智能边缘云

产品介绍

文档版本 10

发布日期 2024-08-09

华为技术有限公司

商标声明


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暗示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

安全声明

产品生命周期政策

华为公司对产品生命周期的规定以“产品生命周期终止政策”为准，该政策的详细内容请参见如下网址：
https://support.huawei.com/ecolumnsweb/zh/warranty-policy

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

华为初始证书权责说明

华为公司对随设备出厂的初始数字证书，发布了“华为设备初始数字证书权责说明”，该说明的详细内容请参见如下网址：
https://support.huawei.com/enterprise/zh/bulletins-service/ENEWS2000015766

华为企业业务最终用户许可协议(EULA)

本最终用户许可协议是最终用户（个人、公司或其他任何实体）与华为公司就华为软件的使用所缔结的协议。最终用户对华为软件的使用受本协议约束，该协议的详细内容请参见如下网址：
https://e.huawei.com/cn/about/eula

产品资料生命周期策略

华为公司针对随产品版本发布的售后客户资料（产品资料），发布了“产品资料生命周期策略”，该策略的详细内容请参见如下网址：
https://support.huawei.com/enterprise/zh/bulletins-website/ENEWS2000017760

目 录

1 什么是智能边缘云

边缘计算

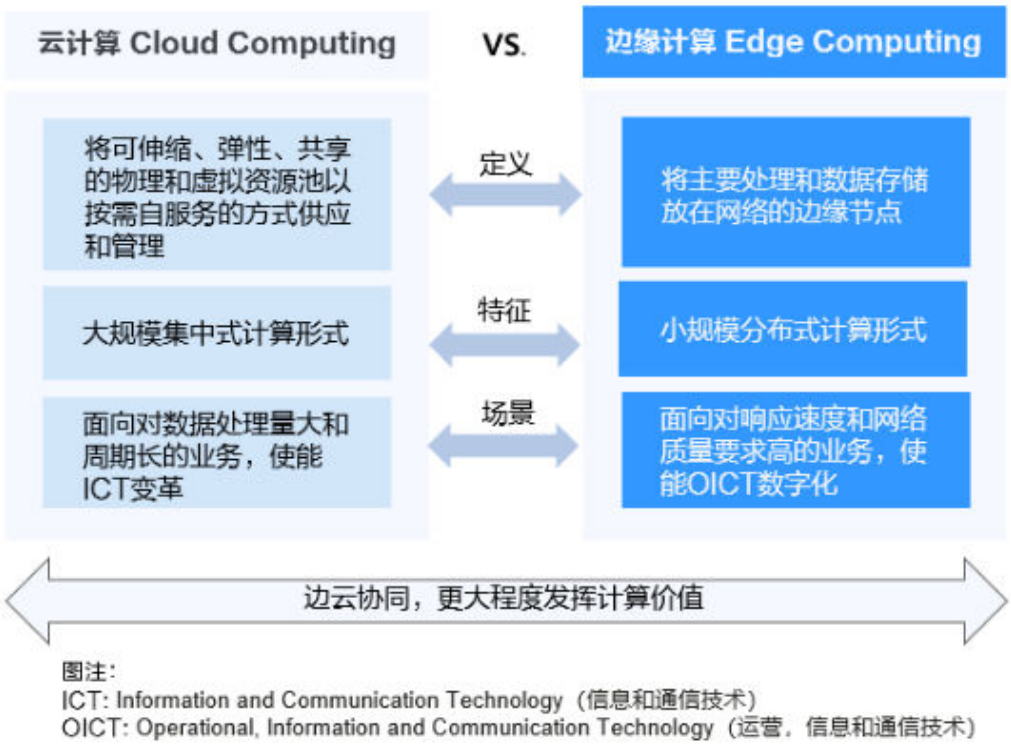
迈入5G和AI时代，新型业务如增强现实AR、虚拟现实VR、互动直播、自动驾驶、智能制造等应运而生。以上这些业务场景对时延和网络带宽有着强烈诉求，而在传统的集中式云计算场景中，所有数据都集中存储在大型数据中心。由于地理位置和网络传输的限制，无法满足新型业务的低时延、高带宽等要求。

- 网络高时延：传统云计算无法即时处理和分析新型业务产生的数据，导致应用终端获得的响应慢，体验差。
- 带宽高成本：新型业务的应用终端产生的数据传回云端将消耗更高的网络带宽，导致服务厂商需要支付高昂的网络成本。
- 数据合规性：新型业务数据存储在云端，无法满足企业对敏感数据本地化存储的要求，直接影响企业数据上云的策略。

面对传统集中式云计算的固有局限性，边缘计算成为应对新型业务和数据合规业务的较好选择。边缘计算通过在靠近终端应用的位置建立站点，最大限度的将集中式云计算的能力延伸到边缘侧，有效解决以上的时延和带宽问题。

您可以参考**图1-1**了解更多关于云计算和边缘计算的区别。

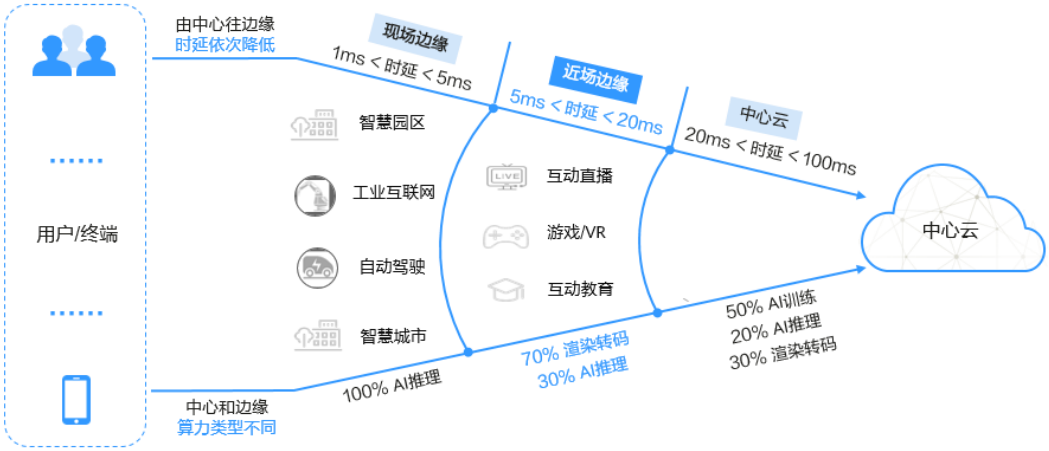
图 1-1 云计算和边缘计算



从广义上讲，云计算囊括边缘计算，边缘计算是云计算的扩展，二者为互补而非替代关系。只有云计算与边缘计算相互协同（简称边云协同），才能更好的满足各种应用场景下的不同需求。

通过图1-2进一步了解边缘计算的范畴。

图 1-2 边缘计算的范畴



按照从用户/终端到中心云的距离，可以划分3个“圈”：

- 第一个“圈”是现场边缘，覆盖1~5ms时延范围，算力以AI推理为主，主要面向自动驾驶，工业互联网等实时性业务。

- 第二个“圈”是近场边缘，覆盖5~20ms时延范围，算力以渲染为主，同时还有一部分推理，主要面向视频场景。
- 第三个“圈”是传统的公有云（也称为中心云），覆盖20~100ms时延范围，用于承载未下沉到边缘的业务，例如海量的数据存储，挖掘，训练等。

面向近场边缘和现场边缘场景，华为云分别推出了**智能边缘云**（Intelligent EdgeCloud，IEC）和**智能边缘小站**（CloudPond）两款产品。

- **智能边缘云**IEC：提供广域覆盖的分布式边缘云，用于客户就近灵活部署业务。
- **智能边缘小站**CloudPond：提供部署在用户数据中心的软硬件一体的边缘解决方案。

除了上述两款产品，华为云还推出了面向客户业务现场场景的**智能边缘平台**（Intelligent EdgeFabric，IEF）产品。作为基于云原生技术构建的边云协同操作系统，IEF可运行在多种边缘设备上，将丰富的AI、IoT（Internet of Things）及数据分析等智能应用以轻量化的方式从云端部署到边缘，满足用户对智能应用边云协同的业务诉求。

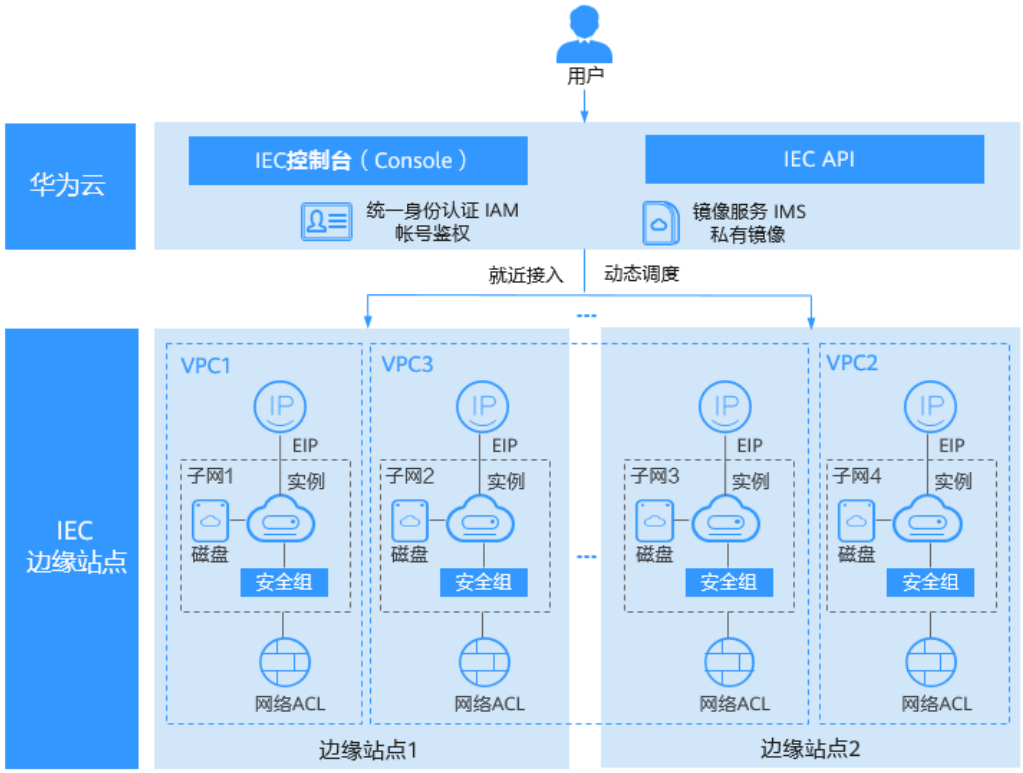
什么是智能边缘云

智能边缘云（IEC）部署在距离企业和热点用户区域更近的位置，具有与中心云一致的体验，为时延敏感型业务如互动娱乐、在线教育、媒体创作等提供低于10ms的时延体验，支持全局智能管理及调度。

您可以通过**IEC和华为云的关系是什么？**了解更多详情。

IEC产品架构如**图1-3**所示。

图 1-3 IEC 产品架构



- IEC控制台和API部署在华为云中，提供边缘业务管理，支持跨边缘站点的统一算力、网络、存储、镜像配置及管理。
- IEC使用华为云统一身份认证（Identity and Access Management，IAM）服务提供账号鉴权功能，使用华为云镜像服务（Image Management Service，IMS）提供创建实例需要的私有镜像。

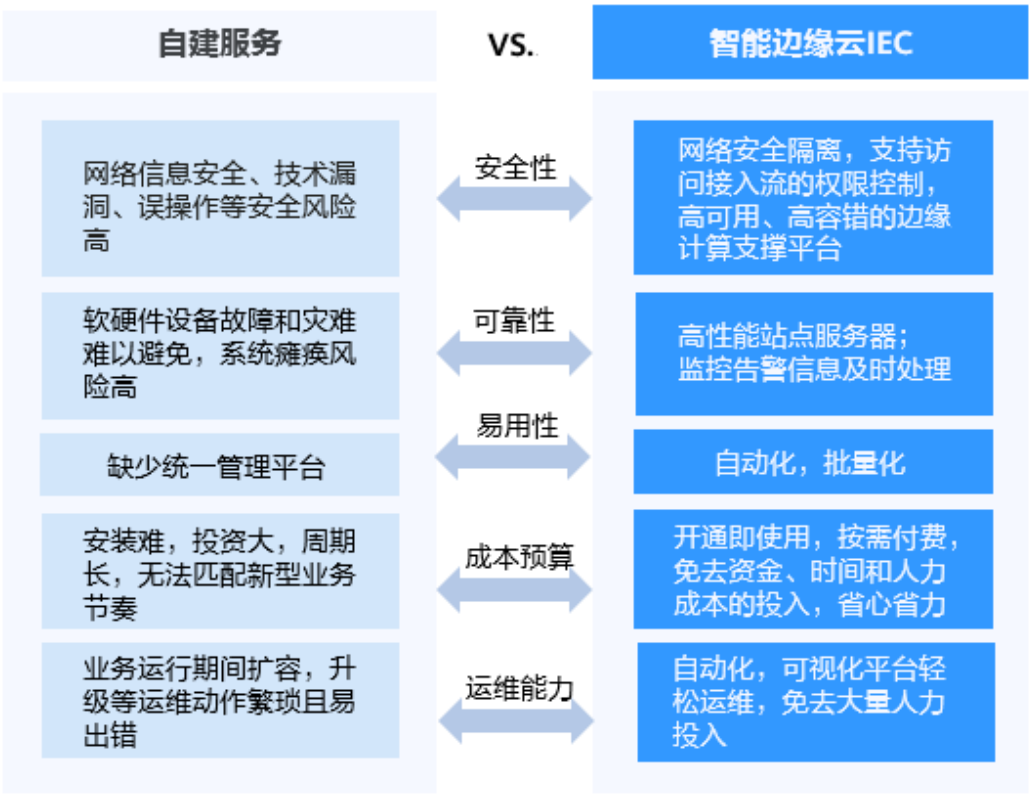
  需要注意的是除了IAM和IMS之外，其余架构图中提到的虚拟私有云（Virtual Private Cloud，VPC），弹性公网IP（Elastic IP，EIP），实例、子网、磁盘、安全组、网络ACL（Access Control Lists，访问控制列表）等组件均属于IEC范畴，与华为云上的云服务，包括弹性云服务器（Elastic Cloud Server，ECS），云硬盘（Elastic Volume Service，EVS）服务，虚拟私有云VPC虽然功能类似，但没有关联关系，各自承载不同的业务。举例说明，通过IEC控制台或者API创建的实例仅归属于华为云服务IEC业务范畴，与通过华为云服务ECS创建的实例没有关联关系。IEC上创建的实例不能通过ECS管理，ECS上创建的实例也不能通过IEC管理。
- IEC在中国大陆建立了多个边缘站点，提供物理隔离的资源池，提供多元算力、存储和网络的能力。
- 边缘站点之间物理隔离，所以归属于不同边缘站点的子网之间不连通；VPC之间逻辑隔离，所以归属于不同VPC的子网之间不连通。如**图1-3**，四个子网彼此互不连通。
- 用户在IEC控制台或者通过API**创建边缘业务**后，系统自动将用户业务就近接入边缘站点。通过动态调度，实现降低网络时延等优势。

详细的各组件介绍内容和配置操作请参见《**智能边缘云用户指南**》。

为什么选择智能边缘云

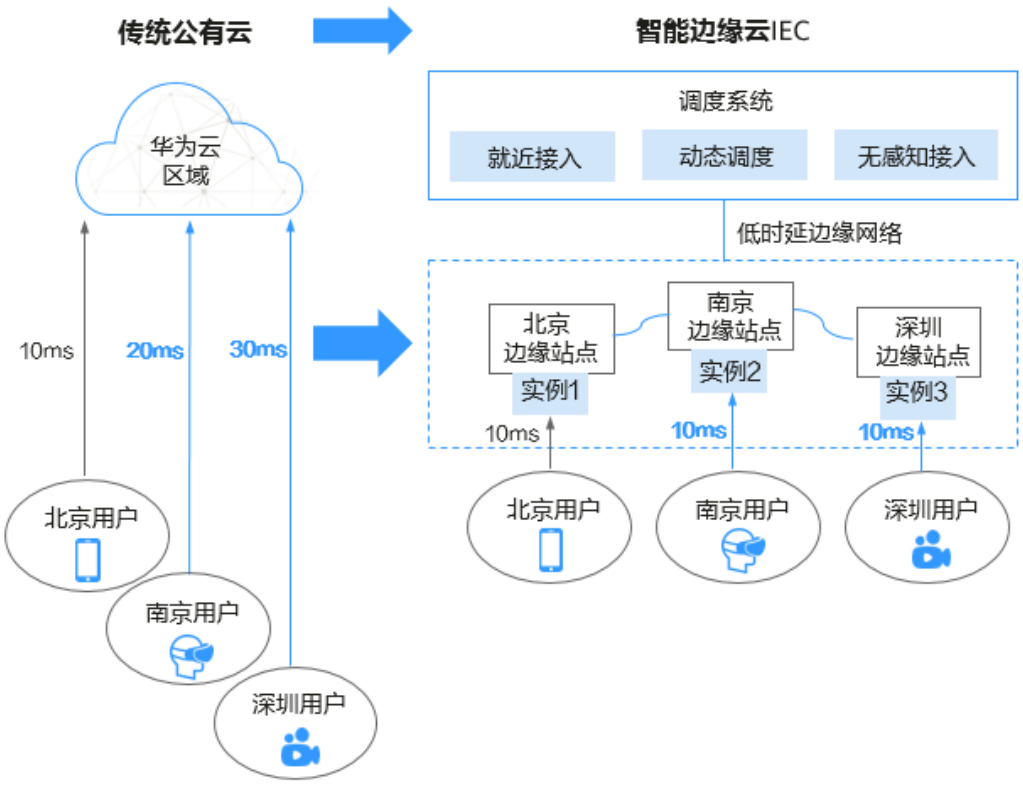
自建服务存在的成本高，安全风险大等诸多劣势已无法满足新型业务的高要求。**图1-4**向您详细展示了IEC与自建服务的优劣势对比。

图 1-4 IEC 与自建服务对比



上一部分**边缘计算**中我们提到华为云边缘计算的范畴，您可以通过**图1-5**进一步了解IEC在面对边缘侧业务下相比传统集中式公有云在降低网络时延方面的优势。

图 1-5 IEC 与传统公有云对比



了解更多选择IEC的优势，请参见**2 产品优势**。

IEC 与相关产品区别

华为提供多种云化产品，您可以通过**表1-1**了解智能边缘云（IEC）和智能边缘小站（CloudPond）、智能边缘平台（Intelligent EdgeFabric，IEF）、IoT边缘（IoT Edge）、内容分发网络（Content Delivery Network，CDN）的区别，以便根据使用场景综合选择。

表 1-1 IEC 与相关产品区别

产品名称	IEC	CloudPond	IEF	IoT Edge	CDN
定位	构建广域覆盖的分布式边缘云	构建部署在用户数据中心的边缘小站	基于云原生技术构建的边云协同操作系统	物联网边缘“小脑”	构建在现有互联网基础之上的一层智能虚拟网络

能力	提供多元算力，满足多种业务需求，用户通过就近部署业务，有效降低网络时延	将华为云可用区拉远，在用户数据中心提供公有云服务，满足数据本地化需求，降低业务延迟	从云端下发应用到边缘，帮助用户在云端对边缘应用进行管理，解决应用“推送/简化部署”到边缘的问题	聚焦边缘设备管理，就近提供计算和智能服务，满足行业在实时业务、应用智能等方面的需求	提高用户访问网站的响应速度与网站的可用性，解决网络带宽小、用户访问量大、网点分布不均等问题
适用场景	直播、边缘渲染加速、云游戏等	创新业务部署、传统业务上云、数据本地留存	园区视频分析、工业视觉、工业预测性维护等	智慧园区、智慧交通、智能制造等	网站加速、文件下载加速等内容加速
部署位置	运营商机房	用户数据中心	任意位置	任意位置	运营商机房

IEC使用过程和其他一些云服务有依赖或协作关系，详情请参见**12 与其他云服务的关系**。

访问方式

您可以通过控制台和API两种方式访问IEC。

表 1-2 访问方式

方式	说明	入口/指导
控制台	提供直观的Web化管理界面，简化您的操作。	请参见《**智能边缘云快速入门**》
API	提供基于HTTPS请求的API，方便您将IEC集成到第三方系统，用于二次开发。	请参见《**智能边缘云API参考**》。

2 产品优势

- 广域覆盖：基于覆盖中国大陆主要省市和主流运营商的优质节点资源进行部署，用户可以将时延敏感业务就近接入部署，保证确定性时延，提升业务体验。
- 多样算力：面向丰富的边缘业务场景，提供多样化的算力类型，用户可以根据业务要求选择合适的算力。
- 卓越性能：基于华为云擎天架构打造，提供软硬结合的卓越性能。单实例包转发性能最高可达千万级pps，基于昇腾AI卡的推理性能是业界主流处理卡性能的2倍。
- 边云协同：提供核心的计算、存储、网络服务能力，使用户可以更快的构建场景化的边缘解决方案。

3 应用场景

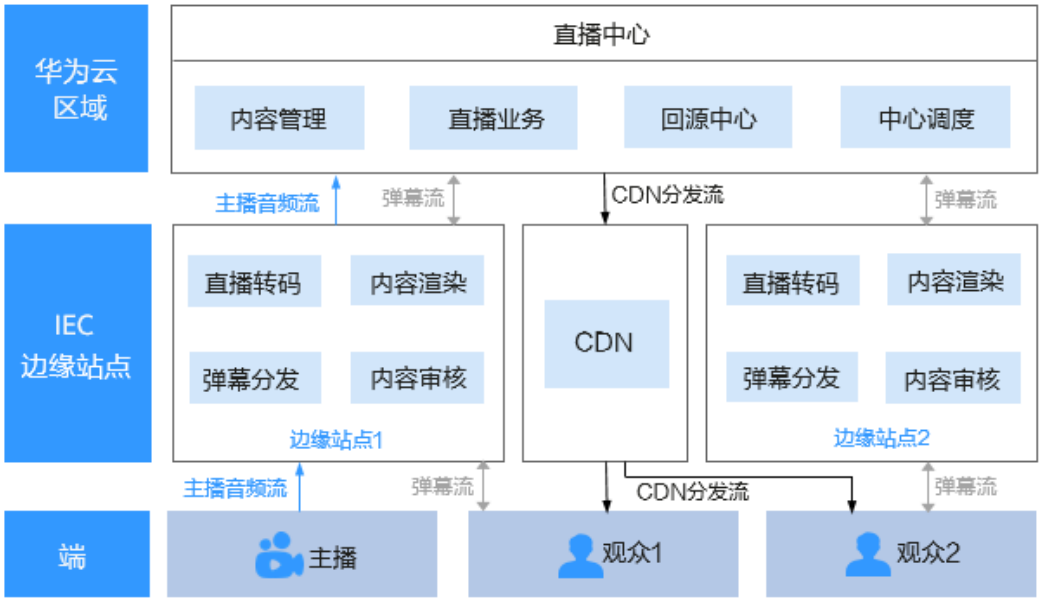
IEC主要面向**互动直播**、**在线教育**、**应用加速**和**自建CDN**等应用场景。

相关链接：

- **使用IEC需不需要对当前业务进行改造？如何改造？**
- **如何将业务数据迁移到IEC？**

互动直播

图 3-1 互动直播



场景特点

将音视频转码、弹幕分发、内容审核等处理能力部署在边缘站点，可以显著提升业务处理质量，优化响应效率，降低流量成本。

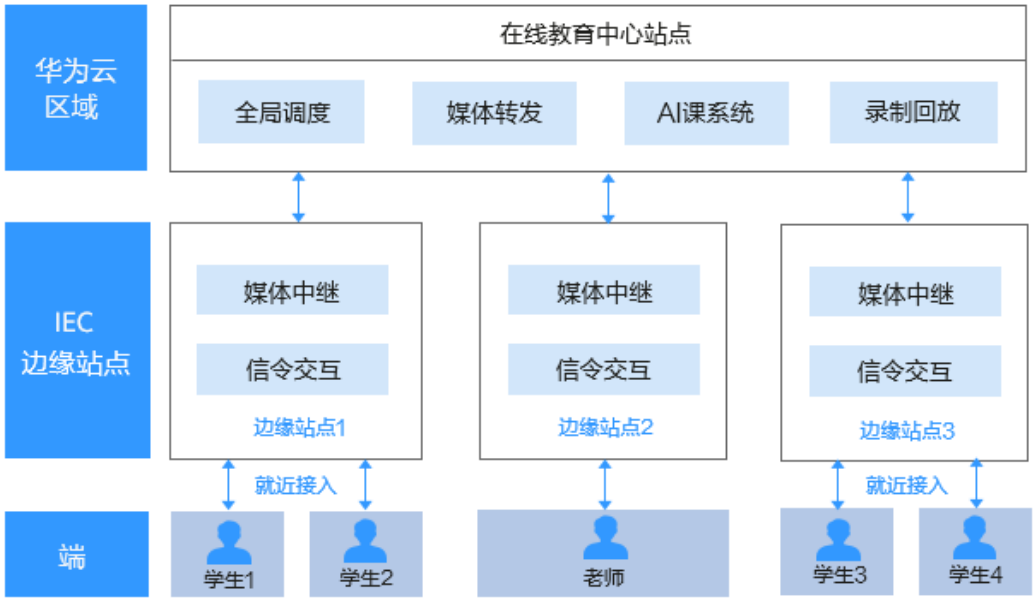
优势

- 多样算力：提供GPU、AI等多样化算力，提升高清转码、内容审核等场景处理的性价比。

- 流量本地化：优化弹幕业务的成本。

在线教育

图 3-2 在线教育



场景特点

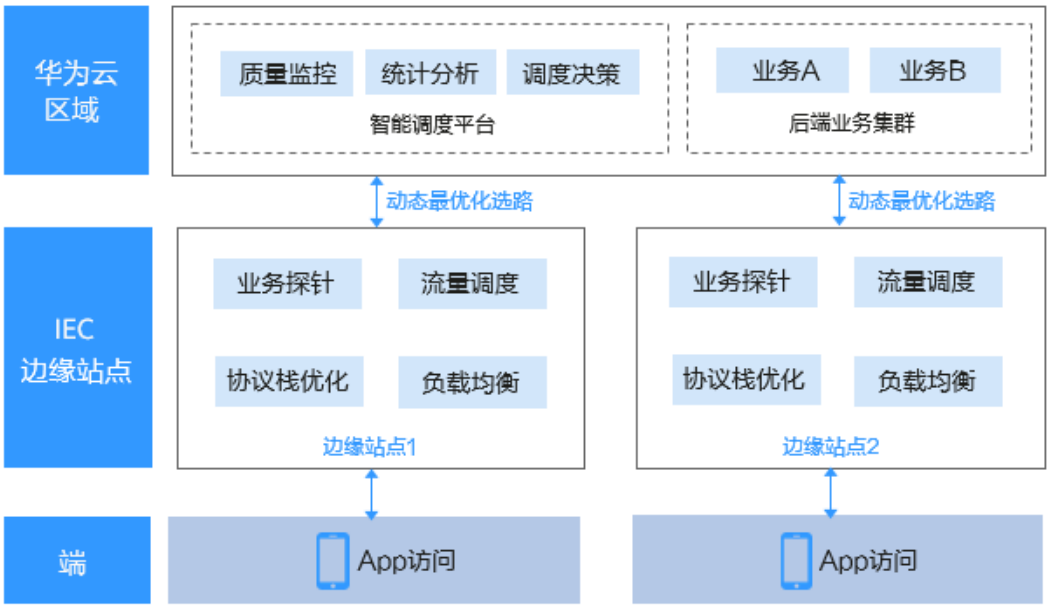
为老师与学生提供实时互动的视频教育体验，需要在边缘侧提供区域间稳定互联的低时延通信链路，从而有效支撑师生间多点对多点实时互动。

优势

- 广域覆盖：遍布中国大陆各主要地域和省市的站点布局。
- 边云网络：基于时延和丢包率实时探测的动态网络选路。

应用加速

图 3-3 应用加速



场景特点

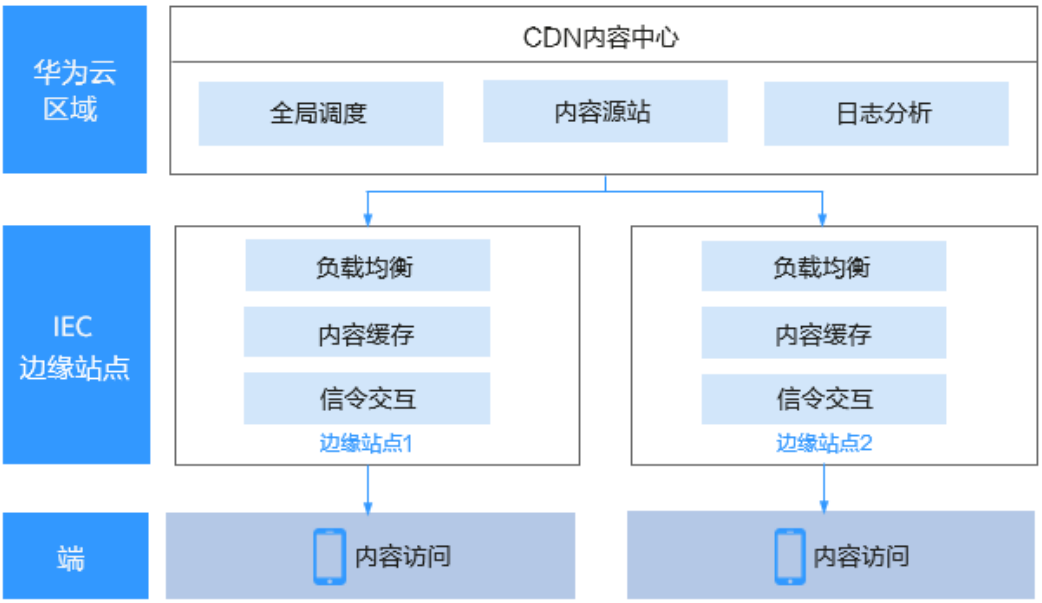
应用加速场景如游戏加速、App加速等，需要根据端到端时延要求，选择靠近最终用户的边缘节点，并通过优化端到端的网络选路，降低端到端时延。

优势

- 弹性扩展：资源按需使用，批量业务创建，有效应对业务的突发增量需求。
- 高效运维：多站点资源的统一管理，基于API的服务管控和监控运维。

自建 CDN

图 3-4 自建 CDN



场景特点

当前互联网企业或服务商自建CDN网络时，大多采取租赁IDC的模式，需要建设和维护遍布多地域的大量站点。IEC提供覆盖中国大陆的边缘算力网络，以及全局管理和自动化运维能力，帮助用户快速搭建和维护CDN网络。

优势

- 广域覆盖：遍布中国大陆各主要地域和省市的站点布局。
- 高性价比：提供内容分发场景所需的含NVMe的高性能本地存储型实例。

4 约束与限制

本章节主要介绍IEC系统和功能级别的约束与限制，参数级别的约束与限制请参见《**智能边缘云用户指南**》的相应章节。

边缘业务

- 系统默认一个华为云账号最多创建10个边缘业务。如果您需要创建更多个边缘业务，请**申请扩大配额**。
- 系统默认一个华为云账号在创建边缘业务时最多选择在10个区域购买实例。如果需要在同一个边缘业务下购买更多个区域的实例，您可以在边缘业务创建完成后，通过扩容边缘业务的方式新增对应区域的实例。

边缘实例

- IEC暂不支持通过VNC（Virtual Network Console，虚拟网络控制台）方式登录边缘实例，请使用远程连接工具登录实例。
- 系统默认一个华为云账号最多创建300台边缘实例，如果您需要创建更多个边缘实例，请**申请扩大配额**。一次最多可以创建50台边缘实例。
- 系统默认一个华为云账号最多创建边缘实例的内存（Random Access Memory，RAM）容量为100GB，vCPU（Virtual Central Processing Unit，虚拟处理器）为100个。如果您需要更多配额，请**申请扩大配额**。

实例规格

- 通用计算增强型（C6、C6s）
- AI加速型（Ai1）
- 磁盘增强型（D3i）

详细规格请以软件界面提供的为准。

边缘硬盘

- 当前IEC提供的硬盘和实例绑定使用，不支持独立挂载或者卸载。当删除实例时，硬盘同时一并被删除。
- 系统默认一个华为云账号最多创建50个边缘硬盘。对于单个边缘实例，系统盘容量最大为100GB，数据盘容量最大为500GB，数据盘数量最多为2个。

边缘镜像

- 当前IEC仅支持在华北-北京四[cn-north-4]的华为云区域通过镜像服务创建边缘私有镜像。
- 对于IAM用户通过镜像服务创建边缘私有镜像，需要账号为该IAM用户同时赋予**IEC FullAccess权限**和**华北-北京四[cn-north-4]区域的IAM ReadOnlyAccess权限**。
- 系统默认一个华为云账号最多创建50个边缘私有镜像（从边缘实例和从镜像服务创建合计）。如果您需要创建更多个边缘私有镜像，请**申请扩大配额**。

说明

IEC场景下不支持windows公共镜像；windows私有镜像仅支持创建虚拟机，但不支持对虚拟机进行激活。

边缘虚拟私有云

- 系统默认一个华为云账号最多创建50个虚拟私有云。如果您需要创建更多个虚拟私有云，请**申请扩大配额**。
- 不同虚拟私有云之间逻辑隔离，网络不连通。不同边缘站点之间物理隔离，网络不连通。

边缘路由和路由表

- 系统默认一个VPC下最多创建10个自定义路由表。如果您需要创建更多个自定义路由表，请**申请扩大配额**。
- 每个路由表最多添加200个路由。
- 一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。
- 系统路由不能修改和删除。
- 通过自定义路由访问Internet网络时，目的地址配置为默认0.0.0.0/0，不能配置为具体的公网网段，下一跳为本VPC内绑定了EIP的边缘实例、绑定了EIP的虚拟IP或互联网网关地址。

边缘带宽

- 创建弹性公网IP后，当使用该弹性公网IP的单条运营商线路不存在共享带宽时，系统自动为该线路分配一条共享带宽。不同线路使用不同的带宽。
- 系统默认一个华为云账号为一个共享带宽最多添加150个弹性公网IP。如果您需要添加更多个弹性公网IP，请**申请扩大配额**。

边缘弹性公网 IP

同一个弹性公网IP只能绑定到同一个边缘站点下的一个计算实例或者一个虚拟IP上。

边缘安全组

- 系统默认一个华为云账号最多创建200个安全组。如果您需要创建更多个安全组，请**申请扩大配额**。
- 由于归属于不同虚拟私有云的多个实例网络不连通，则为同一个安全组下归属于不同的虚拟私有云的多个实例配置网络连通的访问规则是不生效的。
- 由于归属于不同边缘站点的多个子网之间网络不连通，则为安全组配置跨站点多个子网连通的访问规则是不生效的。

- 系统默认一个华为云账号最多创建10000个安全组规则。如果您需要创建更多个安全组规则，请**申请扩大配额**。

边缘网络 ACL

- 每个网络ACL都包含一组默认规则，如下所示：
  - 默认放通同一站点下同一子网内的流量。
  - 默认放通目的IP地址为255.255.255.255/32的广播报文。用于配置主机的启动信息。
  - 默认放通目的网段为224.0.0.0/24的组播报文。供路由协议使用。
  - 默认放通目的IP地址为169.254.169.254/32，TCP端口为80的metadata报文。用于获取元数据。
  - 默认放通公共服务预留网段资源的报文，例如目的网段为100.125.0.0/16的报文。
  - 除上述默认放通的流量外，其余出入子网的流量全部拒绝，如**表4-1**所示。该规则不能修改和删除。

    表 4-1 网络 ACL 默认规则

方向	优先级	动作	协议	源地址	目的地址	说明
入方向	*	拒绝	全部	0.0.0.0/0	0.0.0.0/0	拒绝所有入站流量
出方向	*	拒绝	全部	0.0.0.0/0	0.0.0.0/0	拒绝所有出站流量

- 网络连通性：
  - 由于归属于不同虚拟私有云的多个子网网络不连通，则为同一个网络ACL下归属于不同的虚拟私有云的多个子网配置网络连通的访问规则是不生效的。
  - 由于归属于不同边缘站点的多个子网之间网络不连通，则为网络ACL配置跨站点多个子网连通的访问规则是不生效的。
- 规则优先级：
  - 网络ACL规则的优先级使用“优先级”值来表示，优先级的值越小，优先级越高，最先应用。优先级的值为“*”的是默认规则，优先级最低。
  - 多个网络ACL规则冲突，优先级高的规则优先生效。如果某个规则需要优先或落后生效，可在对应规则（需要优先或落后于某个规则生效的规则）前面或后面插入此规则。

5 实例规格

您可以通过本节快速浏览在售的所有边缘实例规格清单。

通用计算增强型

表 5-1 C6 型边缘实例的规格

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	网卡个数上限	虚拟化类型
c6.large.2	2	4	4/1.2	40	2	2	KVM
c6.large.4	2	8	4/1.2	40	2	2	KVM
c6.xlarge.2	4	8	8/2.4	80	2	3	KVM
c6.xlarge.4	4	16	8/2.4	80	2	3	KVM
c6.2xlarge.2	8	16	15/4.5	150	4	4	KVM
c6.2xlarge.4	8	32	15/4.5	150	4	4	KVM
c6.3xlarge.2	12	24	17/7	200	4	6	KVM
c6.3xlarge.4	12	48	17/7	200	4	6	KVM
c6.4xlarge.2	16	32	20/9	280	8	8	KVM
c6.4xlarge.4	16	64	20/9	280	8	8	KVM

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	网卡个数上限	虚拟化类型
c6.6xlarge.2	24	48	25/14	400	8	8	KVM
c6.6xlarge.4	24	96	25/14	400	8	8	KVM
c6.8xlarge.2	32	64	30/18	550	16	8	KVM
c6.8xlarge.4	32	128	30/18	550	16	8	KVM
c6.16xlarge.2	64	128	40/36	1000	32	8	KVM
c6.16xlarge.4	64	256	40/36	1000	32	8	KVM

表 5-2 C6s 型边缘实例的规格

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	网卡个数上限	虚拟化类型
c6s.large.2	2	4	1/1	30	2	2	KVM
c6s.large.4	2	8	1/1	30	2	2	KVM
c6s.xlarge.2	4	8	2/2	60	2	3	KVM
c6s.xlarge.4	4	16	2/2	60	2	3	KVM
c6s.2xlarge.2	8	16	4/4	120	4	4	KVM
c6s.2xlarge.4	8	32	4/4	120	4	4	KVM
c6s.3xlarge.2	12	24	5.5/5.5	180	4	6	KVM
c6s.3xlarge.4	12	48	5.5/5.5	180	4	6	KVM
c6s.4xlarge.2	16	32	7.5/7.5	240	8	8	KVM

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	网卡个数上限	虚拟化类型
c6s.4xlarge.4	16	64	7.5/7.5	240	8	8	KVM
c6s.6xlarge.2	24	48	11/11	350	8	8	KVM
c6s.6xlarge.4	24	96	11/11	350	8	8	KVM
c6s.8xlarge.2	32	64	15/15	450	16	8	KVM
c6s.8xlarge.4	32	128	15/15	450	16	8	KVM
c6s.12xlarge.2	48	96	22/22	650	16	8	KVM
c6s.12xlarge.4	48	192	22/22	650	16	8	KVM
c6s.16xlarge.2	64	128	30/30	850	32	8	KVM
c6s.16xlarge.4	64	256	30/30	850	32	8	KVM
ct6conn.12xlarge.4	48	192	35/27	750	32	4	KVM

表 5-3 C3 型边缘实例的规格

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	云硬盘基础带宽（Gbps）	虚拟化类型
c3.large.2	2	4	1.5/0.6	30	2	1	KVM
c3.xlarge.2	4	8	3/1	50	2	1.5	KVM
c3.2xlarge.2	8	16	5/2	90	4	2	KVM
c3.3xlarge.2	12	24	7/3	110	4	2.5	KVM

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	云硬盘基础带宽（Gbps）	虚拟化类型
c3.4xlarge.2	16	32	10/4	130	4	3	KVM
c3.6xlarge.2	24	48	12/6	200	8	3.5	KVM
c3.8xlarge.2	32	64	15/8	260	8	4	KVM
c3.15xlarge.2	60	128	16/16	500	16	8	KVM
c3.large.4	2	8	1.5/0.6	30	2	1	KVM
c3.xlarge.4	4	16	3/1	50	2	1.5	KVM
c3.2xlarge.4	8	32	5/2	90	4	2	KVM
c3.3xlarge.4	12	48	7/3	110	4	2.5	KVM
c3.4xlarge.4	16	64	10/4	130	4	3	KVM
c3.6xlarge.4	24	96	12/6	200	8	3.5	KVM
c3.8xlarge.4	32	128	15/8	260	8	4	KVM
c3.15xlarge.4	60	256	16/16	500	16	8	KVM

AI 加速型

表 5-4 Ai1 型边缘实例的规格

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	Ascend 310	Ascend RAM（GiB）	网卡多队列数	网卡个数上限	虚拟化类型
ai1.large.4	2	8	4/1.3	20	1	8	2	2	KVM
ai1.xlarge.4	4	16	6/2	35	2	16	2	3	KVM
ai1.2xlarge.4	8	32	10/4	50	4	32	4	4	KVM
ai1.4xlarge.4	16	64	15/8	100	8	64	8	8	KVM

磁盘增强型

表 5-5 D3i 型边缘实例的规格

规格名称	vCPU	内存（GiB）	最大带宽/基准带宽（Gbps）	最大收发包能力（万PPS）	网卡多队列数	网卡个数上限	本地盘（GiB）	虚拟化类型
d3i.5xlarge.4	20	75	20/15	400	16	8	6 x 9095	KVM
d3i.10xlarge.4	40	150	30/30	800	32	8	12 x 9095	KVM

6 云硬盘

什么是云硬盘

云硬盘（Elastic Volume Service，EVS）可以为智能边缘云提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。

云硬盘的类型

不同类型云硬盘的性能各不相同，您可根据应用程序要求选择您所需的云硬盘。

更多关于云硬盘规格、性能等信息，请参见《**云硬盘用户指南**》。

云硬盘的磁盘模式

云硬盘的磁盘模式分为VBD (虚拟块存储设备，Virtual Block Device) 类型和SCSI (小型计算机系统接口，Small Computer System Interface) 类型。

- VBD类型：

  当您通过管理控制台创建云硬盘时，云硬盘的磁盘模式默认为VBD类型。VBD类型的云硬盘只支持简单的SCSI读写命令。

- SCSI类型：

  您可以通过管理控制台创建SCSI类型的云硬盘，该类型的云硬盘支持SCSI指令透传，允许智能边缘云操作系统直接访问底层存储介质。除了简单的SCSI读写命令，SCSI类型的云硬盘还可以支持更高级的SCSI命令。

  说明

  更多关于SCSI类型云硬盘的使用（如驱动安装），请参见“**使用SCSI类型云硬盘需要安装驱动吗**”。

相关链接

- **挂载磁盘**
- **初始化数据盘**
- **弹性云服务器挂载磁盘时有什么限制?**

7 计费说明

计费项

IEC的计费项由边缘实例、边缘硬盘和边缘带宽三部分构成。具体计费项说明如表7-1所示。

表 7-1 计费项说明

计费项	单位	说明
边缘实例	个	购买边缘实例的数量
边缘硬盘	GB	购买边缘实例对应的硬盘容量
边缘带宽	Mbit/s	共享带宽消耗的流量

IEC的收费详情请参见**产品价格详情**。

计费模式

IEC提供按需计费模式，由边缘实例和边缘硬盘使用时长，以及边缘带宽流量叠加计费。具体计费模式说明如表7-2所示。

表 7-2 计费模式说明

计费模式	计费项	计费周期	付费方式	说明
按需计费	边缘实例和边缘硬盘	秒级计费，按小时结算	后付费	按照边缘实例和边缘硬盘实际使用的时长进行计费。 边缘实例关机后仍正常计费，如果需要停止边缘实例和边缘硬盘计费，直接删除边缘实例即可。

计费模式	计费项	计费周期	付费方式	说明
	边缘带宽	增强型95计费，按月结算	后付费	按照边缘带宽实际使用的流量进行计费。 为了防止突然爆发的流量产生较高的费用，您可以为边缘带宽**设置合适的峰值**。 IEC增强型95计费按照多次去峰值后的实际使用带宽付费。 **计费公式**：月峰值带宽 x 月峰值带宽价格 x 共享带宽存在天数 ÷ 自然月天数 详细计费规则请参见**什么是IEC增强型95计费？** 。 如果需要停止边缘带宽计费，需要彻底**删除带宽**。

变更配置

您可以根据实际业务预估消耗的边缘带宽流量变化选择增大或者降低边缘带宽大小（即设置的带宽峰值），带宽可以设置最小为300Mbit/s。

变更成功后，将立即按照新的带宽值进行收费。

续费

如需续费，请在管理控制台**续费管理**页面进行续费操作。详细操作请参考**续费管理**。

欠费

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，账号进入欠费状态，需要您在约定时间内支付欠款，详细操作请参考**欠费还款**。

8 安全

8.1 责任共担

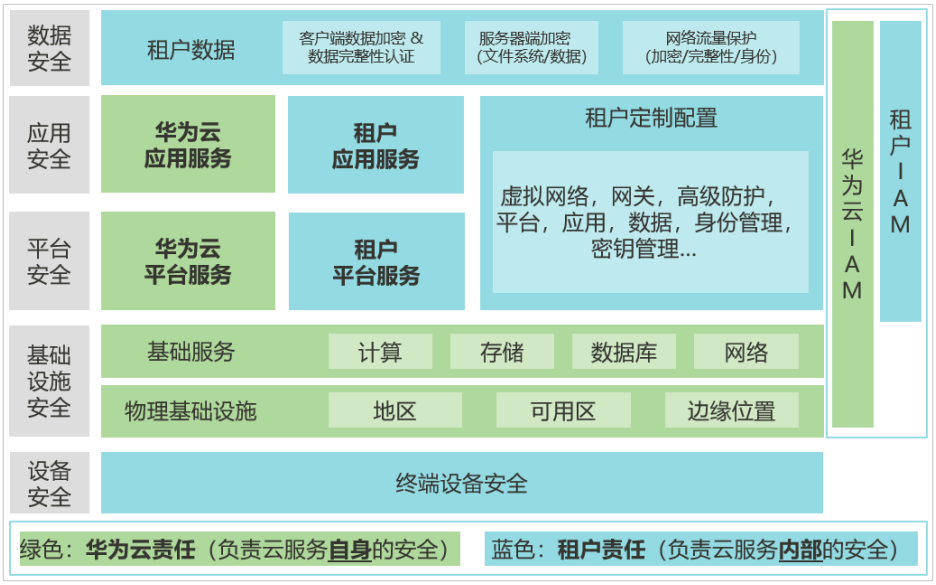
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

8.2.1 服务的访问控制

IAM 身份认证

智能边缘云支持通过IAM进行精细的权限管理，实现用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

您可以在账号中创建IAM用户，并授权控制他们对资源的访问范围。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。详情请参见**权限管理**。

访问控制

- 虚拟私有云

  虚拟私有云（Virtual Private Cloud，以下简称VPC）为边缘服务构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为边缘业务构建一个逻辑上完全隔离的专有区域。您还可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。同时，您可以自定义安全组内与组间边缘业务的访问规则，加强边缘业务的安全保护。

- 安全组

  安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的边缘业务提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当边缘业务加入该安全组后，即受到这些访问规则的保护。

如何设置虚拟私有云和安全组，请参见**边缘网络**。

8.3 数据保护技术

镜像加密

镜像加密支持私有镜像的加密。在创建边缘实例时，用户如果选择加密镜像，边缘实例的系统盘会自动开启加密功能，从而实现边缘实例系统盘的加密，提升数据的安全性。

创建加密镜像的方法有两种：

- 通过外部镜像文件创建加密镜像
- 通过已有的加密弹性云服务器创建加密镜像

更多关于镜像加密的信息，请参见**镜像加密**。

8.4 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录CloudPond的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- IEC支持审计的操作事件，请参见**支持审计的关键操作**。
- 查看审计日志，请参见**查看IEC审计事件**。

8.5 监控安全风险

云监控服务，为用户提供一个针对边缘实例、带宽等资源的立体化监控平台。使用户全面了解IEC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。

用户开通云监控后，CES可以查看带宽、弹性公网IP的使用情况，也可以创建和设置告警规则，自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。

- CES的详细介绍，请参见**CES功能介绍**。
- IEC支持的监控指标，请参见**支持的监控指标**。
- 查看监控指标步骤，请参见**查看监控指标**。

9 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 9-1 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 9-2 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 9-3 销售许可证&软件著作权证书

10 权限管理

使用场景

如果您需要对华为云上购买的IEC资源，给其他用户设置不同的访问权限，以达到不同用户之间的权限隔离，您可以使用统一身份认证服务IAM进行权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给他人创建IAM用户，并授权控制他们对华为云资源的访问范围。

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用IEC资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将IEC资源委托给更专业、高效的云服务，这些云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用IEC服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

IEC 权限

IEC的控制台部署时不区分物理区域，为全局性的。访问IEC控制台时，不需要切换区域。存在如下一个特殊情况：在使用Tenant Administrator和Tenant Guest两个系统权限时需要选择一些仅为IEC使用的特殊华为云区域，详见**表10-1**。以上提到的区域是指华为云整体上按照物理位置划分的区域，和IEC服务业务上的边缘区域是有差别的，详见**华为云的区域和IEC的区域有什么区别？**。

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略和角色，才能使得用户组中的用户获得策略定义的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对IEC服务，管理员能够控制IAM用户仅能查询网络ACL列表，而不能创建网络ACL。多数细粒度策略以API接口为粒度进行权限拆分，IEC支持的API授权项请参见**权限和授权项说明**。

表10-1列出了IEC的所有系统权限。

表 10-1 IEC 系统权限

权限名称	描述	作用范围	类别	依赖关系
IEC FullAccess	拥有该权限的用户可以对IEC资源执行任意操作。	仅选择“全局服务”	系统策略	无
IEC ReadOnlyAccess	拥有该权限的用户可以查询IEC资源的利用情况，即仅拥有IEC读权限。	仅选择“全局服务”	系统策略	无
Tenant Administrator	拥有该权限的用户拥有除IAM外，其他所有服务的所有执行权限。	选择“全局服务”和“区域级项目”， 区域级项目为： • cn-north-900 [华北-北京边缘二]	系统角色	无
Tenant Guest	拥有该权限的用户拥有除IAM外，其他所有服务的只读权限。	选择“全局服务”和“区域级项目”， 区域级项目为： • cn-north-900 [华北-北京边缘二]	系统角色	无

表10-2列出了IEC常用操作与系统策略的关系。

表 10-2 IEC 常用操作与系统策略的关系

操作	IEC ReadOnlyAccess	IEC FullAccess
查询带宽列表	√	√
查询指定带宽	√	√
修改带宽信息	x	√
删除带宽信息	x	√
删除子网	x	√

操作	IEC ReadOnlyAccess	IEC FullAccess
查询指定子网	√	√
更新子网	x	√
查询子网列表	√	√
创建子网	x	√
删除虚拟私有云	x	√
查询虚拟私有云列表	√	√
更新虚拟私有云	x	√
查询指定虚拟私有云	√	√
创建虚拟私有云	x	√
查询网络配额	√	√
创建路由表	x	√
查询路由表列表	√	√
查询路由表详情	√	√
更新路由表	x	√
删除路由表	x	√
查询路由列表	√	√
添加路由	x	√
更新路由	x	√
删除路由	x	√
路由表关联子网	x	√
路由表解关联子网	x	√
查询子网关联的路由表	√	√
查询网络ACL列表	√	√
创建网络ACL	x	√
更新网络ACL	x	√
更新网络ACL规则	x	√
删除网络ACL	x	√
查询指定网络ACL	√	√

操作	IEC ReadOnlyAccess	IEC FullAccess
删除弹性公网IP	x	√
查询指定弹性公网IP	√	√
更新弹性公网IP	x	√
查询弹性公网IP列表	√	√
创建弹性公网IP	x	√
删除安全组	x	√
查询指定安全组	√	√
查询安全组列表	√	√
创建安全组	x	√
删除安全组规则	x	√
查询指定安全组规则	√	√
查询安全组规则列表	√	√
创建安全组规则	x	√
删除边缘业务	x	√
查询指定边缘业务	√	√
查询边缘业务列表	√	√
查询边缘业务配额	√	√
查询实例列表	√	√
操作实例（启动、关闭、重启）	x	√
批量删除实例	x	√
修改实例	x	√
查询指定实例	√	√
创建实例	x	√
切换操作系统	x	√
更新实例网卡配置	x	√
删除实例网卡	x	√
添加实例网卡	x	√

操作	IEC ReadOnlyAccess	IEC FullAccess
查询实例规格列表	√	√
查询指定的任务	√	√
查询站点列表	√	√
查询指定云硬盘	√	√
查询云硬盘类型列表	√	√
查询云硬盘列表	√	√
查询边缘镜像列表	√	√
创建边缘镜像	x	√
查询指定边缘镜像	√	√
删除边缘镜像	x	√
查询边缘镜像支持的区域列表	√	√
查询边缘镜像的配额信息	√	√
查询特定华为云区域的镜像列表	√	√
从边缘实例创建镜像	x	√
查询边缘实例的统计数据	√	√
查询带宽的统计数据	√	√
查询资源使用率	√	√

创建IAM用户并授权的具体操作请参见**示例流程**。

11 常用概念

边缘站点

靠近终端应用的位置，基于一个或多个运营商建立的一个城市级站点。边缘站点提供物理隔离的资源池，提供多元算力、存储和网络的能力。用户可以将业务灵活就近部署在边缘站点上，以降低网络时延和成本。

边缘区域

边缘区域即为依据边缘站点的物理位置划分的区域，一个边缘区域包含多个相靠近的边缘站点的集合。

IEC提供站点级、城市级、省级和大区级四个分布层级的边缘区域。

您可以通过**边缘站点和边缘区域的关系**进一步了解大区级、省级、城市级边缘区域和运营商以及边缘站点的关系。

边缘业务

一个边缘业务简单说即为逻辑层面的一套资源管理集合。这里的资源主要是指计算实例，包含实例规格、镜像、硬盘、网络等方面。通过指定计算实例的数量、调度策略以及区域分布等形成一套管理集合。

边缘实例

边缘实例为边缘云场景下专享的实例资源，是由CPU（Central Processing Unit，中央处理器）、内存、操作系统、云硬盘组成的基础的计算组件。

IEC范畴下的边缘实例与华为云上弹性云服务器ECS完全独立，没有关联关系，各自承载不同的业务。但从两者的功能维度来看，又是相类似的。

举例说明，通过IEC控制台或者API创建的实例仅归属于华为云服务IEC的业务范畴，与通过华为云服务ECS创建的实例没有关联关系。IEC上创建的实例不能通过ECS管理，ECS上创建的实例也不能通过IEC管理。

边缘镜像

镜像是一个包含了软件及必要配置的实例模版，包含操作系统或业务数据，还可以包含应用软件（例如数据库软件）和私有软件。

IEC使用的边缘镜像支持公共镜像和私有镜像两种镜像类型。

- 公共镜像：IEC支持的公共镜像预置在IEC系统中，供所有用户使用。与华为云镜像服务中提供的公共镜像功能类似，但没有关联关系，各自承载不同的业务。

  IEC上创建的公共镜像不能通过云服务IMS管理，云服务IMS上创建的公共镜像也不能通过IEC管理。
- 私有镜像：IEC的私有镜像由用户首先在**镜像服务**中创建，然后在IEC上进行注册，注册完成后可以选择使用。

  注册到IEC的私有镜像和镜像服务中原私有镜像互相独立，后者的修改不影响前者。已注册到IEC的私有镜像不能修改。如果当前镜像不能满足需求，您可以重新创建和注册。

边缘网络

边缘网络为边缘云场景下专享的网络子服务。通过虚拟私有云，构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。同时，通过弹性公网IP，使得虚拟私有云内的实例与公网Internet互通。

IEC范畴下的边缘网络与华为云上其他网络相关的云服务，如虚拟私有云、弹性公网IP完全独立，没有关联关系，各自承载不同的业务。但从两者的功能维度来看，又是相类似的。

举例说明，通过IEC控制台或者API创建的虚拟私有云仅归属于华为云服务IEC的业务范畴，与通过华为云服务VPC创建的虚拟私有云没有关联关系。IEC上创建的虚拟私有云不能通过云服务VPC管理，云服务VPC上创建的虚拟私有云也不能通过IEC管理。

12 与其他云服务的关系

与 IEC 有功能依赖的云服务

IEC和其他周边云服务的功能依赖关系如表12-1所示。

表 12-1 与 IEC 有功能依赖的云服务

相关服务	功能依赖关系	参考内容
镜像服务	边缘私有镜像需要首先在镜像服务中创建，然后在IEC控制台界面上进行注册，注册完成后可以选择使用。	边缘镜像概述 通过镜像服务创建边缘私有镜像
统一身份认证服务	通过统一身份认证服务，给IEC的其他用户设置不同的访问权限，以达到不同用户之间的权限隔离。	权限管理 创建IAM用户并授权使用IEC

与 IEC 有业务交互的云服务

IEC和其他周边云服务的业务交互关系如表12-2所示。

表 12-2 与 IEC 有业务交互的云服务

相关服务	业务交互关系	使用方法
智能边缘平台	智能边缘平台将IEC中的边缘实例作为边缘节点进行纳管，纳管之后向IEC下发应用。	通过智能边缘平台控制台界面注册IEC节点类型的边缘节点，注册完成后系统自动进行纳管。

与 IEC 有区别对比的产品

- 面向不同应用场景的多种云化产品（智能边缘云（Intelligent EdgeCloud，IEC）和智能边缘小站（CloudPond）、智能边缘平台（Intelligent EdgeFabric，IEF）、IoT边缘（IoT Edge）、内容分发网络（Content Delivery Network，CDN））之间的区别，请参见IEC与相关产品区别。

- IEC范畴下的实例、镜像和网络与弹性云服务器，镜像服务，虚拟私有云等云服务的区别，请参见**边缘实例**，**边缘镜像**，**边缘网络**。

