



國泰金控

Cathay Financial Holdings

2023 國泰金控技術年會

混血共融 新智慧

與生成式 AI 共存 - 基於安全、可控、有效目標發展雲端 AI 知識顧問平台
國泰金控 顏勝豪 Otto Yen

AGENDA

第一章：Cathay 6R x 生成式 AI

第二章：安全的 SaaS

第三章：可控的 LLM

第四章：未來的 Multi-Cloud

<<<<

第一章

Cathay 6R x 生成式 AI

國泰雲端發展史

/ / / / / / / / /



國泰雲端策略發展史 2021-2022 : Cloud Ready

- Cloud Ready for 銀行 啟動
- Cathay 6R 方法論誕生

2021 H1



2021 H2

- 台灣雲端大會：上雲首部曲分享
- 國泰技術年會：跨界雲端新常態

- Cloud Ready for 人壽 啟動
- Cloud Ready for 產險 啟動

2022 H1



2022 H2

- Cloud Ready Phase 2 啟動
- 國泰技術年會：雲的多重宇宙
- 台灣雲端大會：上雲二部曲分享



- ChatGPT 全球爆紅



國泰從 2021 開始雲端轉型，累積了大量雲端經驗與知識，甚至能對外輸出至各技術研討會，而 2022 年底正好碰上 ChatGPT 在全球爆紅



國泰雲端策略發展史 2022-2023 : Cloud War Room

- 雲端策略發展部正式成立
- 銀行上雲戰情室

- Cloud Ready for 證券 啟動
- 台灣資安大會：上雲三部曲分享

2022 H2

2023 Q2

2023 Q4

2023 Q1

2023 Q3

- 人壽上雲戰情室
- 國泰資訊資產平台 啟動
- 雲端資安檢測 CGuard 啟動
- 雲端遷移評估 CCMA 2.0 啟動

- 金融業委外法規放寬，正式進入大規模上雲時期
- Cloud Ready Platform 啟動
- 國泰技術年會：與生成式AI共存



隨著大規模上雲需求出現，雲端策略發展部正式成立，便開始自研自建許多平台，也開始思考如何結合 **GAI** 來提供自動化服務，於是誕生了「雲端顧問 Chatbot」的點子



對，我們想得很簡單，就是一個可以回答任何雲端問題的 Chatbot。

而且要知道什麼是 Cathay 6R！

雲端顧問即時諮詢



Carol Chen 你好，我是雲端AI顧問，為幫助大家上雲之路可以更快解惑而生，你可以問我任何有關雲端技術的問題。我會針對你的問題提出分析與方案。



什麼是 Cathay 6R? 並舉例說明



Cathay 6R 是國泰金控自建的雲端遷移方法論，包含 Rehost、Re-platform、Refactor、Rewrite、Replace 和 Retain 六種遷移架構，並能對應到 IaaS、PaaS、SaaS 三種不同上雲模式。

1. Rehost：也稱為 lift and shift，將本地 VM 直接遷移到雲端，不需改動程式，對應到的上雲模式是 IaaS。
例如：將本地的資料庫系統直接遷移到雲端的 VM 上。
2. Re-platform：對應用服務本身進行 cloud-native 改動，部分服務改為使用雲端託管服務，或將應用程式容器化，對應到的上雲模式是 IaaS 或 PaaS。
例如：將本地的資料庫系統改為使用雲端的 SQL 服務。
3. Refactor：低度應用程式調整，使系統達到上雲最適狀態，如前後端分離或改用較現代化的程式框架，對應到的上雲模式是 IaaS 或 PaaS。
例如：將本地的資料庫系統改為使用雲端的 SQL 服務，並將應用程式容器化。
4. Rewrite：對系統進行大幅度的改寫，轉為 Cloud Native 架構，對應到的上雲模式是 PaaS 或 SaaS。
例如：將本地的資料庫系統改為使用雲端的 SQL 服務，並將應用程式改寫為微服務架構。
5. Replace：全面改以 SaaS 服務型態進行上雲。
例如：將本地的郵件系統改為使用雲端的郵件服務。

輸入你想知道的事



<<<<

第二章

安全的 SaaS

Network, Data, Management

/ / / / / / / / /

ChatGPT 資安相關事件，其實是發生在公開的網頁版



三星解禁員工用 ChatGPT 機密資料就遭外洩

Samsung 員工在使用 ChatGPT 查詢問題並驗證答案時，不慎將這些資訊加入到 ChatGPT 的學習資料庫中。若其他使用者在 ChatGPT 上提出相關問題，可能導致 Samsung 企業機密外洩。



ChatGPT 也將你的信用卡 資訊也暴露了嗎？

OpenAI 指出 redis-py 開源資料庫中一個 bug 造成了快取問題，可能會向一些活躍用戶顯示其他用戶的信用卡末 4 碼、到期日期、用戶姓名、電子郵件地址、付款地址，且可能看到其他人的聊天紀錄片段。



因涉違隱私法 義大利封鎖 ChatGPT 限20天改善

義大利隱私保護監管機構表示，ChatGPT 不重視用戶資料，涉嫌違反私隱法，而且無法核實用戶年齡，因此下令暫時禁用 ChatGPT、暫時限制 OpenAI 處理義大利用戶資料，並展開調查。

我們要打造的 Chatbot，則是使用雲端 SaaS，
三大公有雲皆有推出自己的 GAI 服務



Azure 強勢結盟 OpenAI

GPT 3.5 / GPT 4



GCP 自行研發 Vertex AI

PaLM 2

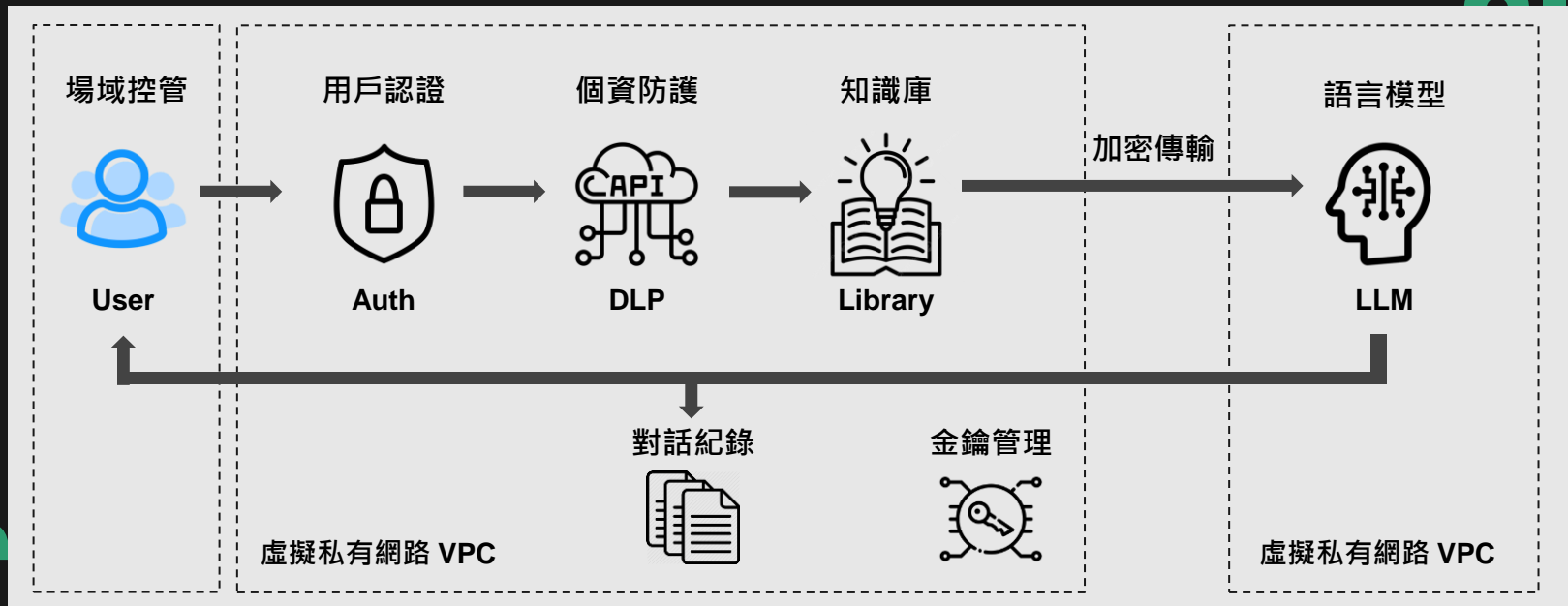


**AWS Bedrock
結合多種第三方模型**

Claude 2 / Jurassic-2

我們也在一開始就把安全做到位：

虛擬私網、加密傳輸、權限控管、軌跡紀錄、資料防護、金鑰管理



<<<<

第三章

可控的 LLM

Prompt, Vectorstore, Knowledge

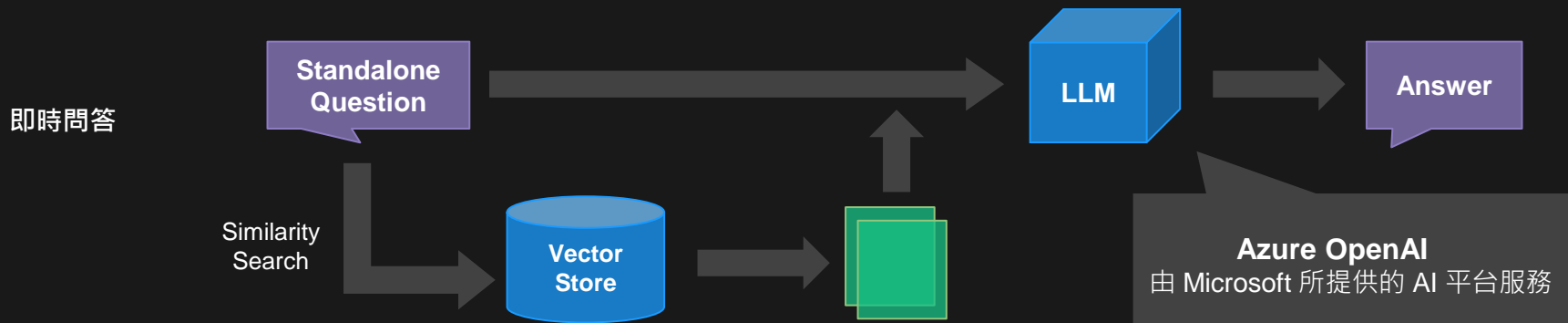
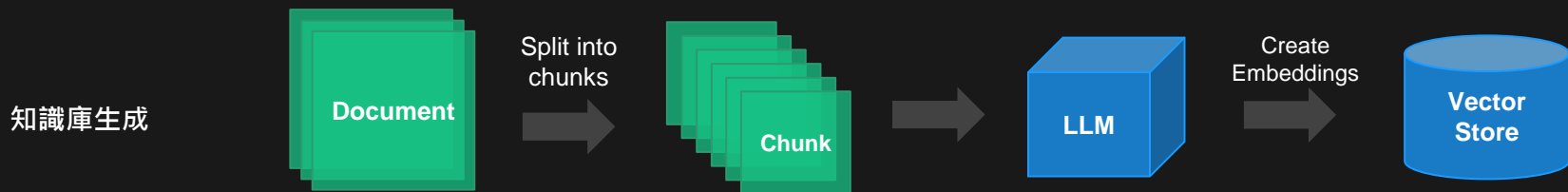
/ / / / / / / / /

我們將 Prompt 模組化，打造雲端架構師的人設

角色	你的角色是「雲端架構師」，
用途	專門解惑雲端相關知識，像 GCP, AWS, Azure 的雲端架構設計與評估，包含效能、安全、費用等議題，可以針對金融行業特性舉例說明。
格式	然後，回答格式請「條列式」，回答字數在「200字以內」。
注意事項	還有回答原則與規範，不需要重新覆述問題，若問題需要有建議方案，請做方案比較後，再給出結果。
超過範圍	如果問題與雲端無關，你要說「不好意思，我只能回答雲端相關資訊。」
銜接問題	用戶的問題是：
回答風格	Temperature: 0.1 (近乎精準，一點點創意性回答)

ARTIFICIAL INTELLIGENCE (AI)

我們採用 Vector 知識庫，打造 AI 的圖書館



ARTIFICIAL INTELLIGENCE (AI)

一切看起來很美好，但中途還是踩了一點坑...



什麼是cathay 6r?



I don't find any information related to your question from the fetched documents. As a result, I am unable to provide an answer.

直接找不到文本



什麼是Cathay 6r?



從搜尋結果來看，Cathay 6R是國泰航空公司一種上雲的策略，透過將資料上傳至雲端進行分析，以協助公司做出更好的決策。6R的策略是“消滅虛擬機”，透過分析整體上雲的效益，以決定如何上雲，包括風險、業務效益、技術適合度等等。[doc1][doc2]

部分資訊錯誤



什麼是 Cathay 6R?



根据检索到的文档，Cathay 6R 是一个云计算架构的上云策略，旨在消灭虚拟机，提供更快的交易市场、资源申请效率、省钱、天然的高可用性和更少的维护。这个策略是为了保证整个上云架构的判断 [doc1][doc2]

無意義的出處、
出現簡體字

AIN
[AI]

當我們找到 LangChain 開源神器之後，期盼已久的事終於發生了！



什麼是6R?



6R是國泰金控集團在進行系統上雲遷移時所使用的一套方法論，用於評估和分類系統的上雲方式。以下是6R的詳細說明：

1. Rehost（搬遷）：將系統直接遷移到雲端，不做任何改動，使用IaaS模式上雲。
2. Re-platform（平臺轉換）：對應用服務進行一些改動，例如使用雲端託管服務或將應用程式容器化，可以使用IaaS或PaaS模式上雲。
3. Refactor（重構）：對低度應用程式進行調整，使系統達到最適上雲狀態，例如改寫程式碼以串接雲服務API或進行前後端分離，可以使用IaaS或PaaS模式上雲。
4. Rewrite（重寫）：對整體系統進行大幅度改動，包括程式碼和系統架構的重新設計，例如改變程式語言或轉換為Cloud Native架構，可以使用PaaS或SaaS模式上雲。
5. Replace（替換）：使用SaaS雲端服務取代現行服務進行上雲。
6. Retain（保留）：系統可能因合規性、系統合併或預計下線等因素而保留在地端運作。

根據不同的系統特性和需求，可以選擇適合的6R方式進行系統上雲。例如，對於金融行業的系統，可能需要考慮安全性和合規性的因素，可以選擇Refactor或Rewrite方式進行上雲，以提升系統的安全性和效能。

ARTIFICIAL

INTELLIGENCE

[AI]

Chatbot Demo

我們以國泰大規模上雲策略的新聞稿為文本，
詢問 AI 什麼是 Cathay 6R，以及與 AWS 7R 的比較？

[AI]

會員登入

✉ 電子信箱

🔒 密碼

登入

☐ 記住電子信箱

[忘記密碼?](#)

ARTIFICIAL

INTELLIGENCE



列出AWS 7Rs以及Cathay 6Rs的差別



AWS 7Rs和Cathay 6Rs的主要差異如下：

1. 定義：AWS 7Rs包含了7種雲端遷移策略，包括：Rehost、Replatform、Repurchase、Refactor、Retire、Retain和Relocate。而Cathay 6Rs則是國泰金控自行定義的6種雲端遷移策略，包括：Rehost、Re-platform、Refactor、Rewrite、Replace和Retain。
2. 策略內容：AWS 7Rs中的Repurchase和Relocate在Cathay 6Rs中並未明確提及。Repurchase是指更換或升級現有的應用程式授權，Relocate則是將應用程式遷移到新的物理位置。而Cathay 6Rs中的Rewrite和Replace則是國泰金控特有的策略，Rewrite是指將應用程式和系統架構進行大幅度的改寫和更改，Replace則是全面改以SaaS服務型態進行上雲。
3. 適用情境：AWS 7Rs適用於所有使用AWS雲端服務的企業，而Cathay 6Rs則是針對國泰金控自身的業務需求和特性所訂定的策略。
4. 策略目標：Cathay 6Rs的策略目標是「消滅虛擬機」，希望能夠盡量避免使用虛擬機，而改用容器來取代。而AWS 7Rs則沒有明確的策略目標，主要是提供企業在進行雲端遷移時的參考策略。

[AI]



第四章

未來的 Multi-Cloud

Azure, AWS, GCP



企業級 GAI 的未來在多雲，我們將逐步驗證出最佳 SaaS 組合方案

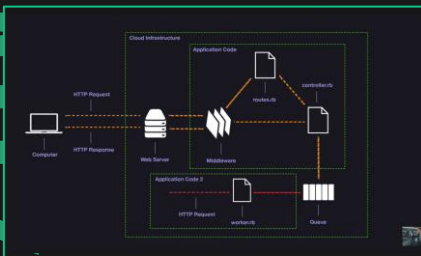
	AWS	GCP	Azure	Open Source
DLP	DLP	DLP	DLP	-
Knowledge Base	Open Search	Vector Search	Cognitive Search	Langchain ✓
LLM	Claude 2	PaLM 2	GPT4 / GPT3.5 ✓	Llama 2
AI Platform	Bedrock	Vertex AI	Azure Open AI ✓	-

而這只是起點，我們下一步還會強化 AI 學會更多雲端事...



情境一：雲端知識解惑

- 雲端技術輸出文章
- 雲端管理辦法諮詢



情境二：架構評估設計

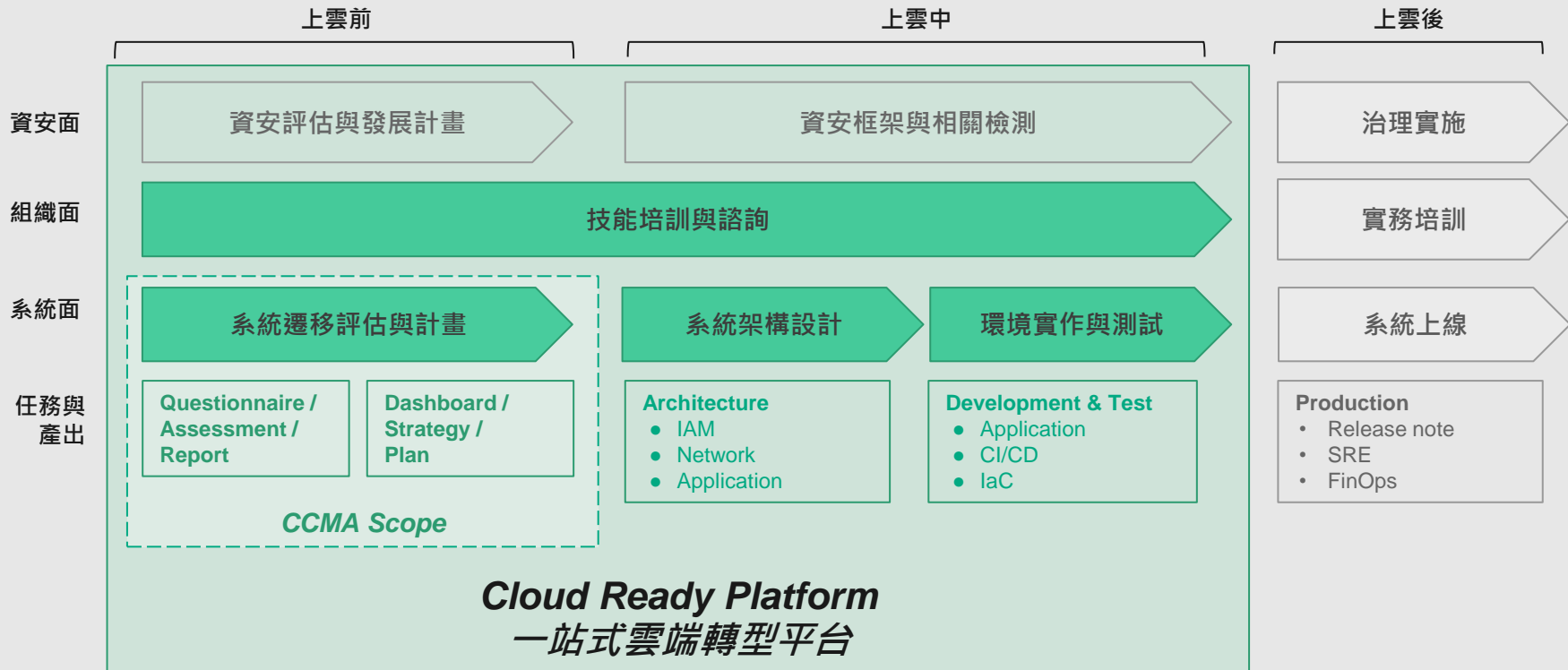
- 雲端架構範本生成
- 雲端架構設計評估



情境三：環境實作測試

- IaC 程式碼範本生成
- IaC 程式碼品質審查

以及整合所有 AI 功能在 Cloud Ready Platform，一站式加速雲端轉型！





國泰金控

Cathay Financial Holdings

Thank you!