

智能边缘平台

产品介绍

文档版本 01
发布日期 2024-10-17



版权所有 © 华为技术有限公司 2024。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://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

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>

目录

1 什么是智能边缘平台.....	1
2 产品功能.....	3
3 产品优势.....	6
4 服务实例版本.....	8
5 应用场景.....	10
6 基本概念.....	12
7 与其他云服务的关系.....	14
8 约束与限制.....	15
9 权限管理.....	18
10 配额说明.....	22

1 什么是智能边缘平台

为什么选择智能边缘平台

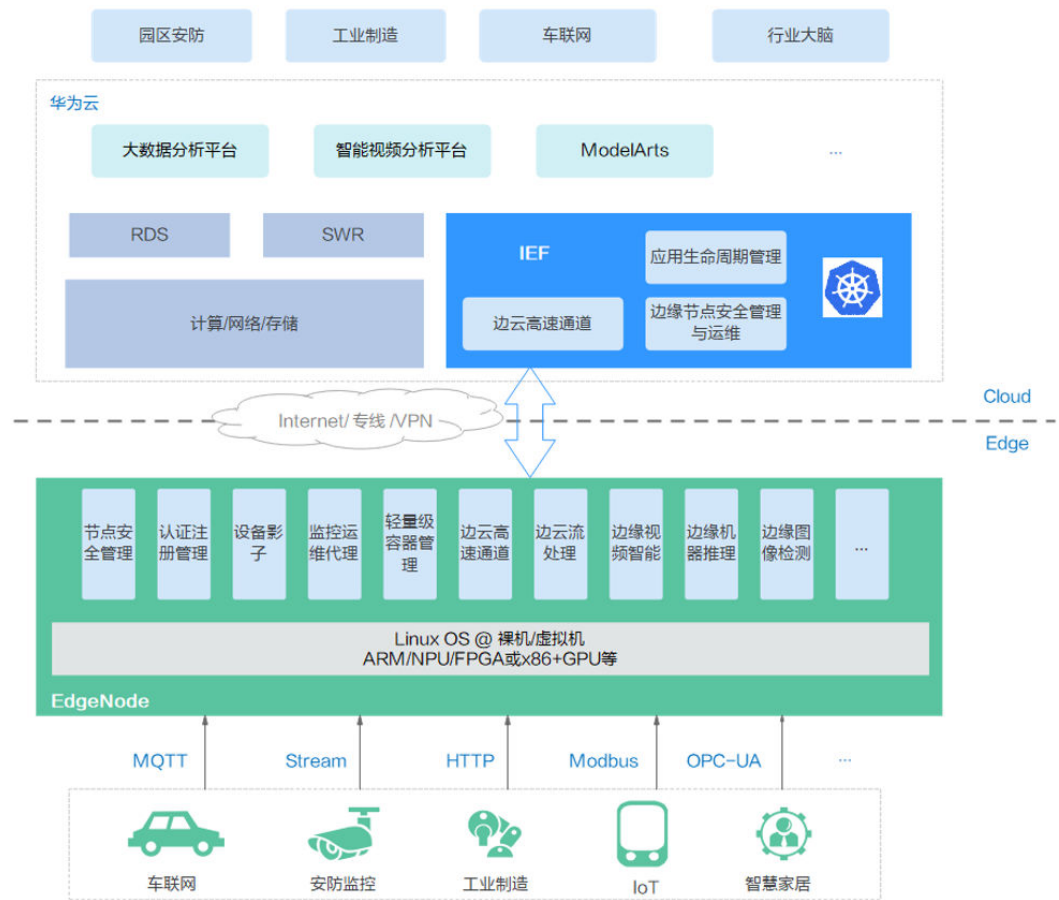
云计算是集中化的，离终端设备（如摄像头、传感器等）较远，对于实时性要求高的计算需求，把计算放在云上会引起网络延时变长、网络拥塞、服务质量下降等问题。而终端设备通常计算能力不足，无法与云端相比。在此情况下，边缘计算顺应而生，通过在靠近终端设备的地方建立边缘节点，将云端计算能力延伸到靠近终端设备的边缘节点，从而解决上述问题。

智能边缘平台（Intelligent EdgeFabric）通过纳管您的边缘节点，提供将云上应用延伸到边缘的能力，联动边缘和云端的数据，满足客户对边缘计算资源的远程管控、数据处理、分析决策、智能化的诉求，同时，在云端提供统一的边缘节点/应用监控、日志采集等运维能力，为企业提供边、云协同的一体化边缘计算解决方案。

产品架构

如图1-1所示，IEF将云端AI应用等能力下发到边缘节点（EdgeNode），将公有云能力延伸到靠近终端设备的一端，使得边缘节点拥有云端相同能力，能够实时处理终端设备计算需求。

图 1-1 边缘云计算



访问方式

智能边缘平台IEF提供了Web化的服务管理平台（即管理控制台）和基于HTTPS请求的API（Application programming interface）管理方式。

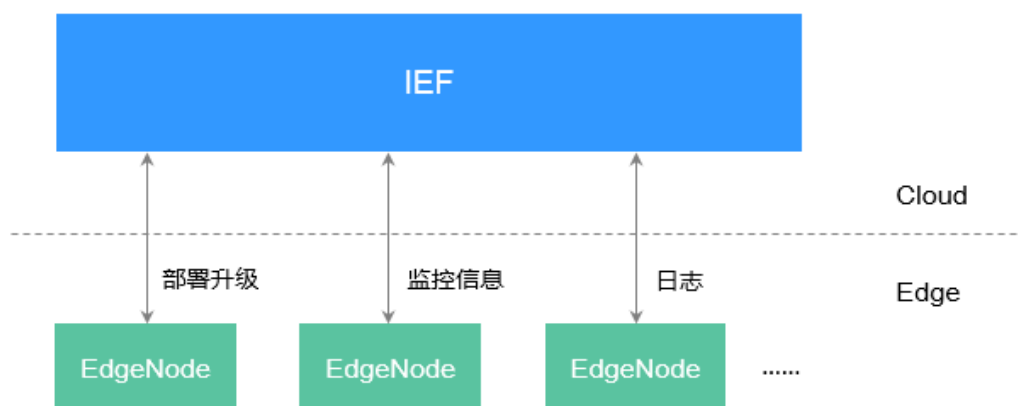
- API方式
如果用户需要将智能边缘平台集成到第三方系统，用于二次开发，请使用API方式访问智能边缘平台，具体操作请参见《智能边缘平台API参考》。
- 控制台方式
直接登录管理控制台，从主页选择“智能边缘平台”。

2 产品功能

边缘节点管理

IEF支持接入海量的边缘节点（EdgeNode），在IEF中可以自动生成边缘节点的配置信息，能够高效、便捷的纳管（安装Edge Agent）边缘节点，所有边缘节点可以在云端统一管理、监控和运维。

图 2-1 边缘节点管理



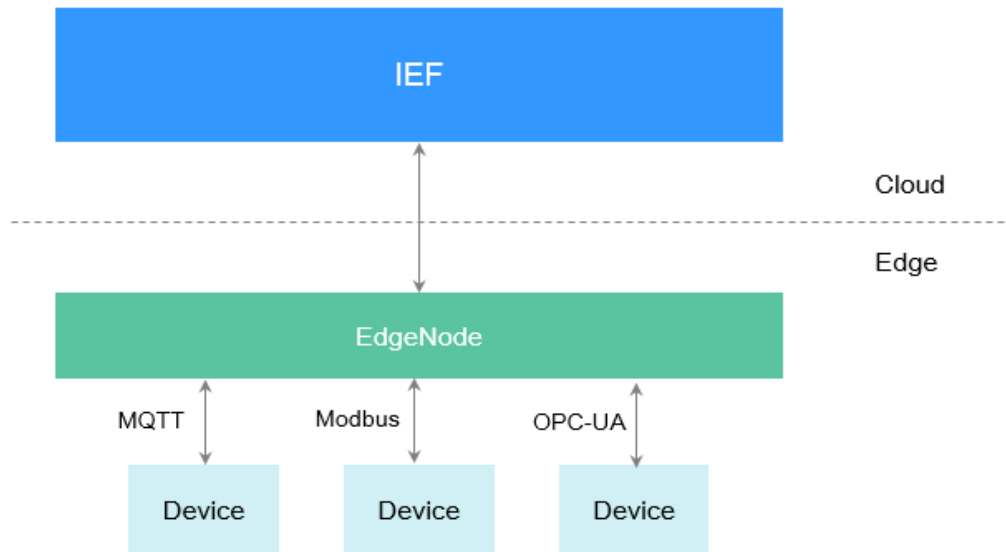
终端设备管理

支持终端设备连接到边缘节点，终端设备支持通过MQTT协议、Modbus协议和OPC-UA协议等接入。终端设备接入后，可以对终端设备进行统一管理。

📖 说明

专业版实例仅支持MQTT协议。

图 2-2 终端设备管理



边缘应用管理

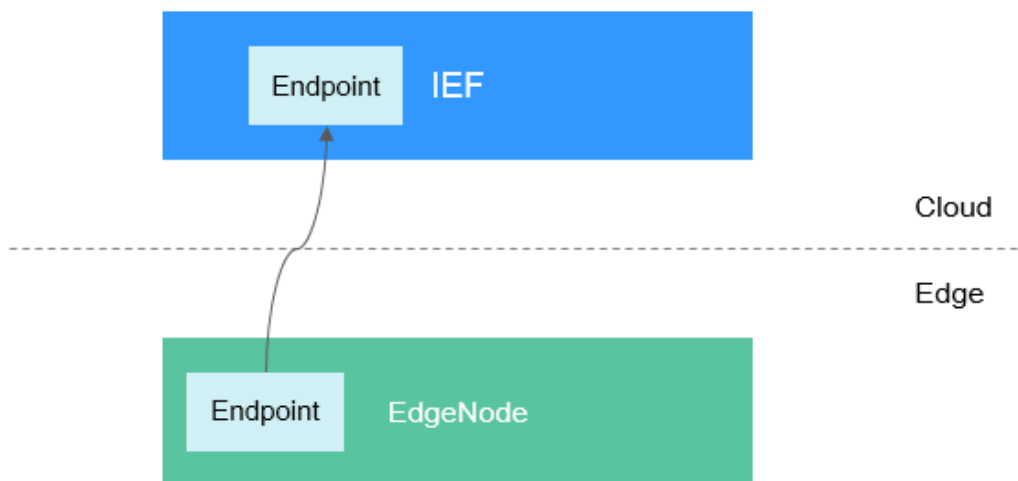
IEF支持以容器的形式将边缘应用快速部署到边缘节点运行。您可以将自己的边缘应用程序打包成容器镜像，并上传到容器镜像服务，然后通过IEF将容器镜像部署到边缘节点运行。并且IEF支持对应用进行版本升级、配置变更、卸载、监控和日志采集。

容器具有更繁荣的生态，能帮助您的容器应用无缝切换到其他的运行环境中，具有更好的可移植性，而且容器具有更好的资源隔离性，并支持CPU/GPU调度。

消息路由管理

IEF提供了消息路由功能，您可以配置消息路由，IEF根据配置的消息路由将边缘消息转发至对应消息端点（Endpoint，发送或接收消息的一方），让消息按照规定的路径转发，灵活控制数据路由，并提高数据安全性。

图 2-3 消息转发路径



批量作业管理

IEF提供了批量作业管理功能，您可以批量注册边缘节点，批量升级边缘节点的版本，批量部署应用，批量升级应用（更换容器镜像和访问配置）。详见[用户指南 > 批量管理](#)。

3 产品优势

支持高性能边缘智能硬件

IEF提供软硬一体化解决方案，为用户提供低成本、开箱即用、云上集中运维的一站式服务，提供华为通用服务器和AI专用硬件，与昇腾芯片深度集成，提供高性能、低成本的边缘AI推理算力，支持华为鲲鹏通用中央处理器的泰山服务器。

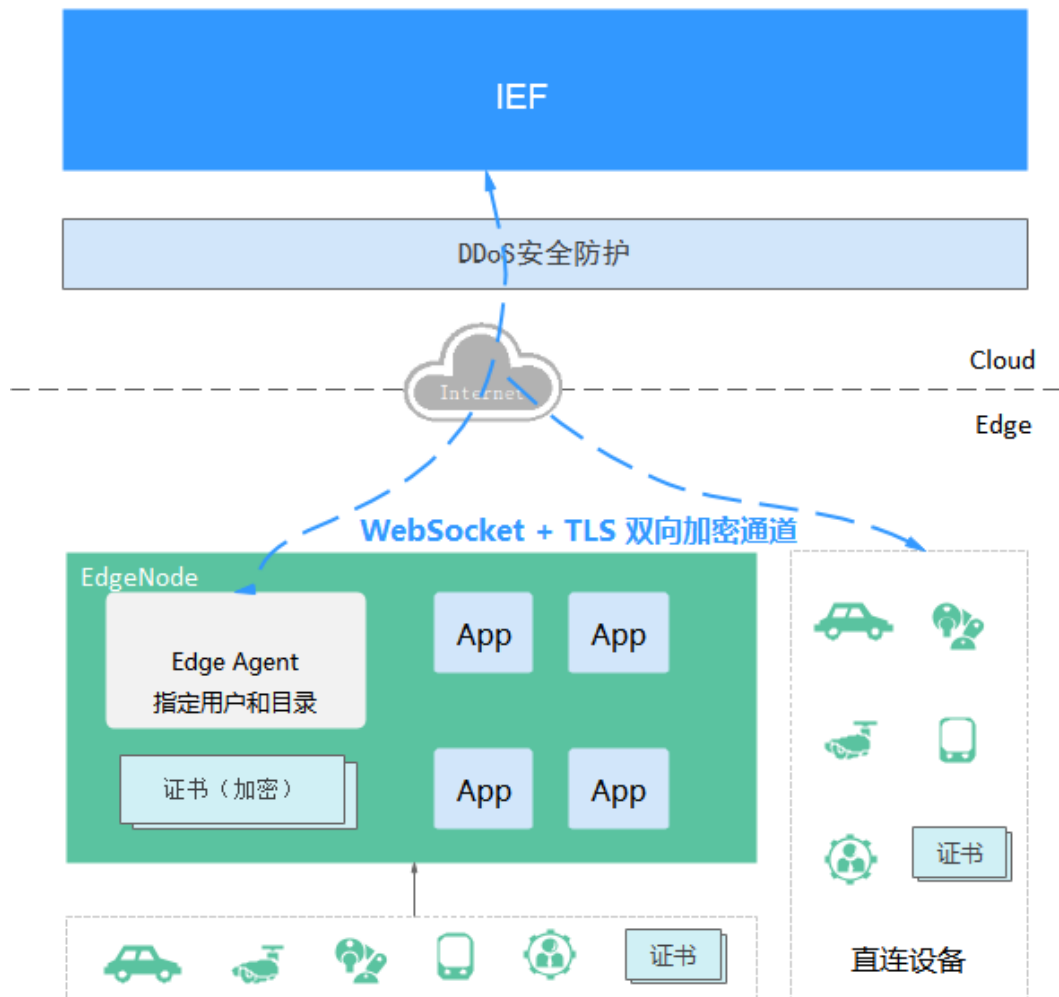
图 3-1 边缘硬件



安全可靠

- IAM认证
通过创建IAM角色，允许从边缘节点访问AOM、SWR、DIS等资源。
- 边缘节点安全
Edge Agent创建专属服务用户，能够访问的目录和拥有的权限都受限，向云端上传日志、监控信息由用户自行选择。
- 云边协同通讯安全
Edge Agent与IEF建立双向加密通道，Edge Agent自下向上发起，双向消息收发通过证书认证、加密。
- 云安全
前置DDoS网络安全防护，防恶意攻击。
为每个边缘节点颁布唯一接入证书，双向通讯通过证书认证、加密。
- 设备安全
终端设备使用证书进行身份认证。

图 3-2 IEF 安全性方案



开放兼容

IEF基于开源的KubeEdge软件实现，KubeEdge基于Kubernetes构建，为云和边缘之间的网络、应用程序部署和元数据同步提供基础架构支持。

使用KubeEdge便于开发者对边缘节点运行时（Edge Agent，边缘节点的管理程序）进行定制和裁剪，降低边缘的使用难度。

低成本

- 云计算和边缘计算结合，在边缘节点处实现了对数据的过滤和分析，大幅提高效率，降低云端计算成本。
- 在进行云端传输时通过边缘节点进行一部分简单数据处理，进而能够缩短终端设备响应时间，减少从终端设备到云端的数据流量，降低带宽成本。

4 服务实例版本

IEF有专业版和铂金版服务实例供您选择。

- 专业版：共享管理面集群。支持节点管理、设备管理、容器应用管理、批量作业管理和边云消息等功能。
- 铂金版：独享管理面集群，支持管理大规模节点，性能更高。在专业版基础上，增加支持节点组、应用网格等功能。

具体差异请参见[表4-1](#)。

表 4-1 版本功能说明

功能特性	说明	专业版	铂金版
边缘节点管理	支持注册、纳管边缘节点	√	√
终端设备管理	支持注册终端设备，支持绑定终端设备到边缘节点	√	√
容器应用管理	支持下发容器应用到边缘节点	√	√
边云消息路由	提供边云消息通道，支持边云消息转发	√	√
多网络接入支持	支持Internet、VPN和专线接入	√	√
监控运维	支持监控运维	√	√
批量作业	支持批量创建容器应用、批量更新容器应用、批量注册边缘节点、批量升级边缘节点	√	√
边缘节点组	支持创建边缘节点组，将具备相同属性（如硬件架构）的多个边缘节点组成一个边缘节点组，以便统一化管理	×	√
多实例支持	支持多个容器应用实例	×	√

功能特性	说明	专业版	铂金版
独享集群	支持独享管理面集群	×	√
应用网格	支持服务发现；应用流量治理，包括负载均衡等多种治理能力	×	√
插件管理	支持插件管理能力。	√	√
Kubernetes原生接口开放	支持通过kubectI操作服务实例对应的Kubernetes集群	×	√

5 应用场景

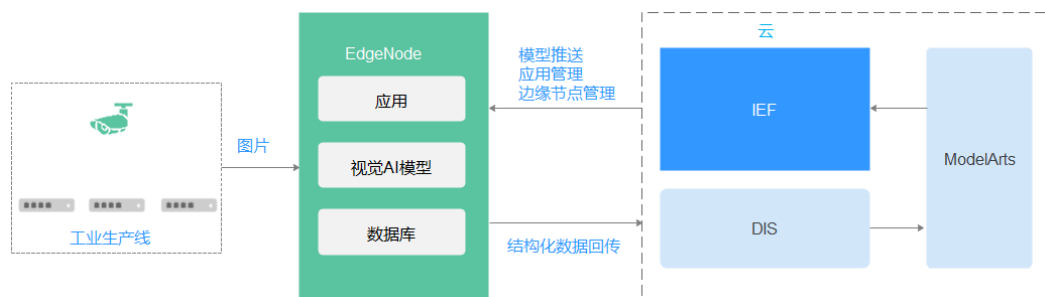
工业视觉

传统的工业制造主要采用人工肉眼检测产品的缺陷，不仅使得检测产品速度慢、效率低下，而且在检测过程中容易出错，导致误检、漏检等问题。基于机器视觉的质检方案，通过云端建模分析与边缘实时决策的结合，实现自动视觉检测，提升产品质量。

优势：

- **高效：**云端已训练的视觉模型，在边缘侧部署，实现产品实时预测，提升检测效率，提高产品质量
- **模型优：**提供边云协同架构，云端模型训练，数据边缘处理，模型增量训练优化，实现模型性能优异
- **统一管控：**智能边缘平台可以实现统一模型下发，节点状态统一监控

图 5-1 工业视觉场景



CDN 边缘站点管理

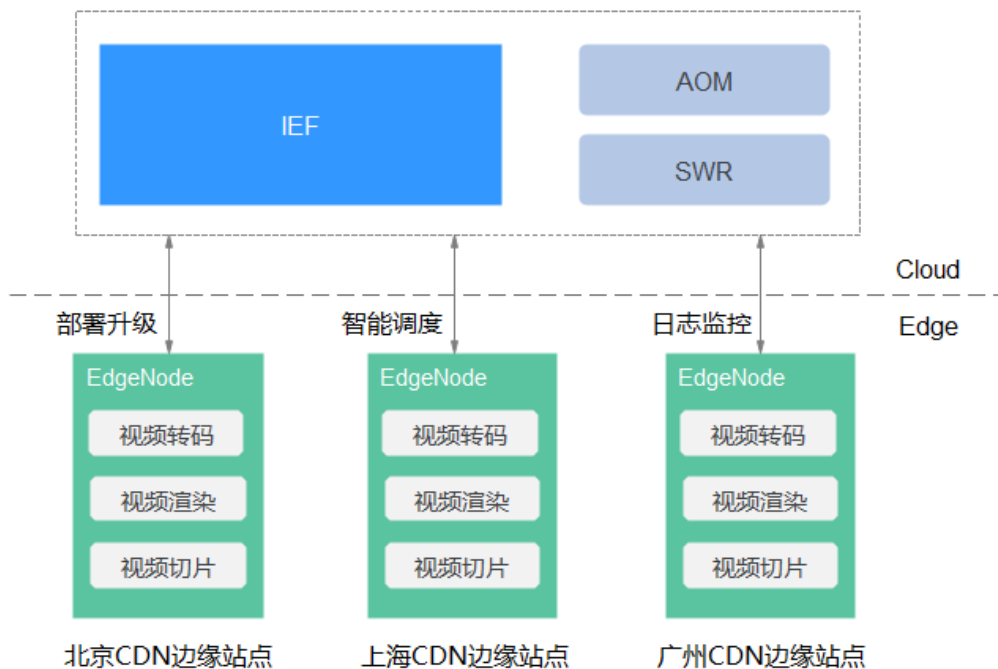
对部署在全国各地的CDN边缘站点进行统一管理，帮助用户实现应用自动化调度，弹性伸缩以及边缘站点和边缘应用运维。

优势：

- **弹性伸缩：**可根据用户的业务需求和预设策略，自动调整计算资源，使云服务器或容器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。
- **智能化调度：**提供节点间亲和性调度以及应用间亲和性调度。

- **立体化运维**：实时监控业务健康状态和边缘节点状态，保障应用稳定运行。
- **本地自治**：支持边缘节点离线处理，在边缘节点与云中心网络断开后，业务可以正常运行。

图 5-2 CDN 边缘站点管理

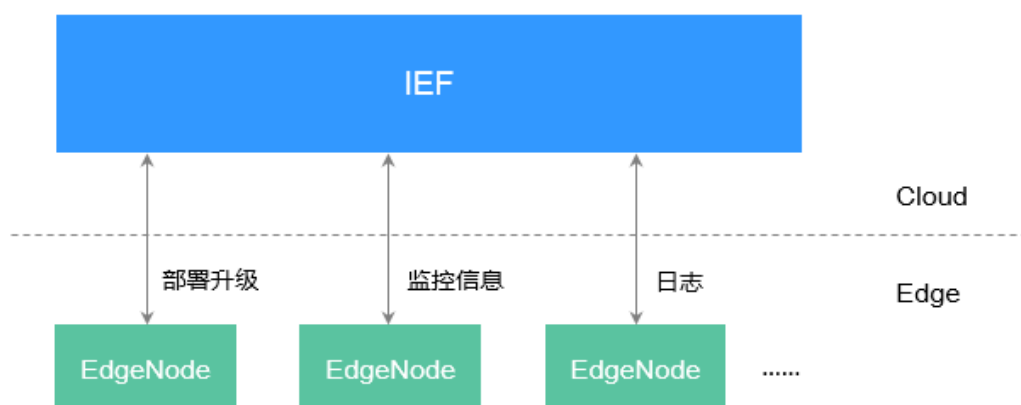


6 基本概念

边缘节点

边缘节点（EdgeNode）是您自己的边缘计算设备，用于运行边缘应用，处理您的数据，并安全、便捷地和云端应用进行协同。

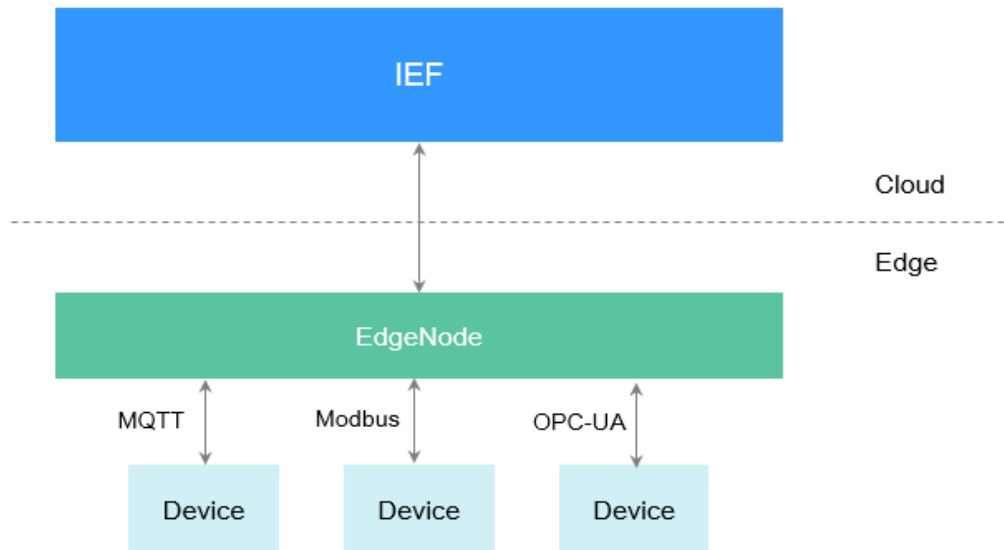
图 6-1 边缘节点



终端设备

终端设备可以小到传感器、控制器，大到智能摄像机或工控机床。终端设备可以连接到边缘节点，IEF支持以MQTT协议、Modbus协议和OPC-UA协议等接入终端设备。

图 6-2 终端设备



容器应用

容器应用是您需要在边缘节点上运行的功能模块，通过部署所需应用来构建您自己的边缘计算能力。

在专业版本中，一个容器应用只能拥有一个实例；在铂金版本中一个容器应用可以拥有多个实例。

消息端点

数据发送的起始点或者数据接收的目的点，如数据从终端设备发送到云端服务，终端设备为源端点，云端服务为目的端点。

消息路由

由源端点，源端点资源，目的端点和目的端点资源组成，系统会根据消息将消息从源端点指定资源转发到目的端点的指定资源上。

证书

证书是作为边缘应用或者终端设备接入边缘节点MQTT Broker的凭证。

7 与其他云服务的关系

IEF与其他服务之间的关系如图7-1所示。

图 7-1 IEF 与其他服务之间的关系

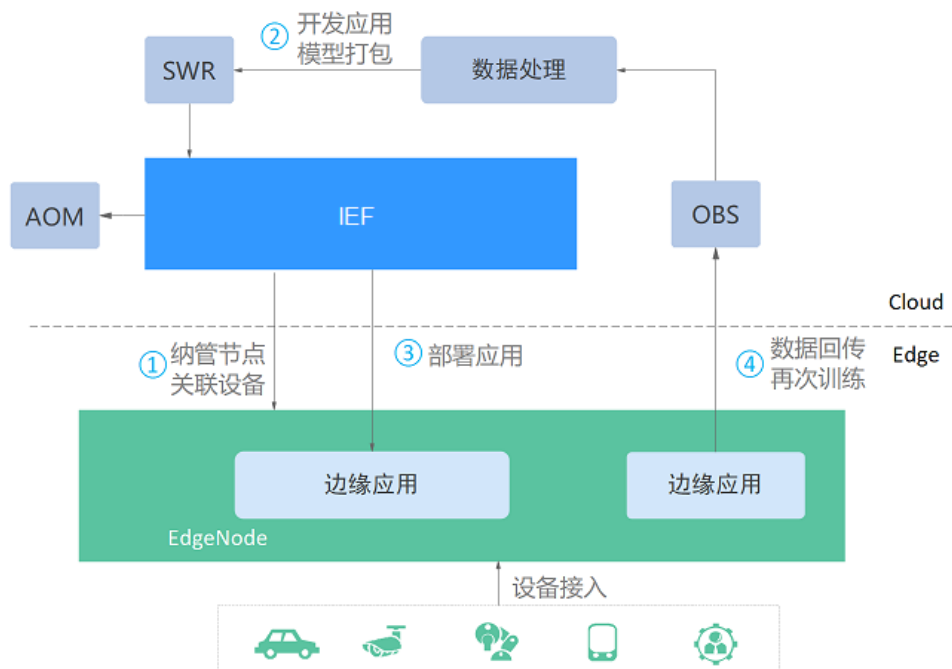


表 7-1 IEF 与其他服务之间的关系

云服务名称	描述
SWR	边缘节点从SWR拉取容器镜像。
OBS	用户可以将边缘节点生成的数据上传到OBS存储，从而在云上做进一步处理。
AOM	边缘节点的日志、监控和告警上报至应用运维服务AOM。

8 约束与限制

边缘节点规格要求

边缘节点既可以是物理机，也可以是虚拟机。边缘节点需要满足表8-1的规格要求。

表 8-1 边缘节点要求

项目	规格
OS	<p>操作系统语言必须切换至英文。</p> <ul style="list-style-type: none">• x86_64架构 Ubuntu LTS (Xenial Xerus)、Ubuntu LTS (Bionic Beaver)、CentOS、EulerOS、RHEL、银河麒麟、中兴新支点、中标麒麟、openEuler、uos (Unity Operating System)、ol (Oracle Linux)、hce (Huawei Cloud Euler)、openEuler 23.09 Edge• armv7i (arm32) 架构 Raspbian GNU/Linux (stretch)• aarch64 (arm64) 架构 Ubuntu LTS (Xenial Xerus)、Ubuntu LTS (Bionic Beaver)、CentOS、EulerOS、RHEL、银河麒麟、中兴新支点、中标麒麟、openEuler、uos (Unity Operating System)、ol (Oracle Linux)、hce (Huawei Cloud Euler)、openEuler 23.09 Edge <p>说明 推荐使用面向边缘计算场景的openEuler 23.09 Edge操作系统。</p>
内存	边缘软件开销约128MB，为保证业务的正常运行，建议边缘节点的内存大于256MB。
CPU	>= 1核
硬盘	>= 1GB

项目	规格
GPU（可选）	<p>同一个边缘节点上的GPU型号必须相同。</p> <p>说明</p> <p>当前支持Nvidia Tesla系列P4、P40、T4等型号GPU。</p> <p>含有GPU硬件的机器，作为边缘节点的时候可以不使用GPU。</p> <p>如果边缘节点使用GPU，您需要在纳管前安装GPU驱动。</p> <p>目前只有使用x86架构的GPU节点才能纳管到IEF中使用。</p>
NPU（可选）	<p>昇腾AI加速处理器。</p> <p>说明</p> <p>当前支持集成了昇腾处理器的边缘节点，如Atlas 300推理卡、Atlas 800推理服务器。同时支持昇腾310P、昇腾310B、昇腾310P共享模式和虚拟化切分的NPU规格。</p> <p>如果边缘节点使用NPU，请确保边缘节点已安装驱动（目前昇腾310仅支持1.3.x.x和1.32.x.x的固件版本，例如1.3.2.B893，可用npusmi info命令查看固件版本）（NPU驱动需不小于22.0.4版本，进入驱动所在路径如“/usr/local/Ascend/driver”，执行cat version.info命令查看）。如果没有安装驱动，请联系设备厂商获取支持。</p>
容器引擎	<p>Docker版本必须高于17.06。使用高于或等于1.23版本的docker时，需设置docker cgroupfs版本为1，不支持docker HTTP API v2。</p> <p>（请勿使用18.09.0版本Docker，该版本存在严重bug，详见https://github.com/docker/for-linux/issues/543；如果已使用此版本，请尽快升级。）</p> <p>须知</p> <p>Docker安装完成后，请将Docker进程配置为开机启动，避免系统重启后Docker进程未启动引起的系统异常。</p> <p>Docker Cgroup Driver必须设置为cgroupfs。详细配置方法请参考在边缘节点安装Docker后，如何设置Docker Cgroup Driver?。</p>
glibc	版本必须高于2.17。
端口使用	边缘节点需要使用8883端口，8883端口用于边缘节点内置MQTT broker监听端口，请确保该端口能够正常使用。
时间同步	边缘节点时间需要与UTC标准时间保持一致，否则会导致边缘节点的监控数据、日志上传出现偏差。您可以选择合适的NTP服务器进行时间同步，从而保持时间一致。详细配置方法请参见 如何同步NTP服务器? 。

MQTT 使用限制

表 8-2 MQTT 使用限制

描述	限制
支持的MQTT协议版本	3.1.1

描述	限制
与标准MQTT协议的区别	<ul style="list-style-type: none">• 支持QoS 0• 支持Topic自定义• 不支持QoS 1和QoS 2• 不支持will、retain msg
MQTTS支持的安全等级	采用TCP通道基础 + TLS协议（TLSV1.2 版本）

9 权限管理

如果您需要对华为云上购买的IEF资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。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员工创建IAM用户，并授权控制这些用户对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些用户拥有IEF的使用权限，但是不希望拥有删除IEF等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用IEF，但是不允许删除IEF的权限，控制这些用户对IEF资源的使用范围。

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IEF服务的其他功能。

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](#)。

IEF 权限

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或角色，才能使得用户组中的用户获得对应的权限，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。

IEF部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京四）对应的项目（cn-north-4）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问IEF时，需要先切换至授权区域。

权限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。具有Tenant Administrator系统角色的用户可以操作IEF所有资源。
- 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。多数细粒度策略以API接口为粒度进行权限拆分。

如[表1](#)所示，包括了IEF的所有系统权限。

表 9-1 IEF 系统权限

系统角色/策略名称	描述	类别	依赖关系
IEF FullAccess	IEF管理员权限，拥有该权限的用户可以操作并使用IEF的基本资源。注意：如需操作IEF所有资源，请配置Tenant Administrator系统角色。	系统策略	无
IEF ReadOnlyAccess	IEF只读权限，拥有该权限的用户仅能查看IEF资源。	系统策略	无

表9-2列出了IEF常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-2 常用操作与系统权限的关系

操作	IEF FullAccess	IEF ReadOnlyAccess	Tenant Administrator
创建/删除/修改服务实例	√	x	√
查看服务实例	√	√	√
切换实例	√	√	√
创建/删除/修改边缘节点	√	x	√
查看边缘节点	√	√	√
创建/删除/修改边缘节点组	√	x	√
查看边缘节点组	√	√	√
创建/删除/修改边缘容器应用	√	x	√
查看边缘容器应用	√	√	√
创建/删除/修改设备	√	x	√
查看设备	√	√	√
创建/删除/修改应用部署	√	x	√
查看应用部署	√	√	√

操作	IEF FullAccess	IEF ReadOnlyAccess	Tenant Administrator
创建/删除/修改应用模板	√	x	√
查看应用模板	√	√	√
创建/删除/修改节点注册作业	√	x	√
查看节点注册作业	√	√	√
创建/删除/修改消息端点	√	x	√
查看消息端点	√	√	√
创建/删除/修改消息路由	√	x	√
查看消息路由	√	√	√
创建/删除/修改批量作业	√	x	√
查看批量作业	√	√	√
创建/删除/修改配置项	√	x	√
查看配置项	√	√	√
创建/删除/修改密钥	√	x	√
查看密钥	√	√	√
创建/删除/修改加密数据	√	x	√
查看加密数据	√	√	√
创建/删除/修改系统订阅	√	x	√
查看系统订阅	√	√	√
创建/删除/修改插件	√	x	√
查看插件	√	√	√

相关链接

- [IAM产品介绍](#)

- 创建用户组、用户并授予IEF权限，具体请参考[创建用户并授权使用IEF](#)。
- [权限和授权项](#)

10 配额说明

IEF对单个用户的资源数量和容量限定了配额，配额的详细信息请参见[表10-1](#)和[表10-2](#)。

表 10-1 专业版配额

资源对象	默认配额
节点	10
终端设备	500
终端设备模板	10
容器应用	500
应用模板	10
应用模板版本	10
标签	每个资源最多20个
配置项	50
密钥	50
加密数据	50
消息端点	20
消息路由	100
节点注册作业	50
节点证书	5000
批量作业	20

表 10-2 铂金版配额

资源对象	默认配额
服务实例	5
节点	创建铂金版服务实例时选择，支持选择50、200、1000节点。
终端设备	节点数量 x 50
终端设备模板	与节点数量一致
容器应用	节点数量 x 50
应用模板	与节点数量一致
应用模板版本	10
标签	每个资源最多20个标签
配置项	节点数量 x 5
密钥	节点数量 x 5
加密数据	50
消息端点	20
消息路由	100
节点注册作业	50
节点证书	节点数量 x 500
节点组	100
节点组证书	节点数量 x 50
服务	500
网关	500
虚拟服务	500
批量作业	20