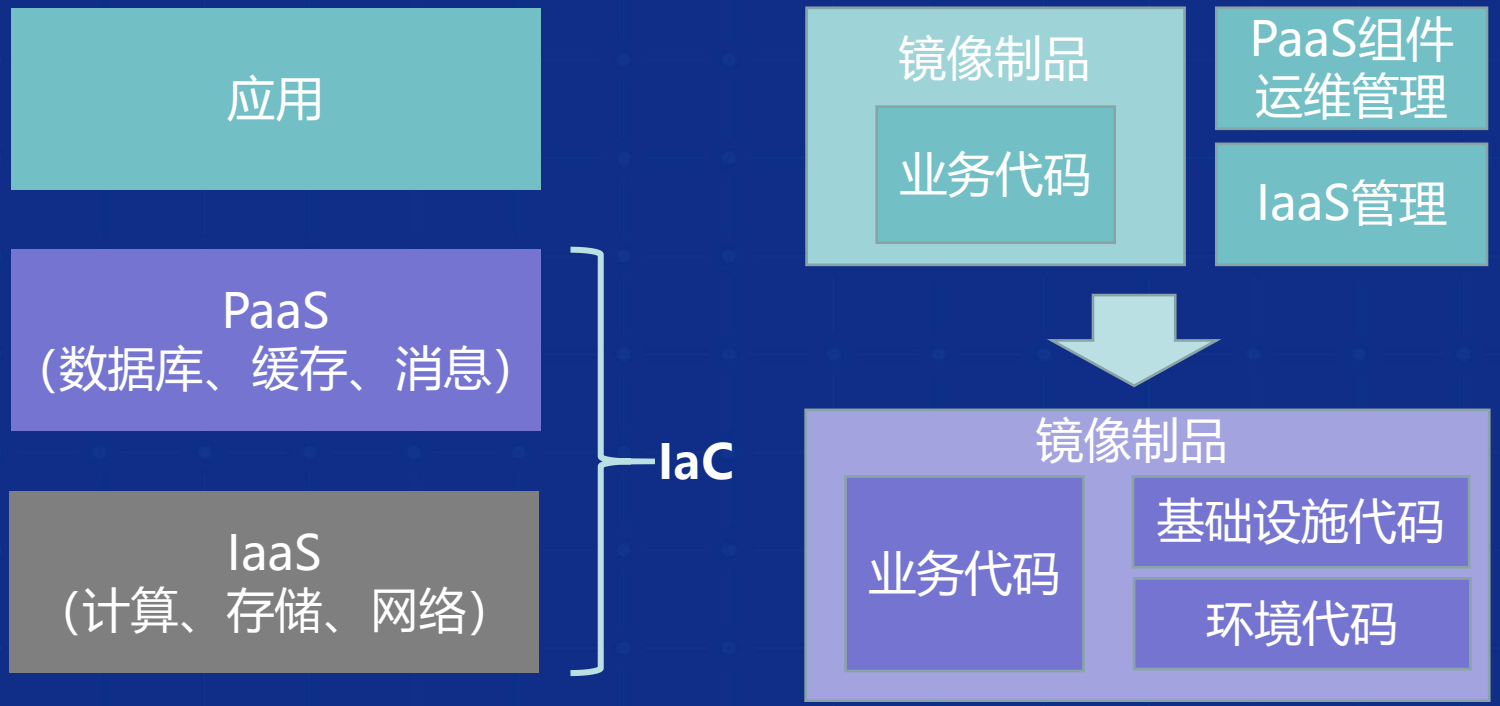
1 企业数字化转型面临的挑战

2 联通IT基础设施演进历程与成果

3 未来探索与展望

后续探索方向-基础设施即代码

- 业务的交付，除了业务代码之外，还需要PaaS资源（如缓存、数据库、消息）和IaaS资源（计算、存储、网络，以及容器）；在实施持续交付的过程中，必须考虑将PaaS与IaaS的使用、管理、配置与维护纳入进来，作为支持产品运行的一部分。
- 基础设施即代码，就是用代码化的方式，定义及管理PaaS资源和IaaS资源，进而提升可重用性、一致性、可见性。
- K8s平台为IaC（基础设施即代码）实践提供了绝佳的平台。



基础设施即代码的优势：

标准化： 以代码来定义环境，实现开发环境、测试环境、生产环境的标准化。

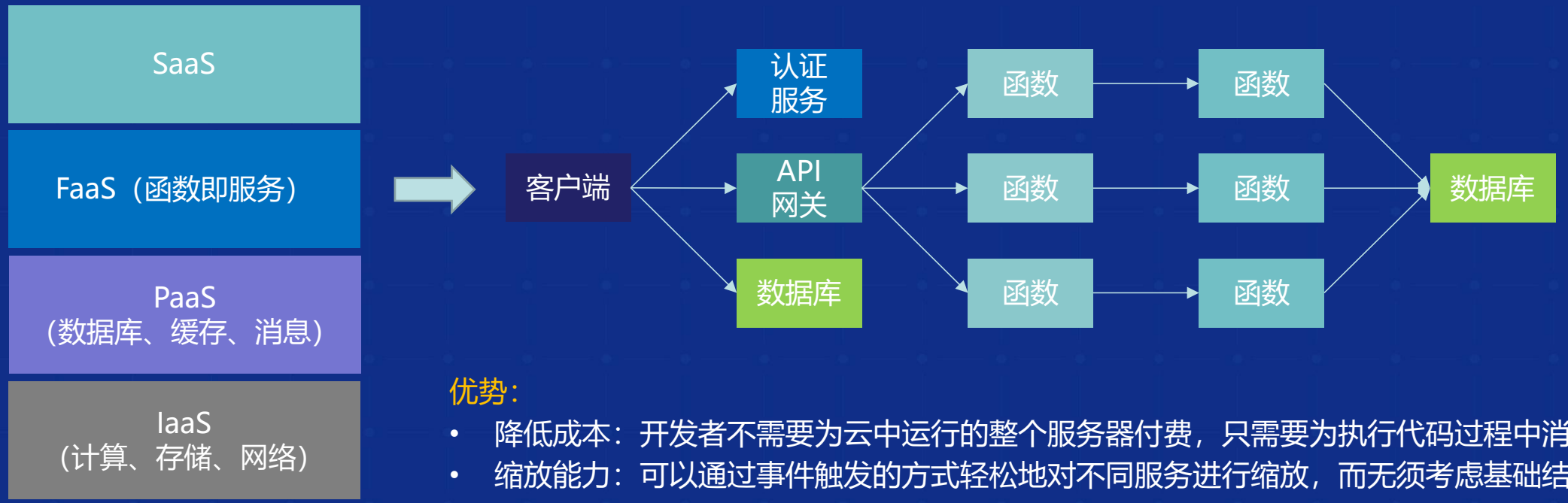
自动化： 以自动化工具来驱动代码准备环境。包括创建环境、更新环境以及销毁环境。

可视化： 以监控来可视化环境信息。环境当前状态可视、环境变更历史可视、可追溯。

基础设施即代码实践会产生高成熟度的持续交付和DevOps。

后续探索方向-Serverless与FaaS

- Serveless的初衷是帮助开发者摆脱运行后端应用程序所需的服务器设备的设置和管理工作。
- 通过 Serverless容器，一方面可以根本性解决 K8s 自身的复杂性，让用户无需受困于 K8s 集群容量规划、安全维护、故障诊断等运维工作；一方面进一步释放了云计算的能力，将安全、可用性、可伸缩性等需求下沉到基础设施实现，可以帮助云厂商形成差异化竞争力。
- FaaS将Serverless框架提高到一个全新的层面，为云中运行的应用程序提供了一种全新的系统体系结构，不需要在服务器上持续运行进程以等待 HTTP 请求或 API 调用，而是可以通过某种事件机制触发代码的执行。



优势：

- 降低成本：开发者不需要为云中运行的整个服务器付费，只需要为执行代码过程中消耗的资源付费
- 缩放能力：可以通过事件触发的方式轻松地对不同服务进行缩放，而无须考虑基础结构的运维和维护

后续探索方向-安全容器

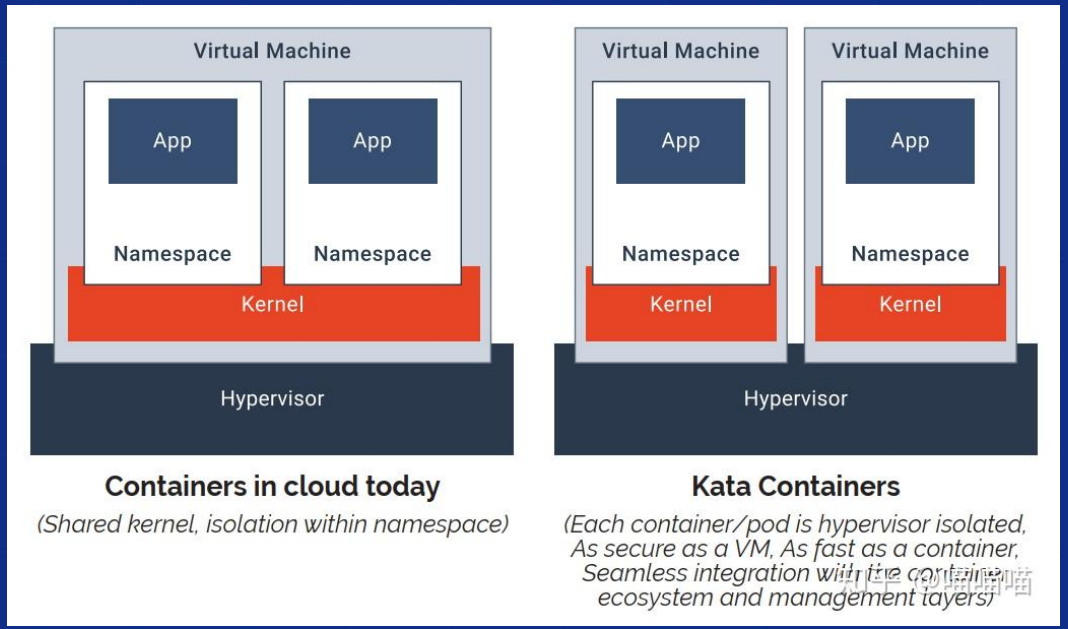
- 现状：企业采用容器技术依然面临安全挑战

  基于容器技术实现资源共享在带来业务弹性和资源高利用率的同时，也会增加业务的安全风险几率。风险在于同一主机上的多个容器需共享同一个主机内核，而同一宿主机上可能运行不同租户的容器，这就可能会威胁到整个云基础架构和租户业务及数据的安全。

- 现在，所谓“安全容器”是指一种容器运行时技术，为容器应用提供一个完整的操作系统执行环境，但将应用的执行与宿主机操作系统隔离开，避免应用直接访问主机资源，从而可以在容器主机之间或容器之间提供额外的保护。

Kata Containers是一个使用虚拟化来提供隔离层的开源安全容器项目，完全兼容 Kubernetes等云原生生态系统。

安全性/虚机特性：基于独立内核构建安全的容器引擎，容器运行在自己的内核之上，不和其他容器共享。
容器特性： 支持OCI以及CRI接口，可以无缝对接容器编排方案，比如 Kubernetes 等；启动速度达到百毫秒级，内存开销小，类似容器。



云原生 产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

THANKS !

CAICT 中国信通院