



全栈专属服务

介绍

文档版本 02

发布日期 2020-01-11

华为技术有限公司



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

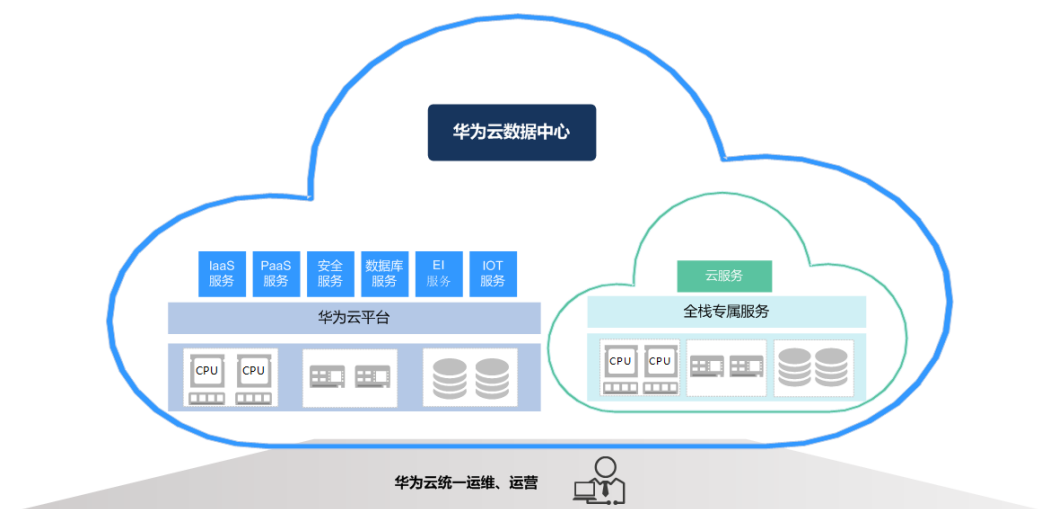
目录

1 什么是全栈专属服务.....	1
2 为什么选择全栈专属服务.....	3
3 产品架构.....	4
3.1 系统架构.....	4
3.2 网络架构.....	5
3.3 安全架构.....	7
3.4 运维管理.....	8
4 产品全景.....	10
5 应用场景.....	11
5.1 泛政府.....	11
5.2 金融行业.....	12

1 什么是全栈专属服务

华为云全栈专属服务为金融、政府和大企业客户提供计算、存储、网络和云服务管控平台完全物理隔离的专属云服务，满足客户对安全合规的较高要求。全栈专属服务与公有云统一架构，统一运维、运营，统一API接口，默认配套十个基础云服务，您还可以根据业务需求选择配套其他高级云服务。

图 1-1 全栈专属服务



公有云服务体验

- 全栈专属服务与华为云统一架构，继承公有云大规模商用成熟架构，稳定可靠、开放兼容。
- 全栈专属服务提供与华为云一致的API和管理工具，降低客户开发适配成本。
- 全栈专属服务能力与华为云同步，云服务之间互相解耦，可根据业务场景按需部署、平滑扩展、快速同步华为云能力。
 - 提供完整的IaaS专属服务。
 - 按需搭配数据库、大数据、安全服务、中间件和应用服务。

独享物理资源

全栈专属服务部署在华为云数据中心，从底层硬件到上层软件系统均支持专属独享，从而满足行业法规对业务云化的严苛规定。

由公有云统一运维、运营

全栈专属服务由华为云专业运维团队统一运维、运营，降低运维、运营成本，是政府、金融、以及大企业客户核心业务上云的优选途径。

2 为什么选择全栈专属服务

专享合规

全栈专属服务部署在华为云数据中心，用户独享计算、存储、网络以及云服务等资源，物理隔离以满足特定性能、业务应用和安全合规等要求。

技术领先

全栈专属服务能力与华为云同步，云服务之间互相解耦，可根据业务场景按需部署、平滑扩展、快速同步华为云能力，保持技术领先。

开发协同

全栈专属服务提供与华为云一致的API和管理工具，降低客户开发适配成本。

共享生态

全栈专属服务继承华为云大规模商用成熟架构，和华为云共享生态，保持一致的云服务体验。

简易运维

全栈专属服务接入华为云运维中心，由华为云专业运维团队统一运维，简化运维，降低成本。

快速上云

- 全栈专属服务采用自动化部署，可实现快速上线投入使用。
- 华为云提供多种专属迁移服务，支持业务平滑迁移上云。

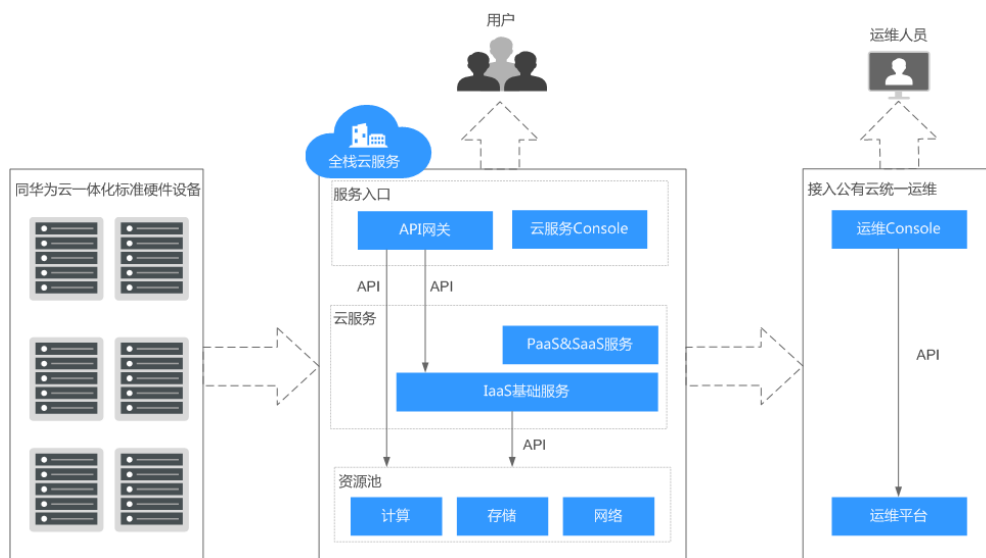
3 产品架构

3.1 系统架构

全栈专属服务架构具体说明如下：

- 基础设施：指的是硬件设备及虚拟化平台，包括计算、存储、网络和防火墙等设备。基础设施虚拟化层将物理资源转化为虚拟资源池，从而可以轻松、动态的调度各类资源。
- 云服务系统：指的是IaaS服务、PaaS服务和SaaS服务。我们为您提供Console、API或者SDK等多种使用云服务的方法，同时提供在线帮助中心。使用云服务过程中涉及的计算资源、网络资源和存储资源，都需要从基础设施虚拟资源池中申请。
- 运维平台：主要服务对象为云服务的运维管理工程师，主要提供云服务的安装和升级、虚拟化系统及物理基础设施的日常监控与告警管理、日志管理、工单管理、安全管理，成本管理等。

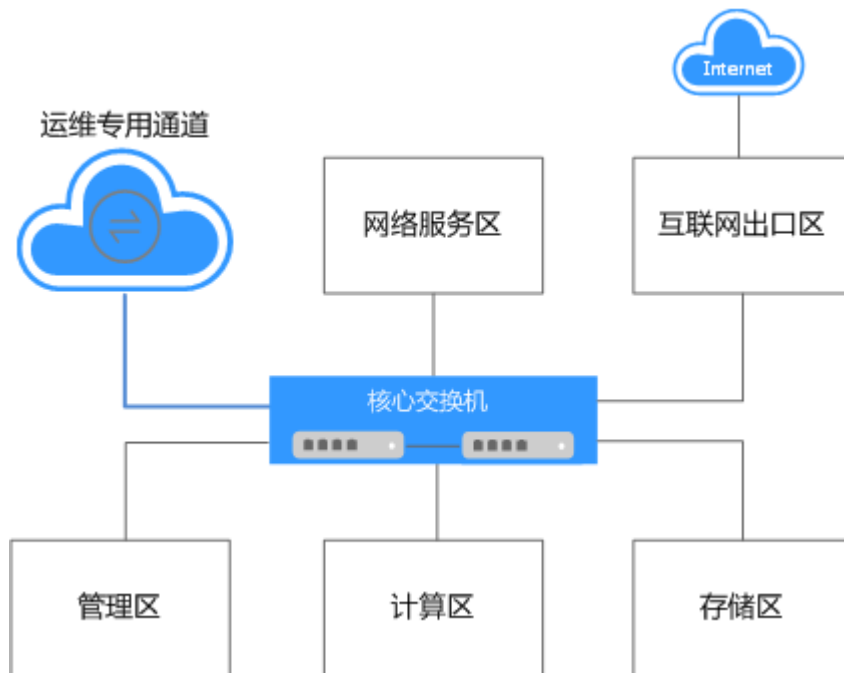
图 3-1 全栈专属服务系统架构



3.2 网络架构

全栈专属服务的网络采用“扁平化”架构设计，内部交换结构简单明了。对于服务器和存储的基础设施，网络划分为核心层和接入层。

图 3-2 全栈专属服务网络架构



组网按照逻辑功能划分为五大区域：

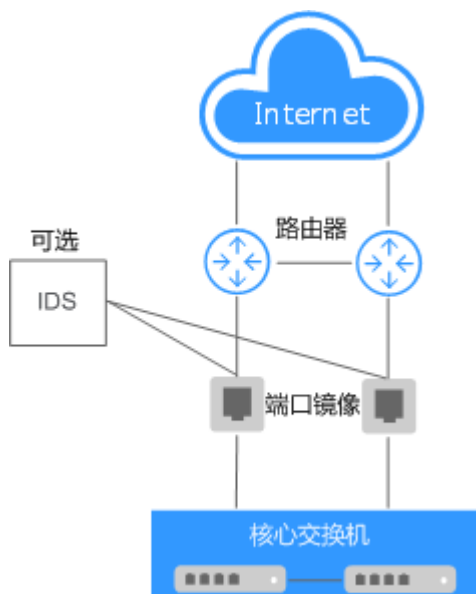
- 互联网出口区：主要功能是对接Internet线路和接入网络。
- 网络服务区：提供流量统计、防火墙、负载均衡、VPN等增值服务。
- 管理区、计算区和存储区：是实际业务所在区域，结构类似，都是服务器连接接入交换机

各个区域通过核心交换机进行互联，核心交换机由高性能交换机组成。核心机框式交换机做集群，使用“多虚一”的技术，将多台交换机在逻辑上虚拟成一台交换机，提高设备冗余，只需要一个管理IP即可对设备进行管理。

互联网出口区

互联网出口区主要功能是数据中心网络对接Internet线路和接入专线网络。

图 3-3 互联网出口区



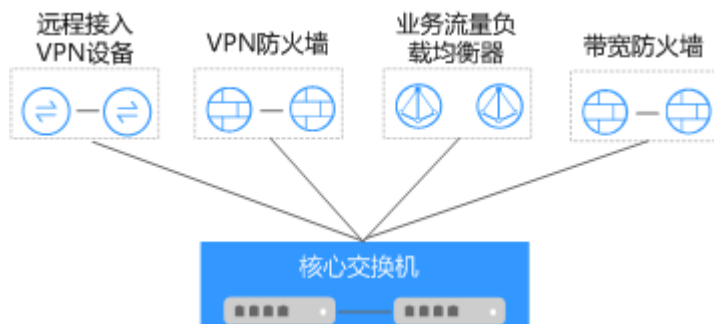
互联网出口区使用路由器与MPLS承载网络(多协议标签交换, Multi-Protocol Label Switching)与Internet网络、DCN网络(数据通信网络, Data Communication Network)等进行互联。使用BGP协议(边界网关协议, Border Gateway Protocol)或者静态路由与外部网络进行互通, 企业接入采用静态路由方式。可靠性方面通过主备链路方式实现, 即采用双线双链路接入, 每线连接一个运营商, 以此保证数据中心外联线路的可靠性。

数据中心互联网出口区防火墙为可选组件, 串联部署。串联防火墙工作采用路由模式, 分为Untrust、Trust、DMZ和Management四个区域, 各安全域通过域间策略控制安全访问。防火墙与出口路由器之间使用OSPF路由协议, 动态学习内网发布的路由条目。

网络服务区

网络服务区包括远程接入VPN设备、业务流量负载均衡器和安全防护设备防火墙。

图 3-4 网络服务区



防火墙隔离各个安全域, 对安全域之间的互访进行权限限制。防火墙提供虚拟防火墙功能, 为需要高安全需求的租户提供网络防护能力。VPN防火墙提供VPN功能, 提供用户远程加密接入, 维护和管理用户自己数据中心的资源。

负载均衡功能为租户的应用服务提供负载均衡能力。负载均衡设备提供虚拟负载均衡，各个虚拟负载均衡资源之间实现逻辑隔离。每个租户可以使用至少一个及以上的虚拟负载均衡资源，租户之间的数据配置互不影响。

多租户隔离

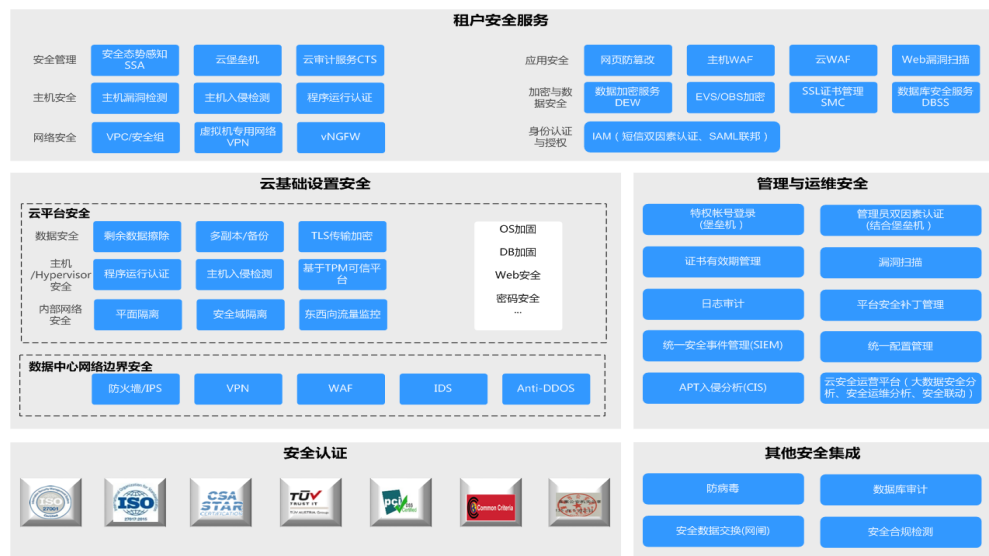
IT管理员将为每个租户部署专用的基础设施资源。在数据中心部署多租户共享的公共基础设施，能够优化资源利用率。要实现以较低成本合理利用资源，数据中心必须具备不同租户资源的隔离设计，以确保端到端的路径隔离，并满足租户的安全要求。

3.3 安全架构

全栈专属服务架构是根据业界最佳实践，并结合华为自身多年来的项目积累，提取经验中的精华进行设计的。安全架构的设计目标是全面满足用户业务的安全、可靠以及数据完整等安全需求，向客户提供全栈立体安全防御。

- 可靠性：全栈专属服务整体架构中的安全设备、安全系统的核心部件均采用高可靠性的设计方案，即采用双机热备的方式进行部署，以满足数据中心业务长期运作的安全保障需求。
- 模块化：全栈专属服务架构从物理层安全、网络安全、主机安全、应用安全、虚拟化安全、用户安全六大块内容进行设计。安全架构可以根据客户实际的需求，快速组合，形成满足用户实际需求的安全体系，更具针对性。
- 易扩展：全栈专属服务架构是为满足用户的安全需求而提出的一个指导性框架。用户可以根据该指导性框架，结合其不同时期的安全需求进行相应的安全建设，在满足用户安全需求的同时保护了用户的投资。

图 3-5 全栈专属服务安全架构



全栈专属服务的主要安全测评及认证包括：CSA STAR 金牌认证、CSA C-STAR、ISO/IEC 27001、ISO/IEC 27017、CC EAL3+、PCI DSS、公安部等保三级、中国DC联盟可信云服务认证。

3.4 运维管理

运维优势

随着云计算和虚拟化技术的发展，IT基础架构的管理向自服务管理、IT服务自动化、横向扩展的服务器、存储及网络架构管理、以及对不同技术领域的统一管理的方向转变。新一代的数据中心管理需求主要有：

- 有效的控制物理服务器成本
- 降低数据中心运营成本
- 降低管理成本
- 降低数据中心能耗
- 解决数据中心业务上线周期长的现状
- 兼顾不同厂商物理、虚拟资源统一管理
- 提高数据中心基础架构设备利用率
- 解决关键应用故障恢复和灾难保护
- 简化运维

为适应新一代数据中心管理需求，全栈专属服务在运维管理方面有以下优势：

- 端到端的自助服务管理
- 统一的业务运营和运维管理
- 自动化的流程编排及资源分配、应用部署
- 多数据中心的统一管理
- 支持多种硬件设备、软件的集成服务
- 服务器、网络、存储、数据库、中间件等的运维管理

运维架构

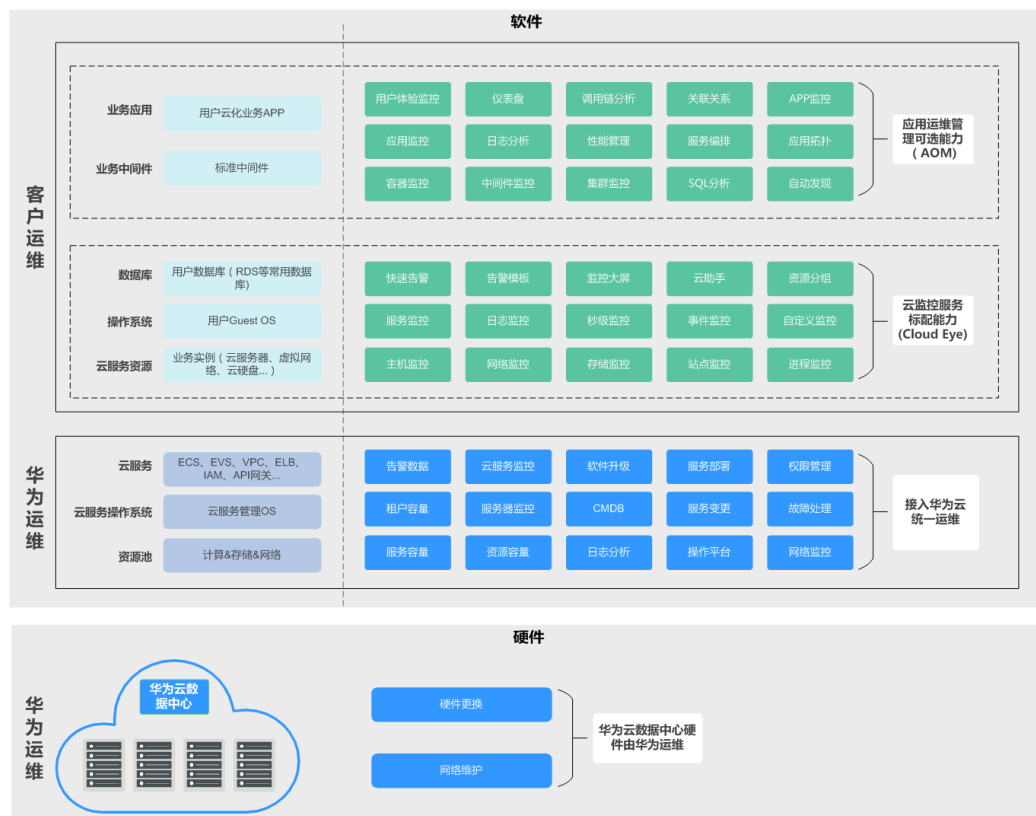
全栈专属服务的运维包括硬件和软件两部分，运维架构如图3-6所示。

- 硬件：全栈专属服务部署在华为云数据中心，硬件更换及网络维护等工作需要由华为云统一运维。
- 软件：软件运维需要客户和华为运维团队共同承担。
 - 客户侧：客户侧运维标配能力由云监控（Cloud Eye）提供，主要针对用户数据库、用户操作系统以及云服务资源等。云监控为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。云监控不需要开通，监控服务会根据您创建的资源自动启动，您可直接到云监控查看资源的运行状态并设置告警规则。

客户侧运维可选能力由应用运维管理（Application Operations Management, AOM）提供，主要针对用户云化业务APP以及业务中间件等。AOM作为云上应用的一站式立体化运维管理平台，可以实现对云主机、存储、网络、WEB容器、docker、kubernetes等应用运行环境的深入监控并进行集中统一的可视化管理，能够有效预防问题的产生及快速帮助应用运维人员定位故障，降低运维成本。

- 华为侧：提供云平台的远程运维服务，相关服务内容包括：监报告警、部署变更、故障处理、网络管理、运维数据分析等，提供7 × 24小时全时监控，保障客户业务稳定运行。同时，助力客户从基础设施运维中解决出来，聚焦核心业务，成就客户价值。

图 3-6 全栈专属服务运维架构



4 产品全景

全栈专属服务将华为云丰富的云服务持续提供给客户，满足客户不同场景的需求，并且服务能力同步华为云持续迭代升级。

- **基础服务**
提供基础计算、存储、网络以及管理服务。包括：弹性云服务器、裸金属服务器、弹性伸缩服务、云硬盘、云硬盘备份、对象存储服务、文件存储服务、云服务器备份、虚拟私有云、弹性负载均衡、VPN服务、NAT网关、域名解析服务、统一身份认证、云审计服务、云监控服务等。
- **数据库服务**
提供多种数据库引擎。具体包括：云数据库Mysql、云数据库PostgreSQL、文档数据库服务、分布式数据库中间件等。
- **大数据服务**
针对不同场景提供多种大数据服务。包括：MapReduce服务、数据仓库服务、图引擎服务、数据湖工厂、云搜索服务、云数据迁移等。
- **中间件和应用服务**
提供应用中间件、帮助客户应用实现容器化、微服务架构升级改造。包括：应用管理与运维平台、容器镜像服务、云容器引擎、应用运维管理、应用性能管理、分布式消息服务、应用编排服务、分布式缓存服务等。
- **安全服务**
提供多种安全服务，保障客户应用与数据的安全。包括：安全中心、流量清洗、数据加密服务、数据库安全服务等。

5 应用场景

全栈专属服务可以满足金融、泛政府、大企业等核心业务上云时，对数据隔离部署、安全等保合规的需求。在确保用户数据安全的情况下，快速同步华为云EI、PaaS、数据库、大数据等创新服务，并由华为云向客户提供专业统一运维能力。

5.1 泛政府

《推进“互联网+政务服务”开展信息惠民试点实施方案》（国务院[2016] 23号）文件中提出：以数据为中心驱动政府治理能力提升，通过以省、市、区县为单位的政务云项目和政务大数据项目，实现打破信息孤岛，变“群众跑腿”为“信息跑路”，变“群众来回跑”为“部门协同办”，变被动服务为主动服务。

2016年12月国务院正式发布《“十三五”国家信息化规划》，其中确定了新型智慧城市的建设行动目标，通过人工智能AI，大数据，物联网等新技术转变城市发展和建设方式，优化整合地方资源，有效进行城市治理，提供高质量的公共服务，解决或缓解各种问题，促进城市可持续性发展。新型智慧城市建设涉及精准治理、惠民服务、生态宜居、产业与经济服务的相关泛政府部门，包括经信委、交通、国土、税务、社保、水利、水务、供暖、环保、燃气、发改委以及招商局等。

方案亮点

- 自主可控：云平台部署在华为云数据中心，华为完全自主知识产权，国产软硬件一体化交付，自主可控。
- 安全合规：内网区与互联网区完全隔离，提供从基础设施层到外联接入，运维管理，租户云服务层的全栈端到端立体安全防御，满足等保安全合规的要求。
- 全栈云服务能力：完全继承华为公有云丰富的云服务能力，提供智慧城市各类应用所需的云服务平台，包括IaaS、PaaS及EI人工智能等，并跟随华为云迭代演进。
- 云服务按需选取，平滑扩展：云服务之间独立解耦，可按业务实际需求选装云服务，轻量化起步，并且后期支持平滑扩展。

客户价值

- 统一规划建设，统一运维运营，降低投资成本。
- 全栈云服务能力及各类智能体，助力智慧城市善政、惠民、兴业。
- 物理隔离、资源独享，满足安全合规的要求。

5.2 金融行业

中国金融业信息技术“十三五”发展规划（2017）指出：支持实力较强的机构独立或者联合建设金融业云服务平台，面向同业特别是中小金融机构提供云服务，提高行业资源使用效率。

多家银行系金融科技公司成立，以行业云方式，对信息建设、业务流程、金融应用软件开发等能力做输出。服务从集团内部到中小银行、基金、保险、证券、信托等金融机构，再到其他非金融企业。云、大数据、区块链、人工智能等金融科技日益成为各行业云核心竞争力重要关键因素。

方案亮点

- 具备公有云丰富的云服务能力，并能够安全隔离，资源独享。
- 接入华为云实现统一运营运维，大幅降低节运维复杂度和成本，客户可聚焦上层业务可靠性。
- 从芯到云，立体安全防御，运维面、管理面和租户面安全隔离，满足等保三级标准。
- 具备独立的门户网站，独立的IAM认证系统。

客户价值

- 安全合规：全栈专属服务全栈隔离，满足金融、保险行业高安全合规要求。
- 快速创新：全栈专属服务提供稳定丰富的IaaS和PaaS能力，协助客户进行联合创新。
- 快速交付：交付工期短，服务版本升级快，能够快速同步公有云的最新能力。