



AWS 雲端中用戶端生命週期管理的銀行現代化策略

AWS 方案指引



AWS 方案指引: AWS 雲端中用戶端生命週期管理的銀行現代化策略

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介	1
現代化挑戰	2
不斷變化的期望和新型銀行	2
業務問題	2
客戶生命週期管理	2
客戶入門	3
入門之旅	4
無伺服器入門	5
入門解決方案	5
安全和合規	7
常見問答集	9
如何確定 AWS 服務不會儲存任何個人資料？	9
該架構是否符合 GDPR 規定？	9
如何確保適當的資料機密性？	9
我可以將 AWS 銀行現代化解決方案與任何舊版銀行系統整合嗎？	9
我可以自訂入職對話方塊嗎？	9
後續步驟	10
Resources	11
文件歷史紀錄	12
.....	xiii

AWS 雲端中用戶端生命週期管理的銀行現代化策略

Patrick Rotzetter 和 Florent Batard , Amazon Web Services (AWS)

2022 年 6 月 ([文件歷史記錄](#))

金融服務 (FS) 產業正面臨嚴重的混亂。越來越多的客戶期望甚至更喜歡金融科技公司和新型銀行 (即沒有實體分支機構的數位化銀行) 作為零售客戶入職流程的一部分提供的完全數位化自助銀行服務。傳統金融機構無法跟上金融科技公司和新型銀行的步伐。這是因為大多數傳統金融機構的銀行流程仍然是手動或半自動。

即使這些流程對於所有金融機構都是通用的，但沒有用於實作傳統銀行流程的標準框架。缺乏這樣一個標準框架正在妨礙創新。例如，傳統金融機構不能利用銀行業的最新趨勢之一：內嵌式金融。也就是說，非銀行提供類似銀行服務的能力。如需詳細資訊，請參閱 McKinsey & Company 的[內嵌式金融和銀行即服務趨勢對金融服務意味著什麼](#)。為了讓傳統金融機構能夠充分利用內嵌式金融，就必須將自己的業務能力無縫地暴露給其他企業。

此策略定義了現代化方法，透過使用建置在 AWS 雲端服務上的 API 導向無伺服器架構，來實作可擴展且安全的標準銀行程序。為了說明這種方法的挑戰和機遇，該策略著重於用戶端生命週期管理 (CLM) 的案例研究。此策略的目標受眾包括零售銀行和財富管理產業的 CEO、CFO、CIO 和高級經理。

銀行業現代化挑戰

不斷變化的客戶期望和新型銀行的興起

金融服務產業正面臨著巨大變革。客戶不僅期待完全數位化的旅程，還期待個人化體驗。為了滿足這些客戶期望並與新型銀行競爭，傳統金融機構必須進行大規模轉型，這需要速度、敏捷性和創新。這種轉型需要傳統金融機構克服以下近期挑戰：

1. 傳統銀行必須跟上新型銀行的步伐，由於沒有技術和流程負擔，新型銀行本質上更加靈活。
2. 傳統金融機構必須透過銀行即服務 (BaaS) 來開發和提供內嵌式銀行服務。
3. 傳統金融機構必須開發並啟用可自訂且靈活的客戶體驗，以便快速且經濟實惠地整合機器學習模型。

未來幾年要考慮的關鍵策略因素是利用內建的雲端服務，以及透過與服務供應商合作和靈活轉型所帶來的上市時間優勢。

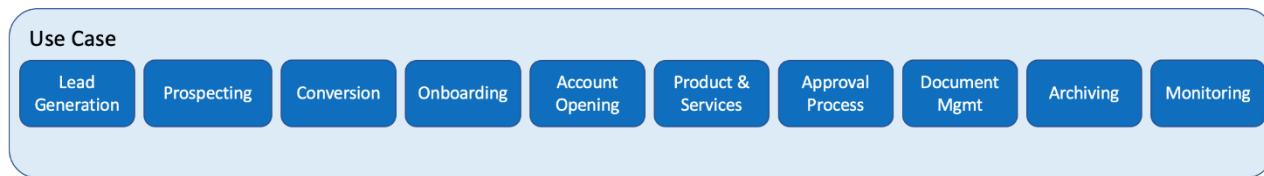
業務問題

傳統金融機構仍然使用手動或半自動流程。常規銀行業務流程沒有適用的產業標準，即使這些流程對於類似轄區的所有金融機構都通用。為了克服這些挑戰，傳統金融機構可以使用建置在 AWS 雲端服務上的無伺服器方法來實作可擴展且安全的標準程序。例如，[Amazon Lex](#) 和 [Amazon Rekognition](#) 提供訓練有素的機器學習模型，可以將其整合到增強的客戶旅程中。過去，這種創新受到複雜整合和昂貴開發流程的阻礙，但現在這些創新可以透過 API 呼叫直接用於客戶應用程式。

AWS 雲端服務不僅提供額外的創新和整合速度，還利用最新的安全功能來確保資料的機密性和隱私權。我們想強調 CLM 環境中銀行業的現代化方法。客戶生命週期是客戶關係的核心，這就是為什麼它必須緊急進行現代化甚至數位化的原因。如 McKinsey & Company 的[內嵌式金融和銀行即服務趨勢對金融服務意味著什麼](#)所示，想要提供 BaaS 的銀行必須使其正常運作，並且「使其正常運作將需要新技術和能力，因為 BaaS 通常透過 API 分發給客戶，並且需要內嵌式金融合作夥伴的強大風險和合規管理。」此策略中的無伺服器入門一節說明了如何使這樣的策略發揮作用。

客戶生命週期管理使用案例

CLM 是一組鬆散的相互依存和強制性流程，用於定義客戶與其金融機構或保險公司的業務互動。下圖提供了銀行和保險產業 CLM 階段的概述：



考慮到這些流程因客戶群體而異。例如，商業客戶入門不同於零售客戶入門。這些流程也可能因產業而異。讓銀行客戶入門不同於讓保險客戶入門。此策略著重於銀行零售客戶體驗。

在上圖中，每個方塊 (例如勘探) 代表現代化候選人。您可以使用這樣的圖表將使用案例分解為互不相連的獨立使用案例。例如，勘探使用案例可以分解為組成使用案例。然後，可以將每個獨立的使用案例映射至現有功能，無論是來自雲端服務提供商還是 BaaS 提供商。此映射方法說明銀行業的文件歸檔本身可以是由外部提供的服務。將客戶生命週期管理使用案例分成互不相連的獨立使用案例，使您能夠設計和開發重點服務。

此策略側重於開設新銀行帳戶的使用案例範例。對於客戶而言，這通常是一個冗長、高度手動且容易出錯的過程，會導致沮喪和不滿。如今，大多數入門工作仍在透過電話或實體聯絡點手動進行。但是，研究表明客戶更喜歡數位體驗。根據 Open Research Europe 的[金融業的數位入門：新穎模式及相關網路安全風險](#)所示，70% 的客戶更喜歡以數位方式簽約產品。

客戶入門機會

在後 COVID 危機時代，銀行和金融服務機構客戶必須面臨繁瑣而複雜的流程。實際上，如今很少有客戶能夠透過行動裝置完成開立支票帳戶的整個過程。大多數客戶必須遵循手動入門流程才能開立類似以下銀行帳戶：

1. 客戶或最終使用者必須提交身份證明、合法 ID 和其他各種資料點。在許多情況下，這些資料點包括實際地址、就業證明等文件。通常，客戶必須造訪分公司才能獲得此資訊，或透過標準郵件將其傳送給銀行。
2. 在客戶使用銀行帳戶之前，他們將收到幾份紙質文件。然後，客戶必須簽署文件並將其交還給銀行 (即每種銀行產品有一份單獨合約，例如個人帳戶、聯名帳戶、交易帳戶、電子銀行、信用卡或安全碼)。
3. 銀行將所有已簽署的文件數位化，並將其鏈接到「正在進行的工作」帳戶，以使帳戶正常運作。
4. 根據客戶群體或申請人的風險評定，銀行必須定期部分或全部重複此過程。
5. 如果客戶地址、公民身份或任何其他被視為「情況變化」的資料被更新，則會再次啟動該過程。

完成此過程可能需要數天甚至數週的時間，並且通常需要來自不同部門的多名銀行員工的介入和批准。

入門客戶之旅

現代化的客戶開戶之旅應包括以下特徵和功能：

- 客戶可以透過網站、虛擬助理或呼叫中心存取入門服務。虛擬助理可以是面向文字或語音的聊天機器人，它可以整合到網頁中，也可以整合到 Messenger 或 Telegram 等消息傳遞應用程式中。
- 虛擬助理可以透過使用預定義的意圖與客戶互動，以了解客戶的需求和背景。例如，虛擬助理可以要求客戶分享他們的興趣，共用個人資訊來開設帳戶，掃描他們的 ID 並自拍，或確認他們想繼續開設帳戶。
- 聊天機器人可以使用多種語言。
- 客戶可以使用語音或文字與聊天機器人互動。
- 當您從客戶那裡收集所有必需的資訊後，可以將該資訊傳送到銀行以啟動開戶過程。客戶將收到一封電子郵件通知，確認該過程已開始。
- 可以在帳戶開啟後關閉對話方塊。
- 避免將客戶資訊存儲在雲端中。此資訊必須是暫時的，並且僅在客戶參與期間存在。開戶過程完成後必須刪除資料，並在可能的情況下提供一些刪除證明。即使對話方塊被中斷，也必須確認所有個人資料都已刪除 (無快取)。
- 避免儲存帶有個人身分識別資訊 (PII) 的日誌。
- 客戶可以確信不會儲存任何 PII 資料。如果使用的服務是無伺服器服務，則不會保留包含個人資料的資料或日誌。

無伺服器入門

本節重點介紹用戶端入門使用案例。它是如何重複使用無伺服器模式以現代化重要客戶旅程的範例。

入門解決方案

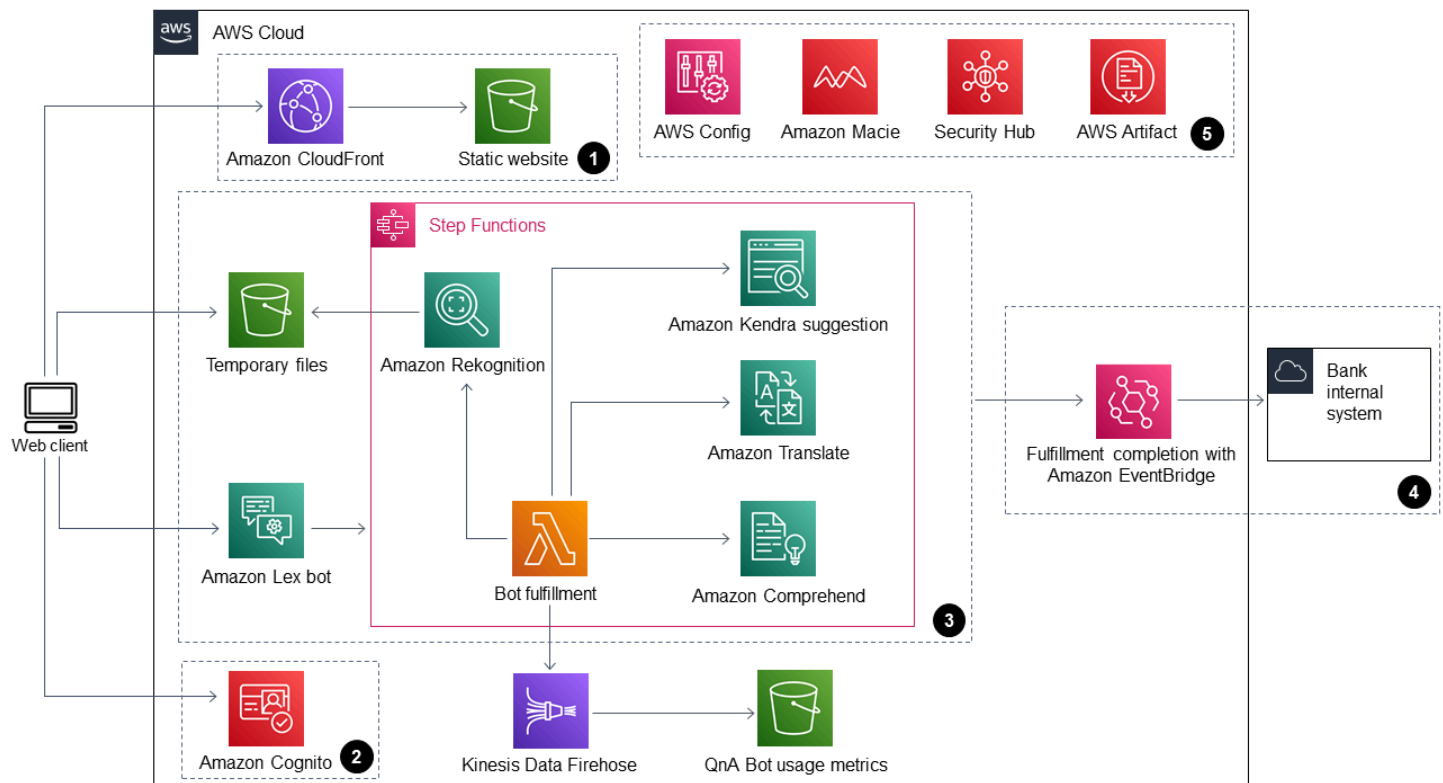
入門解決方案通常不會孤立出現，而是大局的一部分。整合所需的元件和服務包括：

1. 潛在客戶開發 (CRM 系統)
2. 盡職調查 (AML、風險和合規)
3. 中央用戶端資料檔案 (核心銀行系統)
4. 數位簽章管理 (使用 DocuSign 等第三方工具)
5. 生物識別驗證
6. 數位合約管理週期
7. 流程和操作模式自動化

注意

這些元件與外部應用程式的整合已超出此策略的範圍。

下圖說明透過 AWS 雲端中的聊天機器人與客戶互動的無伺服器架構：



注意

架構是以 AWS 解決方案上的 QnA 機器人和 Amazon Rekognition 的更新為基礎。如需詳細資訊，請參閱《AWS 解決方案程式庫》中的 [QnA Bot on AWS](#)，以及《AWS Machine Learning 部落格》中的 [Amazon Rekognition 宣布其臉部偵測、分析和辨識功能的更新](#)。

該圖顯示以下工作流程：

1. 客戶存取前端元件以與機器人互動。在這種情況下，前端程式庫可以透過各種方式包含在現有資產中。例如，可以將這些元件整合到公司網站中，或將其連結到主要聊天應用程式。這些元件會以 JavaScript 形式交付，並使用 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudFront 透過靜態資產管理提供服務。
2. 前端元件會內嵌到後端元件的連線，透過 Amazon Cognito 驗證憑證。一旦獲得授權，用戶端服務就可以與入門解決方案的服務進行通訊。
3. 客戶使用 Amazon Lex 機器人與服務互動。透過使用 呼叫必要的 服務來完成程序 AWS Step Functions，執行預先定義的加入案例。可以根據銀行系統的需求量身打造此案例 (例如，滿足攝影需求、多語言翻譯以及符合客戶意圖的自然語言處理)。您可以使用 AWS Lambda 函數與客戶一起完成 Amazon Lex 機器人的動作，並根據加入階段呼叫 服務。

4. Step Functions 的輸出會透過 Amazon EventBridge 批次傳送到銀行內部系統，它會使用您偏好的方法連接到銀行內部系統。您可以對等到另一個 AWS 帳戶，或透過虛擬私有網路 (VPN) 對等到銀行系統來處理此通訊。
5. 整個架構旨在透過使用 AWS Config、Amazon Macie 和 來確保安全性 AWS Artifact和合規性 AWS Security Hub CSPM。

安全和合規考量事項

維護安全性和處理敏感資訊是無伺服器入門方法的核心。無伺服器入門設計為無狀態，不會儲存任何 PII 或重要業務資料。為了確保持續的安全性和合規性，必須落實下列服務並正確地進行設定：

- AWS AppConfig 透過專為合規量身打造的規則，確保服務的完整性和機密性。適當的控制將驗證整體合規性，並防止組態中的偏離。
- Macie 會在整個過程中偵測並標記任何 PII。
- Security Hub CSPM 可確保在安全範圍內定義和使用所有服務。
- AWS Artifact 提供稽核證據以遵守 AWS 服務。

使用客戶受管金鑰或出於稽核目的而密封的專用硬體安全模組 (HSM) 來存儲和加密交易及不可否認性證據。您也可以低成本地密封資料，同時使用 Amazon Glacier 確保完整性和安全性。

Note

自 2025 年 12 月 15 日起，Amazon Glacier（原始獨立保存庫型服務）將不再接受新客戶，不會影響現有客戶。

Amazon Glacier 是一項獨立服務，具有自己的 APIs，可將資料存放在保存庫中，並與 Amazon S3 和 Amazon S3 Glacier 儲存類別不同。您現有的資料將在 Amazon Glacier 中無限期保持安全且可存取。不需要遷移。對於低成本、長期的封存儲存，AWS 建議[採用 Amazon S3 Glacier 儲存類別](#)，透過 S3 儲存貯體型 APIs、完整 AWS 區域 可用性、降低成本和 AWS 服務 整合提供卓越的客戶體驗。如果您想要增強功能，請考慮使用我們的解決方案指南，將資料從 Amazon S3 Glacier 保存庫傳輸至 Amazon S3 Glacier 儲存類別，以遷移至 Amazon S3 Glacier 儲存類別。 [AWS Amazon Glacier Amazon S3](#)

只允許運營團隊存取該環境。應透過自動持續交付來簡化任何開發活動，以防止任何人存取生產環境。出於稽核目的，應提供額外的角色，以存取平台上的成品和合規報告。

AWS 有助於確保您符合法規和合規標準。如需詳細資訊，請參閱 AWS 文件中的 FINMA ISAE 3000 類型 2 報告。您也可以直接從 下載相關的銀行成品 AWS Artifact，包括 FINMA Circular 2008/21、FINMA ISAE 3000 Type 2、FINMA Circular 2018/03 和全球金融服務法規原則。

常見問答集

如何確定 AWS 服務不會儲存任何個人資料？

您可以使用 AWS Config 檢查架構元件與 Macie 結合的合規性，以偵測和修復發現的任何個人資料。

該架構是否符合 GDPR 規定？

是的，根據 GDPR 第 2 章的[第五條](#)，該架構的設計不會長期保留與使用者有關的任何資料，而僅用於處理 PII。這是透過持續的合規機制來確保的。此外，Macie 還可確保對任何可能危害 GDPR 合規性的 PII 資料進行標記和分類。

如何確保適當的資料機密性？

使用 Security Hub CSPM 和 Macie AWS Config，透過持續合規和安全性模式來確保機密性。會立即偵測、補救並上報機密性違規行為。也建議在部署階段加入防護機制。防護機制有助於確保任何可能危及機密性的重大變更都不會被推送到架構。

我可以將 AWS 銀行現代化解決方案與任何舊版銀行系統整合嗎？

該解決方案的設計具有適應性，並且可以與任何可接受標準 API 呼叫的舊版銀行系統整合。

我可以自訂入職對話方塊嗎？

是的，您可以自訂聊天機器人對話方塊以適應您的使用案例和目標對話方塊順序。如需詳細資訊，請參閱 AWS 解決方案程式庫中的 [上的 QnA 機器人 AWS](#)。

後續步驟

除了用戶端加入之外，還有其他 CLM 使用案例，這些使用案例可以透過內建 AWS 雲端 服務進行現代化。下列案例會探索一些潛在的現代化使用案例：

1. 透過使用 [Amazon Personalize](#) 或其他自訂建議，將產品推薦整合到烘焙產品和服務中。儘管金融服務產品與零售產品不同，但根據 The Financial Brand 的[行業領導者預測到 2025 年銀行業將發生巨大變化](#)，預計到 2025 年，個性化程度仍然很高。客戶可能願意為高度個人化和情境式服務付出更多費用。這只能透過基於機器學習的更智慧型解決方案來實現。
2. 可以使用基於機器學習的線上欺詐檢測器 [Amazon Fraud Detector](#) 來監控帳戶。也可以自訂其他內建演算法，以提供標準化帳戶監控服務 (例如，使用異常偵測)。

Note

自 2025 年 11 月 7 日起，Amazon Fraud Detector 不再向新客戶開放。對於類似 Amazon Fraud Detector 的功能，請探索 Amazon SageMaker、AutoGluon 和 AWS WAF。如需詳細資訊，請參閱 [Amazon Fraud Detector 可用性變更](#)。

3. 可以使用 Amazon Lex 和以最新自然語言模型為基礎的聊天機器人，讓智慧助理直接與客戶互動。

創意解決方案沒有限制，但必須大規模且快速整合和部署此類解決方案。

Resources

- [內嵌式金融和銀行即服務趨勢對金融服務意味著什麼](#) (McKinsey & Company)
- [金融數位化：新穎模式及相關網路安全風險](#) (Open Research Europe)
- [行業領導者預測到 2025 年銀行業將發生巨大變化](#) (The Financial Brand)
- [AWS 瑞士金融服務法規和指導方針使用者指南和 FINMA 工作手冊出版物](#) (AWS 安全部落格)
- [FSI 服務焦點：精選 AWS Lambda](#) (AWS 部落格文章)
- [Amazon Rekognition 宣佈更新其臉部偵測、分析和辨識功能](#) (AWS Machine Learning 部落格)
- [上的 QnA 機器人 AWS](#) (AWS 解決方案程式庫)

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 [RSS 摘要](#)。

變更	描述	日期
初次出版	—	2022 年 6 月 8 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。