亚马逊云科技

使用Amazon IoT Core 构建安全合规的智能产品

郑辉　　亚马逊云科技解决方案架构师

亚 马 逊 云 开 发 者
Tech Talk

目录

CONTENTS

01. 智能产品存在的挑战

02. 实现智能设备常见业务需求

03. IoT Core如何解决安全合规问题

04. Demo演示

01

第一章 / 智能产品存在的挑战

智能产品存在的挑战

安全合规，大规模设备连接

构建IoT平台会遇到的问题

数据服务

如何在收到IoT 消息后处理数据?

控制服务

如何控制，管理和保护我的设备?

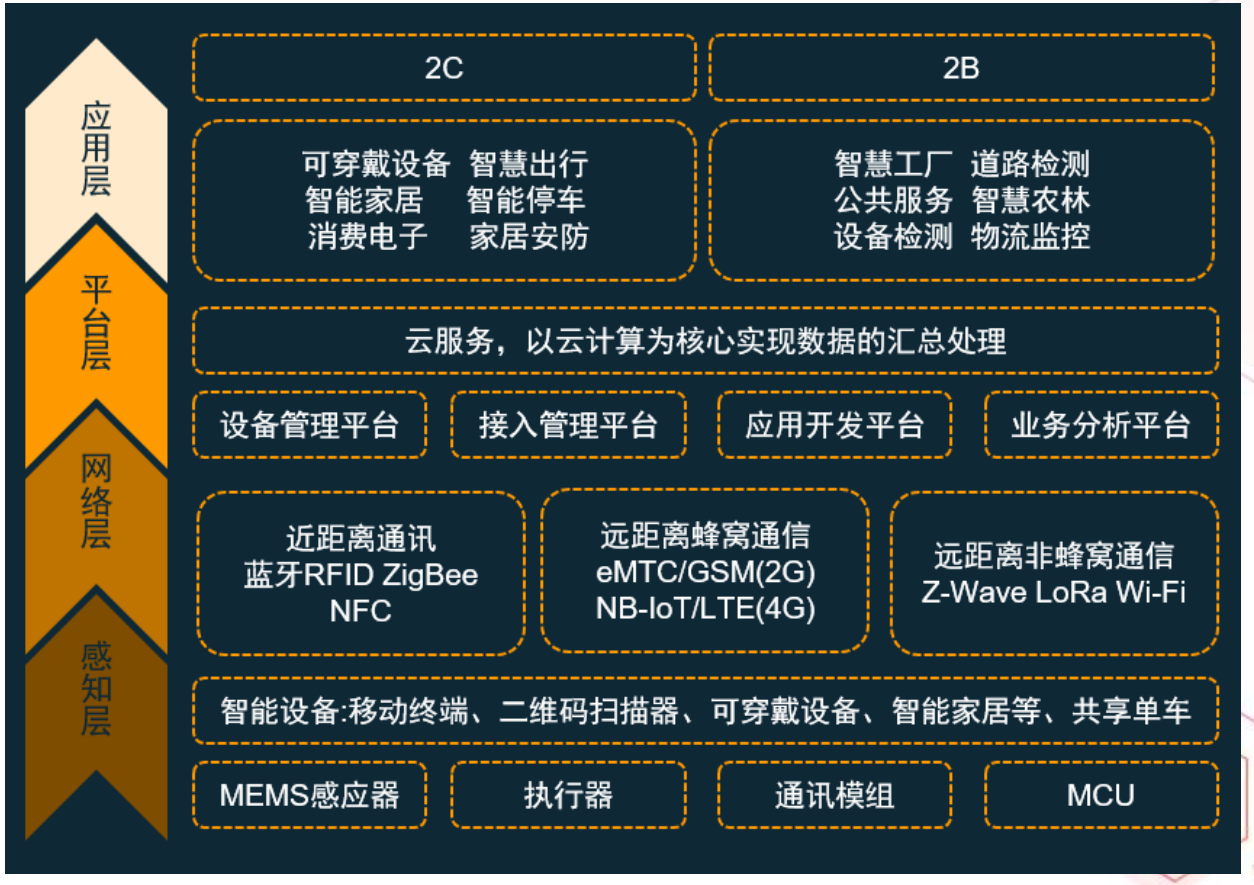
消息传递

如何构建低延迟和高吞吐量的IoT消息平台?

构建智能设备遇到的烦恼

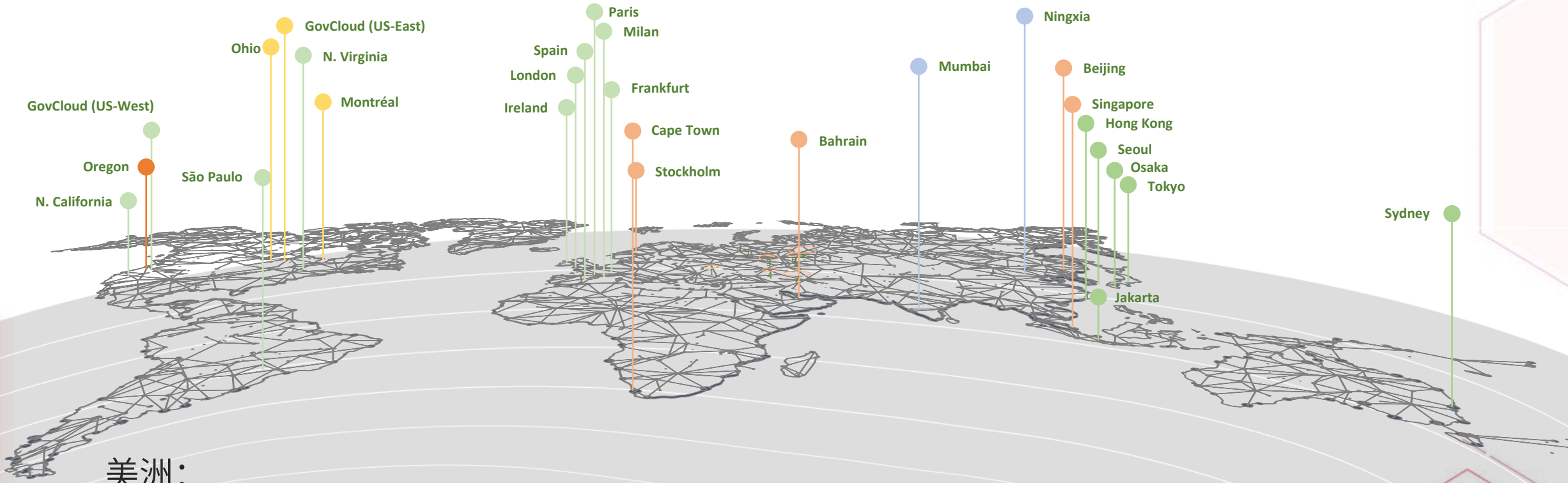
终端碎片化。由于终端设备的多样化，物联网的开发和应用存在较严重的碎片化问题。

协议多样化。在物联网应用中，通信技术包括Wi-Fi、RFID、NFC、ZigBee、Bluetooth、LoRa、NB-IoT、GSM、GPRS、3/4/5G网络、Ethernet、RS232、RS485、USB等。物联网技术框架体系中所使用到的通讯协议主要有：AMQP、JMS、REST、HTTP/HTTPS、COAP、DDS 、MQTT等。



世界各国都有相应的数据隐私法规

亚马逊云科技



美洲：

加利福利亚消费者隐私法案 (CCPA)
加拿大数据隐私法 (PIPEDA)
阿根廷数据隐私法

欧洲：

CISPE
欧盟 GDPR
西拔牙DPA授权
欧盟-美国隐私护盾

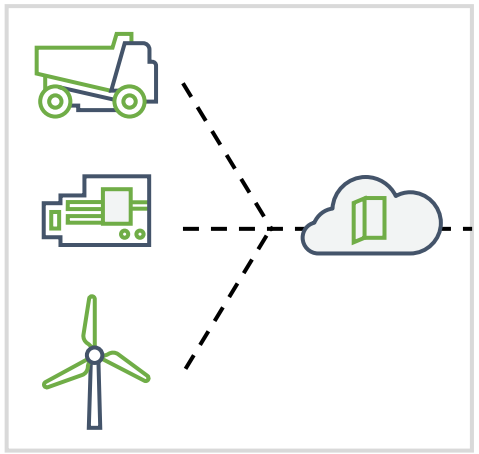
亚太：

中国 网络安全法
日本 数据隐私法
澳大利亚数据隐私法
印度数据隐私法

亚 马 逊 云 开 发 者
Tech Talk

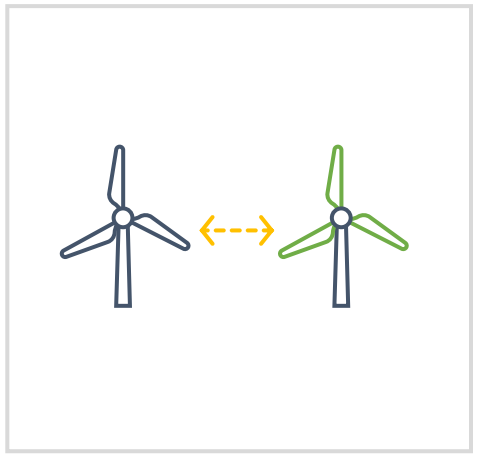
Amazon IoT Core

Amazon IoT Core 是一项托管服务，可让连接的设备轻松安全地与云端应用程序和其他设备进行交互。



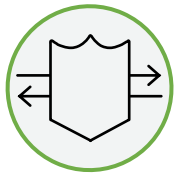
将设备安全地大规模连接到亚马逊云和其它设备

路由、处理 来自连接设备的数据



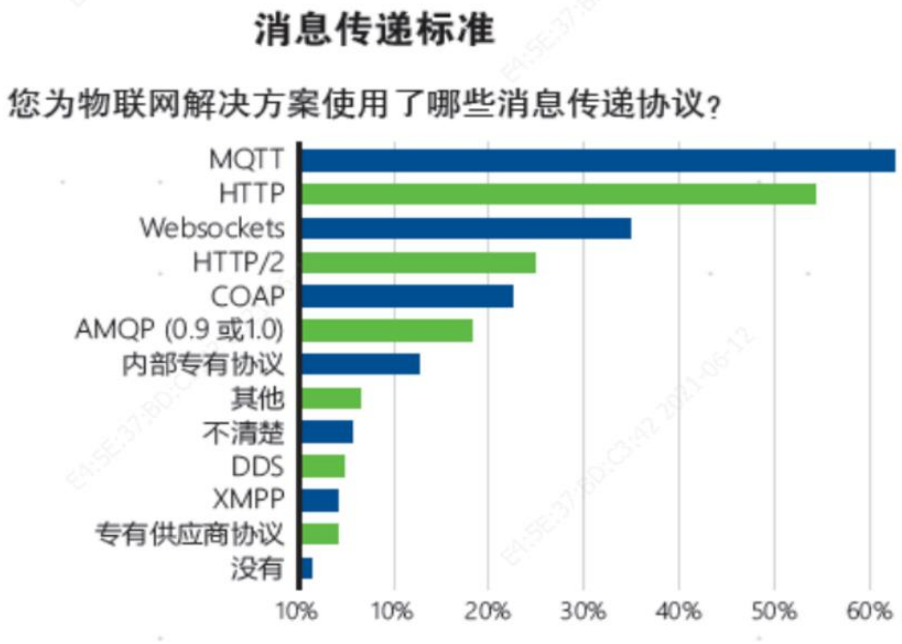
使应用程序即使在离线时也能与设备进行交互

其他亚马逊云科技服务完美集成在数据之上进行推理
(分析, 数据库, AI, 等.)



控制服务

物联网消息传递协议



Eclipse 基金会的调查，MQTT是物联网解决方案中最常用的消息传递协议

亚马逊云科技IoT Core服务支持的协议与功能

协议	支持的操作	身份验证	端口
通过 WebSocket 的 MQTT	发布、订阅	Signature Version 4	443
通过 WebSocket 的 MQTT	发布、订阅	自定义身份验证	443
MQTT	发布、订阅	X.509 客户端证书	443†
MQTT	发布、订阅	X.509 客户端证书	8883
MQTT	发布、订阅	自定义身份验证	443†
HTTPS	仅发布	Signature Version 4	443
HTTPS	仅发布	X.509 客户端证书	443†
HTTPS	仅发布	X.509 客户端证书	8443
HTTPS	仅发布	自定义身份验证	443

亚马逊云科技 IoT Core 使用 TLS 1.2 版加密所有通信。客户端还必须发送服务器名称指示 (SNI) TLS 扩展。不包括 SNI 的连接尝试将被拒绝。

连接协议选择-MQTT

MQTT协议

- ISO 标准(ISO/IEC PRF 20922)下基于发布/订阅范式的消息协议。

适合场景

- 硬件性能低下的远程设备
- 网络状况糟糕的情况
- 低成本
- 电池与能耗
- 工作环境不稳定
- 传递数据量小

服务质量级别（QoS）

- QoS 0：最多一次传送。
- QoS 1：至少一次传送。
- QoS 2：正好一次传送。

亚马逊云科技上的MQTT

协议规范

- 基于 MQTT v3.1.1 规范，但有一些差异
- 使用TLS 1.2加密所有连接

与MQTT v3.11主要差异

- 支持MQTT 服务质量 (QoS) 级别 0 和 1。但是不支持第三级 QoS（即级别 2）。
- 在亚马逊云科技 IoT 中，订阅具有 QoS 级别 0 的主题意味着将消息传送零次或多次。消息可能会多次发送。多次发送的消息在发送时可能会使用不同的数据包 ID。在这些情况下，不会设置 DUP 标志。
- 其他项目参考官方文档（协议细节不同点）：https://docs.aws.amazon.com/zh_cn/iot/latest/developerguide/mqtt.html#mqtt-differences

使用IoT Core构建终端的硬件要求

- 某ODM使用ESP32-C3+2M RAM构建智能灯泡

02

第二章 / 安全与合规

智能产品的安全合规

亚马逊云科技如何解决安全合规问题

Amazon IoT Core

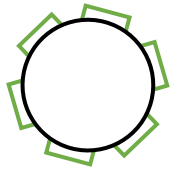
亚马逊云科技

认证服务

管理设备授权并且提供大规模的身份认证

设备网关

完全托管的，针对物联网场景的连接优化

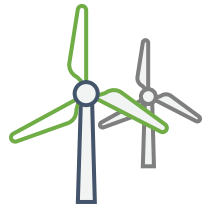


消息代理

为物联网设备列队提供可靠、快速的通信

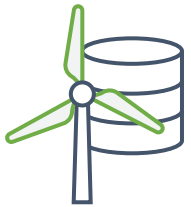
规则引擎

以低成本获取大量物联网数据，对其进行预处理，并将其提供给10多种服务，用于分析、报告和可视化



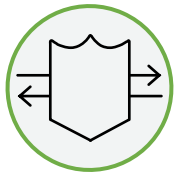
设备影子

随时了解和控制设备的状态



注册表

定义和登记设备以便其它服务使用



控制服务

亚 马 逊 云 开 发 者

Tech Talk

认证服务

亚马逊云科技

管理设备授权并且提供大规模唯一性认证服务

使用您自己的Root CA和客户端证书，或者让Amazon IoT Core 为您生成证书

通过即时注册实现自动化设备配置

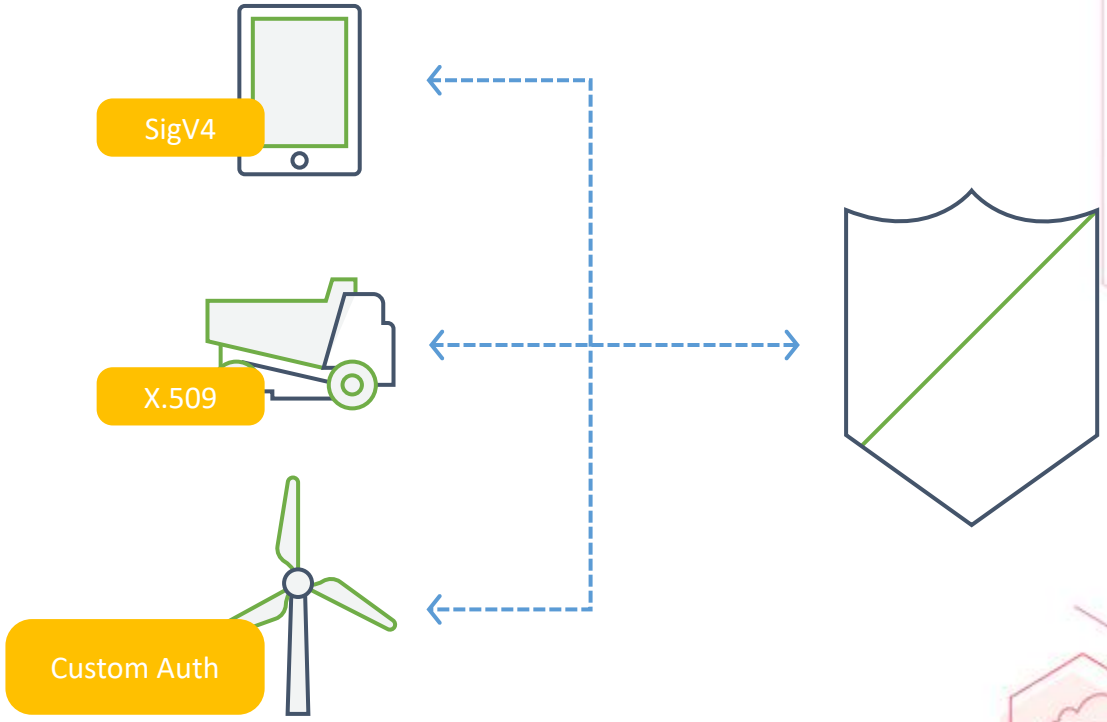
通过Fleet Provisioning实现自动化设备配置

支持SigV4，X.509，Cognito和自定义身份验证

通过IoT策略实现灵活、细粒度的访问控制

策略可以与身份认证或者注册表项目关联

访问控制可以控制到MQTT 主题级别

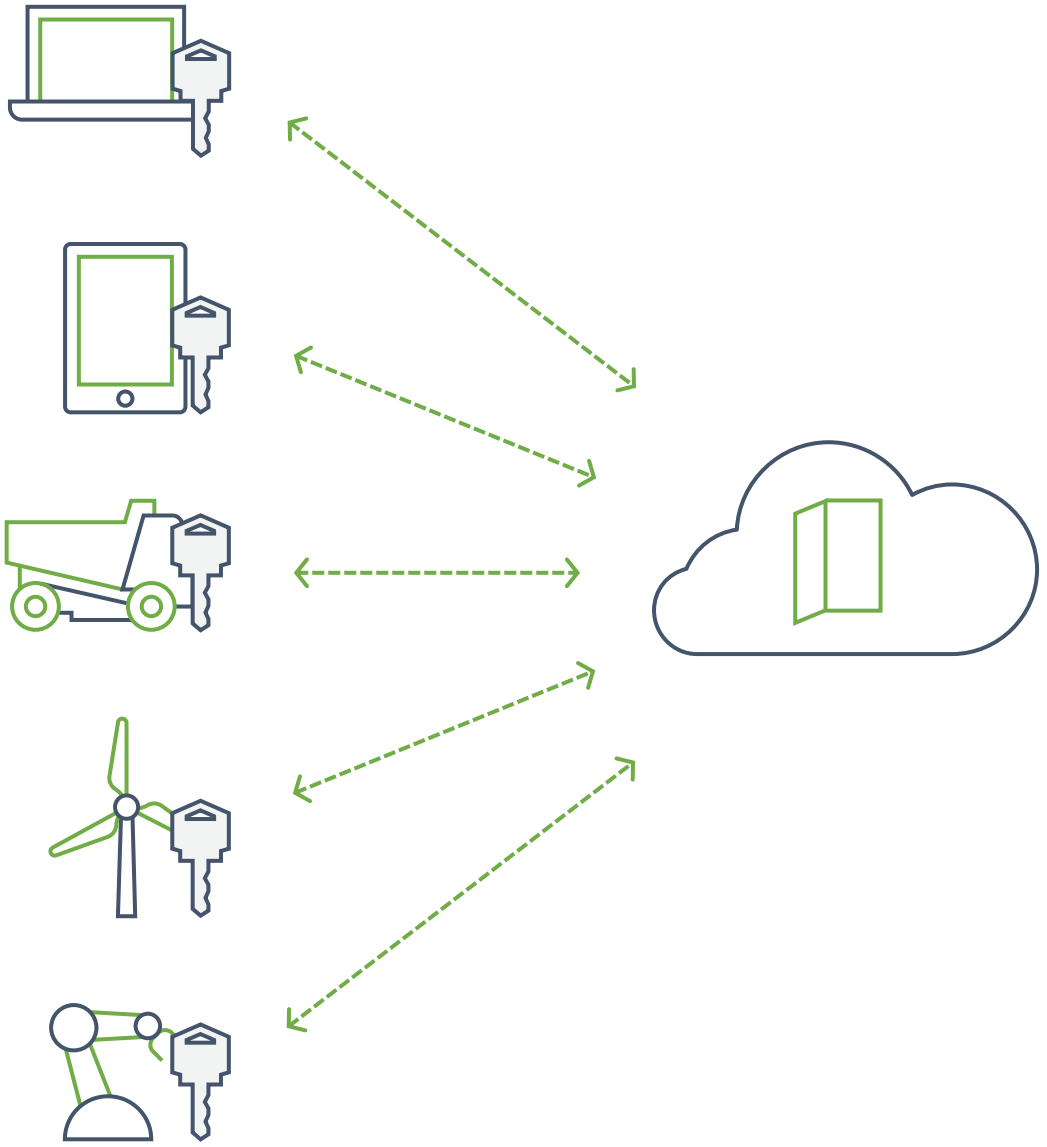


设备网关

亚马逊云科技

- 完全托管的连接优化，针对物联网场景
- 支持多种协议
  包括 MQTT, WebSocket, HTTP
- 通过TLS 1.2 进行安全通信
- 可配置的终端节点和自定义域名
- 优化性能受限的设备

ECC密钥交换和证书



设备的安全控制解决方案

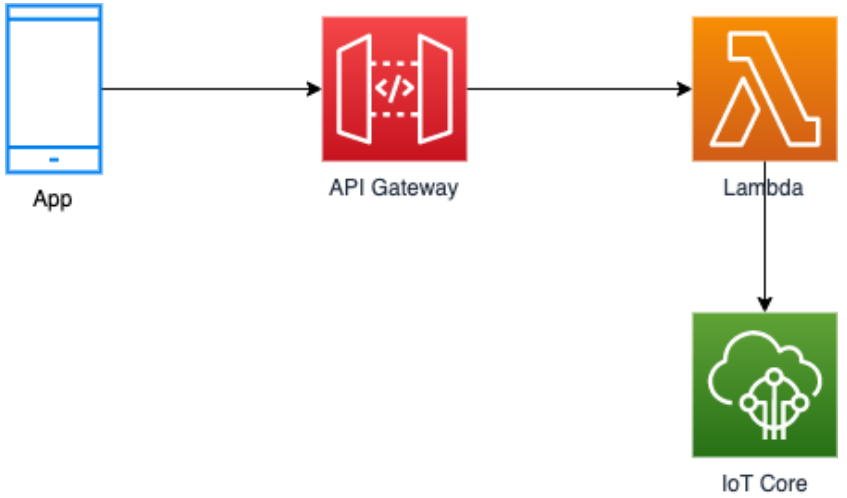
亚马逊云科技

解决方案一

IoT Core中证书与设备绑定， 证书附加策略，策略规定连接上云的范围，一个证书对应一个设备；

在策略中，通过精细定义策略内容，达到最小化设备连接权限，实现安全需求；

解决方案二



手机端App不直接连接IoT Core，通过网关做一层中转，方便在网关处进行权限控制；

通过策略进行精细化的权限控制

亚马逊云科技

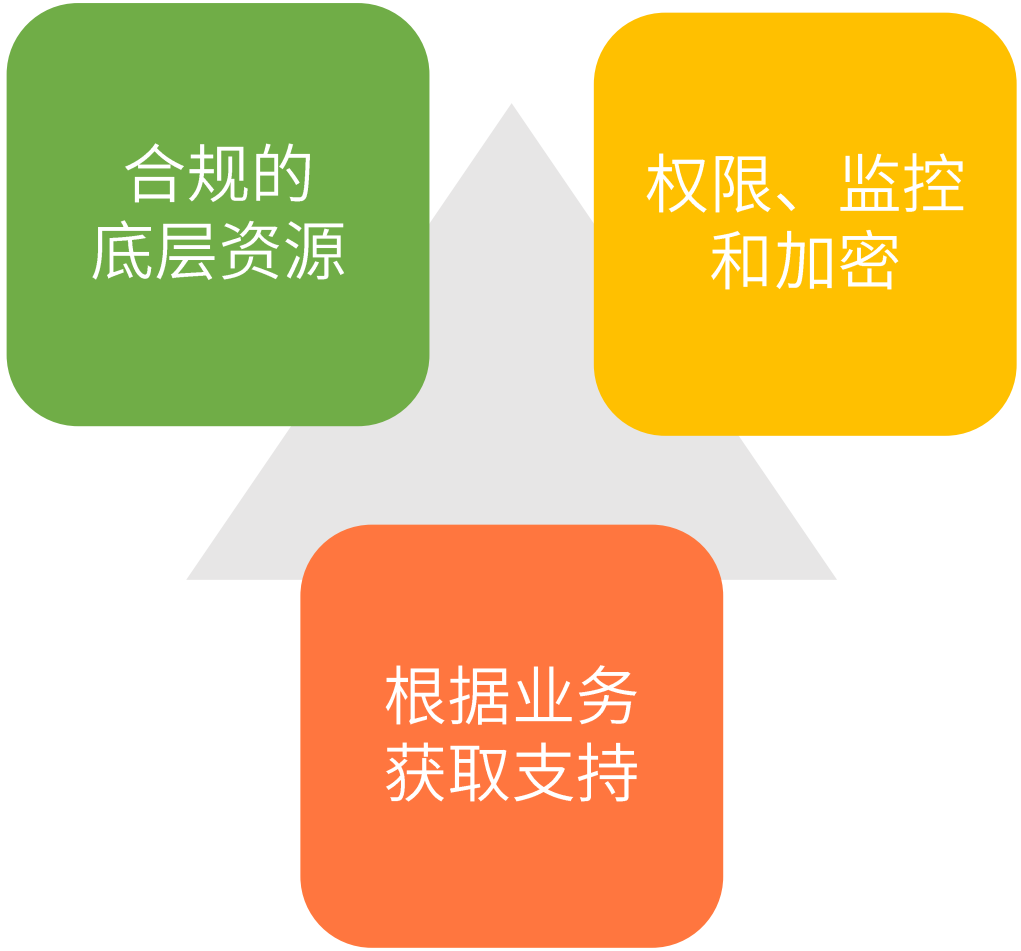
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
                "iot:Connect",
                "iot:Publish",
                "iot:Receive",
                "iot:Subscribe"
                ……
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
                "arn:aws:iot:us-west-2:*:client/${iot:ClientId}",
                "arn:aws:iot:us-west-2:*:topic//pid1/device1/*",
                "arn:aws:iot:us-west-2:*:topicfilter//pid1/device1/*",
                "arn:aws:iot:us-west-2:*:topic//pid2/device2/*",
                "arn:aws:iot:us-west-2:*:topicfilter//pid2/device2/*",
                ……
            ]
        }
    ]
}
```

亚马逊云科技

亚马逊云科技赋能客户合规建设

亚 马 逊 云 开 发 者
Tech Talk

从三个方向去实现整体合规性



以GDPR举例，个人数据要求

内容：

客户（或任何最终用户）存储或处理的任何内容，包括：

软件、数据、文本、音频、视频等

个人数据（适用于 GDPR）：

可以识别或定位自然人的信息（根据欧盟数据保护法），如：

- 基本的身份信息，如姓名、地址和身份证号码等
- 网络数据，如位置、IP地址、Cookie数据和RFID标签
- 医疗保健和遗传数据
- 生物识别数据，如指纹、虹膜等
- 种族或民族数据
- 政治观点
- 性取向

客户的 “内容” 可能包括 “个人数据”

GDPR 针对个人数据处理的六大原则

Lawfulness, fairness and transparency
透明性，公平，合法性

合法的收集数据，并公开收集何种类型的数据

Purpose limitation
限制使用目的

不得违反原有目的对数据进行额外处理

Data minimization
数据最小化

只采集恰当的，相关的和有需要的数据

Accuracy
数据内容的准确性

确保准确性，需要时只使用最新的数据

Storage Limitation
储存限制

储存数据的时间不长于所需要的目的对应的时间

Accountability
管理责任制

数据应有相应的机制来防范非法的，没有授权的处理，防止数据外泄，被破坏等损失

第一要素-基于对全球标准的合规遵从构建您的合规体系

亚马逊云科技

认证 & 鉴证

Cloud Computing Compliance Controls Catalogue (C5)	DE ✓
Cyber Essentials Plus	GB ✓
DoD SRG	US ✓
FedRAMP	US ✓
FIPS 140-2	US ✓
IRAP	AU ✓
ISO 9001	✓
ISO 27001	✓
ISO 27017	✓
ISO 27018	✓
MLPS Level 3	CN ✓
MTCS	SG ✓
PCI DSS Level 1	✓
SEC Rule 17-a-4(f)	US ✓
SOC 1, SOC 2, SOC 3	✓

法律, 法规和隐私

CISPE	EU ✓
EU Model Clauses	EU ✓
FERPA	US ✓
GLBA	US ✓
HIPAA	US ✓
HITECH	✓
IRS 1075	US ✓
ITAR	US ✓
My Number Act	JP ✓
Data Protection Act – 1988	GB ✓
VPAT / Section 508	US ✓
Data Protection Directive/GDPR	EU ✓
Privacy Act [Australia]	AU ✓
Privacy Act [New Zealand]	NZ ✓
PDPA - 2010 [Malaysia]	MY ✓
PDPA - 2012 [Singapore]	SG ✓
PIPEDA [Canada]	CA ✓
Agencia Española de Protección de Datos	ES ✓

协议 & 框架

CIS (Center for Internet Security)	✓
CJIS (US FBI)	US ✓
CSA (Cloud Security Alliance)	✓
Esquema Nacional de Seguridad	ES ✓
EU-US Privacy Shield	EU ✓
FISC	JP ✓
FISMA	US ✓
G-Cloud	GB ✓
GxP (US FDA CFR 21 Part 11)	US ✓
ICREA	✓
IT Grundschutz	DE ✓
MITA 3.0 (US Medicaid)	US ✓
MPAA	US ✓
NIST	US ✓
Uptime Institute Tiers	✓
Cloud Security Principles	GB ✓

https://aws.amazon.com/cn/compliance/programs/

第二步亚马逊云科技帮助客户落地GDPR合规

亚马逊云科技

除了确保的合规性，亚马逊云科技还致力于为客户提供服务和资源，帮助他们遵守可能适用于GDPR 要求。

存取控制

IAM 身份认证&访问控制

对 Amazon S3、Amazon SQS 和 Amazon SNS 中的对象实现精细访问控制

API 请求验证

通过 Amazon Security Token Service 获取的临时访问令牌

监控纪录

通过 Amazon Config 执行资产管理和配置

通过 Amazon CloudTrail 进行审核和安全分析

通过 Amazon VPC 流日志获取网络中流量的详细信息

通过 Amazon Config 规则执行基于规则的配置检查和操作

通过 Amazon CloudFront 中的 Amazon WAF 功能筛选和监视对应用程序的 HTTP 访问

加密

使用 AES256 (EBS/S3/Glacier/RDS) 对闲置的数据加密

集中化托管密钥管理 KMS

IPsec 通过 VPN 网关进入 Amazon

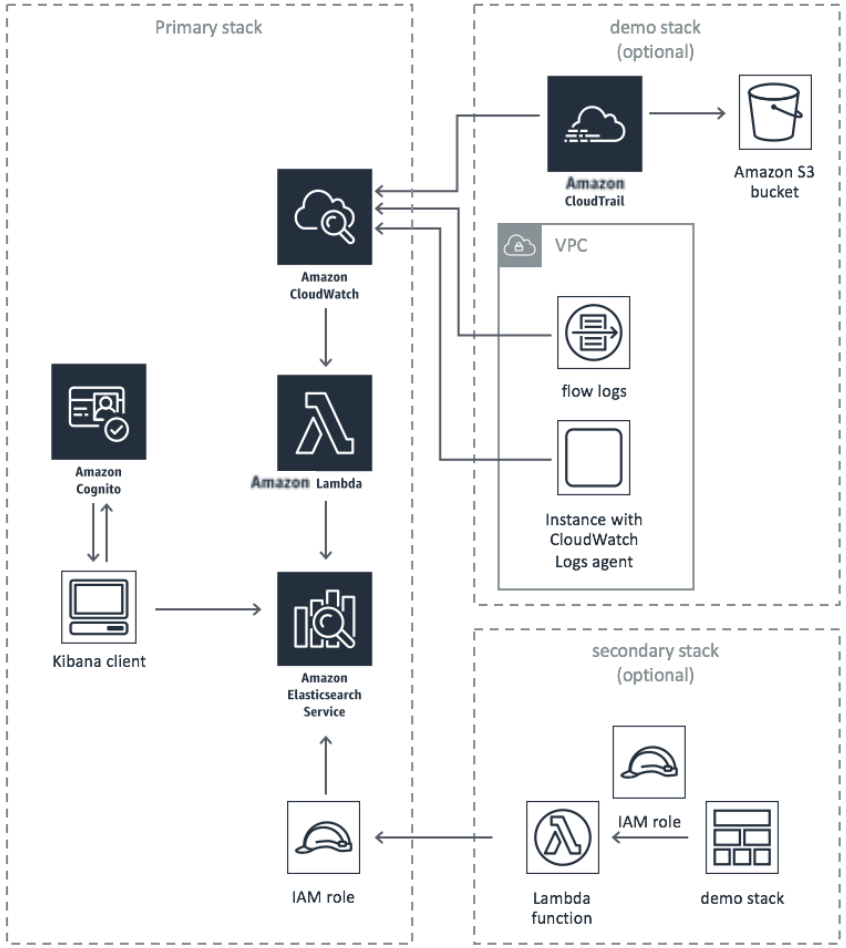
通过 Amazon CloudHSM 在云中使用专用 HSM 模块

安全认证

符合各种严格的国际标准，包括：技术方法的ISO 27001、云端安全的ISO 27017、云端隐私的ISO 27018、SOC 1、SOC 2 和SOC 3、 PCI DSS 第1级，以及欧洲特有的认证，例如BSI的Common Cloud Computing Controls Catalogue (C5) 和ENS 高级认证。

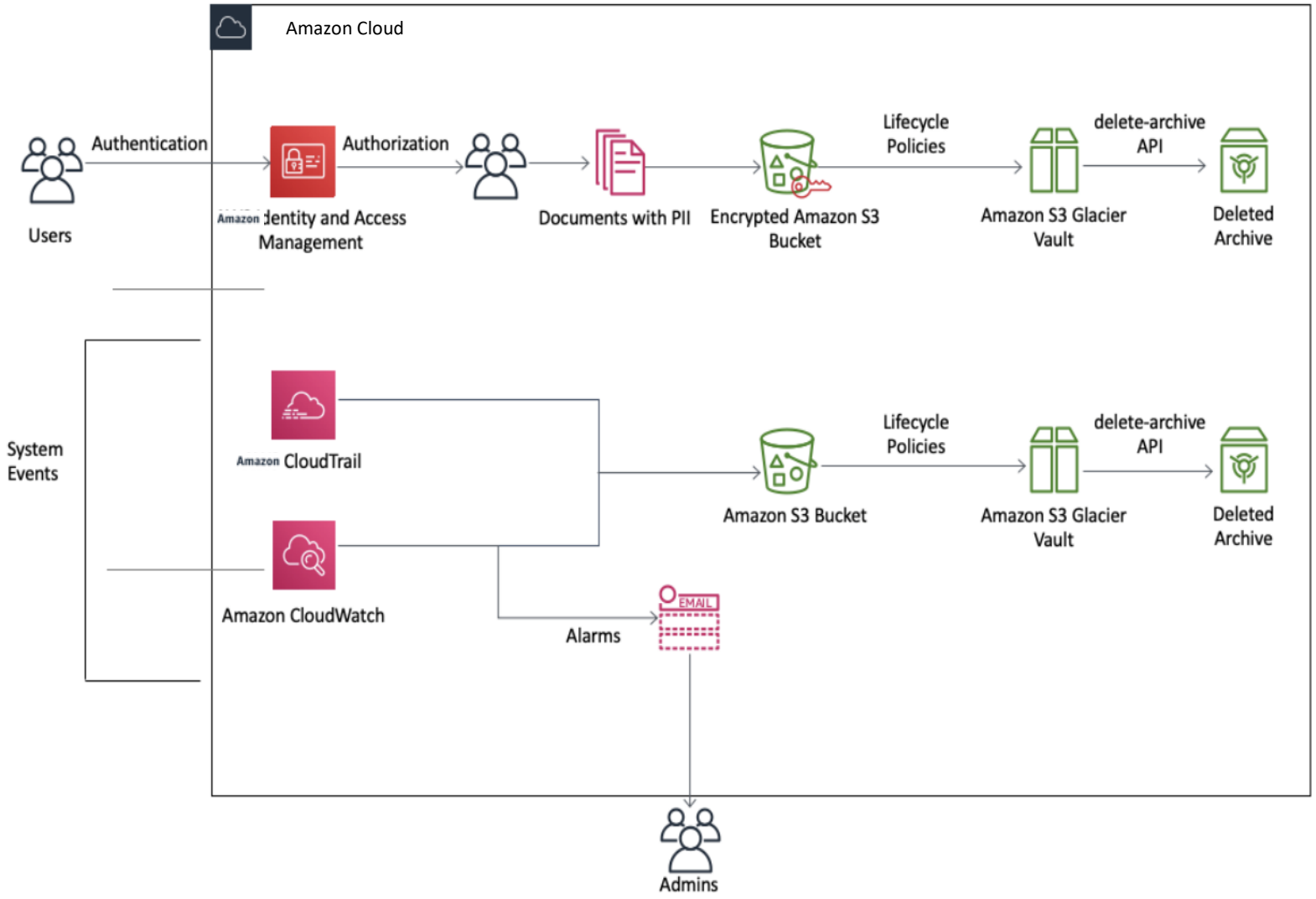
Amazon 也宣布符合 CISPE 行为准则。

集中化的日志管理



- 集中式日志记录解决方案使组织能够跨多个账户和Amazon区域收集，分析和显示Amazon上的日志。
- 该解决方案使用可简化Amazon云中Elasticsearch集群的部署，操作和扩展的托管服务Amazon Elasticsearch Service（Amazon ES）以及与Amazon ES集成的分析和可视化平台Kibana。结合其他Amazon托管服务，此解决方案为客户提供了可自定义的多账户环境，以开始记录和分析其Amazon环境和应用程序。

云上的隐私数据存取与归档



- 开发人员将仅出于履行订单（订单发货后不超过 30 天）或计算/缴纳税款的目的和必要时间保留 PII（个人资料）。

- 法律要求开发人员出于税收或类似监管目的保留 PII 的存档副本，此存档的亚马逊信息必须作为“冷”或离线（例如，不能立即或交互式使用）备份存储在物理安全的设施中，并且备份媒体上的所有存档数据都必须加密。

第三步-安全保障服务团队/持续与全球监管机构展开合作

亚马逊云科技

亚马逊云科技与美国和世界各地的
监管机构持续合作有两个目的：

分享我们的合规方法和合规工具

赋能监管机构以帮助审核人员考核 亚马逊云科技云环境

帮助塑造法规格局，以反映技术的变化

促进业界与监管机构之间的对话

评估和解读政策

监管政策评估，以评估法规的潜在影响

按不同国家进行影响评估，以帮助企业应对如何运作

针对具体区域和具体国家的合规指南，以记录关键的政策变化和如何应对

亚马逊云科技

专业服务团队

寻找亚马逊云专业服务团队，获取安全保障服务

客户收益: 持续为我们的客户提供了解合规要求的所需环境和反馈渠道，从而更有信心的进行业务创新

与合规遵从生命周期保持一致的服务

亚马逊云科技


Amazon Security Hub

Amazon Organizations


Amazon Transit Gateway


Amazon VPC


Amazon IoT Device Defender


Amazon Cloud Directory


Amazon GuardDuty


Amazon Macie


Amazon CloudWatch


Amazon Step Functions


Amazon Systems Manager


Amazon Lambda


Amazon Control Tower


Amazon Trusted Advisor


Amazon VPC PrivateLink


Amazon Direct Connect


Resource Access manager

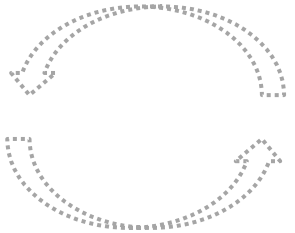

Amazon Directory Service


Amazon Config Rules


Amazon Security Hub

Automate

Identify → Protect → Detect → Respond → Recover




Amazon Service Catalog


Amazon Config


Amazon Shield


IAM


Amazon Secrets Manager


KMS


Amazon Cognito

Investigate


Amazon S3 Glacier


Amazon Well-Architected Tool


Amazon Systems Manager


Amazon WAF


Amazon Firewall Manager


Amazon Certificate Manager


Amazon CloudHSM


Amazon Single Sign-On


Amazon CloudWatch


Amazon CloudTrail

Amazon Detective

Amazon Route 53


Snapshot

Archive

通过 APN 与 Marketplace 为企业用户提供合规保障

亚马逊云科技

咨询类合作伙伴

亚马逊云科技认证咨询合作伙伴可以帮助客户实现GDPR合规

Deloitte. sopra steria direktgruppe

THALES

技术类合作伙伴

亚马逊云科技认证技术合作伙伴为GDPR合规提供安全/认证方案

BigID evident.io FORTINET

THALES

awsmarketplace

Advanced Threat Analytics	Application Security	Identity and Access Mgmt	Server & Endpoint Protection	Network Security	Encryption & Key Mgmt	Vulnerability & Pen Testing
ALERTLOGIC	IMPERVA	CIPHERGRAPH networks	TREND MICRO	SOPHOS	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	FORTINET	Vormetric	QUALYSGUARD
	Barracuda	M-Pin SSO Authentication for Enterprises		Check Point We Secure the Internet.	HYTRUST	
				paloalto networks.		

03

第二章 / 常见业务场景

智能产品的构建

实现智能设备常见业务需求

注册表

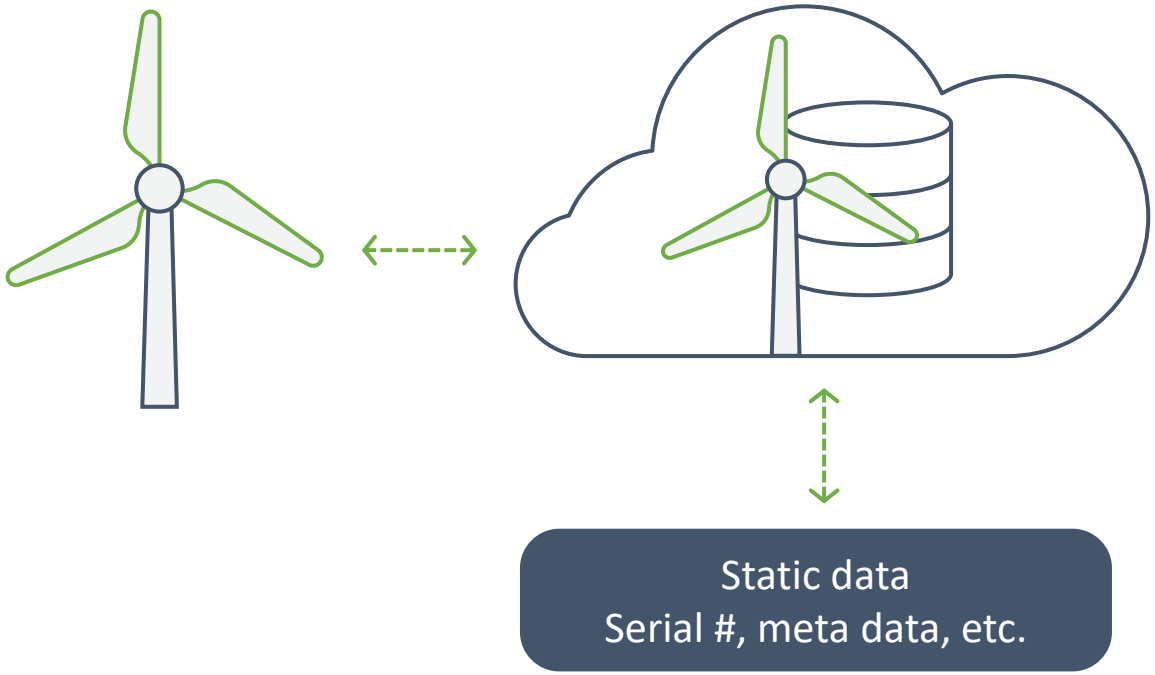
亚马逊云科技

定义和登记设备以便亚马逊云科技其它服务使用

简化搜索 (例如，哪些设备是2010年生产的?)

定义 事物类型 (例如 本田和丰田属于汽车类型) 以实现跨设备的属性和策略的标准化

定义 群组 (例如：汽车传感器) 以实现更简单的管理（运行作业，设置策略等）



规则引擎

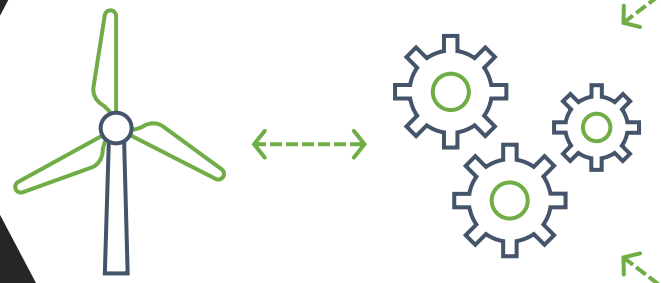
低成本获取大量物联网数据，对其进行预处理，并将其提供给10多种服务，用于分析、报告和可视化

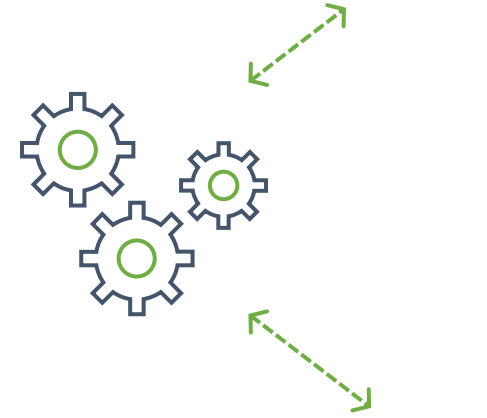
转换 – 内置函数，用于数学公式，字符串操作，日期等

过滤 – 使用WHERE子句仅捕获所需的数据

丰富 – 通过设备阴影和Amazon Machine Learning 或者 通过Amazon Lambda执行从外部源 获取上下文

路由 – 将您的数据发送到10多个Amazon Web Services服务和第三方服务，如Salesforce HERE等；支持HTTP Action





设备影子

亚马逊云科技

随时了解和控制设备的状态

报告设备的最后已知状态; 例如，灯泡的最后已知颜色是红色

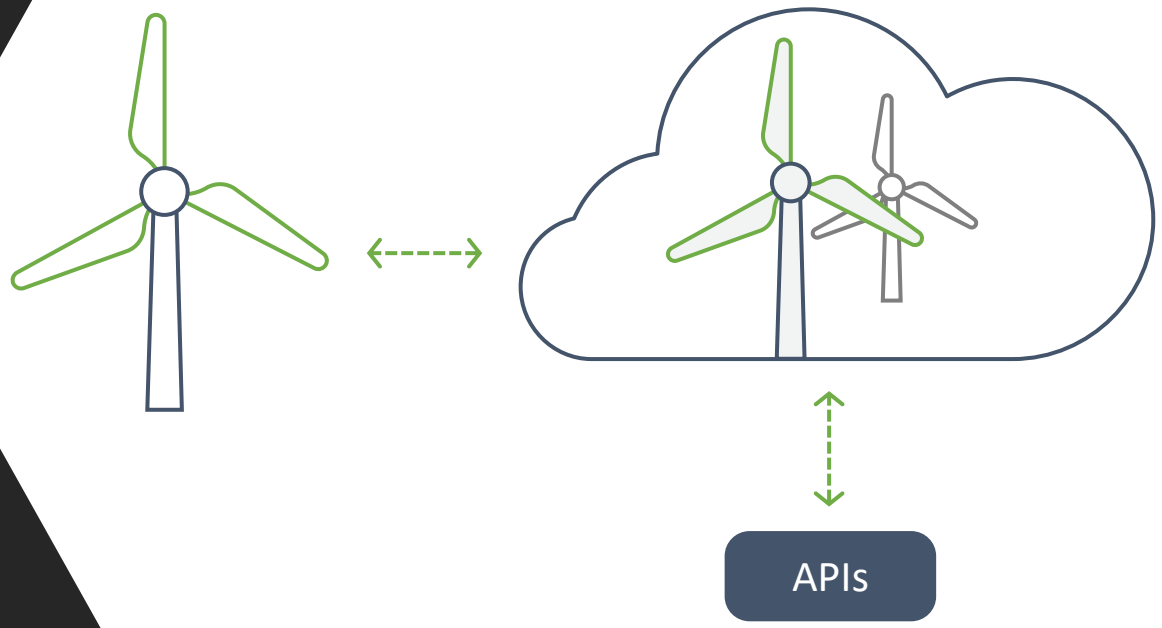
改变设备的状态; 例如，将灯泡的颜色改为蓝色

使用MQTT实现实时状态更改通知

与离线设备的异步通信

可在设备上轻松实现Device SDK集成

使用REST API实现应用程序与设备交互



设备影子的MQTT消息主题

亚马逊云科技

设备影子消息主题游prefix和function组成, prefix规则如下：

ShadowTopicPrefix 值	影子类型
$Amazon/things/thingName/shadow	未命名的（经典）影子
$Amazon/things/thingName/shadow/name/shadowName	命名的影子

设备影子消息字段如下：

```
{
  "state": {
    "desired": {
      "attribute1": "value"
    },
    "reported": {
      "attribute1": "value"
    }
  },
  "metadata": {
    "desired": {
      "attribute1": {
        "timestamp": 12322312312
      }
    }
  },
  "timestamp": 12322312312,
  "clientToken": "token",
  "version": 111
}
```

设备影子的MQTT消息主题-Function

亚马逊云科技

主题	允许的客户端操作	说明
ShadowTopicPrefix/delete	发布/订阅	设备或应用程序向此主题发布消息以删除影子。
ShadowTopicPrefix/delete/accepted	Subscribe	当一个影子被删除时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/delete/rejected	Subscribe	当删除影子的请求遭拒时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/get	发布/订阅	应用程序或事物向此主题发布空消息来获取影子。
ShadowTopicPrefix/get/accepted	Subscribe	当获取影子的请求获批时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/get/rejected	Subscribe	当获取影子的请求遭拒时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/update	发布/订阅	事物或应用程序向此主题发布消息以更新影子。
ShadowTopicPrefix/update/accepted	Subscribe	当影子更新成功时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/update/rejected	Subscribe	当影子更新遭拒时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/update/delta	Subscribe	当检测到影子的 “reported”部分与 “desired”部分之间存在差异时，Device Shadow 服务将向此主题发送消息。
ShadowTopicPrefix/update/documents	Subscribe	每次影子更新成功执行时，Amazon IoT 都会向该主题发布状态文档。

使用Shadow进行设备的状态控制

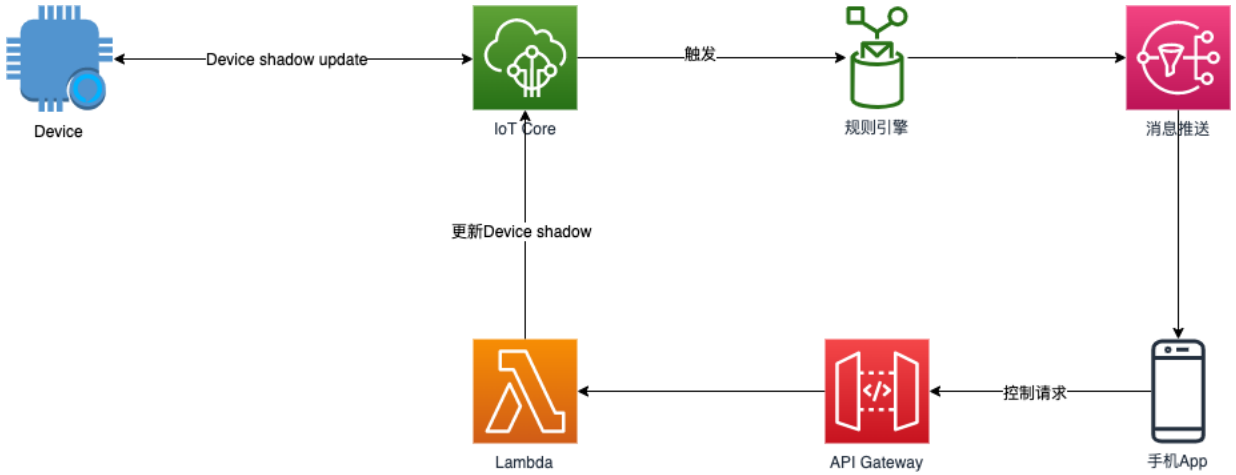
亚马逊云科技

解决方案：

使用device shadow作为设备状态控制，state字段中写入自定义设备属性；

设备状态更新，更新reported字段属性，
控制端（手机）更改设备，更新desired字段属性；

设备重新上线时，使用get方法获取最新设备属性；
使用version确定消息的最新版本，实现最终一致性；



优势：

无需复杂开发即可实现设备管理，Retain标识逻辑设置等；
已定义好的消息版本，不用维护消息实时性；
每个设备都可以设置自己的影子，方便进行权限控制；

传统的MQTT-LWT

亚马逊云科技

因为智能设备的网络环境，工作环境不稳定，电量消耗，意外情况等原因，导致设备意外离线；

MQTT协议中，为了应对这类情况，有**LWT(Last Will and Testament)**机制；

遗愿相关的设置是在建立连接的时候,在CONNECT数据包里面指定的。包括以下这些设置：
Will Flag：是否使用LWT
Will QoS：发布遗愿消息时使用的QoS
Will Retain：遗愿消息的Retain标识
Will Topic：遗愿主题名，不可使用通配符
Will Message：遗愿消息内容

```
def on_connect(client, userdata, flags, rc):
    if rc == 0:
        client.publish(“will_test”, payload=“client is online”,
qos=1, retain=True)
    else:
        print(“connection failed ”, rc)


mqtt_client = mqtt.Client(client_id=“demo_mqtt_pub”)
mqtt_client.on_connect = on_connect
mqtt_client.will_set("will_test ", payload=“client is offline”,
qos=1, retain=True)
mqtt_client.connect("iot-core-endpoint", 8883)
mqtt_client.loop_forever()
```

IoT Core上的设备生命周期管理

亚马逊云科技

设置LWT消息，需要我们在嵌入式做额外的开发，设定设备的online/offline机制；
而在亚马逊云科技的IoT core上，会提供**连接/断开连接事件**
IoT Core在客户端建立连接或断开连接时将消息发布到以下 MQTT 主题：

- $Amazon/events/presence/connected/clientId — 连接到消息代理的客户端。
- $Amazon/events/presence/disconnected/clientId — 与消息代理断开连接的客户端。

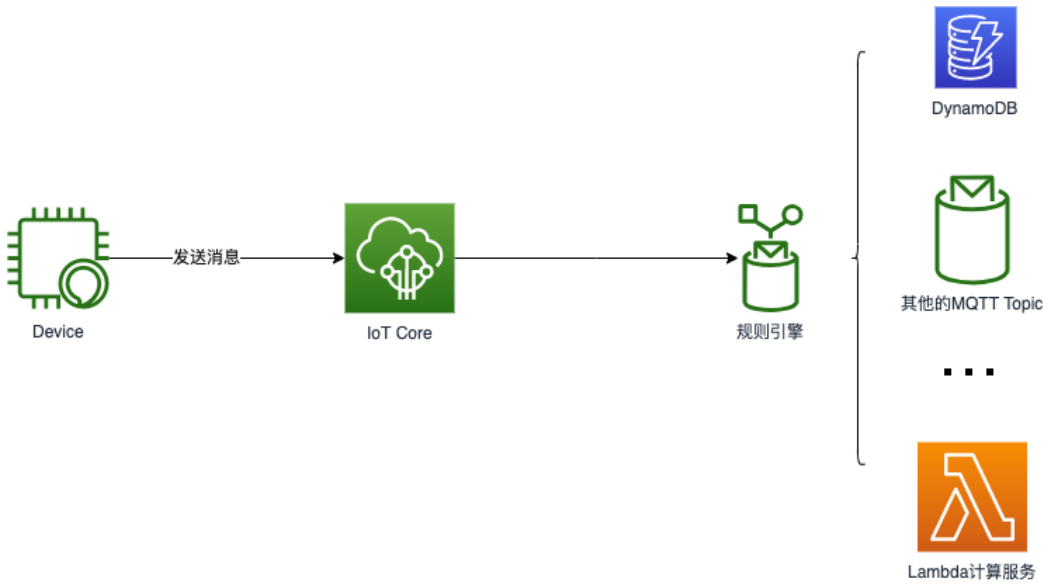
管理方式一

- 设备在云上注册时，以自身SN码进行注册，连接MQTT时，使用SN码作为clientId
- 规则引擎设定对$Amazon/events/presence/connected(disconnected)/#的过滤
- 在DynamoDB中维护一张以设备SN码为主键的表，使用规则引擎监听**连接/断开连接事件**更新到DynamoDB

管理方式二

- 设备在云上注册时，以自身SN码进行注册，连接MQTT时，使用SN码作为clientId
- 规则引擎设定对$Amazon/events/presence/connected(disconnected)/#的过滤
- 使用规则引擎监听**连接/断开连接事件**重新发布给影子设备，更新影子设备state字段

两种方案，都需要借助规则引擎

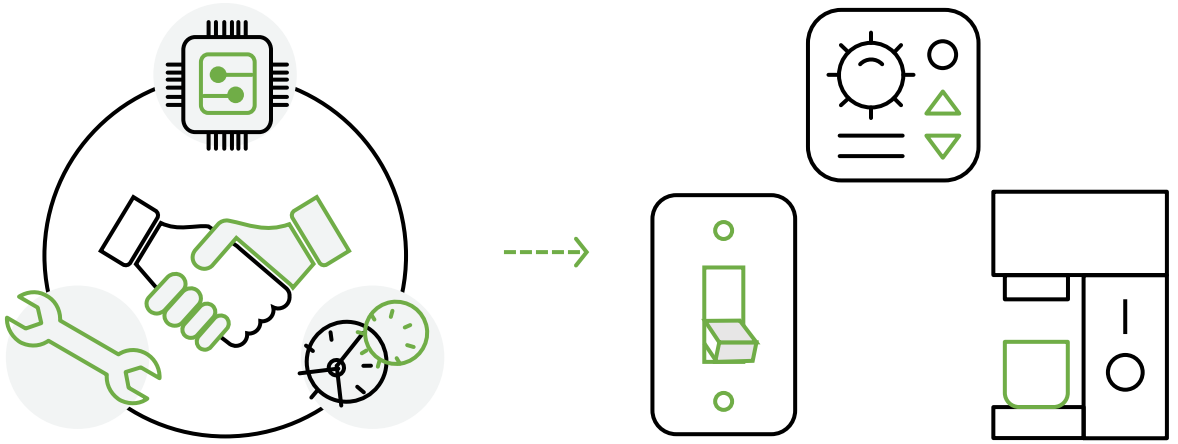


Alexa Voice Service 集成

亚马逊云科技

经济高效地将Alexa Voice带到任何类型的连接设备上

通过减少物理设备所需的计算和内存占用空间，将生产Alexa内置设备的成本降低多达50%



使设备制造商能够使用资源受限的设备（ARM的‘M’型微控制器和小于1MB的嵌入式RAM）来构建新型的Alex内置产品

适用于电灯开关，恒温器，小型家电等设备

与AVS集成配合使用的合作伙伴开发套件可降低复杂性并帮助设备制造商缩短产品上市时间

亚马逊云科技

谢谢

THANK YOU!

领取IoT资料礼包&
免费开通IoT账户

预约10月13日盛大开启的
亚马逊云科技中国峰会

请助手加入亚马逊云科技
IoT群咨询与了解

亚 马 逊 云 开 发 者
Tech Talk