AWS Hack’n’Roll
Cloud 101

AWS User Group Taiwan

whoami

- 呂昭寬 `clifflu` *clifflu@gmail.com*
  AWS User Group Taiwan
  Chief Cloud Architect at EMQ Inc.

- Formerly
  104, TrendMicro, …

講在前面

- 主要目標
  透過實作，建立對 CDK 與部分 AWS 服務的認知，足以完成 AWS & Twitch Hack’n’Roll

- 學無止境
  AWS 服務後隱含了各種設計模式、分散式編程等；有紮實基礎，充分認識，才能善用

準備工作

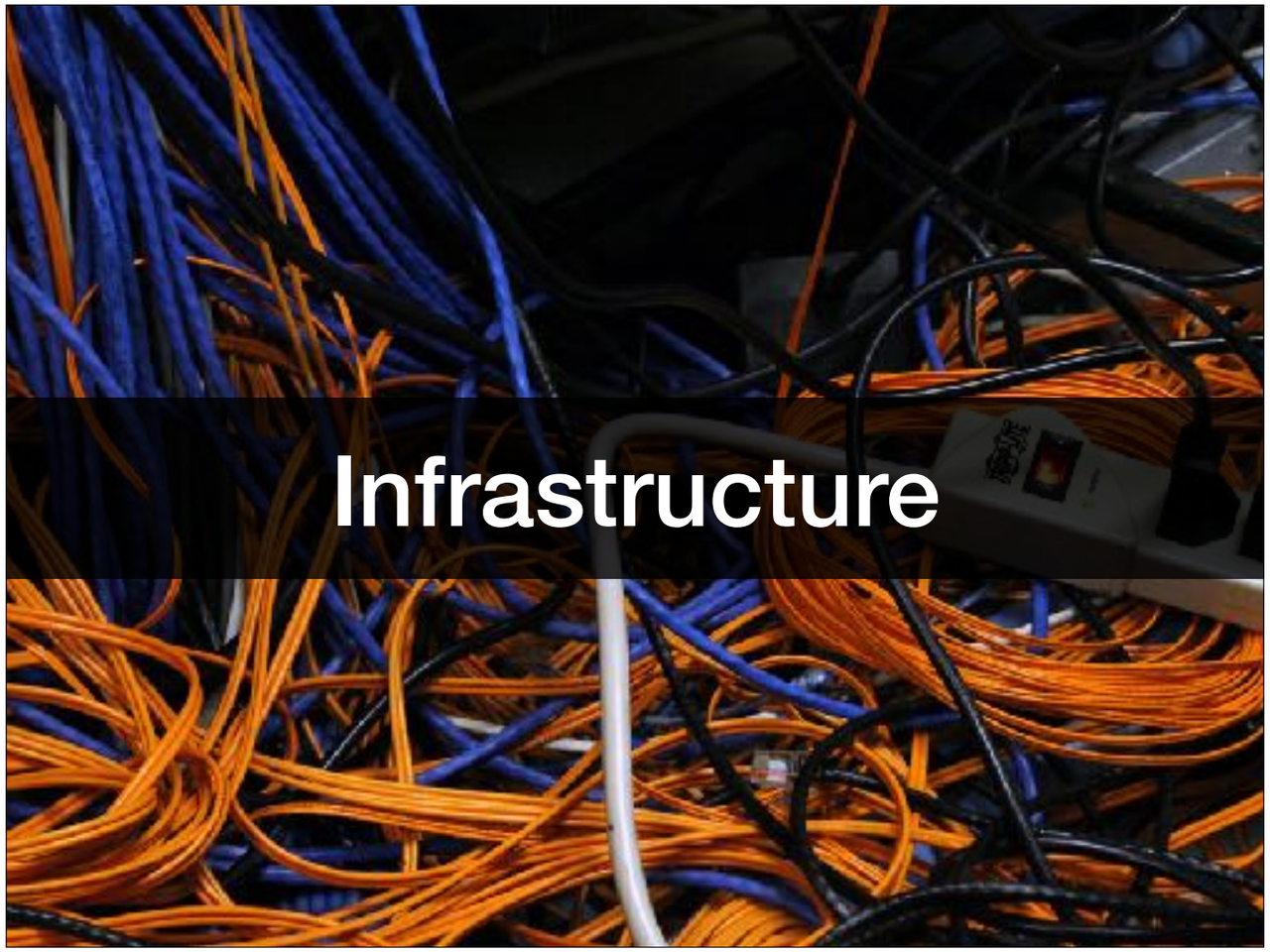
- 安裝軟體
  - git, nodejs
  - cdk
    `npm install -g cdk`
  - 安裝 Boilerplate
    `git clone https://github.com/clifflu/ug-workshop-2019`
- Docker
- 註冊 AWS 帳號並設置 Credentials
- 註冊並取得 氣象資料開放平臺授權碼
  https://opendata.cwb.gov.tw

Agenda

- Cloud Computing
- Infrastructure-as-Code
- Service Intro
- Common Patterns
- Prep

Cloud Computing

- 老生長談
- NIST 定義
  寬頻、監控、彈性、資源池
- HP 模式
- *-as-a-Service 模式


Infrastructure

Code

- 有工具
  - 版本控制
  - 測試、建置、監控
- 有流程
  - Code Review
  - Pair Programming
  - DevOps

Infrastructure-as-Code

- 使用 Code 描述 Infrastructure
- 可以被記錄、稽核、分析
  git bisect; git blame
- 容易複製、刪除、重建

AWS CloudFormation

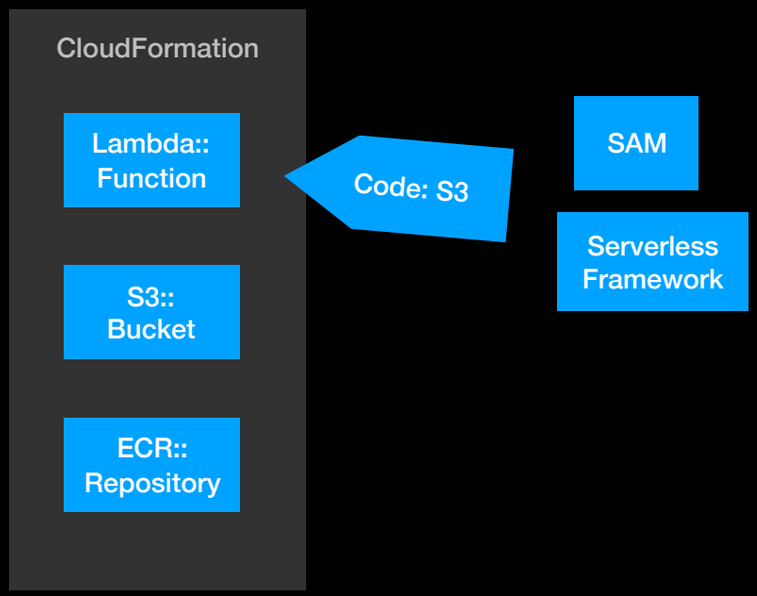
- 使用 JSON 或 YAML 描述 AWS 的資源
  支持大多 AWS 服務
- 需完整定義資源內容
- 支持透過巢狀結構、Export Variable 共享資訊
- 透過 Custom Resource 客製化

AWS CDK

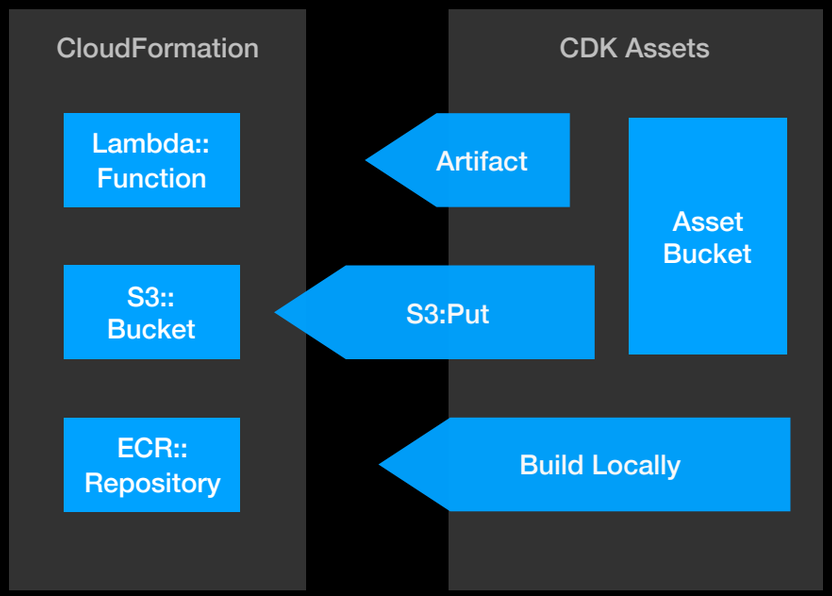
- Cloud Development Kit
- 基於 AWS CloudFormation
  - 以程式碼描述 AWS 資源
  - 強化 Template 部署前、後能做的事
- 預設值大多可用
- 簡化資源間的關聯與權限設定

CDK Demo:
HelloWorld

WHAT Happened



What Happened



CDK Demo: HelloWorldStack

細節留待 11:00: Workshop helloWorld

我看 CDK

- 持續改進中，機制、介面大致底定
- 參數 (Parameter) 機制能否滿足需求
- 簡化 CFN Template 編輯，與部署流程整合
- 適合 PoC 式的專案，與學習 AWS (及 CFN)

```
************************************************************
*** Newer version of CDK is available [1.14.0] ***
*** Upgrade recommended                                ***
************************************************************
```

AWS

- amazon.com 的 infrastructure
- 萬物皆 API
- 多透過主控臺、CLI、SDK、API 操作
- CLI 由 Python / boto3 實現

權限模型

- Root Account 持有該帳號的資源
- 有完全之權限，負完全之義務
- IAM / STS 幫助 Root Account 管理該帳號

IAM / STS

- User, Group, Role
- Credentials / MFA / Password
- Principal
- Policy

IAM Identities

- Group
  用於將 Policy 賦予一群 User
- User
  持有長或短效期 Credential，可以 Password 登入控制臺，
  可持有 MFA
- Role
  持有短效期 Credential

Authentication in IAM

- Credentials
  AWS_ACCESS_KEY_ID
  AWS_SECRET_ACCESS_KEY
  AWS_SESSION_TOKEN

- Password
  用於登入主控臺

- MFA
  用於主控臺、sts:AssumeRole 與 sts:GetSessionToken

- Federation

Credential 取用次序

- 各 SDK 實作略有差異，或透過 Helper 達成

1. 函式參數 (SDK)
2. 環境變數
3. Credentials 檔 (~/.aws/credentials)
4. Instance / Task Metadata

IAM Policy

- 決定可以 (Allow) 或不可以 (Deny) 做什麼
  Explicit Deny > Explicit Allow > Default Deny
- Action
  被呼叫的 API
- Resource, Condition
  部分 Action 支援，需查閱文件

Amazon VPC

- Virtual Private Cloud
- 管理機器間（LAN）與對 Internet（WAN）的連線
- Placement
  AvailabilityZone, Subnet
- Connection
  Gateway, VPN, Route Table
- Control
  Security Group, Network ACL
- Audit
  Flowlog

Amazon VPC

- 現支持 …
  - 跨帳號授權使用
  - Peering
    可跨帳號，同 Region，有限跨 Region
  - Traffic Mirroring

Amazon VPC 注意

- NAT Gateway、Load Balancers 方便但有低消
- 除非以 NACL 爲主進行控制，無需過分切細 Subnet 區網 broadcast & collision 的問題在 VPC 不存在
- 儘可能由應用層控制授權，避免依賴內網對接

Amazon EC2

- Elastic Compute Cloud
- 建立各種大小、特性的虛擬機
  - 動態調整虛擬機週邊資源，如 EBS、ENI、Elastic GPU 等
  - Family: 硬體與配置特性
- 是大多 AWS 服務的基石

EC2 Family
* [a, c]: 1 vCPU to 2 GB RAM
* [t, m]: 1 vCPU to 4 GB RAM
* [r, z] : 1vCPU to 8 GB RAM; z: Intel Xeon Scalable
* x: 1vCPU to 16 (x1) or more (x1e)
* g: GPU; p: Tensor core
* f: FPGA

AWS Lambda

- Function-as-a-Service 的鼻祖
- 預設運行與 Internet，支持 Lambda in VPC
- 冷啓動時間與運行限制較常爲人詬病
- 分派的 Memory 決定 CPU 與網路能力
- 有條件 Freeze / Thaw 以重用 Container

AWS Lambda

- 原生支持 Node.js 8 / 10、Python 2.7 / 3.6 / 3.7
  Ruby 2.5、Java 8、Go 1.x、.Net Core 1.0 / 2.1
- 可利用 Custom Runtime 與 Layers 拓展
- 搭配 API Gateway 生成 Web Endpoint

Amazon ECS

- Docker Container Scheduler
- Cluster
  VPC {Subnet, Gateway, Route Table, Network ACL}
  Subnet, Security Groups
  Instances
- Network
- Service
- Task
- Task Definition
  - Container

Amazon ECS Fargate

- Docker Container Scheduler
- Cluster
  VPC {Subnet, Gateway, Route Table, Network ACL}
  Subnet, Security Groups
  ~~**Instances**~~
- Network
- Service
- Task
- Task Definition
  - Container

Amazon S3

- 非常 Durable 的 Object Storage
- 最終一致性
- 廣泛作爲其他服務的儲存機制
- Regional / Owner (Account) 設置較特別

Amazon S3

- Feature 不勝枚舉
- Versioning
- Encryption
  None, SSE-C, SSE-KMS, SSE-S3
- Storage Class
- Lifecycle
  依照物件上傳時間，自動刪除或變動 Storage Class
- S3 Event Notification

Storage Class
- STANDARD, REDUCED_REDUNDANCY
- STANDARD_IA, ONEZONE_IA
- GLACIER, DEEP_ARCHIVE

Events
- ObjectCreated [*, put, post, copy, completedMultipartUpload]
- ObjectRemoved [*, Delete, DeleteMarkerCreated]
- ObjectRestore
- ObjectReducedRedundancyLostObject

Amazon S3

- 非 File System
  - 無法直接操作 Prefix
  - 不支持 Append
- 支持 Static Website 但 http certificate 比較麻煩
  直接或透過 CloudFront、Lambda 間接提供靜態檔案

Amazon DynamoDB

- 重視拓展性的 NoSQL
- 僅支持有限資料型別
- 主鍵
  Partition and Sort Key
- Local and Global Secondary Indexes
- Data Stream

Amazon DynamoDB

- Read / Write Capacity Units
  - Leaky bucket algorithm
  - Adaptive Capacity
- Read Consistency
- Conditional Expression
- Transaction

DynamoDB 小祕訣

- 平均分散讀寫負載
- 以循序讀取代隨機讀
- 把 Table 當 RDBMS Partition 用
- 表格即索引，也能搭配外部索引

AWS ALB

- 整合服務
  - S3: Access Log
  - CloudWatch: Performance metrics
  - {EC2, Application} AutoScaling: Health check

AWS ALB

- Application Load Balancing
- 主要用途
  - Load balancing
  - HTTPS termination
  - Health check
  - Monitoring
  - Content-based routing

Amazon Kinesis

- Data Streams
  通用 Data Stream

- Data Firehose
  將資料轉存至 { ES, RedShift, S3, Splunk } 的 Mailbox

- Data Analytics
  近即時資料查詢、分析

- Video Streams
  近即時視訊流轉發與分析

Kinesis Data Stream

- Shard 從屬於 Stream
- 每個 Shard 處理能力有限
- Shard 是 Immutable，但 Stream 裡的 Shard 可動態調整
- 往 Stream 寫資料，從 Shard 讀資料
- 多半用 Kinesis Consumer Library (KCL) 記錄進度 (cursor)

Kinesis Data Stream

- 適用於各種 Producer / Consumer 場景
- Shard 調控可參考官方範例 (Application AutoScaling)
- Idempotency
- 格式版本號

Kinesis Data Firehose

- Target in { ES, RedShift, Splunk }
  搶 DMS 飯碗
- Target == S3
  - 資料落地，長久儲存
  - 將資料流轉爲 Mini-batch
    多併用 S3 Event

Kinesis 類似服務

- Amazon SNS
- Amazon SQS
- Amazon CloudWatch Events
- Amazon CloudWatch Logs w/ Filters
- Amazon MQ

AWS Certificate Manager

- 生成並管理 HTTP Certificate
- 支持 DNS 與 Email 驗證
- 憑證可由 API Gateway、CloudFront 或 ELB 使用
  CloudFront 只支持在 us-east-1 的憑證

Read the Fabulous Documents

- AWS CDK
  `https://docs.aws.amazon.com/cdk/api/latest/versions.html`
- AWS Documents
  `https://docs.aws.amazon.com/index.html`