跨雲加密分持與雲原生安全治理實踐
2024經驗分享與未來展望

楊世鈺

114.4.17

大綱

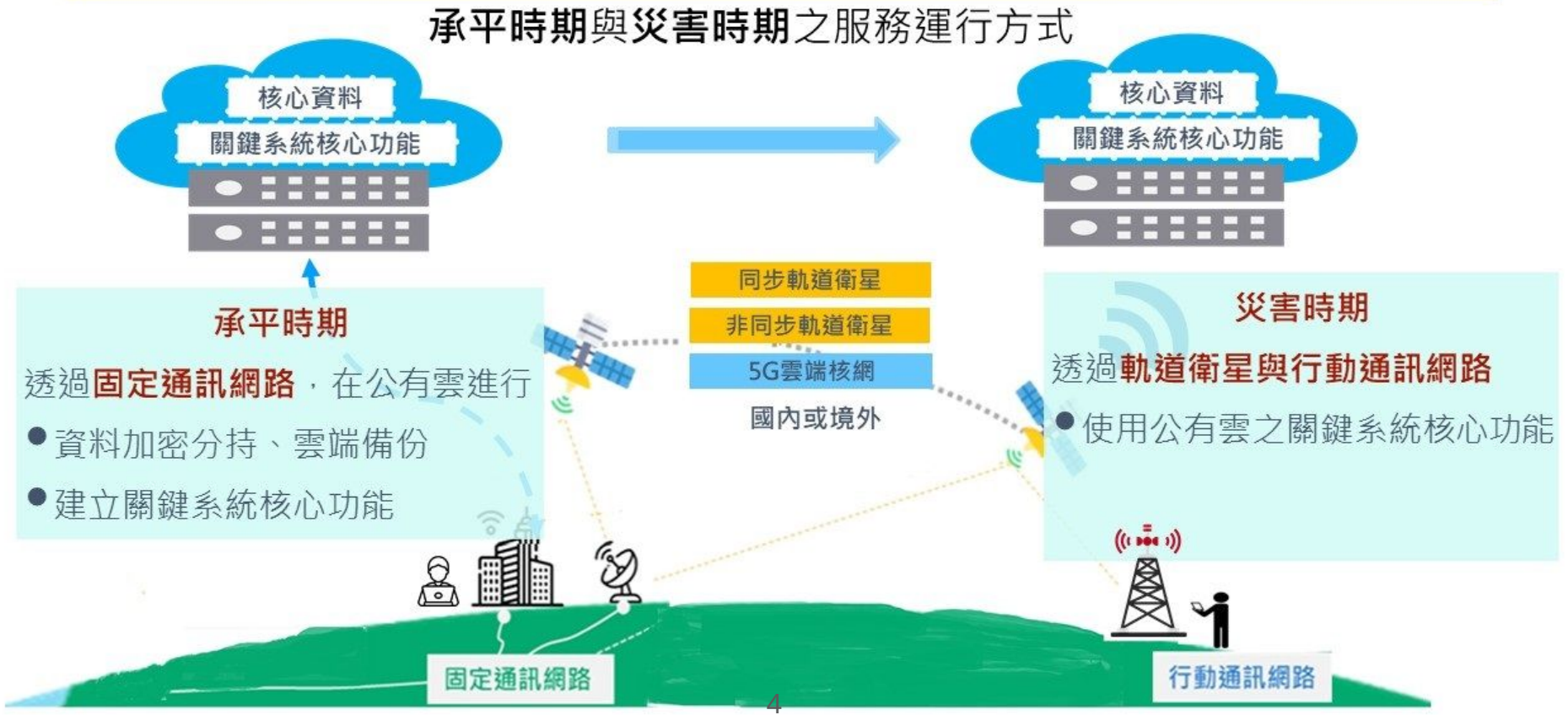
雲原生系統加密分持備份執行經驗分享

雲原生應用程式防護平台與雲端治理框架之後續展望

講者

- 2024 ~ 至今：數位發展部共通系統科分析師，負責擬定數位發展部資通系統整合部署安全策略與雲端治理及防護方案研擬
- 2022 ~ 2024：衛生福利部資訊處第一科分析師，負責醫療領域關鍵基礎設施資安技術業務
- 2019 ~ 2022：臺北市政府資訊局，負責北市府整體資安防護架構規劃業務

關鍵民生系統運作韌性推動策略



圖片來源：https://www.ey.gov.tw/Page/448DE008087A1971/741703a9-710b-40dd-9891-1c1bcb655e94

計畫重點與概述

	平時	災害時期	災後復原
目標	•維持系統可用性 •資料加密分持備份	• 保存關鍵民生系統與資料 • 維持系統核心功能與資料可用	• 迅速重建與回復服務

實施策略與方法

1. 盤點重要關鍵民生系統及災害時期應維持基本運作之系統核心功能
2. 採用跨境公有雲雲端儲存服務
3. 檔案、資料庫加密與分持儲存
4. 精進系統、資料庫備份與加密作業程序，提升機關自主操作能力
5. 系統核心功能模組化及導入零信任機制
6. 落實備份、回復與營運持續演練作業及教育訓練
7. 成立專業輔導團隊，協助技術諮詢

圖片來源：https://www.ey.gov.tw/Page/448DE008087A1971/741703a9-710b-40dd-9891-1c1bcb655e94

雲端不是銀行

Google Cloud出事了！**因系統錯誤配置，Google Cloud竟刪除澳洲退休金基金理財公司「UniSuper」的私有雲帳戶，導致50萬名用戶的退休金「一度消失」，差點損失逾1240億澳元（約2.65兆元台幣）的資產。**

透過<Google新聞> 追蹤風傳媒

綜合外媒報導，**澳洲退休基金Unisuper擁有61.5萬會員，負責管理超過1240億澳元（約2.7兆元台幣）的資產**，然而5月初卻**有用戶發現，無法正常登入網站及APP**，因此無法查看或存取自己的退休金帳戶。

用戶一度以為是UniSuper遭到駭客攻擊，不僅有個資外洩風險，更有可能失去退休金。沒想到經過查證才知道，原來是UniSuper使用的**Google Cloud系統出事，錯誤的組態設定導致他們刪光所有帳戶資訊**，甚至連備份資料都刪光。

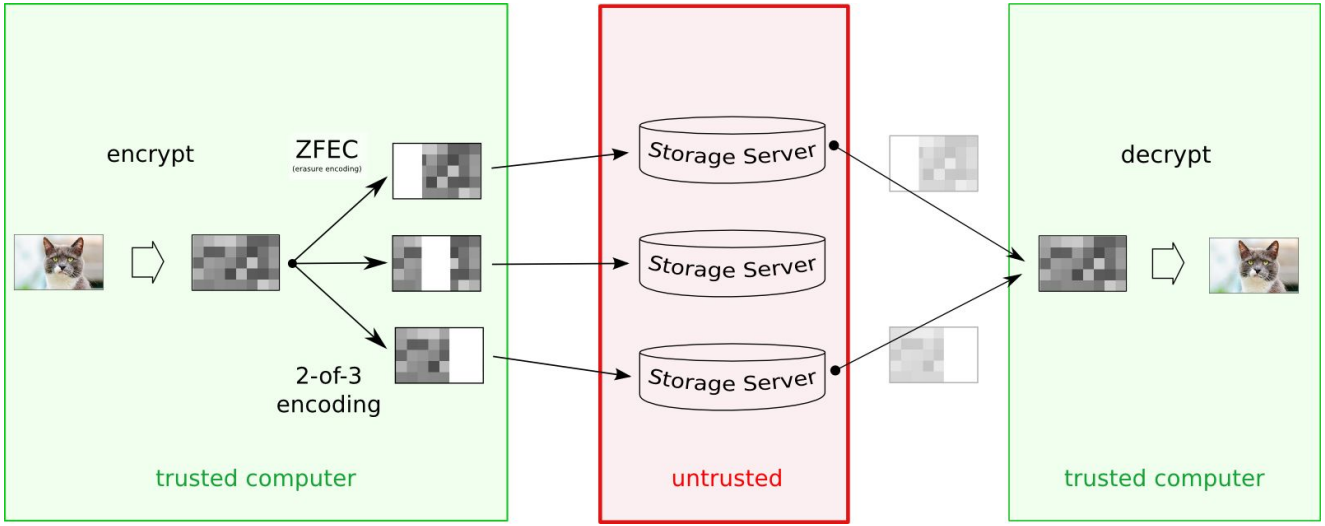
UniSuper執行長Peter Chun與Google Cloud執行長Thomas Kurian隨後發表共同聲明致歉，說明**是雲端服務出問題**，但強調並非遭到駭客攻擊，**沒有任何用戶的個資外洩**。（相關報導：弄丟信用卡「沒常識1行為」她被盜刷6.4萬！申訴銀行恐沒用…可能得認賠｜更多文章）

Google Cloud表示，過去他們從未發生過類似情況，「這不應該發生」，目前已經採取措施並全面檢討此事件，確保未來不會再有用戶受害或服務中斷的風險。

所幸，**UniSuper在另一家雲端服務供應商仍保有備份資訊**，在事件發生一周後，經過搶修已經逐步恢復用戶服務，目前已經可登錄網站及APP進行使用。

https://www.storm.mg/lifestyle/5123667

加密分持備份架構參考 - Tahoe LAFS

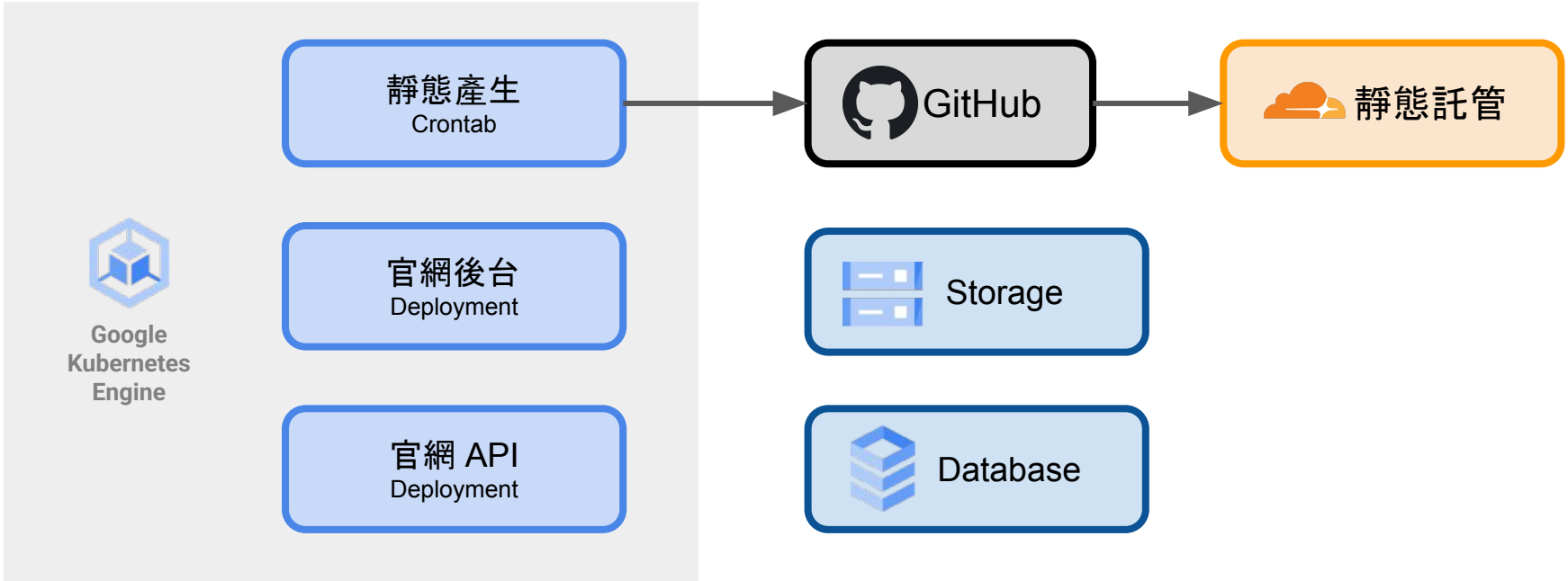


預設參數:
N=10(片段)
K=3(可復原最低片段數)
H=7(存放主機數)

最多可容許H-K=4台主機同時異常

圖片來源: https://blog.torproject.org/tor-heart-tahoe-lafs/

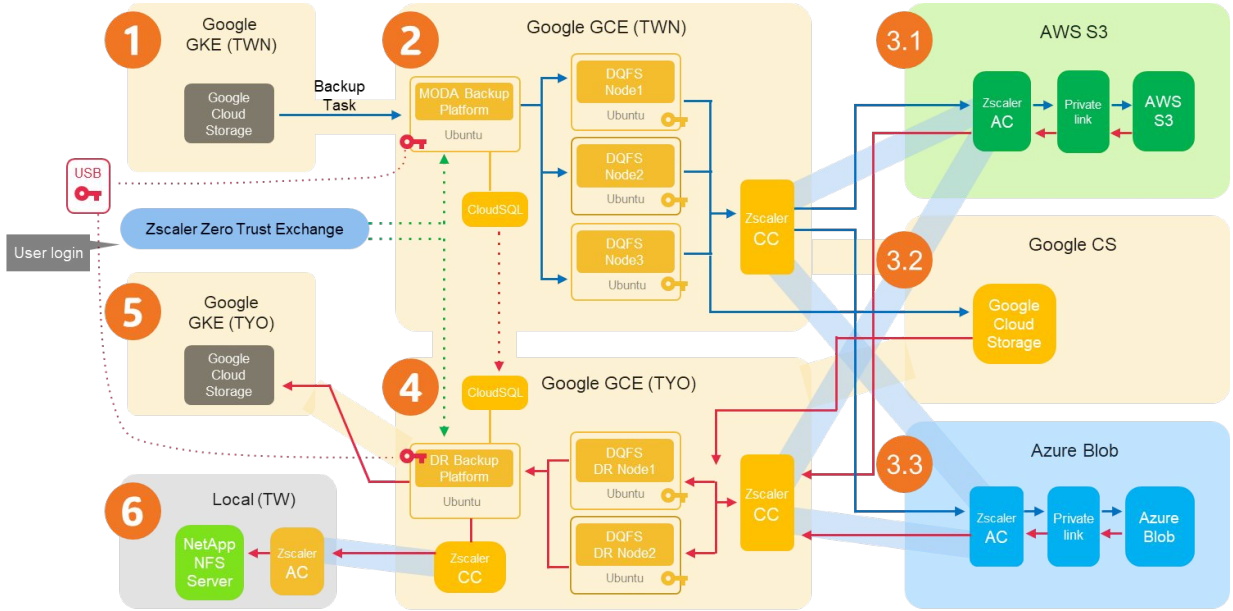
官網架構


靜態產生
Crontab
GitHub
靜態託管
官網後台
Deployment
Storage
官網 API
Deployment
Database
Google
Kubernetes
Engine

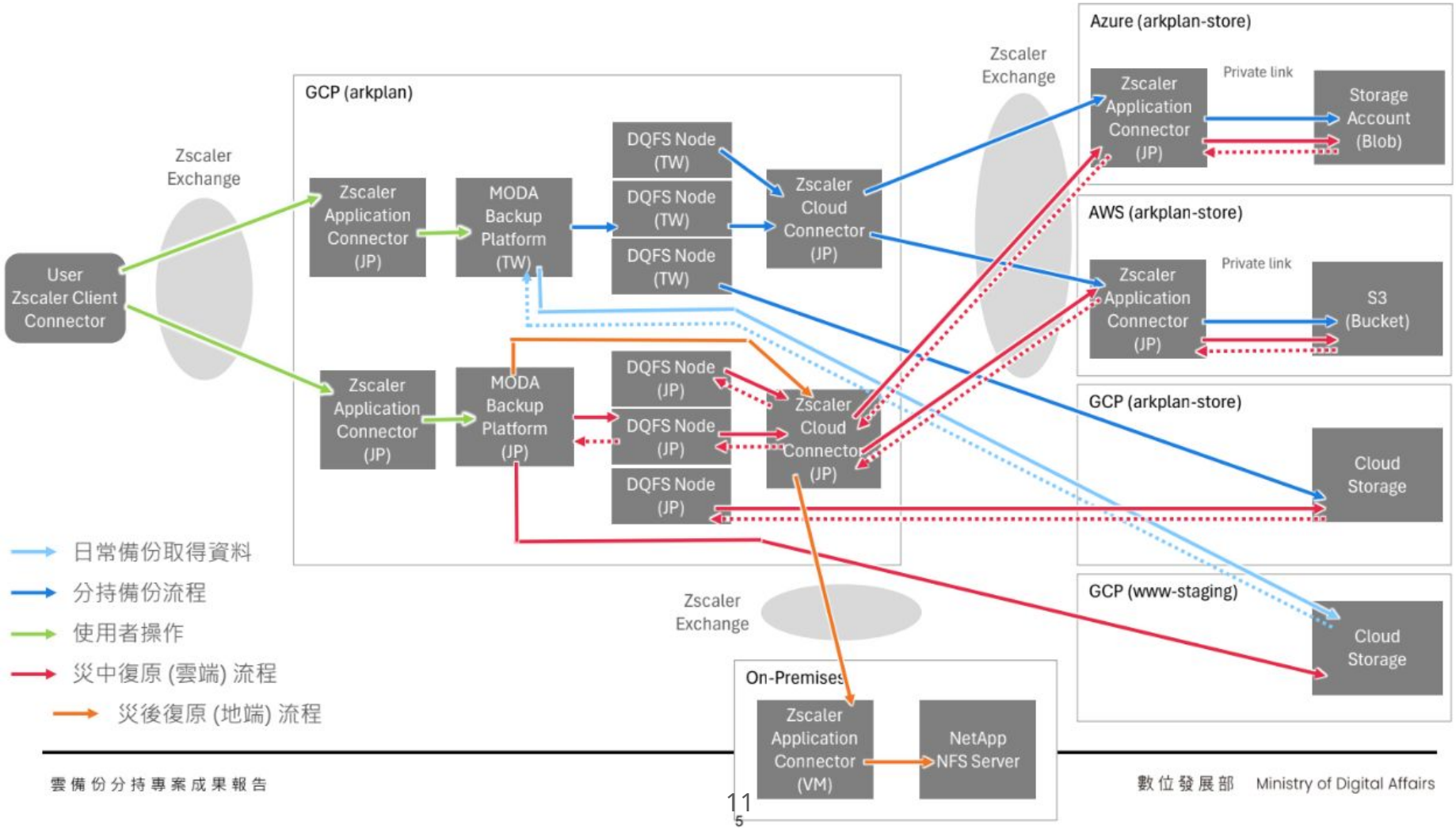
雲原生系統加密分持備份架構原則

1. 承平時期在台灣，災中時期在日本，災後時期回台灣
2. 需要備份的資料有 網站檔案(Filebase)與資料庫(CloudSQL)
3. 資料加密分持備份前不得 離境
4. 跨雲需要 SASE 並與 ZTA 整合
5. 使用三大公有雲(GCP , Azure , AWS)進行分持
6. 可用性可容許 一份毀損
7. 加密金鑰 可攜
8. 盡可能使用 DevOps Pipeline 執行所有步驟
9. 符合系統 RPO/RTO 要求
10. GitHub , Cloudflare , GCP GAR/GKE Autopilot , Azure DevOps Service 等均預設有多區域 (Multi-Region)可用性或 Pipeline 快速移轉機制

加密分持備份架構



本案完成架構包含 1 正式區(資料來源)、 2 分持作業區、 3 分持儲存區、 4 分持重建區、 5 雲端復原區(災中)、 6 地端復原區 (災後)，共六大區域


User
Zscaler Client
Connector
Zscaler
Exchange
GCP (arkplan)
Zscaler
Application
Connector
(JP)
MODA
Backup
Platform
(TW)
DQFS Node
(TW)
DQFS Node
(TW)
DQFS Node
(TW)
Zscaler
Cloud
Connector
(JP)
Zscaler
Application
Connector
(JP)
MODA
Backup
Platform
(JP)
DQFS Node
(JP)
DQFS Node
(JP)
DQFS Node
(JP)
Zscaler
Cloud
Connector
(JP)
Zscaler
Exchange
Azure (arkplan-store)
Zscaler
Application
Connector
(JP)
Private link
Storage
Account
(Blob)
AWS (arkplan-store)
Zscaler
Application
Connector
(JP)
Private link
S3
(Bucket)
GCP (arkplan-store)
Cloud
Storage
GCP (www-staging)
Cloud
Storage
Zscaler
Exchange
On-Premises
Zscaler
Application
Connector
(VM)
NetApp
NFS Server
日常備份取得資料
分持備份流程
使用者操作
災中復原 (雲端) 流程
災後復原 (地端) 流程

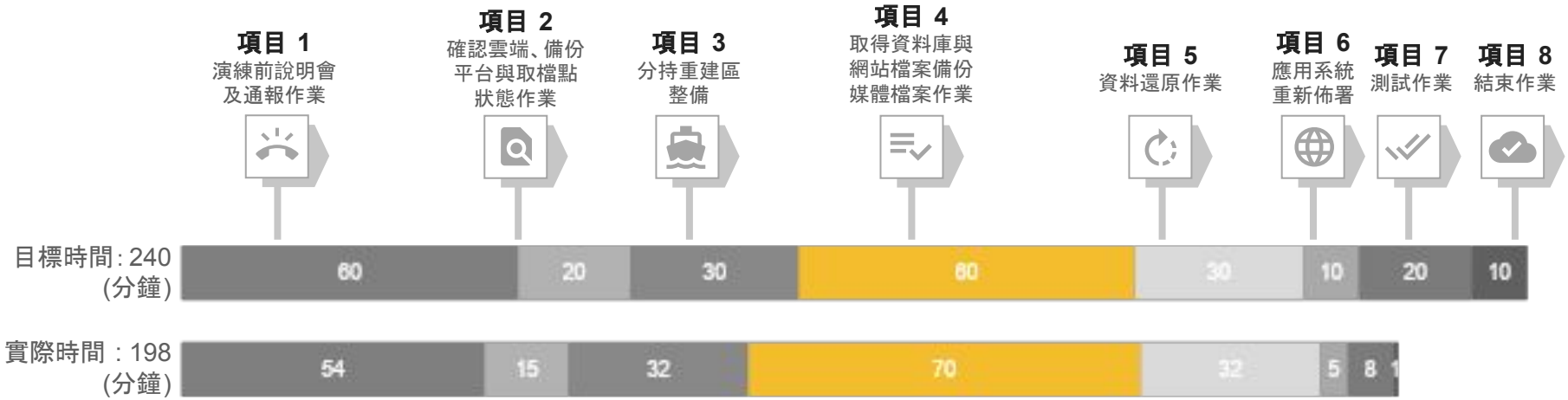
災中復原 (雲端) 演練計畫

演練日期	113.12.26
演練目標	最大可容忍中斷時間 (MTPD):8小時 復原時間目標 (RTO):4小時 復原點目標 (RPO):24小時
演練範圍	官網系統境內災害時期(災中)
演練情境與腳本	1.分持專案架構包含六大區域如下 ： 1.1. 官網正式區(資料來源) 1.2. 分持作業區 1.3. 分持儲存區 1.4. 分持重建區 1.5. 雲端復原區 (災中) 1.6. 地端復原區 (災後) 2.境內發生災難，造成正式區機房無法營運，有關人員立即依據部 內「資通與個資安全事件通報及應變處理作業管理程序書」即時通報危機應變小組等相關單位請求協助。 3.由危機應變小組依據事件情況研擬損害控制、復原作業及跡證保存計畫。 4.依照損害控制，計劃從境外雲端啟動雲端復原區，以及透過分持重建區取得分持儲存區其中二份資料回復運行，復原完成後須確認相關資訊系統作業是否正常，並持續監控與追蹤管制。

演練人員	1.分持備份資訊處承辦 2.Zscaler SASE維護廠商 3.分持備份系統維護廠商 4.分持雲端環境維護廠商 5.資訊處雲端組 SRE人員 6.官網承辦人與廠商
演練設備/設施/耗材	1.分持作業區設定檔 2.存有分持作業金鑰的 USB 3.數位發展部 Entra ID 資訊處群組使用者帳號 4.官網GCP CloudSQL 與Filestore 備份 5.備份平台 Cloud SQL備份
演練系統	官網系統、分持備份平台
其他資源項目	

災中復原 (雲端) 執行結果：符合計劃要求

- 目標時間: 4小時
- 實際時間: 3小時 18分鐘



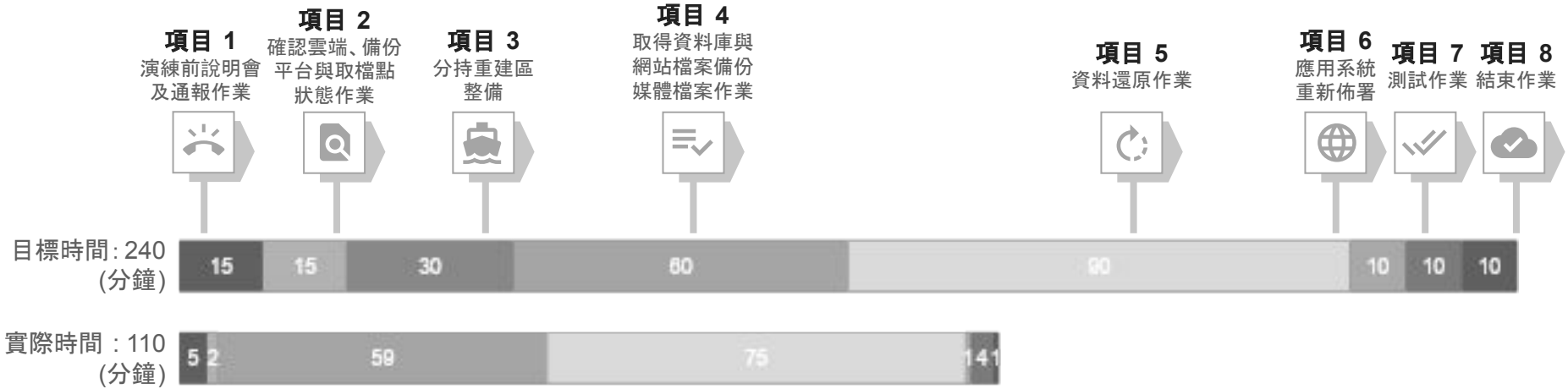
災後復原 (地端) 演練計畫

演練日期	113.12.26
演練目標	最大可容忍中斷時間 (MTPD):8小時 復原時間目標 (RTO):4小時 復原點目標 (RPO):24小時
演練範圍	官網系統災後復原境 內機房(災後)
演練情境與 腳本	1.分持專案架構包含六大區域如下 ： 1.1. 官網正式區 (資料來源) 1.2. 分持作業區 1.3. 分持儲存區 1.4. 分持重建區 1.5. 雲端復原區 (災中) 1.6. 地端復原區 (災後) 2.官網系統境 內災害時期 啟動營運持續作業，於境外建立官網系統服務，境內災害已確認排除，計劃建立地端回復區環境，透過分持重建區取得分持儲存區其中二份資料回復運行，復原完成後須確認相關資訊系統作業是否正常，並持續監控與追蹤管制。

演練人員	1.分持備份資訊處承辦 2.Zscaler SASE維護廠商 3.分持備份系統維護廠商 4.分持雲端環環維護廠商 5.資訊處雲端組 SRE人員 6.官網承辦人與廠商
演練設備/設施/耗材	1.分持作業區設定檔 2.存有分持作業金鑰的 USB 3.數位發展部 Entra ID 資訊處群組使用者帳號 4.官網GCP CloudSQL 與Filestore 備份 5.地端虛擬主機與 NetApp設備 6.備份平台 Cloud SQL備份
演練系統	官網系統、分持備份平台
其他資源項目	

災後復原 (地端) 執行結果：符合計劃要求

- 目標時間: 4小時
- 實際時間: 1小時 50分鐘



檢討與優化

1. 6GB 資料重組耗時1小時多
2. 碎片組合檔案欠缺完整性比對
3. 技術人力依賴，不夠簡單與自動化
4. 雲端維持費用高昂

1. 去重技術(De-duplication)導入
2. 多雲備份與金鑰分持取代資料加密分持
3. DevOps Pipeline 全程管線化
4. 排程或指令化開關、VM 容器化、使用雲端封存儲存與長期租用等方案降低成本
5. 進階方案：BYOK 金鑰管理方案

Storage Overhead = 6GB x (N/K) = 9MB，N=3 , K=2，N 越大空間占用更多
9GB x Deduple ratio = 0.9GB 至 2.7GB

因本案標的為官網等無敏感資料之分持備份，如為機密資料仍有資料分持之必要性

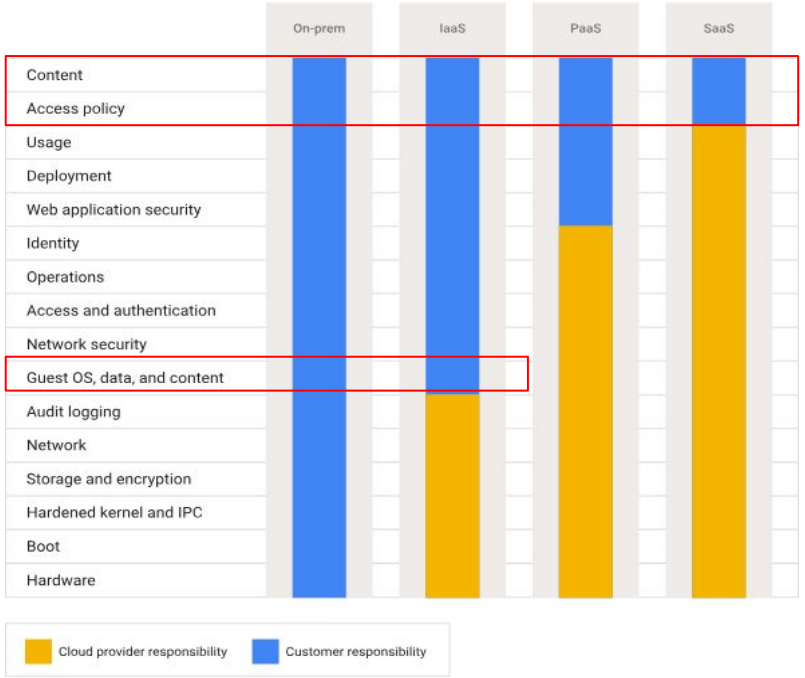
moda Cloud Platforms

雲原生架構管理議題

- 資安與合規
  - 政府組態基準(GCB)為主機基準，尚無雲原生服務之相關基準
  - 防毒軟體、端點偵測及應變機制於雲原生環境無法安裝
  - **傳統資通安全威脅偵測管理機制之資安監控於雲原生環境效果不佳**
  - 資安健診目前無雲端健診標準
- 雲端治理
  - 架構師人才流失
  - 多單位使用的管理問題
  - 雲端財務管理，節費節費再節費

雲端資安共同責任 (Shared Responsibility for Cloud Security)

依據各公有雲服務之資安共同責任，各類型之雲端服務仍需客戶自行負擔資安維護責任，而也有客戶無法插手的地方

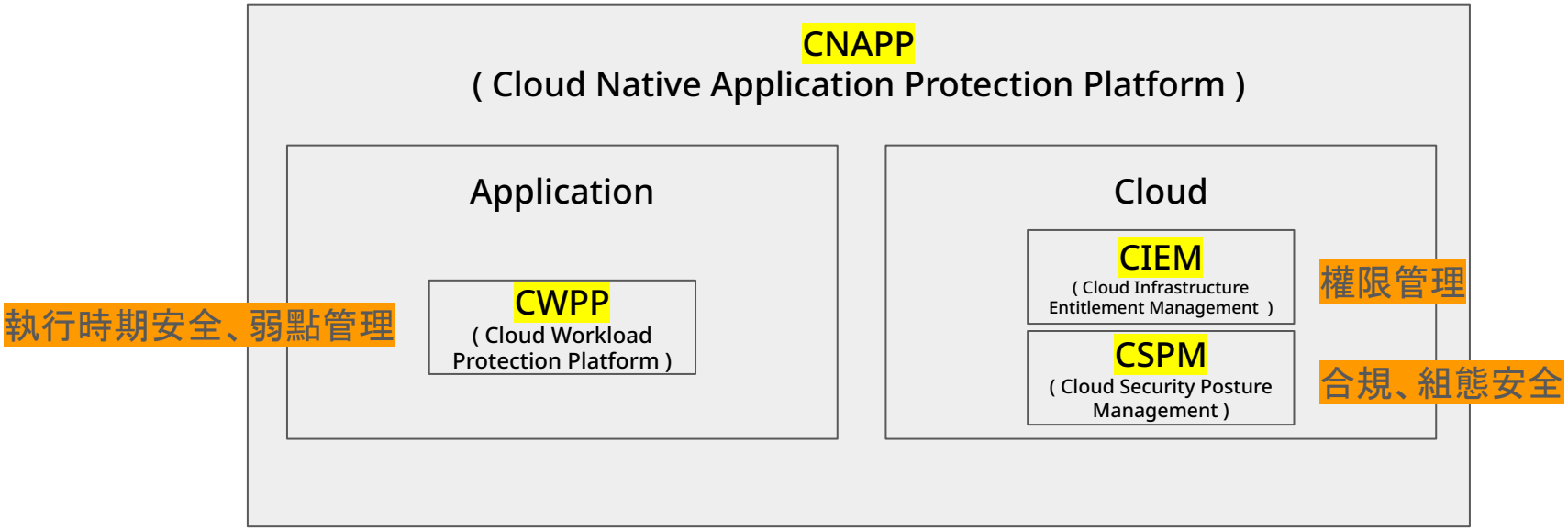


圖片來源：https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

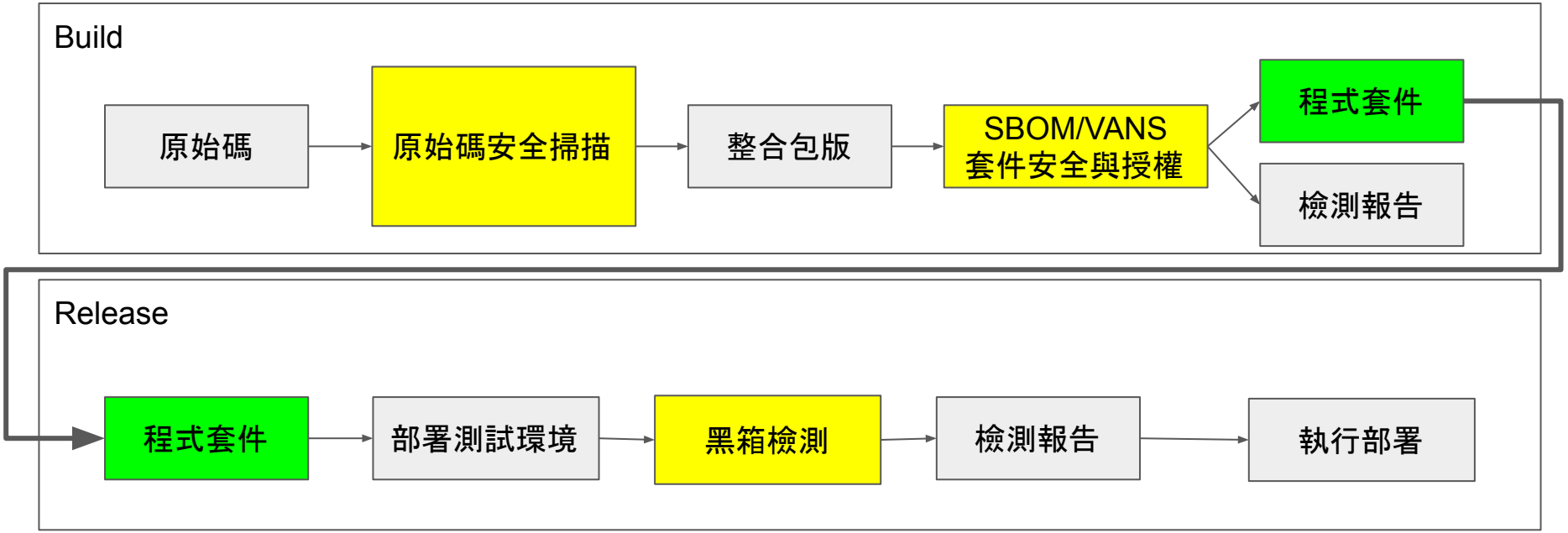
OWASP Cloud-Native Application Security TOP 10 (under review)

1. CNAS-1: Insecure cloud, container or orchestration configuration
2. CNAS-2: Injection flaws (app layer, cloud events, cloud services)
3. CNAS-3: Improper authentication & authorization
4. CNAS-4: CI/CD pipeline & software supply chain flaws
5. CNAS-5: Insecure secrets storage
6. CNAS-6: Over-permissive or insecure network policies
7. CNAS-7: Using components with known vulnerabilities
8. CNAS-8: Improper assets management
9. CNAS-9: Inadequate ‘compute’ resource quota limits
10. CNAS-10: Ineffective logging & monitoring (e.g. runtime activity)

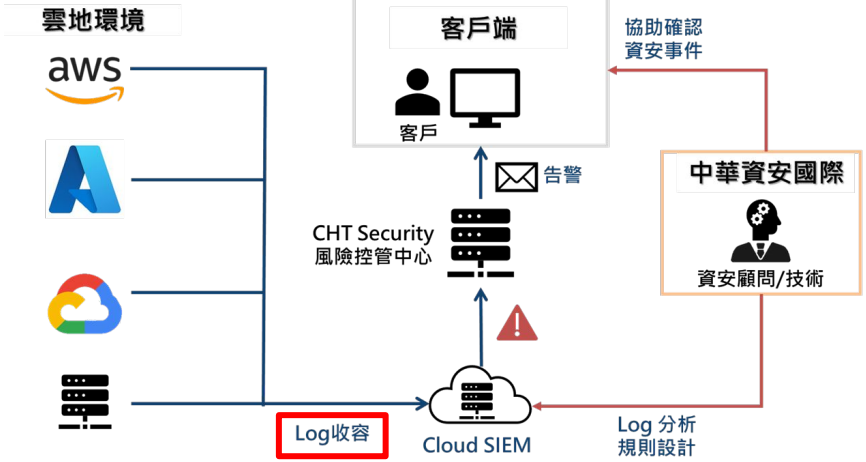
CNAPP (CWPP + CIEM + CSPM)



Shift Left Security



未來展望: Cloud SOC 議題 全落地 vs 雲歸雲 地歸地



https://www.chtsecurity.com/service/m803

回傳 Log 或回傳 Ticket
成本、正規化、合規

雲地聯防 最佳實踐
ACSI Cloud SOC

https://www.acercsi.com/tw/service/49/131

未來展望: Landing Zone/moda Cloud Shared Responsibility

- 身分權限架構集中(Microsoft Entra ID)
- 組織層級政策管理
- 帳務與成本管理(各司處/各專案)
- 網路架構(Hub and Spoke/Cloudflare DNS , CDN , WAF , Access)
- 日誌與監控
- 安全合規(ISO , CIS , TWGCB)

組織要與架構一致，架構要與組織一致

未來展望：moda 雲原生營運分工

資訊處

- 擬定政策
- 帳務管理
- 預算審查
- 申請審查

SRE

- 配置資源
- 配置帳號與權限
- 共同查看日誌與即時流量

開發編譯

- 上傳原始碼至 DevOps Repos
- CI 流程進行品質/資安檢查
- 持續修正與提交

部署營運

- 申請金鑰取得資源權限
- 撰寫 Pipeline IaC Code
- 執行 Staging/Production 部署
- 共同檢視營運狀況與排除

單位承辦

- 雲資源費用估算與預算編列
- 檢視履約廠商作業
- 審查批准 Production 部署

Thanks

moda

數位發展部

Ministry of Digital Affairs