

Case-1

跨國公司、總部在歐洲、主要生產家用電器。公司的原則是：「法規第一、安全第一，錢不是問題。」

IT 團隊大部分都在台灣, 總部有小量的運維團隊，負責在歐洲 on-premise 機房。運維人員只用 remote power shell，而且將 scripts 存在本機。

在傳統機房裡有 legacy workload、finance 系統；有自建 AD server 跟 Exchange Server。也有 Zabbix 機器用來監控所有的機器。

在 AWS 日本、新加坡、歐洲都有佈署。大量的 EC2 (MS)、SQL on RDS、s3。但是最初佈署 AWS 的人員已經離職了，當時是依照 traffic peak 來選機器跟決定數量，而且買了 3 年 all upfront 的 RI。

公司生產的工廠在中國及東南亞。工廠端設有生產產線的監控、人員的監控，log 都會先用 API post 集中到新加坡的 s3，然後進入 redshift 處理。

Dev 團隊都在台灣，每個人都有單獨的 IAM user 跟 EC2.*權限，只有 Manager 的 IAM user 有所有的權限。

(CTO*1, EU-DevOps*1, MS-ADM*1, DEV*n)

Case-2

Fintech 公司，創業團隊。

從 Day 1就把所有的 workload 放上 AWS。使用 EC2,ECS,Lambda....等等。公司只有 CTO 跟 DevOps Lead 有 Root Account 的帳號密碼，DevOps Lead 有兩個 IAM user，分別用來管 Staging/Prod 的環境。

在安全方面使用了 KMS,ACM，另外還使用了自己開發的加密模組。公司的源代碼存儲用的是 gitlab，會使用 Codebuild，使用 S3+ansible 的方式來作 deploy。

因為覺得 cloudformation 太難，所以選擇使用 Terraform 來作佈署，但曾經遇到版本的問題，臨時採用手動的方式來修改 infra 的佈建。

App 層的 monitor 用免費的 newrelic。但是在 EC2, ECS 裡面的 Application Log 會隨著 instance/container 關閉而消失。

Developer 可以經由 DevOps 給的 pem 檔連到 AWS 的開發機上面做事情或跑 simulation。但是全公司用的 pem 檔好像都是同一個。

(CTO*1, DevOps Lead*1, DevOps*3, Dev*n)

Case-3

本地企業的數據團隊。

公司同時有地端機房、及 AWS。

數據團隊擁有自己的 AWS Root Account 由組長負責，每個資料科學家都有自己的 IAM User，每個人都有設定 MFA。地端機房歸其他團隊管，我們只負責收資料，另外還開了一台 tableau 來作輸出，給管理團隊看報表。

大家會隨自己的需求上去開 EMR cluster 作事情，也都有權限。沒有買任何的 RI 或是 spot instance。如果要 deploy 東西，都是各自負責自己的部分。

公司的 raw data 是從地端的機房往 AWS 走，目前是走 VPN 傳到 AWS 的。這些 raw data 可能是從金融體系或是廣告公司收到的 user behavior data，而且是帶有 user identity 的。

雖然公司很看重資料團隊，但是上個月的帳單爆量了三倍，還不知道發生什麼事，好像是馬克的機器跑完就一直放著沒關。