物联网云平台上云与自建对比分析白皮书

2022 年 11 月

亚马逊云科技

目录摘要

1 摘要介绍 4
1.1 摘要 4
1.2 概念和架构分层 4
1.3 物联网管理平台模块构成 5
1.4 物联网平台的通用设计原则建议 8
2 物联网云平台的成本构成 8
2.1 云平台成本构成 8
2.2 云平台场景分类 9
3 自建云平台的常规成本构成 10
3.1 基于公共云资源自建 10
3.2 纯专有云自建 11
4 托管模式与自建模式对比 11
5 托管模式与自建模式其他对比和差异 11
6 亚马逊云科技物联网 IoT 平台服务概述 15
6.1 设备软件 16
6.2 连接控制和服务 17
6.3 数据应用和服务 18
7 总结 18
8 缩略语 19
9 文档历史 19

10 说明 19

1 摘要介绍

1.1 摘要

本白皮书第一部分通过介绍物联网的发展、组成和分层逻辑进行物联网平台的简要介绍并以亚马逊云科技物联网平台为例进行平台相关功能模块的介绍以及商业计费方式的展示。第二部分通过对于利用云基础设施进行云平台自建以及使用云计算服务商的物联网管理平台相关的功能特性、成本构成进行了分析和对比。第三部分在成本基础上对于其他重要要素进行了对比和讨论。最后介绍了亚马逊云科技物联网 IoT 平台相关物联网设备管理服务的适用场景和优势特性。

1.2 概念和架构分层

物联网

从传统的互联网（“IoI”，Internet of Information) 到移动互联网（“IoP”，Internet of People) 再到物联网(IoT, Internet of Things)，物联网，即万物相连的互联网，作为在互联网基础之上的延伸和扩展和移动物联网基础上人机物的互联互通, 通过网络（局域网或蜂窝网）将物与物以及物与人进行连接而无需人为管理就能实现正常运行的机制。物联网让此前的移动互联网的主体从”人”变为了”物”。“物”替代了“人”成为了信息的重要生产者和消费者。

物联网平台

根据 Frost 报告数据(链接), 2021 年全球约有 300 亿物联网设备。到 2026 年预计将达到 659 亿台设备（年复合增长率 16%）。作为物联网设备管理中的“大脑”，物联网平台作为让互联设备可以轻松安全地与云应用程序和其他设备交互的管理控制层, 承担着对于设备的连接管理、数据安全保护、数据处理与分析以及联动云平台上层其他模块和服务等各项核心职能。如何基于业内最佳实践的方法论构建物联网平台成为了相关企业的重要议题。

物联网系统

组网形态上, 一个典型的物联网系统通常包括**终端硬件, 终端软件, 终端管理平台, 数据业务服务**等几大模块和构成。

终端硬件即工业生产环境及日常生活等现实环境中的各种终端硬件。

终端软件包括运行在终端硬件上的操作系统，SDK，连接组件，软件接口等相关软件和服务。

物联网管理平台包括设备鉴权、网关、双向消息通讯、规则引擎、设备影子、设备注册管理等包括消息管理、控制管理及数据管理功能在内的平台系统。

数据服务包括设备管理平台上层的其他服务，包括数据库、存储、机器学习，人工智能（AI）、流分析、搜索服务、消息管理、监控检测等各项上层服务，帮助物联网平台用户快速完成设备的联网控制以及上层应用的快速开发。

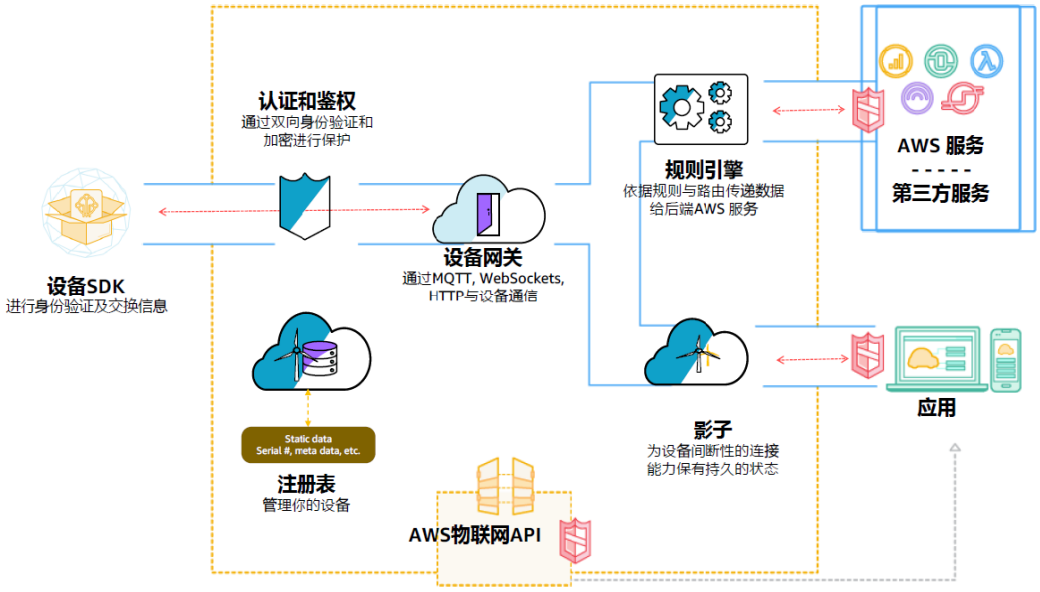
基于亚马逊云科技的行业实践，将物理网设备管理分为如下分层和抽象：

	功能要点	IoT管理负荷关注重点
分析应用层	获得数据洞察、构建上层应用	存储、分析、AI/ML、上层应用
提取层	将设备数据提取并进行解耦和分离	规则引擎、流处理、队列管理、消息通知
通信层	连接、消息路由、端云连接	设备注册、设备影子、API网关
供给层	设备识别、公钥设施、设备运维及退网	X.509证书、私有CA证书
边缘层	物理硬件、嵌入操作系统、固件和软件	指令集、端侧（及周边）的操作系统，协同性
设计和制造层	产品概念、商业和技术需求、产品生产及制造	产品功能性能要求、设备证书管理

1.3 物联网管理平台模块构成

组网结构

一个较典型的物联网管理平台组网结构如下图，终端设备在本地完成数据采集后，基于设备 SDK（软件开发工具包）， 通过 MQTT 协议的“发布”（Publish）机制将主题（Topic）及相关载荷（Payload）上送到终端管理平台。终端管理平台主要完成设备经过认证鉴权后的消息代理路由，安全连接管控，设备影子管理，规则引擎触发及平台云业务集成等功能。



物联网管理平台功能

在物联网管理平台上，核心的功能模块如下：

各个模块的具体功能描述如下表：

模块	具体功能
消息收发类	
设备网关	基于 MQTT, WebSockets 及 HTTP 等协议的设备网关。使设备能够安全高效地与 Amazon IoT 进行通信。设备通信由使用 X.509 证书的安全协议提供保护。同时包括 LoRa 等设备的网关功能。
消息管理	基于 MQTT 等协议的消息管理机制（发布与订阅模式）及基于消息的双向响应触发机制以及消息的 QOS 管理。
规则引擎	包括对消息计算处理、过滤、填充、路由等规则的管理、基于规则相关服务 API 的管理并将数据连接到其他 IoT 服务以进行存储和额外处理（如写入数据库，调用无服务计算，消息处理后的重新发布等）。
控制服务类	
安全鉴权	设备和物联网平台之间基于 X.509、Sigv4 等其他数字证书进行终端和平台的相互认证和鉴权。包括终端侧鉴权和服务器端鉴权。 安全保护包括数据加密、传输加密、授权及接入管理、访问控制、日志监控、合规验证等功能；同时包括客户基于平台的无服务器计算平台的自定义鉴权机制。
设备管理	设备物模型在物联网平台的创建、描述、更新和删除以及对应证书的管理；设备的静态和动态的分组分类、增删改、策略管理
设备监控	日志、命令行、参数指标的监控和管理
数据服务类	
设备影子	将实体设备同线上状态解耦和状态同步管理，无论设备是否在线可保持设备的状态，以便应用程序可以与设备通信。

其他类	包括设备群管理、配置审计、预部署验证管理、Alexa 语音服务（AVS）

1.4 物联网平台的通用设计原则建议

根据亚马逊云科技的行业实践，物联网平台的设计时需考虑的原则如下，而亚马逊云科技的物联网管理平台也是基于此原则进行构架和设计。

海量容量的处理层

多任务处理，不影响正常业务

面向离线行为设计

面向设备的离线行为和状态进行设计和考量

“瘦”于端而”富”于云

基于端侧的原始数据进行云端的处理

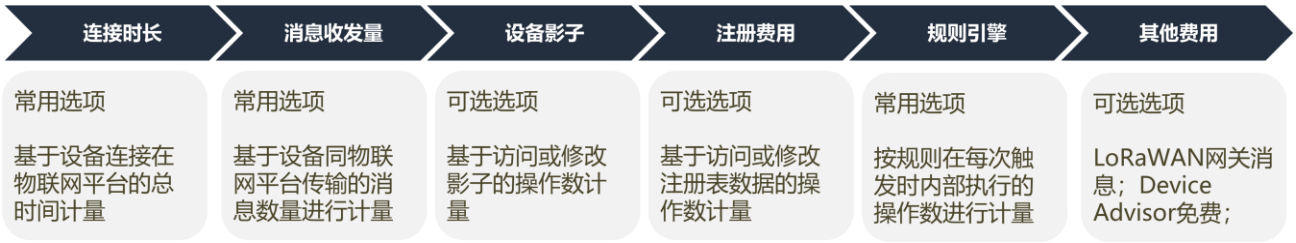
确保设备的状态检查

固件设计时需设计定期同步机制

2 物联网云平台的成本构成

2.1 云平台成本构成

以亚马逊云科技物联网管理平台 Amazon IoT Core 为例，下面是此管理平台的基本成本构成要素：



具体成本计算规则概要如下：

成本项目	计量规则
连接时长	连接按分钟级别的增量进行计量，基于设备连接到 Amazon IoT Core 的总时间进行计量
消息收发量	设备传入和传出 Amazon IoT Core 的总消息量。消息收发按设备与 Amazon IoT Core 之间传输的消息数进行计量
设备影子	按实际访问或修改设备影子操作数进行计量
注册表	按实际访问或修改注册表操作数进行计量
规则引擎	规则引擎的用量按实际规则在每次触发时基于规则内执行的操作数进行计量，其中每条规则至少执行一项操作
LoRaWAN 消息及 FUOTA	LoRaWAN 基于消息数量定价，FUOTA 基于设备任务，每次每台设备的 FUOTA 定义为一个任务

2.2 云平台场景分类

场景分类

本白皮书对于设备云管理平台的成本进行预估基于如下场景和模型设定：

分类	定义量化模型指标定义	典型场景
小规模	设备量在 10,000 (10K) 台以内；消息频度在分钟级别（每 5 分钟 1 次消息），正常报文长度（5K 字节内）；24 小时连接；小型和中型设备不考虑设备影子；总量按月平均注册；	固定设施类充电桩，医疗设备，工业设备，清洁/送餐机器人等
中等规模-常规场景	设备量介于 10K-100K 间，消息频度在分钟级别（每 5 分钟 1 次消息），正常报文长度（5K 字节内）；24 小时连接；	二轮车，家用机器人，家电设备等
中等规模-高频场景	设备量介于 10K-100K 间，消息频度在秒级别（每分钟 6 次消息），正常报文长度（5K 字节内）；24 小时连接；	跟踪器，商用零售设备收银机，扫码枪， 工业网关，除草机等
大型规模-常规场景	设备量大于 100K，消息频度在分钟级别（每 5 分钟 1 次消息），正常报文长度（5K 字节内）；24 小时连接；	城市水表电表、路灯，监控 IPC
大型规模-高频场景	设备量大于 100K，消息频度在秒级别（每分钟 6 次消息），正常报文长度（5K 字节内）；24 小时连接；	运动手表，智能音箱，实时 IPC，汽车电子等

3 自建云平台的常规成本构成

3.1 基于公共云资源自建

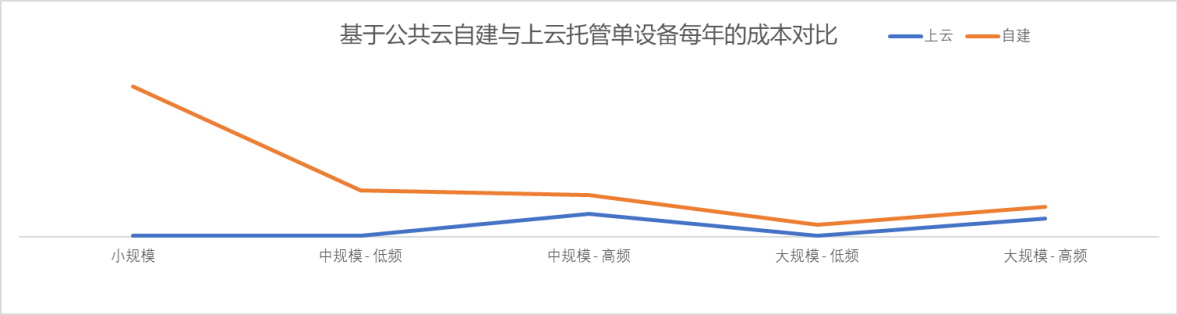
基于公用云基础设施资源进行 IoT 物联网平台进行构建，总体的成本构成如下：

3.2 纯专有云自建

基于公共云基础设施的规模效应，公共云基础设施总体 TCO 已远低于纯专有云，因此纯专有云自建成本将远高于基于公共云基础设施的建设成本。且按照业界实践，基于专有云自建的物联网管理平台通常承载的功能和业务一般不限于设备管理本身，而是包括了公司整体的其他 IT 系统，因此本白皮书将不对纯专有云自建进行详细讨论。

4 托管模式与自建模式对比

如下为汇总后的基于云平台的物联网托管管理平台（“托管模式”）和基于云计算基础设备进行物联网管理平台自建（“自建模式”）的综合成本均摊到设备每台每年的成本费用估算示意如下：



5 托管模式与自建模式其他对比和差异

除成本维度的区别外，如下维度也是托管模式和自建模式在选择过程中需要关注的维度和重点。

考虑维度	需关注重点	基于亚马逊云科技 物联网平台所具备的现有能力	自建平台
功能层面	除常用的设备网关、消息代理等之外的其他自建需考虑的功能模块满足	1. 设备认证、鉴权、签名等身份鉴别管理； 2. 数据分析工具集成； 2. 多种协议网关支持（除 MQTT 外的 LoRa、HTTPS、TLS 等）； 3. 设备影子功能和设备注册功能； 4. 数据化可视化分析； 7. Alexa 语音集成，轻松构建智能家居控制 8. 基础设施托管和维护；	均需另行独立开发，基础设备需专职维护和管理
其他上层应用的对接的全栈服务	上层各项扩展功能的水平和垂直扩展能力	无缝对接亚马逊云科技全球 200 多个大类的包括人工智能、机器学习、数据训练、图像视频流分析、无服务器计算、搜索服务、告警监控、机器人仿真和机群管理等服务在内的多项功能服务； 从边缘到云端提供功能完备的服务，您可以针对广泛的设备类型为几乎任何用例构建所需的解决方案的全栈服务；	均需另行独立开发
行业经验沉淀	在您所从事行业的平台行业经验沉淀	在工业制造领域、智能家居、智能安防、机器人等领域以及能源管理、远程医疗、车联网和自动驾驶、农业生产、物流仓储、智慧城市等场景上基于海量客户使用经验和需求满足沉淀的不可被压缩的行业经验算法。	需自行累计和沉淀

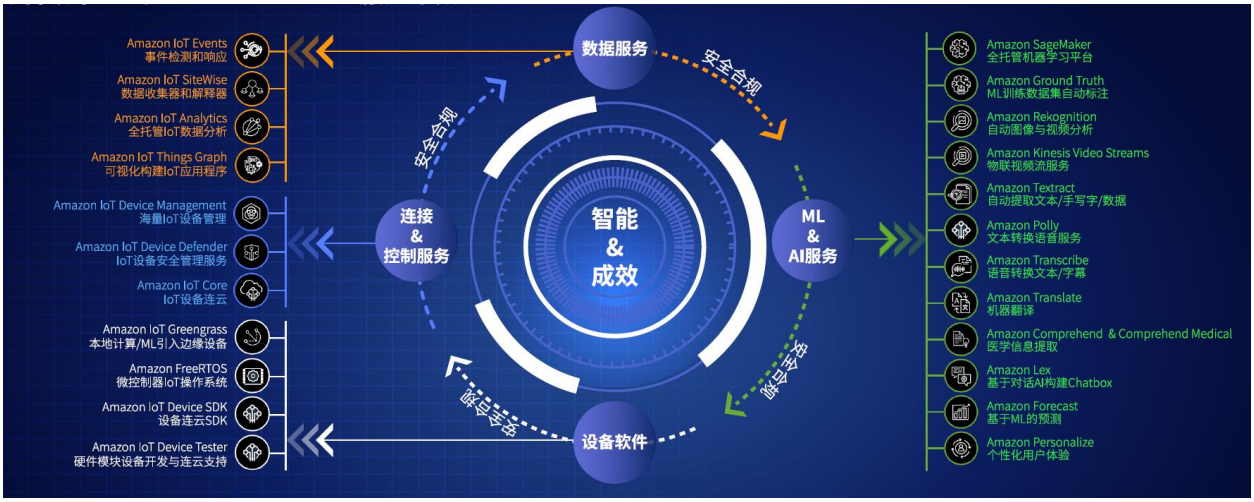
安全合规可信可控	平台及基础设施在全球各地相关认证/鉴证，法律/法规，协定/框架，隐私要求的符合和遵从；	亚马逊云科技旨在成为当今市场上最灵活、最安全的云计算环境。核心基础设施是为了满足全球的银行和其他高度敏感性组织的安全要求而构建。一组深度云安全工具对此提供支持，其中包括超过 300 项安全、合规性和监管服务及功能。亚马逊与科技支持 98 个安全标准和合规性认证，而且存储客户数据的全部 117 项 亚马逊云服务均具有加密此类数据的能力。实现多层安全服务功能，在云中和边缘满足严格的安全要求。 包括 C5/ GSMA/ K-ISMS/ CMMC /HDS、/ MTCS 第 3 级/Cyber Essentials Plus/ IRAP/ OSPAR/ DoD SRG/ ISMAP/PCI DSS 第 1 级等在内的多项认证； 包括 CLOUD Act HIPAA/IRS 1075/ITAR/SEC 规则 17a-4(f)/VPAT/Section 508 等在内的法律法规以及包括各项相关协定和框架的符合和遵从。 详情可参考：https://aws.amazon.com/cn/compliance/programs	均需自行认证和申请，工作量和难度极大
全球接入和覆盖	全球接入区域数量以及低延时保障	全球 30 个地理区域 96 个可用区以及全球 410 多个入网点，保障设备的就近接入和低延时；	需进行全球基础设备的构建和管理
平台稳定性和并发性能	平台总接入量以及总消息处理能力	在可扩展且久经考验的全球云基础设施上进行构建，通过十亿级别以上设备接入量，万亿消息体量平台处理能力；百万级客户的验证能力；	需时间的验证和打磨

平台可用性	高于 99.9%的平台稳定性	高于 99.9%的平台稳定性承诺及对应的业务赔偿机制	需专业开发和维护团队及高冗余的基础设备
平台易用性	平台操作界面的多样性和友好性	开通即用，控制台、SDK、Console 物模型，	需独立开发
平台持久性	平台的持续开发和运营稳定性	从 2006 年创立云计算业务到 2015 年推出物联网 Amazon IoT Core 服务，亚马逊云科技作为全球云计算的探路者及物联网云平台的领导者，在物联网平台领域深耕细作，长期投入，形成了深厚积累和显著领导优势	需时间的验证和打磨
全球合作伙伴	同合作伙伴共同构建的组合方案	全球 700+合规认证合作伙伴；300+亚马逊云科技同合作伙伴形成的 IoT 解决方案	需自行构建合作方案
产品上线速度	平台对于业务的支持和响应速度	分钟级开通和业务当日快速上线	通常需要半年以上的开发和测试周期

综上，除成本因素考虑外，亚马逊云科技云上物联网平台托管服务的优势总结如下：

6 亚马逊云科技物联网 IoT 平台服务概述

亚马逊云科技物联网 IoT 平台服务概述：物联网 (IoT) 服务和解决方案用来连接和管理数十亿台设备。连接、存储和分析工业、家居消费、商业和汽车业工作负载的 IoT 数据。主要分为设备软件、连接和控制服务、分析服务三大类别并在此基础之上轻松集成上层 ML&AI 相关服务。具体产品和服务逻辑关系如下图所示：



6.1 设备软件

产品	主要功能	适用场景	亮点优势
Amazon FreeRTOS 	适用于微控制器的开源实时操作系统	将低功耗的小型设备安全地连接到本地及云服务	开源、可信内核、缩短推向市场的时间、安全地连接、编程、部署和管理低功耗设备、广泛的 APN 合作伙伴支持
Amazon IoT Greengrass 	开源边缘运行时和云服务，用于构建、部署和管理设备软件	将亚马云服务扩展到边缘设备用于本地化场景的计算处理分析和存储	边缘运行、本地计算/消息处理/影子处理/数据同步/容器支持和安全以及最新的 OTA、OPC-UA 协议、LRA、机器学习推理等；
IoT Device SDK 	适用于微处理器的实时操作系统	快速简便地将设备连接到 Amazon IoT Core 平台上	可将任意操作系统（包括 RTOS/Linux/POSIX 等）接入到云平台上；

6.2 连接控制和服务

产品	主要功能	适用场景	亮点优势
Amazon IoT Core 	包含了消息服务、控制服务、数据服务和支持服务在内的托管平台，将设备同应用进行连接	所有终端设备的管理、消息路由、处理及响应	无需关注基础设施全托管服务，轻松可靠地连接、管理和扩展设备机群；双向身份验证和端到端加密保护设备连接和数据；自定义的业务规则快速筛选、转换和处理设备数据
Amazon IoT Device Management 	大规模地注册、组织、监控和远程管理 IoT 设备。与 IoT Core 集成以轻松地连接和管理云端的设备	对于批量设备的注册、管理（包含远程管理）、监控的需求场景	设备批量注册、设备集群编队和查询、设备日志和监控定位、安全隧道
Amazon IoT Device Defender 	对于设备集群的异常管理、识别安全风险、基于风险的管理管控和预防	审计 IoT 配置和连续监测 IoT 设备包括设备离线告警、设备信号门限告警等	安全配置检测、设备行为和异常检测、安全告警、风险消除等

6.3 数据应用和服务

产品	主要功能	适用场景	亮点优势
Amazon IoT Events 	检测来自 IoT 传感器和应用程序的事件并做出响应的托管服务	例如皮带卡住时设备的变化或运动检测器使用移动信号来激活灯和监控摄像机	轻松提取运营数据、轻松构建规则、触发一系列操作；
Amazon IoT SiteWise 	简化收集、组织和分析工业设备数据的操作的托管服务	生产线和多处设施的传感器数据流组织、制造流水线、组装机器人和工厂设备的性能指标等；	与工业数据湖集成的时间序列存储、资产建模、资产指标、基于 SiteWise Edge 进行本地部署、数据摄取、网关管理、并可基于 SiteWise Monitor 创建无节点完全托管的 Web 应用程序
Amazon IoT Analytics 	对大量物联网数据轻松运行和操作复杂的分析的构建分析平台托管服务	智能农业、预测性维护、主动补充物资、处理效率评分	操作分析工作流、轻松运行 IoT 数据查询、针对 IoT 进行了优化的数据存储、准备 IoT 数据以便分析、机器学习工具、自动扩展

7 总结

基于前述讨论：

1. 在企业整体管理设备体量为处于大规模以下时，使用云服务商的托管物联网平台服务无论从成本、功能、效率及安全合规等方面都具有显著优势。

2. 在企业整体管理设备体量达到大规模体量且高频消息场景时，成本差异逐步减少。但是从功能完整度、平台稳定性、安全合规满足度、全球覆盖、方案及伙伴生态等多方角度考虑，自建模式相对于云服务商托管模式将消耗企业额外的人力和时间成本、合规风险及将影响业务上线和落地时间。

8 缩略语

缩略词	全称
MQTT	Message Queuing Telemetry Transport 消息队列遥测传输协议
MRC	Monthly Recurring Charge 月度固定费用
NRC	Non-Recurring Charge 一次性固定费用
SDK	Software Development Kit 软件开发工具包
TCO	Total cost of ownership 总综合成本

9 文档历史

Date	Description
2022 年 11 月 28 日	第一版

10 说明

本白皮书阅读者有责任自行对本文档中的信息进行独立评估。 本文档：(a) 仅供参考，(b) 代表当前的亚马逊云科技产品和实践，具体请以亚马逊云科技的官网信息 (https://aws.amazon.com/cn/)为准，并且本白皮书 (c) 不构成亚马逊云科技及其关联公

司、供应商或许可人对于阅读者的任何商业或合同承诺。亚马逊云科技产品或服务按“原样”提供，不提供任何明示或暗示的保证、陈述或条件。亚马逊云科技对其客户的责任和义务由亚马逊云科技协议控制，本文档不属于亚马逊云科技与其客户之间的任何协议。