HUAWEI | CAICT 中国信通院

云原生 2.0 白皮书

2021 年 4 月

CONTENTS

目录

第一章
云原生发展历程

云原生是近几年云计算领域炙手可热的话题，云原生技术已成为驱动业务增长的重要引擎。同时，作为新型基础设施的重要支撑技术，云原生也逐渐在人工智能、大数据、边缘计算、5G 等新兴领域崭露头角。伴随各行业上云的逐步深化，云原生化转型进程将进一步加速。

1.1 云原生创新回顾

1.1.1 开源技术创新

云原生的技术理念始于 Netflix 等厂商从 2009 年起在公有云上的开发和部署实践。2015 年云原生基金会 CNCF 成立，标志着云原生从技术理念转化为开源实现，并给出了目前被广泛接受的定义：

云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。云原生的代表技术包括**容器、服务网格、微服务、不可变基础设施和声明式 API**。

CNCF 致力于通过培养和维持一个开源、供应商中立的项目生态系统来推动云原生技术的广泛采用，进而实现让云原生无处不在的愿景。CNCF 对云原生的定义让云原生的概念进一步具体化，从而让云原生更容易被各行业理解，为云原生在全行业广泛应用奠定了基础。过去几年中，云原生关键技术正在被广泛采纳，CNCF 调查报告显示，超过 8 成的用户已经或计划使用微服务架构进行业务开发部署等，这使得用户对云原生技术的认知和使用进入新的阶段，技术生态也在快速的更迭。

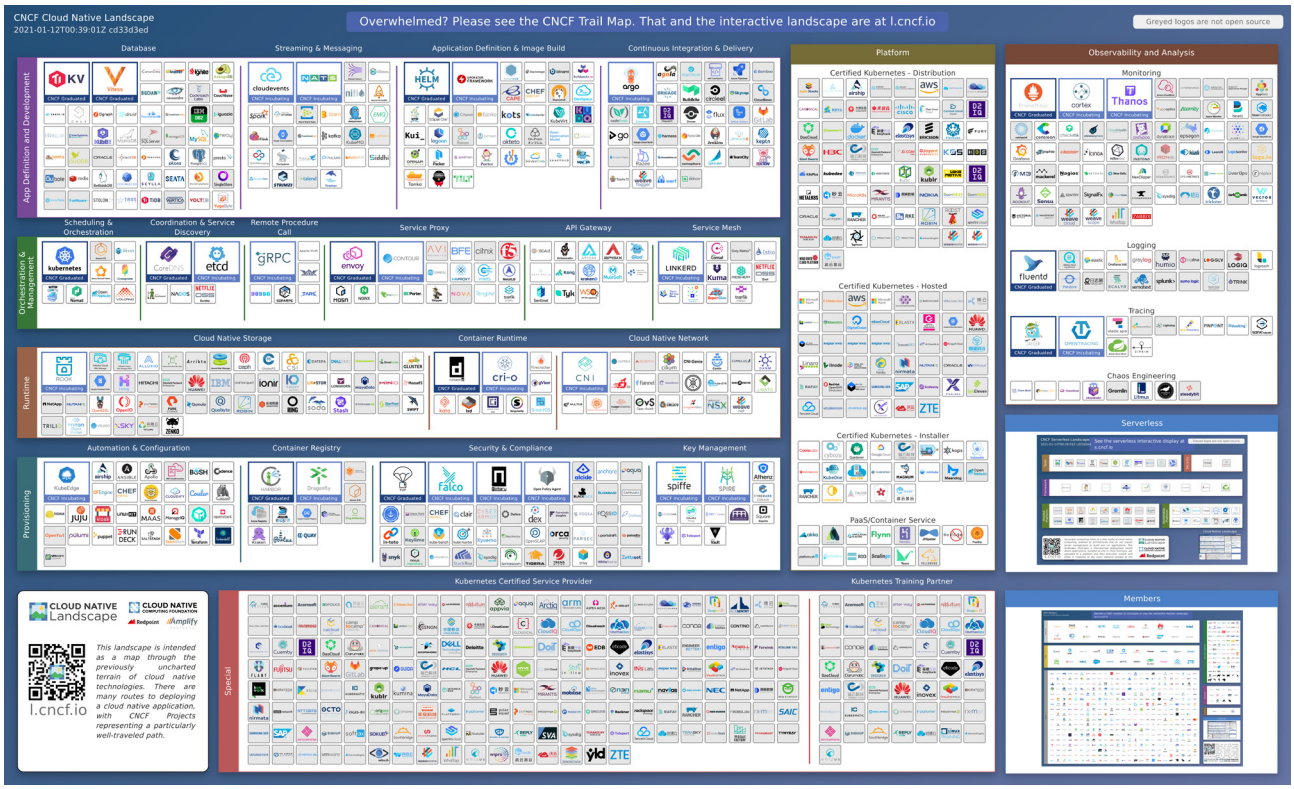


图 1 CNCF 云原生技术图谱（来源：https://landscape.cncf.io）

CNCF 成立 5 年多来，开源为云原生技术带来了前所未有的发展浪潮，极大的加速了云原生在全球范围内快速应用和发展。云原生技术生态也日趋完善，细分项目不断涌现。相较于早年的云原生技术生态主要集中在容器、微服务、DevOps 等技术领域，现如今的技术生态已扩展至底层技术、编排及管理技术、安全技术、监测分析技术、大数据技术、

人工智能技术、数据库技术以及场景化应用等众多分支，初步形成了支撑应用云原生化构建的全生命周期技术链。同时细分领域的技术也趋于多元化发展，CNCF 的云原生开源版图，由开始单一的容器编排项目 Kubernetes，发展到如今 5 大类 100 多个项目的，Kubernetes 已经成为云原生的操作系统，在其上发展出面向各行业、不同功能、不同应用场景的开源项目，Spark、Flink、Kafka、Redis 等开源项目也陆续加入 CNCF 的云原生技术图谱，进一步完善了云原生技术生态。

云原生开源项目从基础的容器引擎出发，不断扩展应用领域，对边缘、异构等各类场景的适配能力不断深入。从早期开源的容器引擎项目 Docker，到实现容器高效编排的 Kubernetes、Swarm、Mesos，再到为了更好的解决微服务治理的难题，基于 Service Mesh 技术推出的 Istio，以及针对边缘场景推出的 KubeEdge、K3s、OpenYurt，面向高性能异构计算场景的 Volcano 等项目，无一不成为加速云原生与行业融合、推动各行业创新的助推器。

1.1.2 商业解决方案创新

开源项目的不断更新和逐步成熟，也促使各企业在 AI、大数据、边缘、高性能计算等新兴业务场景不断采用云原生技术来构建创新解决方案。

早在 2017 年，就有大量企业尝试使用容器替换现有人工智能、大数据的基础平台，通过容器更小粒度的资源划分、更快的扩容速度、更灵活的任务调度，以及天然的计算与存储分离架构等特点，助力人工智能、大数据在业务性能大幅提升的同时，更好的控制成本。各云厂商也相继推出了对应的容器化服务，比如华为云的 AI 容器、大数据容器，AWS 的深度学习容器等。

云原生技术与边缘计算相结合，可以比较好的解决传统方案中轻量化、异构设备管理、海量应用运维管理的难题，如目前国内最大的边缘计算落地项目——国家路网中心的全国高速公路取消省界收费站项目，就使用了基于云原生技术的边缘计算解决方案，解决了 10 万 + 异构设备管理、30 多万边缘应用管理的难题。主流的云计算厂商也相继推出了云原生边缘计算解决方案，如华为云智能边缘平台 IEF、AWS 的 GreenGrass、阿里云的 ACK@Edge 等等。

云原生在高性能计算（HPC）领域的应用呈现出快速上升的势头。云原生在科研及学术机构、生物、制药等行业率先得到应用，例如欧洲核子研究中心（CERN）、中国科学院上海生命科学研究院、中国农业大学、华大基因、未来组等单位都已经将传统的高性能计算业务升级为云原生架构。为了更好的支撑高性能计算场景，各云计算厂商也纷纷推出面向高性能计算专场的云原生解决方案，比如华为云推出的云原生高性能计算解决方案、AWS 推出了可运行在容器平台的 Batch 服务。

云原生与商业场景的深度融合，不仅为各行业注入了发展与创新的新动能，也促使云原生技术更快发展、生态更加成熟。

1.2 企业 IT 建设的三阶段两转变，进入云原生阶段

简单来看，企业 IT 建设所依赖的基础资源经历了从服务器到云化资源的发展历程，正在快速进入云原生阶段。

服务器阶段 ：其特点是以硬件设备为中心，业务应用随不同厂商设备、操作系统、虚拟化软件的差异化进行定制；设备的安装、调试，应用的部署、运维基本靠人力完成，自动化程度低，缺乏统一的设备和应用管理能力。后期随着虚拟化软件的出现，资源的利用率、扩缩容器的灵活性方面得到一定的提升，但并未从根本上解决基础设施与软件割裂、运维复杂的难题。

云化阶段：传统模式下分布离散的设备，被统一起来，实现了各类资源如计算、存储、网络的池化，通过统一的虚拟化软件平台，为上层业务软件提供统一的资源管理接口，实现资源管理能力的自动化，屏蔽一部分基础设施的差异，使得应用的通用性增强，但因为虚拟化软件平台差异化较大，尤其是各厂商的一些商业化增强，无法在厂商间进行能力共享，应用还是无法以完全标准化的模式构建，应用部署还是以资源为中心。

云原生阶段：在这一阶段，企业的关注点从以资源为中心转移到以应用为中心，包括应用敏捷交付、快速弹性、平滑迁移、无损容灾等。因此，企业开始考虑如何将基础设施与业务平台融合，为业务应用提供标准的运行、监控、治理平台，并将业务的通用能力下沉到平台侧，更好的帮助企业实现应用的自动化。

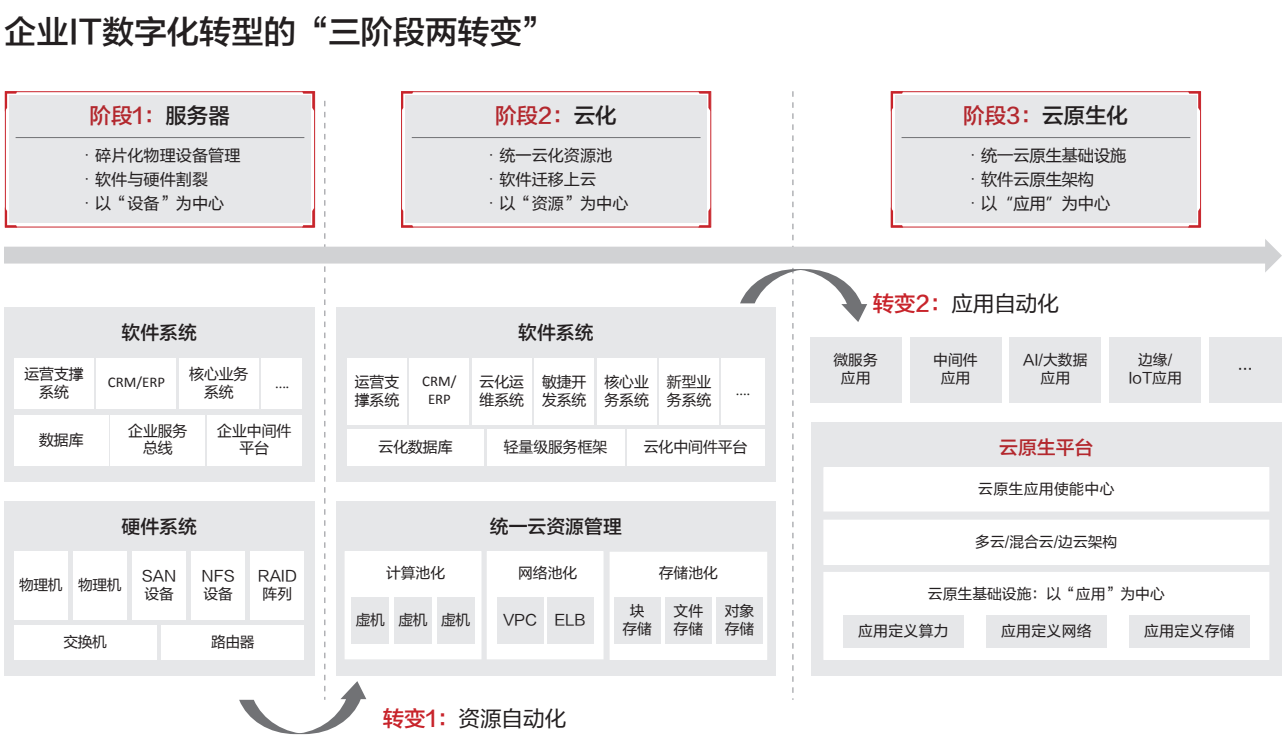


图 2 企业 IT 建设的三阶段两转变

1.3 以应用为中心，开启云原生 2.0 时代

企业数字化转型初期，主要是将业务从线下搬迁上云，在这一阶段企业主要是的把业务简单部署和运行在云上，可以称之为 ON CLOUD。这种形态下，通过资源池云化，解决了 IDC 时代运维、部署、扩容的难题，但传统应用单体架构厚重、烟囱式架构等带来的一系列应用层面的问题并没有得到有效解决，云对业务的价值主要还停留在资源供给的阶段，无法充分发挥出云的价值。

随着企业数字化转型的深入，企业需要充分享受云计算带来的红利，需要让业务能力生于云、长于云，由现在的 ON CLOUD 进阶到 IN CLOUD，同时基于云构建的新生能力与既有能力有机协同、立而不破。生于云是指基于云原生的技术、架构和服务来构建企业应用，长于云是指充分利用云的优势来助力企业应用和业务发展，将企业的数字化建设、业务智能升级带入新阶段，我们称之为云原生 2.0 时代。

从为企业带来的价值来看，云原生 2.0 有着如下优势：

资源高效	通过对多元算力的支持，满足不同应用场景的个性化算力需求，并基于软硬协同架构，为应用提供极致性能的云原生算力；基于多云治理和边云协同，打造高效、高可靠的分布式泛在计算平台，并构建包括容器、裸机、虚机、函数等多种形态的统一计算资源；以“应用”为中心打造高效的资源调度和管理平台，为企业提供一键式部署、可感知应用的智能化调度，以及全方位监控与运维能力。
应用敏捷	通过最新的 DevSecOps 应用开发模式，实现了应用的敏捷开发，提升业务应用的迭代速度，高效响应用户需求，并保证全流程安全。对于服务的集成提供侵入和非侵入两种模式辅助企业应用架构升级，同时实现新老应用的有机协同，立而不破。
业务智能	帮助企业管理好数据，快速构建数据运营能力，实现数据的资产化沉淀和价值挖掘，并借助一系列 AI 技术，再次赋能给企业应用，结合数据和 AI 的能力帮助企业实现业务的智能升级。
安全可信	结合云平台全方位企业级安全服务和安全合规能力，保障企业应用在云上安全构建，业务安全运行。

云原生 2.0 的参考架构如下：

图 3 云原生 2.0 参考架构

第二章
云原生基础设施

经过十几年的发展，云计算作为数字化转型的重要基础设施，已经由“面向云迁移应用”的阶段演进到“面向云构建应用”的阶段，即由“以资源为中心”演进到“以应用为中心”的云原生基础设施阶段。云原生基础设施为用户带来了多方面的革新，利用智能的调度、运维系统高效管理更为丰富的应用，天然混合云的架构可将业务快速分发部署到到分布式云的场景中，同时软硬协同的基础设施架构在为应用提供更好的性能的同时，也对隔离性、安全性等多方面能力进行了加强。

2.1 多元算力、软硬协同，为应用打造高效的资源平台

容器服务早期的部署形态多基于虚拟机，以虚拟机节点作为容器集群的计算节点，并基于此构建容器的网络、存储和编排能力。这样的堆叠架构虽然可以让整个软件栈分工明确、边界清晰，但是带来了较大的性能损耗和功能冗余，并且难以满足客户对实例安全隔离的较高要求。在云原生 2.0 时代，基于裸金属搭建容器服务成为一些对性能和实例隔离性较高用户的选择。同时，为了进一步提高容器负载性能和稳定性，原来部署在裸金属之上的非业务负载组件也逐步的由专门的卸载硬件来承载，例如容器存储、容器网络、容器引擎以及服务网格组件。将容器组件下沉到卸载卡后，有两方面好处：

» 资源高效：裸金属节点上的计算资源可以 100% 被业务负载使用，避免了对业务负载的性能干扰。

» 性能提升：容器网络、容器存储组件下沉到卸载卡后可以与传统 IaaS 层的网络、存储组件垂直打通，减少冗余；直接以硬件设备直通方式将存储、网络资源分配给容器实例，缩短 I/O 路径，提高性能。

随着人工智能、5G、HPC、边缘计算等新业务的逐渐落地和普及，对算力多样化提出了更高的要求。针对特定的业务场景采用专有的硬件可以提供更好的计算效能，越来越多的异构计算硬件如 GPU、FPGA、ASIC、SoC 等被应用到专有的领域。云原生 2.0 时代，基础设施的特征之一就是向下统一管理和支持各种异构硬件，向上屏蔽底层多种硬件的差异性。真正做到以应用为中心，应用无需关心底层的硬件设备，无需针对特定硬件做任何特殊处理。

大规模的网络资源供应、泛在的网络安全隔离、极致的网络弹性和细粒度的网络 QoS 是承载大规模云原生业务的基础网络要求。资源供应方面，单 VPC 内多集群的容器端点数可以达到甚至超过百万，灾备场景的集群迁移要求容器级的网络配置、隔离，例如 QoS，带宽限速大批量容器快速发放（10 万 / 分钟）；网络弹性方面 ，Serverless/Function 等轻量级云原生运行时的要求毫秒级创建，秒级冷启动（包含网络端到端打通）；安全隔离方面，无边界、零信任、海量端点和高动态性的云原生网络安全，要求即时生效的容器粒度安全隔离与 ACL；资源力度方面，在 / 离线业务混部场景下，为了能够发挥出云原生极致资源利用率和性价比，要求容器网口粒度的 QoS（包括带宽保障和优先级支持）。不断变化的云原生业务诉求正推动着云网络架构的不断演进。

传统高性能计算 (HPC) 领域广泛采用 InfiniBand 技术获得高吞吐和低时延的无损网络通讯能力，但这一技术体系专用网络硬件成本高昂、组网规模不可扩展、技术演进缓慢，无法满足云原生时代的平民化可支付、高弹性大规模使用要求。领先的云厂商开始基于智能网卡的可编程和卸载能力，对无损网络通讯协议进行了重新设计，在主机侧智能网卡中采用创新的拥塞控制算法，在大大降低丢包发生概率的同时，保持转发队列的低水位，从而兼顾大带宽和低时延要求，并且也去除了对 PFC 的依赖，利用普通的以太网交换设备就可以实现大规模组网，解决了横向扩展的问题。以 AWS SRD 和华为云 CurreNET 为代表的高性能协议栈技术在高性能计算（100G）和低时延云存储（10 微秒级时延）技术领域取得突破。未来高性能网络通讯协议在云原生领域的应用将不再局限于传统的高性能计算和存储领域，会在扩展至更广泛的云原生技术和行业应用中，如：ServiceMesh、 云原生的中间件（内存数据库，消息中间件等）等技术，云视频、云原生的金融交易等行业。

云原生存储是指面向云原生应用的存储解决方案，云原生应用与传统应用对存储诉求的具有本质的不同。较传统应用而言，云原生应用具备如下特点：

» **提供声明式的资源的申请接口：**当前 CSI 已经成了云原生应用使用存储资源的统一标准，不管是传统 IaaS 云存储，还是新型容器化部署（CAS）的存储架构，都采用该接口来为云原生负载提供存储资源。但是对于不同的云提供商或者存储提供商，他们提供的 CSI 配置参数仍存在差异性，不能做到一次配置到处运行。为了解决该问题，可以采用 CAS 架构存储，让存储随着负载一起部署在容器集群中，基础设施层只提供基础块设备的供应，类似于 Portworx、OpenEBS，或者管控面增加一个存储接入中间层，中间层北向提供统一的 CSI 配置，南向适配不同存储，类似于华为的 SODA、NeTApp 的 Trident。

» **控制面和数据面性能同等重要：**传统应用大都采用单体架构，对存储资源的诉求也大都是由管理员先通过界面操作分配好资源，然后挂到运行的节点上使用，该场景下负载对存储数据面性能要求较高，忽略了管控面的性能。但是在云原生场景，可能很多微服务组件并发调用存储卷的管理面功能，比如创建、删除、快照等，这就需要云原生存储系统在设计时就要考虑管控面的性能。

» **以应用为中心：**云原生场景下所有的服务层都是围绕应用诉求来构建，包括存储资源的供应、生命周期管理，监控、灾备等。传统应用场景下，存储的管理还都是以资源为中心，比如存储的备份恢复、实时灾备，客户要明确指定需要处理的数据盘，而缺少应用负载的联动。云原生场景下，应用的备份恢复和容灾就需要从负载本身触发，将应用本身配置、运行状态、使用的存储卷等都一起备份恢复，从而达到应用负载与所依赖资源状态的整体一致性。此外，数据面也要做到以应用为中心，云原生应用关注的只是数据源的存放，而不关心数据源如何被应用来使用。存储供应层需要根据负载要求的性能指标来自动选择合适的数据面对接方案。比如负载使用的数据可能在性价比较高的对象存储中，但是又要求负载访问时具有较高的性能，存储提供层就需要借助缓存加速能力，自动为存储卷启动缓存加速实例来提高访问性能，而这一切对于负载而言都是不可见的，负载只需要在资源诉求中配置高性能即可。

» **策略驱动的自动化管理：**随着云原生实例规模的增加，存储卷的管理将会非常复杂，需要提供基于策略的自动化管理手段。客户可以配置存储卷的管理策略，存储层按照策略来自动化管理存储卷。比如用户可以定义好卷的生命周期动作，然后存储层按照配置自动化为负载提供卷，周期性清理残旧卷，周期性对卷进行健康检查、备份恢复等。

操作系统是承载云原生应用运行实例的底座，云原生下操作系统与普通操作系统的本质区别是其从管理硬件、资源等职能转变为以应用为中心，提供应用特征最优组合的底层运行环境。

依据云原生应用的基本特征，云原生下操作系统应具备如下能力：

» 轻量化组件构成：云原生下应用采用容器化标准部署模式，应用依赖自包含，对操作系统依赖降低。传统操作系统为满足多类型应用，组件功能复杂完备，在云原生场景下则较为冗余。冗余组件压缩应用可利用资源，降低了应用部署密度，同时暴露更多攻击面，降低系统稳定性。因此在云原生场景下，操作系统应仅包含最小依赖组件，如系统 1 号管理组件、网络管理组件、设备管理组件、日志组件与基础依赖软包等。

» 标准化功能组合管理：软件包是组成传统操作系统的最小单元，如 CentOS/openSuse 使用的 RPM 软件包管理体系或 Debian/Ubuntu 使用的 deb 软件包管理体系，云原生应用使用 Operator/Helm 等标准应用模式，传统软件包管理模式较难融入标准生态。云原生下提出统一运维管理界面的要求，操作系统内基础软件包应以符合标准化应用模

式提供原子功能级的管理，如使用 Operator/Helm 部署基础能力，或将整体根文件系统打包组合成容器镜像原子化管理，或将原有软件包管理模式封装可接入生态格式，最终通过 kubernetes 统一 API 入口进行生命周期管控。

» 应用定义操作系统：以应用为中心要求整体软件栈围绕应用诉求构建，传统操作系统一般以通用使用场景，无法针对特定应用提供最优软件栈组合与调优策略，如针对在线 / 离线业务混合部署场景，需进行服务级别资源精细化 QoS 控制与快速抢占协同调度；针对大数据应用场景，可使用冷热页面分级，提升热数据性能访问性能等。针对不同应用场景的特征进行操作系统最优策略制定，基于标准化功能组合管理，抑制基础设施版本管理膨胀，提供应用性能 / 体验最优的操作系统。

» 智能运维与调优：随着节点规模与部署密度的增加，云原生应用的运维与调优变得愈加困难，引入 AI 来进行大规模应用的运维和调优成为了必要手段。整体智能系统应包括应用行为观测、应用指标度量与智能决策三个部分。其中云原生下操作系统应提供低负载且应用无感的观测手段，提供结构化、标准化的观测数据，为后续决策提供必要的数据基础。同时结合应用指标度量手段，提供应用相关性分析，提供应用性能 / 体验调优策略建议，针对故障应用，智能诊断应用故障，进而实现整体故障级预测。同时，因调优 / 故障导致操作系统自身组件的变化应保持应用影响最小化，如提供 OTA 级操作系统基础组件升级能力或操作系统内核热替换能力。

如今各个云服务厂商大力推广的 Serverless 计算，能在很大程度上提高用户的灵活性和创新能力，使用户可以在不考虑服务器的情况下构建并运行应用程序和服务，消除管理基础设施的压力。但当前的 Serverless 架构仍被限定在某个 Region 内，大部分的云服务厂商仍依据成本，用户量等因素在不同的地域（Region）建设资源，用户再根据业务、成本、性能等因素选择相应 Region 的资源提交作业。随着用户业务量的增长，多 Region 投递任务的管理能力也成为一个重要的考量因素，尤其考虑到不同 Region 的建设、运维、商业成本差异。全域调度（Regionless）是面向跨 Region 场景的下一代无服务计算（Serverless 2.0）。根据业务请求、资源成本等因素在多个 Region 中选择最合适的资源池来处理客户的计算任务，并且支持多种任务投递策略，满足客户各种业务场景下的诉求，比如成本优先、速度优先、指定时间执行等等。全域调度不仅能够通过全局资源的调配来达到降本增效的目的，还能将用户从多 Region 的管理与运维中解放出来，让客户聚焦到业务本身，提供真正的 Serverless 体验。

2.2 泛在计算、统一计算，让各类应用更有机的协同

随着企业生产环境容器集群规模爆发式增长，越来越多的企业核心业务切换到容器，容器技术需要应对的场景也越来越复杂，单数据中心的强硬基础设施性能、单厂商跨 Region 的 Serverless 资源无感知调度，虽然可以满足企业大规模业务部署的诉求，但在某些场景下，如容灾、跨云迁移等，单独的云厂商已经无法满足用户需求。因此跨云服务商的业务部署能力成为客户重点关注对象，以满足业务连续性、降本增效等场景诉求，如：

» 解除厂商锁定，应用可以灵活地部署在不同云供应商或本地 IDC 的集群中，不再依赖某一家云服务厂商；

» 跨云业务容灾，在云服务商发生故障时可以快速切换到其他的云服务商或者混合云环境中去，实现业务的容灾管理；

» 跨云弹性伸缩，利用公有云超大资源池应对短期流量高峰场景，大幅提高业务的承载能力；

» 公私云分离部署，部分核心业务部署在私有云环境，满足行业监管和数据安全要求，普通业务部署在公有云上，利用公有云强大的计算能力，同时节约成本。

当前所有主流云厂商均支持基于 Kubernetes 的容器服务，Kubernetes 已然成为容器调度管理的事实标准，这也为多云统一管理提供了技术条件。云原生 2.0 多云架构应该具备以下特征：

» 天然多云：基于 kubernetes 容器技术的统一标准，应用可以跨云在多个 Kubernetes 集群间自由迁移而不必担心对环境的依赖（云厂商的 Kubernetes 服务需兼容社区标准 API）。

» 多云治理：结合服务网格实现多云多集群全局统一服务治理，单网格控制面支持管理 10W+ 服务实例，支持灰度发布、流量治理、流量监控等完善的服务治理能力。

» 统一运维：基于容器技术的轻量级技术方案，支持 100W+ 海量容器集群统一管理（含边缘集群），支持跨云业务的统一构建和维护，无需关注大量基础设施的问题。

» 跨云弹性：基于容器技术的秒级弹性机制，扩缩容及时性 <5s，1 分钟扩容 1000+ 容器实例，可实现业务按需极速跨云弹性伸缩，不需要为多云和混合云解决方案维护额外的本地资源，降低企业 IT 基础设施投资成本 50% 以上。

除了跨公有云或公有云与私有云之间这种多云管理场景外，随着边缘技术的日趋成熟和广泛使用，应用大量被部署在边缘侧设备上，以减少数据传输时延带来的业务损耗。权威机构预测，未来 5 年，企业的数据存储和业务计算会更多的在边缘发生，边缘计算的各种创新也会逐渐增多。其中推动边缘计算快速发展主要有四大因素：

» 低时延：为满足低时延要求，需要在离业务现场最近的“边缘”构建解决方案，减少业务处理时延；满足工业互联网、智慧城市等现场边缘场景小于 5ms 时延，互动直播、游戏 /VR 场景下部大于 20ms 的要求。

» 海量数据：物联网时代边缘数据爆炸性增长，按照 Gartner 的统计，2020 年全世界有多达 250 亿的智能设备连接互联网并产生 50 万亿 GB 的数据。如此多的数据难以全部直接回传至云端且成本高昂，数据需要在本地进行分析和过滤，节省网络带宽；

» 隐私安全：数据涉及企业生产和经营活动安全，在边缘处理企业保密信息、个人隐私；

» 本地自治：本地网络在于云端断连的情况下，依然不能影响边缘侧的业务，边缘侧需要不依赖云端的离线处理能力、自我恢复能力。平台要提供业务自愈的能力，当边缘业务出现故障的时候，可以在 3s 内对故障做出自动修复，保证业务连续性。

边缘的运行环境对应用和管理平台提出了新的挑战，如应用的简单化轻量化、严格的施工环境承载要求、边缘网络低速度和低稳定性甚以及环境恶劣地域的大范围部署等，为应对以上这些挑战，边缘计算平台应具备以下特点：

» 统一管理：基于 Kubernetes 等云原生技术，实现异构设备接入、镜像管理、应用分发、应用升级、应用运维等，边缘业务完整生命周期管理，业务效率提升 10 倍；

» 极致轻量：支持轻量化容器和函数管理，最小可支持百兆内存的边缘设备；

» 高可靠性：支持离线场景和节点故障场景下，边缘应用秒级恢复业务，保障高可用；

» 边云 / 边边协同：支持边缘应用间轻量级服务发现与负载均衡；支持边缘应用与云端应用的服务发现；

» 大规模管理：可支持百万节点，千万级应用，镜像极速分发分钟级分发至万级节点；

除了解决应用跨云域分布式部署和管理的问题之外，以容器为核心构建裸金属服务器、虚拟机、容器、函数等多形态资源共池的统一计算平台，使得企业在云原生转型过程中，传统的应用能与新的云原生应用共平台统一部署，更好的实现新老业务的协同。

2.3 智能调度、敏捷运维，让资源的利用更智能、高效

随着云计算的发展，越来越多的应用面向云构建，从早期业务类应用以及与之配套的各类中间件应用上云，再到AI、大数据、HPC 等计算类应用全面上云，云计算进入了以“应用为中心”的云原生 2.0 阶段，所有应用能力将“生于云、长于云”。

有状态应用、中间件等都有定制的生命周期管理需求，很难用一种或几种工具有效的管理其生命周期，例如Kuberentes 默认的部署元素很难管理像 MySQL、Kafka 这样的有状态应用和中间件。因此，定制化生命周期管理成为主要解决方案。在以应用为中心的云原生 2.0 阶段，Kubernetes + Operator 以其良好的可扩展性及较高社区活跃度，已经成为各个企业的主流选择，将极大降低云原生应用全生命周期管理的难度，加快企业业务的云原生化升级。同时，定制化在解决生命期管理的同时，也引入了社区项目分散，构建不规范等问题，因此需要提供以下几方面的能力，才能有效的管理有状态应用、中间件等：

» 部署标准：基于 Operator 以及 Helm 的开源标准，支持通过增加配置文件声明使能弹性伸缩、配置更新、数据迁移等云原生能力。

» 开发规范：自动生成服务包和配置文件，开发者聚焦业务开发和配置使能。

» 服务中心：提供服务生态、种类丰富，同时接入服务提供商提供的服务社区版以及企业版供企业自主选购，一键服务实例分发，秒级部署，开箱即用。

» 服务生命周期管理：结合多集群管理和边缘云管理，提供跨公有云、混合云、边缘的全场景服务生命周期管理。

随着企业云原生应用数量的快速增加，对应用服务的流量治理、运行监控、访问安全以及发布等能力诉求也相应提升。在云原生 1.0 阶段所流行的以 SDK 方式进行微服务治理框架的模式，在云原生 2.0 的阶段，逐步被非侵入式的微服务治理解决方案取代。Istio 作为现在主流的非侵入式微服务治理框架，为用户提供了包括负载均衡、熔断、限流等多种治理能力。但原生的 Istio 无法满足用户在生产环境中的需求，还需提供以下几种能力，以提高用户的对应用的治理能力：

服务灰度发布

允许用户按照标准制定一套流量分发规则，并且无侵入的下发到实例中，平滑稳定的实现灰度发布功能。为应用治理提供的灰度发布功能，稳定高效地推动企业应用的迭代升级。

服务网格化

随着微服务的大量应用，其构成的分布式应用架构在运维、调试、和安全管理等维度变得更加复杂，开发者需要面临更大的挑战，如：服务发现、负载均衡、故障恢复、指标收集和监控，以及灰度发布、蓝绿发布、限流、访问控制、端到端认证等。服务网格通过无侵入的方式，面向容器云原生应用，提供容器化和治理的完整解决方案。

服务流量治理

根据微服务的流量协议，提供策略化、场景化的网络连接、安全策略管理能力。支持基于应用拓扑对服务配置负载均衡、熔断容错等治理规则，并提供实时的、可视化的服务流量管理。应用无需任何改造，即可进行动态的智能路由和弹性流量管理。

进入云原生 2.0 阶段后，不仅仅有更多的在线业务进行云原生升级，离线类计算业务也开始了云原生升级，包括 AI，大数据和 HPC 等。在升级过程中，各个领域的应用架构逐渐向云原生转型，例如 Spark, Cromwell 等，并通过云原生基础设施构建统一的计算平台以提高运维效率和资源使用率。为了有效的支持离线作业，云原生基础设施在云原生 2.0 时代的技术特征是：

- 面向高性能负载的调度策略，如公平调度，组调度等，提供达到 70% 以上的资源使用率；
- 支持多种作业生命周期管理，如 multiple pod template, error handling；
- 支持多种异构硬件，如 GPU，NPU，FPGA；
- 面向高性能负载的性能优化，例如支持 2 万节点的大规模集群，提供 10k/s 的容器启动速度。

第三章
云原生应用敏捷

Gartner 也提出，到 2023 年，新应用新服务的数量将达到 5 亿，也即是说：“每个企业都正在成为软件企业”。据 IDC 预测，到 2025 年三分之二的企业将成为多产的“软件企业”，每天都会发布软件版本。越来越多的企业将使用软件来交付服务，企业需要敏捷的业务能力来应对快速变化的市场，同时需要领先的创新能力来形成差异化的市场竞争力。

面对这样的趋势，传统应用陈旧的架构和开发模式将拖累企业业务创新。传统应用存在一系列的问题，如架构耦合度大、应用愈发复杂、技术债务持续积累、无法按需弹性、开发模式落后、部署发布周期长、开发运维割裂等。这些问题，严重阻碍了企业应用的迭代，限制了技术演进和业务创新。

因此，企业亟需通过应用现代化建设来实现敏捷商道。应用现代化已成为业界的热点，但各厂商对应用现代化的理解不同。AWS 认为，应用现代化包括 Ownership 文化的构建、微服务化、数据管理、计算、敏捷开发、服务器运维模式、利用程序化护栏等。谷歌认为，应用现代化应实现基础架构与应用解耦、各个团队解耦、开发与运维解耦、安全与开发和运维解耦等。微软认为，在应用模式方面上云、在开发实践方面采用 DevOps、在技术选择方面选择最适合的开发语言、框架和工具，是实现应用现代化的核心。

华为基于服务数百万企业客户的经验沉淀，以及结合自身 30 年的数字化实践总结，提出“基础设施现代化、应用架构现代化、开发运维现代化、治理运营现代化”这四个现代化是企业走向应用现代化的关键，让企业走上以业务和应用为中心的敏捷道路，重塑应用的商业价值。

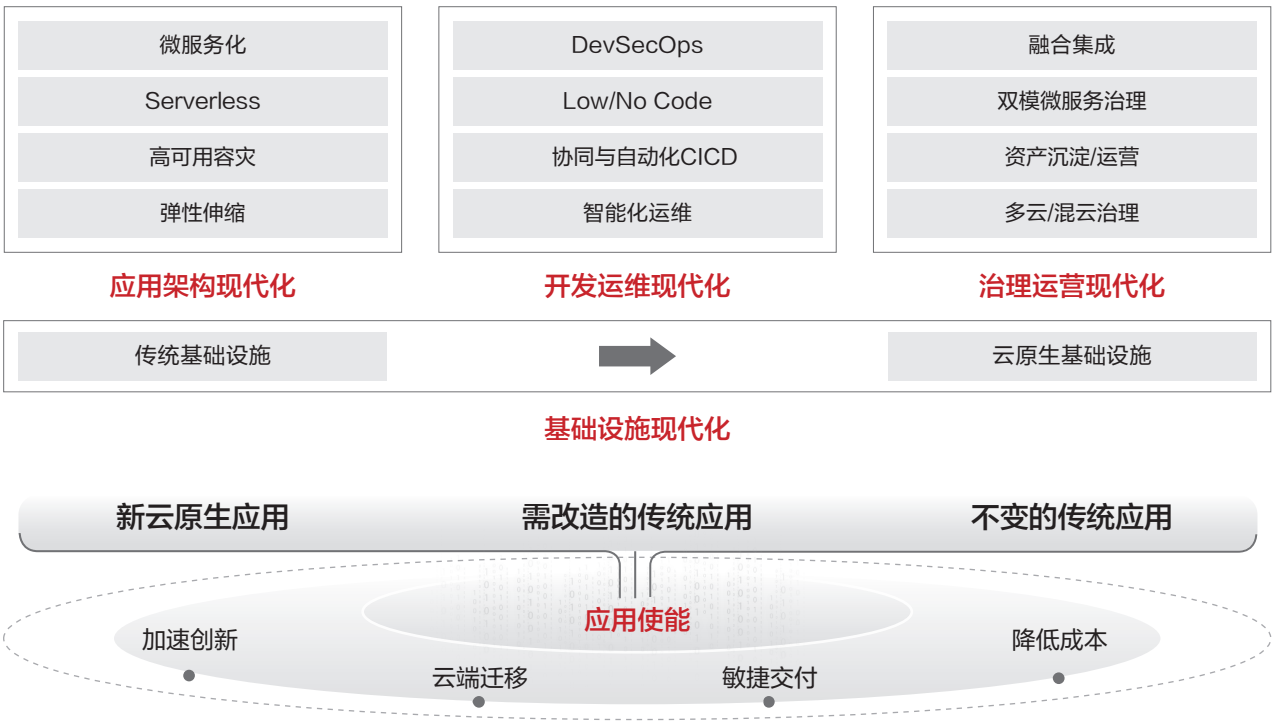


图 4 应用现代化参考架构

3.1 基础设施现代化，让企业聚焦于应用开发和业务创新

基础设施现代化的本质是通过将企业应用迁移上云，使用容器、多元算力、Serverless、分布式云等技术，对应用的底层架构进行重构，实现承载应用的基础设施资源的高弹性和高可用，最大化利用云平台的技术和优势，帮助客户实现资源的智能调度、简化运维、降低成本，将开发人员从繁琐的资源管理和运维等低值工作中释放出来，聚焦于应用开发和业务创新等能给企业带来高价值的工作。

3.2 应用架构现代化，让应用高内聚、低耦合、高可用与弹性

应用的架构现代化是指使用微服务、Serverless 等技术，将应用拆分为能独立运行，满足客户需求的独立模块，实现应用的高可用、弹性扩展。应用架构现代化是应用走向敏捷开发的基础。

» 微服务架构旨在让每个微服务块集中和独立处理一个内聚的业务逻辑，以便于独立的运行和交付。微服务基于单一职责、服务自治、轻量通信、服务化接口等原则实现应用上的“松耦合”，使得应用的开发、部署、运行和治理得以独立进行，为获得更好的可用性和更高的研发效率创造了基础。微服务的推广，对应用的开发和治理也提出了更高的要求，因此诸如 Spring Cloud、ServiceComb 等大批优秀开发框架和微服务治理服务也相继推出，进一步推动了微服务的大规模应用。

» Serverless 通过业务系统感知到负载需求时动态的调整和分配相应的底层资源，当业务处理完毕时，资源会被自动释放和回收，实现了资源利用的最大化。使得应用的开发、部署和运行再也无须调度和管理服务器资源，这无异于一种生产力的解放，让客户专注于对业务和应用开发中最有价值的工作，而无须担心底层资源细节。无论是构建新应用，还是迁移老应用，优先使用 Serverless 技术，都可以让客户在云上获得最大的敏捷性。

» 应用的高可用和高弹性架构，首先要做到系统和数据的冗余；其次，通过跨 AZ 部署以及跨地域异地容灾来实现业务的灾备；最后，通过云平台提供的能力做故障的追溯和流量的切换，来做到故障的快速响应与恢复。应用的弹性伸缩，要综合前端的负载均衡、后端的微服务弹性以及业务数据的可伸缩来综合设计。

3.3 开发运维现代化，革新研发模式，提升软件交付效率

数字化时代，应用的数量爆炸性增长，应用的迭代速度越来越快，而随着微服务架构的普及，现代的应用开发必定是多团队跨地域的并行开发，每天 10 万级以上的 CICD 流水线并行执行将成为企业常态。而当前代码的抽象程度不高，软件交付过程未标准化，应用构建部署人工执行占比居高，开发和运维的“混乱之墙”都严重制约了应用敏捷交付的效率，同时也带来客户对于应用交付质量和安全的担忧。传统的应用开发和交付模式需要转变为以 DevOps 为核心的开发运维一体化模式，来加速软件交付速度，同时抽象化、模板化、自动化、智能化、立体运维是开发运维现代化的主要特征。

在代码中抽取出与业务逻辑无关的基础性的公共代码，使用代码框架（也称为脚手架或胶水代码）和与之匹配的研发工具链来封装这部分代码，供其他服务调用。框架和工具中应内置安全、性能、部署等最佳实践，让开发人员尽可能只关注业务逻辑，花更多的时间在写业务相关的代码上，减少写公共代码所花费的时间。

现代化的云基础设施是可以被代码所声明和定义的，即“基础设施即代码”模式。在这种模式下，应用的环境、中间件、依赖服务都可以被声明所定义，软件的部署也因此可以模板化，也就为应用的大规模、批量化复制与部署提供了基础。

采用 DevOps 实现开发的自动化，可以使软件的生产交付过程变成可复制、可批量化的生产流水线。DevOps 持续集成（CI）/ 持续交付（CD）作为自动化的最重要实践，已经让众多企业从中获益。企业的流程、治理、安全（DevSecOps）等能力也需要内嵌在 CI/CD 中，让 CI/CD 自动化执行的过程中也执行了企业的流程和安全检查，进一步提升交付效率。

应用开发是个上游不断生产代码，下游不断消费代码的过程，整个应用开发过程涉及到大量的研发数据（需求，缺陷，代码，MR，分支，制品库，测试用例），随着研发作业的数据和信息不断沉淀，针对应用开发全生命周期的数据分析与智能化会大大改进应用开发的全过程，比如最新的代码检查不再只是静态的扫描，同时兼顾广度和深度的扫描成为常态，基于最佳实践和优化推荐的智能化的代码修复建议为开发人员增加效率和质量的帮助。

这是基于云的多层多维度运维方式，包括虚拟机、容器和存储等基础设施运维，中间件、数据库等平台运维，微服务、进程实例和应用性能等业务运维。同时，云平台提供了丰富的运维数据，可进一步帮助业务团队提升运维自动化、智能化能力，包括告警关联分析、链路追踪、事务监控和海量日志分析等。

3.4 治理运营现代化，立而不破，发挥应用的融合价值

据 Gartner 预测，到 2025 年 90% 的现有企业应用仍将继续使用，而随着数字化转型的深入，业务应用系统的增多，系统间相互割裂和缺乏交互，又容易导致应用间出现信息孤岛。企业的新老应用并存、业务在不同环境、多云部署等是企业应用部署的常态。治理运营现代化旨在利用云的敏捷性，实现新生应用和现有应用的有机协同，立而不破，构建可平滑演进的企业 IT 架构；通过数字资产的复用性，简化企业应用开发的复杂度，降低试错成本和风险，发挥新老应用和资产的最大价值。实现治理运营现代化的方法和实践主要有：

3.4.1 应用治理双栈模式

微服务可以解决技术栈异构性的问题。通过应用双栈模式，用户可选择侵入式的微服务框架（如 SpringCloud、Dubbo、ServiceComb JavaChassis 等 Java 框架或 GoChassis 等 Go 框架），或者选择非侵入式的服务网格开发、接入微服务，来实现基于不同技术栈的微服务的统一接入与管理。这些微服务可以共同接入到同一个微服务引擎中，通过该引擎帮助开发者处理微服务运行时面临的协同交互问题，比如日志框架、健康检查、分布式追踪等。

3.4.2 应用融合集成

随着云原生技术的普及，使用云原生技术或框架开发新应用成为了主流，但企业不可能完全抛弃“老”应用。应用类型的多样化，又呼唤能将应用间的服务、消息、数据等进行统一封装和集成以提供统一服务的平台的出现。融合集成，在上述需求的驱动下应运而生，成为新老应用共存的最佳实践，其主要方法和实践包括：

1）构建企业联接能力

应用间 API 跨云跨地域集成：集团与各地区子公司的 IT 系统以 API 方式互相开放访问，同时加强 API 调用安全防护，实现跨云跨地域协同。

异构数据间跨网集成：主要考虑应用的完备性和高效性。在完备性上，应用需要考虑 API 类、文件类、设备类、消息类、数据库类、大数据类等的集成。在高效性上，考虑支持全量或增量能力，定时或实时方式。同时，考虑复杂环境下跨网络、跨云、跨数据中心和跨机房等网络环境间数据的同步问题。

跨设备数据集成：将设备与 IT 系统、大数据平台进行连接，收集设备的运行状态等信息，实现设备信息的集成和可视化。设备数据的集成能力，主要体现在标准协议的支持上，包括标准 MQTT、MQTT Client SDK、Link Agent、软 / 硬网关、HTTP 等。

集成开发创新：包括打包开箱即用的功能（如集成流、领域模型、流程模型和业务规则等），以缩短价值实现时间；提高用于集成的连接器和其他资产的质量；扩展支持现代应用和集成设计的可用功能等。

2) 业务信息化关联与融合

自定义业务模型与连接映射：了解行业和业务，才能构建好应用。开发应用所需的大量的业务知识，可以使用“领域驱动设计 DDD”方法论进行管理；业务资产管理，则可通过“元对象机制 MOF”标准来搭建通用化模型管理平台，做到模型管理的标准化与通用化；同时，考虑将数据资产、业务接口、事件消息等技术资产进行自动化映射管理和领域划分，最终形成面向领域和业务对象的模型对接体系，成为业务人员和技术人员自助沟通的桥梁。

业务化集成工作室：集成众多资产，只解决了资产连接的问题，而非融合的问题。而构建集成、编排无码化的集成工作室，实现场景化联接模型关系，形成行业领域模型关系知识；行业领域知识体系之间相互融合和分拆；基于无码化、图形化操作开放场景化数据服务，才能支撑应用的快速构建，实现应用资产真正的融合。

3.4.3 统一 API 治理

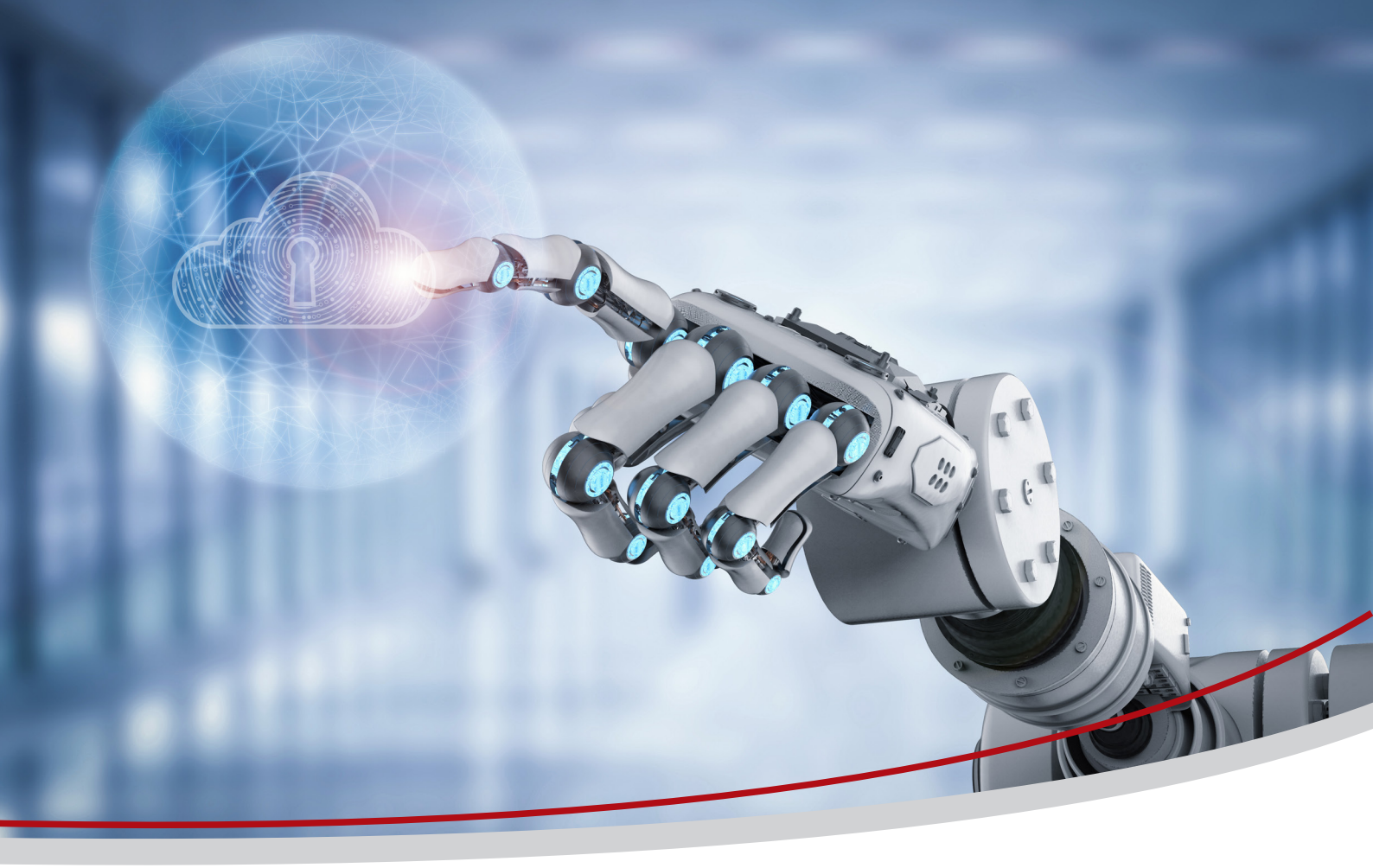
API 已成为企业连接业务与对外提供服务的核心载体，也是微服务架构的事实标准。快速增长的 API 规模和调用量，使得企业系统面临更多的挑战。而使用 API 网关将企业对外提供服务的 API 聚合起来，并提供完整的全生命周期治理能力，成为企业进行统一 API 治理的最佳实践。

3.4.4 多云及边云协同

应用现代化将应用和底层运行环境解耦，这意味着可以将应用部署到更多的不同的环境中。因此，开发人员要构建或利用支持跨云治理运营的应用集成平台，提升应用在多云环境中开发和部署的敏捷性，比如云原生应用既要能在 Kubernetes 的云端环境下运行，也能在边缘侧运行，保障应用在端 - 边 - 云环境下的协同与运营。

3.4.5 资产沉淀与运营

在企业数字化转型中，基于应用开发平台构建的 API、IDE 插件、大屏卡片、业务逻辑单元、微服务、算法等，都属于数字资产的范畴。通过持续的调用与迭代，形成一套高度抽象、可以快速复用的数字资产能力；通过持续的治理与运营，形成数字资产“共建、共用、共享”的普遍共识，促进数字资产的复用与共享，使能信息化应用快速构建与创新。



第四章
云原生业务智能

以容器、微服务、Serverless、DevSecOps 等为代表的先进云原生技术和理念推动着云原生技术的蓬勃发展。企业应用走向全面云化，企业对云原生的需求升级，需要进一步实现业务智能。以数据库、数据仓库、大数据、AI、视频等为代表的传统技术领域也纷纷转变为云服务的方式，成为新的云原生技术，并与其他云原生技术相互融合，呈现出来更加强大的云原生能力，从而实现企业云原生应用的智能升级。

4.1 云原生使能数据资产化

随着5G、IoT、AI等技术的飞速发展，社会每天产生的数据量都在极速增长。据中国信通院《大数据白皮书2020》显示：未来4年里数据量将激增4倍，到2035年呈50倍增长。

2020年3月30日，国务院发布《关于构建更加完善的要素市场化配置体质机制的意见》，意见指出“数据成为与土地、资本、技术、劳动力并列的第五种生产要素”。作为要素，意味着在数据产生、数据共享与流通、数据确权、数据定价等领域需要更多的技术支撑。但从现实情况看，大量数据资源并没有得到有效的治理，更不用说形成有价值的数据资产。

如今80%+的企业将会致力于提升在其所处行业的“数据”能力，随着数据、算法的发展，资产的形态和范围正在出现全新的革命性变化，比如狭义的数字资产（如加密的数字货币）和广义的数据资产。

在政企数字化转型的过程中，越来越多的组织将容器、微服务、Serverless、DevOps等开发周期更短、迭代更快、资源复用率更高、维护扩容更灵活的云原生技术引入数据领域，同时广泛的使用基于云原生2.0开发的AI、区块链、数据库、数据仓库、大数据等组件快速开发数据应用，使得数据资源加速成为有价值可复用的数据资产。

4.1.1 云原生提供一站式、智能的数据治理能力

传统的数据治理手段，不仅需要复杂的技术工具组合，也需要数据分析、数据建模、数据开发、DBA等许多数据专业人员的配合。随着数据的异构多源、实时性要求、数据量的需求变化，数据治理正在从以前关注组织内部管理经营所需的结构化数据为主，转变为以OT数据、互联网数据、以及越来越多的外部数据为主，面向数据全生命周期对一站式的数据治理能力诉求越来越迫切，不仅要解决快速精确性，还要实现实时可预测、可解释，加速数据的资产化过程。过去一些典型的技术手段，如商业智能BI、数据仓库DW、关系数据库等面临越来越多的挑战。

1）灵活统一的数据接入与集成工具

对于庞杂的存量数据，以及不断增加的新的各种各样的数据，数据的接入与集成已经不是一个简单的技术组合问题，更多的是要从数据消费的角度倒推到底应该怎样使用这些数据接入与集成技术。云原生带来的敏捷能力，使得数据消费需求可以快速的实现。

云原生的数据接入与集成工具需要考虑几个方面：

- 支持多类型的数据源：如Oracle，MySQL等关系型数据库，消息/API，数据仓库，Hive，HBASE等大数据各类系统的结构化、半结构化、非结构化数据；
- 支持分布式架构：利用原生架构并行化处理技术实现对海量数据的高校稳定接入，并支持横向扩展，以应对数据接入量的变化；
- 提供数据安全保障措施：如数据高可靠防丢失，数据加密，防泄漏等
- 支持灵活的接入集成调度能力：按需提供定时，周期性任务自定义调度策略
- 统一的管理能力：具备数据接入集成任务统一管理、查看、修改、删除等能力；具备向导式配置等易用性操作界面；提供运维能力，如监控告警等。

2) 数据治理对向智能化转变

在传统数据技术领域，主要依赖 SQL 脚本以及一些简单的图形化操作，数据集成、开发和治理的各个环节都依赖大量人工操作。随着供不应求的技术和数据呈指数增长，数据量快速递增、数据种类复杂，组织需要自动执行数据管理任务，必须要有灵活敏捷高性能的技术手段。大数据软件供应商正在运用机器学习和人工智能（AI）能力，使数据管理过程能够自我配置和自我调整，以便高技能的技术人员可以专注于更高价值的任务。这种趋势正在影响所有企业数据管理类别，包括数据质量、元数据管理、主数据管理、数据集成和数据安全。据 Gartner 预测，到 2022 年，通过增加机器学习和自动化服务水平管理，数据管理手工任务将减少 45%。

云原生湖仓一体平台支持统一元数据管理：解决海量复杂数据治理的核心在于元数据的统一管理，传统政企客户往往采用自建或多家软件供应商的大数据和数仓平台，数据分散在多个技术平台或 IDC 中，企业无法进行数据融合分析和统一标准化治理。基于云原生湖仓一体平台，数据统一共享存储，数据计算引擎整合调度及资源按需弹性扩展。云原生湖仓平台支持跨组织、跨区域、跨云的元数据采集和统一管理，并且数据处理全链路血缘可追溯。

基于元数据的智能增强数据管理技术：在统一元数据管理的基础上，增强型数据管理利用 ML 和 AI 技术优化并改进，让元数据管理从协助数据审计、沿袭和汇报转为支持动态系统。 增强型数据管理技术能够审查大量的运营数据样本，自动发掘数据，自动识别数据中的价值，以及自动采用适合数据的安全措施，实现在最短时间内推送基于数据的精准业务洞察和运营自动优化。

智能增强数据质量管理，保障业务决策准确：利用数据相似度识别、自然语义、NLP 等智能技术自动识别和提取非结构化数据，建立非结构化数据业务词语库。可以帮助自动发现重复、错误等数据质量问题。借助第三方可信数据源，还可以快速修复问题数据。相较于基于规则的数据质量稽查方式，可极大提升数据质量管理效率。

智能增强数据安全治理，支撑隐私保护和合规：利用 AI 技术，可自动对数据进行分类分级和标记，自动发现敏感数据，并对其进行动态脱敏和标注数字水印。通过对用户采集、处理、访问数据全过程操作日志和行为分析，还可以帮助企业进行数据操作合规审计，保障数据共享和交换的安全合规。

智能增强数据融合分析，实现数据价值裂变：利用图像 / 语音识别、多维向量搜索和图计算技术，可自动提取非结构化数据的特征信息，并自动建立数据知识图谱。基于统一的元数据管理，结合一站式数据平台技术，将大数据、数仓、AI 等计算引擎整合调度，实现 OT 与 IT，结构化与非机构，实时与批量的数据融合分析，让数据业务价值产生裂变。

3) 数据管理正在向高效化转变

Gartner 预测到 2022 年使用动态元数据去连接、优化、自动化数据集成流程的企业，数据类项目交付时间将减少 30%。到 2023 年，在数据管理中使用人工智能技术能够帮助企业机构进行更多的自动化工作，企业对于 IT 专业人士的需求将减少 20%。

以数字化场景需求为切入，建立以“数据”为核心的管理和运营体系，构建以数据驱动的数字化转型的新一代 IT 架构和组织能力，是数字化转型最核心的工作。基于技术平台之上，以系统的数据管理和运营体系，管好数据；用高质量的数据驱动业务的运营、战略的制定和创新的产生。

数据资产管理包括四个部分：

» 方法论：结合业界数据实践与数据云服务产品，建立以“数据”为核心的管理和运营体系。

» 管理体系：通过数据治理实现数据清洁，形成统一的数据资源，为应用提供智能数据服务；通过数据运营构建持续机制释放数据价值，实现数据驱动运营。

» 技术平台：政企构建混合数据管理最佳实践的数据湖技术体系架构的数据使能平台。

» 应用场景：对标业务战略、洞察数据需求，政企建设数据应用价值场景，使能卓越运营和有效增长。

4.1.2 构建面向行业的数据资产中心

数据从资源成为资产，最后需要实现数据资产的交换或者交易。在数据资产这个领域，可以分为模型资产和内容资产。模型是内容的框架和约束，具有相对通用的属性。一般来说，70% 的数据模型是通用模型，20% 的模型是行业通用模型，只有不到 10% 的模型是具有高度定制的特点。数据资产中心首先要解决模型的规范。这个模型更多的是国家标准联盟、行业领导者、产业联盟等具备中立属性的机构为主来构建，并提供交换和交易云原生的安全可信能力可以为模型资产交换。

4.1.3 为产业链提供更高效聚合的使能工具

当前数据治理过程繁琐，提供的一些工具又相互独立，很难贯穿整个数据生命周期，并且缺少管理项目交付方法论的工具，导致数据治理项目实施效率低成本高。

数据治理使能工具需要贯穿整个数据生命周期，提供端到端的数据使能工作台，能够打通大数据平台各个组件，贯通整个项目交付过程，流程标准化，方法论服务化，统一 Portal 的资产化过程工作台。同时需要具备数据使能知识库，汇聚行业知识，提供知识管理、检索、标准库、标签库和知识图谱等，同时开放接口，伙伴注册过程套件，以 AI 驱动知识沉淀和运用。

4.1.4 数据全生命周期的云原生技术底座

对于企业来说，弹性、敏捷、高效、安全、统一的数据技术平台支撑，降低业务分析人员、开发人员、维护人员的技术理解难度，提升最终用户试用数据的体验，基于云原生技术构建的数据湖已经被各行各业所接受。

1）云原生数据湖，发挥海量数据价值

大数据系统云端部署逐渐替换传统的线下集群部署方式，成为企业构建大数据平台的首选方案。企业通过将服务托管上云，云厂商对大数据平台做全面优化，带来更优的存、用数体验，企业只需要关注自身业务的开发和维护工作，其价值集中表现在以下几个方面：

» 湖仓一体灵活的架构，有效缩短分析链路，提高分析效率，减少数据冗余。基于云原生技术开发的计算和存储分离架构，实现更高的性能和更好的投资保护，通过裸金属、虚拟机、容器等实现弹性伸缩和灵活部署。随着云上的 IoT、AI 以及千行百业的 IT 应用，越来越多的数据在云上聚集。云原生数据湖也在大数据处理方面产生了离线数据湖（又叫湖仓一体，即 Lakehouse）、实时数据湖（又叫“实时数仓”）、逻辑数据湖等三个重要方向，特别是逻辑数据湖，基于多个离线或者实时数据湖形成的虚拟数据湖，实现租户间资源隔离、多级权限管控，保证跨源协同分析数据安全性。

» 弹性裸金属部署，具备物理机性能，实现大数据上云最佳算力底座。大数据传统物理机软件方案存在以下问题：1）硬件统一采购，配置固定，不合理；2）手工部署大数据步骤多、工程周期长、易出错；3）资源弹性不足，大数据物理机资源往往需要先申报再部署，至少 3 个月，且物理机资源池还是独占，无法共享，难应对波峰波谷业务。在此背景下，基于云原生的弹性裸金属的部署方式成为目前主流，其在大数据场景下通过软硬协同，实现低时延的数据存储和网络 IO、分钟级的资源弹性发放等优点。

» 存算分离实现资源池化，弹性伸缩，降本增效。存算分离方案有效的实现资源价值最大化，存储与计算资源全面云化。存算分离在大数据场景下可以实现数据共池、按需扩容、计算优化、存储冗余优化等特性。

» Serverless 全托管，支持业务敏捷开发，云上自动部署维护。很多企业使用大数据分析时会面临使用门槛高、业务与数据量波峰波谷带来资源利用率低、创新业务落地慢等问题。云原生 2.0 时代使用 Serverless 技术解决以上挑战。Serverless 主要特点是完全托管及免运维、容器化与秒级扩缩容、结合 AI 实现智能创新，避免了传统虚拟机安装部署周期长、灵活性差的问题。

2）数据仓库提速全场景数据分析

随着云原生 2.0 时代的到来，数据仓库的实时推荐、实时风控、实时监测、实时数据和历史数据关联分析等技术能力，可广泛应用在工业 IoT、金融、车联网等不断丰富的业务场景中。云原生数据仓库提供完整的高扩展，高性能解决方案以实现多种部署形态，资源弹性、敏捷发放。这意味着云原生数据仓库不再是大型企业的专有设备，同时也可满足大中小企业各类应用的数据分析需求。云原生数据仓库支持裸金属、虚拟机、集群等多种部署形态，无论哪种部署方式，都具备弹性、隔离、高性能、高拓展的特性。

云原生数据仓库充分利用云对象存储高扩展和低成本的优势，构建多温存储的存算分离架构。本地盘性能加速，云对象存储作为冷数据存储，实现分层存储，自动冷热数据迁移。用户可以按需选择，数据冷热动态切换，降低数仓存储成本同时，也灵活应对业务的场景变化。进一步的支持表内不同分区间的冷热数据交换，并支持以列存数据块作为单元的更细粒度的交换，以及更加智能和精细化的冷热数据管理，同时类 Multi-Cluster 集群和多租户技术，将存储和计算资源进行了更细粒度的隔离，用户可以对不同的业务划分不同的逻辑集群或租户，实现更加灵活的弹性。

从离线报表到实时计算的全场景数据分析，通过降低数据入库时长和提升数据分析速度，实时数仓应对用户提供实时入库、实时分析的能力：

» 实时入库：通过高并发小批量模式，线性扩展流数据入库性能，理论上能达到上千万级每秒的入库性能，彻底改变传统数仓的 T+1 大批量加载模式。

» 实时分析：支持基于流式数据的持续计算查询，通过 SQL 完成流式计算，实现亿级数据秒级聚合。

3）聚焦全场景，构筑云原生数据库全栈能力

进入云原生 2.0 时代，云原生数据库不仅仅要利用云的硬件资源池化能力实现数据库的计算存储能力弹性伸缩、分布式部署和高可用，还需要能利用云基础设施本身的能力，如跨 AZ 部署能力实现数据库的跨 AZ 访问，基于云存储理解数据库语义的能力实现数据层能预处理数据库语义等等。

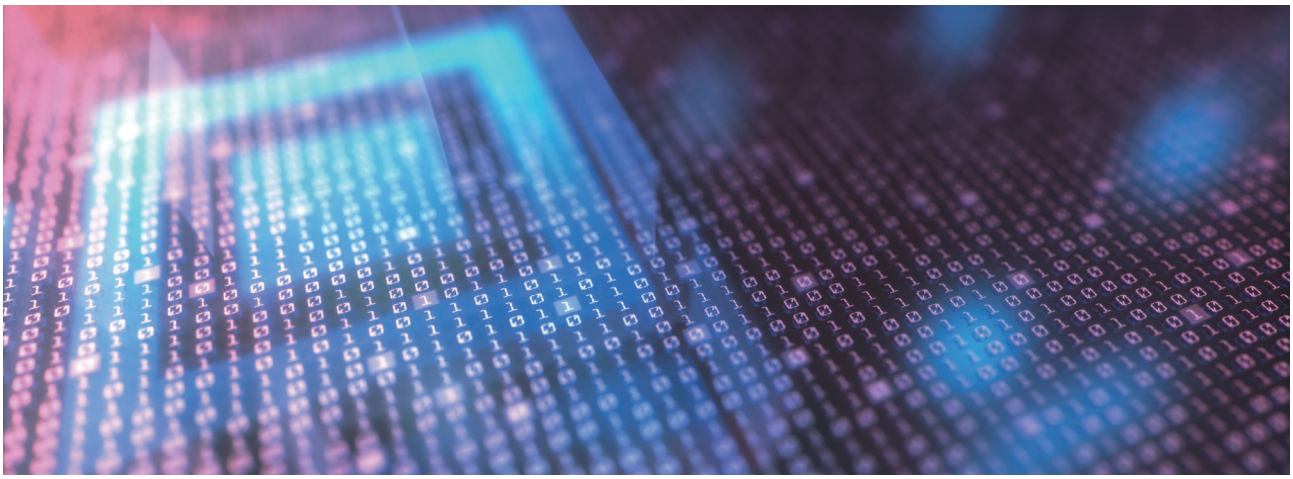
■ **存算分离，极致弹性**

在云原生 2.0 时代，计算资源层中 CPU 算力与内存也会解耦，计算能力池化、内存容量池化、存储能力池化，“计算 - 内存 - 外存”三层资源彻底解耦，分别弹性伸缩。

云原生数据库要可以支持分钟级别的节点扩展能力，秒级的高可用切换、存储扩展能力、资源释放回收、快照备份能力。

■ **多平台软硬协同，数据存储可靠**

存储层应支持近存储处理（NDP）能力，计算层下推语义到存储层，在存储层预处理数据库的算子。比如范围查询，



在确保事务隔离性、数据一致性的前提下过滤掉不需要的数据，避免计算层和存储层无意义的数据交互。

存储层应支持日志回放能力，数据库写节点只需要把日志写到存储层，将日志回放为数据页面，并在多副本上提供一致性版本给其他节点访问。

云原生数据库应针对云底座的基础设施进行深度优化，支持 ARM、x86 等多种平台并针对不同平台进行优化，各平台性能差异低于 20%。

存储层应确保全场景负载数据文件绝对可靠，至少三副本存储，并具备多副本强一致访问能力，单副本故障不影响数据可靠性和访问速度，故障可自动恢复。

- **跨 AZ/Region 部署能力，让数据底座更加稳定可靠**

云原生数据库需要具备跨 AZ 的部署能力，并且提供跨 AZ 的读一致性访问，多 AZ 节点必须读到一致的数据。2AZ 部署下需要保证单 AZ 故障不影响云数据库的读访问。3AZ 部署下需要保证单 AZ 故障不影响云数据库的正常读写，单盘访问故障、AZ 间网络短时抖动故障不影响性能。

- **统一架构，多模兼容，开放生态**

云原生数据库应该具备统一的架构兼容多种生态接口，利用同样的云基础设施资源，可以使用 MySQL、PostgreSQL 这样的 SQL 接口访问数据库，Redis、MongoDB 等 NoSQL 接口访问。同时也应该支持多种模型的兼容访问，比如支持 KV 模型、时序模型、文档存储模型、宽列模型等。

云原生数据库应该支持用户在不同的数据库之间迁移数据，不应该绑定用户。开放生态的数据库将成为云原生数据库的主流。

- **智能运维，自动调度，让数据库运维更加高效、极简**

AI 与数据库结合是近些年行业研究的热点，云原生数据库的优势之一就是可以利用技术手段实现数据库的自动化运维，当前比较前沿的手段是利用 AI 技术实现数据库自调优、自诊断、自安全、自运维、自愈等能力，借助于 AI 技术能更好的优化数据库的性能，协助 DBA 降低运维难度，提升运维效率，自动调度平衡资源池。典型场景如慢 SQL 发现，索引推荐，基于性能指标的时序预测与异常发现，参数智能调优等。

4.2 云原生 AI 开发及知识计算加速行业 AI 落地

新一代人工智能在全球范围方兴未艾，并成为引领科技革命和产业变革的重要驱动力。一批创新活跃的企业正在通过应用 AI 实现加速成长，并呈现出蓬勃发展的态势。

进入云原生 2.0 时代，AI 逐步在行业广泛应用。在汽车行业，中国第一汽车集团有限公司通过应用 AI，将知识基于业务场景，以数字化的方式呈现在员工的眼前，快速提升员工能力。在医疗行业，通过 AI 技术将 DNA 羟甲基数据以及经过大量实验积累的基因知识图谱进行整合运算，更加准确地识别出血液中的关键生物标记物，将早期诊断的准确性提升了 9 个百分点，这有助于对食道癌患者的早期发现。在油气领域的储层识别场景，AI 将多源异构数据、空间地质关系、录井传感器特征等进行联合表征，通过结合联合表征与深度学习预测模型，缩短了 70% 的油气层评估时间。上述例证都验证了 AI 对于实体经济有着卓越驱动力。

云原生 AI 开发，更是以全流程的极简和自动化升级传统 AI 开发模式，让数据准备、算法开发、模型训练、模型推理、边缘设备纳管、以及围绕 AI 的代码和资源的分享，全链条产生质的飞越。借助“AI 增强 AI”的理念，云原生 AI 开发需要将“自动标注”、“沉浸式开发”、“模型自动调优”、“弹性推理”等能力以自动化、流程化的形式提供给用户，进一步减低用户的技术门槛和落地难度，为用户快速实践人工智能扫清障碍。接下来将对云原生为传统 AI 开发流程所带来转变分别进行阐述。

4.2.1 智能化数据服务，简化数据准备，降低开发成本

人工智能开发过程中，开发者往往专注于算法的创新设计和开发，而较少去做数据采集、处理、标注、分析等工作。但伴随数据规模及种类的急速增长，数据准备的工作量和难度会越来越大。针对实际业务场景面临的数据采集难、数据质量差、数据冗余大、标签少、数据分析难等问题，基于云原生，可以让 AI 数据管理更加系列化智能化，简化数据准备过程，大幅降低开发成本，提升开发效率：

- 轻松采集多种数据：支持从数据库、云存储服务等多种数据源采集数据，将 csv 文件，非结构化的视频、音频、图片、文档、文本及自由格式数据轻松导入，用户可以通过版本管理工具进行数据管理。
- 丰富的数据处理能力：统一的数据处理能力，包含校验、转换、清洗、选择、增强等多种处理算子，通过分布式任务加快海量数据处理速度，从而为用户省去线下筛选或增强数据的成本，提升数据质量。
- 智能化标注：除了提供通用的标注工具外，还提供了基于机器学习技术的智能数据标注、团队标注等功能提升用户的标注效率。
- 可视化分析：提供可视化曲线对数据进行细粒度的分析诊断，帮助用户了解数据特点，如图片的清晰度、亮度、高宽比等特征，进一步挖掘数据价值。

4.2.2 开箱即用，云原生 AI 开发环境，解放开发者生产力

传统的 AI 开发过程复杂，涉及到海量数据处理、模型开发、训练加速硬件资源、模型部署服务管理等方方面面。基于云原生，AI 开发过程简化成为可能，让开发者可以聚焦业务实现，提升开发效率。

» 开发环境软硬件齐聚，开箱即用：当下，不同的开发者习惯使用不同的 AI 开发框架（Tensorflow、PyTorch、MindSpore 等）开发算法，而且基于业务的复杂程度需要的计算加速硬件（CPU、GPU、Ascend 等）也不同。云原生 AI 开发平台可以根据开发者的场景提供不同软硬件组合的快速启动、即开即用的 AI 开发环境，开发环境声明式获取，开发者无需关注环境搭建和维护过程。

» 开发过程简单易用：开发平台可提供多样化的开发模式以满足各类开发者的开发习惯，如基于 Web 方式可提供良好交互式编程体验的 JupyterLab，完全基于于云端开发 AI 工程的 WebIDE，基于本地 IDE 连接云端开发计算环境进行远程开发 AI 工程等。开发者对计算资源规格需求随着开发阶段不同而动态变化（如代码编辑阶段无需训练加速硬件，调试阶段需要低性能计算资源，模型训练需要高性能计算加速硬件），云原生开发平台可满足开发者动态切换开发环境计算规格的需求。AI 开发过程中涉及海量数据，而海量数据一般都是存储在云存储服务，开发环境应该提供开发者灵活地数据访问方式，如支持 SDK 的方式对云存储数据上传下载，支持动态挂载云储存数据到开发环境文件系统，方便开发者以 POSIX 语义方式读写云存储数据等。

» 开发成果可快速输出应用：AI 开发环境还需要满足开发者沉浸式完成 AI 工程开发生命周期，在开发环境中快速流畅地将开发调试阶段的输出（代码、模型等）和部署发布（大规模分布式训练、模型部署等）完整地串联起来。开发环境平台可方便开发者分享开发的案例，如开发的 notebook 案例可一键分享给伙伴，伙伴一键打开开发环境体验案例。

4.2.3 资源动态扩展，参数自动调优，助力普惠 AI

AI 算法创新和模型训练技术日新月异，目前有三个大的趋势和挑战：

» 随着无监督技术、神经网络结构搜索等技术的发展，AI 模型训练的规模越来越大，其算力需求呈指数上升；

» AI 模型训练不可避免地需要进行不断的调参，在深度学习越来越主流的今天，调参更加需要加速；

» 联邦学习逐渐成为保护数据隐私、联合多方数据提升模型精度的关键技术，场景落地越来越多。

基于云原生的 AI 训练可以提供弹性训练的方式使得训练作业可以充分利用闲置资源提升训练性能。在常见的图像识别场景下，可以从单节点动态扩展到多节点，实现 10X 倍的训练性能加速；基于云原生的训练平台还可以提供训练过程中自动调参能力，使得用户无需代码修改，即可根据自定义的搜索目标和超参搜索，相比人工调优而言，可以提升几倍的搜索速度；此外，基于云原生的训练平台还可提供联邦训练能力，使得用户可以联合多方数据实现模型训练效果的提升，FedAMP 模型聚合算法，相比业界主流的 FedAVG 算法，可使模型精度提升 2% 以上。

4.2.4 云原生 AI 推理，性能卓越，稳定在线

AI 在各行业开始广泛落地，云原生 AI 推理应运而生。快速交付，高性能推理快速扩容，在线稳定运行是云原生 AI 推理的核心特征。提供完整的云原生 AI 推理能力是一站式 AI 开发平台的必备特征。

传统 AI 应用的门槛高，不仅是算法学习门槛高，还包括了工程落地门槛，需要更新很多前沿的系统技术栈，包括深度学习框架、分布式技术、容器技术、云边端协同技术、并行推理、算子编排等，云原生推理系统提供一系列相关支持。云原生推理在高性能算子、算法 / 模型优化、任务调度、高效执行引擎、异构资源利用等方面构建了性能竞争力，在弹性推理方面，根据业务运行情况弹性伸缩，提升硬件资源使用率和利用率。云原生推理作为云上 always online 的服务，服务稳定性至关重要。云原生系统通过弹性扩容、API 限流、熔断、故障自动恢复等各种能力可以保障推理业务稳定运行。

4.2.5 云原生知识计算加速 AI 进入行业核心生产系统

AI 在发展过程中，经历了知识驱动和数据驱动两个阶段。第一阶段是由知识驱动的人工智能，包括知识、算法、算力三要素；第二阶段是由数据驱动的人工智能，包括数据、算法、算力三要素。这两个阶段都有一定的局限性，无法解决 AI 深入行业的所遇到的问题。例如：

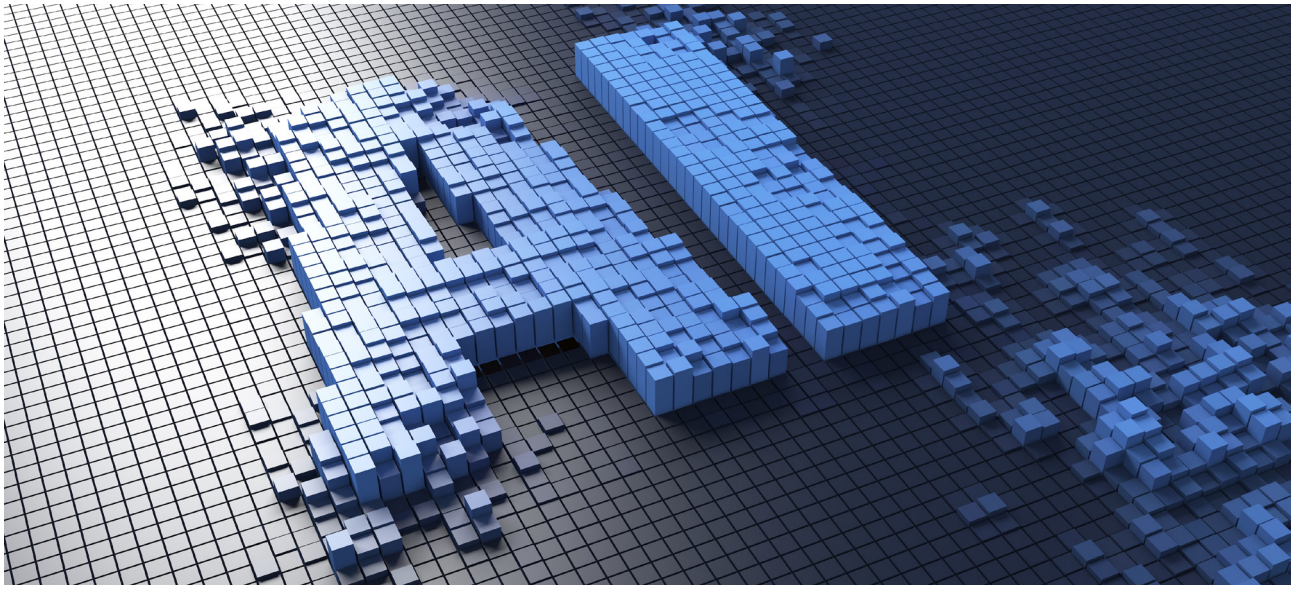
» 行业专家与 AI 专家的合作：如何让行业专家和 AI 专家，双方能够相互听得懂，围绕一个共同的目标相互促进？

» 行业机理与 AI 模型的结合：不同行业都有自己数十年甚至上百年的专业积累，形成了大量成熟的物理、化学、生物等知识表达的机理模型，这些模型和数据驱动的 AI 模型能不能结合，如何有效结合？

» 行业应用与 AI 系统的结合：行业自身多年积累的应用系统、控制系统和 AI 系统到底是什么关系？如何让这些行业应用平滑有序地升级成智慧系统？

这些问题背后的核心焦点，是如何将行业知识与 AI 进行结合。新一代人工智能技术要解决如何与各行各业深度融合的问题，要做到真正的落地就需要把知识驱动和数据驱动结合起来，实现 AI 与行业知识的高效结合并充分利用知识、数据、算法和算力四个要素，这是 AI 未来发展的必然方向。云原生对资源的高效组织和其上的丰富应用加速了这一进程的到来。

每个行业都在发展的历史长河中沉淀了大量的知识，比如生产系统中的机理模型、大量的行业技术典籍文献、专家大脑里面的宝贵经验、历史积累的方法总结、测试报告等等。行业不缺知识，但是缺乏高效利用知识的方法。



华为云发布业界首个全生命周期知识计算解决方案，该方案包含知识获取、知识建模、知识管理，以及知识应用四大模块，覆盖知识在企业的生产环节中的全生命周期。

» 知识获取：对多模态的行业知识，如生产系统中的机理模型、行业技术文献、专家经验、历史方法总结、测试报告等，进行解析和处理，这是数据转化为知识的第一个关键阶段。多模态知识抽取技术可以对多源异构数据（包括结构化、非结构化、半结构化数据）进行快捷便利的知识识别和知识抽取。为了减少模型对训练样本的依赖，减少标注工作量，小样本学习技术非常关键。

» 知识建模：根据业务场景进行知识建模，提供流水线式自动化构建知识图谱的能力，可以使得图谱构建时间由数星期缩短到数分钟，同时可以实现知识图谱的自动更新。

» 知识管理：对于企业知识提供超大规模图谱存储能力和高性能查询，以及自动化更新、冲突管理、质检控制等能力。企业的海量知识通常用图结构进行表示，华为超大规模知识图谱，单实例支持百亿节点，万亿边规模。

» 知识应用：提供知识搜索、可视化分析、知识推荐等基础能力，以及智能对话、预测分析、知识推理等高级能力，匹配企业多样化的应用需求。华为云支持单实例 10W+ QPS（每秒查询率）图谱查询，可以实现秒级响应；在行业应用上，知识计算将油气行业测井解释效率提升 3 倍。

通过应用知识计算解决方案，企业将可以打造自己的知识计算平台，整合分散在不同介质、多种形态的企业数据，形成带有建议性的知识，有效用于预测分析和辅助决策，提高企业的经营效率。云原生对资源的高效组织和其上的丰富应用加速了知识计算的落地进程。

4.3 云原生视频服务，重塑体验，激发创新

视频上云成为趋势，视频全流程云服务化成为新常态。IDC 预测显示，到 2024 年，中国视频云市场规模将会超过 220 亿美元。随着 ICT 基础设施升级，视频全流程能力将逐步上云，视频内容的创建和存储的位置会由端向云和边转移。预计到 2025 年，网络流量中 90% 将是音视频数据，数据创建的位置中心 + 边缘将达到 50%，数据存储的位置中心 + 边缘将达到 70%。视频的制作、处理、传输在云上将成为新常态。

实时音视频迎来大发展，互联网直播进入毫秒级时代。在互联网视频领域，疫情极大加速了实时音视频相关的在线教育、远程协作等行业，同时电商直播兴起，带动直播业务领域的进一步发展。2021 年在云上转发的实时音视频分发数有望超过 1000 亿分钟 / 月，产生约 700EB/ 月的实时音视频流量。为了支撑互联网视频业务的发展，互联网视频技术也将迎来以下升级：

» 实时音视频技术将广泛应用在在线教育、远程协作、社交、金融、医疗等各个领域。为了实现更实时的交互，实时音视频通过端侧的实时编码、渲染、云侧的 Mesh 化网络架构、超低时延的合流转码、极致的抗弱网能力，实现稳定、高效、实时的音视频交互能力。

» 互联网视频直播将由秒级进入到毫秒级时代，通过 Mesh 化的网络架构、超低时延的实时编码、智能化的全局调度，互联网视频直播时延将降低到百毫秒级，极大提升用户体验。

4.3.1 视频业务由分发段上云演进到生产段上云

一部顶级影视节目或综艺节目，节目素材是几个 PB 级别，中间经过多个制作环节才能形成可播出的内容，节目制作周期长。内容商期望通过生产端上云的方式，实现云上的高效内容制作，缩短节目制作周期，同时满足远程协作、智能生产等需求，因此在视频生产制作环节，有以下新趋势：

» 电视台直播将逐渐云化、轻量化。通过 5G 实现直播信号的回传、云上进行低时延的云导播、云媒资、云快编处理，实现面向电视屏和互联网终端的实时分发，最终降低直播成本，实现随时随地进行的轻量化直播业务。

» 顶级的影视、电视剧、综艺节目制作将在云上完成。5G 和专线超级上行技术，解决了 PB 级内容素材高速上云的问题。通过整合合作伙伴能力和云服务能力，并依托于云的灵活弹性扩容、并行处理、高安全机制，将可实现在云上的拍摄、后期制作、发行等全流程服务，让视频制作效率提升 10 倍以上，同时视频生产更加智能化、标准化、远程化。

4.3.2 统一架构、云边协同、资源复用型的云原生媒体网络

当前整个视频产业现状是不同的视频业务都有一个媒体网络支撑，而这些媒体网络都是互相割裂的，呈烟囱式的孤岛状态，他们之间的资源无法充分复用，比如在线教育领域，背后依托的是 RTC 传输网络，互联网视频的直播、点播，依托的是 CDN 直播网络，行业视频依托的是连接几百万台摄像机在云上进行视频处理的网络，这几个网络之前都是互相割裂的。

新一代的媒体网络，基于统一架构来构建，承载下行的直播点播业务、双向的实时音视频业务和上行的行业视频业务，实现云基础设施的共享和复用，最优化视频传输的成本，保障体验的一致性。新一代的媒体网络有以下特点：

» Mesh 化网络架构：网络内视频的路由均取决于用户体验和传输成本，通过智能调度进行优化选择、就近传输。

» 容器化的边缘站点：资源可以灵活分配给各服务，所有服务实现资源的共享，最大化复用带宽成本，实现所有业务成本最优

» 智能调度：将所有网络数据均汇聚到大数据平台，通过分析这些实时数据选择最优路径，确保最短的路径转发，实现体验最优和时延最低。

» 云边协同：通过边缘媒体处理框架，基于函数计算平台，将函数级的视频处理能力灵活部署到边缘进行处理，降低回源处理成本，提升用户体验。视频处理能力按需部署到不同网络位置，减少回源到中心处理的流量，降低传输成本。

4.3.3 通过云原生视频服务，持续拓展视频业务边界，实现视频体验创新

从 2G、3G 到 4G，内容产业与网络带宽总是协同发展。当前，随着更大带宽、更低延迟的 5G 时代呼啸而至，4G 滋养的移动互联网小屏视频时代亟待向 TV 大屏 + 手机小屏 +VR 第三屏的融合视频时代转型升级，而以 5G+4K/8K+ 多视角 / 自由视角 /VR 全景视角为代表的超高清视频技术及体验，正是这一进程的最大牵引力。

5G+ 云 + 视频的化学反应，将推动视频产业、视频体验的进一步发展：

» 由新技术赋能催生出全新的空间视频类体验：空间视频（如自由视角）相比传统视频提升的不仅仅是画面清晰度，更在于极强的临场感、交互性及自由度。这样的新内容、新体验一旦通过千兆网络及电视屏、手机屏、VR 屏与数亿互联网用户见面，毫无疑问将打开巨大的内容产业新空间，创造新的增量价值。以自由视角举例，去年湖南卫视推出的《舞蹈风暴》节目就采用了这一创新实践，可以看到一方面这样的技术可以产生新内容，让原本难以实现的场景变成现实，产生新的爆点。

» VR 视频率先进入 8K 时代：通过云端 VR 编码、基于 FOV 的分片传输技术和 VR 云渲染技术，VR 业务所需要的带宽降低了 70% 以上。随着新一代更轻便、更清晰的 VR 设备发展，基于云的 VR 视频和 VR 游戏业务将成为主流，VR 业务体验将迈上新台阶。

» AR 虚实融合技术将打造一个全新的镜像世界。通过云上的空间计算、云渲染、数字世界引擎、RTM 等服务，将逐渐在城市、园区打造虚实融合的镜像世界。人们通过手机、AR 眼镜，可以观看叠加在现实世界上的镜像世界信息，参与镜像世界活动，观看镜像世界表演，实现镜像世界中的广告营销、地图导航、虚拟展览、城市活动、智慧文旅等。

第五章
云原生安全可信

针对云原生架构特点制定的安全防护手段，与基于传统数据中心及云计算平台应具备的安全措施有效配合，最终形成完善、可靠、安全且具备韧性的云原生系统，才能有效地支撑云原生应用的正常运行。

随着云原生技术的不断发展与落地，在实际的生产系统中云原生安全包含两层含义：一方面是“面向云原生环境的安全”，另一方面是“具有云原生特征的安全”。面向云原生环境的安全，其目标是防护云原生环境中的容器、编排系统和微服务等安全，而具有云原生特点的安全则是具有云原生特点的安全防护机制，这些特性包括弹性敏捷、轻量级、可编排等。

5.1 云原生基础设施安全

针对云原生基础设施，应该自底层物理服务器开始，逐层向上实施安全防御加固，从而达成针对云原生基础设施的纵深防御体系。

5.1.1 针对物理服务器 / 虚拟机安全防护

应针对云原生基础设施的宿主机（物理服务器 / 虚拟机）实施安全加固，基于业界最佳实践进行系统安全配置，并使用安全的容器专用操作系统，将容器系统中不需要的模块、服务、对外端口进行关闭。进行必要的权限管理和访问控制。确保宿主机上使用的操作系统、系统软件等不存在已知的安全漏洞。可利用安全配置基线检查工具对宿主机实施安全基线检查，确保基础设施已按照最佳实践进行安全配置和加固。

此外，为了应对针对宿主机的入侵攻击，还可以使用和部署主机入侵检测 / 防御工具 / 服务，及时发现并响应入侵行为，阻止攻击行为并减少影响范围。

5.1.2 针对云原生组件安全防护

应针对云原生组件实施定期漏洞扫描，及时发现软件存在的已知漏洞并及时实施漏洞修补，确保云原生组件无已知的组件漏洞风险；其次，应基于业界最佳实践对组件进行安全加固，如访问控制策略、账号管理、启动策略等，避免用户使用不安全参数导致安全风险，例如特权容器启动、root 账号启动、挂载主机敏感目录等。云原生系统维护者应基于业界最佳实践与系统实际反馈信息制定安全基线规范，形成标准化的基线检查 checklist 并及时更新，确保云原生系统在设计及部署之初即具备足够且合理的基本加固与安全防护能力。

5.1.3 针对云原生网络安全防护

可利用 Kubernetes 组件原生的 Network policy 实施不同容器实例及 Pod 之间的访问控制，以弥补传统网络防护机制无法感知容器级 /Pod 级网络流量。此外，可使用 Sidecar 或 DaemonSet 的方式在 Pod 或宿主机上部署网络 Agent，用于检测容器间东西向流量并实时控制策略，提供更细粒度、控制策略更丰富的网络防护机制。业界已有的开源软件如 Cilium 即可通过 Overlay 组网的方式实现细粒度的网络安全防护。

5.1.4 针对云原生运行时安全防护

应针对容器运行时实施多层次的安全防护，保障容器按照预期设定运行，敏感信息不丢失：

» 应实施充分的运行时安全策略控制，以最小权限与必要原则确保每一个拉起的容器只运行必要的程序、使用必要的资源、访问必要的文件，避免由于额外的权限、资源、代码形成异常行为。

» 应实施全面的运行时监测手段，以监控节点中容器运行状态，发现挖矿、勒索等恶意程序，发现违反安全策略的容器行为。应实施容器逃逸攻击检测机制，以应对容器运行时最大的威胁风险。逃逸检测应不仅仅基于容器镜像内文件的 HASH 计算特征值作为判定容器逃逸行为的关键因素，更需要对容器行为规律进行监控与分析，真正从逃逸行为规则的角度判定容器是否出现逃逸行为。目前，业界已出现利用 AI 技术，从宿主机角度通过机器学习结合规则检测逃逸的机制，实现更加精确的逃逸行为检测，可有效检测出 shocker 攻击、进程提权、DirtyCow、Meltdown&Spectre、Docker in Docker 等逃逸攻击行为。

5.1.5 复用云计算平台安全能力

除了针对云原生系统设计的安全机制与安全加固外，支撑云原生系统运行的底座，云计算平台亦具备丰富的安全能力和安全服务，云原生系统可借助这些强大的安全能力 / 服务强化系统安全能力，弥补防护方面的短板。这些能力包括云计算平台提供的防 DDoS 攻击能力以应对资源耗尽型攻击；入侵检测 / 防御能力以应对容器入侵攻击行为；密钥管理服务 / 组件用于协助用户统一管理系统中使用的加密密钥，确保系统中的敏感信息不被泄露；云盘加密服务帮助客户保护有状态型业务应用的落盘数据安全。

5.2 云原生服务安全

5.2.1 软件供应链安全

针对软件供应链面临的安全风险，云原生系统应围绕容器镜像提供全生命周期的安全防护能力，确保处于生命周期各阶段的镜像安全。

1) 功能全面的镜像扫描能力

云原生系统应为用户提供功能全面的镜像扫描工具，协助用户有效应对镜像安全风险。一个功能全面的镜像扫描工具应能够对镜像仓库中的镜像和工作节点中运行容器的镜像进行检测扫描。检测扫描的内容应包括基于权威漏洞库信息（如 CVE 等）的镜像内组件安全漏洞情况、镜像不安全配置信息、镜像是否含有恶意代码、镜像是否存在密钥等机密信息的硬编码情况等。除了具备安全扫描功能外，还应提供必要的漏洞管理能力，帮助用户清晰明了的了解每一个镜像的安全漏洞情况，给出关于漏洞的修复建议。

2) 镜像完整性保护能力

云原生系统应为用户提供用于保障镜像完整性的机制或功能，并通过一定的控制手段阻止无法通过完整性校验的镜像部署到容器集群中。可通过签名技术实现镜像完整性保护，并通过与镜像构建的 CI/CD 流水线工具进行整合，实现镜像构建过程控制，从构建、测试、扫描到完整性检测全流程管控镜像内容安全可靠。业界已有类似 Google 开源的 Kritis 组件以及 Docker 提供的 DCT（Docker Content Trust）机制用于镜像完整性检测以及基于完整性进行安全控制。

3) 镜像内容安全保护

对于用户利用自研代码构建的镜像来说，云原生系统应提供足够的代码检测能力，帮助开发者在编码完成后执行静态安全检查及代码质量检查，并提供缺陷的改进建议，有效管控代码质量，确保镜像在源代码构建阶段就将逻辑错误或安全缺陷问题解决，降低基于镜像启动的容器攻击面。

4) 镜像仓库安全防护

对镜像仓库的安全防护主要通过部署访问控制机制来控制镜像的拉取与访问，确保只有合法的用户才能访问相应的镜像。此外，应基于最佳实践确保镜像组件配置符合安全要求，镜像组件不存在已知的安全漏洞。

5) 镜像传输安全

无论从研发环境将镜像推入镜像仓库或者从镜像仓库将镜像拉取至工作节点，均需采用加密的安全通道进行镜像传输，确保镜像的完整性与机密性。

5.2.2 微服务安全

针对微服务架构中服务众多、接口交互频繁且复杂的特点，云原生系统应利用如服务网格之类的微服务治理框架对微服务进行细致的安全防护与控制。

1) 微服务组件安全

微服务治理框架通常由多个部分组成。一般而言，包括数据面的代理 Agent 与控制面的相关管理组件，每一个组件应首先确保不存在已知的安全漏洞且相应的系统配置符合最佳实践要求。

2) 认证授权

众多的微服务通过 REST API 对外暴露，会给系统带来权限控制相关的安全问题。因此，微服务治理框架针对微服务架构应提供面向 API 的认证授权机制，这里主要需要解决两方面的问题：第一个方面是对调用者进行身份认证鉴别，第二个方面是对 API 级别的操作权限控制，且这两个问题是具有先后顺序的。应首先对调用者进行身份鉴定，当鉴定完毕后，再对于该身份判断某个 API 操作是否具有相应的权限。

3) 安全通信

微服务之间的 API 调用存在大量的数据交互，微服务治理框架应提供可靠的通信传输能力。一般通过 SSL/TLS 通信协议将 API 通道做加密传输处理，为数据的传输提供足够的安全保障。另一方面，微服务治理框架应提供 L4/L7 层的访问控制机制，确保每一个微服务只与必要的微服务进行安全通信，避免某个微服务被攻击者突破后实施东西向攻击尝试。除此之外，框架应提供 API 调用 / 通信的可视化关系图，协助用户针对异常行为进行有效分析与异常响应。

针对上述微服务安全防护要求，云原生系统可考虑采用 Istio 等服务网格组件实施微服务治理。Isito 是一个流行的开源服务网格软件，其提供一种非入侵的方式来建立已部署的服务的网络，具备负载均衡，服务到服务双向认证，加密通信、L4/L7 流量监控等等功能，而不需要改动任何服务代码。

5.2.3 Serverless 安全

为了应对 Serverless 在前一小节中提及的安全风险，我们应该从如下几个角度进行相应的安全防护。

1) 应用程序代码防护

应用程序代码防护应从两个方面考虑，一是安全编码，二是漏洞防护。

安全编码需要开发者能够充分考虑 serverless 场景下函数面临的安全风险，进而在函数设计之初进行相应的安全考虑。首先，由于 Serverless 函数的执行为事件触发，因此针对不同的事件源，我们都应该视为不可信，在代码设计的过程中进行相应的事件源管控，如采取白名单机制进行筛选。其次，针对函数中可能存在隐含威胁的字符，需要进行编码转换，防止代码注入攻击。最后，切忌勿将敏感数据进行硬编码。

漏洞防护则是针对 Serverless 函数引入第三方库可能存在的安全漏洞进行防护。通过自动检测工具进行分析，从而协助开发者及时发现函数中依赖项存在的安全漏洞并做及时的修补工作，确保函数上线前无已知安全隐患。

2) 数据安全防护

数据安全防护应当覆盖安全编码、密钥管理、安全协议三方面。安全编码涉及上一条提及的敏感信息编码，密钥管理涉及密钥的存储与更换，安全协议涉及函数见数据的安全传输。

安全编码方面，开发者常常为了方便调试，将一些敏感信息写在日志中，再最后上线时却忘记将相关的信息从代码中删除，从而引发敏感信息泄露。例如 python 的 OAuthLib 依赖库曾在其日志文件中写入敏感信息，可从 Debug 日志中获取开发者的用户名与密码。

密钥管理方面，开发者可利用云计算平台 / 云服务商提供的密钥管理服务或模块进行密钥管理。相较于用户手动进行密钥管理，云计算平台 / 云服务商提供的密钥管理服务可在密钥数量较多时提供安全有效地的批量密钥管理。

安全协议方面，与传统通信场景一致，为避免中间人攻击等安全风险，函数间应使用安全的通信协议进行加密传输，如使用 mTLS 协议。

3) Serverless 平台账号安全防护

为了应对 DoW 攻击，云服务商可通过提供账单告警机制对用户进行账号消费告警，如 serverless 使用者可通过设定调用频率与调用费用门限值进行及时的 DoW 攻击响应；除此之外，还可以基于资源限额进行控制，即函数到达一定副本数就不再进行扩展，从而降低 DoW 攻击带来的影响。

5.3 云原生安全过程可信

云原生的服务根植于从需求规划、架构设计、系统开发、运维运营到客户服务的全生命周期中。无论内部业务流程还是对外客户服务，都完全遵从法律法规和国际标准提出的安全、合规和隐私保护基本原则，将功能与质量、安全与隐私保护融入云服务全生命周期，同时特别关注个人信息在采集、使用、保留、传输、披露和处置等处理过程中的隐私保护，确保流程透明、结构完善、控制严谨、过程可追溯。

5.3.1 云原生的开发运维流程

吸收业界先进理念的基础，持续改进开发运维流程，形成开发、运维、安全一体化的 DevSecOps 可信流程，并通过工具和技术规范实现了流程的固化，使过程和结果透明可见、从故障现象到模块代码可追溯，从而实现云服务全生命周期的过程可信。

DevSecOps 流程聚焦质量与效率两个关键指标，在软件开发的整改过程中，落实：

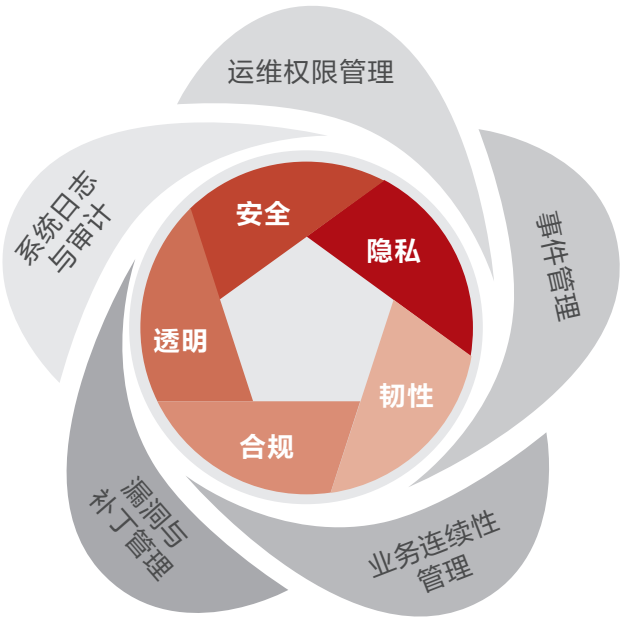
- 安全、可信是团队所有人的责任，实现安全、可信成为每个团队成员的思维方式和工作状态；
- 安全、可信始于研发规划与需求梳理，建立安全、可信是设计的出发点，将安全和隐私融入设计并默认执行（Security & Privacy by design and by default）；
- 安全和质量保证手段无缝嵌入到 DevSecOps 的全生命周期并能自动化实现；
- 加强反馈和持续改进机制，模块间建立小循环，运维运营驱动服务产品创新，不断推出引领行业发展的云服务；
- 技术架构解耦是 DevSecOps 流水线的基础，云软件产品均能实现独立开发、独立测试、独立发布、独立部署和独立运维。

5.3.2 安全稳定的可信运营

安全、可信的运维运营内容包括运维权限管理、系统日志与审计、漏洞与补丁管理、事件管理、业务连续性管理等。覆盖了安全运营的事前防范，事中响应、事后审计的全生命周期。在保证常规安全运营的基础上，还特别需要关注合规、透明和隐私保护等可信要求，如监控与日志管理方面，日志保存超过 180 天满足监管合规要求，日志不保存用户个人敏感信息以符合隐私要求；漏洞和事件信息及时通知客户符合透明要求，用户可自主选择通知推送的方式满足隐私的要求。

· 唯一ID登录+多因素认证
· 账号统一集中的全流程管理

· 运维堡垒机安全审计
· 账号权限符合SOD原则



· 集中的日志管理与审计系统
· 日志保存时间不低于180天
· 满足监管部门的审查要求

· 全面事件管理规范和流程
· 7×24小时专业事件响应团队
· 安全专家资源池的优质服务

· 专职产品安全事件响应团队
· 国际应急响应论坛成员之一
· 完善的漏洞感知与收集渠道
· 及时推送漏洞规避修复方案

· 基于地区特点的风险评估
· 针对性的灾难恢复计划
· 灾复计划的演练和持续改进

5.3.3 高质量的客户服务

客户服务是云服务供应商与客户沟通的窗口和渠道，优质的服务也是可信的一种体现。除了完整可信的内部控制流程，透明完善的客户服务机制，也是建立信任的重要体现。

1) 服务协议与隐私协议

清晰透明的云用户协议、云服务等级协议（SLA）、隐私政策声明，让用户了解云服务提供商的责任、产品服务的指标以及隐私保护的信息；同时提供多种交互渠道，以便客户获取并行使数据主体的权利。

2) 客户服务与支持计划

根据不同级别的需求，建立可供选择的服务包，用户可通过在线工单、智能客服、自助服务、热线电话等多种方式获取专业的服务和帮助。服务保障能够满足如下几点：

» 7x24 小时
» 最快 10 分钟响应
» 5 天无理由退订
» 免费备案

3) 服务请求与客户授权

在处理服务请求时，所有涉及操作客户网络的活动必须事先获取客户的授权，并严格按照授权的范围、期限和用途进行操作，确保授权和操作记录可追溯。同时，通过访问控制、加密、脱敏显示等技术手段，有效保护客户隐私数据。

4) 意见反馈与建议渠道

任何用户均可通过多种渠道进行服务咨询、意见反馈和投诉建议，除基础性的站内在线客服和投诉 建议热线电话外，系统复杂的企业客户可以选择适用的支持计划，获取由 IM 企业群、技术服务经理（TAM）、服务经理等组成的专属支持。

5.4 云原生安全治理

认证机构对一个组织或业务系统进行认证，是基于已有的国际标准或行业规范，对被评估组织或业务系统的关键流程活动和实施结果进行遵从性或有效性的评估，从第三方的角度对被评估组织或业务系统的合规性给出严谨的意见。在此过程中，认证机构通常会要求获取完整的举证材料，并基于这些进行认证审核与评估。在云时代到来之前，这个过程可能持续数月甚至数年，认证机构和被评估组织可能针对一些细节进行反复确认和澄清。

云原生模式下，将业务系统搭建在公有云上，并使用公有云上的标准服务，将有可能降低认证审核的难度及复杂度，从而缩短认证周期。

5.4.1 基于云原生的安全合规体系建设

1) 制定安全合规计划

作为公有云服务提供商，在对外提供服务前，需根据开服区域和行业提出的安全要求，与认证机构、监管单位等利益相关人进行沟通，制定其安全认证计划，并年度例行针对开服区域的法律法规、安全标准及行业规范等进行持续跟踪，确保其安全认证计划的完整性及有效性。

2) 安全认证计划实施

为确保安全认证计划有效实施，企业应设置专职的安全组织。相关组织和人员应负责完善认证要求的业务流程、优化管理制度、开发 IT 工具等，并将要求赋能全员，做到所有业务流程均符合认证标准。

与传统认证不同，云上拥有较多管理类和安全类服务，能够帮助业务组织快速构建一套符合认证要求的系统。例如 IAM 服务，能实现组织、人员的身份唯一标识；DDoS 防护类服务能提供云原生的抗 DDoS 攻击能力；云监控、云审计、云日志等监控类服务能支持存储 180 天以上的审计信息；主机安全、数据库审计、漏洞扫描等安全类服务能针对虚拟机、数据库、业务系统提供资产管理和操作审计功能。云上的业务系统 Owner 可基于“责任共担模型”，并复用公有云平台侧的部分合规认证报告，大大缩短业务系统的认证周期，并简化取证流程的复杂性。

3) 云原生的安全认证管理体系

为提升效率，部分公有云服务商将常规云安全相关的标准、法规和最佳实践进行提取、合并和汇聚，将合规要求映射到不同的业务控制域，以方便云内、外部各业务团队可以像查字典一样快速地查询对应的认证要求。

CSA CCM 的16项控制领域

领域	领域名	领域	领域名
AIS	1、应用与接口安全	HRS	9、人力资源
AAC	2、审计保证与合规	IAM	10. 标识和访问管理
BCR	3、业务连续性管理与业务弹性	IVS	11、基础设施和虚拟化安全
CCC	4、变更控制和配置管理	IPY	12、互操作性和可移植性
DSI	5、数据安全与信息生命周期管理	MOS	13、移动安全
DCS	6、数据中心安全	SEF	14. 安全事件管理，电子发现和云取证
EKM	7、加密与密钥管理	STA	15. 供应链管理，透明度和问责制
GRM	8、治理和风险管理	TVM	16、威胁与漏洞管理

CSA CCM v3.0.1 合规性说明 (来源：cloudsecurityalliance.org)

说明：CSA CCM 是由国际领先的云安全组织——云安全联盟发布的云上安全控制矩阵。云安全联盟在 2009 年成立，致力于国际云计算安全的全面发展。目前云安全联盟已协助美国、 欧盟、日本、澳大利亚、新加坡等多国政府开展国家网络安全战略、国家身份战略、国家云计算战略、国家云安全标准、政府云安全框架、安全技术研究等工作。

云服务商可以将上述合规要求内嵌到各个云服务中，形成基于云原生的安全遵从最佳实践，做到将云上资源的合规检查例行化、可视化，帮助企业的云上业务实现高效运营、持续合规。

第六章
云原生产业生态

云原生产业生态逐渐完善，产业链条趋于精细，分工和协作成为主流。云原生的理念不断丰富、落地、实践，进入了快速发展期，Gartner 预测，到 2024 年发达国家中有 75% 的大型企业将在业务应用中部署容器[1]。根据《中国云原生用户调查报告（2020）》数据显示，43.9%[2] 的用户已在生产环境中采纳容器技术，超过七成的用户已经或计划使用微服务架构进行业务开发部署。

[1] 数据来源：Gartner《预测分析：全球容器管理（软件和服务）》

[2] 数据来源：中国信息通信研究院《中国云原生用户调查报告 2020》

用户对云原生技术的认知和使用进入新阶段，云原生化需求也从行业头部企业逐步下沉到中小规模企业，从领先企业尝鲜变为主流企业必备，云原生已成为新常态。持续丰富的用户需求和不断细化的技术能力，衍生了不同的产业赛道，吸引越来越多的技术提供商涌入，诞生实力强劲的细分领域独角兽，行业用户以及上下游厂商逐步开展深层次的分工协作，衍生出越来越多的互促式合作伙伴和精细化合作方案，出现越来越多的细分市场，共同推动了云原生产业生态的持续完善，带动云原生产业链条全线联动、共同繁荣。

企业用户越来越专注于自身业务的价值挖掘。不同的企业在基础设施和应用架构方面都有自身的个性化差异、任务复杂性等挑战。中国率先控制住疫情为国内企业在数字化转型方面争取到窗口期，数字化转型在疫情和后疫情时期越发重要，企业上云已经成为一种必然趋势。疫情之下，虽然各行各业都受到了不同程度的影响，但那些数字化能力健全的企业抵御风险的能力更强。

技术服务商从寡头垄断走向丰富多元，细分领域的专业服务商爆发式增长。相较于早年的云原生技术生态主要集中在容器、微服务、DevOps 等技术领域，现如今的技术生态已扩展至底层技术、编排及管理、安全技术、监测分析以及场景化应用等众多分支，形成了支撑应用云原生化构建的全生命周期技术链。同时，云原生细分领域也趋于多元化发展，如在容器技术领域，从 Docker 这种通用场景的容器技术逐渐演进出安全容器、边缘容器、Serverless 容器、裸金属容器等多种技术形态。云原生技术生态的多维度发展为具备局部优势的中小型技术服务商提供了发展空间，在诸如云原生网络、云原生安全等细分领域，涌现出众多初创公司，依托对细分领域需求和痛点的多年探索，致力于解决云原生关键技术问题，赋能云原生技术生态的繁荣发展，填补了生态空白。

生态伙伴是联接产业供需的重要纽带，咨询服务成为技术落地的关键一环。最终用户的 IT 应用开发形式（自研或和第三方技术厂商合作）决定云原生生态的格局。除互联网企业外，对于更多中大型企业来说，经过充分调研会发现云原生技术难度和自研成本很高，大部分企业需要和专业技术厂商合作，共同落地云原生技术，打造技术中台。专业的技术厂商能够提供完善的咨询服务、解决方案和方法论。同时云原生技术的部署也一定程度上伴随着对企业 IT 文化、流程的变革，也需要技术厂商和企业的配合。传统软件服务体系，纷纷与云原生技术对齐，构成云原生生态合作，其中典型代表有：

独立软件开发商

长期聚焦某些行业或者垂直领域，在技术、产品和客户方面都有深厚积累的企业，有能力依托云原生核心技术和平台优势，开发可规模推广的行业产品或解决方案。独立软件开发商深耕行业，持续摸索行业或垂直领域的特性，致力于开发普适性较强的通用产品，直击行业痛点。企业可直接复用独立软件开发商提供的可靠产品，也可根据自身需求进行微量改造或功能扩展，即开即用的产品优势显著加速了企业需求的落地，避免重复造轮子，极大提高了企业云原生化转型的效率。

软件集成商

具备系统集成资质，有一定的客户基础和方案整合能力，能够为企业提供优质的云原生解决方案和服务。软件集成商依托自身在云原生领域的经验积累，可灵活地根据客户业务需求，提供定制化个性化的解决方案，协助企业实现从需求到方案、从方案到架构、从架构到落地的云原生改造全链路闭环。软件集成商为企业的云原生改造需求提供了完备的方法论与成熟的配套服务，有助于提高企业信息化智能化水平，强化创新竞争力。

咨询与交付服务商

企业在使用云原生技术进行业务系统架构设计、开发和上线过程中，面临着严苛的困难和挑战。企业缺少实际业务场景实践经验，应用云原生化改造路径不清晰、技术方案可行性难预估、价值收益难衡量等现实问题成为云原生技术实践的最大绊脚石。同时高可靠、高扩展、高性能和高安全的云原生技术架构的实现也对企业 IT 技术人员的专业知识储备和实践经验提出严苛要求，专业咨询服务成为企业云原生技术落地的重要“助推器”。

围绕企业云原生落地的困难和挑战，云原生咨询与交付服务商应具备下述方面的能力：

业务场景分析

从企业业务系统调研出发，对业务系统进行场景评估分析，结合实践经验给予企业云原生业务改造建议，如：业务哪些业务适合采用容器作为基础设施、哪些业务的数据适配迁移到云原生数据平台进行管理，企业当前阶段哪些业务可以优先进行改造，如何分阶段进行上线，以及组织上是否需要进行调整，以促进整个业务架构全面云原生化升级。

全流程的云原生应用架构升级设计方案

帮助企业构建标准化、高效能、可演进和安全的云原生系统，如：是否采用多云、混合云架构，采用传统 SDK 方式或是 ServiceMesh 方式进行服务治理架构的升级，企业的大数据、AI 等系统是否与业务生产系统共架构统一部署等。

面向企业开发运维相关人员技术知识赋能

利用全面的课程体系和以练带学的方式，快速提升企业人员的云原生技能水平，加速落地云原生的进程，包括容器、微服务、数据库、AI 等方面的专业知识，以及基于云原生的业务架构，如何更高效的开发、运营、运维等。

第七章
云原生未来展望

以容器、Kubernetes、微服务等为代表的云原生技术，经过近几年的蓬勃发展，在弹性扩展、降低使用成本、技术成熟度等方面均取得了长足发展，成为赋能业务创新的重要推动力，其应用场景也由一开始的以互联网企业为主，逐步扩大到金融、政府、工业制造等传统行业，并已经逐步深入到企业的核心业务，给企业的数字化转型带来了极大的价值。

7.1 趋势一：云原生能力与分布式云有机协同，让云无处不在

业务上云和云原生改造已是大势所趋，但对于企业客户而言，出于对数据产权、安全合规、隐私保护、应用时延、成本优化、组织治理结构等的考量，会采用分布式云的部署架构，将全栈云原生能力延伸到更靠近企业业务所需的位置（如现场边缘、近场边缘、混合云等），来满足企业的业务需求，以公有云为中心的分布式云部署架构将成为企业上云的新常态。

7.2 趋势二：基础设施资源与应用需要相互感知、高效协同

现有的云原生基础设施中，云原生技术栈各部件之间以离散的状态叠加部署在基础设施之上，无法基于应用的负载状态来提供高效、动态的资源供给，尤其在高密部署场景下，会带来较大的资源损耗，限制了基础设施的最大价值发挥。未来一方面需要突破架构以及功能上的限制，发挥软硬协同的优势来持续提升资源利用率；同时，基础设施资源需要与应用状态相互感知，能够根据应用需求来进行资源的动态调度与编排，以及构建边云协同调度的能力来支持分布式云部署形态下的资源管理，来充分发挥基础设施的最大价值。

7.3 趋势三：云原生技术逐步上移到应用层，效率、安全成为企业的核心关注

未来，以应用为视角、标准化、最佳实践 Built-In 的应用平台将成为企业应用全面上云的首选。DevOps 会在 Dev 右移和 Ops 左移的过程中成为最佳应用开发模式，基于云原生场景的新一代云原生开发运维平台也会涌现（如：基于应用模型一键 CICD 研发基础设施随拉随启随释放，Cloud-Native IDE），云原生技术会带来高度自动化和极致的并发协同，未来企业内百万级应用开发流水线并行的场景将成为常态。

Serverless 作为下一代云计算范式，基于 Serverless 的应用生命周期将出现重大的改变，整个过程将完全无须调度和管理任何的服务器，并且应用天生具备高可用高弹性。企业内异构的微服务技术栈还长期存在，微服务双模治理会成为企业的主要治理模式。声明式定义的应用模型（Application Model）是云原生应用的关键技术突破，帮助企业实现高度的应用自动化和并发协同。

7.4 趋势四：AI 与数据、应用深度融合，让智能无所不及

随着企业的数据和应用转移到云上，数据的采集、传输、存储、标注、分析、应用等数据全生命周期管理的能力将基于云来构建。降低数据治理的成本、释放数据最大价值是企业客户的强烈诉求。基于云原生的技术构建一站式融合数据分析平台，打破数据边界，减少数据搬迁，实现高效的跨源跨域协同分析能力将是重点发展方向。

容器化部署具有资源高效、资源隔离、弹性扩展、环境标准化、简化版本控制、跨平台性等特点，并结合存算分离、分布式部署等云原生特征，将成为云原生数据服务部署的发展趋势。

随着云上 AI 技术和生态的成熟，云平台将持续丰富算法库，提供自动学习、自动超参搜索、“预置”算法、预训练模型等来降低 AI 开发门槛，结合云上超大规模的算力和海量数据，将支撑使企业更好的挖掘数据潜力，处理复杂问题，支撑企业做好业务决策。

7.5 趋势五：安全服务自身需要云原生化，来保障云原生环境的安全运行

面向云原生环境的安全诉求，其目标是防护云原生环境中的容器、编排系统和微服务等的安全；现阶段针对云原生环境的安全，如镜像扫描、主机安全防护、容器平台安全防护、边界安全工具目前主要是采取传统模式部署，未来需要基于云原生技术来重构安全服务，实现弹性敏捷、轻量级、可编排的安全服务能力等来保障云原生环境的安全运行。

第八章
附录：云原生 2.0 行业实践

感谢以下企业的云原生 2.0 行业实践分享（排名不分先后）：

陕西财政、中国一汽、中国工商银行、深圳证券交易所、永安保险、爱学习教育集团、亚洲渔港

8.1 陕西财政轻装上云“放”出效率“管”出规范

在经济高速的发展下，为了缓解陕西省各部门财政业务递增的压力，陕西省财政厅（以下简称陕财）率先提出了构建“陕西财政云”的计划。在 2018 年，陕西省财政厅提出要加快财政信息系统一体化，计划用 2 到 3 年时间基本建成“陕西财政云”。

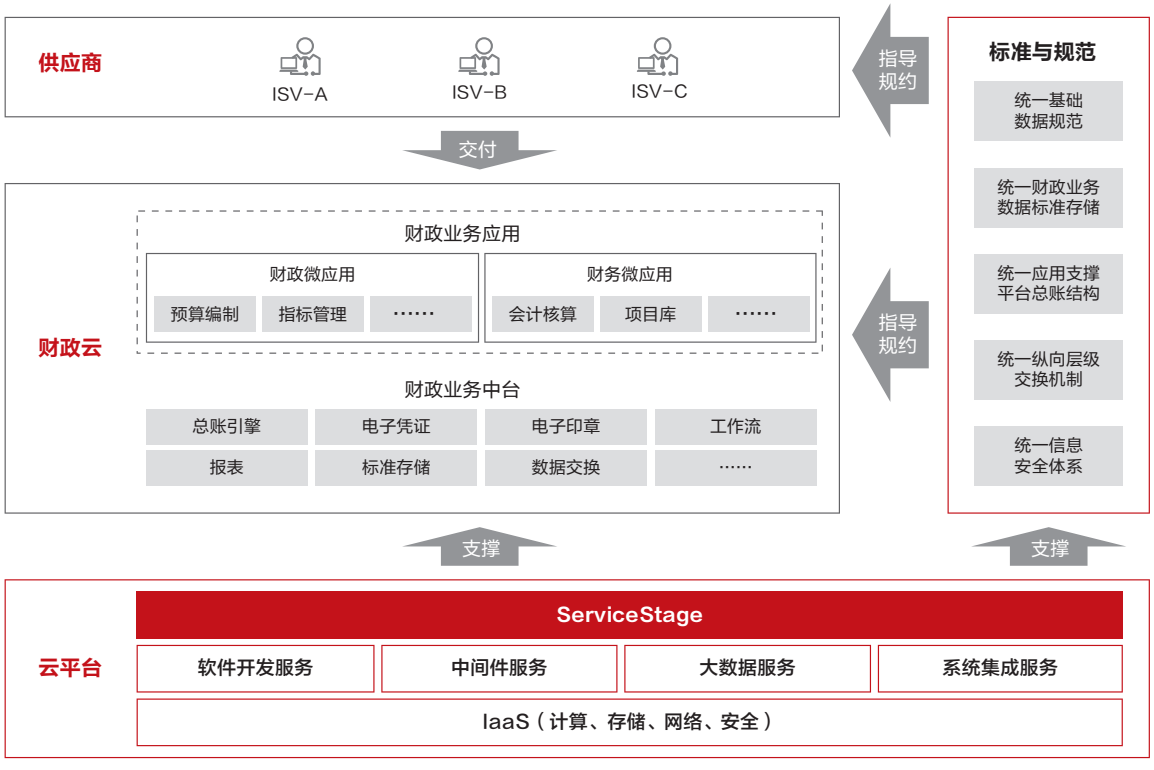
系统分散的烟囱式 IT 系统阻碍了业务系统一体化

分散的烟囱式 IT 系统几乎是所有政务部门上云的头号痛点，由于每个系统是由不同的 ISV（Independent Software Vendors）独立开发，导致各地政务系统资源烟囱直立一般基本处于“信息孤岛”状态，无法集中管控。

因此，政务系统上云的关键是要先从架构上与业务平台进行设计，再从开发框架上调整 ISV 的协作模式，合理均衡资源，最后从本质出发解决系统流程上的难题。

华为云解决方案五部曲：四个标准化，一个大平台

华为云咨询团队针对陕财上云情况提出了“一个大平台，四个标准化”的架构建议，提供了一站式微服务云应用平台。



» 基础设施标准化：为“财政云”提供全套的标准化研发环境和工具，业务按需弹性，支持域名管理、SSL 证书管理、分布式会话、缓存加速、数据库连接，统一的标准指导着应用开发商 ISV，应用开发效率提高 60%-80%，财政新应用上线由原来的半年提升至 60 天以内。

» 应用架构标准化：应用全微服务化，接口标准由财政厅统一管控，ISV 只需聚焦微服务交付，可随时替换，整体进度可控可管。

» 数据集成标准化：统一业务模型和数据集成标准， 46 个系统可实现无缝对接，财政数据统一呈现，业务全盘管控。

» 交付过程标准化：标准化研发环境和工具，为“财政云”提供开发框架和运行环境，支持 Web 应用、微服务应用、移动应用和 AI 应用，并与华为云基础服务无缝集成。开发者只需聚焦微服务交付，无需担心部署运维以及环境问题。

“财政云”轻松实现四个一体化目标，构建友好生态环境

根据陕财实际业务情况，通过华为云微服务能力框架概要设计，累计设计微服务 40+ 个，包括 SaaS 层前台后端服务 23 个。

经过微服务改造后的陕西财政云系统有着更加开放的生态：

» 解耦的微应用和微服务，帮助陕财与 ISV 协同更加顺畅，财政应用生态更开放。

» 华为云 ServiceStage 一站式微服务应用平台全生命周期管理和微服务治理能力，帮助财政云构建可靠稳定的分布式服务。

改造后，“财政云”充分享受到了云原生 2.0 时代的技术红利:

» 业务全面监控：陕财工作人员通过一个门户完成所有业务，各业务衔接顺畅，财政部门内部、财政与预算单位之间、上下级财政部门之间信息横向到边、纵向到底全联通，实现财政业务智能化管理。

» 数据统一呈现：以应用为支撑，统一管控，形成财政内生和外部数据资源池，所有数据上“云”，实现数据资源一体化管理。

» 应用快速上线：快速响应财政业务改革发展对业务应用系统快速升级变更的要求，财政新应用从月级上线提升至周级，实现真正领先的“财政云”。

华为云帮助陕财顺利改装上云，“财政云”的完成也促进了政府各部门、泛政府以及社会各企业的数字化转型。云原生 2.0 时代，政务部门、企业数字化转型加速，合作伙伴以及技术平台的选择至关重要，用户需求、市场竞争等驱动着云技术的迅猛发展，云技术也将耕耘更为开放的生态沃土反馈给各企业、各个用户。

8.2 AI 释放知识力量，中国一汽“维修智库”诞生记

2018 年，是汽车产业的一个分水岭。这一年，市场开始告别爆发式的增长，进入从设计、生产到销售、售后服务的全产业链竞争时代。一波强过一波的数字化浪潮，给汽车企业造成了巨大的冲击。与此同时，这场风潮也加速了中国一汽技术创新和自主品牌建设的步伐。同样在这一年，中国一汽发布新红旗品牌战略，开启了复兴红旗的伟大征程。

变革的开始：打通数据

对于老一辈的中国人来说，与其将“红旗”和“解放”说成是一个个品牌，倒不如说成是一种种情怀。作为“共和国长子”，1956 年 7 月，中国一汽造出了新中国第一批汽车；1958 年 9 月，无畏的一汽人硬是用手工凿出了用于国庆检阅的第一辆红旗检阅车，大长了国人的志气。

即使进入被称为是中国汽车业分水岭的 2018 年，中国一汽依然保持了上升的势头，销量一路高歌猛进。2020 年，受新冠肺炎疫情影响，汽车市场受到不小的冲击，但一汽各品牌却逆势上扬。红旗 1-8 月同比增长 108%，超过 2019 年全年销量，超额完成年销售 20 万辆的目标。

然而中国一汽也同样意识到，在新科技革命的推动下，汽车产业正在经历百年未有之大变局，产品形态和产业生态发生重大变化，数字化成为汽车产业转型升级和高质量发展的核心驱动。基于过往的实践，2020 年 4 月，中国一汽发布了数字化战略，以数字驱动美妙出行为愿景，围绕“业务赋能、产品智能、生态智慧、数据增值”，以中台为核心、数据为引擎，实现核心业务的创新化、数字化、价值化。

在本次数字化转型之战中，重要突破点之一就是上云。中国一汽将车联网业务、数字化营销业务、出行业务等都放到了华为云平台上。中国一汽的上云之路，为日后知识计算平台的应用、打造“智慧通才型”员工，打下了坚实的基础。

“维修智库”诞生记

数字化转型不仅仅是产品生态和运营模式的转型，更重要是员工能力的转型升级。在汽车行业，智能网联、新能源等新业务方向也对员工能力提出了新的要求。

以销售环节为例，以往，当新车上市时，销售人员首先需要学习新车知识，如果遇到客户打来电话咨询疑难问题，销售人员会先在脑海中回忆历史培训，甚至要搜索培训教程；一旦教程里面没有写，就要电话咨询分散在不同部门的专家。整个知识获取的过程存在繁琐、分散、缓慢、复杂等诸多不便。当新型汽车不断推出时，这个问题就被不断地放大。而同样的情况，还出现在设计、生产、维修等多个环节。

对此，中国一汽表示：“如何快速提升员工能力是车企转型面临的重大挑战之一。我们希望有一个平台，能够基于业务场景，将知识便捷、数字化的方式呈现在眼前，以便快速解决问题。”

简单来说，是否能有一个让员工“问不倒”的智慧通才型专家？通过 AI 等技术汇集老专家积累的经验，更快地传授给员工？

一汽的知识计算平台以数据中台和“红旗智云”混合云平台为底座，引入华为云知识计算解决方案、薄言轻语虚拟助手平台。平台提供从知识获取、知识沉淀、知识应用的一站式知识服务闭环，将专业知识结构化、数据化，并基于专业性、人员角色，将知识关系化，实现知识标准化、共享化和智能化；在知识应用方面，实现从过去的“人找知识”，变为现在的“知识找人”，助力员工快速成长为领域专家，推动企业的知识化转型。

借助这个平台，中国一汽设计了一款“维修智库”手机应用，解决车辆维修过程中，新技师经验不足、故障分析效率低、维修周期长、用户体验差等问题。通过提取维修手册、维修记录、维修案例和专家经验，构建售后维修知识图谱，提供“故障问诊”和“知识搜索”功能。维修技师使用这个 APP，通过语音交互描述故障现象，即可智能推荐维修方案，查看相关零件的拆装图纸等关键信息。

基于红旗 4S 店员工的实践，“一汽知识计算平台”很快交出了自己的第一份成绩单：应用上线后，一次性修复率提升 4%，用户维修等待时间平均下降 23%；提升用户体验的同时，厂家支持介入率降低 30%，技师培养周期缩短 30%，降本增效成果显著。

接下来，中国一汽将面向汽车产业全价值链，不断地丰富知识计算平台的应用场景。比如，将中国一汽在售后、生产、路测领域的质量知识赋能到产品设计，用以提升研发质量，提高研发效率。比如在制造领域将各种复杂设备进行数字化管理，缩短技师的培养周期。

当各个环节的智慧通才型员工群英荟萃之时，“人才”就实实在在地转化成了中国一汽的核心竞争力之一。

“行业知识 +AI”助力汽车行业升级

众多类似汽车行业的技术密集型产业，不管是在研发、制造、营销、运营还是售后环节，都需要经验丰富的技术专家支撑。在行业中，原本很多知识都分散在各个地方，比如文档里、工作手册中，甚至是专家的脑袋里，而企业无法将其整合。这就导致很多知识无法发挥其最大的效能，企业更无法进一步提高精度、降低成本。

所以行业、企业升级过程中最关键的一环，就是找到一个平台，能够将知识系统呈现在员工眼前，通过自然语言交互即可准确理解问询意图，锁定问题。并能够将专家的经验与问题现象进行关联，让新员工也可以解决复杂问题，让普通人快速成长为专家。

行业知识与 AI 相结合，走进企业的核心业务，这对于整个行业、产业来讲，意味着全面跃迁的机遇。

这正是华为云知识计算服务的历史使命：基于知识图谱、自然语言处理、深度学习、迁移学习、联邦学习等 AI 技术，与行业知识结合，生成高效 AI 模型，使机器控制更精准，降低生产成本，提升分析和决策水平，缩短人员培养周期，实现经验、知识的快速沉淀与传承。

8.3 中国工商银行打造云原生金融数据湖

工商银行作为数字金融的领导者，践行“科技引领，创新赋能”的发展理念，持续提升工行金融服务实体经济的能力。工商银行和华为开展联创工作，引入了华为云 FusionInsight 智能数据湖，搭建了自主可靠的大数据平台，解决了大数据全场景生态化应用的存储、算力和算法挑战，支撑了工商银行企业级数据湖、数据仓库、集团信息库的建设，数据智能服务由事后快速演进到事前、事中的阶段。

传统大数据存储计算耦合，TCO 高

工行之前使用传统大数据的三副本存储性价比低，往往 10PB 的存储空间，有效容量仅 3PB；同时存在存储、计算等资源不均衡，往往存储利用率超过 70%，但 CPU 利用率不足 50%，扩容时需要计算、存储资源一起扩容，存在资源浪费现象。

湖仓数据割裂，产生数据孤岛，协同分析难

工行内部使用 SAS 等工具通过 HiveQL 访问数据湖数据性能差，平均响应时间 5 分钟 ~2 小时，并发能力不足（<10 并发）。湖仓数据割裂，关联分析需要通过繁杂的 ETL 任务，将数据加工后加载到 OLAP 集市，数据链路长，分析效率和开发效率都很低。

平台升级需中断，缺少平滑演进能力

工行大数据平台的 Hadoop 批量集群已超过 1000 节点，日均处理作业 10 万 +，数据存储数十 PB，承载了全行重点批量作业，其中包括反欺诈、精准营销等多个重要业务场景，服务连续性需求较高。而大数据技术迭代快，传统升级方式需断电、重启等操作，升级操作复杂，影响现网业务运行，且大集群升级耗时长，突发故障易中断升级动作。

华为云 FusionInsight MRS 云原生数据湖助力构筑金融大数据平台

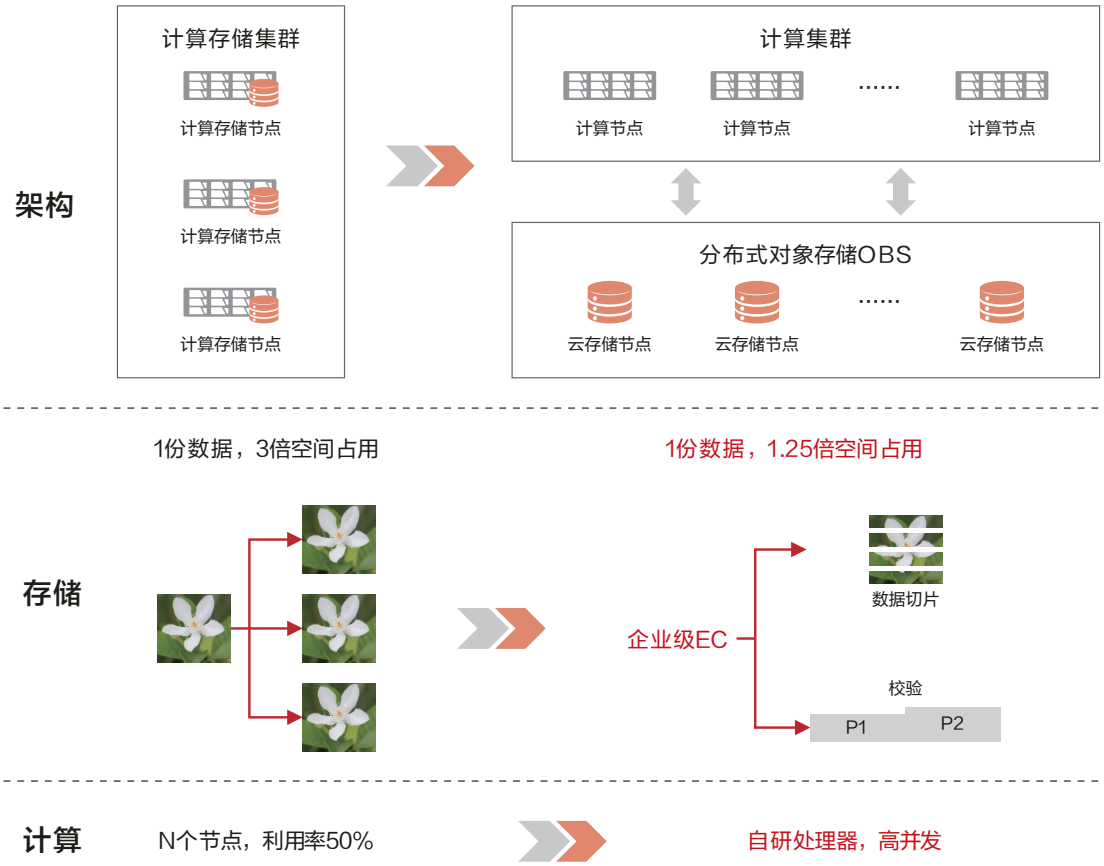
工行采用了华为云 FusionInsight MRS 大数据存算分离方案，实现了大数据平台与 OBS 对象存储服务的对接，将原有的 HDFS 数据无缝迁移到 OBS 上。在保证性能的前提下，实现了计算与存储独立按需扩容，轻松应对业务浪涌，提升资源整体利用率。华为独有的 Flex-EC 技术将副本率降低至 1:1.25，存储资源优化提升 2.4 倍。

工行大数据平台承载了总行和 200+ 分支行的数据，为了解决数据分布散、协同难等问题，降低金融分析师的用数难度，工行采用了华为云 FusionInsight MRS 的 HetuEngine 服务，通过 HetuEngine 引擎实现跨地市的协同计算，一个 SQL 连接就可以访问全部数据源，直接做碰撞分析，实现湖仓互联互通协同分析，避免不必要的 ETL 流程，减少数据搬迁。

大数据技术快速发展，为满足业务变化发展需求，工行采用了华为云 FusionInsight MRS 滚动升级方案，借助于 Hadoop 核心组件的高可用机制， MRS 按照依赖层次，多层次并行，在不影响集群整体业务的情况下，一次升级 / 重启少量节点，依据组件和实例的依赖关系，自动编排升级批次。升级过程中，隔离故障节点，待升级完成后，再进行故障处理。循环滚动，直至集群所有节点升级到新版本。

MRS 存算分离方案，TCO 降低 60%

计算 / 存储解绑定，精准投资，灵活扩展，计算资源利用率提升 30%+，存储资源利用率提升 100%+，TCO 降低 60%。统一数据存储底座，多个计算集群共享同一份数据，降低业务规划、扩容、维护难度，提供百亿文件 EB 级扩展能力。

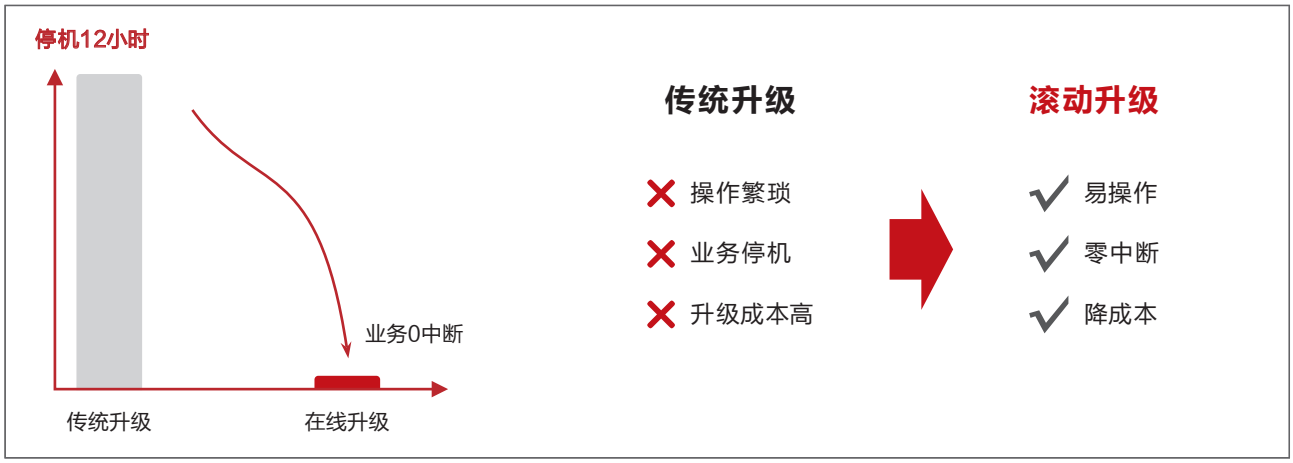


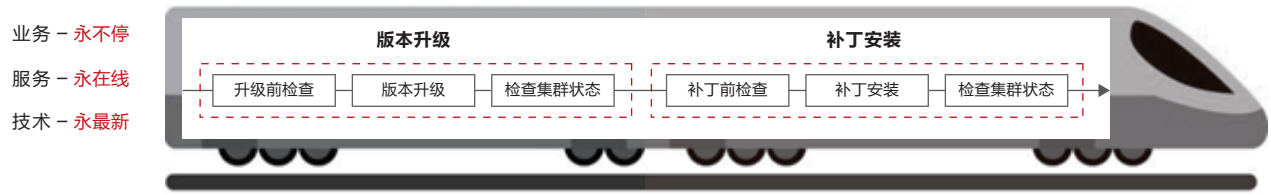
HetuEngine 跨仓协同

使用华为云自研 HetuEngine，采用算子下推，降低资源消耗，仅原 1/5 的硬件资源即可支持 45+ 并发，跨湖协同分析性能提升 50 倍，兼容 99% Hive 语法。

MRS 滚动升级实现架构平滑演进，业务 0 中断

通过华为云 FusionInsight 滚动升级能力，实现大集群分批次滚动升级，业务 0 中断；故障节点隔离功能确保升级动作的稳定运行，实现 7*24 小时不间断服务；1000+ 精细化运维指标及可视化操作简化运维，实现一个架构持续演进。





未来为满足工行业务高速发展需求，工行金融数据湖规模将达 3000+ 节点，满足工商银行批处理、流处理、交互式分析等大数据应用场景，进一步提升数据洞察能力和基于场景的数据挖掘能力，充分释放大数据作为基础型战略资源的核心价值。

8.4 云原生基础设施加速深交所数字化转型

深圳证券交易所（以下简称“深交所”）成立于 1990 年，是经国务院批准设立的全国性证券交易场所。深交所在证券市场中履行市场组织、市场监管和市场服务等职责。经过多年的建设，目前深交所建成近 300 个系统，根据类型可划分为三大类：核心交易系统、业务管理系统、市场实时监察和信息服务系统，经过多年发展，深交所技术架构也在持续的创新和转型，转型的动力主要来自于三大驱动：一是市场在产品与制度创新、产品快速迭代等方面给技术带来的需求和压力，二是行业监管和系统安全的需求也要求系统技术架构向更稳定、更可靠、可安全方向进行转型，三是以云计算、大数据、人工智能为代表的新技术发展也要求技术架构不断进行更新。

深交所首先构建了基于容器的高效云原生基础设施，为应用提供可定制的模块化资源，同时以 API 形式开放基础设施的各项能力，通过一个统一的平台来满足不同应用在性能、成本、可靠性等关键指标方面的差异化需求，提升了基础设施的自动化运维程度以及资源使用率。深交所云原生基础资源设施主要基于华为云 CCE 云容器引擎构建，CCE 在原生 K8S 基础上做了优化，与原生 K8S 相比，资源损耗更小，调度效率更高；在容器网络方面，深交所采用 3 层网络 BGP 路由方案，以满足安全隔离要求，同时集成华为 SDN，构建保障性更高、性能更好的网络资源平台；在存储方面，容器存储支持块存储、对象存储、文件存储等不同类型，通过基础设施平台统一构建融合存储平台，满足应用的需求。该设计大幅提升了基础设施的性能和利用率、降低了成本，提升了用户的体验。

第二个转变是建立统一的计算、存储资源池，通过容器引擎统一管理，可进行更细粒度资源配额调配，比如可实现 CPU、内存、GPU 等计算资源的动态调配，资源利用率和分配效率得到显著提高，并实现了算力的灵活调度和弹性扩容。

云原生带来的第三个转变是以应用为中心再升级应用架构，本质是云原生基础设施带来了应用架构的模式转变。传统模式是以基础设施为主体，根据基础设施容量分配额定资源去部署有限应用运行，而现在以应用为中心定义基础设施，根据应用需求分配基础设施资源，例如计算资源、网络资源、存储资源等。同时应用架构做升级成更为轻量无状态的微服务，这样不仅可保证应用弹性伸缩能力及快速部署、快速迭代，结合微服务的全方位治理能力，实现了灰度发布、多版本并行、链路跟踪、限流熔断、自动化测试等能力。

目前深交所各类应用已陆续基于上述云原生架构进行升级改造，以新 OA 系统为例：最初以烟囱模式开发，各个子系统之间关联性较低，随后进行了服务化改造，将业务逻辑以服务方式提供，形成一定规模的复用；再后升级成为微服务架构，并运行在云原生基础设施上，可以实现 OA 系统的高效部署和弹性伸缩，并具备灰度发布、熔断限流、链路监控等能力，从而提升了 OA 系统的交付效率。

8.5 云原生数据库助力永安保险实现“云端保险”

随着云 +5G+AI+IoT 新一代信息技术的发展，数字化转型已经成为数字中国、智慧社会建设的重要动能。自 2019 年《金融科技 (FinTech) 发展规划 (2019-2021 年)》和 2020 年《统筹监管金融基础设施工作方案》两部重大规划指导文件发布以来，金融科技成为国家层面重点统筹发展的领域之一，金融基础设施的建设愈发重要。

得益于数字技术和国家政策的助力，保险行业也在数字化转型中表现出强大的张力。永安保险作为全国财产险排名前列的保险公司，积极拥抱云计算、大数据、移动互联网技术、云数据库等，积极为未来打造高可靠、高安全、高扩展、及时响应业务需求的基础设施。此次携手华为云进行云上业务改造，更是大幅提升了销售、承保、理赔等环节的效率，实现从内部运营到外部销售全业务链条的云化。

那么，永安保险是如何实现“云端保险”服务的呢？华为云又是如何帮助永安保险安心上云呢？

打破痛点，精准上云

永安保险正在积极探索和持续完善线上渠道，并与互联网等多渠道构建合作生态，实现线上线下、生态多渠道的融合，以及简化运营、降低成本并保证一致的客户体验，但这都迫切需要永安保险创新 IT 架构，构筑强大稳健高效的数字化基础平台。因此，永安保险现有的 IT 架构需要解决如下问题：

» 高性能需求：永安保险业务发展迅速，线下数据库数据量已达到几十 TB，对数据库的扩展性、性能等要求极高。

» 满足高安全与可靠性：满足数据安全与灾备监管要求，线上渠道需要 7*24 小时为社会和投保人提供不间断服务。

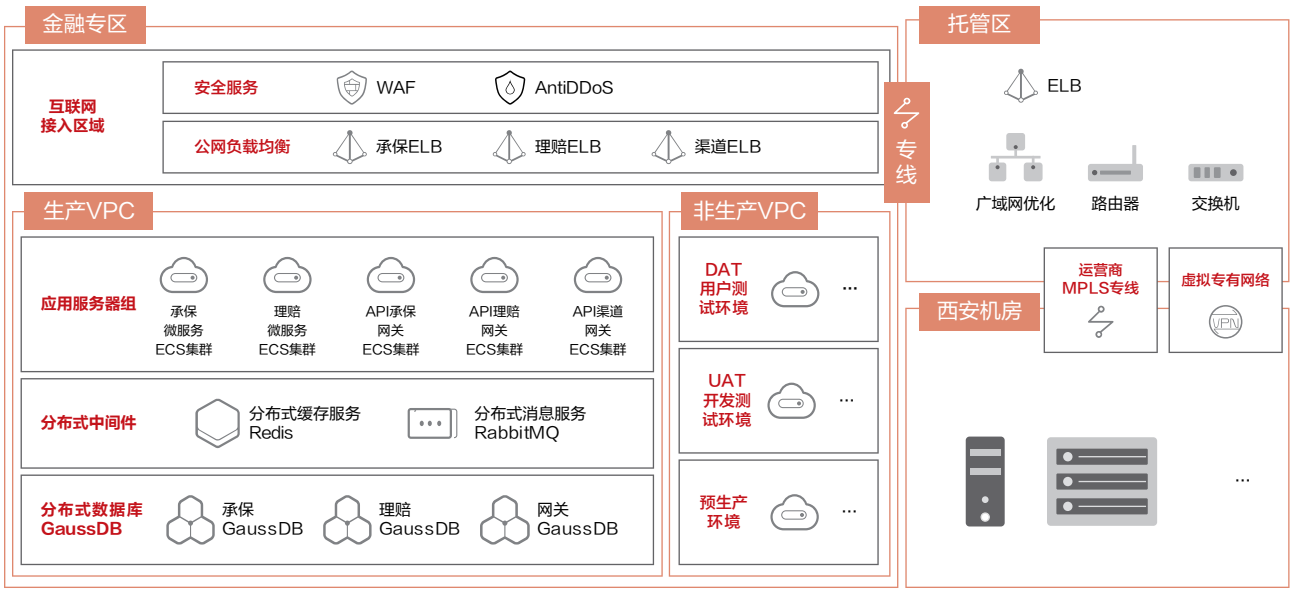
» 业务敏捷创新与上线：云化开放架构和分布式改造是大势所趋，基于业务转型需求，永安保险需要重新部署金融云平台。

» 降低运营成本：封闭商业数据库的运维成本高昂，数据同步操作频繁且只能手工操作，工作量大且繁琐，投入成本高。

» 符合政策监管：IT 基础设施要求信创，主流商业数据库需要使用国产数据库替代。

基于保险业务的安全诉求、多元融合以及金融监管的要求，华为云数据库团队对永安业务系统进行了精准评估与分析，快速制定出一套高安全、高可靠、高可用、高性能的数据库迁移方案，实现了主流商业数据库的安全切换，大幅提升了业务运转效率。

重构核心金融云平台，创新“云端保险”服务



永安保险意健险上云方案架构图

此次迁移，华为云重新构建了分布式金融云平台和数据库，成功助力永安保险将意外险和健康险两套业务系统迁移上云，实现 RPO=0，RTO 秒级。

全新分布式架构部署，数据上云更安全稳定

华为云根据永安意外险和健康险两个业务系统的特点及要求，聚焦新业务服务架构优化调整，基于华为云服务一体化、高可靠、高可用的分布式金融云平台架构部署，重构核心系统并实现主流商业数据库切换。华为云金融云平台有效应对流量高峰场景下可靠性和性能的问题，确保系统在高访问场景下数据不丢失，同时降低了运维压力，实现 RPO=0、RTO 秒级，不仅满足了金融监管要求，而且整体资源投入节省了 25%，为未来数字化转型打下了坚实的云上核心分布式架构和数据底座基础。

超高性能，海量访问无压力

永安保险的保单数据量巨大，预计几年内会达到几十 TB，会对数据库造成很高的并发压力，对性能要求极高。永安保险通过部署华为云 GaussDB(for MySQL) 数据库，实现了 7 倍性能的提升，海量访问无压力。而且 GaussDB(for MySQL) 支持 1 写 15 读， 128TB 海量数据存储，分钟级扩容，可以承受线上大型保险代理平台带来的巨大压力，高并发场景下仍可以保持超高性能，极大满足了永安保险对高性能数据库的诉求。

业务不中断，数据平滑迁移

针对永安保险复杂的数据迁移需求，华为云数据复制服务 DRS 通过单库拆分迁移，为系统后台提供分库分表和微服务的能力，满足客户特殊需求。同时提供数据对比功能，快速实现行数对比，给客户直观展示迁移过程中源库和目标库的数据一致性情况，确保数据 0 丢失。此外，在异构数据库迁移方面，华为云数据库提供了完整的改造迁移方案，包含对象改造、SQL 优化、割接方案等，确保业务平稳割接，整个过程业务无须停机，做到了对客户最大程度的平滑无感迁移，让客户在迁移时对业务安心、使用省心、割接有信心。

经过此次对主流商业数据库的上云切换，永安保险的业务系统实现了较大幅度的效率提升，业务可靠性和安全性得到极大增强，企业资源投入成本降低 25%。未来华为云会持续助力永安保险进一步业务创新，提升客户服务能力、承保和理赔创新服务能力，为保险业务提供更多可能性。

8.6 爱学习构建超低时延线上互动课堂，推动教育 OMO 升级

爱学习教育集团是在线教育 ToB 赛道的领头羊，目前，爱学习合作机构已覆盖全国 31 个省市自治区的 1600 多个县市，拥有 20000 余家合作机构，累计服务学员超 2500 万人次。

随着云、5G、AI、实时音视频等技术与教育融合带来了新的发展机遇，爱学习在教育 OMO 模式上持续创新，打造了包含在线课件等在内的具有丰富课堂互动体验的在线课堂，帮助 1 万多家教育机构顺利实现了在线一对一、在线小班和在线双师等形式的教学。

当前线上教学普遍存在的问题和困难：

» 老师迫切需要高质量、稳定的推流，以能跟学生更好地互动；学生所处的网络环境多样，但都希望能够享受到高清流畅的学习体验。

» 不同业务种类各有痛点，比如小班课互动多，但最多只支持 16 人连麦，超出人数只能另开新班，或者老师轮流点名，制约了老师教学的发挥；大班直播课时延高达 3-5 秒、互动少，影响学生课堂归属感。

» CDN 和 RTC 合流后，旁路直播引入也存在延时，学生在观看和互动之间来回切换，时差明显，学习体验大打折扣。

» 在开发上，互动直播和传统直播是两套 SDK，对接困难、成本高；在运维上，CDN、RTC 两套系统问题定界难，修复周期长。

华为云 RTC 实时音视频服务打造极致音视频体验

爱学习机构遍布全国，需要构建一个覆盖好、低延迟、弱网抗丢包的音视频网络，以支持万人在线、千人互动、自由连麦。

华为云 RTC 实时音视频服务帮助爱学习快速构建了全场景、全互动、全实时的视频能力，充分发挥了其在视频业务领域长期积累的技术优势：

» 超低时延：音视频端到端延迟 <200ms，操作指令延迟 <30ms。

» 一网原生：1 套网络、1 套技术架构支持直播 / 连麦 / 交互 / 会议全场景，新场景 VR/AR/ 全息等无需切换。

» 极致体验：50% 视频抗丢包，80% 音频抗丢包。

» 极智编码：支持最高 4K 的视频分辨率，通过先进的编码技术将同等质量视频码率降低 30%。

» 千人互动：单房间最高支持千路用户连麦互动，单房间自由分组，分组间自由互动。

» 海量覆盖：全网 2500+ 节点，全运营商覆盖，确保用户就近接入。

基于华为云 RTC，爱学习为用户提供更好的在线学习体验

» 线下授课场景在线上高质量还原，学生在观看与互动之间自由无感知切换，课堂互动更丰富、上课更积极，老师更容易把握学情，教学质量得到大幅提升。

» 老师教学画面与教材屏幕共享画面一致同步，课堂教学更流畅。

» 全终端覆盖，抗弱网丢包，让不同场景、不同网络下的教学都能清晰流畅。

» 统一架构，一套 SDK 覆盖直播、连麦、推流，极大降低开发对接成本；一套打通的实时音视频网络，问题定位定界简单，极大提升运维效率。

8.7 亚洲渔港搭建供应链互联平台

随着生活水平的提高，人们对海鲜的需求逐渐增多。日益扩大的市场规模在给亚洲渔港带来利润的同时，也带来了不小的挑战。

亚洲渔港全称亚洲渔港股份有限公司，由亚渔实业、美团网、新希望集团共同投资成立，是中国领先的海鲜产业互联网公司（互联网 + 海鲜）之一，同时也是国家商务部认定中国电商平台示范企业。

随着交易量的激增，传统海鲜供应链和物流管理方面都面临严峻压力，如何快速响应客户的订单需求，如何及时对客户订单进行配送，这些都是亚洲渔港迫切要解决的问题。而要解决这些问题，物流项目和供应链项目的优化更新则起着至关重要的作用。

2018 年初，亚洲渔港正式接触华为云 DevCloud，华为云 DevCloud 作为一站式的云端研发平台，提供项目管理、测试管理、代码托管、代码检查、编译构建、部署、发布仓库、流水线等功能，有针对性的帮助亚洲渔港解决了在业务过程中遇到的阻碍和困难。

权限分工轻松管理

亚洲渔港有很多项目研发部门，每个部门成员都有不同职责的分工，不同的研发人员代码操作权限不同。在之前，亚洲渔港并没有很好的工具来对操作权限进行分工，更多的是在前期会议中进行规划和确定，这很容易导致职责权限的混乱，带来操作上的失误。

华为云 DevCloud 的权限管理方便简单，对所有开发者和操作者分角色、分功能划分，不同的权限下，可操作的范围和功能都是不同的，在人员职责出现变动的时候，只要在平台上修改即可，简化了管理模式，为公司管理和审计提供了可靠依据。

研发上云，打破研发条件限制

亚洲渔港在开发过程中遇到的另一个问题是开发环境问题。此前，亚洲渔港物流和供应链项目都只能在公司内部的局域网内作业，产品经理查看项目进度也只能在局域网内部才能查看。在公网环境进行的开发，只能临时编码或传给公司同事进行提交，若在同一办公地点，这种情况还较好处理，而一旦项目成员出差或者异地办公，代码的提交、进度的查看，只能通过与内网成员沟通才能进行，沟通成本高和代码时效性差成为了项目进展的阻力。

华为云 DevCloud 提供的一站式云端开发服务完美解决了这一难题，华为云 DevCloud 所有的研发服务都转到了线上，开发环境可以不受地域的限制，不论是异地办公还是本地办公，只要登录账号，都是统一的研发环境和场景，研发进度也可以在线上实时查看到，大幅度降低了沟通成本，打破了地域环境的限制，对物流和供应链项目的开发和交付提供极大便利和帮助。

产品上云，客户实时掌握开发进程

亚洲渔港的客户分布在全国各地，这就容易导致一个问题——因为距离的原因，客户在开发测试阶段很难在现场看到软件开发的进展，需要首次上线后才能得到客户的反馈，这导致客户反馈周期特别长，很大程度上影响了产品的交付进度。

华为云 DevCloud 与华为云资源无缝对接，通过代码托管模块实现服务与代码上云，开发和测试阶段可以根据客户要求及时让客户查看系统，获取客户的改进意见，有效的解决了异地沟通困难、客户反馈信息滞后的问题。

依托华为云 DevCloud 的前沿研发理念，亚洲渔港以大数据、云计算能力为基础，搭建了高效的垂直供应链产业互联模式，为产业链提供精准数据导入，进行资源重新匹配，提升产业价值，打造出高效的产业互联网平台，领导着庞大的海鲜产业集群，被誉为“中国国内具有优秀商业模式的海鲜垂直产业互联网公司”。

华为技术有限公司
深圳龙岗区坂田华为基地
电话：+86 755 28780808
邮编：518129
www.huawei.com

商标声明
HUAWEI，HUAWEI，是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

免责声明
本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有 © 华为技术有限公司 2021。保留一切权利。
非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。