如何面對雙十一的海量數據: 分析 TB 級日誌的實踐

徐靖翰 / Hans Hsu
Infra Team
Sr.Engineer

講師簡介

講師簡介

TECH - DAY

91APP Infra Team

- Sr. Engineer
  - 負責各種 AWS 相關解決方案
  - 分析公司內部服務的流量
- Open Source 專案的貢獻者
  - Moto: 用來 mock out 測試 AWS 服務的 Library
- 過去在擔任某雲端代理商的方案解決架構師

Agenda

TECH-DAY

- Introduction
- Challenge
- Compare Solutions
- Practice
- Summary

Introduction

我們想像中的 Log 能解決什麼問題

TECH-DAY

- 讓維運人員能即時了解，並確保應用程式正常的監控及警示
  - 維運人員想知道 HTTP Status Code 200 佔總請求數的比率，如果低於 90% 請寄封信通知
- 讓開發人員或維運人員可以做應用程式除錯 (debug)
  - 開發人員想知道開發的應用出現 Error 時寫出的 Log，藉此改善他開發的程式
- 讓開發人員或管理人員能知道公司的系統或商業狀況
  - 管理人員想知道這個月替客戶發的簡訊成功及失敗的數量，要跟客戶收多少錢
- 讓管理人員能知道公司的系統的合規性 (Compliance)
  - 管理人員想知道這個月有登入公司後台，修改客戶資料的員工有誰，以及改了什麼

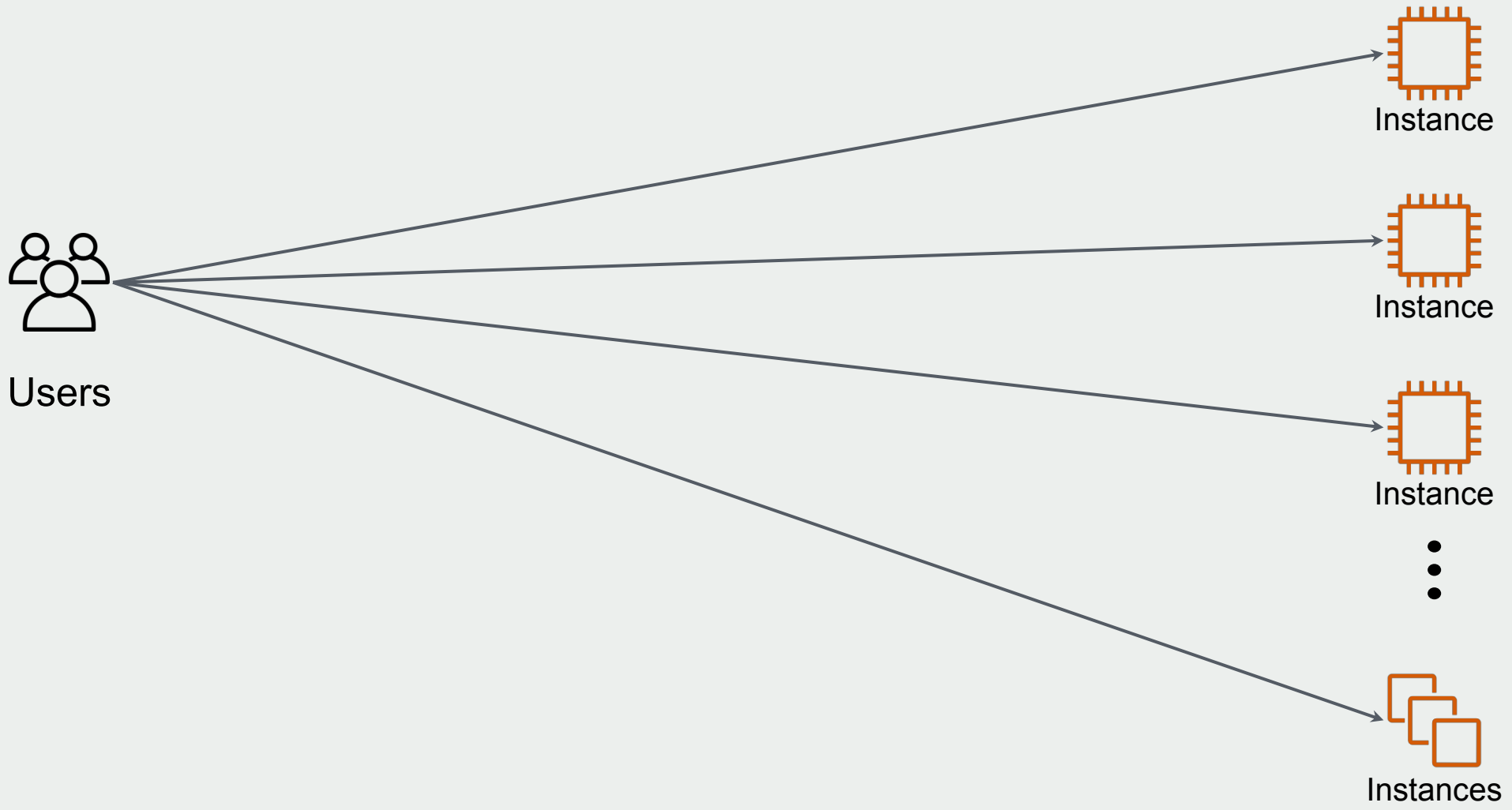
常常現實是

TECH-DAY

- 維運人員要進去每一台機器分析 Log 來確保應用程式正常的監控及警示
- 開發人員也要進去每一台機器分析 Log 來做應用程式除錯
- 管理人員~~命令~~請開發人員進每一台機器分析 Log，
  才能知道公司的系統或商業狀況
- 管理人員又要~~命令~~請開發人員進每一台機器分析 Log，
  才能確保公司的系統的合規性 (Compliance)

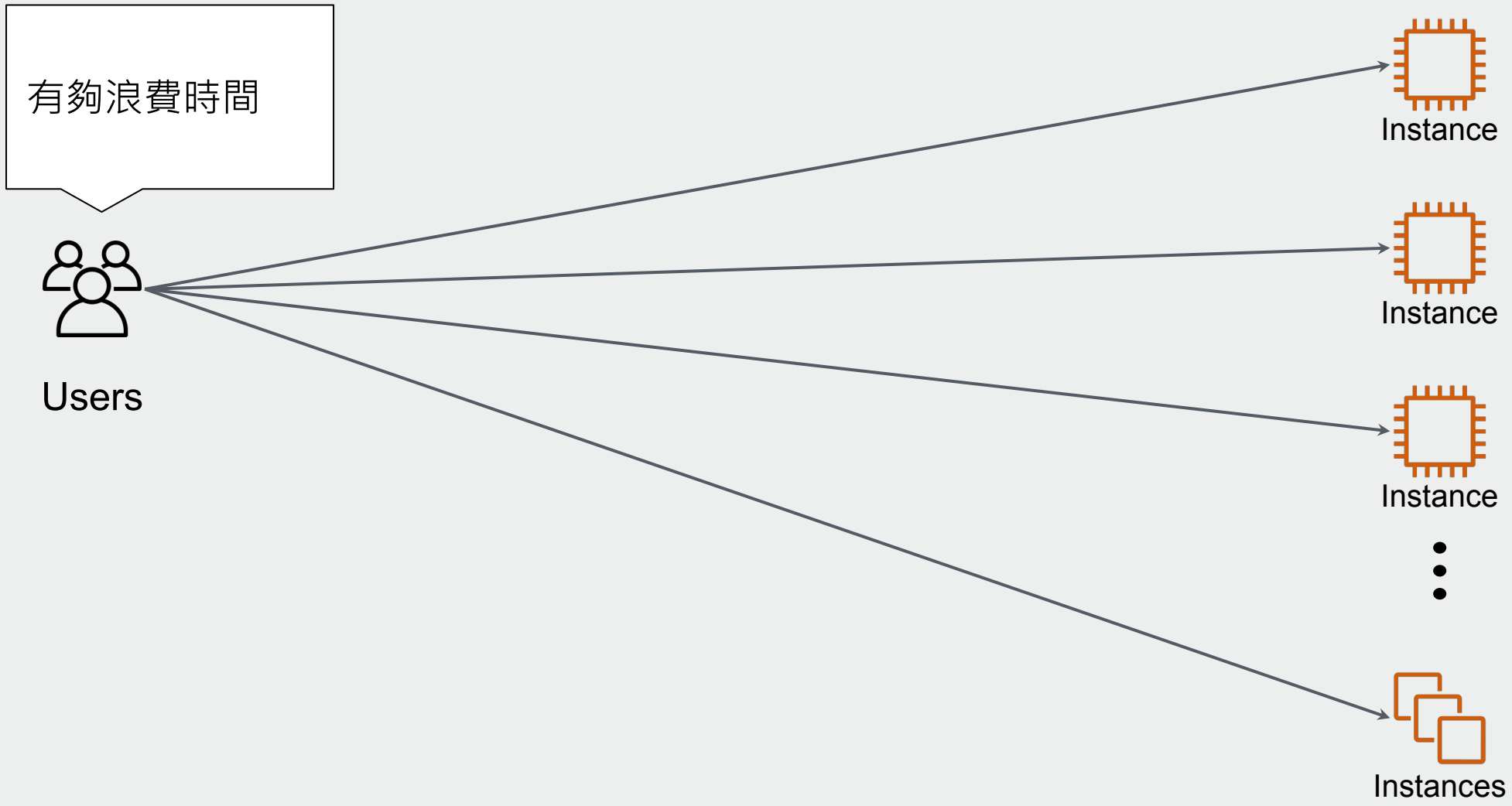
Analyze Log

TECH - DAY



Analyze Log

TECH - DAY



拆解需求 - 維運及開發人員

TECH - DAY

- 維運人員能即時了解，並確保應用程式正常的監控及警示 (alarm)
  - 監控 -> 指標 (metric)
  - 警示 -> 即時性 (near real-time 最小可在 1 分鐘)

- 開發人員或維運人員可以做應用除錯 (debug)
  - 應用除錯 -> 能夠搜尋及分析
  - 不需警示 -> 即時性 (near real-time 最小可在 1-2 分鐘)

拆解需求 - 管理人員

TECH - DAY

- 管理人員能知道公司的系統或商業狀況
  - 商業狀況 -> 報表
  - 即時性 (可接受 > 15 分鐘)

- 管理人員能知道公司的系統的合規性 (Compliance)
  - 合規性 -> 報表
  - 即時性 (可接受 > 15 分鐘)

Introduction - Summary

TECH-DAY

使用角色	應用場景	警示及指標功能	即時性	分析及搜尋
維運人員	維運人員能即時了解，並確保應用程式正常的監控及警示	是	大於或等於 1 分鐘，小於 2 分鐘	是
開發人員	開發人員或維運人員可以做應用除錯	否	大於或等於 1 分鐘，小於 2 分鐘	是
管理人員	管理人員能知道公司的系統或商業狀況	否	大於 15 分鐘，小於 24 小時	是
管理人員	管理人員能知道公司的系統的合規性	否	大於 15 分鐘，小於 24 小時	是

Introduction - Summary

TECH - DAY

- 需不需要警示及指標功能？
- 需要的即時性？
- 分析及搜尋

Introduction - Summary 根據 <自行帶入>

TECH-DAY

使用角色	應用場景	警示及指標功能	即時性	分析及搜尋
<自行帶入>	<自行帶入>	是	大於或等於 1分鐘， 小於 2 分鐘	是
<自行帶入>	<自行帶入>	否	大於或等於 1分鐘， 小於 2 分鐘	是
<自行帶入>	<自行帶入>	否	大於 15 分鐘， 小於 24 小時	是
<自行帶入>	<自行帶入>	否	大於 15 分鐘， 小於 24 小時	是

Challenge

General Challenge

TECH - DAY

- 組織
- 預算
- 技術組合
- 維運跟開發
- 使用機制

組織

TECH-DAY

- 政治正確永遠是最重要的事
  - 原本我覺得不是，但 ... 我錯惹
- 範例
  - 開發團隊 V.S. 維運團隊
  - 老闆不喜歡把 Agent 裝在 Server 上

    (*謎之音1: 那你是要怎麼收 Log? 謎之音2: 你不會登進去機器看?*)
  - ~~懶~~有更有~~老闆命令~~價值的事可以做

預算

TECH-DAY

- 預算政策
  - 採購或是財務團隊如何規劃預算
- 範例
  - 明天就要決定年度預算，然後你說你想起一個收集 Log 的新 Project ，要花大錢惹
  - 採購或是財務不懂你在幹嘛，所以拒絕採購

技術組合

TECH - DAY

- 技術組合 = 技術債 (Technology Stack = Technical Debt)

  我們只關心商業邏輯，Log？我不在乎 ~
- 範例
  - 根本沒有 Log 系統
  - 舊有的系統難以整合到現代化的 Log 系統

維運跟開發

TECH-DAY

- 維運複雜度
  - 越多元件增加，維運複雜度增加，維運的工作就變得更多
- 開發複雜度
  - 如果既有的 Log 收集管理解決方案缺少一些功能，
    就只好花時間開發

使用機制

TECH-DAY

- Log 的種類
- Log 的格式

- Log 的生命週期
- Log 如何送出

- Log 存在哪
- Log 怎麼存

- Log 怎麼分析

91APP Challenge

TECH - DAY

- 91APP 的系統該如何收集 Log
  - 300 以上的 VM + K8s workload 的 pods
  - 40 以上的服務
- 效能: 需要在短時間內 (< 1hour) 能搜尋及統計，能搜尋 > 1TB 以上的數據
- 權限: 要管理誰可以查 Log
- 成本: 要降低成本，理想上 1 USD / 每 GB 以內

Compare Solutions

Compare Solutions

TECH - DAY

- Log Producer (Agent)
- Log Consumer
- Log Storage
- Log Analytic Tool
- Cost

Log Producer (Agent) Example

TECH - DAY

- Fluentd
- Fluentbit
- CloudWatch Agent
- Kinesis Agent

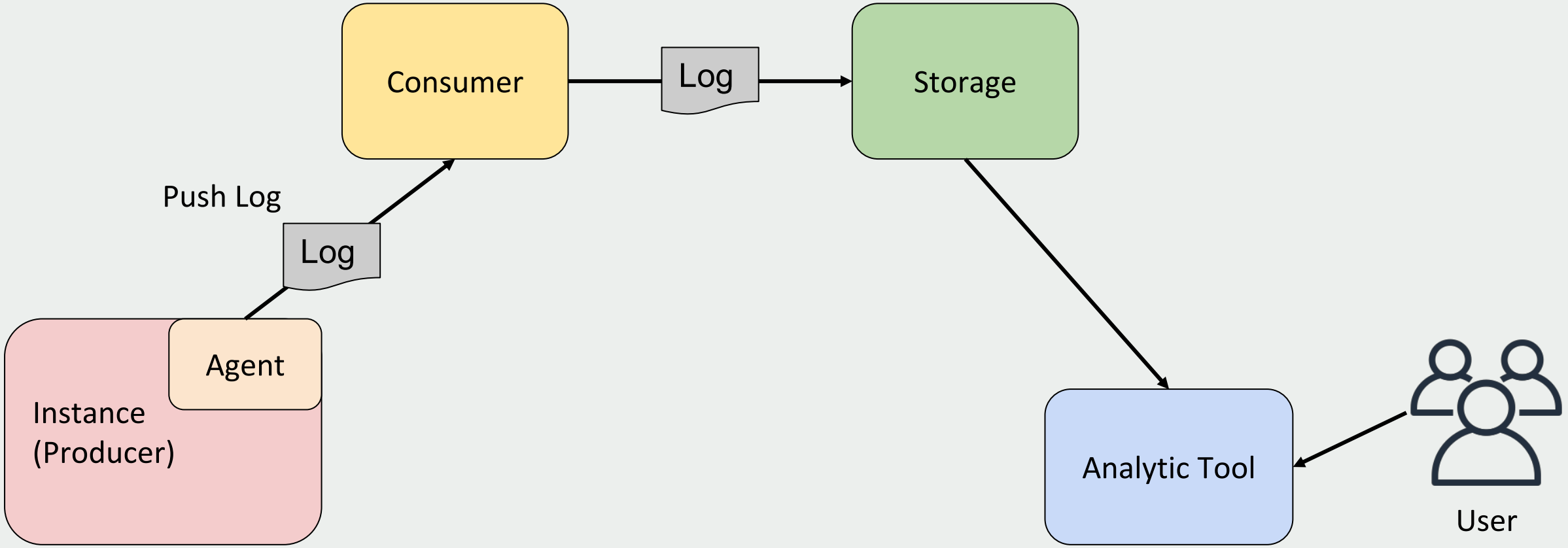
Log Role Example

TECH - DAY

- CloudWatch Log
  - Consumer + Storage + Log Analytic Tool
- Cloud Logging
  - Consumer + Storage
- Fluentd
  - Consumer
- Elasticsearch
  - Storage + Log Analytic Tool

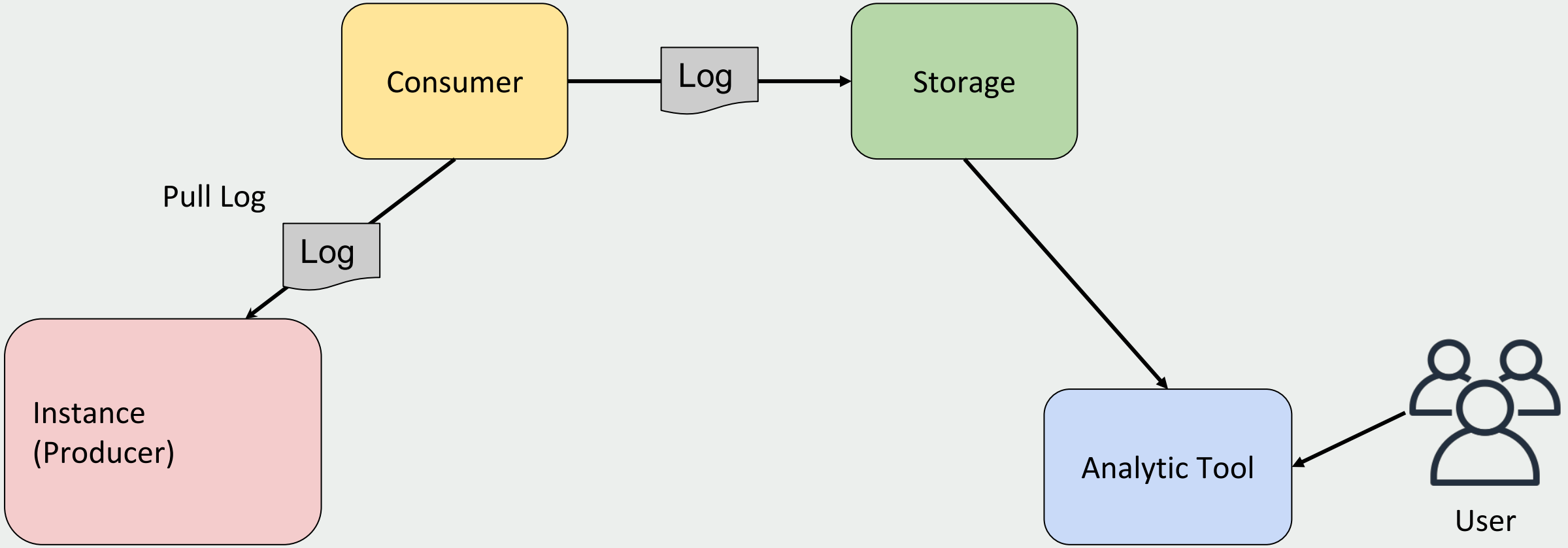
Log Solution General Architecture - Push Mode

TECH-DAY



Log Solution General Architecture - Pull Mode

TECH-DAY



假設需求

TECH-DAY

- 1 天 1 TB 的 Log
- 資料保留 30 天
- 自訂指標 1,000 個
- 伺服器主要在 AWS 上

TECH - DAY

解決方案	USD/每月每 GB	Total USD/月	服務費用 USD/月	AWS 對外傳輸費用 USD/月	人力小時/月	參考連結
Amazon CloudWatch + CloudWatch Log	0.79	24,332.74	24,232.74	0	10	連結
* Amazon CloudWatch + CloudWatch Log + Kinesis + S3 + Athena	0.35	10,644.16	10,444.16	0	20	連結
GCP Cloud Logging + Big Query + GCS	0.60	18,524.97	15,335.00	2,989.97	20	連結
** Azure Monitor	1.19	36,676.47	33,486.50	2,989.97	20	連結
Elasticsearch	0.63	19,264.62	18,864.62	0	40	連結

需求:
1 天 1 TB 的 Log
資料保留 30 天
自訂指標 1,000 個
伺服器主要在 AWS 上

* 此方案將 ⅓ 的 Log 送入 CloudWatch Log，⅔ 送入 S3

** Azure 的成本計算器連結可能失效

Practice

91APP Log Practice

TECH - DAY

- Log 的種類
  - 區分是否需要警示
- Log 的格式
  - jsonline + gz (溝通成本較低)
- Log 的生命週期
  - 按照公司規範設定 CloudWatch Log 或 S3

91APP Log Practice

TECH - DAY

- Log 如何送出
  - K8s: Fluentbit
  - VM: CloudWatch Agent 或 Kinesis Agent
- Log 存在哪
  - 要警示: CloudWatch Log
  - 不用警示: S3
- Log 怎麼存
  - CloudWatch Log: 不用管
  - S3: 按照日期存取 (YYYY/MM/DD)

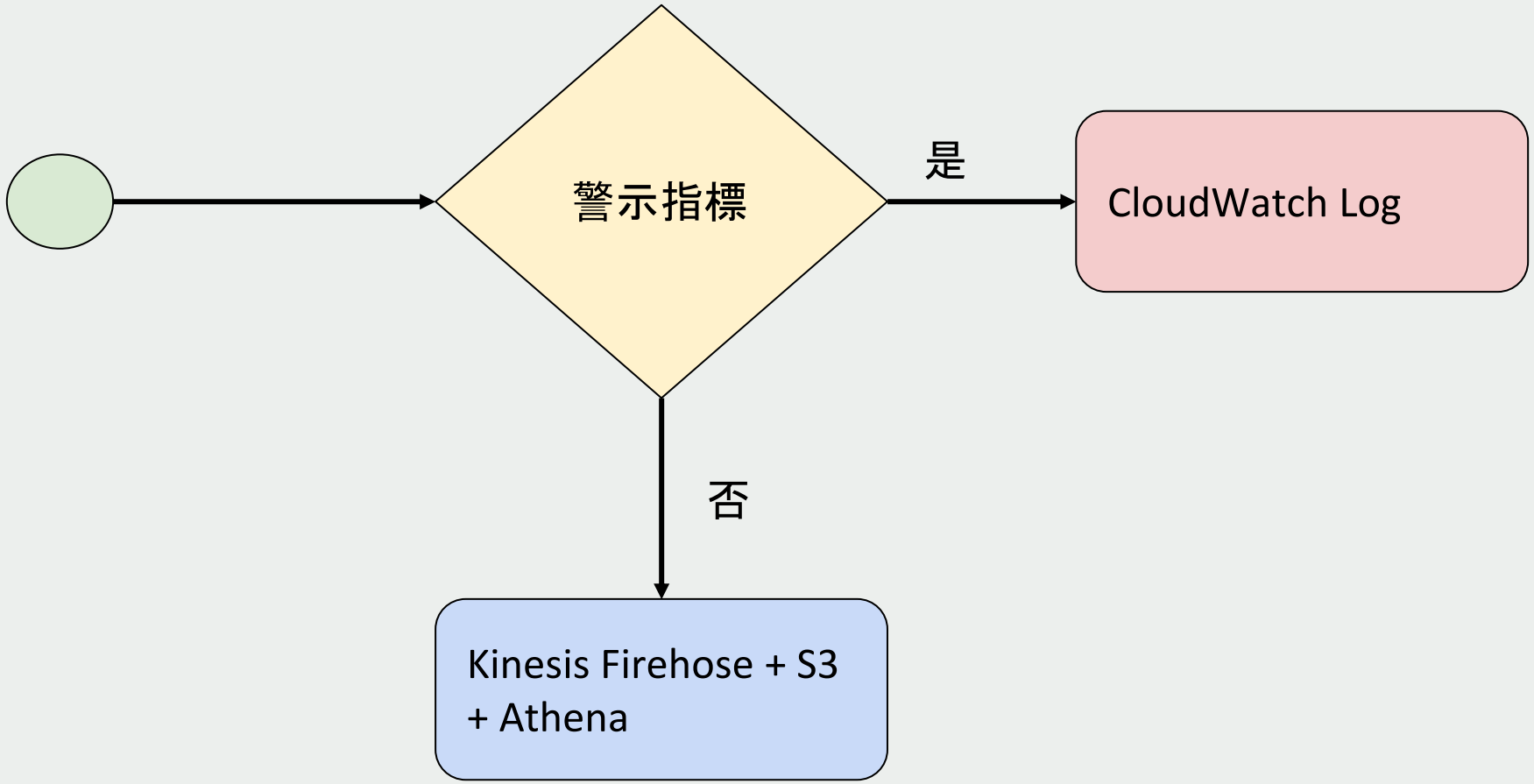
91APP Log Practice

TECH - DAY

- Log 怎麼分析
  - CloudWatch Log: CloudWatch Log Insight
  - S3: Athena

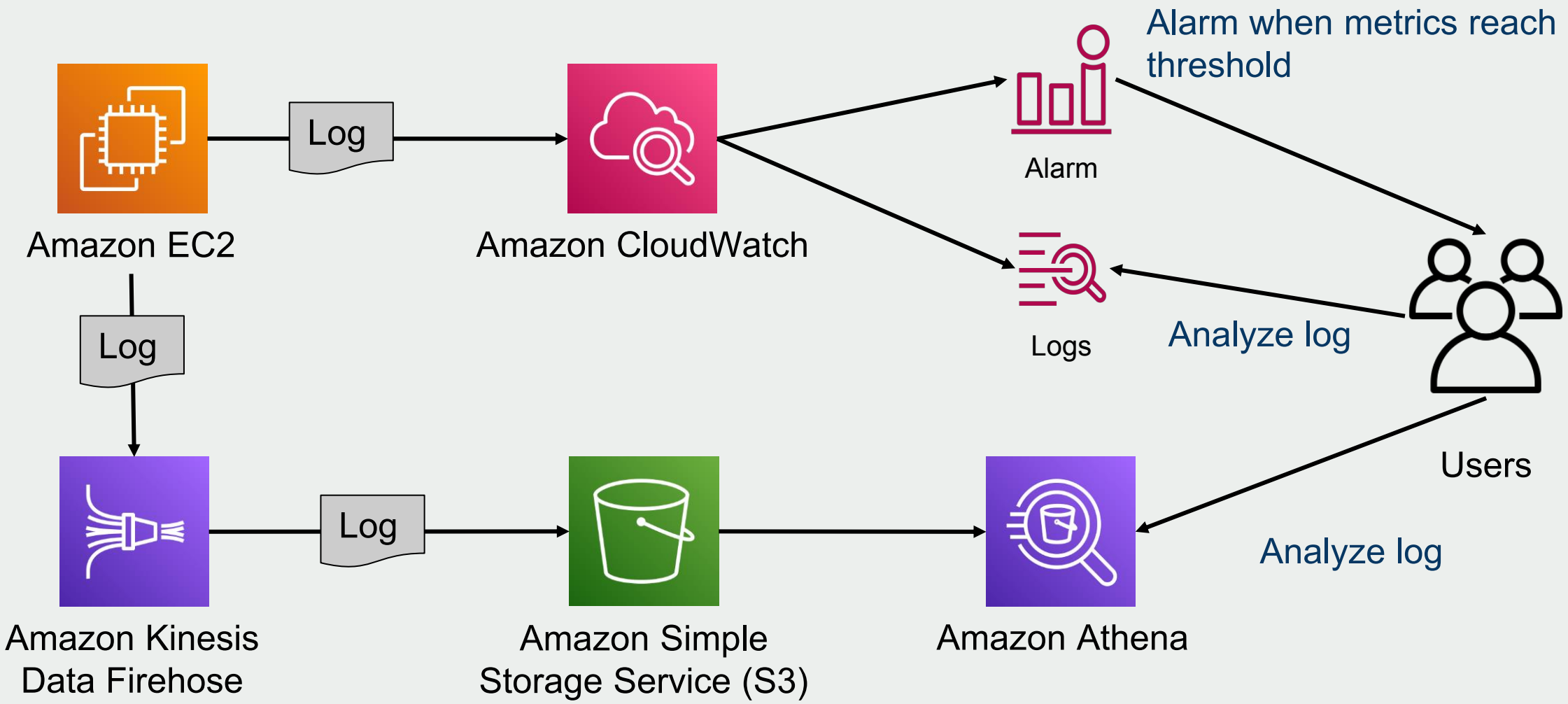
91APP Log Practice Decision

TECH - DAY



91APP Log Practice - Architecture

TECH - DAY



91APP Practice Result

TECH - DAY

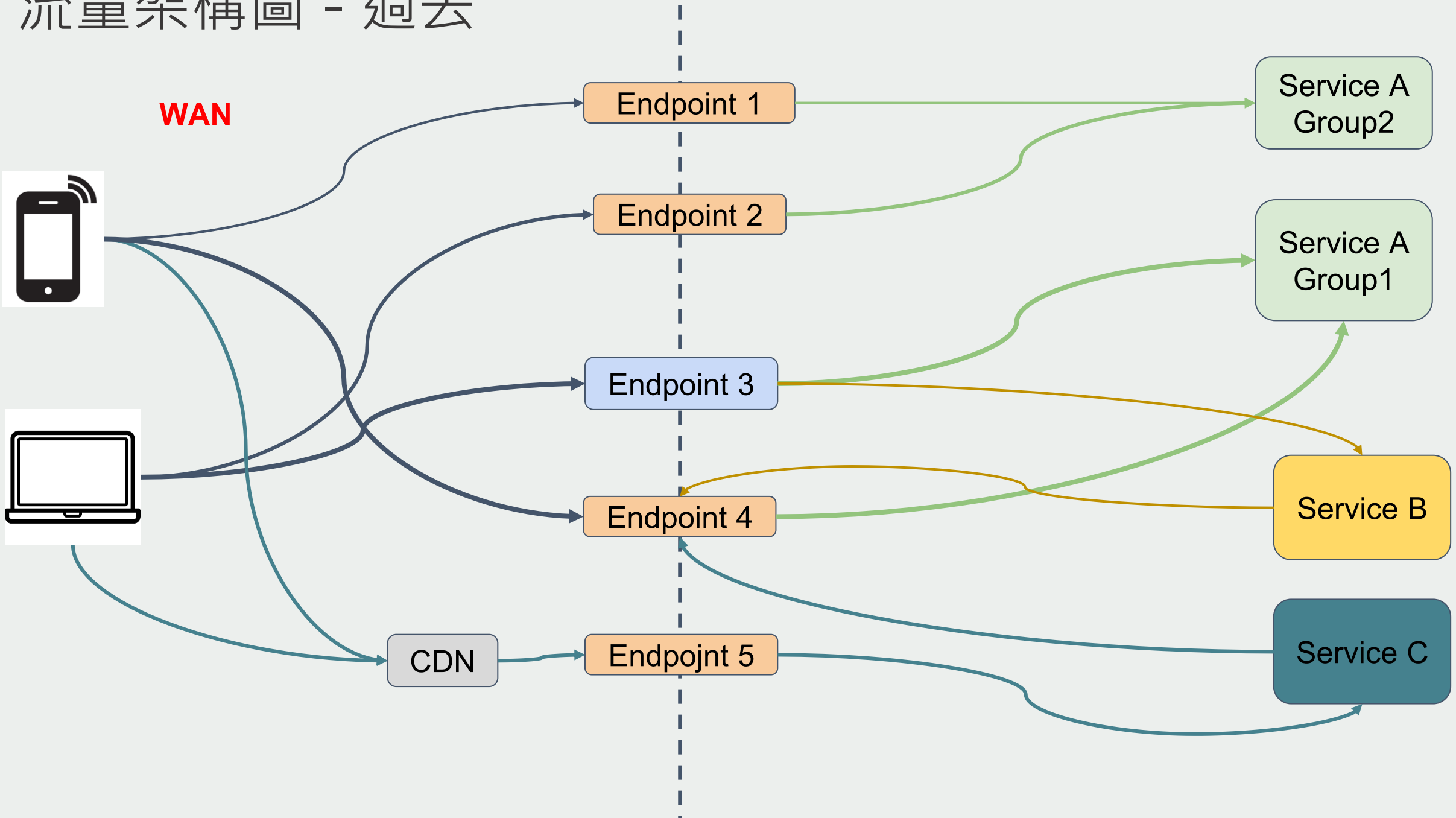
- 效能
  - CloudWatch Log 或 Athena 都能在短時間內 (< 1hour) 能搜尋及統計，能搜尋 > 1TB 以上的數據
- 權限
  - CloudWatch Log 或 Athena 都能利用 AWS IAM 限定權限
- 成本
  - 每 GB 約 0.35 USD / month

91APP Practice Result

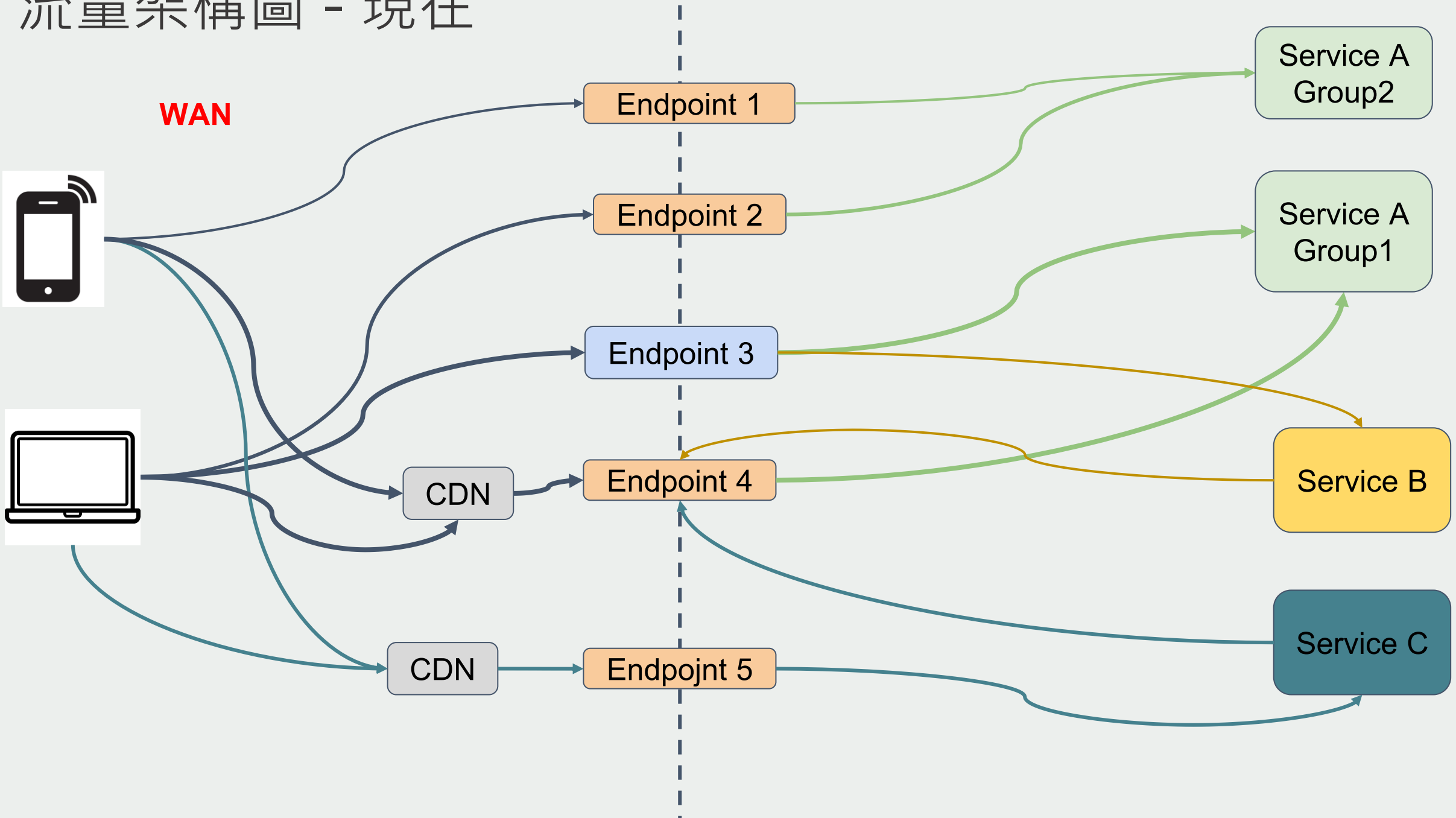
TECH - DAY

- 過去
  沒辦法分析服務之間的流量
- 現在
  可以分析快速分析 TB 級的數據，找到流量異常的部份
- 成效
  可以快速定位問題並修正架構，
  修正後對後端存取流量下降約 40%

流量架構圖 - 過去


WAN
Endpoint 1
Endpoint 2
Endpoint 3
Endpoint 4
Endpojnt 5
CDN
Service A
Group2
Service A
Group1
Service B
Service C

流量架構圖 - 現在


WAN
Endpoint 1
Endpoint 2
Endpoint 3
Endpoint 4
Endpojnt 5
CDN
CDN
Service A
Group2
Service A
Group1
Service B
Service C

Summary

Summary

TECH-DAY

- Log 的解決方案評估，按照這下面的方向來分析需求
  警示及指標、即時性、分析及搜尋
- 組織、預算、技術組合、維運跟開發、使用機制
  按照公司規模，用 量化的指標 來選擇適合的 Log 系統
- 評估有極限，建議評估評估 3 套 左右，在這之中做決定
- 成本 永遠是~~老闆~~重要的考量

Thanks for your listening.

謝謝你的聆聽。