

# 使用AWS为企业用户开发移动App和无服务器的微服务

蒙维，AWS解决方案架构师

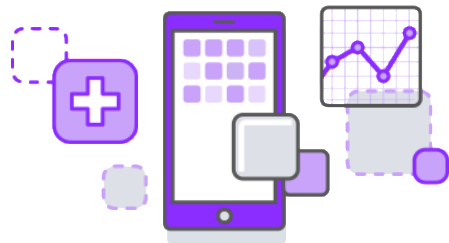
# 通过本次讲座，您将了解

在AWS上构建企业移动App和无服务器的微服务后台的架构设计、最佳实践和应用模式。

# 企业用户正将AWS服务用于大量的场景...



Web 应用



移动应用



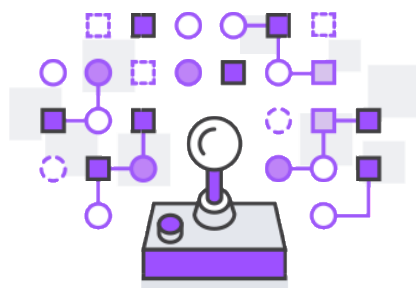
物联网



媒体和娱乐



商务应用



游戏开发



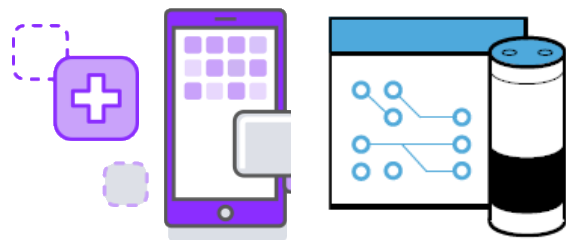
医疗保健



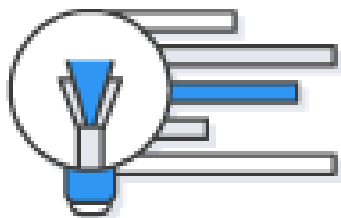
数据分析

灾难恢复, 备份, 虚拟桌面以及更多...

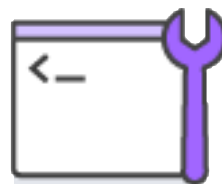
# 为了构建不同移动应用，企业用户最关心的是...



全新的  
功能与用户体验



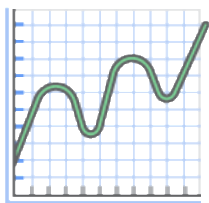
敏捷、  
快速投放市场



便于开发、  
测试、部署和管理



与现有的应用  
和数据源集成



可扩展和高可用



安全性



身份管理，  
联合身份认证



用户吸引，  
行为分析和洞察

# 架构设计

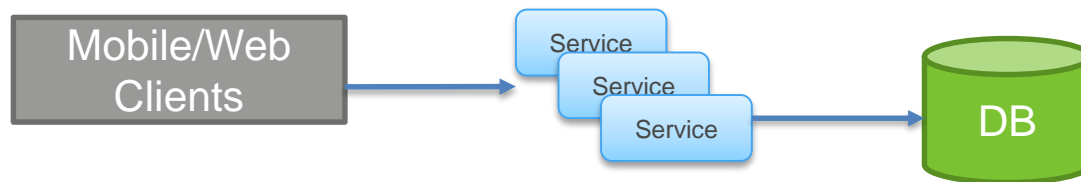
## 客户端-服务器架构



## 包括web层、应用层和数据库层的多层架构



## 面向服务的架构 (SOA)



## 面向消息的架构（消息中间件）



可以看到软件系统架构其实一直在不断演进...

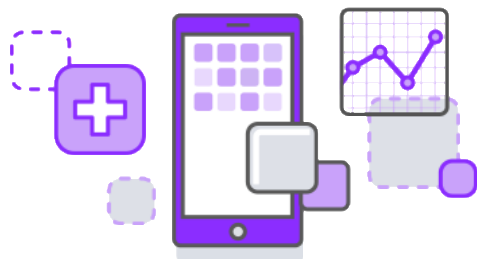
# 对于后台实现，请看一个大的架构演进..

## 微服务

- 原子化、自包含的代码单元
- 易于开发，部署和分享
- 遵循JSON/REST/HTTPS范式

## 无服务器

- 开发、运行和扩展应用程序和微服务
- 不需要提供和管理服务器



微服务



## 使用AWS服务创建无服务器的微服务



AWS Lambda



Amazon API Gateway



Amazon Cognito



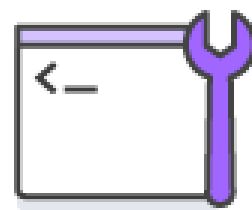
# AWS Lambda



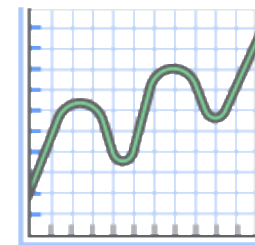
直接运行您的代码而  
不用关心基础设施



只为您消耗掉计算时  
间付费



易于开发和部署



持续扩展和监控

- 使用Lambda创建您的无服务器的微服务
- 支持Java、Python、node.js和C#开发语言



# 使用AWS Lambda开发无服务器的微服务

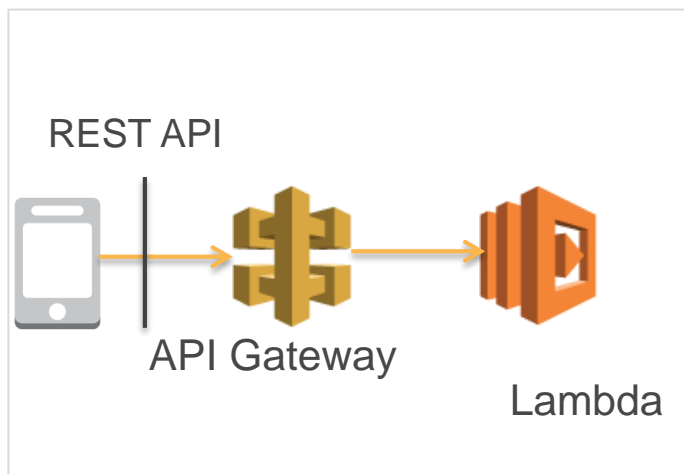


AWS Lambda

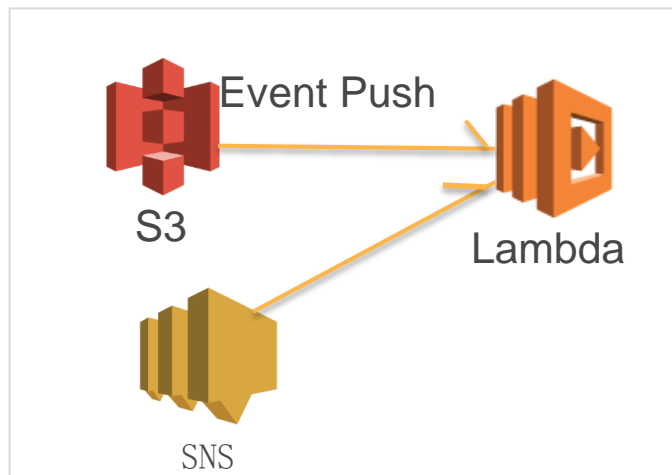
- 一个功能或者应用逻辑单元
- 通过事件触发或者同步的请求响应模式调用
- 无状态的编程模型
- 独立打包、部署和扩展的单元
- 可声明的配置和扩展需求

无服务器的应用程序就是由一组松耦合的微服务组成

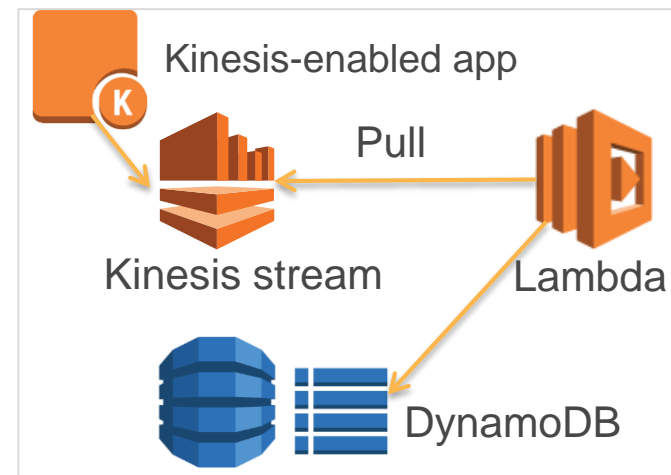
# 使用AWS Lambda



使用API Gateway  
调用Lambda API



事件推送到Lambda



Lambda事件拉取



定时事件

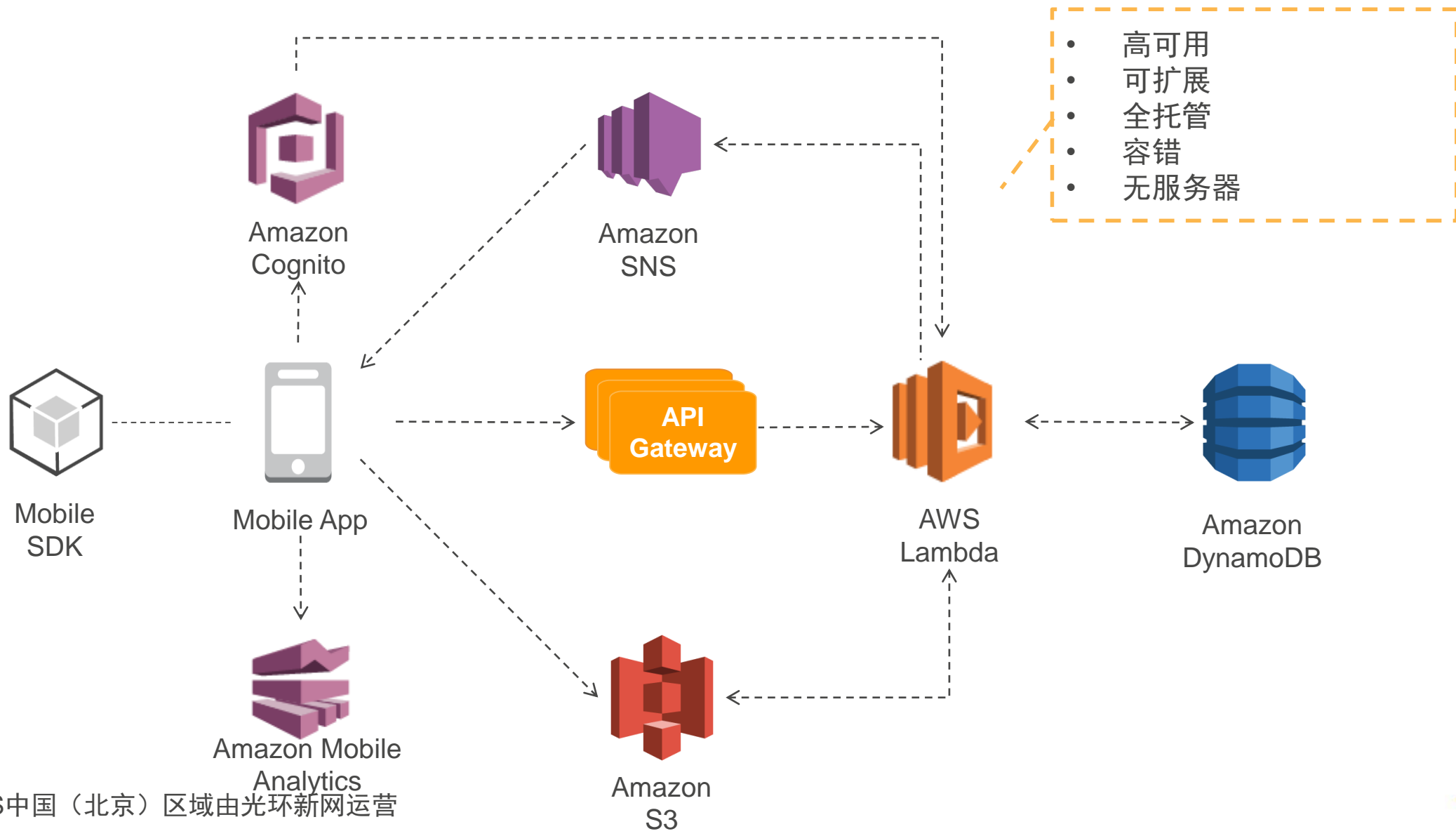


使用客户事件源调用Lambda



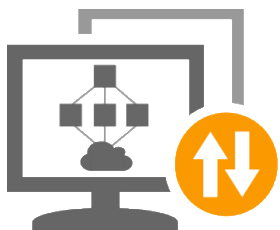
客户认证流

# Lambda无服务器移动后台架构的典型场景





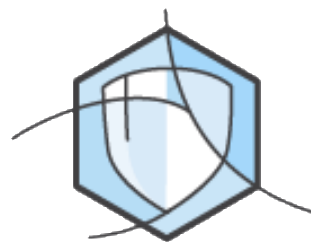
# 亚马逊API Gateway服务



简单的API  
开发



可扩展的性能



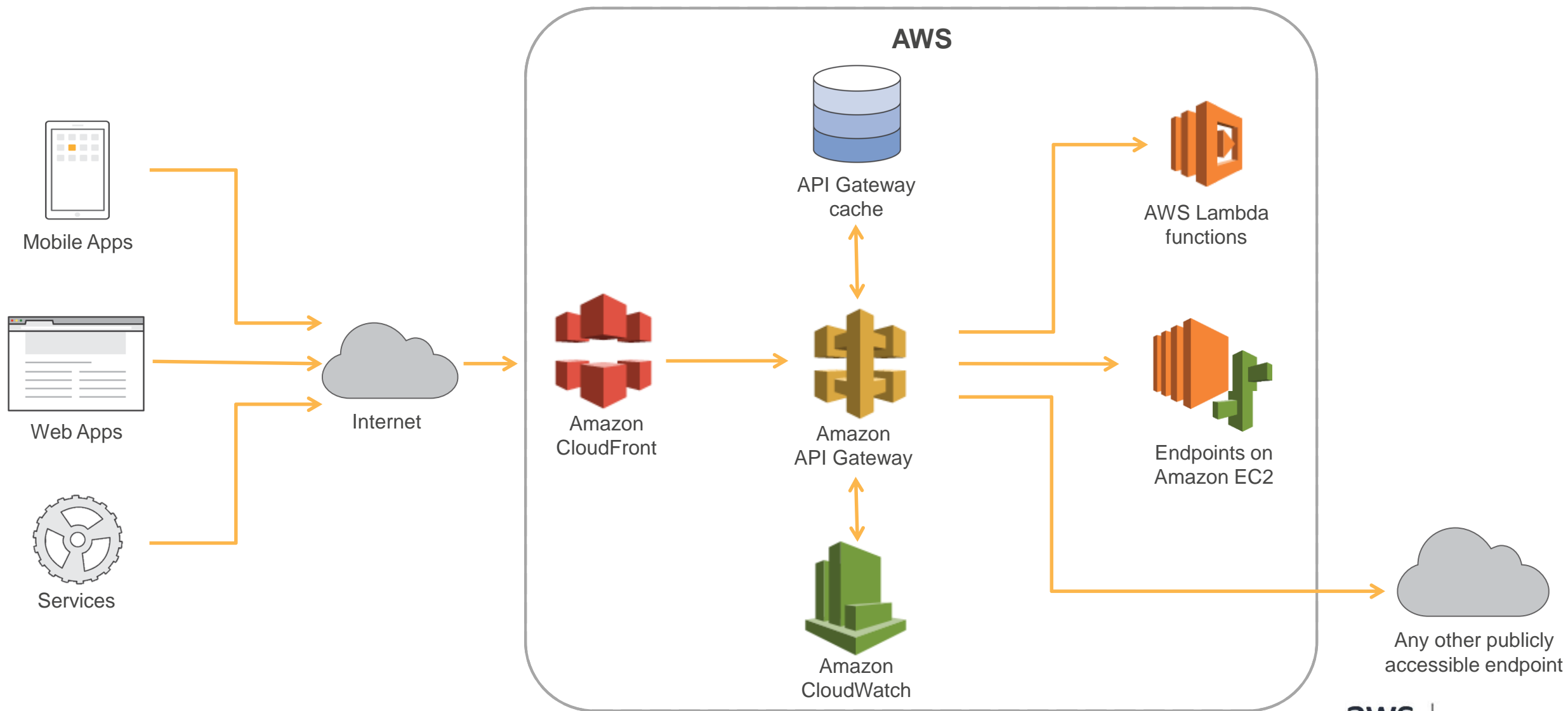
安全控制



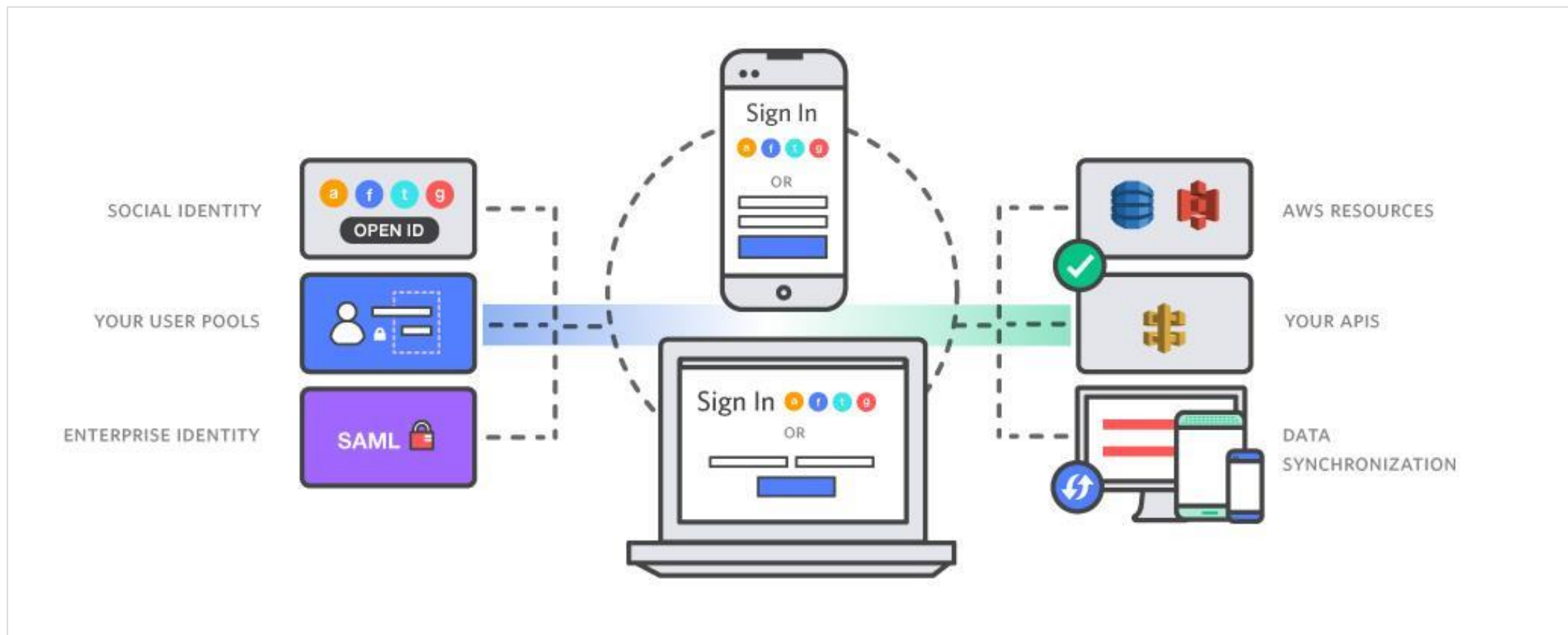
监控和度量  
API行为

使用API Gateway创建，发布，监控和保护您的API

# 亚马逊API Gateway: 无服务器的API



# 使用亚马逊Cognito服务管理用户身份



# 亚马逊Cognito概览

## 1

### 身份管理



来宾 开发者 用户池  
身份认证

跨越不同身份提供商管理认证  
用户身份，同时支持未认证用  
户访问

## 2

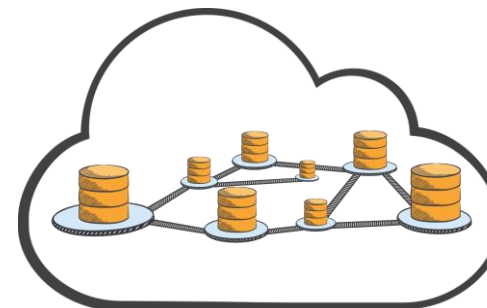
### 安全访问AWS服务



通过不同移动设备和平  
台安全地访问AWS服  
务

## 3

### 数据同步



- 利用云实现跨设备和平台的用户数据同步
- Cognito事件：触发AWS Lambda函数
- Cognito流：发送数据同步事件给亚马逊Kinesis流

# 亚马逊Cognito身份管理

## 支持多个身份提供商

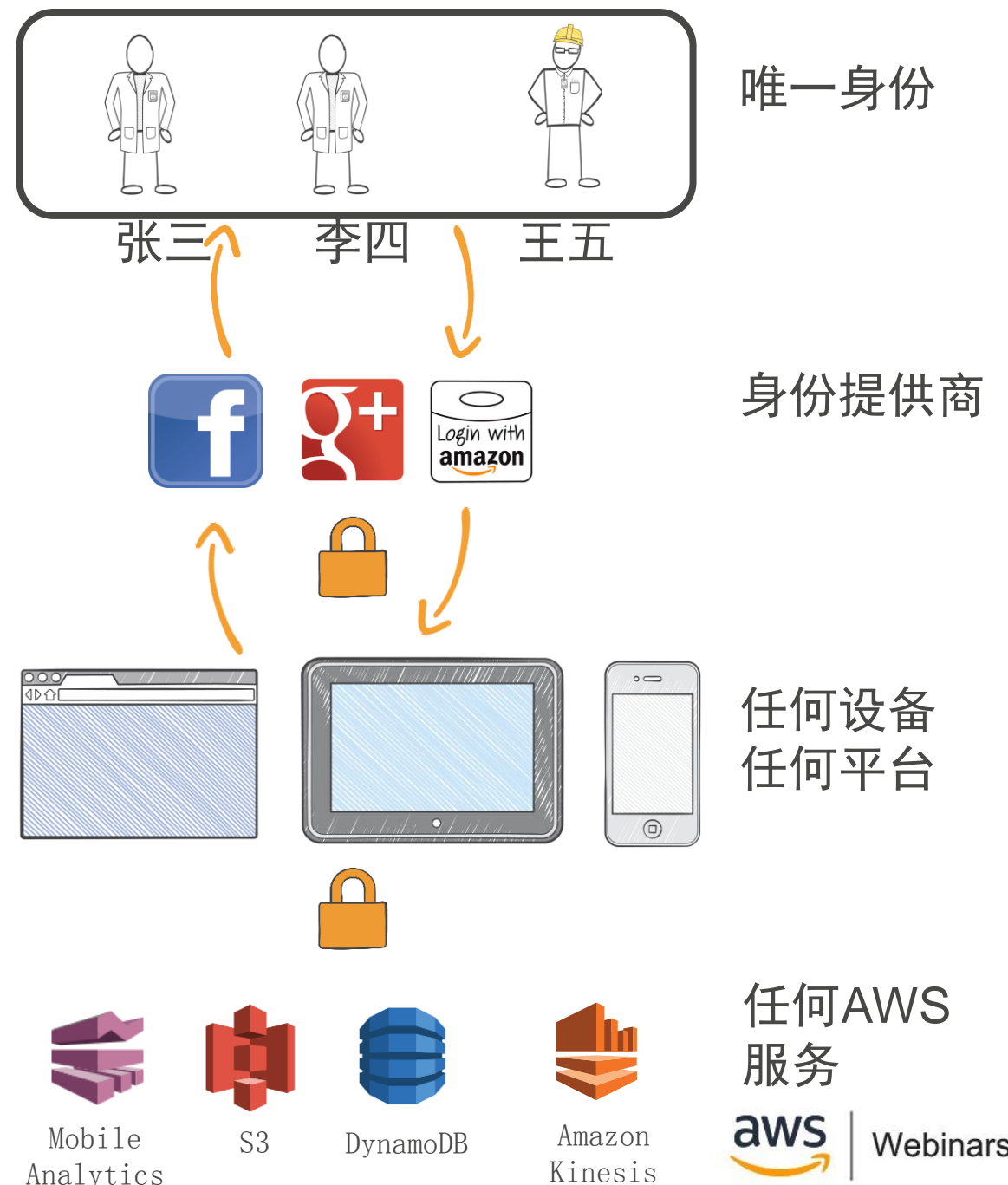
轻松集成主要的身份提供商实现用户身份验证

## 唯一的用户身份VS不同设备

管理唯一身份. 跨不同设备和平台自动识别唯一用户身份

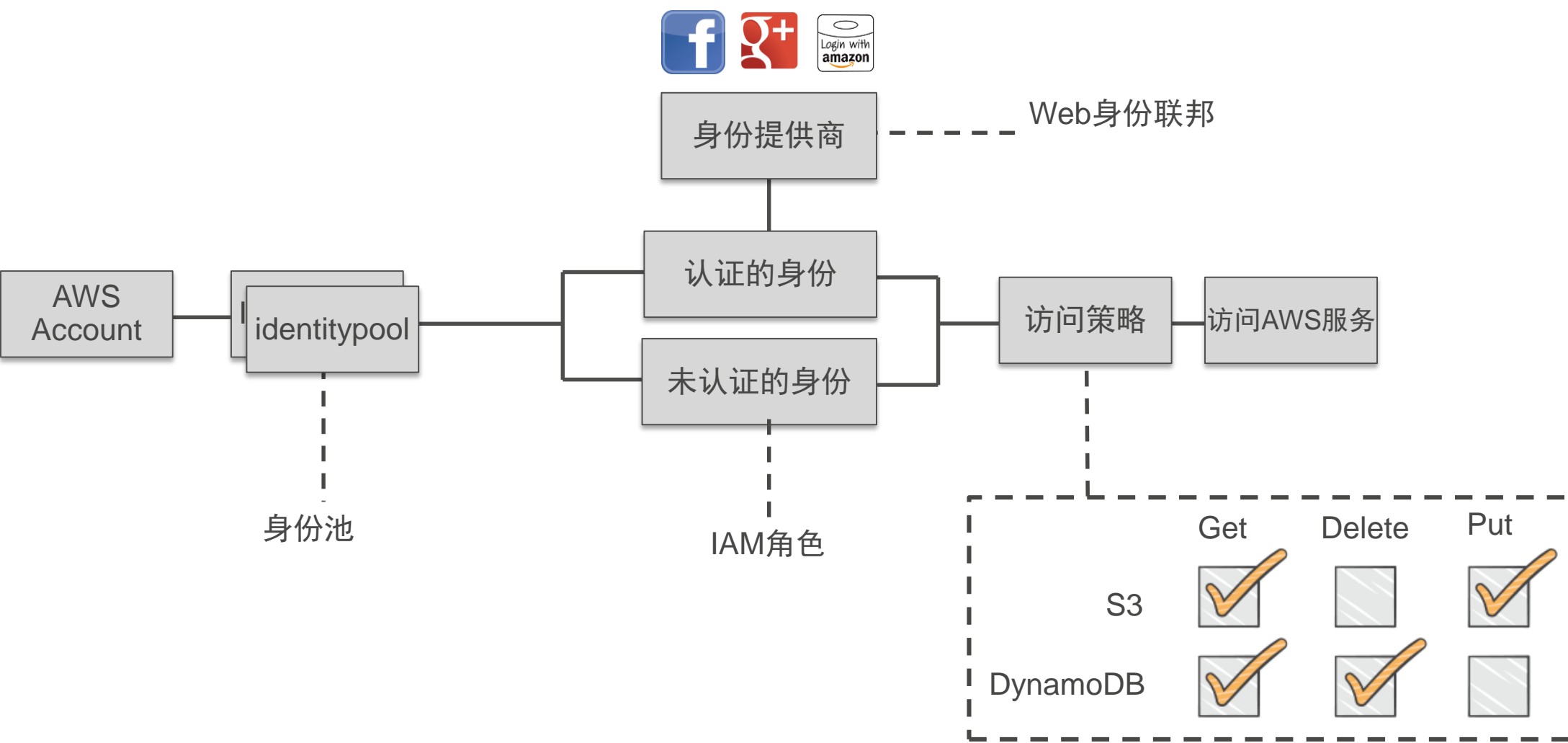
## 帮助实现安全最佳实践

使用移动设备安全访问任何AWS服务  
简化用户程序和AWS IAM服务的交互过程





# 亚马逊Cognito身份池

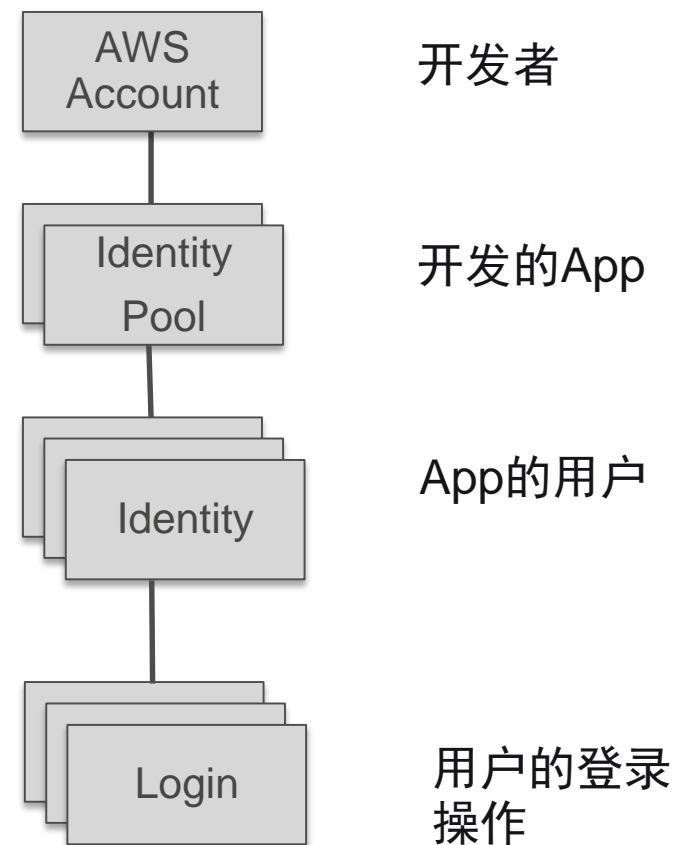


# Cognito身份管理数据模型

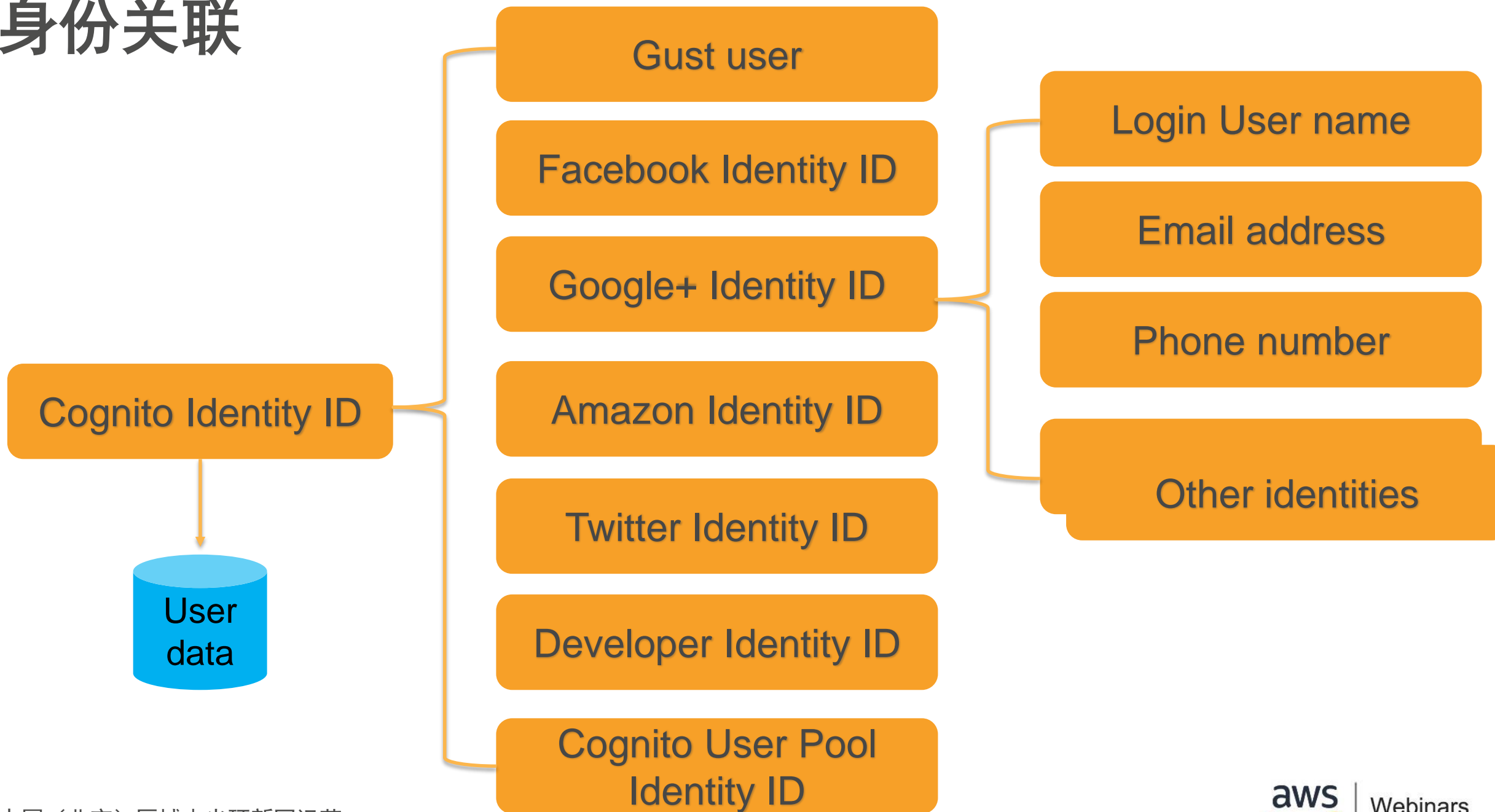
**Identity Pool:**身份池是用于存储特定于您的账户的用户身份数据的存储区， 可以被多个app共享

**Identity:** 代表单个用户身份。在多个用户身份提供商间保持一致，也可以是一个来宾用户

**Login:** 代表一个身份提供商的用户身份



# 身份关联



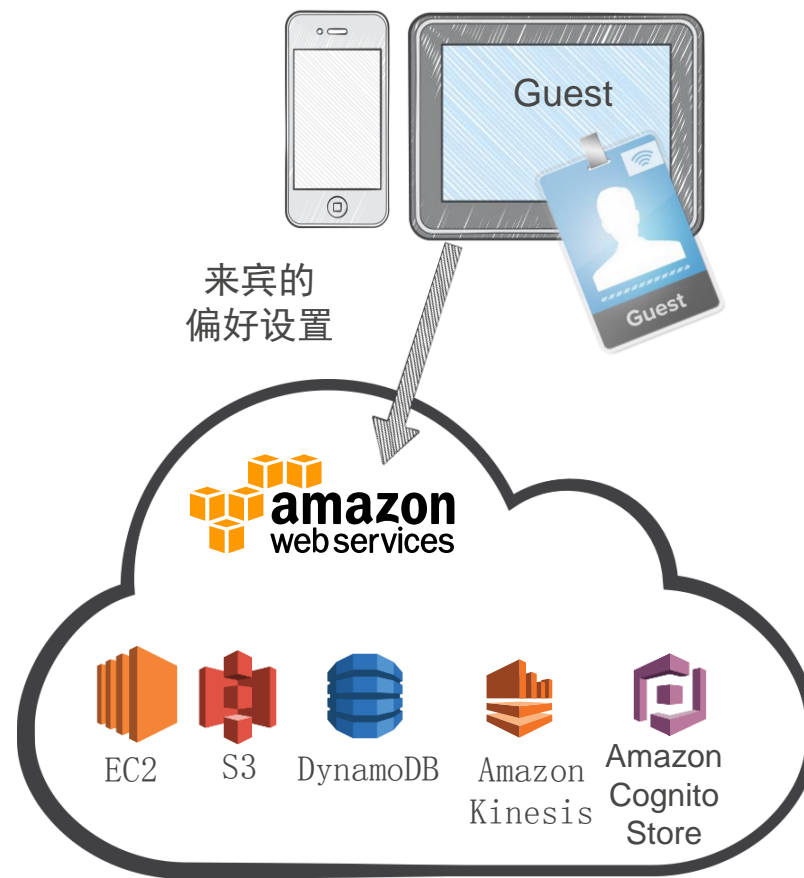
# 亚马逊Cognito支持未认证的用户身份

## 来宾用户访问

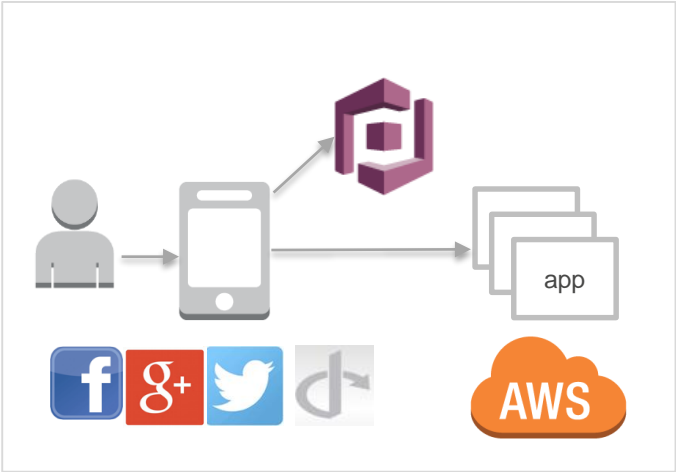
安全的访问AWS资源，使用App功能，无需创建账号或登入

## 在云端保存数据

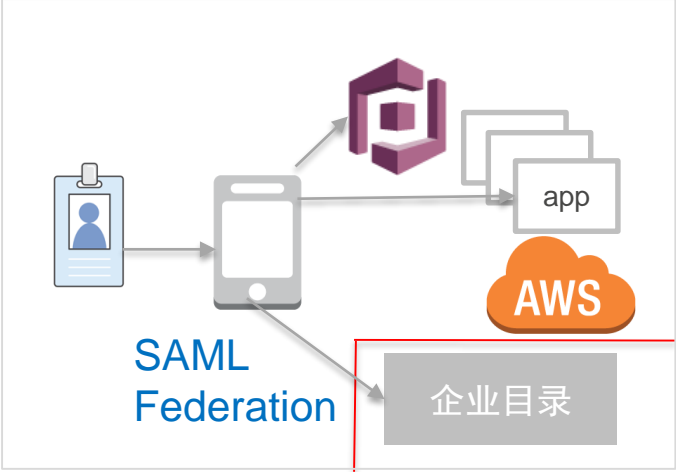
在云端保存app和设备数据，当用户登录后再合并



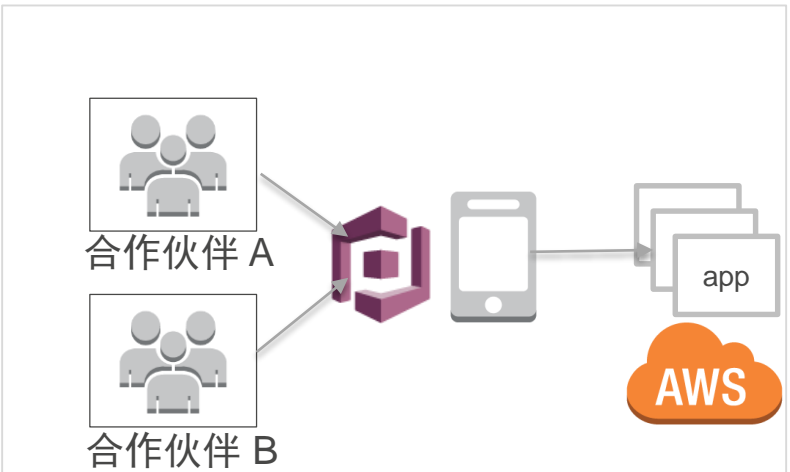
# 使用亚马逊Cognito服务管理用户身份



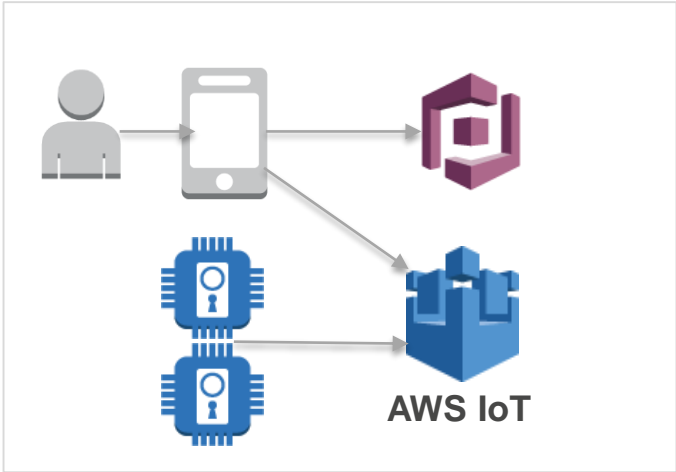
B2C



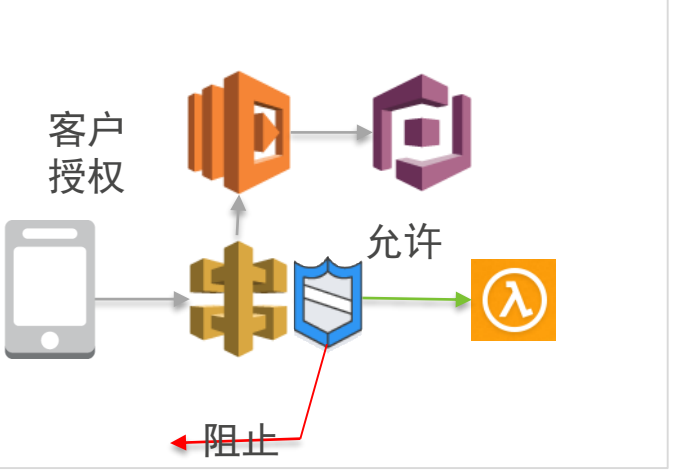
B2E



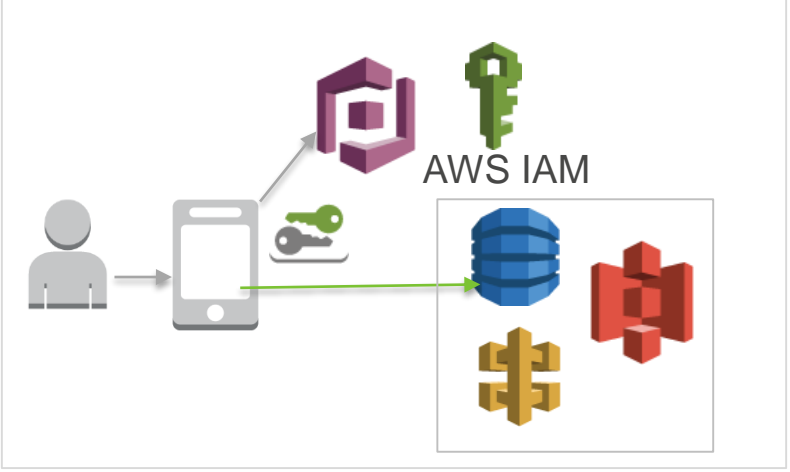
B2B



IoT场景



API网关和Lambda



对AWS资源的  
访问控制

# 使用亚马逊Cognito保存和同步用户数据

## 保存App数据，用户偏好和状态

在云端保存app和设备数据并且在用户登录后执行数据合并

## 跨设备 跨操作系统数据同步

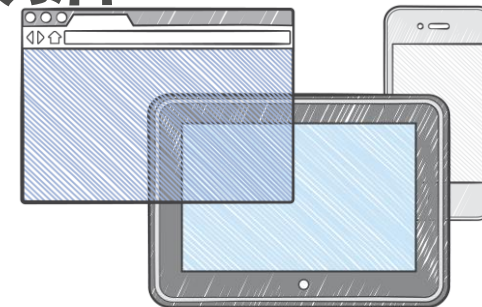
只需要一行代码即可实现在不同设备和操作系统间同步用户数据和偏好

## 离线工作

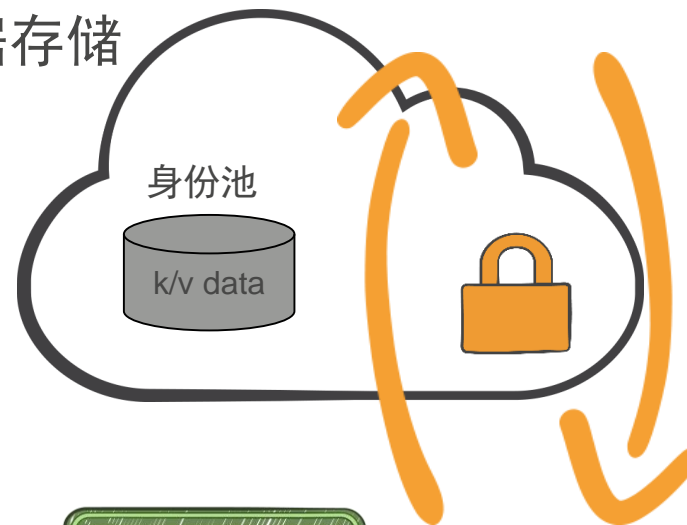
数据总是先保存在本地的SQLite数据库，即使在网络质量不佳或者断网环境下也可以正常工作

## 不需要开发后台服务

简单的客户端SDK调用即可， 去除了服务器端开发的需求



用户数据存储  
和同步



任何平台



iOS/Android/FireOS



Webinars

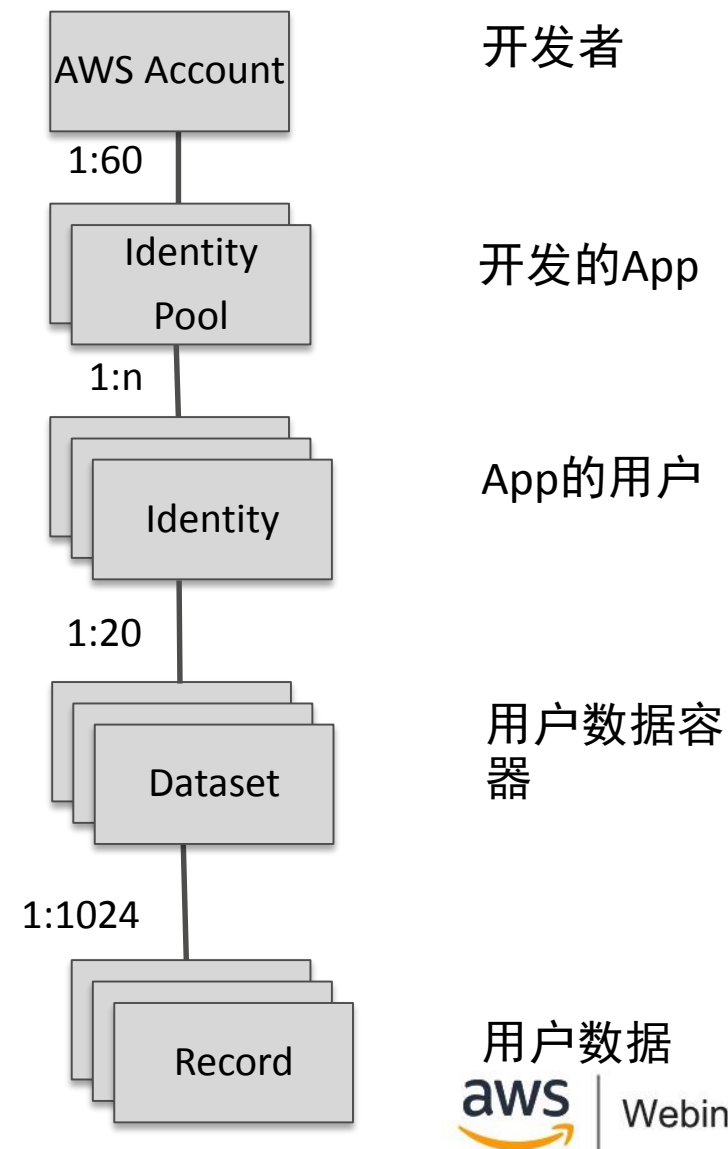
# 亚马逊Cognito同步功能数据模型

**Identity Pool:**身份池是用于存储特定于您的账户的用户身份数据的存储区，可以被多个app共享

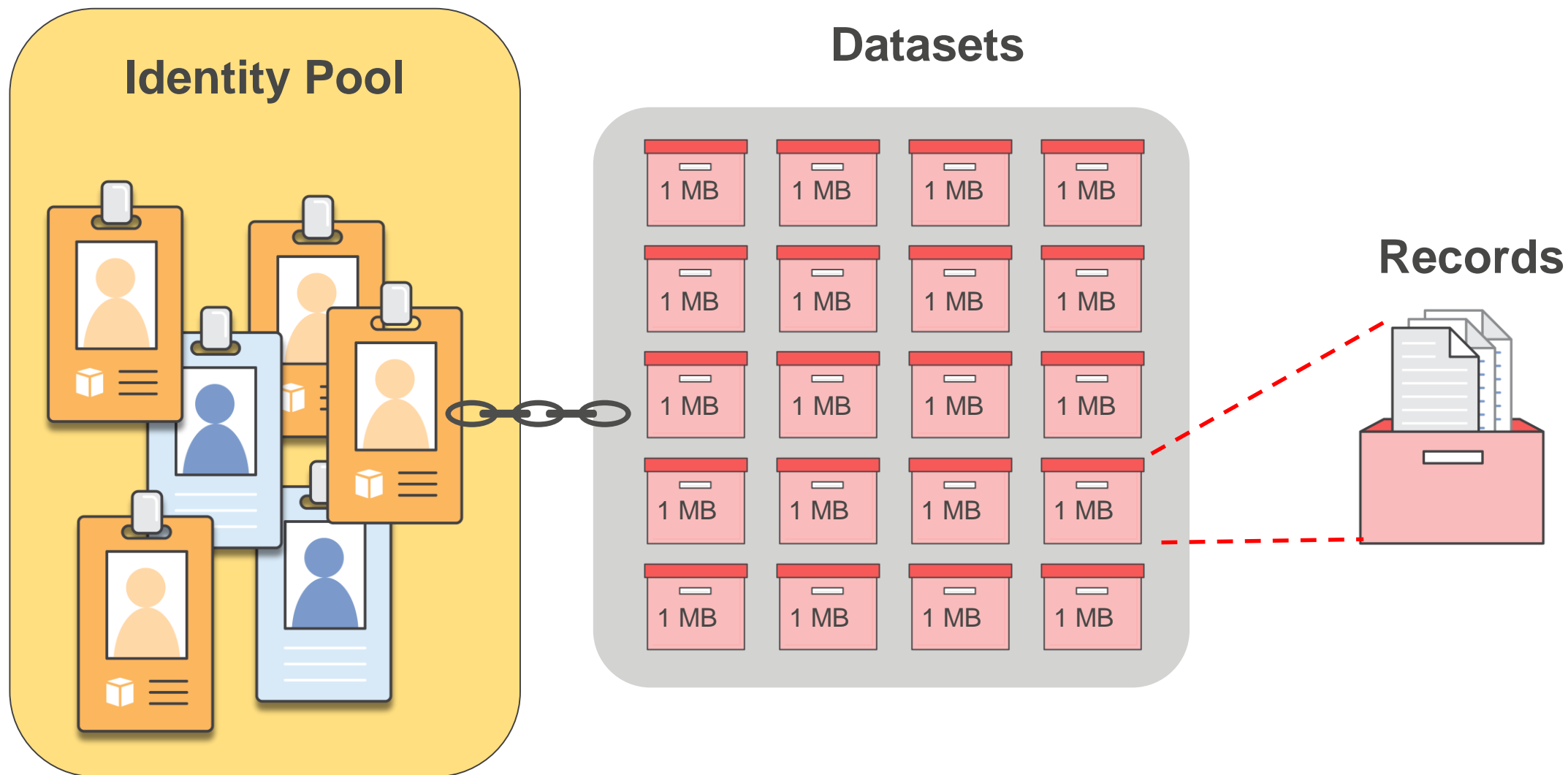
**Identity:**代表单个用户身份。在多个用户身份提供商间保持一致，也可以是一个来宾用户

**Dataset:** 代表单个用户管理下的一组数据，是每次执行数据同步的最小单位，一个Dataset最多保存1M数据

**Record:** 代表实际数据的键/值对



# 亚马逊Cognito同步功能数据模型

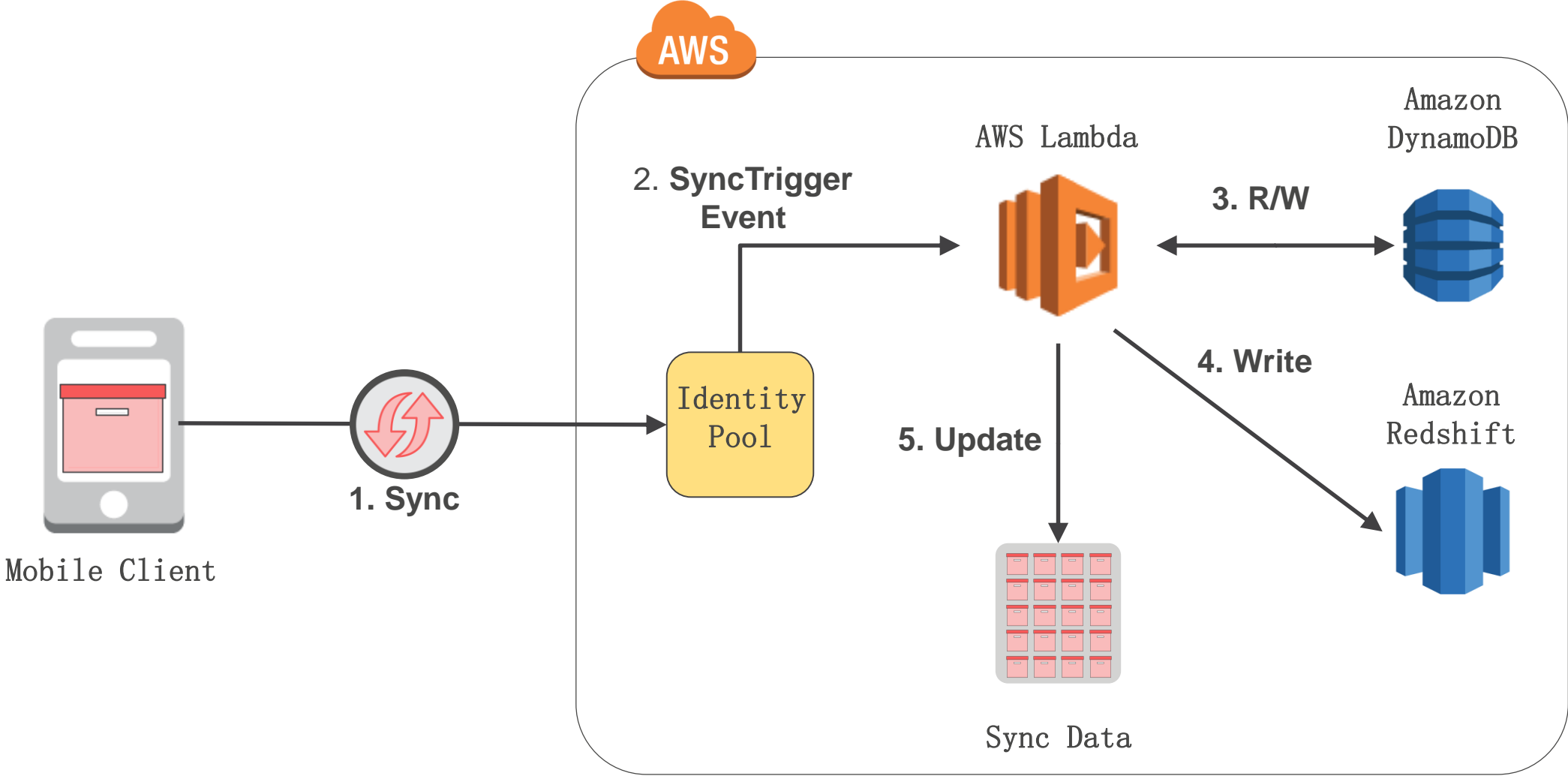




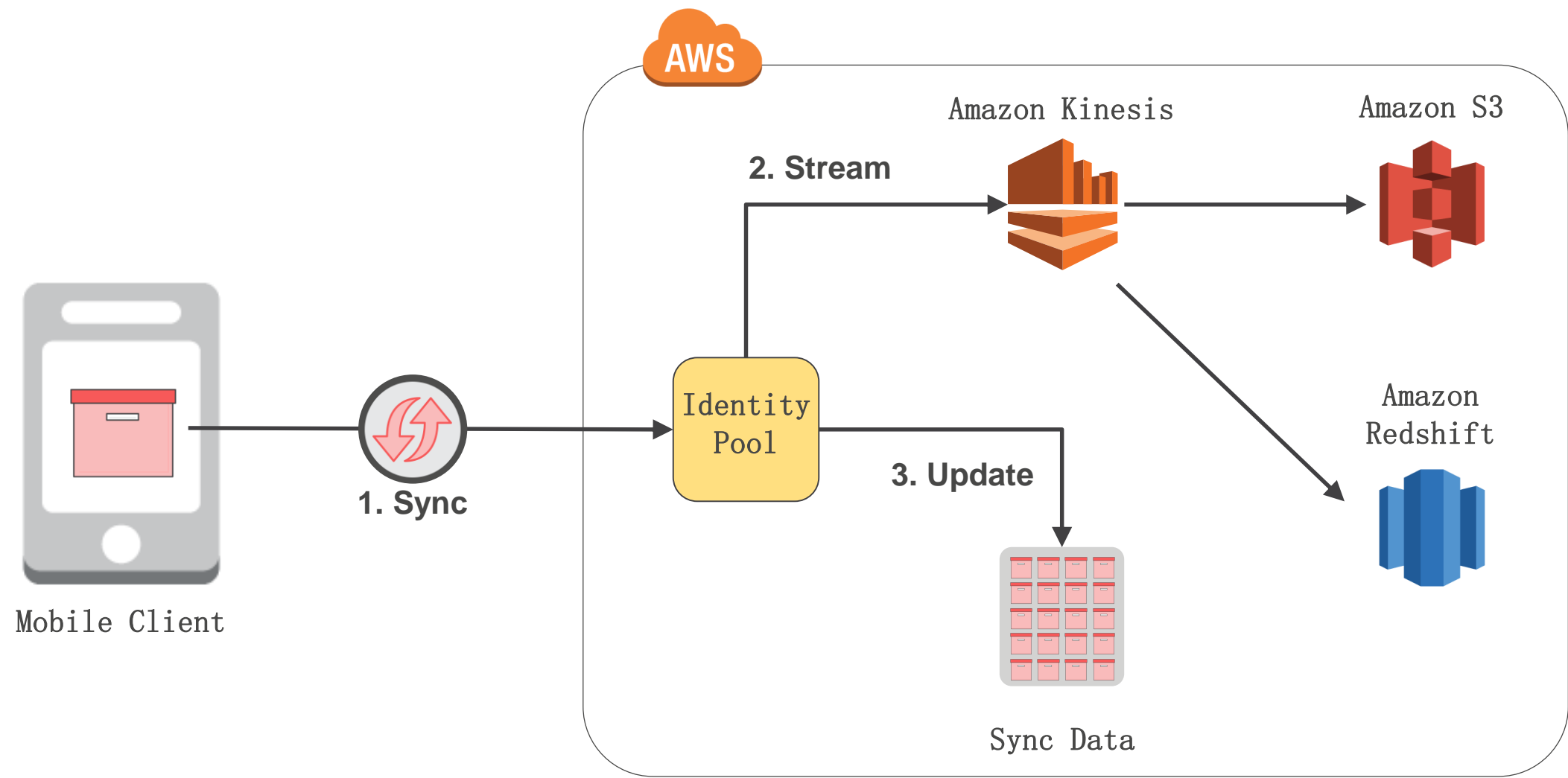
# 关于Cognito数据同步

- 移动客户端主动将变化的数据推送回Cognito.
- 移动客户端从Cognito拉取发生变化的数据
- 订阅以便接受数据变化的静默通知

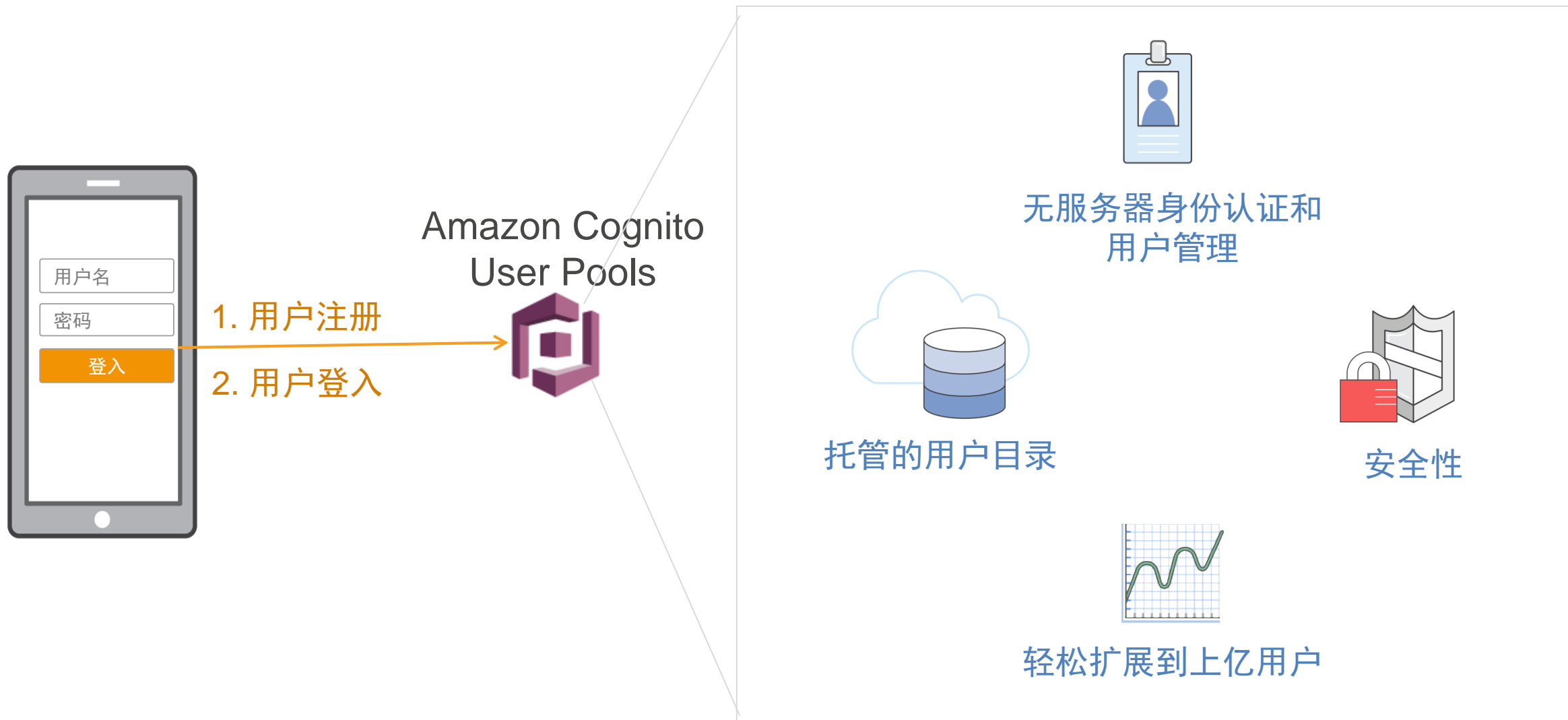
# Cognito数据同步事件处理



# Cognito Streams



# 使用Cognito用户池管理用户注册和登入安全



# 预定义用户流程

## 用户注册和登入

允许用户使用电子邮箱、电话号码或用户名注册和登入您的应用

## 用户个人信息

允许用户查看和更新个人信息 – 也包括定制的用户属性

## 忘记密码

允许用户在忘记密码的时候通过邮件或手机短信方式验证身份修改密码

## 基于令牌多身份认证

使用基于OpenID Connect (OIDC)和OAuth 2.0标准的JSON Web Tokens (JWTs)用于后台的用户认证

## 电子邮件或电话号码验证

在完成注册前要求用户校验电子邮件或电话号码

## 短信多因子认证

作为认证步骤的一部分，要求用户输入通过短信获得的安全码来完成第二因子认证。

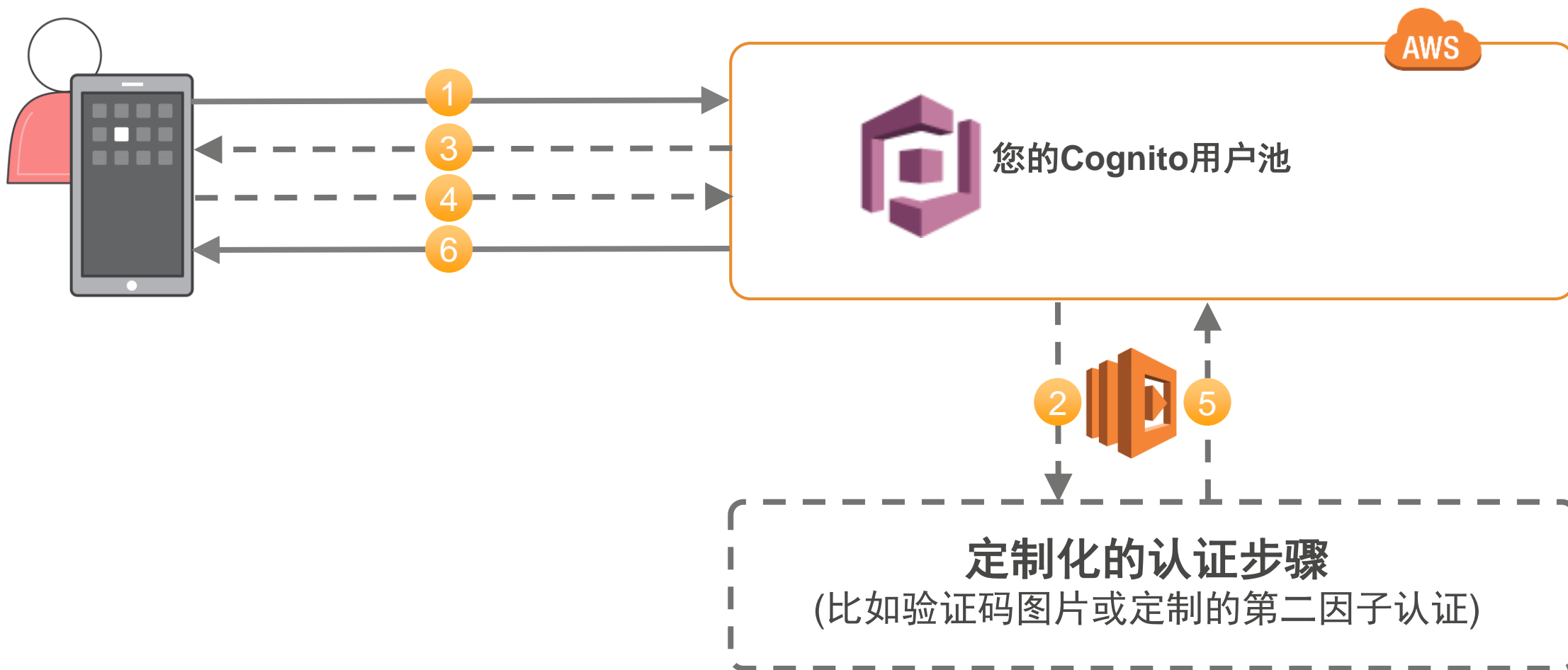
**可以使用Lambda定制化这些标准流程**

# 使用Lambda函数定制用户流程



分类	Lambda函数	例子场景
定制化认证流程	定义认证质询	确定一个定制化认证流程中的下一个质询
	创建认证质询	为一个定制化认证流程中创建一个质询
	校验认证质询响应	决定一个定制化认证流程中，用户针对认证质询给出的回应是否正确。
认证事件	认证前	增加自己的校验逻辑来允许或阻止用户登入请求
	认证后	记录日志以便事后分析
注册	注册前	增加自己的校验逻辑来允许或阻止用户注册请求
	确认后	定制通知消息个事或者记录日志以便事后分析
消息	定制消息	高级的定制化或本地化的消息

# 定制化认证流程



# 可扩展的管理能力

## 创建和管理用户池

创建、配置和删除多个用户池

## 自定义属性

可以添加自定义的用户属性

## 要求某些属性必须提供

可以选择一些属性，要求用户在注册过程中必须提供

## 为每个 app 单独设置权限

可为不同的app设置每个用户属性的读写权限

## 设置密码策略

强制用户密码策略比如最小密码长度，必须要包含特定类型的字符等

## 搜索用户

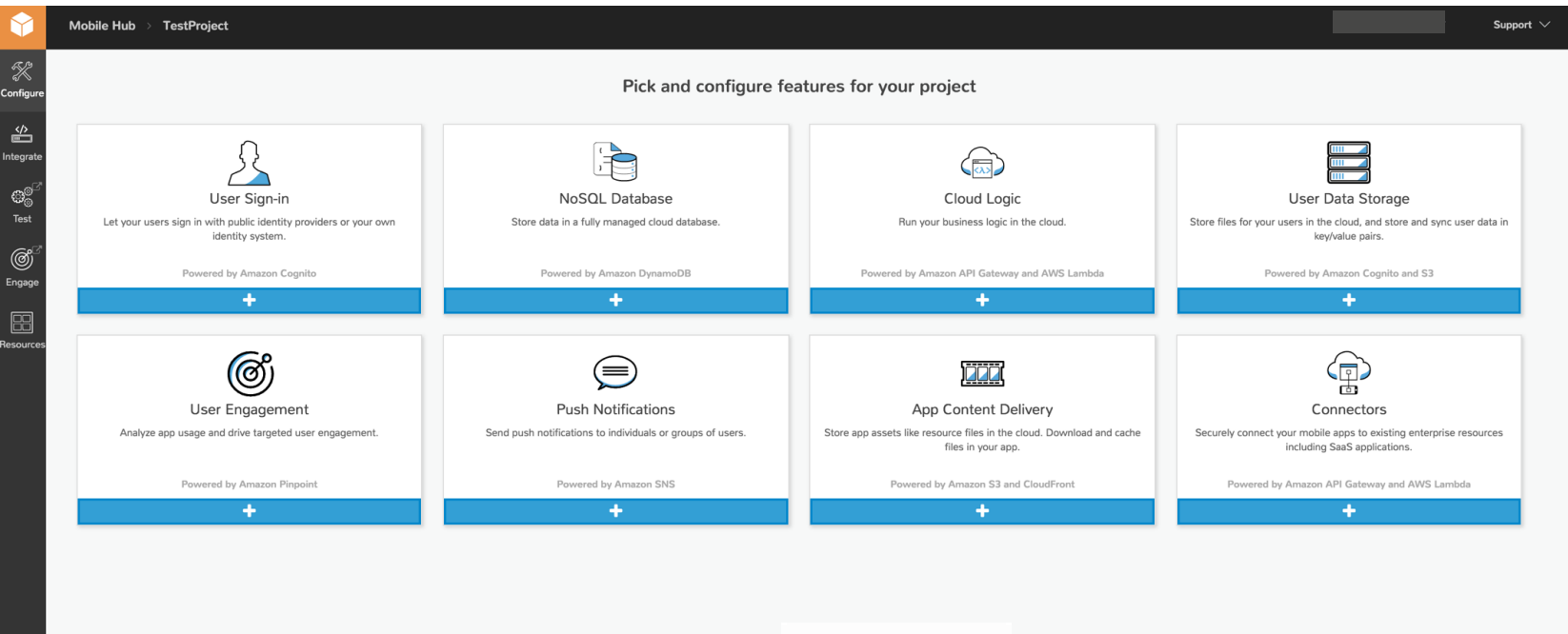
通过控制台或管理API以属性精确匹配或前缀匹配方式搜索用户

## 管理用户

执行管理操作比如重置密码、确认用户、启用MFA、删除用户和全面登出



# 亚马逊Mobile Hub和SDK



iOS SDK



Android SDK



JavaScript SDK



React Native



Xamarin



Windows



Unity



Android Studio

Objective-C, Swift

原生移动应用



混合移动应用

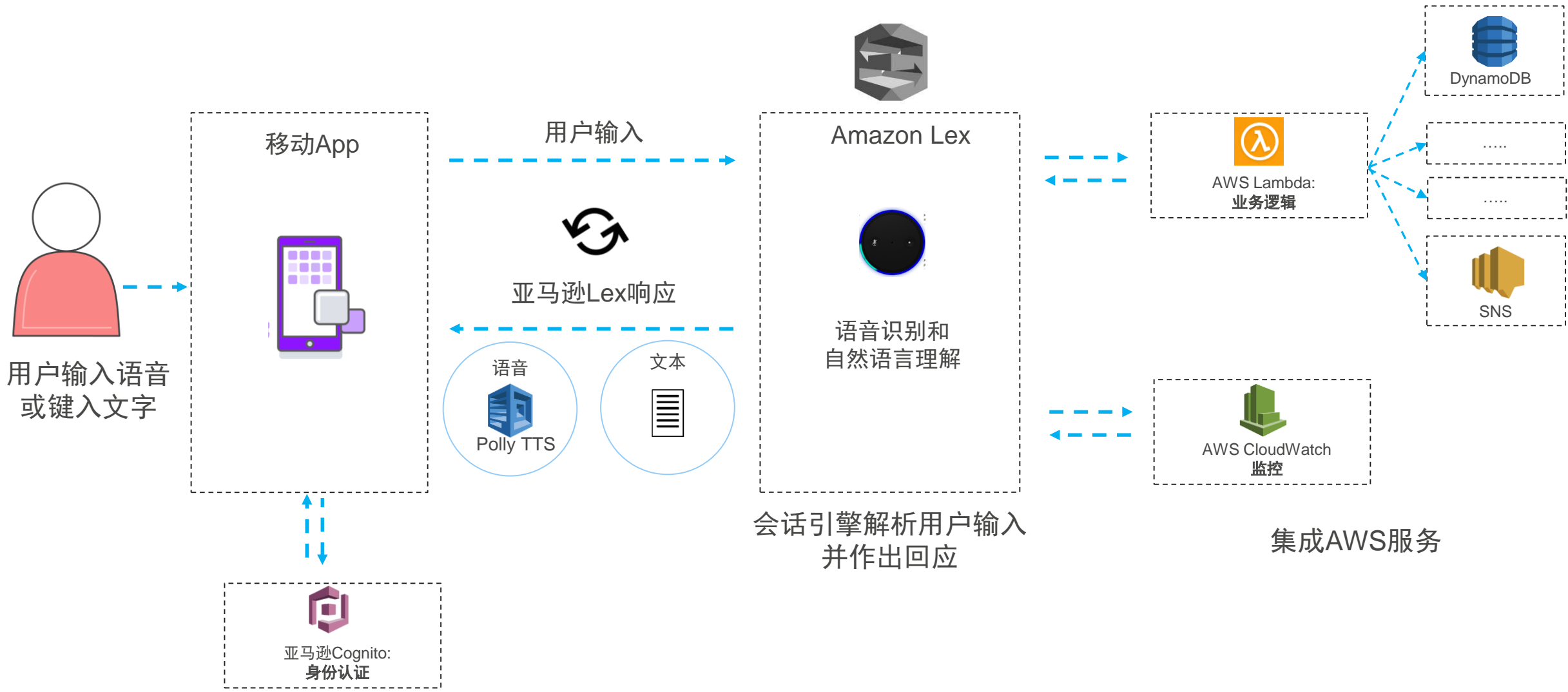


Web应用



















Webinars

# 亚马逊Lex：移动应用的语音交互界面



# 总结：使用AWS开发移动App和无服务器微服务

移动App开发	无服务器 后台	身份管理	测试和 部署工具	数据	存储和 内容	移动分析	分析和 大数据	邮件+ 推送
 Mobile Hub	 AWS Lambda	 Amazon Cognito Identity	 AWS Device Farm	 Amazon DynamoDB	 Amazon S3	 Amazon Mobile Analytics	 Amazon EMR	 Amazon Simple Email Service
 Android SDK	 API Gateway	 Amazon Cognito User Pool	 AWS CodeCommit	 Amazon RDS	 Amazon CloudFront	 Amazon PinPoint	 Amazon Kinesis	 Amazon SNS
 iOS SDK			 AWS CodeDeploy	 Amazon Cognito Sync			 Amazon Redshift	
 JavaScript SDK			 AWS CodePipeline					

# 客户案例



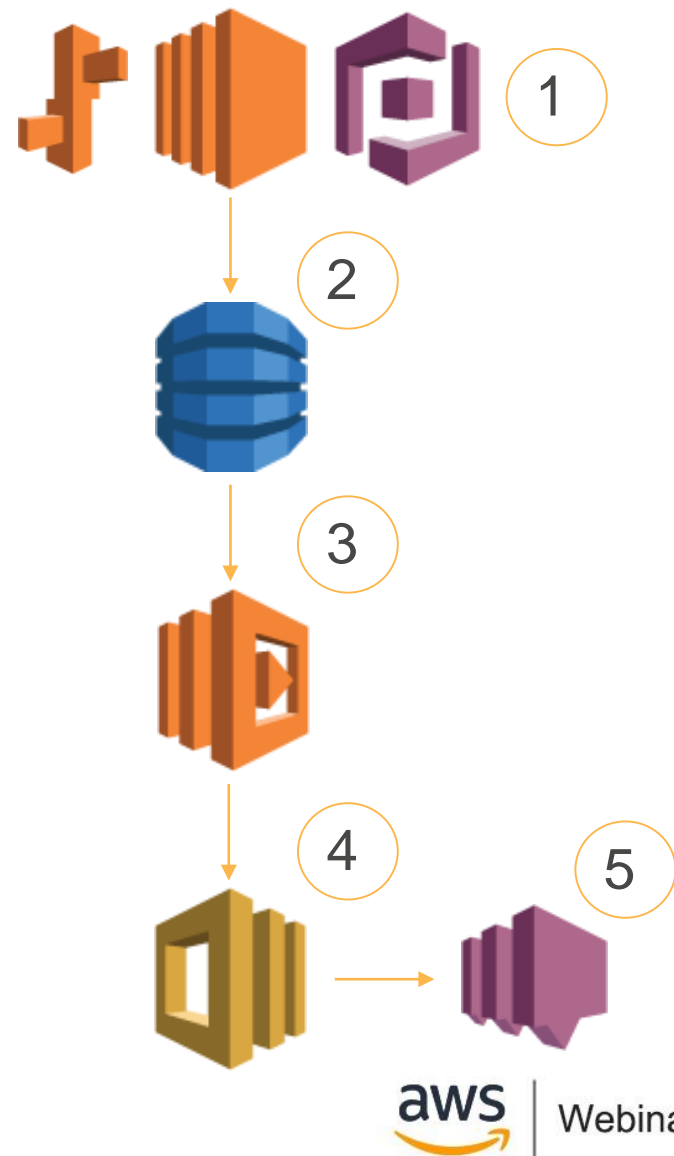
## 纽约生活实验室

# 关于纽约生活实验室

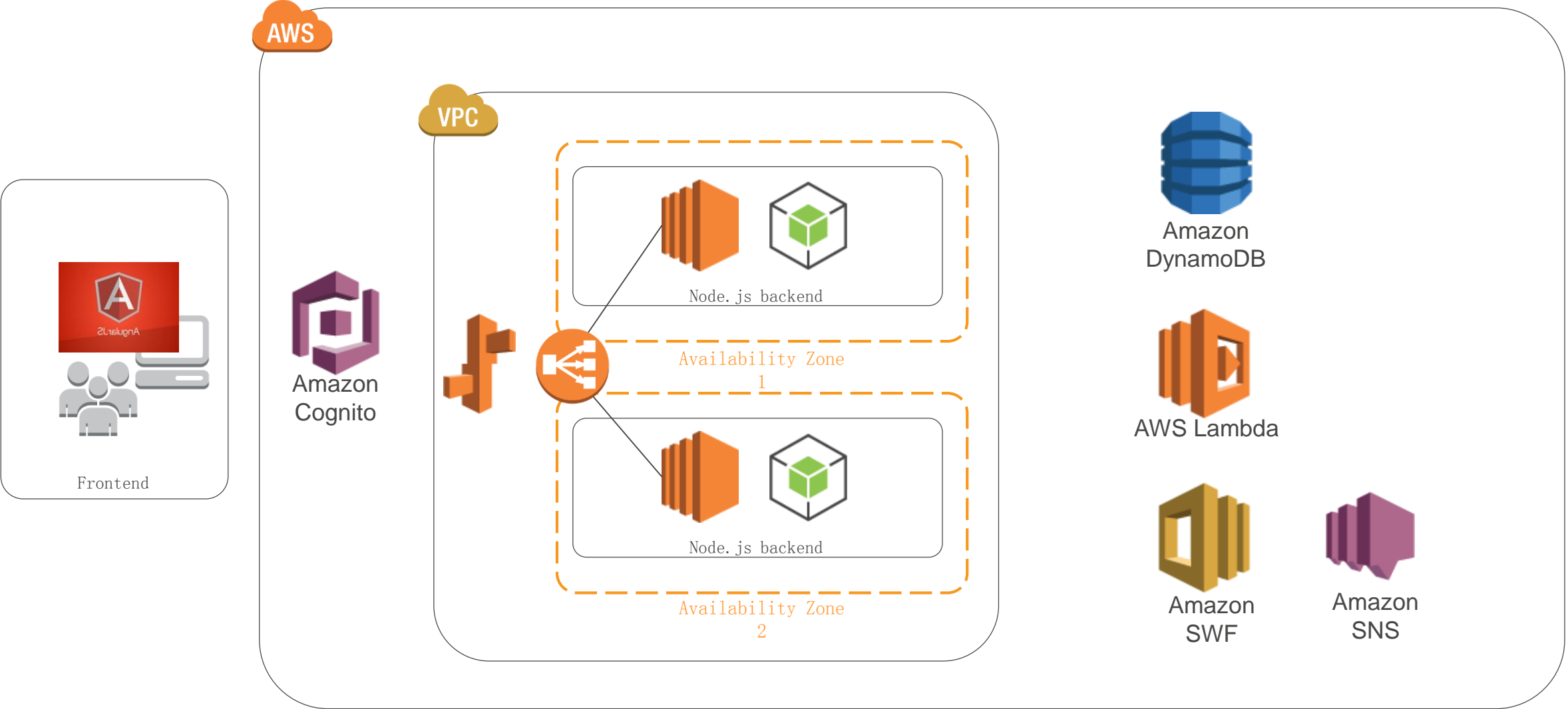
- 纽约生活实验室是纽约人寿风险投资公司的子公司，它是纽约人寿保险公司的企业风险投资公司
- 拥有思想家，工程师和精算科学家
- 正在试验聊天机器人，人工智能和区块链
- 连接，协作和创建下一代保险产品和服务

# 理赔处理

1. 受益人在线提交理赔申请
2. 声明被保存并且检索出策略信息
3. workflow 被触发
4. 自动理赔处理 workflow 启动
5. 状态更新通知发送给受益人



# 应用程序架构



# 用户认证和授权

- 为什么使用亚马逊Cognito服务？
  - 安全地访问那些我们应用需要的AWS服务和资源
  - 支持验证过的和未验证过的身份
  - 允许多个用户对身份池策略中定义的服务和资源具有相同的访问权限



# 亚马逊Cognito用户池

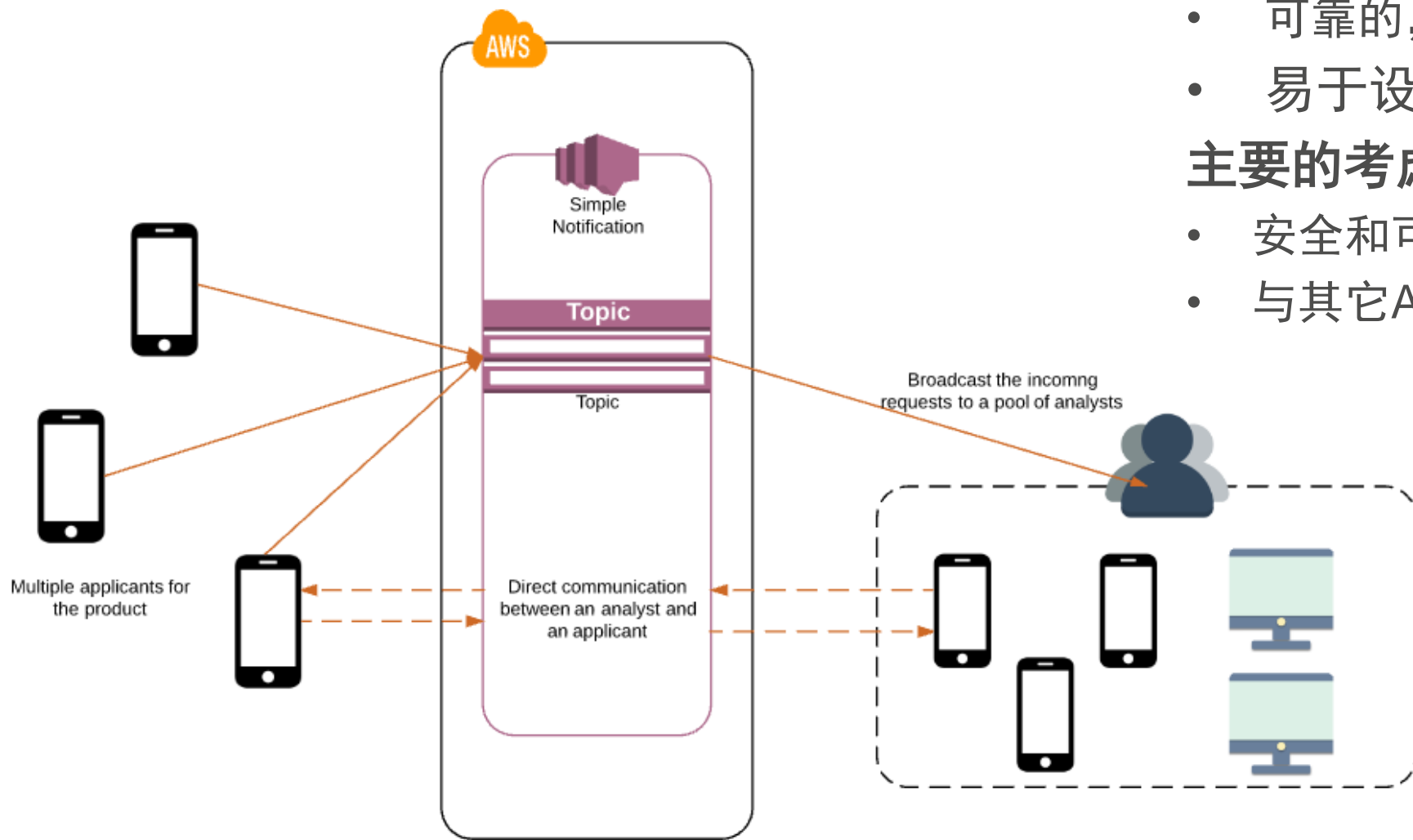
- 为什么我们选择亚马逊Cognito用户池？
  - 可扩展，全托管的用户目录
  - 提供增强的安全
  - 对注册和登录过程进行精细化控制
  - 作为一家初创公司，用户池推动的业务持续快速增长是一个关键因素
- 做为早期Beta版用户和AWS产品团队紧密合作

# 使用AWS Lambda实现事件处理

- 亚马逊DynamoDB事件流触发AWS Lambda函数，调用亚马逊SWF工作流
- Lambda同样被用于由SWF调用的活动Worker



# 利用亚马逊SNS服务实现推送通知



## 为什么选择SNS?

- 可靠的，可扩展和安全的
- 易于设置，简单和成本效益

## 主要的考虑因素

- 安全和可靠性
- 与其它AWS服务的集成能力

# 谢谢大家！