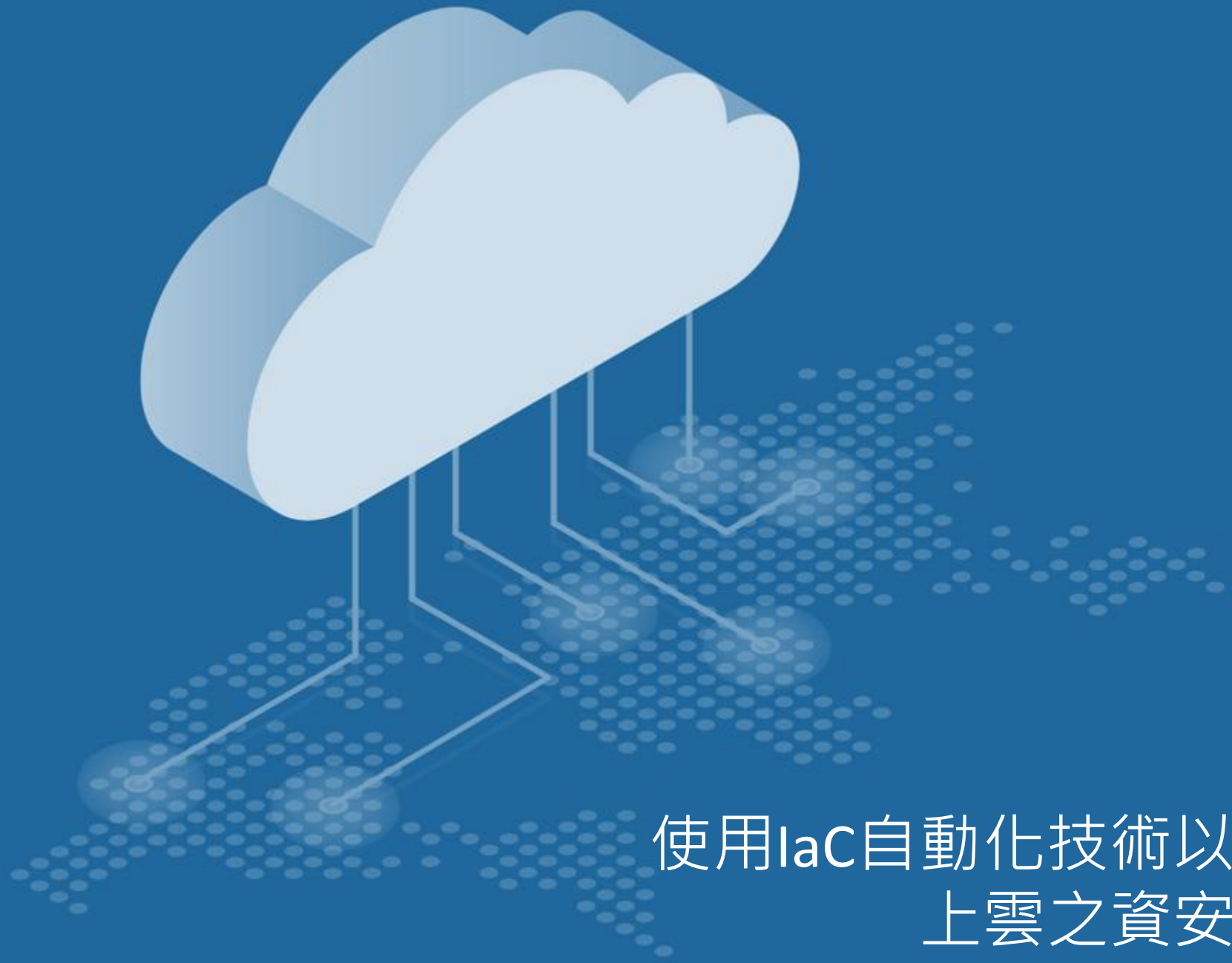
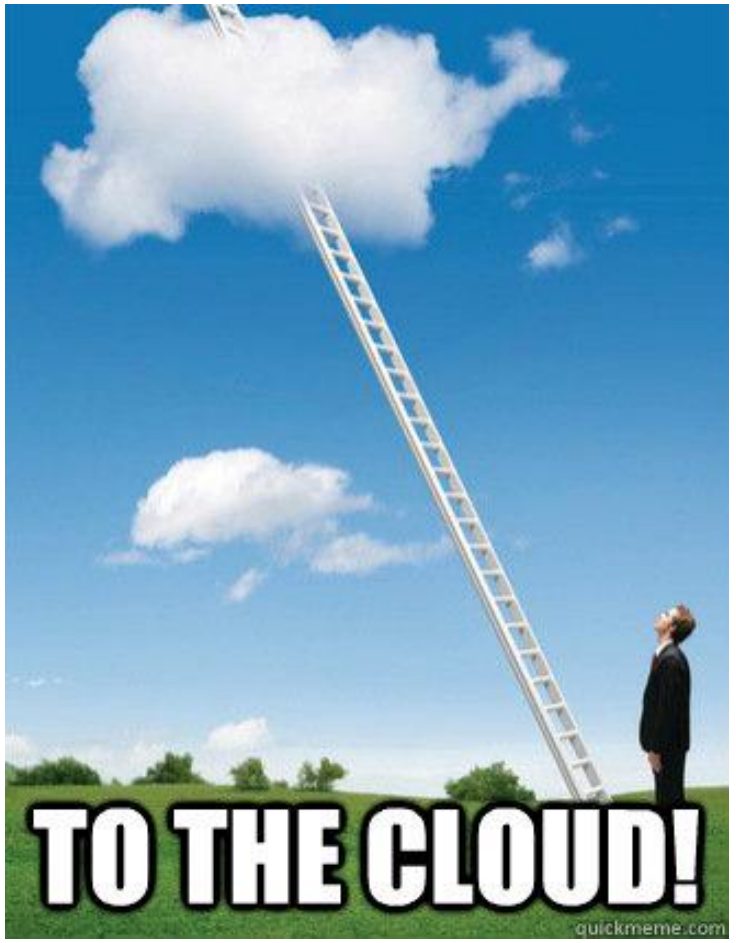


使用IaC自動化技術以符合金融業上雲之資安與合規要求

Agenda

- 金融業上雲資安與合規議題
- 雲端轉型面臨的新課題
- 為什麼導入IaC雲端自動化技術
- Why Policy as Code
- CloudFormation Guard v.s TF Sentinel
- Live Demo

應用系統上雲？不就是就在雲端上開個虛擬機再把程式放上去就好了



未考慮資安與合規，就別談金融業上雲

產物保險股份有限公司管理電子商務系統，核有違反保險法相關規定，爰依保險法第171條之1第4項規定核處罰鍰新臺幣(以下同)120萬元整，並依同法第149條第1項規定予以2項糾正

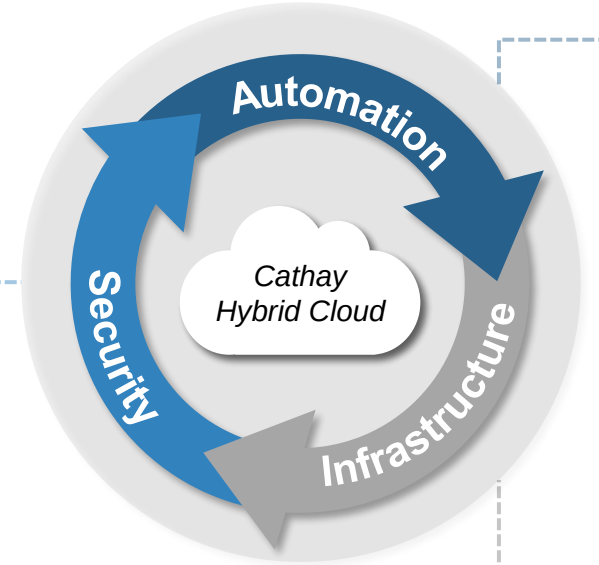
2021-06-09

一、裁罰時間：110年6月9日
二、受裁罰之對象：　　產物保險股份有限公司
三、裁罰之法令依據：保險法第149條第1項、第171條之1第4項
四、違反事實理由：
(一)該公司107年8月於資訊部門下增設資安專責單位，依法應配置適當人力資源及設備，負責規劃、監控及執行資訊安全管理作業，然當時僅配有1名資安人力，直至109年1月起始增加為2人，檢查發現系統弱點修補管控欠妥，防火牆規則設定審核欠落實，以及未建立重要日誌監控及告警機制等資安防護作業欠妥事項，顯示資安專責單位未能妥適行使職權及有效發揮監督功能，核有未落實執行保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第6條之1規定情事，依保險法第171條之1第4項規定，核處罰鍰新臺幣(下同)60萬元。
(二)該公司107年4月16日租用雲端基礎設施(IAAS)，運用　　，以雲端架構建置「　　投保系統」，查有未妥善訂定資料加密金鑰管理程序、未訂定妥適之緊急應變計畫及退場機制等情事，又辦理　　投保系統」之開發及維護作業，未受公司網路保護機制管控，主機系統日誌未納入資訊部門集中管控，與公司所訂內部規定不符。該公司雲端服務控管機制欠妥，未落實「保險業作業委託他人處理應注意事項」第7點規定，不利資訊安全及客戶權益之保護，核有違反保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第5條第1項第14款規定情事，爰依保險法第171條之1第4項規定，核處罰鍰60萬元。
(三)有關資安管理部分，有提報董事會之資安整體執行報告欠完整、對廠商交付之報告未確實檢核、未訂定重要性主機監控管理規範及系統修補程序、對主機帳號密碼管理欠妥、弱點掃描範圍欠完整等缺失，不利資訊安全防護，經核有礙健全經營之虞。
(四)辦理委外廠商管理部分，所訂委外開發人事系統合約，同意廠商遠端連線辦理維護，未妥為評估必要性及資安風險；另相關委外作業服務未訂定緊急應變計畫且辦理實地查核作業有欠確實等情事，經核有礙健全經營之虞。
五、裁罰結果：核處罰鍰120萬元整及2項糾正。
六、其他說明事項：保險業辦理電子商務，應確實建置或完備電子商務系統資訊安全管理規範及標準作業程序、配置適當人力並落實執行，俾利確保有效發揮資安維護管控功能。另委外作業應確實評估資安風險並妥為訂定緊急應變計畫，以維資訊安全及消費者權益之保護。

關鍵字：資料加密、金鑰管理、緊急應變計畫、退場機制、系統日誌集中管控、雲端服務控管機制...

雲端轉型將面臨很多新課題

我們透過雲端運算技術驅動數位轉型



資安面

資安/風險/合規性管理框架

- 避免身份存取控制管理失誤
- 依據數據類別調整加密方式
- 金鑰放置位置 (雲 or 地)
- Log 收攏責任歸屬問題
- DR 雲端演練方式…

自動化

雲端自動化部署

- 程式佈署 AP CI/CD
- 基礎服務佈署 IaC CI/CD…
- 顯示執行蹤跡並方便追溯
- 避免 console 人為操作失誤
- 不成熟流程導致風險增加

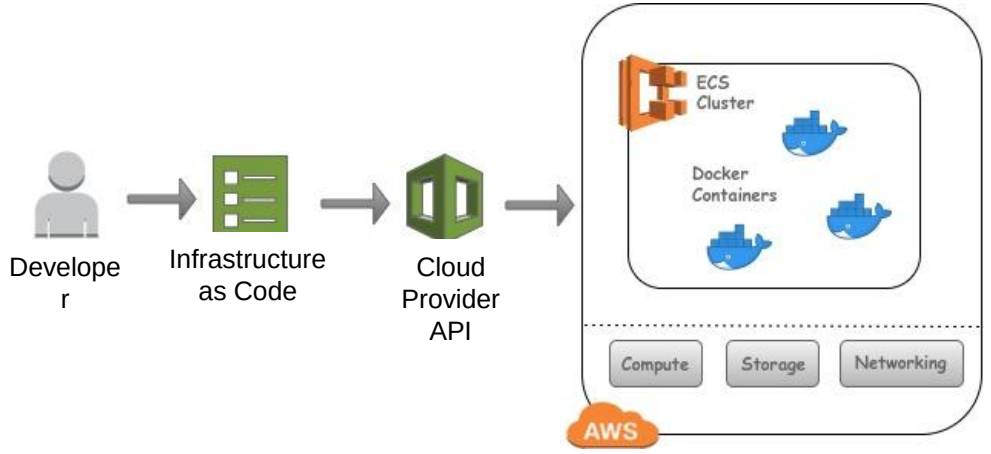
雲端架構

完善國泰混合雲環境

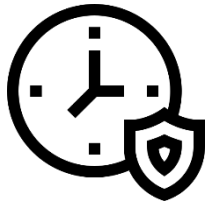
- 合適多雲管理工具
- 雲地間傳輸管道 (專線配置)
- 開發/正式環境隔離
- 流量進出控管避免資安攻擊…

Why IaC (infrastructure as code) ?

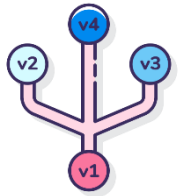
- IaC 為自動化的實現手段。
- 避免人直接操作 Web Console，防止 Key 外流問題。
- 增加額外的 Auto Policy Check 於管理、治理或資安檢核項。
- 快速簡單的建置複雜環境，減少直接操作偏差等人工錯誤。



使用IaC雲端自動化技術，有助於資安、合規、管理、治理等要求

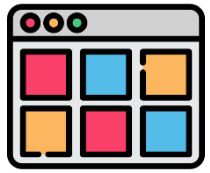


速度與安全性



可版本管理

環境一致

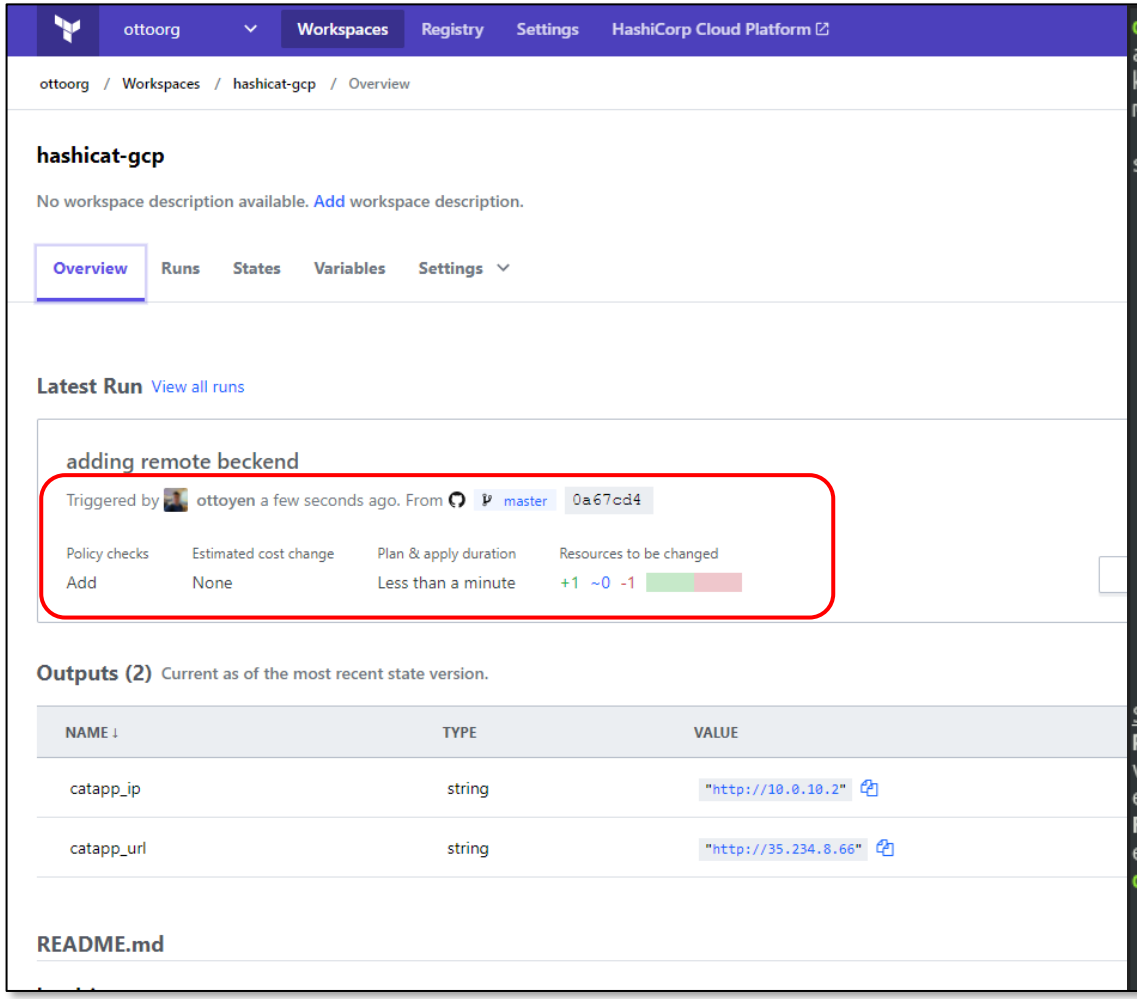


檢核作業面合規性

容易追蹤問題

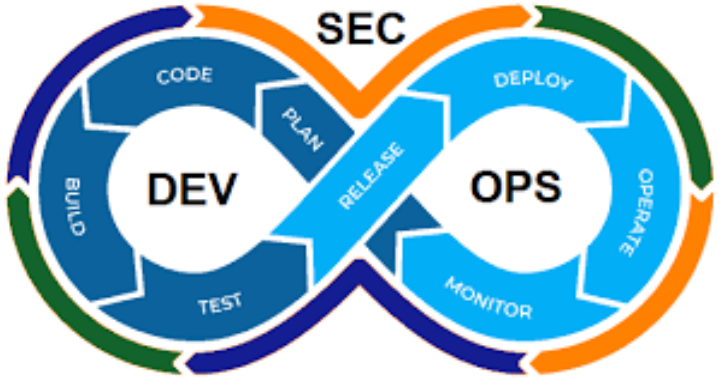
稽核與軌跡

我們使用Terraform、CloudFormation Guard解決各種資安與合規性問題




```
diwakar@uc78be0f83ba356:~/demo/kubernetes$ cfn-guard validate -r pod-containers.guard
apiVersion: v1
kind: Pod
metadata:
  name: frontend
spec:
  containers:
  - name: app
    image: images.my-company.example/app:v4
    resources:
      requests:
        memory: "64Mi"
        cpu: 0.25
      limits:
        memory: "128Mi"
        #cpu: 0.5
  - name: log-aggregator
    image: images.my-company.example/log-aggregator:v6
    resources:
      requests:
        memory: "64Mi"
        cpu: 0.25
      limits:
        memory: "128Mi"
        cpu: 0.75
Summary Report Overall File Status = FAIL
PASS/SKIP rules
version_and_kind_match                PASS
ensure_container_has_memory_limits    PASS
FAILED rules
ensure_container_has_cpu_limits       FAIL
diwakar@uc78be0f83ba356:~/demo/kubernetes$
```

Why Policy as Code



- Version Control
  - Easily determine if the policy has changed
- Automation
  - Integration with CI/CD provides visibility and control over cloud environments
- **Pre-check** (Test Before Deployment)
  - Prevention is better than cure

國泰於 Policy as Code 關注面向

- **Policy**
  - Limit region
  - Naming rule
- **Security**
  - Can’t assign public ip
  - Firewall source range
- **Compliance**
  - CIS benchmark
  - PCI DSS
- **Cost limit**
  - Limit machine type
  - Limit disk size

CloudFormation Guard v.s Sentinel

CloudFormation-Guard	Sentinel
Open source	Terraform Enterprise
Cloudformation, k8s, terraform (YAML-, JSON- formatted)	Terraform Provider (HCL)
Local file-based	Version Control System (github, gitlab…etc.)
Has policy unit test	Has policy unit test

Demo

- 以 Terraform 部署 AWS 為例，加入 Cloudforamtion Guard 檢查是否通過 policy check 並執行部署

Thank You