

面向消费终端的企业云原生实践 白皮书



前言

当前，云计算已经成为推进数字经济发展和生产力变革的重要基础设施，而云原生作为下一代云计算的核心技术，重要性愈加凸显，成为驱动业务创新和增长的重要引擎。云原生以容器、微服务、DevOps 等技术为基础，用于构建、部署和运行应用，以充分发挥云计算优势，是当前先进的用云方法论。随着云原生技术和理念不断成熟，各行各业云原生实践也在不断深化，一般场景的云原生解决方案逐渐趋于完善，但对于一些面向消费终端的企业而言，其多元的业务属性，使其在面向跨场景、跨地域、跨形态的复杂消费终端云时仍存在诸多痛点，国内尚缺乏针对性的云原生解决方案路径指引，或成为面向消费终端的企业高质量发展的阻碍因素。

基于以上背景，华为云联合中国信通院研究并撰写《面向消费终端的企业云原生实践白皮书》，基于华为终端云的云原生改造和实践经验，为企业提供面向消费终端的云原生转型路径以及云原生实践经验，助力企业终端实现高水平数字化转型，促进产业高质量发展。

CONTENTS

前言

一、 数字经济时代，面向消费终端企业面临发展痛点	04
1. 自建基础设施四大问题阻碍企业发展	05
2. 业务持续交付的各个阶段效率低下	05
二、 全面上云走向全面云原生，解决面向消费终端企业的发展困局	06
1. 云计算步入云原生时代	06
2. 三步走策略实现业务终端云原生化	07
三、 企业云原生平台核心能力构建方法论	08
1. 基于 DevOps 的软件工程能力构建	09
1.1. 开发态（Dev）	10
1.2. 运行态（Runtime）	10
1.3. 运维态（Ops）	12
2. 基于 DataOps 的软件工程能力构建	12
3. 基于 MLOps 的软件工程能力构建	13
4. 沉淀平台的六大关键技术	13
4.1. 多活容灾高可用架构	15
4.2. 全球化网络部署技术	16
4.3. 微服务化	16
4.4. 云数据库	17
4.5. 大数据能力	18
4.6. AI 能力	19
四、 展望未来	20
1. 高效的数据化、智能化推动消费者业务的“个性化”发展	20
2. 统一的基础设施能力支持消费者企业“出海”	20
2. 融合数字化运营能力的平台工程帮助企业保持长效发	20
附录、 基于华为终端云的云原生实践案例	21
1. 华为终端云云原生模型	22
2. 微服务计算平台支持业务全量微服务化	23
3. 数据计算平台重铸底层架构	23
4. AI 计算平台发挥模型算力优势	24
5. 极简网络引擎，实现超低时延的最优体验	25
6. 典型业务场景及解决方案	26



1 数字经济时代，面向消费终端企业面临发展痛点

目前，随着数字技术的飞速发展，数字经济也迎来了快速创新的高速增长阶段，已经广泛渗透到其他经济领域，深刻改变世界经济的发展动力、发展方式，重塑社会治理格局。数字经济是新一轮信息技术革命催生的第三种主要经济形态，能够从技术、要素、创新、融合等多个层面促进经济高质量发展。在数字经济时代，线上消费保持高速增长，移动消费成为主流消费渠道，消费人群代际更替加快，年轻群体成为购买主力，后发区域消费潜力得到释放，为消费升级提供了强有力的基础保障，成为消费升级的坚强动力。消费需求的变化，促进了消费业务的多样性，在消费者青睐的移动终端，更是迎来了难得的历史发展机遇。

在国内，随着政策的扶持，数字经济更是进入高速发展的快车道，面向消费终端的企业应用全面迸发。面向消费终端的企业是指以消费者为主要服务对象的企业，通常业务范围广泛，涵盖全球市场，具有海量用户和海量数据，并面临着高可靠性、高并发性、百倍浪涌等业务特点：

· **用户规模庞大**：随着移动互联网的高速发展，面向消费终端业务规模呈现爆发式增长，以华为终端全球月活用户数量为例，2021年已经超过 7.3 亿，全球加入华为开发者联盟的注册开发者已超过 540 万，集成 HMSCore 能力的应用超过 18.7 万个。

· **覆盖范围广**：消费终端业务，围绕社交、健康、出行、娱乐等众多场景为用户提供数字生活体验。

· **业务增长迅猛**：随着移动终端越来越走近人们的生活，消费终端的全球应用数量年增长率超过 100%，以华为的 HMS 为例，全球应用数量年增长率达到 147%，全球应用分发量超过 4320 亿次，拥有手机、平板、电脑、穿戴设备、智慧屏等众多产品，海量的设备规模对基础设施运维成本、网络安全要求越来越高。

· **突发流量**：618、双 11 等集中消费的业务场景，呈现出典型的突发性，要求资源按需弹性伸缩，否则很难适应突发流量访问。

· **网络时延**：越来越多的消费终端企业选择出海，为全球客户提供服务，因此对跨区域网络传输的时延要求大幅提升。

· **网络安全**：随着业务规模的增大，服务器面临的互联网攻击风险越来越大。

· **高可靠性**：对数据中心网络可靠性的要求在增加，需要高效的双活 / 主备 + 异地容灾。

1.1 自建基础设施四大问题阻碍企业发展

消费终端业务需求和业务的多变性，系统的复杂性远非传统的自建 IDC 基础设施可以满足的。在很多方面出现了瓶颈，原有的技术架构也无法支撑业务演进：

· **建设成本高**：为了提升消费者的用户体验，我们需要建设全球化的高速网络和边缘接入节点。然而，随之而来的是高额的建设成本。这种成本不仅包括硬件和设备的投资，还包括维护和更新这些设施所需的持续投入。

· **运维成本高**：线下的部署方式需要全部自运维，由于全球异构架构的复杂性，维护工作需要高度专业化的团队，并且随着业务的增长和机房数量的增加，维护成本会快速增加。此外，不同时期建设的基础设施可能存在技术差异和兼容性问题，这也会增加运维的难度和成本。

· **基础设施弹性不足**：在全球化的业务环境中，热点活动或事件可能会导致业务浪涌，导致流量突增。为了应对这种浪涌，IDC 部署必须按照最高流量预估提前进行资源建设。虽然这种方式可以抵抗浪涌的冲击，但会造成极大的资源冗余。随着业务的扩展，冗余成本也逐渐增大。

· **新技术应用慢**：在技术日新月异的今天，企业必须不算跟进最新技术的发展，快速引入新兴技术能力，才能抢占市场先机。例如：大数据、AI、区块链等。而新技术发展不是空中楼阁，往往需要依赖配套的基础设施，在基础设施不完善的情况下，也无法塑造出技术落地的环境。

1.2 业务持续交付的各个阶段效率低下

研发和运维效率一直是企业关注的主题。随着 DevOps 理念的普及，以及平台化、自动化和智能化的发展趋势，企业越来越重视效能问题，正在不断探索新的方法和工具，以提高研发和运维的效率，从而更好地满足业务需求。

在此过程中，企业大多会遇到下面这些问题：

· **平台化服务增加推高使用者成本**：随着平台服务能力的逐步丰富，也给使用者带来了越来越多的复杂性，了解平台有哪些能力、怎么快速使用平台这些能力就成了硬币的一体两面，功能越丰富使用就越复杂。

· **需求跨多工具平台**：开发人员一个场景需跨多个平台操作跳转。

· **研发环境管理复杂**：存在个人级、版本级、产品级环境，涉及中间件等其他服务交互时，环境搭建复杂，缺少快速构建研发测试环境能力。

· **缺少研发数据的洞察和分析**：缺少对业务高价值的洞察及分析，如需求工作量管道承载情况、漏洞分析处理、版本需求进度、溯源信息在具体版本中的流向等。

· **资源难以复用**：各业务系统烟囱式构建，中间件、业务应用的计算资源静态分配，各业务独占使用，资源浪费严重，资源成本高。

· **微服务缺乏可观察性**：随着微服务增多，架构呈现离散化趋势，缺少系统性可观察能力，如微服务依赖关系情况、产品服务粒度的可视化拓扑图等。只能凭经验识别核心调用链路和关键服务风险，对领域架构的优化也难以得到有效反馈。

· **微服务治理能力分散**：治理能力散落在多个平台和中间件，故障容错、限流、降级、熔断散落在各个服务中，难以实现统一管控和故障隔离。

· **部署周期长**：新上线一个服务，各种权限、审批流程繁多，自动化程度低，导致 IT 交付过程漫长。

· **配置人工变更效率低**：网络、环境、参数配置采用线下人工维护，容易遗漏，网络策略复杂易出错，不支持自动化/IT 化管理。

· **缺少服务视角的统一监控**：服务所使用的（计算、网络、存储）、中间件（SLB、DCS、DMQ）、公共服务等服务监控等分散在各服务内，每个服务都需要对接运维公共服务。

· **缺少端到端故障自动化演练**：需进一步完善故障模式库、故障场景等，提升容器场景演练能力、过程快速感知、自动决策、全自动化执行的能力。



2 全面上云走向全面云原生，解决面向消费终端企业的发展困局

2.1 云计算步入云原生时代

随着企业的数字化进程进入到的一个新的阶段，企业上云不仅仅是把业务简单搬迁到云上，更应该让业务能力“生于云、长于云”。

云计算的发展已进入云原生时代。麦肯锡调研数据显示，通过对云原生技术的应用，全面解锁云的价值后，全球财富 500 强企业的 EBITDA（Earnings Before Interest, Taxes, Depreciation, and Amortization，息税折旧及摊销前利润）在 2030 年将提升超过 1 万亿美元。近年来，云原生技术有了新的发展，其目标是更好地服务于全球范围内的政府和企业，推进他们的数字化、智能化改造，同时保障业务高效、可靠、安全，其用云的广度和深度也与之前的消费互联网时代明显不同，进入了全新的时代。

企业为持续发展，则应当依托云原生，以应用为中心构建全新的云服务体系。通过云原生基础设施升级、应用的现代化改造、数智融合等新技术手段，缩减基础设施建设、交付、运维等成本，并且加速上层业务的全球化布局与创新升级。

通过从线下走向线上，共享使用云服务商的全球站点，可大幅降低建设成本。同时，实现运维分层，企业只专注业务层面运维，基础设施运维能力可全面依托云服务商提供。利用云原生容器化对业务进行改造，实现不同业务间的资源共享，弹性调度和按需使用，有效提升资源利用率，通过灵活使用公有云的各类基础、高阶服务，满足新业务快速上线的诉求。并且云计算已经发展非常成熟，新的技术通常也以云服务的方式呈现。因此获取新技术最高效的方式是以云服务的方式获取，例如：大数据、AI、区块链等。

2.2 三步走策略实现业务终端云原生化

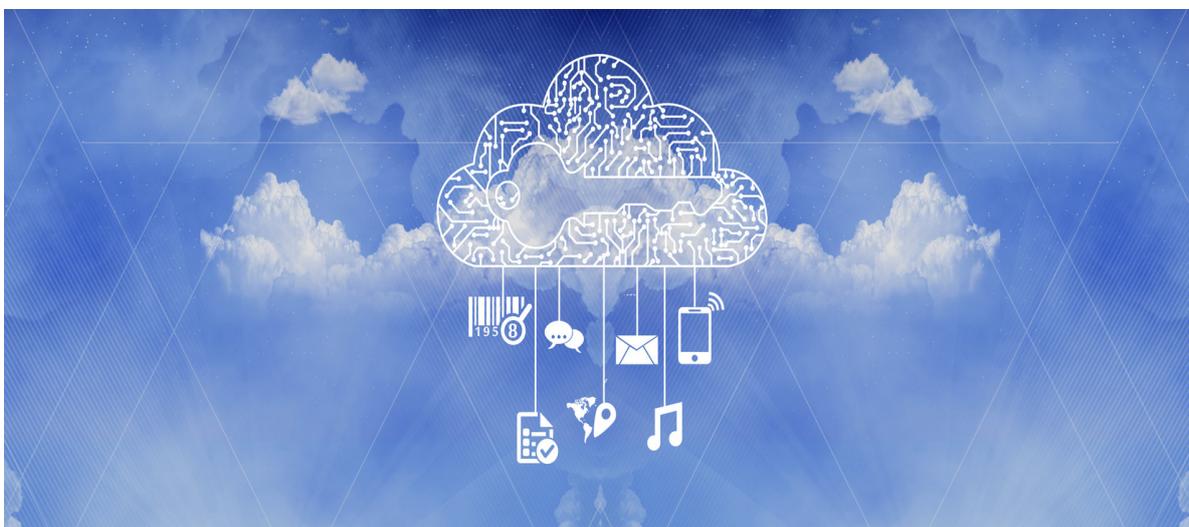
上云之初，企业应当制定一个上云的策略，建议分为三个阶段。第一阶段为 IaaS 上云，第二阶段为高阶服务上云，第三阶段为深度应用云原生。

1 IaaS 上云：作为全球化企业，首先需要考虑的是在全球各国的隐私数据保护条例，欧盟的 GDPR 下，基于最优用户体验，构建全球部署架构，满足不同区域业务时延要求。而由于越来越高的 ESG 目标，数据中心能效比 PUE 也是一个重要的考量指标，必须满足绿色低碳的要求。

2 高阶服务上云：云服务提供商通常具有丰富的云原生技术积累，可以提供高效、安全、可靠的云服务能力，从而大大提高业务开发和运行效率。因此，企业直接使用云上的高阶云服务，如数据库、大数据、AI、容器等，而非自己构建，可以使企业更专注于核心业务的开发，而无需投入大量资源自行维护和扩展这些服务。

3 深度应用云原生：在 IaaS 和高阶服务均上云的情况下，需要深入研究和应用云原生的各种技术，如：业务微服务化、在离线混部等，以逐步提升资源利用率，实现降本增效。此外还可以利用云服务提供的能力，构建运维治理工具，并通过自动化来持续提升运维效率，降低运维成本。

通过这样的“三步走”策略，可以将业务平稳、高效的推进到全面云化的战略目标，并随着业务的发展，快速落地新技术，通过持续降本增效，帮助企业更好地应对市场变化和竞争压力。





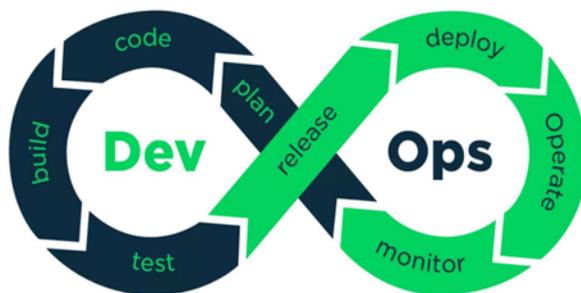
3 企业云原生平台核心能力构建方法论

企业软件开发已经进入了新的时代，应用开发、数据开发和模型开发成为了企业软件开发的三个核心领域。DevOps 的理念也已广泛被应用于这三个领域，因此构建三大领域端到端的软件工程能力，实现应用、数据、模型的高效交付和运维是核心目标。

同时需要将大容量、高可靠、全球化、安全隐私等关键技术能力下沉在平台内部，以服务化方式向应用提供，通过 DevOps 端到端工具链为用户提供便捷接入和使用，让开发人员更专注业务代码实现。

3.1 基于 DevOps 的软件工程能力构建

云原生 DevOps 平台的应当以服务使用者为视角，以提升企业应用的开发，运维，运营的全流程运作效率为目标，聚焦 Dev-Runtime-Ops 进行能力构建。



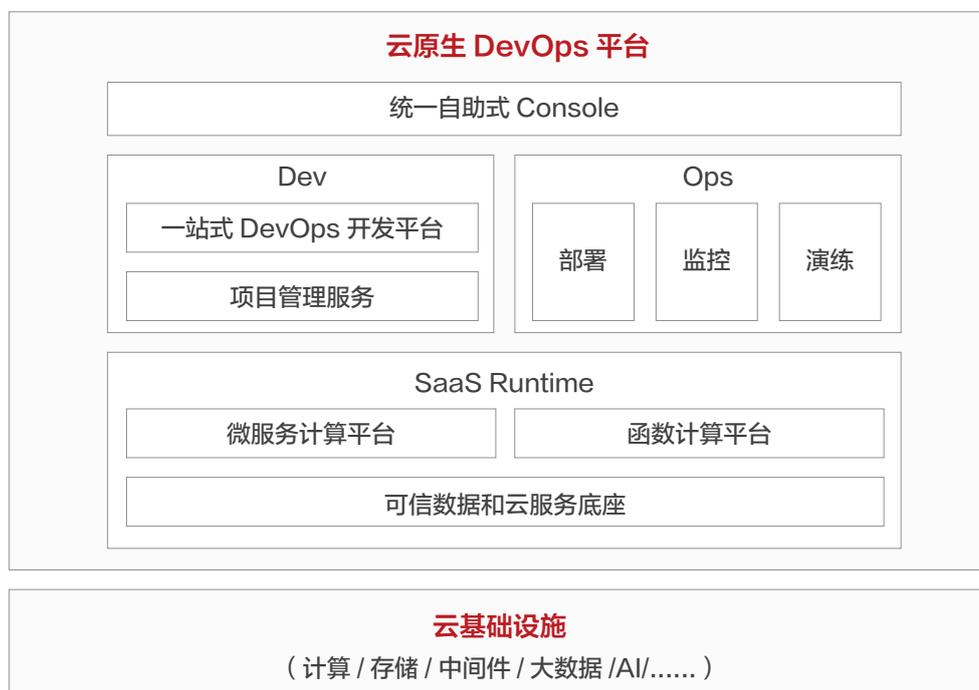
需要以软件交付件为核心，并将流程 Built-in 到软件生产过程中。

· **以软件交付件为核心：**“业务代码 +BaC= 软件包，软件包 +IaC= 可运行环境”。

BaC 指构建即代码，IaC 指基础设施即代码，软件包则应该包括应用、云侧服务以及数据和 AI 算法等。

· **流程 Built-in 到软件生产过程**：指 BaC 和 IaC 执行过程中可针对流程中需要进行的质量控制项进行控制。

比如 IaC 执行时发现现网有删除数据库的操作那么主动拦截触发审批，BaC 执行时发现此软件版本有使用的开源软件有严重漏洞那么则不允许发布等。



3.1.1 开发态 (Dev)

构建项目管理服务和一站式开发平台，通过软件信息树实现全流程可信。解决研发过程中的跨角色、跨组织协作问题，开发人员在本地图可以完成个人级编码 / 调测 / 检视 / 提交等活动，实现函数 / 微服务 / IaC 的一站式操作部署。

面向云原生应用开发者提供一站式 DevOps 开发工作台：覆盖持续开发阶段全链路活动，使能开发者免工具切换完成全栈工作流，通过个人工作台查看并处理需求、缺陷、检视活动等任务，并能随时监控、管理个人 CI&CD 工作流

· **聚焦可信编码**：提供 IDE 工程一键配置、消费软件信息树、部署信息树以及信息仓进行最优软件的推荐、检查，做到过程可信，提供本地代码静态检查以及代码合入能力

· **函数开发全生命周期管理**：提供函数创建、开发、调试、测试、部署、监控和优化的全生命周期一体化作业平台

· **微服务开发全生命周期管理**：提供微服务创建、开发、调试、测试、部署、监控和优化的全生命周期一体化作业平台，支持可视化引用各类中间件、公共组件

· **IaC 一站式开发部署**：提供 IaC Model 模板化创建、定义自动补全、智能校验、计划预执行能力

· **融合 DevOps 持续开发过程中的工作流和信息流**：结合软件信息树实现编译 / 构建依赖和漏洞管理

· **支持本地调测**：一键端云联调，基于本地沙箱环境极简化开发调测反馈循环

3.1.2 运行态 (Runtime)

提供大容量、弹性、安全、高可靠的服务运行环境，让业务看不到云，按需快速集成。

· **可信数据和云服务底座**：统一托管业务运行时的 IaaS 资源（计算、网络、存储等）和数据库，将服务运行时的可信公共能力（可靠可用、服务治理、流量调度、韧性等）下沉到平台，提供包括注册中心、配置中心、灰度发布、限流降级、服务隔离等一系列服务治理能力，实现平台和业务解耦，让业务聚焦代码开发，提升交付和维护效率。

· **微服务计算平台**：微服务改造后，微服务数量急剧发散、调用链路极度增长，在现网出现故障时，定位问题是非常复杂的。因此需要提供一个全托管式微服务运行环境，全面实现容器化和基于流量的弹性伸缩。并提供调用链、日志服务、基础监控等能力，可实现自助诊断能力，而业务只需聚焦自身代码开发。

· **函数计算平台**：函数计算（Function-as-a-Service 简称 FaaS）是当今最流行的 Serverless 计算服务。函数计算将应用程序所需的底层基础设施和管理任务交由平台完成，开发者则可以将更多的精力集中在应用程序的业务逻辑上。通过函数计算平台可提升函数的开发和灰度升级易用性，优化弹性伸缩和调度策略，帮助业务提升研发效率和降低资源成本，助力应用生态全面 serverless 化。

3.1.3 运维态 (Ops)

随着很多企业逐渐将越来越多的业务系统往云上迁移，企业客户需要将 IT 治理模式延伸或迁移到公有云上。因此需要围绕运维阶段 3 个核心场景：部署、监控、演练进行自动化、数据化、智慧化运维能力的构建，提升运维效率，为高品质业务提供保障。通过运维管理体系建设，实现流程 IT 化和可控可回溯的运维安全管控能力，并最终实现无人值守运维。

部署服务

目标围绕部署的全生命周期过程进行管理，通过 IaC 全面全自动化部署，实现无人值守变更。依托流程、工具和运营能力，从变更提交和变更结束，打通全流程各个环节，实现场景化的无人值守。

· **变更管理**：完善变更通知，变更检测，变更执行，变更记录各阶段的自动化能力，在变更过程中自动识别高危变更操作，差异化区分不同类别变更操作的处理方式，提升变更流程的自动化率，通过工具和流程保证变更过程和结果的可信。

· **声明式 IaC**：开发人员只需要通过 IaC 声明定义需要资源或状态，后端将复杂的业务逻辑进行封装，简化 IaC 代码开发。IaC 提供标准化模板，并开放参数，定制参数通过规格进行抽象，对类似删除数据库等高危操作进行主动拦截，避免事故，支持全球一份 IaC 代码。

· **服务环境**：服务 IaC 代码执行后生产服务环境，部署服务提供环境的创建，删除，更新，归档，恢复等全生命周期管理，并按照环境聚合环境包含的资源的监控数据，支持对现网存量部署的业务资源按环境维度进行纳管，业务平滑过渡到云原生 DevOps 平台。

· **网络自动化**：抽象“隔离域”概念，对业务屏蔽公有云网络细节，实现网络资源的业务声明式定义和配置自动化。业务通过定义网络隔离域 IaC 代码实现部署视图 IT 化，部署服务调用网络服务自动化配置服务需要使用网络信息。关键技术点包括：一、抽象公有云网络资源概念，自动规划和分配网络资源，让业务不感知网络；二、根据服务依赖关系自动生成网络访问策略，实现服务间网络自动按需开通。

监控服务

面向开发和运维 SRE，围绕故障生命周期，以自有服务视角汇总 IaaS、PaaS、SaaS 的监控信息，构建开箱即用的一体化可观测性平台；同时构建运维数仓以及故障 RPA 处理能力。

· **故障预防**：故障预防重点构建健康管家（巡检能力），基于系统化监控及分析能力，面向自有服务和生态开发与运维，提供自定义巡检和编排，可视化度量现网风险，驱动业务改进，提升巡检效率

· **故障检测**：围绕服务状态，构建事件中心及全景化事件诊断能力。并给业务提供内网拨测能力，研发发布测试用例能够在拨测平台进行自动化拨测监控，提前发现问题。

· **故障诊断**：分为基于专家经验故障诊断工具包括数据库故障诊断、服务调用诊断等诊断工具，同时结合 AI 算法逐步构建根因分析等智能化诊断能力。

· **故障通报**：实现故障通报 IT 化管理，提升故障通报效率

· **故障恢复**：通过知识库、应急预案、故障自愈等能力构建，实现故障自动化恢复。丰富和构建故障恢复原子能力，通过自动化编排故障处理流程，逐步实现故障轻量化、智能化处理。

演练服务

演练服务是基于混沌工程理论主动干预提前识别风险，围绕演练生命周期管理提供平台能力。重点构建以下能力：

· **IT 化管理**：实现演练计划、演练方案，演练报告的可管理、可重用、可追溯等 IT 化能力

· **最小化爆炸半径**：通过接口级以及会话级故障模式，控制演练最小化爆炸半径，实现常态化的演练

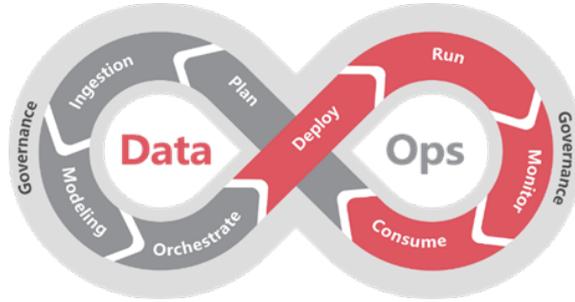
· **混沌工程**：建立稳态指标系统，实现全业务的故障场景自动化执行、监控指标采集、测试与度量，快速评估服务可靠性质量属性，识别可靠性风险

· **集成调用链**：支持基于规则的链路自动化故障注入能力。



3.2 基于 DataOps 的软件工程能力构建

DataOps 的目标是汇集 DevOps 全流程数据，进行建模、度量、诊断及改进，通过数据驱动研发效能持续提升。



面向管理，对研发全流程数据进行关联挖掘分析，识别并预警风险点，确保可信合规。

面向作业，从时间、速率、负载、效率、分布等维度识别价值流瓶颈点，采取针对性行动，促进效能提升。包括研发领域数据模型、研发领域指标模型和可视化自助分析等能力。

数据计算平台的构建涵盖数据开发、数据治理、数据运维的全流程工程能力。提供数据建模、数据接入、数据开发、任务管理与调度、数据共享、数据分析、数据地图、数据质量、数据安全、数据运维等全域的 DataOps 服务。

3.3 基于 MLOps 的软件工程能力构建

MLOps 的目的是借鉴 DevOps 理念，构建机器学习系统平台，提供全流程 AI 模型交付支持，使业务人员聚焦于数据和算法。



MLOps 平台需要具备数据准备、模型训练、执行与反馈的能力，通过资源容器化管理、统一调度、分布式训练提升资源利用率。支撑数据高效准备，海量数据快速训练，高并发低时延模型执行以及应用效果及时反馈闭环。

核心组件包括

数据准备平台（Data Prepare Platform，简称 DPP），聚焦于构建特征平台能力，实现离线与实时特征的规范化高效生产、特征的离线与在线存储，为模型训练提供特征选择与样本生成能力，为模型实时推理提供特征在线获取服务，同时实现全链路特征监控，为 AI 开发者提升特征生产、管理与使用效率，并保证特征质量。

模型训练平台 (Model Training Platform, 简称 MTP) , 聚焦高效分布式训练, 使业务聚焦领域特征工程、算法、模型。应具备全球化部署, 支持多种训练框架, 支持数据管理, 支持观测训练过程和算法在线编辑能力, 支持多种训练任务模式, 提供分布式训练能力与 GPU 加速能力, 支持租户级资源隔离能力。

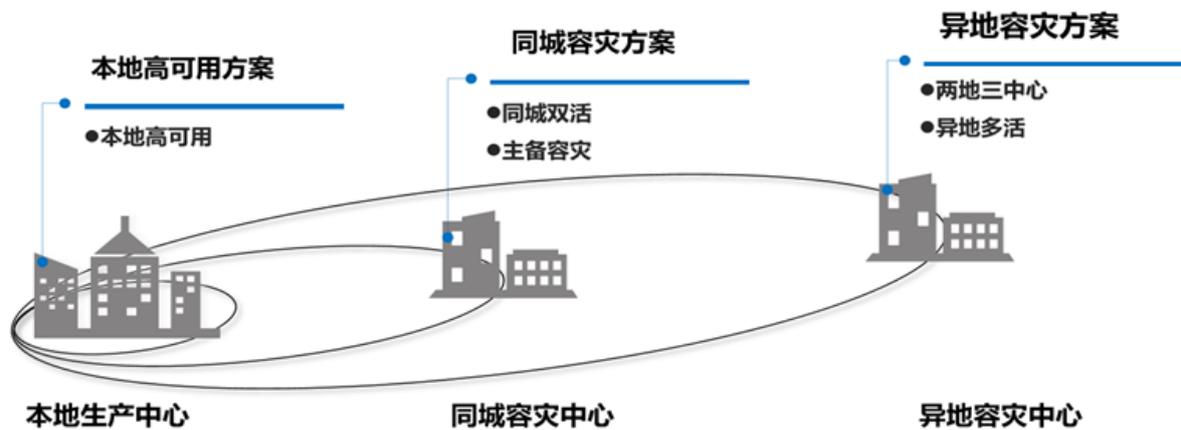
模型执行平台 (Model Execution Platform, 简称 MEP) , 提供高效、稳定、可靠的模型运行环境, 提供模型在线执行全生命周期托管, 简化业务集成模型的过程, 让业务聚焦于业务逻辑开发, 算法工程师更聚焦于算法的迭代优化。

模型效果评估 (ABTest) , 基于先进的底层算法, 提供科学分流能力, 提供智能的统计引擎, 实验结果可靠有效, 助力业务决策。

3.4 沉淀平台的六大关键技术

对于消费者终端企业而言, 由于其业务规模庞大且拥有海量用户基数, 因此业务大多需要全球化布局, 并采用高可用性、资源高效和数据高效等关键技术, 依次需要将这些关键技术沉淀在平台中, 供上层业务以服务的方式使用。而智能化是企业发展的最大助力, 无论是对研发运维效率的提升还是对新业务形态的诞生都具有重大意义。因此, 高效的模型开发平台也应作为关键技术在平台中构建。

3.4.1 多活容灾高可用架构

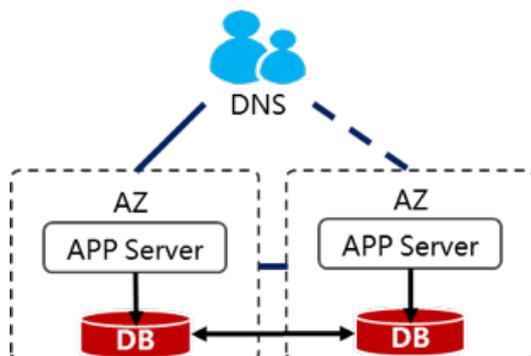


衡量容灾系统有 3 个指标: 容灾半径 (生产系统和容灾系统之间的距离)、RPO (灾难发生时允许丢失的数据量)、RTO (系统恢复的时间)。

按照容灾半径不同, 有同城容灾、异地容灾方案, 分别应对机房级、地域级故障, 保障对应层级的数据安全和业务连续性。企业可应用多个云服务实现数据容灾、存储容灾、同城双活、异地多活 4 大容灾解决方案, 支持业务 SLA 达到 99.99% 以上。

· 同城双活

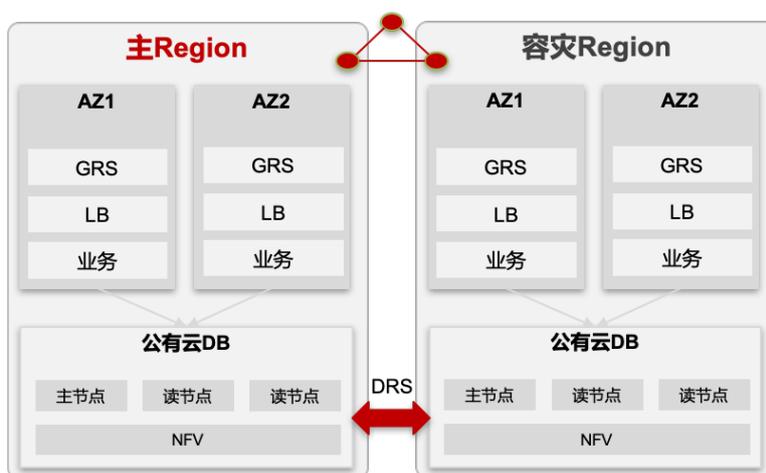
主备 AZ 同时承载业务，通过控制节点监控双 AZ 状态，包括与外网连通性检测，相互间连通性检测，以及数据存储（数据库、缓存）状态，机房状态等，供故障切换使用。



· 异地（跨 Region）多活

构建跨地域多中心负荷分担的异地多活方案，Region 内保持双活，双 AZ 均故障时，才向其它 Region 切换。支持异地多 Region 的多活检测、数据自动采集、多活状态可视化监控，支持多活故障切换、异地多活可运维等能力。

可用多活故障恢复 RTO 指标进行评估，该指标表示从多活状态检测，到状态异常发现与故障决策，并执行多活故障切换 / 修复，直到终端用户业务恢复的时间。



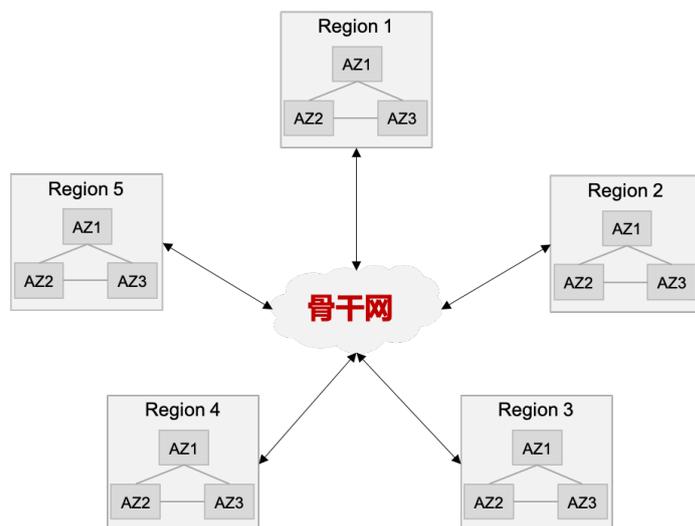
· 异地数据容灾

数据库关键数据 (MySQL/SDS/ 公有云 DB) 本地备份 + 异地数据容灾

在数据本地备份基础上，针对核心业务构建数据异地容灾和恢复方案，防止 Region 故障导致数据倾覆式风险，数据异地容灾 RPO 小于 10 分钟，容灾数据恢复 RTO 小于 12 小时。

· 数据本地多副本 + 跨 Region 数据异地备份

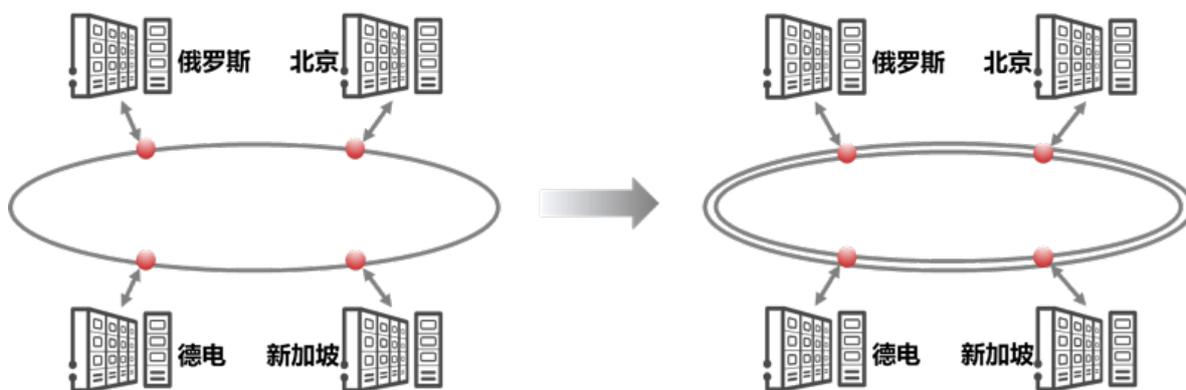
为了提升业务体验，同时网络 / 存储故障实现快速切流恢复，在多地部署接入点（如华为终端云在华北、华东、西南、华南等区域均有部署）。保证用户就近接入，降低时延和提升用户使用体验，同时也提升了数据可靠性和服务 SLA。



3.4.2 全球化网络部署技术

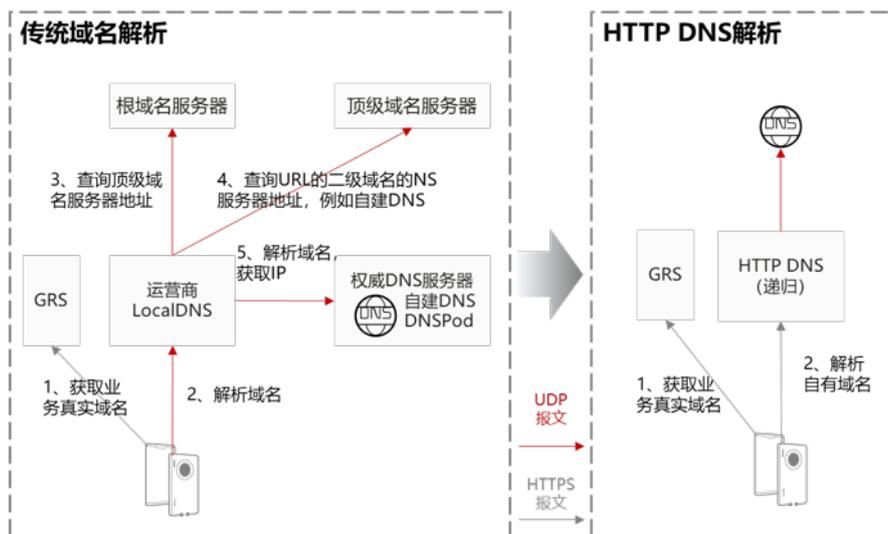
· 全球 4 大主站 + 双链路高可靠骨干网

在遵守隐私安全条例的前提下，可在德国、俄罗斯、北京、新加坡部署四大主要站点，覆盖全球用户。其中，德国站点覆盖欧洲地区，北京站点覆盖中国地区，而新加坡站点则覆盖东南亚 / 拉美 / 非洲地区，俄罗斯由于特殊的隐私要求需要独立部署。



通过骨干和专线封装两条 ER Peering 链路，做 BGP 负载分担，将全球骨干网络可靠性从 99.9% 提升至 99.999%。主站业务多 VPC 互通，由 VPC Peering 改为 ER 连接，东西向流量从网状互联升级为中心辐射，简化网络运维和提升流量转发效率。

为提升用户体验，可以在部分地区部署边缘节点。通过服务下沉的方式，缩短时延，提升用户体验。



· GRS 技术 (Global Router Service, 全球路由服务)

GRS 用于端侧 App 进行服务发现，端侧访问 GRS 的域名，会自动查询 DNS 服务器，给 GRS 分配一个 IP，访问指定的 GRS 服务器。GRS 帮助端侧 App 根据当前上下文(目前主要为相应国家码，例如注册地，服务地等) 查找其依赖的云服务的正确地址 (URL)，简化端侧逻辑，有效地支撑“服务地接入”的原则，满足合规诉求。

· HTTP DNS 技术

通过 HTTP DNS，绕过 LocalDNS、根、顶级和权威服务，解决现网 LocalDNS 故障问题和根服务器的连续性问题。实现域名防劫持能力，包括自有域名和第三方 CDN 的域名。降低解析时延、提高可靠性和可用性，结合端侧提供更强大的准调度能力。

3.4.3 微服务化

在云时代，大多数企业服务，都会经历从云化到云原生的转变。上云初期，业务主要部署在虚拟机上，但随着业务规模不断增长，会面临资源利用率、扩容效率、网络管理自动化等问题。同时，业务的单体应用随着功能的增多，变得越来越厚重，功能模块之间耦合，不利于维护，故障范围增大。通过对业务进行微服务化改造，并基于云容器引擎服务，实现云原生 DevOps 在云服务的全面落地。

云容器引擎 (Cloud Container Engine, 简称 CCE) 提供高度可扩展的、高性能的企业级 Kubernetes 集群，支持运行 Docker 容器。借助云容器引擎，可以在云上轻松部署、管理和扩展容器化应用程序。云容器引擎深度整合高性能的计算、网络、存储等服务，并支持 GPU、NPU、ARM 等异构计算架构，支持多可用区、多区域容灾等技术构建高可用 Kubernetes 集群。

借助于云容器引擎服务，可以实现：

- **提升资源利用率：** 容器可更细粒度划分资源，使应用可充分使用资源；

· **复杂系统简单管理**: 单体应用解耦拆分为多个轻量模块, 每个模块升级 / 伸缩更加灵活, 轻松应对市场变化;

· **保障业务高可用**: 秒级弹性扩容, 快速响应并发高峰, 保障业务高性能、高可用。

在实际应用中, 还可使用一些容器服务的创新技术, 助力企业进一步降本增效:

· **CPU 潮汐亲和**: 在不绑核场景, 同一微服务多个 Pod 间 CPU 使用率差异过大 (峰值 25%), 如果采用传统静态绑核方式, 可以提升 CPU 性能, 但 CPU 资源不能 Pod 间共享, 不利于资源利用率提升。通过动态绑核, 可消除业务容器 CPU 不均衡和性能下降问题 (接近静态绑核), POD sidercar 容器进行一定的超分, 整体提升资源利用率 5%。

· **在离线混部**: 企业的业务一般可以分为在线业务和离线业务, 在线业务的特点是需要及时处理, 优先级较高, 若无法及时处理影响用户体验, 例如: 应用市场业务, 用户从应用市场下载 APP, 需要及时响应, 在线业务的流量主要在 6:00~24:00 (20:00 左右是高峰), 00:00~6:00 业务量较少。而离线业务的特点是对实时性要求没那么高, 但是需要持续的算力支持。例如: 输出每日的运营报表, 华为浏览器智能资讯推荐模型训练。若在线业务需要资源时, 有限的资源被离线业务占用, 势必需要规划更多的资源以支持在线业务。而事实上, 离线业务的时间敏感度不高, 可以将资源释放出来支援在线业务。通过在离线混部技术, 相同资源情况下承载更多业务, 进一步提升资源利用率。

3.4.4 云数据库

作为数字经济的“根技术”, 数据库的重要性不亚于芯片。一切数据, 都必须在数据库中奔跑。比如华为终端云服务的很多核心业务, 如应用市场、云空间、商城、账号、支付、游戏、视频、浏览器等, 均运行在数据库上。云原生数据库, 是云原生技术中非常核心的一环, 云原生数据库为企业核心业务而生, 其特性和能力有力的支持了业务运行和体验的改善。

随着业务的飞速发展, 传统的集中式数据库, 已经无法适应数字经济时代的需要, 分布式数据库应运而生。与集中式数据库相比, 分布式数据库在数据文件组成、用户访问、高可用等方面, 有以下几个方面的区别:

集中式数据库	分布式数据库
由单个中央数据文件组成	由位于不同站点的多个数据文件组成
多个用户同时访问同一文件时易发生瓶颈	允许多个用户访问和操作数据
文件传递给用户可能需要更长的时间	从离用户最近的位置快速传送文件
单站点意味着系统发生故障时停机	如果其中一个站点故障数据可以恢复

在数据库架构的选型上, Shared Nothing 的数据架构, 更能适应移动终端业务的特点及发展需要。按照计算和存储的共享形式, 数据库架构分为以下三种:

· **Shared Everything**: 一般指的是单个主机的环境, 完全透明共享的 CPU / 内存 / 硬盘, 并行处理能力较差, 典型代表就是 SQL Server、单机版 Oracle 和 MySQL, 一般不考虑大规模的并发需求, 架构比较简单, 一般的应用需求基本都能满足。

· **Shared Disk:** 各处理单元使用自己的私有 CPU 和 Memory，共享磁盘系统。典型的代表是 Oracle RAC、DB2 PureScale。例如 Oracle RAC，共享存储，做到了数据共享，可通过增加节点来提高并行处理的能力，扩展能力较好，使用 Storage Area Network (SAN)，光纤通道连接到多个服务器的磁盘阵列，降低网络消耗，提高数据读取的效率，常用于并发量较高的 OLTP 应用。其类似于 SMP(对称多处理)模式，但是当存储器接口达到饱和的时候，增加节点并不能获得更高的性能，同时更多的节点，则增加了运维的成本。

· **Shared Nothing:** 各处理单元都有自己私有的 CPU/内存/硬盘等，Nothing，顾名思义，不存在共享资源，各处理单元之间通过协议通信，并行处理和扩展能力更好。典型代表为华为公司自主研发的新一代企业级分布式数据库 GaussDB，各节点相互独立，各自处理自己的数据，处理后的结果向上层汇总或在节点间流转，支持 x86 和 Kunpeng 硬件架构，基于 Share-nothing 架构，提供高吞吐强一致性事务处理能力、两地三中心高可用能力、分布式高扩展能力、大数据高性能查询能力。

3.4.5 大数据能力

大数据是人类进入互联网时代以来面临的一个巨大问题：社会生产生活产生的数据量越来越大，数据种类越来越多，数据产生的速度越来越快。传统的数据处理技术，比如说单机存储，关系数据库已经无法解决这些新的大数据问题，主要存在几个方面的挑战和痛点：

· **数据孤岛严重，数据共享低效，平台治理困难:** 全网大数据集群几十个，元数据分散在多个集群，造成治理的困难。存算一体架构下数据共享只能通过数据拷贝完成，业务造成不必要的存储浪费。核心集群规模大（可能达到上千节点），存在故障域大，维护困难等问题。

· **自建 IDC 机房的成本较高:** 一方面 IDC 机房的 TCO 成本高，另一方面需要建设独立的大数据组件研发团队维护几十个组件。技术上缺乏弹性机制，存算一体存储扩容造成算力被动扩容，成本高企。依据峰值建设大数据集群，架构上缺乏弹性，造成资源的浪费。

· **集群可靠性和数据共享易用性之间的两难:** 为解决融合模型计算的数据共享问题，在存算一体下建设了超大规模大集群，虽然数据共享方便，但也造成大集群在升级、维护和故障爆炸半径过大的问题。如果拆分为小集群，虽然能解决故障爆炸半径大的问题，但是无法高效共享数据，并且造成算力因存储被动扩容，成本过高。

针对以上挑战和痛点，许多云厂商，均推出了大数据平台，这其中，以华为云提供的大数据 MapReduce 服务（MRS）为代表。MRS 是一个在华为云上部署和管理 Hadoop 系统的服务，一键即可部署 Hadoop 集群。MRS 通过统一元数据、存算分离、高可用架构，可有效的解决目前大数据面临的问题。

· **统一元数据使能新一代数智融合架构创新:** 打破原有的大数据、数仓、AI 的数据孤岛，把数据目录、数据权限、多版本管理等能力都统一到一个中心点，都依赖这个中心点来访问数据，这样数据的使用就不会被孤立的系统束缚。例如，同一个表格可以被不同的分析工具做分析，既可以跑数仓任务，也可以做大数据和机器学习任务，不同的用户角色不管用什么工具访问数据，不再需要在专用系统之间来回导入导出数据。

· **云原生存算分离技术创新:** 通过云存储 + 缓存 + 计算的三层分离架构，使性价比足够高，计算也足够灵活。拉远存储，使得计算和存储可以各自弹性伸缩，按需使用。通过缓存，弥补拉远后的性能损失，把损耗控制在很小范围内，业务不感知。

· **高可用架构及低成本**：核心业务多 AZ 多活和全量故障域部署，可靠性全面提升到 4 个 9。业务的连续性和可用性是数据平台上云改造的重要关切点，例如 CBG 数据平台改造后可以达到机柜级故障业务无感知，单 AZ 故障重点业务不中断，运维效率全面提升。同时，MRS 可以按业务低谷，自动弹性伸缩，帮助客户节省大数据平台闲时资源。用时再创建、用时再扩容，用完就可以销毁、缩容，确保低成本。

3.4.6 AI 能力

AI 开发当前面临的巨大挑战是，随着模型复杂性和数据量增加，计算过程越来越耗时，导致训练时间延长，资源紧张。

因此，亟需一个面向 AI 开发者的一站式开发平台，可以提供海量数据预处理及半自动化标注、大规模分布式训练、自动化模型生成，以及端 - 边 - 云模型按需部署能力，帮助用户快速创建和部署模型，管理全周期 AI 工作流。比如华为云的 ModelArts，就是一个快速、普惠的 AI 开发平台，能够支持昇腾异构加速芯片，提供全栈式 AI 服务。该平台包括 TB 级 embedding Table、MemArts 缓存加速、RDMA 网络、芯片间高速互联等能力，能够在海量检索、内容审核、智能问答、NLP、大模型等场景中提供高效的 AI 服务。

利用一站式 AI 开发平台，可以百倍提升数据准备效率，降低一半的模型训练耗时，一键部署模型到云、边、端，并利用 AI 加速 AI 开发过程。平台提供多样性编排、开发调测以及实验记录管理等能力，并通过基于 Console 的运行态账号、资源、配置、Workflow 全链路管理能力，加速应用的迭代效率。

Notebook 的开发模型，可快速接入分享案例内容，让 AI 探索与教学更简单。在一站式开发平台中统一管理 AI 开发全流程，提升开发效率，记录模型构建实验全流程，提高模型可靠性，支持机器学习、深度学习、强化学习、决策优化等框架。本地 IDE+ 一站式开发平台插件远程开发能力，运行环境自定义，云上云下，无缝协同。

一站式开发平台提供基于 Notebook 的参数化、图形化、交互式的能力加速开发过程，帮助开发者在数据处理、模型调优以及模型预测方面进行可视化的操作，低门槛完成多种场景的 AI 算法开发与应用，配套提供的算法套件可以更加高效进行 AI 开发。

在工具方面，为了更加匹配通用的 IDE 工具使用习惯，一站式开发平台提供 VSCode\PyCharm 插件，支持本地化代码开发，使用插件远程连接云上资源进行远程开发调测，并且可以调用模型训练、模型部署等能力。





4 展望未来

随着云计算技术的不断发展和普及，面向消费者企业应用云原生的发展趋势将会越来越明显。构建基于云原生的平台工程，可以帮助企业降低技术人员的认知负担，标准化工作流程，改善开发体验，统一化公共能力。通过全面提升企业效能，应对市场的快速变化和激烈竞争。

4.1 高效的数据化、智能化推动消费者业务的“个性化”发展

在消费者业务中，数据化和智能化已经成为实现个性化发展的有效手段。通过结合人工智能 (AI) 和大数据技术，企业能够从消费者行为、偏好、需求等方面获取海量数据，并对其进行深入分析，以实现更精准的产品设计、营销策略和客户服务。

海量的消费者数据需要高效的大数据和 AI 平台能力支撑。构建统一的平台能力，可以帮助企业快速进行数据价值挖掘和模型优化，为消费者提供更为个性化的产品和服务，提升消费者的满意度和忠诚度。

4.2 统一的基础设施能力支持消费者企业“出海”

随着全球化进程的加速和数字技术的不断发展，越来越多的中国消费者企业开始“出海”，走向国际市场。为了应对这一挑战，企业需要构建云原生平台。云原生平台提供全球分布式的架构，将可靠性、隐私安全性和性能等关键能力通过服务的方式向业务开放，为企业提供必要的基础设施和支持，帮助企业快速推出新业务，确保一致性的用户体验。帮助企业在竞争激烈的国际市场中保持领先地位，满足消费者需求。

4.3 融合数字化运营能力的平台工程帮助企业保持长效发展

企业需要的不仅仅是软件工程能力，而是融合了端到端数字化运营能力的平台工程。这种平台工程还需要包括云资源规划、集成交付、云上资源成本治理、供应商管理等多方面的能力。

资源规划能力可以帮助企业基于业务统筹规划云资源和架构的建设，通过集成交付能力可实现快速交付，提高业务效率。云上资源成本治理能力可以帮助企业更好地控制云上资源的成本，优化云上资源的分配、监控和管理。供应商管理能力可以帮助企业更好地管理供应商，确保供应商的品质和服务，降低风险。

这些能力可以帮助企业实现全面数字化运营，全方位提高资源利用率和业务效率，降低成本，实现可持续增长。



附录：基于华为终端云的云原生实践案例

华为终端云服务遍及全球 170+ 个国家和地区，其全球月活用户数超过 7.3 亿，服务领域包括应用市场、电商、云空间、广告、浏览器等，是一家典型的面向消费者业务的大型企业。经过六年的云原生转型，华为终端云服务所有业务均已上云，基于超过 20 万，存储超过 3000P，积累了丰富的云原生平台构建和技术应用经验。

1 华为终端云云原生模型

为了满足华为终端不同业务的需求，终端云服务基于华为云底层技术，构建了一个云原生平台。该平台围绕复杂的基础设施能力，并基于业务场景进一步抽象建模，提供可信和易用平台产品给业务团队使用。使得业务团队不需要理解底层技术，只需要专注于业务功能逻辑代码开发，从而提升品特性版本交付效率。

华为终端云由四个平台模块组成：微服务计算平台、函数计算平台、AI 计算平台、数据计算平台，并构建了 1 个极简网络引擎和 10+ 个中台服务，支撑消费终端业务持续交付，实现了云原生平台的三大核心能力构建。



2 微服务计算平台支持业务全量微服务化

终端云服务基于华为云 CCE 服务，构筑一个全托管式微服务计算平台，支持 CSE、APIGateway、Web 等微服务和分布式任务的全托管，业务聚焦自身代码开发，屏蔽底层资源，根据流量弹性伸缩，快速完成容器化，并提供了诊断台帮助业务自助定界定位。



在构建 DevOps 的 Pipeline 系统时，创新的引入了 Iac (基础设施即代码) 和 Bac (构建即代码) 的能力，通过 Iac 和 Bac 实现全流程的自动化。



通过华为云的核心技术，如 CCE Turbo 容器、CPU 潮汐亲和、动态超分、在离线混部等，使得终端云服务的纯在线业的 CPU 利用率从 30% 提升至 40%。

3 数据计算平台重铸底层架构

终端云服务基于华为云 CCE 服务，构筑一个全托管式微服务计算平台，支持 CSE、APIGateway、Web 等微服务和分布式任务的全托管，业务聚焦自身代码开发，屏蔽底层资源，根据流量弹性伸缩，快速完成容器化，并提供了诊断台帮助业务自助定界定位。



引入华为云的统一元数据、存算分离、多活容灾架构等技术，改造后的数据基础设施，主机数量比 IDC 减少 20%+，任务减少 50%+，数据共享效率提升 80%（原来是集群间数据拷贝，现在是直接访问 OBS），人力维护成本降低 50%，3 年整体 TCO 降低 20% 左右，让数据架构具备业界先进发展水平。

在大数据开发流水线的构建过程中，创新性的引入了 Daac（接入即代码）的概念，实现数据接入自动化。



4 AI 计算平台发挥模型算力优势

终端云服务使用华为云的一站式 AI 开发平台 ModelArts 构建模型训练平台（MTP）。通过 MTP 支撑业务模型快速训练，支持训练过程可视化、自动化，提高资源利用率，让业务聚焦领域特征工程、算法、模型。



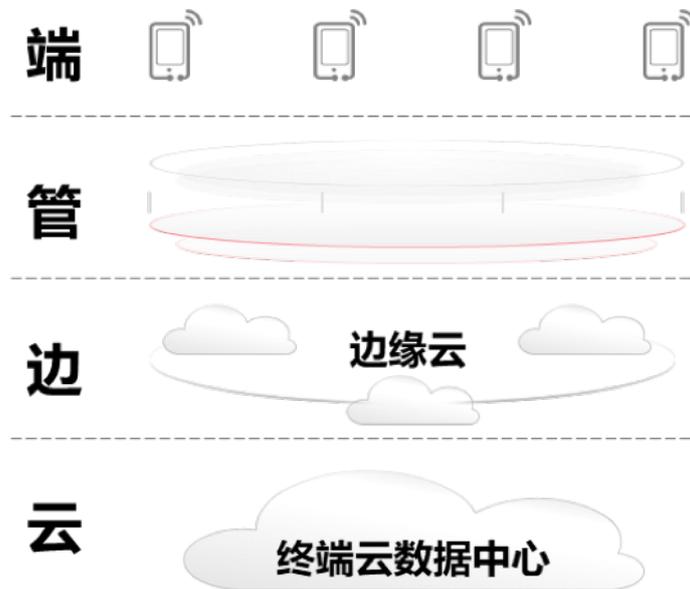
通过多 AZ、多 Region 部署，配套业务边缘机房，将模型服务部署到离用户最近的节点，如广告类推荐等对时延敏感场景。

5 极简网络引擎，实现超低时延的最优体验

通过北京、新加坡、德国、俄罗斯 4 大主站，覆盖全球用户，实现数据本地化存储，确保 GDPR 合规。通过华为云专线构筑的全球高速互联骨干环网，以及 46 个边缘数据中心，最终形成“环 - 圈 - 点”的全球部署架构，为全球用户带来了 100ms 左右的最佳体验。

通过优化后的 QUIC 协议和智能路由调度，实现网络数据稳定、安全的传输，尤其解决全球用户访问卡顿或者延迟过高的问题。

通过上述几大核心技术点以及 GRS 和 HTTP DNS 技术，终端云原生平台构建了端管边云协同的网络架构，针对流媒体通信、音视频会议、在线教育、互动直播等对实时性要求高的业务提供全球 fullmesh OverLay 网络加速服务。



最终实现总流量峰值达 5G bps，账号访问提速 13.5%，支付提速 6.9%，存储上传速率平均提升 48%。

6 典型业务场景及解决方案

1. 应用市场 (AppGallery)

应用市场，当前应用数量有 100 多万，全球月活跃用户超过 5.8 亿。

为应对超大分发量（微服务调用千亿次 / 天）和高并发（10W+tps）要求，应用市场基于极简网络，在全球分站点部署，内容类数据保持全球一套，存储在中国区主站，并通过公有云相关服务同步到全球其他站点。

在可靠性方面，应用市场采用双 AZ 双活架构，通过 ELB 服务实现业务分发和流量控制，最大并发连接可支持到 8 亿。

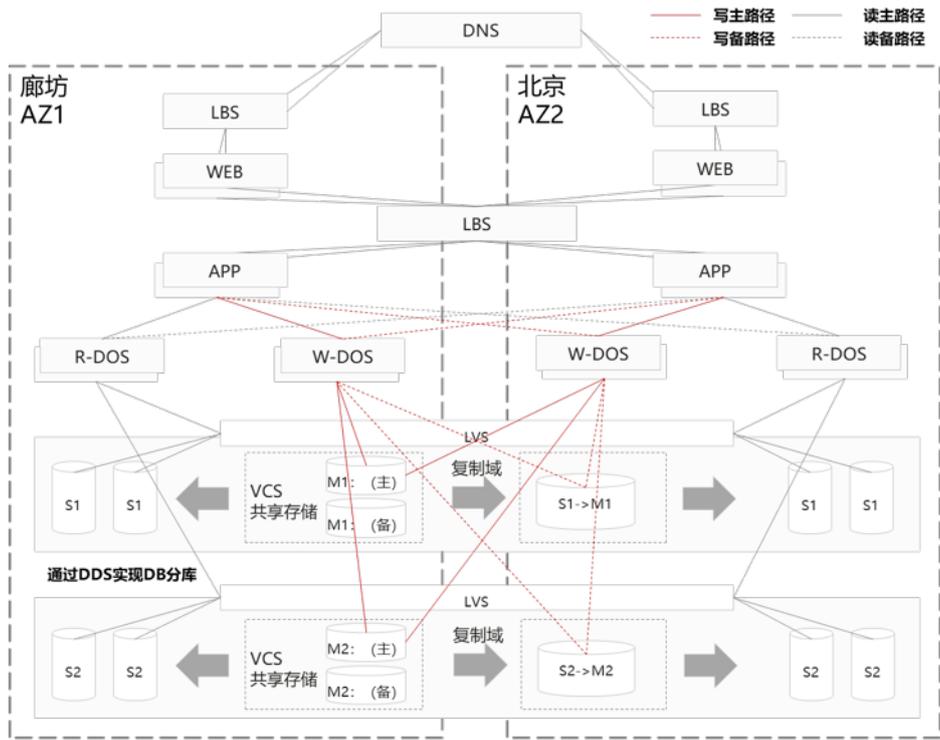
最后，为应对突发流量（比如春晚、618 等数倍或者数十倍的突发流量），应用市场引入客户端降级方案，有效削减流量浪涌峰值。并利用华为云的弹性伸缩能力，精准、快速扩容，有效解决业务浪涌时的资源诉求，保障用户体验 & 收入无损，支撑春晚红包活动，互动总量达到 639 亿次。

2. 华为商城（VMALL）

VMALL 业务的核心聚焦在首销、抢购、大促等线上销售场景，突发业务量一般为平常的 5-10 倍（甚至 100 倍）。需要确保 Vmall 业务系统的可靠性，保证故障时，不扩散、不引起整个系统的不可用。

· 在灾备方面，实现了两地三中心的系统架构

VMALL 选择在北京和廊坊两地建立了同城双活，在广州建立了异地灾备。通过 VPC 实现其他租户的隔离，并通过华为云独有的多业务平面网络设计实现与线下 ERP（企业资源计划）、财务系统的安全互访需求。通过华为云强大的弹性伸缩能力，有效支持华为商城等大型促销活动开展。



注：一般情况下AZ2作为DC复制源库，AZ1完全故障后，将AZ2将升为主库，接管业务

· 在安全方面，从网络安全，业务安全，数据安全等方面进行全面防护

通过全面的安全感知，以DDoS高防、软硬件WAF、主机、数据库安全等产品打造安全防御。以智能风控来防黄牛、防攻击、防验证码暴力破解，防控电商交易风险。另外，通过隐私数据加密存储等，确保数据传输的安全性和完整性。



3. 云空间

云空间为广大用户提供安全可靠的数据存储服务。目前，存储的数据资产超过了1900PB。数据中包含海量的个人信息，这些数据资产需要得到有效的管理和保护。同时，需要为全球用户提供快速上传，下载的优质体验，对业务时延更为敏感。

为此，终端云服务构建了三项核心技术：数据安全、可信可靠、全球触点。

· **数据安全**：端侧加密，一文一密，多级加密，实现个人数据“攻不进、取不到、解不出、丢不掉”，满足GDPR、GAPP、数据安全法的严格要求；

· **可信可靠**：采用华为 GaussDB 数据库，支持数据多副本，做到可管可控，30天数据回溯，数据不丢失；

· **全球触点**：依托极简网络实现全球触点，在保证低时延的同时实现高速上传和下载，并且能够实现秒级同步；

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

中国信息通信研究院(原工信部电信研究院)

地址: 北京市海淀区花园北路 52 号
联系电话: +86 10 62300559
邮 编 : 100191
www.caict.ac.cn

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 © 华为技术有限公司和中国信息通信研究院共同所有。保留一切权力。

非经华为技术有限公司和中国信息通信研究院共同书面同意, 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。