设备接入

产品介绍

文档版本 1.0

发布日期 2024-11-05

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

目 录

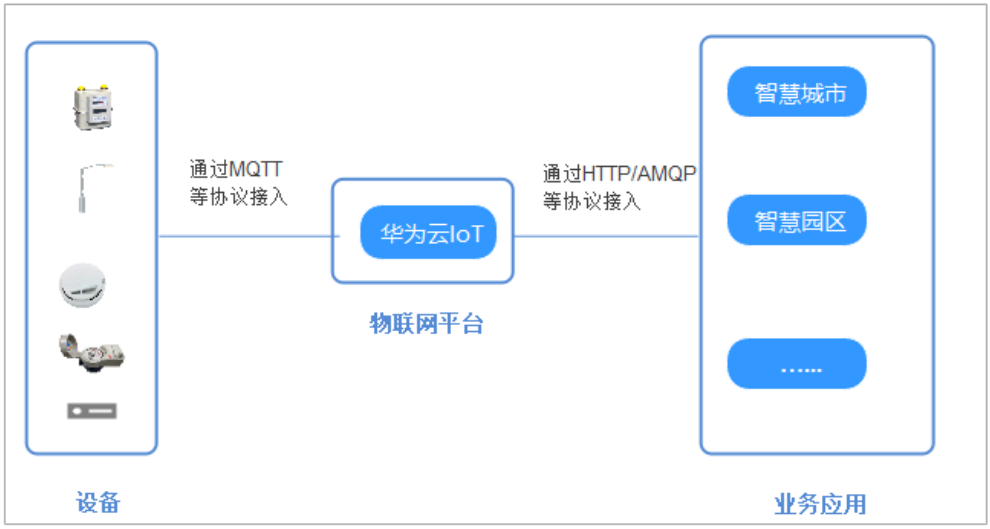
1 什么是设备接入 IoTDA

华为云物联网平台设备接入云服务（IoTDA）提供海量设备的接入和管理能力，将物理设备联接到云，支撑设备数据采集上云和云端下发命令给设备进行远程控制，配合华为云其他产品，帮助您快速构筑物联网解决方案。

使用物联网平台构建一个完整的物联网解决方案主要包括3部分：物联网平台、业务应用和设备。

- 物联网平台作为连接业务应用和设备的中间层，屏蔽了各种复杂的设备接口，实现设备的快速接入；同时提供强大的开放能力，支撑行业用户构建各种物联网解决方案。
- 设备可以通过固网、2G/3G/4G/5G、NB-IoT、Wifi等多种网络接入物联网平台，并使用LWM2M/CoAP、MQTT、HTTPS等主流协议或行业协议将业务数据上报到平台，平台也可以将控制命令下发给设备。
- 业务应用通过调用物联网平台提供的API，实现设备数据采集、命令下发、设备管理等业务场景。

图 1-1 物联网解决方案



设备接入 IoTDA 特性

物联网平台支持终端设备直接接入，也可以通过工业网关或者家庭网关接入。物联网平台支持多网络接入、多协议接入、系列化Agent接入，解决设备接入复杂多样化和碎片化难题，也提供了丰富完备的设备管理能力，简化海量设备管理复杂性，提升管理效率。IoT设备接入云服务支持的特性详见下表。

表 1-1 IoT 设备接入云服务支持特性

特性分类	功能特性	功能说明
设备接入	原生协议接入	支持MQTT/CoAP/LwM2M/HTTPS协议接入。
	系列化Device SDK	支持IoT Device SDK和IoT Device SDK Tiny，覆盖的语言包括C、Java等。详情请参考**IoT Device SDK介绍**。
	行业协议接入	支持通过边缘网关接入Modbus、OPCUA，可通过行业协议插件方式支持行业协议接入。
	设备接入鉴权	支持一机一密，X.509证书等鉴权方式。
	-	-
设备管理	设备全生命周期管理	设备增删改查、设备状态管理、设备冻结/解冻、子设备管理等。
	设备分组&标签	支持对设备进行分组或打标签，详细请参见**群组与标签**。
	设备物模型定义	对设备进行物模型定义（Product Model），详细请参见**产品模型**。
	设备影子	支持影子数据查询和影子设置，详细请参见**设备影子**。
	OTA升级	支持对设备软固件进行升级，详细请参考**OTA升级**。
	设备文件上传	支持设备上传文件到OBS，设备可向云端请求文件，详细请参见**文件上传**。
	设备批量操作	支持对设备的批量操作，包括**批量创建设备**、**批量软固件升级**和**批量命令下发**。
消息通信	双向消息透传	支持设备消息HTTP/AMQP推送到应用服务器，支持应用侧向设备以异步方式下发消息。
	物模型Topic通信	应用侧和设备侧基于物模型定义的属性、命令和事件进行解耦通信。
	自定义Topic通信	支持用户自定义Topic进行双向消息通信。
	数据解析转换	在线开发编解码插件，对设备数据进行数据解析和格式转换。

特性分类	功能特性	功能说明
	命令下发	支持以同步方式向在线设备下发命令，NB场景支持异步方式下发命令，详细请参见**命令下发**。
规则引擎	数据流转	支持数据流转到华为云Kafka/OBS/GaussDB/DIS/DMS/ROMA等服务，详细请参见**规则引擎**。
	规则联动	支持建立设备联动规则，实现联动控制，详细请参见**规则引擎**。
	数据转发	支持平台将设备上报数据通过HTTP或AMQP转发至应用服务器。
监控运维	日志能力	控制台提供消息跟踪功能，对接LTS提供日志分析能力，对接CTS提供审计日志功能，详细请参见**监控运维**。
	告警能力	系统类告警（如阈值类告警）和设备规则触发告警对接AOM提供告警通知管理能力，详细请参见**告警管理**。
	指标监控	租户级业务指标（如设备状态、命令、订阅推送、消息流转等）对接AOM提供监控报表能力，详细请参见**查看报表**。

安全&数据保护

已获国家安全等保2.0四级认证，通过ISO27001/ISO27017/ ISO27018/CSA STAR国际安全认证，数据隐私保护遵从欧盟GDPR数据隐私保护要求，建立端到端可信的安全体系。

- 设备安全：提供一机一密的设备安全认证机制，防止设备非法接入，支持设备的安全检测。
- 信息传输安全：基于TLS、DTLS、DTLS+加密协议，提供安全的传输通道。
- 平台安全：基于华为云整体进行威胁防御，充分利用华为云安全服务/组件和华为的安全研究部门，建立安全分析、设计、编码、测试、安全攻防等一整套安全防御体系。
- 数据保护：满足欧盟GDPR数据隐私保护要求。

2 产品优势

随着业务的发展，越来越多的企业选择结合物联网技术来实现自身效益增长。相比企业自建MQTT集群，使用华为云IoT服务低成本构建物联网解决方案，在能力、成本、运维、安全、生态等诸多方面具有突出优势。

表 2-1 优势对比

维度	子项	华为云IoT服务	企业基于开源MQTT集群自研
能力	协议灵活	• 广泛支持IoT主流的接入协议及私有协议，满足各类设备和接入场景要求。 • 提供插件机制，实现自定义协议解析。	只支持MQTT协议，扩展其他协议时需要再研发扩展，同时维护多协议实现难度大、成本高、效率低。
	快速接入	• 提供系列化、多语言的开源IoT Device SDK。 • 与主流模组、芯片预集成，实现多网络、多协议接入，简化设备接入难度，实现小时级设备极简接入。	需要熟悉各类语言的开发人员投入，开发工作量大。
	性能稳定	• 可实现白天单击购买就可以实现服务资源平滑弹性扩展。 • 支持亿级设备安全稳定连接、10万TPS高并发可靠通信、万级TPS并发设备上线能力。 • 服务可用性99.95%。	需要研发人员进行调优，如果要保证99.9%以上的可用性，需要精通开源MQTT研发人员以及资深的架构人员。

维度	子项	华为云IoT服务	企业基于开源MQTT集群自研
	特色功能	• Cell化技术，实现故障范围的有效控制。 • 支持消息跟踪，方便快速的故障定位和原因分析。 • 支持设备影子。 • 支持OTA升级。 • 支持物模型，将产品功能抽象归纳，形成“标准物模型”，实现软硬件解耦开发，提升系统集成效率。 • 支持插件机制，实现自定义协议解析。 • 支持数据转发规则，数据无缝流转到10+云服务。 • 支持设备联动规则，基于Time-Condition-Action自定义规则，灵活设定场景联动，实现跨应用/子系统，多设备自动化协同。 • 开放架构，及时享受云计算的前沿技术和服务。 • 功能丰富灵活，多行业完整解决方案，已成功服务众多行业客户。	开源MQTT提供了基本的功能，构筑完整解决方案时需要开发人员基于开源能力进行开发。而开发人员对开源代码进行侵入式修改，容易在开源中间件升级时遗漏修改的部分导致现网事故。
	-	-	-
	技术支持	• 7*24小时专业贴心支持。 • 工单系统10分钟响应。	开源MQTT没有支持服务，且有大量的默认配置参数，需要企业根据业务的场景进行调整，在不精通开源代码的情况下，配置者参数使用不当对商用系统造成巨大潜在风险，出现问题时候也只能自行解决。
成本	服务器成本	无需购买服务器。	需购买服务器。
	人力成本	购买云服务，无需额外人力投入。	企业自行构建，需要投入专业的开发、运维团队。
	资源使用	开箱即用，弹性灵活，业务上量，无感扩容。	企业自行构建，需要自己开发具备弹性功能。
	架构成本	基于云原生2.0构建高可用、高性能、高安全架构，持续演进。	企业自行构建，团队基于开源去实现高可用、高性能、高安全功能，难度大、门槛高。

维度	子项	华为云IoT服务	企业基于开源MQTT集群自研
运维	基础设施运维	专业团队统一运维，快速响应，扩容、升级、异常运维都由华为提供。	企业自行构建，自建运维团队或第三方运维，要解决扩容，升级，运维问题。根据业界统计，大部分的业务故障是在扩容、升级操作触发的，所以运维成本是开发成本的几倍甚至几十倍。
	服务平台版本	由公有云服务商统一更新，版本迭代快。	企业自行构建。
	全链路自诊断，高效运维	● 全链路日志分析和消息跟踪。 ● 设备状态实时监控和感知。 ● 灵活自定义业务指标告警。	企业自行构建。
安全	系统安全	已获国家安全等保四级认证，通过ISO27001/ISO27017/ISO27018/CSA STAR国际安全认证，数据隐私保护遵从欧盟GDPR标准，建立了可信的安全体系。 ● 传输网络层：结合WAF、DDOS提供边界安全防护，提供包括DTLS、TLS、HTTPS、COAPS、MQTTS等高效安全传输协议。 ● 设备边侧：提供数字证书、一机一密的接入安全，基于LiteOS的OS安全能力。 ● 平台侧：基于华为云整网视角进行威胁分析，充分复用华为云安全服务产品、公共安全服务/组件，构建安全防御体系。	企业自行构建，端到端安全是一项系统工程，门槛非常高，构筑和看护系统级的安全能力成本高、难度大。
	数据安全	具备完整的安全防护体系，数据存放在云服务提供商的数据中心，云存储级数据安全冗余。	企业自行构建，需要考虑数据冗余存储，备份存储，恢复等能力。
	灾备与容灾	业务双活、多数据中心容灾，利用多region和多AZ构筑高可用和灾备能力。	企业自行构建，自建集群通常不具备容灾能力，业务双活、容灾设备投入大，投入和收益通常不成正比。

维度	子项	华为云IoT服务	企业基于开源MQTT集群自研
	漏洞修复	建立有一整套漏洞管理体系和专门的安全研究部门，从漏洞研究，发现，跟踪，修复，有一整套体系保证漏洞的及时修复。	大部分企业没有建立漏洞的管理机制，对漏洞更新不及时，很容易被攻击，很多企业被攻击，数据被窃取也没有感知到。
生态	第三方接入	整合上下游生态资源，提供增值服务。	厂家自行构建。
	可扩展性	● 平滑扩容，从几万设备到亿级设备做到业务无中断快速扩容 ● 当业务发展需要扩展其他功能时，比如AI智能功能，可以与华为云其他大数据、EI、中间件产品无缝对接，可以方便快捷的实现海量设备数据的存储、计算以及智能分析。并且由于云化产品都可以小规模验证，可以方便客户低成本快速试错，实现业务创新	扩展周期相对长，需要自行开发与各个系统和或者组件的对接，投入的人力物力成本高。

表 2-2 费用对比

项目	华为云IoT服务	企业基于开源MQTT集群自研（以华为云资源为参考）
云资源费用	以购买1个SU3为例，每日消息数上限4,000万，上下行消息TPS峰值1,000TPS，预计折合费用每月约为1,000美元、每年约12,000美元。 总费用：预测约为12,000美元/年。	● 服务器资源：购买2台ECS实例（以新加坡区域为例，选择X86计算，通用计算型、4核CPU、8 GB内存、40 GB高IO磁盘、共享5M带宽）费用为2,102.64美元/年； ● 云数据库RDS：新加坡，一台MySQL、2核4GB、40GB SSD云盘、主备、通用型的实例费用为890.56美元/年； ● 弹性负载均衡：新加坡，按需付费，选择公网共享型负载均衡，叠加最小规格1Mbps带宽，费用预测为262.8美元/年； 总费用：3,256美元/年。

人力费用	无。	使用基础中间件实现基本功能： ● 1位工程师负责平台的日常运维和研发； ● 假设工程师投入50%的工作量，月薪10,000美元； ● 总计：10,000 × 12 × 50% = 60,000美元/年 在基础中间件的基础上叠加部分特色功能： ● 假设不考虑实现平台的高可用、高性能、高安全，仅实现部分功能性能力； ● 2位全栈开发工程师，负责实现设备管理、消息通信、规则引擎等部分能力以及平台前端和后台的开发及运维； ● 1位协议专业人才，负责实现设备接入能力（原生协议、泛协议、行业协议的设备接入能力以及SDK接入）等的设备端开发； ● 假设所有工程师投入100%的工作量，月薪10,000美元； ● 总计：3 x 10,000 x 12 x 100% = 36万美元/年。 不考虑奖金等。
总计	12,000美元/年。	实现基础功能：63,256美元/年。 实现基础功能，叠加部分特色功能：423,256美元/年。

3 应用场景

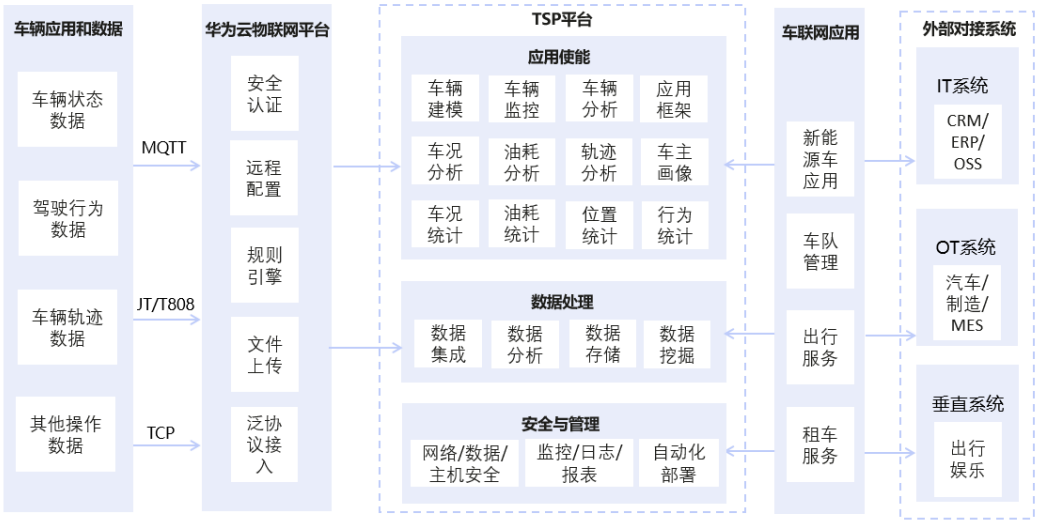
华为云物联网平台提供海量设备的接入和管理能力，支持设备数据采集上云和云端下发消息给设备，本文将介绍华为云物联网平台的典型应用场景。

车联网

需求场景：汽车厂商通过车联网平台实现车辆的便捷接入和管理，需要支持JT/T808、MQTT等协议传输数据到云端，并做数据清洗处理，便于后续做大数据分析和数据挖掘。

解决方案：华为云物联网平台支持安全可靠、低时延的连接，支持多种标准行业协议，将汽车采集的路况、车况、行驶行为等数据上传到云端，通过规则引擎和FunctionGraph做数据处理，可将数据存储在InfluxDB和DWS，便于做大数据分析，利用Modelarts做机器学习，挖掘出有价值的数据。

图 3-1 车联网场景业务架构图

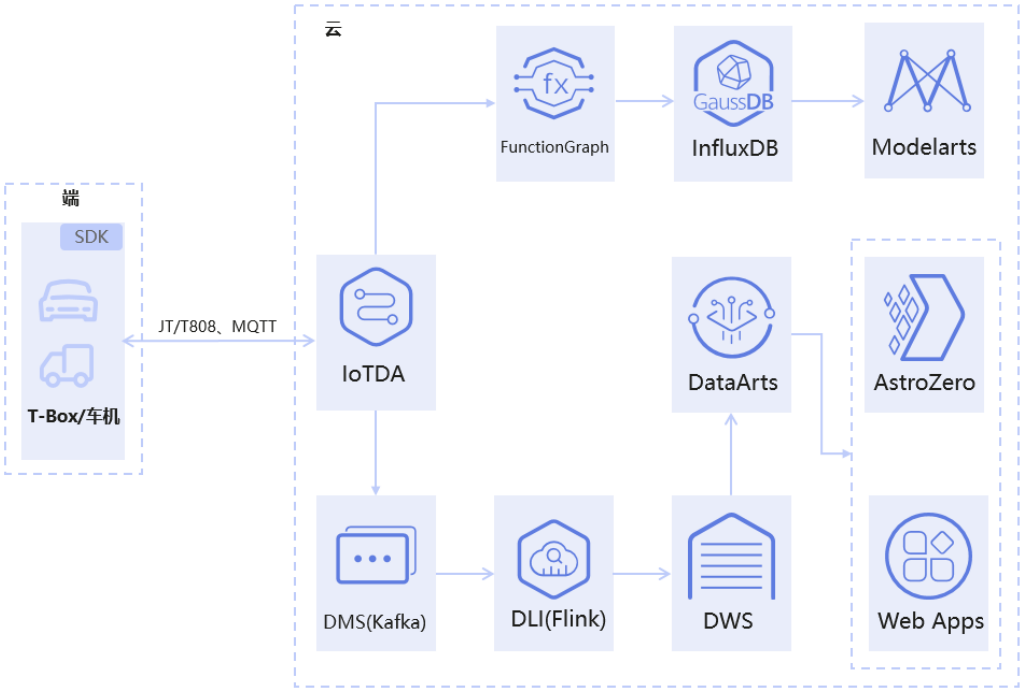


车联网场景参考架构如下：

- 端侧T-Box，车机可通过MQTT或者JT/T808协议上报车辆状态，驾驶行为，车辆轨迹等数据到云端。

- 云端IoTDA支持数据流转到不同云服务进行数据清洗，数据存储，数据分析，从而构筑多种车联网数据应用。

图 3-2 车联网场景参考架构图

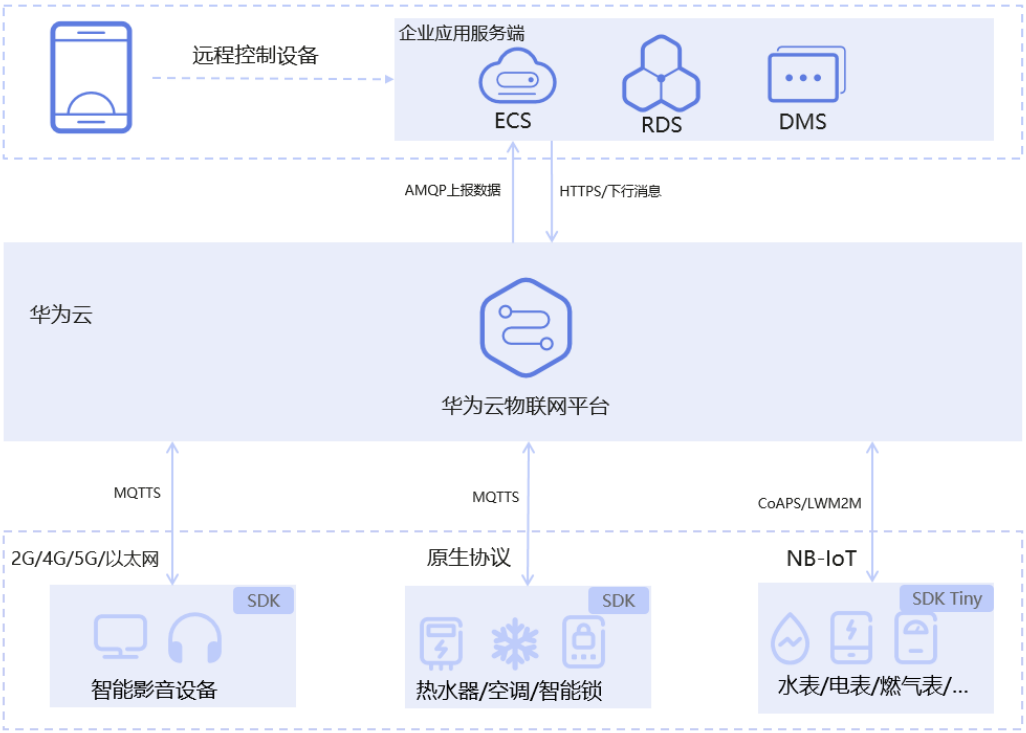


智能家居

需求场景：家用电器冰箱、空调、洗衣机、插座、电视、照明等各种家用设备需要接入上云，支持设备数据上报云端，用于感知设备的运行状态，用户还可在设备厂家提供的APP端执行命令远程控制设备。

解决方案：华为云物联网平台提供安全可靠的连接，支撑海量的设备连接，支持MQTT、CoAP、HTTP、LWM2M、WebSocket等多种协议接入，支持从云端及时下发消息和命令控制设备。

图 3-3 智能家居场景参考架构图

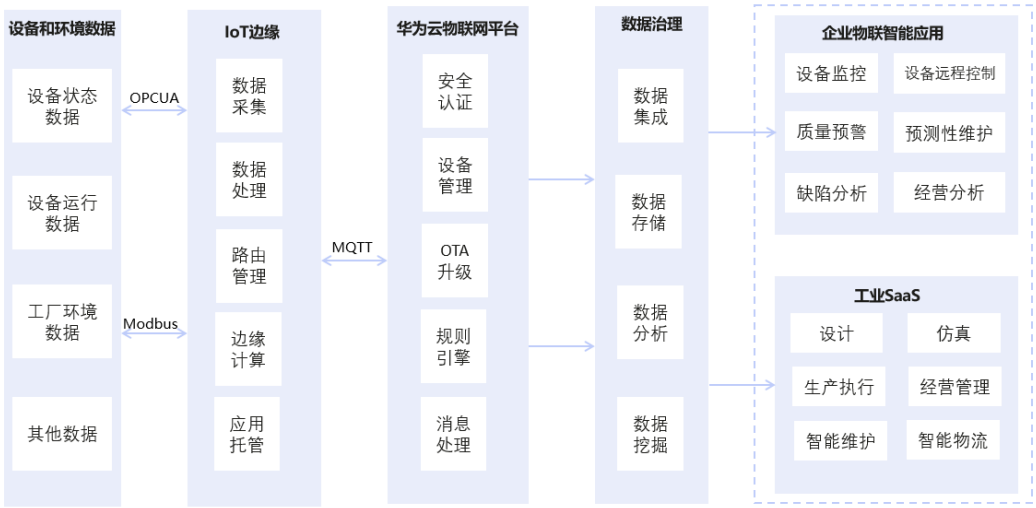


智能制造

需求场景：工厂流水线上存在多种品牌多种类型的机械设备，需要采集设备运行数据和环境监控数据，并实时计算分析设备运行状态，对异常或者故障的设备可以进行预测和告警，还可以远程对设备进行维护升级。

解决方案：工厂设备和环境数据可以通过华为云IoT边缘实现OT数据采集，通过工业网关上报到华为云物联网平台IoTDA上，并支持流转到其他云服务做数据转换和分析，企业可通过采集的设备数据对设备进行监控，如果设备运行状态偏离日常运行状态，可及时发送告警提醒设备保养检修，还可远程控制设备进行升级和维护。

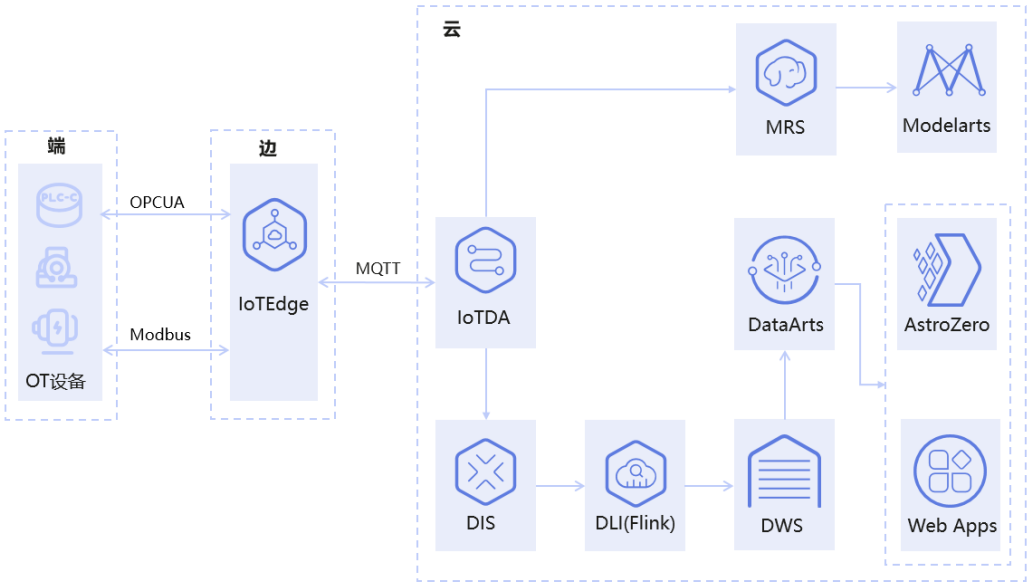
图 3-4 智能制造场景业务架构图



智能制造场景参考架构如下：

- 端侧部署边缘节点支持OPCUA，Modbus等协议，采集各种OT设备的运行数据，状态数据，以及环境监控数据，统一从边缘网关将数据上报至云端IoTDA。
- 云端IoTDA通过规则引擎将数据流转到DIS，并经过DLI-Flink处理后写入DWS，便于后续数据治理。还可流转到MRS进行大数据清洗和处理，便于后续进行AI分析和数据挖掘。

图 3-5 智能制造场景参考架构图

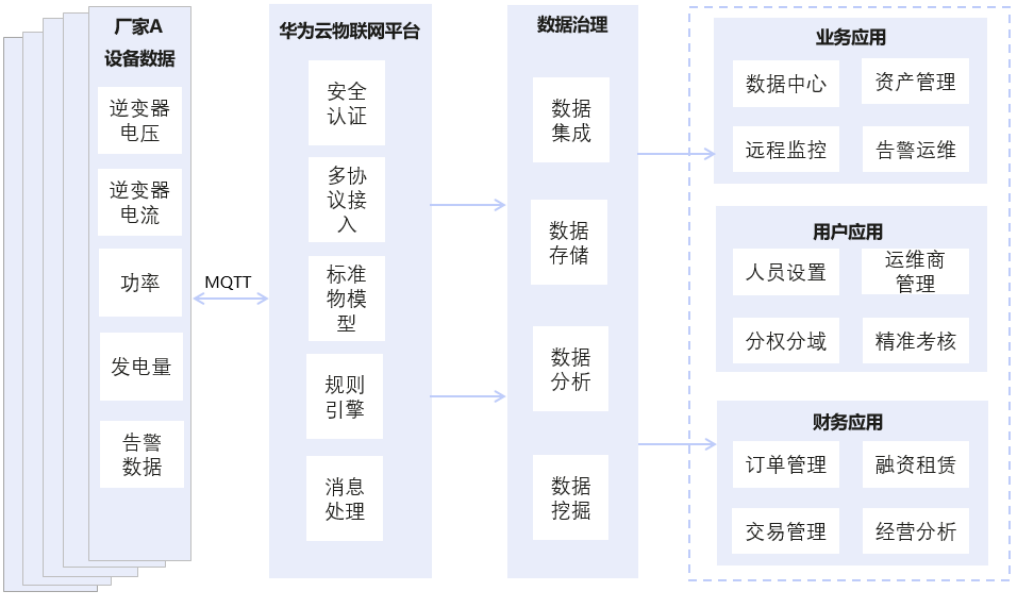


分布式光伏

需求场景：新能源公司需要将各个厂商生产的逆变器设备的电压，电流，功率，发电量以及告警数据采集上云，并做进一步的数据处理，数据分析，便于开发数据中心，告警运维，经营分析等业务应用。

解决方案：IoTDA提供标准物模型，支持多协议接入，可屏蔽多个光伏设备厂家的设备上报数据的格式和协议差异，通过规则引擎将数据流转到OBS进行存储，还可以流转到MRS进行进一步的数据处理。

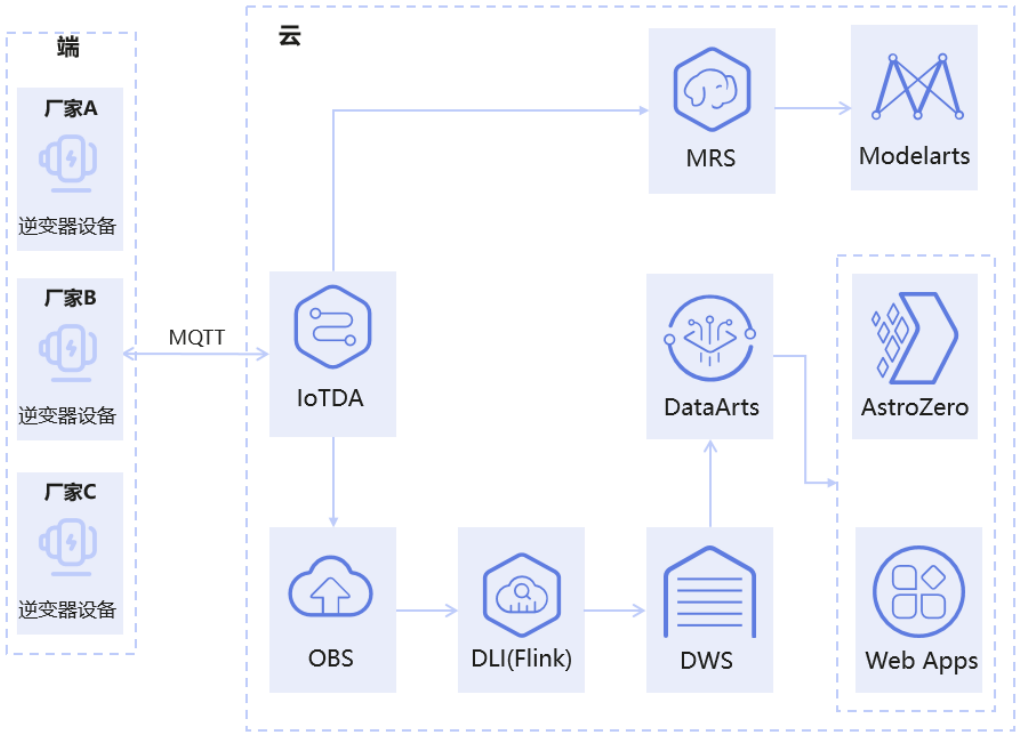
图 3-6 分布式光伏业务架构图



分布式光伏场景参考架构如下：

- 端侧不同的厂家的逆变器设备通过MQTT协议上报电压，电流，功率，发电量等数据到云端。
- 云端IoTDA通过规则引擎将数据流转到OBS存储，并经过DLI-Flink处理后写入DWS，便于后续数据治理。还可流转到MRS进行大数据清洗和处理，便于后续进行AI分析和数据挖掘。

图 3-7 分布式光伏场景参考架构图



智慧充电桩

需求场景：充电桩运营商需要采集不同厂商生产的充电桩设备的充电数据，电表信息，以及充电车辆的信息到云端，云端业务应用能实时感知用户车辆和充电桩的状态，从而进行费用计算。需要支持业务应用下发指令启动充电和关闭充电流程。

- 解决方案一：多个厂家的充电桩设备通过MQTT协议直连云端IoTDA，通过云端部署泛协议插件进行解析，支持多协议接入。云端IoTDA可直接将数据推送给客户的业务应用，还支持业务应用下发命令控制充电流程的启停。该方案适用于充电桩设备安装部署在市区，室外等网络环境较好的地方。
- 解决方案二：多个厂家的充电桩设备数据通过IoTEdge进行采集，可以在边缘节点部署协议插件应用屏蔽多个厂商的各种私有化协议，边缘节点还可以部署一些简单的业务计算应用，减少与云端的交互，边缘网关通过MQTT协议统一上报数据到云端IoTDA。云端IoTDA可将数据直接推送给客户的业务应用，还支持业务应用下发命令控制充电流程的启停。该方案适用于充电桩设备安装部署在高速服务区，地下停车场等网络环境较差的地方。

图 3-8 智慧充电桩场景业务架构图

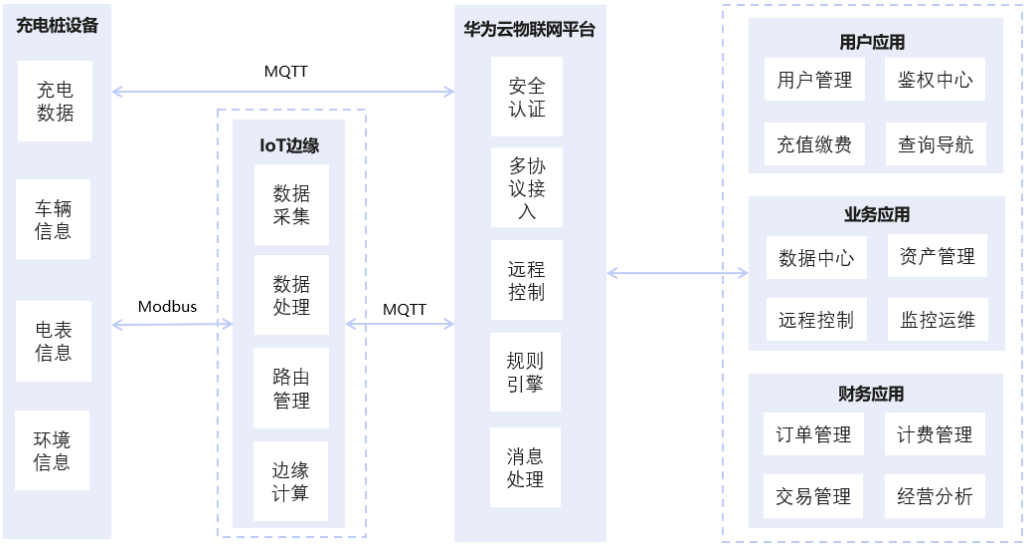
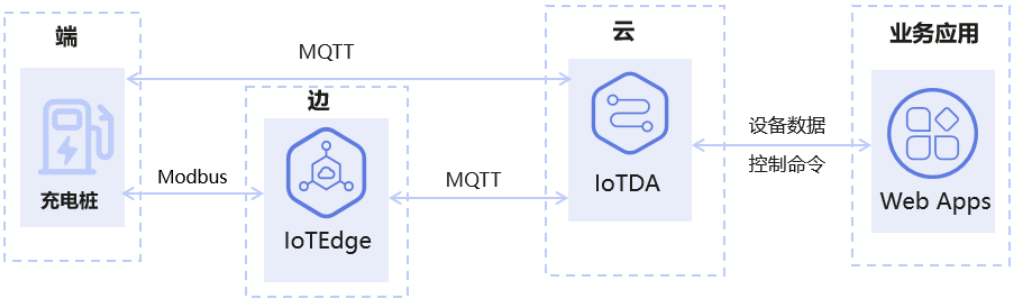


图 3-9 智慧充电桩场景参考架构图



4 产品规格

标准版规格

设备接入服务（IoTDA）提供标准版实例，用于设备接入以及业务处理。每个华为云用户在同一个Region最多可以开通一个标准版实例（若无法满足请提交工单说明需求），在标准版实例中通过选择计量单元的类型和个数来决定该实例每天设备与云端可交互的消息总数，同种类型的计量单元可叠加多个，其消息总数随之叠加，同时决定了对所有功能的**使用限制**。

开通实例后，根据其选择的计量单元类型与个数，按照使用时长（天）进行计费。详细产品价格请参见**价格计算器**，选择您想要购买的配置，然后查看页面下方的“配置费用”。详细计费说明请参见**计费说明**。

表 4-1 计量单元规格

规格名称	单元类型	消息总数/天/单元	单条消息最大大小	消息上下行TPS/单元
iotda.standard.suf	SUF	10,000条	4KB	10TPS
iotda.standard.su1	SU1	400,000条	4KB	10TPS
iotda.standard.su2	SU2	4,000,000条	4KB	100TPS
iotda.standard.su3	SU3	40,000,000条	4KB	1,000TPS
iotda.standard.su4	SU4	300,000,000条	4KB	6,000TPS

说明

- 单个标准版实例可配置多个同类型的计量单元，如5个SU1，但不能配置不同类型的单元，如2个SU1和3个SU2混合。支持随时升降单元个数及类型，如2个SU1升级为5个SU1、2个SU1升级为2个SU2。每个用户支持最多开通1个SUF进行试用，SU1、SU2、SU3、SU4支持最多100个，SUF支持升级至SU1/SU2/SU3/SU4，升级后原SUF不再保留。
- 消息数：参与计费的消息数请参见**计费说明-计费项**。建议限制调用数以确保不会超过限制，如超过限制，IoTDA会产生告警信息并拒绝该消息，请及时升级计量单元规格或增加个数。
- 消息计算大小：实例支持MQTT单条发布消息最大长度为1M，LWM2M/CoAP单个发布消息最大长度为1KB，超过此大小的发布请求将被直接拒绝。纳入消息数计算时以4KB为一条，超过4KB的消息计算为新的一条或多条。
- 设备数：单个标准版实例支持注册的设备上限为2,000,000，如需提高限制，请**提交工单**说明您的需求，支持的同时在线设备数等同于注册设备数，当仅开通SUF时注册设备数上限为1,000。
- 消息上下行TPS：消息上下行TPS是指每秒上下行消息最大吞吐量，即每秒钟实例内所有设备发送到云端，和云端发送到设备的消息总数量，标准版实例的配额根据其计量单元的类型及个数决定。若不能满足您的业务需求，请**提交工单**说明您的需求。
- 其他：除上表所列的实例规格和配额限制外，其他各项默认配额或限制，请参考**使用限制**。

一个计算您需要何种规格实例的样例如下：

- 场景：用户开通设备接入服务标准版实例，计划注册10万设备，平均每天同时在线设备为1万，平均每在线设备每5秒向云端发送一条消息（小于4KB），暂无API调用及推送消息，每天工作时长为8小时。
- 则消息上下行TPS为：1万设备 ÷ 5秒/条消息/设备 = 2,000条消息/秒 = 2,000 TPS，每天消息总数为：8小时 x 1万设备 ÷ 5秒/条消息/设备 = 8 x 60 x 60 秒 x 2,000 TPS = 57,600,000 条消息；则需购买2个SU3（TPS：2,000，每天消息数80,000,000条，设备数默认上限200万，每月约1,050USD x 2 = 2,100 USD）或者20个SU2即可满足诉求，每天产生使用账单触发扣费。

5 使用限制

用户在IoT物联网平台开发或使用时有以下技术规格限制，如果限制数量不能满足您的业务需求，请**提交工单**说明您的需求。

表 5-1 资源约束

分类	对象	描述	限制
实例管理	标准版实例	单个标准版实例可购买单元数量，详情请参考**标准版实例**。	100个
资源空间管理	**资源空间**	单个IoTDA实例支持的资源空间数量。	10个
设备接入	MQTT	MQTT协议标准。	支持MQTT v3.1/v3.1.1/v5.0协议版本，不支持协议中的QoS2、will、retain msg。
		MQTT协议支持的安全等级。	支持TLS1.1、TLSV1.2、TLSV1.3。
		MQTT连接心跳时间。设备端连接心跳设置，请参见**建立连接**。	30至1200秒，推荐设置为120秒。设置的心跳时间不在此区间内，服务器会拒绝连接。
		最大超时时间=心跳时间*1.5，超过最大超时时间未收到设备消息，服务器会自动断开连接。	
		同一时间内，单个设备允许和IoTDA建立连接的数量。	1个
		MQTT自定义Topic支持的最大长度。	128字节
		MQTT单条发布消息最大长度（超过此大小的发布请求将被直接拒绝）。	1MB
		单个MQTT连接的最大订阅数量。	50个

分类	对象	描述	限制
		单个MQTT连接最大带宽。	1MB/s
		单个MQTT连接每秒最大上行消息数量。	50条
		单个IoTDA实例设备每秒最大新建连接请求数量。	标准版请参考**标准版规格**。
		单个IoTDA实例设备侧每秒最大上行的请求数量（单消息payload平均为512字节）。	标准版请参考**标准版规格**。
	CoAP/LwM2M	支持的CoAP协议版本。	支持RFC7252标准3
		支持的LWM2M协议版本。	支持1.0.2版本
		LwM2M/CoAP使用的传输层协议。	使用UDP协议
		CoAP支持的安全等级。	采用DTLS v1.2保证通道安全
		支持CoAP消息包大小。	1KB
		单设备每分钟消息数。	300条
	HTTP	支持的HTTP协议版本。	HTTP/1.0 ，HTTP/1.1
		支持的TLS版本。	TLS1.1，TLSV1.2
		支持的body体最大消息大小。	1MB
设备管理	产品	单个资源空间下产品数量。	1,000个
		单个产品下服务能力JSON大小。	500KB
		单个产品下服务数量。	500个
		单个服务能力下属性/事件/命令数量。	500个
	自定义topic	单个产品自定义topic。	50个
	标准版设备数	单个标准版（SU1，SU2，SU3，SU4）支持的最大注册设备数。	2,000,000个(如需提高限制，请提交工单)
		SUF注册设备数	1,000个
	设备	单个网关设备下最多可添加的子设备数量。	50,000个
		网关结构层次最大深度。	2级
	设备标签	单个设备支持设置的标签数量。	10个
	群组	单个群组层次结构的最大深度。	5级

分类	对象	描述	限制
		单资源空间最大群组数。	1,000个
		单个群组内最多可添加的设备数量。	20,000个
		单个设备最多可以被添加的群组数量。	10个
	批量任务	单次批量注册最多的设备数量。	100,000个
	编解码	单个产品可携带的编解码插件数量。	1个
		离线上传的编解码插件包大小。	4MB
		编解码脚本最大长度。	1MB
		单次调用编解码请求的超时时间。	5s
	设备联动规则	单个IoTDA实例最多可添加的规则数量。	基础版/标准版20个
			企业版200个
		单个规则最多支持设置动作数量。	10个
		单个IoTDA实例设备每秒最大执行规则动作数量。	基础版/标准版10个
			企业版100个。
		单个IoTDA实例持续时长等待任务数限制。	基础版/标准版100个。
			企业版1000个。
	批量任务	单个资源空间下最多同时处理的批量任务数量。	10个
		批量任务文件最大限制。	2MB
		批量任务文件最大行数。	100,000行
		单个IoTDA实例下支持的批量任务文件最大个数。	10个
	OTA升级	单个升级包大小。	升级包上传到IoTDA限制为20MB，升级包上传到OBS存储不限制升级包大小。
		单个资源空间支持上传升级包的个数。	200个
		单个资源空间上传最大文件大小。	文件上传到IoTDA限制为500MB，文件上传到OBS不限制文件大小。

分类	对象	描述	限制
消息通信	同步命令	同步命令设备响应时间。	20秒
	设备消息	设备下发消息老化时长。	24小时
		设备下发消息最大消息大小。	256KB
		单个设备下发消息缓存数量。	20个
	设备属性	网关上报子设备属性时一次最大可上报子设备数量。	100个
	异步命令	设备异步命令老化时长。	48小时
		设备异步命令最大消息大小。	256KB
		设备异步命令缓存数量。	20个
消息流转	转发规则、转发动作	单个IoTDA实例允许配置规则数量。	100个
		单规则允许的最大动作数量。	10个
		转发规则中select参数长度限制。	0.5KB
		转发规则中where参数长度限制。	0.5KB
	消息流转缓存策略	消息缓存大小。	1GB
		消息缓存时间。	24小时
	AMQP	AMQP协议。	支持AMQP1.0协议版本
		支持的TLS版本。	TLS1.2版本
		单个IoTDA实例允许配置的队列数量。	100个
		单连接监听的队列数量。	10个
		单个IoTDA实例连接数量。	32个
	流转积压流控策略	数据转发积压策略配置数量	1个
		数据转发流控策略配置数量	4个
证书管理	证书配置	单个IoTDA实例支持的设备CA证书数量。	100个
		单个IoTDA实例支持的应用CA证书数量。	10个

应用侧API使用限制如下：

单个账号调用单个API的每秒最大次数，具体API无特殊说明的，默认限制100/s。单个账号调用API的每秒最大次数：标准版：100/s。

6 安全

6.1 责任共担

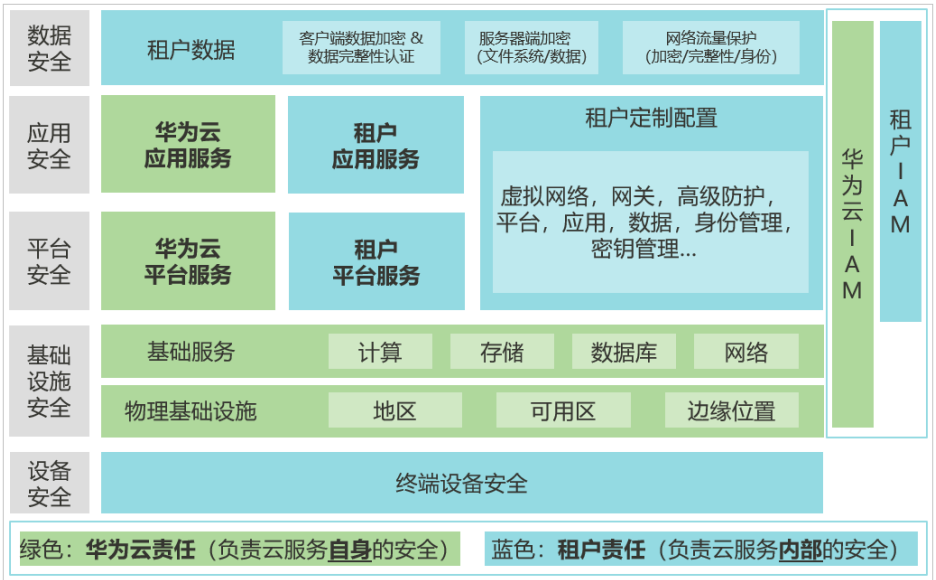
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图6-1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 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

身份认证

用户访问IoTDA的所有接口都需要携带身份凭证，并进行身份的合法性校验。IoTDA不同的接入场景需要携带不同的身份凭证，主要有如下四种场景：

- IoTDA应用侧接口支持IAM Token认证和访问密钥（AK/SK）认证两种认证方式进行认证鉴权，关于Token和访问密钥的详细介绍和获取方式，请参考**认证鉴权**。
- 设备侧MQTT连接鉴权，需要携带ClientId，设备ID和加密后的设备密钥进行认证鉴权，详细流程请参考**MQTT设备连接鉴权**。
- 设备侧HTTP连接鉴权，需要携带设备ID，密码校验方式，时间戳以及加密后的设备密钥进行认证鉴权，详细流程请参考**HTTP设备连接鉴权**。
- AMQP客户端与IoTDA平台连接鉴权，需要携带接入凭证键值（accessKey）和接入凭证密钥（accessCode）进行认证鉴权，详细说明参考**AMQP客户端接入说明**。

访问控制

IoTDA支持通过IAM进行访问控制。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。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予IoTDA所需的权限，组内用户自动继承用户组的所有权限。

IAM中为各云服务预置了系统权限，方便您快速完成基础权限配置，**表1**为IoTDA的所有系统权限。

表 6-1 IoTDA 的所有系统权限

系统角色/策略名称	描述	类别
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。	系统角色
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。	系统角色
IoTDA FullAccess	拥有该权限的用户拥有访问IoTDA资源的所有执行权限。	系统策略
IoTDA ReadOnlyAccess	拥有该权限的用户拥有访问IoTDA资源的只读权限。	系统策略

6.3 数据保护技术

责任共担模式适用于IoTDA的数据保护，如该模式中所述，IoTDA负责服务自身的安全，提供安全的数据保护机制。用户负责安全地使用IoTDA服务，包括使用时的安全参数配置以及维护使用IoTDA及其依赖的其他云服务权限的控制。

表 6-2 数据保护技术说明

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	IoTDA支持HTTPS传输协议，为保证数据传输的安全性，建议使用TLS 1.2或更高版本	**使用HTTPS协议接入**
传输加密（MQTTS）	IoTDA支持MQTTS传输协议，为保证数据传输的安全性，建议使用TLS 1.2或更高版本，加密套件推荐使用TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256和TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	**MQTT协议支持说明**

数据保护手段	简要说明	详细介绍
传输加密（AMQPS）	IoTDA支持AMQPS传输协议，为保证数据传输的安全性，接收方必须使用TLS加密，且使用TLS1.2及以上版本，不支持非加密的TCP传输	AMQP客户端接入说明

6.4 审计与日志

审计

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。CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

用户在使用物联网平台的过程中，通过云审计服务（Cloud Trace Service，CTS），可查看用户及平台的操作及结果。关于设备接入审计记录的详细介绍，请参见**查看审计日志**。

日志

华为物联网平台支持记录平台与设备端，周边应用系统之间的对接情况，并以日志的形式上报到云日志服务（LTS），由LTS提供实时查询、海量存储、结构化处理和可视化图表分析能力。

关于设备接入日志记录的详细介绍，请参见**查看运行日志**。

6.5 监控安全风险

IoTDA提供了多个维度的监控运维能力，包括设备消息跟踪，查看报表，告警管理以及设备异常检测，方便用户实时掌握所有接入IoTDA的设备信息。

- **设备消息跟踪**：在设备鉴权，命令下发，数据上报，平台数据转发等业务场景发生故障时，可以通过消息跟踪进行快速定位和原因分析。
- **查看报表**：IoTDA为用户提供了丰富的报表功能，用户可以通过不同维度查看各类报表统计信息，包括设备消息，设备状态，设备总数等。
- **告警管理**：IoTDA基于AOM的告警通知能力，当用户设置了一定的规则，并且触发了相应的条件后，平台就会上报告警通知到用户，用户需要密切关注告警并及时处理。

6.6 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 6-2 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 6-3 资源中心

7 基础概念

基本概念

名词	描述
设备接入（IoTDA）	是华为云的物联网平台，提供海量设备连接上云、设备和云端双向消息通信、批量设备管理、远程控制和监控、OTA升级、设备联动规则等能力，并可将设备数据灵活流转到华为云其他服务和第三方应用，帮助物联网行业用户快速完成设备联网及行业应用集成。
资源空间	在物联网平台中为您的业务应用划分的一个资源空间，您在平台中创建的资源（如产品、设备等）都需要归属到某个资源空间，您可以基于资源空间实现多业务应用的分域管理，包括资源隔离和授权管理。
AppID	即资源空间ID（接口调用时参数名为app_id）作为资源空间的唯一标识。
ProjectID	项目ID，用于资源隔离，华为云的每个区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以区域默认项目为单位进行授权，IAM用户可以访问您账号中该区域的所有资源。
边缘节点	是物联网的边缘“小脑”，在靠近物或数据源头的边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供计算和智能服务，满足行业在实时业务、应用智能、安全与隐私保护等方面的基本需求。
模组	又称通信模组，由若干个显示模块、驱动电路、控制电路、芯片以及相应的结构件构成的一个独立的显示单元，设备通过通信模组具备与物联网平台的通信能力。当前模组厂商主要提供Wifi、NB-IoT、2G/3G/4G/5G等通信模组。

设备接入

名词	描述
设备	归属于某个产品下的设备实体，每个设备具有一个唯一的标识码。设备可以是直连物联网平台的设备，也可以是代理子设备连接物联网平台的网关。

名词	描述
设备ID	即deviceID，用于唯一标识一个设备，在注册设备时由物联网平台分配获得，是设备在IoT平台上的内部标识，用于设备接入时鉴权，及后续在网络中通过deviceID进行消息传递。
设备标识码	即nodeID，设备唯一物理标识，如IMEI、MAC地址等，用于设备在接入物联网平台时携带该标识信息完成注册鉴权。
CoAP/CoAPS	受约束的应用协议CoAP（Constrained Application Protocol）是一种软件协议，旨在使非常简单的电子设备能够在互联网上进行交互式通信。 CoAPS指CoAP over DTLS，在CoAPS中使用DTLS协议进行加密传输。
LWM2M	LWM2M（lightweight Machine to Machine）是由OMA（Open Mobile Alliance）定义的物联网协议，主要使用在资源受限（包括存储、功耗等）的NB-IoT终端。
MQTT/MQTTS	MQTT（Message Queue Telemetry Transport）是一个物联网传输协议，被设计用于轻量级的发布/订阅式消息传输，旨在为低带宽和不稳定的网络环境中的物联网设备提供可靠的网络服务。 MQTTS指MQTT+SSL/TLS，在MQTTS中使用SSL/TLS协议进行加密传输。
设备CA证书	由国际知名的证书机构VeriSign、Symantec和GlobalSign等CA（Certification Authority）机构进行签发，用于HTTPS建链时服务端和客户端之间的身份合法性验证。
设备X.509证书	是一种用于通信实体鉴别的数字证书，创建认证方式为X.509证书的设备后，物联网平台为设备颁发对应的X.509证书。
密钥	用于设备采用原生MQTT协议接入物联网平台时的鉴权认证。
预置密钥	当NB-IoT设备、集成SDK的设备接入时，预置密钥用于设备和物联网平台之间的传输通道安全加密。

设备管理

名词	描述
IAM	IAM，统一身份认证服务（Identity and Access Management）提供身份认证和权限管理功能，可以管理用户（比如员工、系统或应用程序）账号，并且可以控制这些用户对您名下资源的操作权限。
产品	某一类具有相同能力或特征的设备的集合称为一款产品。帮助开发者快速进行产品模型和插件的开发，同时提供端侧集成、在线调试、自定义Topic等多种能力，端到端指引物联网开发，帮助开发者提升集成开发效率、缩短物联网解决方案建设周期。
产品模型	产品模型（Product Model），也称物模型，用于描述设备具备的能力和特性。开发者通过定义产品模型，在物联网平台构建一款设备的抽象模型，使平台理解该款设备支持的服务、属性、命令等信息。

名词	描述
产品ID	即ProductID，设备所属的产品ID，用于关联设备所属的产品模型。
服务	即Service，产品模型的一部分，描述设备具备的业务能力。将设备业务能力拆分成若干个服务后，再定义每个服务具备的属性、命令以及命令的参数。
属性	即Property，产品模型的一部分，一般用于描述设备运行时的状态，如环境监测设备所读取的当前环境温度等。
Topic	Topic是UTF-8字符串，是发布/订阅（Pub/Sub）消息的传输中介。可以向Topic发布或者订阅消息。
命令	设备的功能模型之一，设备能够被外部调用的能力或方法。
事件	设备的功能模型之一，设备运行时的事件。事件可以被订阅和推送。
编解码插件	物联网平台和应用服务器使用JSON格式进行通信，所以当设备使用二进制格式上报数据时，开发者需要在物联网平台上开发编解码插件，帮助物联网平台完成二进制格式和JSON格式的转换；当设备使用JSON格式上报数据时，开发者也可以开发对应的编解码插件，完成JSON格式之间的转换。
网关	具有子设备管理功能，并代理子设备直接连接物联网平台的设备。
子设备	不与IoT平台直连，通过网关连接IoT平台的设备。
固件	固件（Firmware）一般是指设备硬件的底层“驱动程序”，承担着一个系统最基础最底层工作的软件，比如计算机主板上的基本输入/输出系统BIOS（Basic Input/output System)。 固件升级又称为FOTA（Firmware Over The Air），是指用户可以通过OTA的方式对支持LWM2M协议和MQTT协议的设备进行固件升级。例如，NB-IoT模组的升级称为固件升级。
软件	软件（Software）一般分为系统软件和应用软件，系统软件实现设备最基本的功能，比如编译工具、系统文件管理等；应用软件可以根据设备的特点，提供不同的功能，比如采集数据、数据分析处理等。 软件升级又称为SOTA（Software Over The Air），是指用户可以通过OTA的方式支持对LWM2M协议和MQTT协议的设备进行软件升级。例如，MCU的升级称为软件升级。
PCP协议	平台升级协议（PCP协议）规定了设备和平台之间升级的通信内容与格式，用于实现设备的升级。
群组	群组是一系列设备的集合，用户可以对应用下所有设备，根据区域、类型等不同规则进行分类建立群组，以便处理对海量设备的批量管理和操作。
标签	物联网平台支持定义不同的标签，并对设备打标签。
设备影子	设备影子是一个JSON文件，用于存储设备的在线状态、设备最近一次上报的设备属性、应用服务器期望下发的配置（期望值）。每个设备有且只有一个设备影子，设备可以获取和设置设备影子以此来同步状态，这个同步可以是影子同步给设备，也可以是设备同步给影子。

数据流转

名词	描述
规则引擎	物联网平台根据用户设置的规则和设备上报的数据，当设备满足设置的条件时，即触发对应动作，给设备下发命令或将数据转发给公有云其他服务进行进一步整合利用。包含设备联动和数据转发两种类型。
订阅推送	订阅：是指应用服务器通过调用物联网平台的API接口，向平台获取发生变更的设备业务信息（如设备注册、设备数据上报、设备状态等）和管理信息（软固件升级状态和升级结果）。 推送：是指订阅成功后，物联网平台根据应用服务器订阅的数据类型，将对应的变更信息推送给指定的URL地址或AMQP消息队列。
token	鉴权参数，访问物联网平台API接口的凭证。应用服务器首次访问物联网平台的开放API时，需调用鉴权接口完成认证鉴权，获取X-Auth-Token。
AMQP	指高级队列消息协议（Advanced Message Queuing Protocol），一个提供统一消息服务的应用层标准高级消息队列协议，是应用层协议的一个开放标准，为面向消息的中间件设计。平台可以通过AMQP协议和应用服务器进行通信和数据流转。