出國報告(出國類別：實習)

AWS re：Invent 2023

技術年會及設施參訪(雲治理)

服務機關：台灣電力公司

姓名職稱： 陳沛霖 電腦軟體工程師

派赴國家/地區：美國/拉斯維加斯、西雅圖

出國期間：112 年 11 月 26 日至 112 年 12 月 6 日

報告日期：113 年 3 月 21 日

目錄

目的

隨著混合雲和雲治理在企業 IT 策略中的重要性日益提升,作為台電資訊處的一員,我有幸參加 AWS re:Invent 2023。此行的主要目的如下:

1. **探索建立雲端卓越中心(Cloud Center of Excellence, CCoE)的可行性**

   為了推動台電的雲端轉型,我希望能夠深入了解 CCoE 在不同行業的建立和運作模式。透過學習 AWS 提供的最佳實踐和參考架構,期望能夠評估在台電內部建立 CCoE 的可行性,為制定長遠的雲端採用策略奠定基礎。

2. **學習利用 AI 和資料驅動優化電網運營和決策的方法**

   智慧電網的建設離不開 AI 和資料分析技術的應用。藉由此行，我希望能夠深入了解電力行業如何利用這些技術來提高運營效率並支持資料驅動的決策制定，為台電提供寶貴的參考。

3. **了解如何強化資訊系統的韌性和可恢復性**

   透過參加相關的講座和研討會,我希望能夠學習到先進的韌性設計原則和實踐,如混沌工程、故障測試等,以提高台電資訊系統的可靠性和容錯能力

4. **探索電力行業的可持續發展策略**

   能源行業肩負著推動可持續發展的重要責任。因此此行目的之一是了解全球能源企業如何利用雲端技術和創新解決方案來實現節能減碳、提高能源效率並促進再生能源發展。期許能為台電提供有價值的參考。

5. **學習雲端環境下的安全合規最佳實踐**

   隨著台電加速雲端轉型，確保雲端環境的安全性和合規性變得至關重要。我也希望能夠深入了解 AWS 在資料保護、資訊安全、合規審計等方面提供的服務和最佳實踐，為台電的雲端治理提供參考。

6. **了解自動化維運在電力行業的應用**

   維運自動化是提高系統效率和可靠性的關鍵。藉由此次參訪，我期望能夠學習到業界領先的自動化維運工具和實踐，特別是在雲端環境下如何實現補丁管理、事件處理等任務的自動化，進一步提升台電的自動化維運。

過程

圖說：AWS re:Invent 2023 年會現場。

參與 AWS re:Invent 2023

我於 2023 年 11 月 27 日至 12 月 2 日參加了在美國拉斯維加斯舉辦的 AWS re:Invent 2023 大會。在為期五天的 2000 多場演講中,我主要選擇與雲治理相關的核心領域,如智慧維運(AIOps)、資安、混合雲治理、成本規劃以及環保合規等主題,積極探討雲治理的最新趨勢和技術發展。

專業成長與產業交流

在演講期間，我不僅有機會聆聽多場前沿技術講座，還與來自不同領域的從業人員展開的交流。通過參與各種主題的演講，我吸收了大量的知識與觀念，收穫良多。

深化學習於西雅圖

緊接著，於 12 月 3 日至 4 日在西雅圖參訪了 AWS 的總部。這一階段的學習讓我能夠將大會上獲得的想法透過交流更了解實務的運用，深化了我對雲治理理解與認知。

活動介紹

圖說：AWS re:Invent 現場演講座無虛席。

Services（AWS）的年度技術盛會,自 2012 年起每年在拉斯維加斯舉辦。這場為期一周的活動是面向 AWS 客戶、開發人員、技術領袖和教育者的旗艦大會,專注於雲計算的未來趨勢、AWS 平台的新功能以及與雲技術相關的最佳實踐。

歷史起源

AWS re:Invent 於 2012 年首次舉辦，當時吸引了大約 6 千名參加者。自此之後，參加人數和活動規模逐年增加，今年更達到 7 萬人參與，顯示了 AWS 以及整個雲計算產業的迅速成長。

發展

隨著時間的推移，AWS re:Invent 逐漸增加了更多的演講、研討會、實驗室和認證機會，涵蓋了從基礎架構管理到機器學習、人工智能、資料分析和物聯網等高端主題。

特色演講

包括 AWS 高管的主題演講，介紹 AWS 的新方向、策略和服務。這些演講是洞察 AWS 未來發展的重要途徑。

培訓和認證

提供各種培訓課程和認證機會，幫助開發者、架構師、工程師和系統管理員提高他們使用 AWS 服務的技能和知識。

實作工作坊

參加者可以參加實作工作坊，親自體驗 AWS 最新技術。

交流互動

AWS re:Invent 為來自全球的技術專家和從業人員提供了一個絕佳的機會，參加者可以交流想法、分享經驗和建立專業聯繫。

創新展示

AWS re:Invent 的會場通常會保留一個廣闊的合作夥伴展區，展示來自 AWS 生態系統合作夥伴的最新技術和解決方案。

圖說：大會現場的合作夥伴展區，有眾多知名企業參展。

參考網址：

https://aws.amazon.com/blogs/aws/top-announcements-of-aws-reinvent-2023/

https://www.logicmonitor.com/blog/aws-reinvent-2023-recap

研習內容與參訪過程

雲端卓越中心

導讀

雲端卓越中心(CCoE, Cloud Center of Excellence)是一種組織架構,旨在領導和推動企業的雲端採用策略。CCoE 通常由跨職能團隊組成,這些團隊成員來自企業的不同部門,如 IT、安全、法規遵循、財務和業務運營等。CCoE 的主要目標是確保雲端技術的高效使用,同時遵守相關政策和最佳實踐。

CCoE 對於智慧電網和電力公司尤為重要,主要體現在以下幾個方面:

策略與規劃:CCoE 有助於電力公司制定長遠的雲端採用策略,這包括決定哪些業務流程和系統適合雲化,選擇合適的雲服務提供商和技術棧。

治理與合規:隨著智慧電網的資料量激增,CCoE 確保雲端採用遵守國家和行業的規範標準,例如資料保護法和能源行業的特定規定。

成本管理:透過有效的成本管理和優化策略,CCoE 幫助電力公司控制雲端支出,實現經濟效益最大化。

技術指導:CCoE 促進最新雲技術的採用,例如微服務架構、容器化和無伺服器計算,這些技術可以提高應用程式的彈性、可擴展性和安全性。

創新驅動:通過推動人工智慧、機器學習和大資料分析等先進技術的應用,CCoE 為電力公司的創新項目提供支持,促進智慧電網的發展。

總體而言,CCoE 不僅為電力公司的雲端轉型提供了指導和支持,也為智慧電網的創新和可持續發展奠定了基礎。隨著能源行業面臨的挑戰日益增加,如需求波動、再生能源的整合和電網的可靠性問題,CCoE 的角色變得更加關鍵,它不僅有助於降低營運成本,還能加速新技術的採用,從而提升電力系統的整體效能。

CCoE 的任務和實績通常包括:

1. **策略和規劃**:制定雲端採用和運營的全面策略,包括確定哪些應用適合遷移到雲端,以及選擇最合適的雲服務模型(IaaS、PaaS、SaaS)和供應商。
2. **治理和合規**:建立治理框架來管理雲服務的使用,確保遵守相關的法律法規和行業標準,如 GDPR(一般資料保護條例)或 HIPAA(健康保險流通與責任法案)。
3. **成本管理和優化**:實施成本監控和優化措施,使用如 AWS 成本探索工具、Azure 成本管理和 Google Cloud 平台的定價計算器等工具來預測和管理支出。
4. **技術指導和最佳實踐**:推廣雲架構最佳實踐,如微服務架構、無服務架構和容器化,以提升應用的可擴展性、可靠性和安全性。
5. **培訓和能力發展**:開展培訓計劃提升員工的雲技能,通過研討會、認證課程和實踐研習來加強團隊的雲能力。

6. **創新和數位轉型**：推動使用先進的雲技術如人工智能、機器學習和大資料分析，以支持新業務模型和創新項目。
7. **安全和風險管理**：確保雲環境的安全，實施加密、身份和訪問管理、網絡安全和資料保護等措施。

這些任務和實績有助於企業實現雲端採用的各種好處，包括提升運營能力、降低成本、加速創新和改善客戶體驗。通过案例研究和業界報告，可以找到特定企業和其 CCoE 的具體成就和挑戰。

奇異公司(GE)是在能源領域建立了雲端卓越中心（CCoE）的一個重要參考。GE 在全球 180 多個國家開展業務，是工業製造的領導者，憑藉其世界級的工程技術、軟體和分析能力，幫助這個世界更高效、可靠和安全地運作。GE 的 CCoE 通過使用超過 2,000 個雲應用和 55 項 AWS 服務來增強其航空、能源、醫療保健和再生能源業務的規模、效率和性能

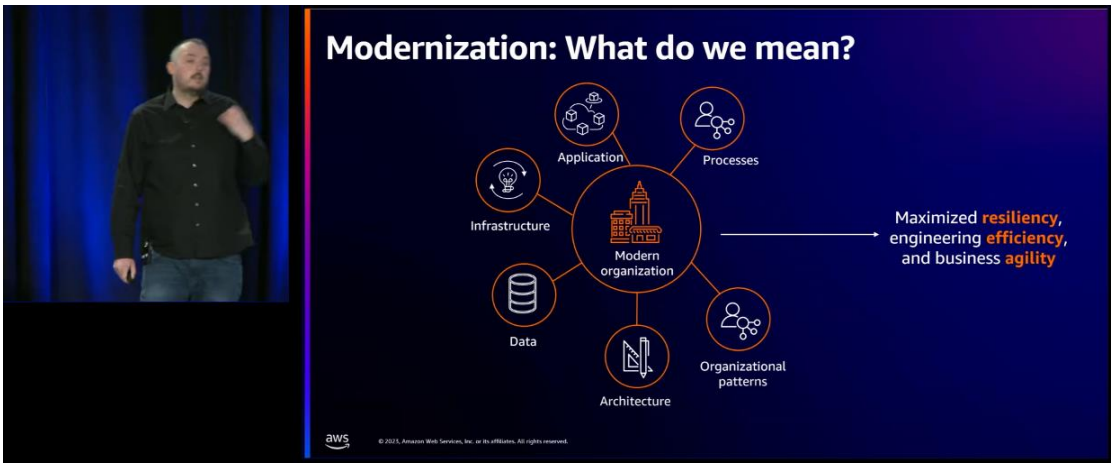
例如，GE 再生能源（GE Renewable Energy, GERE）在 AWS 上現代化了其數位服務平台，提高了可擴展性、可用性和靈活性。為了支持對無碳電力的需求並改善計算能力，GERE 的數位服務團隊進行了平台現代化工作，以改善對其 40,000 多個資產產生的 terabytes 資料的管理、處理和分析。通過遷移到 AWS 驅動的解決方案，GERE 提高了部署頻率，實現了 99.9% 的可用性，並且可以在不預配基礎設施的情況下進行擴展。
https://aws.amazon.com/tw/solutions/case-studies/general-electric/

此外，Microsoft 的網站也展示了多家能源公司利用 Microsoft 技術進行創新和轉型的成功故事，這些公司包括 Eaton、Uniper、XTO Energy、BP、Chevron、Shell、Equinor、C3 IoT 和許多其他公司。這些故事展示了這些公司如何利用雲技術、物聯網（IoT）、人工智能（AI）和機器學習來提高效率、促進創新並改善業務流程
https://www.microsoft.com/energycore/success-stories.aspx

Establishing a modernization CCoE (PEX304)

這場演講有兩個重點：

一、介紹 aws 的現代化途徑



AWS 提供了多種現代化途徑來幫助組織轉型他們的業務和技術環境，以充分利用雲計算的優勢。這些途徑包括但不限於以下幾種：

移至雲原生架構

這個途徑涉及將應用程式和服務轉移到使用雲原生技術和服務的架構，比如無伺服器（Serverless）架構、微服務架構和容器。這有助於提高彈性、可擴展性和創新速度。

容器化

容器化是將應用程式及其依賴的項目打包到一個輕量級、可移植的容器中，這有利於在不同的運行環境中一致且快速地部署和管理應用程式。AWS 提供了多種容器服務，如 Amazon ECS（Elastic Container Service）和 Amazon EKS（Elastic Kubernetes Service）。

無伺服器技術

無伺服器架構允許開發者構建和運行應用程式而無需管理伺服器。AWS Lambda 是一個無伺服器計算服務，它自動管理底層計算資源，只在需要時運行程式碼並自動縮放。

資料庫現代化

資料庫現代化涉及將遺留的、專有的或自我管理的資料庫遷移到完全管理的雲資料庫服務，如 Amazon RDS（Relational Database Service）和 Amazon Aurora。這有助於提高性能、可用性和成本效率。

應用程式現代化

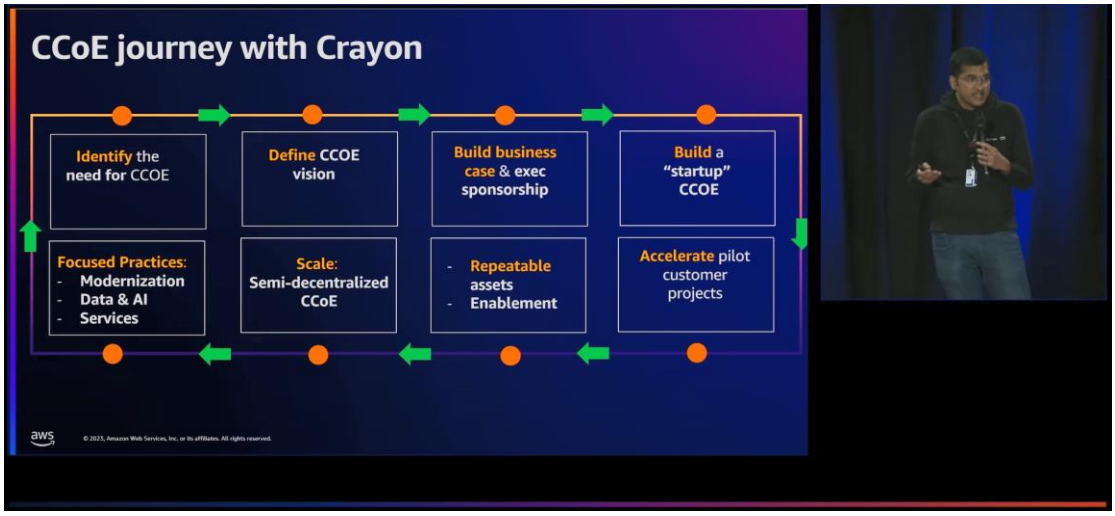
通過重構、重新設計或重建現有的應用程式，利用雲技術和最佳實踐來提高應用程式的靈活性、效率和創新能力。

DevOps 和自動化

採用 DevOps 實踐和自動化工具來提高軟體開發和交付的速度、質量和可靠性。AWS 提供了一系列的服務和工具，如 AWS CodeBuild、AWS CodeDeploy 和 AWS CodePipeline，來支持持續整合和持續交付（CI/CD）。

這些現代化途徑不是孤立的，組織通常會結合使用多種途徑來實現其整體的雲端轉型目標。AWS 提供了全面的服務和工具，幫助客戶在這些途徑上取得成功。

案例介紹 Crayon



Crayon 是一家全球性的 IT 顧問公司，專注於軟體和數位轉型服務，幫助客戶最大化其軟體和雲端技術投資的價值。Crayon 提供從軟體資產管理和軟體授權優化到雲端解決方案和創新技術諮詢的廣泛服務。

建立 CCoE 的願景

Crayon 將 CCoE 視作推動雲端採用的關鍵策略，包括雲端策略、遷移、現代化和管理服務。他們強調了統一的服務質量，不論客戶聯繫的是哪個地區的 Crayon 子公司。

執行策略

Crayon 利用 CCoE 為客戶創建了一系列可重複使用的智慧財產（IP）資產。這些資產使得 Crayon 能夠以更低的成本和更快的速度為客戶提供服務。

客戶項目和反饋

Crayon 執行了多個試點項目，這些項目不僅證明了其 CCoE 的有效性，同時也獲得了客戶的正面反饋。

擴展 CCoE 模型

隨著 Crayon 全球子公司數量的增加，他們實現了 CCoE 的半分散式模型，這樣每個地區的顧問和解決方案架構師都能夠更有效地為當地客戶提供服務。專注實踐和創新：

專注實踐和創新

成立 CCoE 後，Crayon 能夠專注於特定領域，如資料和人工智能，並不斷探索建立現代化 CCoE、雲端服務、容器、無伺服器等方面的可能性。

成就與影響

Crayon 通過其 CCoE 創建了超過 32 個新的可重複使用資產，支援了 70 多個客戶項目，並幫助超過 20 個子公司提供服務。

二、補充說明：

什麼是半分散式的 CCOE 模型?

半分散式的 CCOE（雲端卓越中心中心）模型是一種結構，其中 CCOE 的某些功能和責任在組織內部集中管理，而其他功能則分散到不同的業務單位或地理位置。這種模型旨在結合集中式和分散式 CCOE 模型的優點，以適應大型組織或具有多個子公司和業務單位的公司的需要。

半分散式 CCOE 模型的特點：

集中式治理和策略設定：組織的核心團隊或高層管理層負責確立雲策略、治理標準和最佳實踐，以保持整體方向和一致性。

地方自治：各業務單位或地理位置的團隊擁有在遵循集中制定的指導原則和標準的前提下，根據當地需求和特定情況自行做出決策的彈性。

共享資源和知識：中心 CCOE 與分散單位之間存在積極的知識共享和資源協作，以促進創新和效率。

可重用資產和實踐的標準化：雖然允許一定程度的地方自治，但組織仍鼓勵使用可重用的技術資產和標準化的工作流程，以提高效率和一致性。

半分散式 CCOE 模型的優點：

靈活性和響應性：允許地方團隊根據當地的市場需求和條件，快速做出響應和調整。

標準化與創新的平衡：結合了集中式規劃的一致性和地方執行的創新能力，促

進了最佳實踐的採納，同時也鼓勵了創新。

加強地方參與和認同感：地方團隊能夠在遵守總體戰略框架的同時，對其雲端倡議有更大的控制和貢獻，從而提高了項目的成功率和員工的滿意度。

透過半分散式的 CCOE 模型，組織可以在保持戰略一致性和效率的同時，利用分散團隊的地方知識和專長，從而在全球範圍內有效推進雲端轉型。

為何 CCOE 的建立使 Crayon 能夠專注於特定領域?

CCOE（雲端卓越中心中心）的建立使 Crayon 能夠專注於特定領域，原因包括以下幾點：

專業化和深度專長

CCOE 通過集中專業知識和資源，使組織能夠深入特定的技術或業務領域。這種專注促進了深度學習和專長的發展，使 Crayon 能夠在其選擇的領域（如資料和人工智慧）提供更高質量和更專業化的服務。

資源和知識的集中

透過在 CCOE 內集中資源和知識，Crayon 能夠建立強大的內部知識庫，包括最佳實踐、案例研究和可重用的技術資產。這種集中有助於加速創新並提高解決方案的交付效率，特別是在公司專注的領域內。

標準化和最佳實踐的推廣

CCOE 促進了標準化流程和最佳實踐的採用，這對於在特定技術領域保持一致性和質量至關重要。Crayon 能夠確保其在特定領域內的所有項目和服務都遵循相同的高標準和方法論。

鼓勵創新和專業發展

Crayon 的員工可以在其專業領域內探索新技術、開發創新解決方案並提升其專業技能。

增強市場定位和競爭力

專注於特定技術或業務領域使 Crayon 能夠在這些領域內建立強大的品牌和市場地位。這種專業化策略有助於吸引特定需求的客戶，並使公司在競爭激烈的市場中脫穎而出。

總體來說，CCOE 的建立為 Crayon 提供了一個框架，使其能夠集中資源、促進知識共享、鼓勵創新，並在其選擇的專業領域內追求卓越。這不僅提高了服務質量和客戶滿意度，也加強了 Crayon 在特定技術領域的專業地位和市場競爭力。

AI

導讀

在當今數位轉型的時代，電力公司面臨著前所未有的挑戰與機遇。隨著智慧電網的發展，電力系統變得更加複雜，需要即時、高效的資料處理與分析能力。AIOPS（人工智慧維運）在這方面扮演著關鍵角色，它結合了人工智慧（AI）、機器學習（ML）和大資料技術，能夠即時監控和分析電網狀態，預測和防範潛在故障，從而保證電網的穩定與可靠運行。對於電力公司而言，將AIOPS 整合到其混合雲架構中，不僅可以提升運營效率，還可以加快創新步伐，滿足日益增長的能源需求，同時確保資訊安全與合規性。

AI-driven adaptive engineering for all your cloud workloads (COP105)

這場演講強調了 AI 在雲運算工作負載管理中的應用，特別是在多雲環境下，企業如何利用 AI 技術應對運營挑戰，提升效率和創新能力。通過 Raiffeisen Bank 的案例分析，展示了上雲和 AI 整合的實際效益。

Implementing generative AI responsibly: A talk with Dr. Mitchell (IMP213)

Dr. Mitchell 討論了負責任地實施生成式 AI 的重要性，包括 AI 倫理、資料偏見問題和建立倫理框架的必要性。這對於電力公司在利用 AI 技術時保持社會責任和道德規範具有指導意義。

The real-time database to build your AI future (DAT206)

本場演講探討了實時資料庫在 AI 發展中的作用，特別是對於處理大資料和支持即時決策的重要性。透過 Aerospike 和 AWS 的合作案例，展示了實時資料庫在高壓環境下的應用。

AI amplified: Blueprint for elevating enterprise competitiveness (CEN401)

這場演講討論了 AI 如何幫助企業提升競爭力，包括 AI 轉型過程中的挑戰、建立「認知核心」的重要性，以及 AI 促進企業模式轉變的案例。

AI-driven adaptive engineering for all your cloud workloads (COP105)

圖說：演講開始前講者們密切討論。

隨著雲端運算的日益複雜化，企業如何有效管理其雲端工作負載，並充分利用 AI 技術來優化運營和提升效能？這場演講將探討這一問題，並以日立數位服務公司 CDO Prem 的演講為基礎，深入分析他對於 AI 驅動的雲端運營的看法。

在雲端運算的世界裡，工作負載管理的複雜性正隨著多雲環境的出現而增加。企業不僅需要在 AWS 上運行應用程式，還可能需要管理在其他雲平台上的工作負載，這對許多組織來說是一個巨大的挑戰。Prem 強調，當前的 IT 運營需要轉變為以工程為導向的營運模式，將雲端視為可透過程式碼訪問和管理的基礎設施。這種轉變不僅涉及到技術的革新，更需要對運營流程進行本質上的重構。

為了解雲端運營的現狀和挑戰，Prem 邀請了來自 Raiffeisen Bank 的 Michal 和 AWS 的合作夥伴 Andrea 分享他們的經驗和看法。Michal 詳細介紹了 Raiffeisen Bank 如何規劃和執行其上雲策略，這一策略不僅關注技術轉換，更重視業務模式的創新和敏捷性的提升。他強調，雲端轉型不僅是技術上的挑戰，更是組織文化和營運模式轉變的過程。

此外，Michal 和 Prem 都提到了 AI 技術在雲端運營中的重要性。隨著 AI 和生成式 AI（Generative AI）技術的發展，企業有機會進一步優化其雲端工作負載，從而提高效率和創新能力。這包括利用 AI 進行程式碼複雜性分析、安全掃描、財務運營優化等方面的應用。

Andrea 從 AWS 的角度出發，闡述了 AWS 如何通過其服務和工具支援企業客戶和合作夥伴。她提到了 AWS 的許多服務，如 Amazon Inspector、AWS Trusted Advisor 等，這些服務利用 AI 技術幫助客戶實現運營卓越、成本優化和安全合規。此外，AWS 對於支援企業應用生成式 AI 和其他先進 AI 技術也提

供了強大的基礎設施和平台。

總之，雲端運營的未來將更加依賴於以工程為導向的方法、AI 技術的深度整合以及與雲服務提供商如 AWS 的緊密合作。隨著技術的不斷發展和創新，企業需要不斷適應新的營運模式，以實現更高效、更安全、更具成本效益的雲端運營。

案例探討：Raiffeisen 銀行的雲旅程

Raiffeisen 銀行在其雲遷移和數位轉型過程中設定了遠大的目標，計畫在兩年內將 50%的應用程式遷移到雲端。這一策略不僅要求技術的轉變，更涉及到組織結構、營運模式和企業文化的調整。銀行的雲旅程可分為兩大階段：評估階段和實際遷移階段。

在評估階段，Raiffeisen 銀行重點選擇了能夠最佳支持各地市場優先事項和目標的應用程式。這一階段涉及到對選定應用的雲設計規劃、商業案例計算、合規性檢查，以及相應培訓的安排。此外，銀行在此階段對總體雲架構進行了大量工作，包括網絡設置、安全提升以及帳戶管理流程的強化。

進入實際遷移階段後，遷移工作被劃分為一系列的疊代，每個疊代處理特定的應用遷移，並在完成後進行切換和特別關注（hypercare）階段。在這一階段，Raiffeisen 銀行開始部分汰換原有基礎設施，以實現成本效益和提升效率。

在整個過程中，AI 和生成式 AI 的應用發揮了關鍵作用。Raiffeisen 銀行利用 AI 工具分析程式碼的複雜性，以便於重構，並利用生成式 AI（例如 GitHub Copilot）來生成遷移應用時所需的程式碼。此外，銀行在運行階段使用 AI 工具進行安全掃描，提前發現和修復潛在的安全問題，並且正在選擇使用 AI 驅動的財務運營（FinOps）工具，以提高雲成本管理的效率。

AWS 的支持

AWS 透過其合作夥伴網絡和一系列工具和服務，為 Raiffeisen 銀行等客戶提供了強大的支持，特別是在利用 AI 和生成式 AI 優化雲運營方面。Andrea 從 AWS 的角度強調了與 AWS 合作的優勢，包括訪問先進的基礎設施、利用 AWS 的最佳實踐和框架，以及快速採用新技術的能力。

AWS 的基礎設施層提供了豐富的 AI 工具和服務，如 Amazon Inspector、AWS Security Hub 和 AWS Trusted Advisor 等，這些服務幫助企業實現成本優化、安全合規和運營卓越。這些工具利用 AI 技術自動識別潛在的問題，並提供改善建議。

在應用層面，AWS 提供了如 Amazon SageMaker、Amazon Comprehend、Amazon Lex 等服務，支援企業開發和部署 AI 和機器學習模型。最近，AWS 推出的 Amazon Q 等服務使得企業能夠更輕鬆地利用生成式 AI，例如快速開發聊天機器人或自動化內容創建。

Andrea 還提到了 AWS 的合作夥伴網絡和良好架構框架（Well-Architected Framework），這些資源為企業提供了實現雲運營卓越的指南和最佳實踐。透過這些支持，AWS 使得客戶如 Raiffeisen 銀行能夠更有效地規劃和執行其雲遷移策略，同時充分利用 AI 和生成式 AI 的優勢來創新和優化運營。

Raiffeisen 銀行的雲旅程體現了一個組織如何結合策略性規劃、技術創新和強有力的合作夥伴支持來實現雲遷移和數位轉型。AWS 作為一個平台和合作夥伴，為此提供了必要的技術支持和專業知識，特別是在利用最新的 AI 和生成式 AI 技術方面。

補充：Raiffeisen 銀行

Raiffeisen 銀行是一家具有長遠歷史的國際銀行集團，其根源可以追溯到 19 世紀中葉的歐洲。這家銀行是以其創辦人 Friedrich Wilhelm Raiffeisen 的名字命名，他是一位德國社會改革者，致力於改善農民的經濟狀況。

Raiffeisen 銀行的獨特之處在於其合作社的業務模式，這種模式鼓勵成員之間的相互協助和支持。這家銀行最初是為了提供給農村社區的小型貸款而設立的，目的是幫助農民克服貧困，並提升他們的經濟地位。隨著時間的推移，Raiffeisen 銀行逐漸發展成為一家全面的金融服務機構，為個人、企業以及其他組織提供廣泛的金融產品和服務。

今天，Raiffeisen 銀行集團在全球多個國家和地區經營，尤其在東歐和中歐地區擁有強大的市場地位。這家銀行以其穩健的銀行業務實踐、客戶導向的服務以及對社區的承諾而聞名。

除了傳統的銀行業務外，Raiffeisen 銀行還積極參與社會責任活動，支持各種社會和環境項目，致力於可持續發展和社會福祉。這使得 Raiffeisen 銀行不僅僅是一家金融機構，更是一個積極參與社會改善的組織。

參考網址

https://www.rbinternational.com/en/raiffeisen.html

Implementing generative AI responsibly: A talk with Dr. Mitchell (IMP213)

圖說：Dr. Margaret Mitchell(左)與 Rebecca Gonzales(右)。

在這場演講中，Dr. Margaret Mitchell 與 Rebecca Gonzales 聚焦於負責任地實施生成式人工智慧的關鍵要點和思考。我們將以資訊科技專業人士為目標讀者，用深入且全面的角度來解析這場談話的精華，以及它對當前人工智慧領域的意義。

生成式 AI 的倫理實踐

在對話中，Dr. Mitchell 分享了她在 Hugging Face 擔任首席倫理科學家的經驗，以及如何在機器學習開發、生態系統資料治理、AI 評估和 AI 倫理方面推動前進。這一段對話強調了在技術創新的同時，如何保持對社會責任和倫理的重視，尤其是在生成式 AI 技術迅速發展的背景下。

價值觀衝突與倫理框架的深入探討

在技術創新的世界中，尤其是在迅速發展的人工智慧領域，價值觀衝突是一個無法回避的議題。這種衝突往往源於不同利益相關者，從開發者、研究人員到商業領導者，對於應該如何平衡創新與倫理責任的不同看法。Mitchell 博士在提及 OpenAI 的例子時，特別強調了這一點。她認為，建立一個全面的倫理框架，並在組織內部就核心價值觀達成共識，是解決這種價值觀衝突的關鍵。這樣的框架不僅有助於明確指導決策過程，還能確保技術的發展與組織的核心價值觀保持一致，從而實現商業目標與社會責任的平衡。

資料偏見與責任的深入剖析

Mitchell 博士分享的 AI 系統資料偏見的例子，突顯了資料在形塑 AI 行為中的關鍵作用。這一例子揭示了 AI 系統可能會因為訓練資料的偏差而產生錯誤或不當的反應，從而對特定群體或情境造成不利影響。因此，開發者在設計 AI 系統時必須深入理解資料背後的脈絡，並主動尋找減少偏見和增強公正性的方法。這要求開發者不僅要關注技術的精準度和效能，更要重視其對社會價值觀的貢獻與影響，確保技術創新與人類價值觀相輔相成。

多樣性與包容性的重要性與實踐

在 Mitchell 博士的談話中，建立一個多元化且包容的團隊被視為實現負責任 AI 的基石。透過吸引來自不同學科、文化和背景的人才，一個團隊可以從更廣泛的視角來審視技術開發過程中可能遇到的挑戰和機遇。這種跨學科的合作模式不僅促進了創新思維的碰撞，還有助於團隊成員更全面地理解技術對不同群體可能產生的影響。此外，強調溝通與協作的能力，有助於團隊成員之間建立信任，並在共同的目標下高效合作。透過這種方法，技術開發不僅能夠響應市場需求，還能夠敏感地處理社會倫理問題，從而推動更加負責任和可持續的技術創新。

生成式 AI 的未來方向

最後，對話展望了生成式 AI 的未來，特別是在資料處理和模型透明度方面。Mitchell 博士和 Gonzales 討論了如何通過更好的資料治理、模型評估和持續的倫理審查來推動這一領域的負責任發展。他們強調了開放源碼模型與封閉模型在促進創新和倫理實踐方面的不同作用，以及如何通過教育和多樣性來加強整個行業的倫理標準。

補充-講者介紹

Dr. Margaret Mitchell 是一位在人工智慧領域內享有盛譽的科學家，尤其在機器學習、自然語言處理、計算機視覺、AI 倫理和負責任 AI 的研究中成果豐碩。她的工作重點在於如何使 AI 技術更加公正、透明和負責任，特別是在處理敏感的社會和倫理問題上。

Mitchell 在學術和工業界都有著豐富的經歷。她曾在谷歌 AI 工作，並創立了谷歌的倫理 AI 團隊，該團隊專注於基礎 AI 倫理研究和將 AI 倫理原則落到實處。在此之前，她還在微軟研究院從事計算機視覺到自然語言生成的研究工作，並在約翰霍普金斯大學擔任博士後研究員。

Mitchell 博士持有來自華盛頓大學的計算語言學碩士學位和來自阿伯丁大學的科學博士學位。她的學術貢獻包括發表了大量關於自然語言生成、輔助技

術、AI 倫理等領域的論文，並且擁有多項專利。

除了她在技術開發和研究方面的工作，Mitchell 博士還積極參與公共對話，提高公眾對 AI 倫理問題的認識。她的 TED 演講《我們如何建造既幫助人類又不傷害人類的 AI》觀看次數超過 130 萬次，顯示了她在這一領域的影響力和公眾對這一話題的興趣。

最近，Mitchell 博士加入了 Hugging Face，擔任首席倫理科學家，她在那裡繼續推動負責任的 AI 開發，並促進開放和包容性的 AI 研究社區建設。她的工作不僅對 AI 技術的發展產生了深遠的影響，也對確保這些技術的應用能夠符合更廣泛的社會價值和倫理標準起到了關鍵作用。

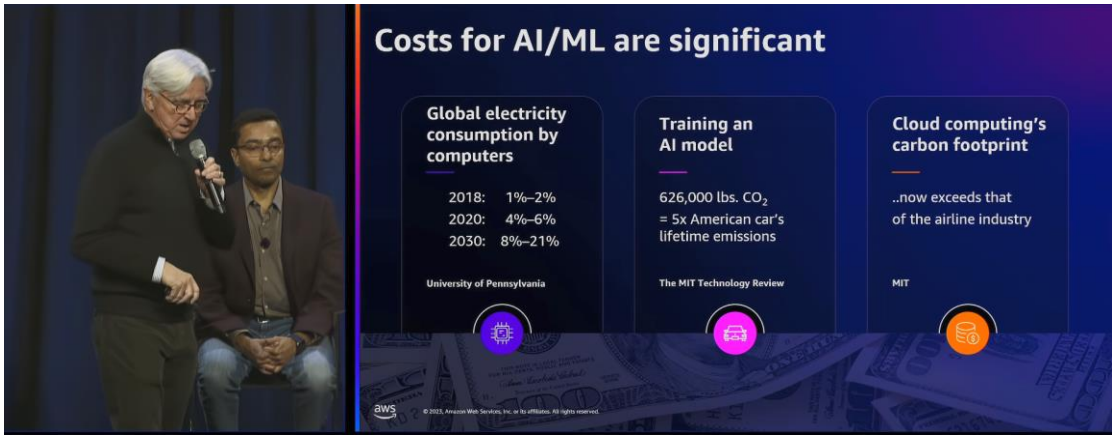
The real-time database to build your AI future (DAT206)

在當今的數位時代，人工智慧（AI）和機器學習（ML）的突破正在迅速改變我們處理資料和實現創新的方式。本場演講深入探討了這個主題，特別是圍繞實時資料庫的應用，這對於構建我們的 AI 未來至關重要。本文將對這場講座的要點進行深入分析，並討論其對技術社群，特別是 IT 專業人員的重要性。

AI 的壓力與成本

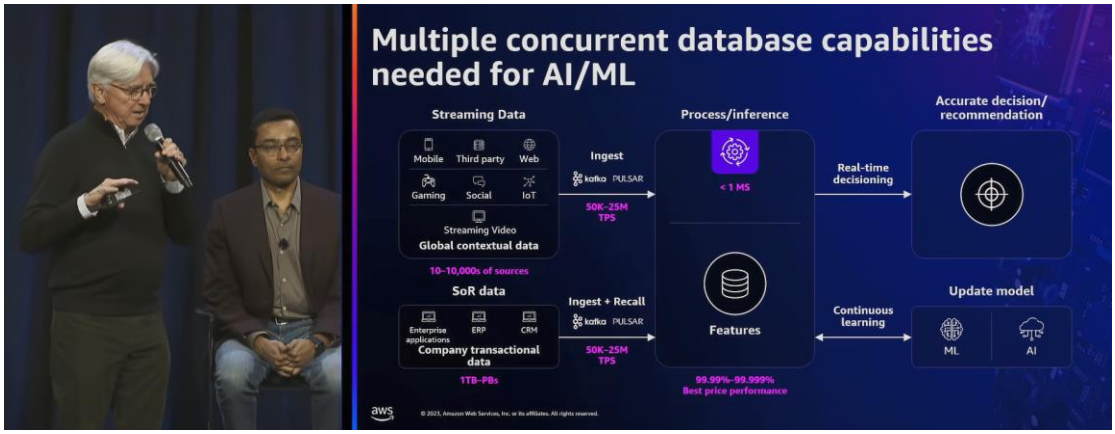
在開場白中，Lenley Hensarling 強調了利用 AI 技術的極端壓力，以及隨之而來的成本問題和對資料的持續需求。這一挑戰在業界普遍存在，許多組織都在尋求解決方案。AI 的應用雖然能夠為業務帶來效率提升和成本節省，但實際操作中卻伴隨著計算能力和儲存需求的大幅增加。

能耗與永續性



圖說：隨著計算對整體電力消耗的比例從 2018 年的 1-2%預計到 2030 年將增加到 8-21%，AI 模型訓練所消耗的碳足跡及其對能源消耗的影響成為了一個不容忽視的問題。這一挑戰迫使行業必須在推動技術創新的同時，也要關注其環境影響。

資料的海量需求



圖說：處理大量資料是實現 AI 應用的一個關鍵環節，無論是生成大型語言模型（LLM）還是操作資料的應用。即時資料的應用要求企業不斷地吸收資料，以便能夠即時做出決策。這就需要

一個強大的資料平台來支撐，以確保資料的及時處理和應用。

Aerospike 作為特徵儲存的選擇

在講座中，兩位演講者分享了他們如何使用 Aerospike 作為特徵儲存，以及為何選擇它的原因。Aerospike 的高效能和能夠在時間受限的服務水平協議（SLA）中處理更多資料的能力是其被選中的主要原因。Quantcast 和一家日本電子商務公司的案例展示了 Aerospike 在處理海量資料和實現即時上下文中的強大能力。

AWS 和 Aerospike 的合作

這種合作使得 Aerospike 能夠在保證性能的同時，也優化成本效益。

補充

Aerospike 的選擇理由

Aerospike 被選為特徵儲存的主要原因在於其出色的性能和高效能。在處理大規模資料集時，Aerospike 能夠提供極低的延遲和高吞吐量，這對於需要即時響應的應用來說至關重要。此外，Aerospike 的設計允許它在嚴格的服務水平協議（SLA）條件下運行，確保即使在高負載下也能保持一致的性能。

實際應用案例

講座中提到的兩個案例 Quantcast 和一家日本電子商務公司展示了 Aerospike 如何滿足特定的業務需求。

Quantcast 的應用：Quantcast 利用 Aerospike 來處理其龐大的資料集，其中包括超過 10 億條記錄和 8TB 的資料儲存。Aerospike 的高效資料處理能力使 Quantcast 能夠即時獲取歷史上下文資料，並在 1 毫秒內完成查詢，從而提供極其迅速的決策支持。

日本電子商務公司的應用：這家公司利用 Aerospike 來支持其即時電子商務平台，特別是在跟踪和反應於快速變化的時尚趨勢方面。例如，當一位名人改變了穿著的風格或顏色時，該平台能夠即時更新，並將最相關的商品推薦給消費者。這種能力依賴於 Aerospike 的即時資料處理和高效能特性。

Aerospike 的技術優勢

Aerospike 之所以能夠在這些應用中表現出色，很大程度上歸功於其獨特的技術架構和功能：

分佈式架構：Aerospike 的分佈式設計使其能夠橫向擴展，處理更多的資料和請求，而不會降低性能。
高效能儲存：Aerospike 利用內存和 SSD 的結合，提供了快速的資料訪問速度和大容量儲存，這對於特徵儲存來說是關鍵。
即時處理：Aerospike 的能力不僅限於儲存，它還能夠即時處理資料，使得即時分析和決策成為可能。

Riskified：防範欺詐的應用

Riskified 是一家提供電子商務欺詐預防解決方案的公司，通過分析和評估交易的真實性來幫助商家減少損失。在這個過程中，Riskified 需要處理和分析來自全球各地數以百萬計的交易資料，這些資料量巨大且需求迅速響應。
資料處理： Riskified 利用 Aerospike 作為特徵儲存，以高效地處理和儲存大量交易資料。Aerospike 的低延遲和高吞吐量能力使 Riskified 能夠即時分析交易，快速識別潛在的欺詐行為。
即時決策： 在電子商務領域，即時決策至關重要。Aerospike 支持 Riskified 在毫秒級別內做出交易是否存在欺詐風險的決策，從而保護商家免受損失。
FreeWheel：廣告技術的應用
FreeWheel 是一家提供廣告技術解決方案的公司，專注於幫助媒體公司和廣告商在多個平台上有效地投放廣告。在這個行業，能夠快速處理大量的廣告請求並即時做出決策是成功的關鍵。

Aerospike 的應用：

高吞吐量和低延遲： FreeWheel 使用 Aerospike 來處理每天數十億的廣告請求，其分佈式架構和高效能確保了即使在極高的請求量下也能保持低延遲。
即時資料分析： Aerospike 的高效資料處理能力使 FreeWheel 能夠即時分析廣告請求，並根據廣告商的需求和用戶的行為特徵即時定制廣告內容。

AI amplified: Blueprint for elevating enterprise competitiveness (CEN401)

隨著人工智慧（AI）和生成式人工智慧（Generative AI）的興起，企業如何利用這些技術來加速成長、提高效率並建立聯繫生態系統，成為業界熱烈討論的主題。這場演講深入了解了企業如何利用 AI 來重塑業務模式並推動創新。

AI 於企業中的運用現狀

在進行 AI 轉型的過程中，許多企業面臨著挑戰。根據針對超過一千名商業和 IT 高管的調查顯示，只有約四分之一的企業對其 AI 項目感到滿意。這一低滿意度背後的主要原因是缺乏明確的商業策略和資料準備不足。這兩個因素是 AI 項目成功的關鍵，缺乏其中任何一項都可能導致項目未能達到預期目標。因此，企業必須在投入 AI 之前明確其商業目標，並確保有足夠的、結構化的、可用的資料來支撐 AI 應用的開發和部署。

資料驅動的核心轉型

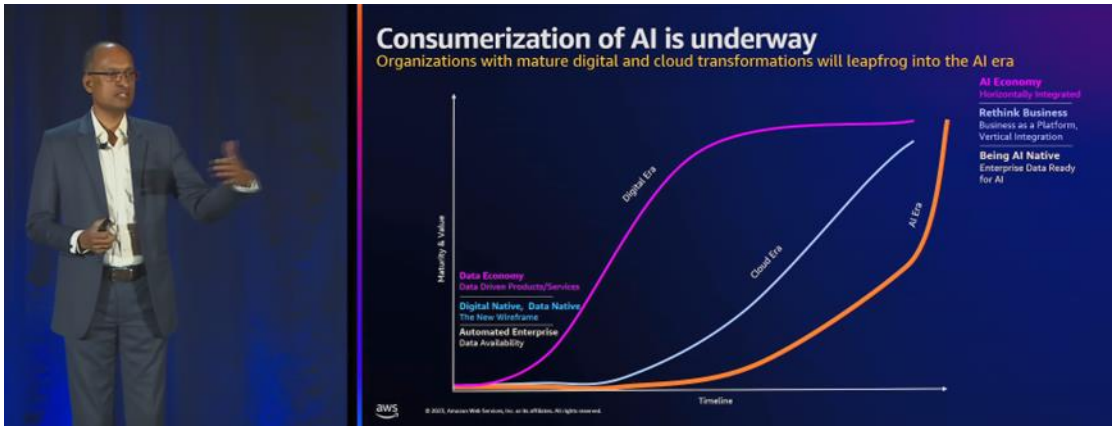
隨著企業逐步從資料驅動轉向 AI 驅動，建立一個稱為「認知核心」的新基礎變得至關重要。這個認知核心是指利用 AI 技術來處理和分析資料，從而支持更加智能的決策制定和業務流程。為了建立認知核心，企業需要加強人機協作，確保人員能夠有效地與 AI 系統合作，以提高工作效率和創新能力。此外，強化資料治理，確保資料的質量和安全，以及建立一個靈活且可擴展的資料架構，是支持 AI 廣泛應用的基礎。

重塑業務模式

AI 技術的引入促使企業必須重新審視和調整其業務模式。透過 AI 的加入，企業能夠推動內部的數位轉型，提高運營效率和創新能力。更重要的是，AI 促進了企業間的垂直整合和生態系統的建立，這不僅加強了企業與其客戶、供應商和合作夥伴之間的協作，也為創新商業模式提供了可能。因此，企業需要思考如何利用 AI 來重構其業務平台，以及如何通過這一平台來促進更廣泛的合作和價值創造。

資料與 AI 經濟

在 AI 時代，資料成為了企業的核心資產和競爭優勢的來源。企業通過橫向整合，即與不同行業的企業進行合作，能夠創建一個新的由資料和 AI 驅動的經濟體。這種跨行業的合作使企業能夠共享和整合各自的資料和 AI 能力，從而開創新的收入來源和商業模式。這一轉變不僅有助於企業在競爭激烈的市場中保持領先地位，也為行業創新和跨界合作提供了豐富的機會。



圖說：這張圖顯示了組織在數位化和雲端轉型的過程中成熟度和價值隨時間增長的路徑，並且進入到 AI 時代的轉變。這個轉變被劃分為數個階段：

1. **自動化企業（Automated Enterprise）**：這個階段著重於使資料可用性達到最大化，以自動化為基礎，提升企業運營的效率。
2. **數字原生（Digital Native），資料原生（Data Native）**：接下來的階段強調的是創建一種新的線框（Wireframe），將數位化和資料化深入整個企業文化和流程。
3. **資料經濟（Data Economy）**：發展到資料驅動產品和服務的階段，這是企業利用資料來創造新的商業模式和收入來源。
4. **AI 時代的開始**：
    - **AI 本土化（Being AI Native）**：企業要準備好進入 AI 時代，需要讓企業資料準備就緒以適應 AI 的需求。
    - **重新思考業務（Rethink Business）**：企業應該將業務視為一個平台，進行垂直整合，從而增強其價值創建的能力。
    - **AI 經濟（AI Economy）**：這是個企業可以進行水平整合，與其他行業進行合作，創造跨行業的資料和 AI 生態系統。

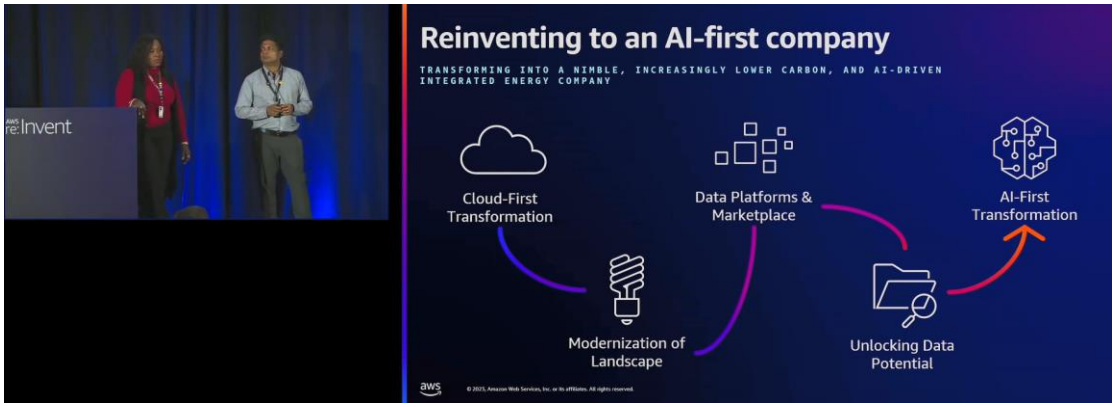
BP 的雲端轉型和 AI 策略

BP 是一家跨國能源公司,其轉型案例突顯了如何透過雲端轉型和 AI 應用來加速向低碳能源轉型的步伐。BP 進行了幾項關鍵的轉型活動:

關閉資料中心：BP 透過關閉其全球範圍內的多個大型資料中心，減少了對傳統 IT 基礎設施的依賴。這一舉措不僅減少了營運成本，也降低了碳排放，符合其可持續發展的目標。

優化雲端架構：BP 積極將其 IT 系統和應用遷移到雲端，這不僅提高了資料處理和儲存的靈活性，也加快了新應用的開發和部署速度。雲端架構的優化使 BP 能夠更快地響應市場變化，並支持其業務創新。

實施 AI 策略：BP 利用 AI 技術來優化其運營效率和決策制定過程。例如，BP 在其生產優化和低碳資產管理中使用 AI，以提高能源效率並減少二氧化碳排放。這些 AI 應用有助於 BP 在能源轉型中保持領先地位。



圖說：這張圖展現了一家企業轉型為 AI 首選公司的過程。圖片分為三個階段：

1. **雲端優先轉型（Cloud-First Transformation）**：這是企業轉型旅程的起點，強調將業務和服務遷移到雲端的重要性。
2. **資料平台和市場（Data Platforms & Marketplace）**：在成功轉移到雲端之後，下一步是創建資料平台，這些平台能夠收集、整合和分析資料，從而提供洞見並為決策提供支持。
3. **現代化業務景觀（Modernization of Landscape）** 和 **解鎖資料潛力（Unlocking Data Potential）**：這兩個階段相互關聯，指出企業需要通過現代化其技術堆棧來為 AI 轉型鋪路，並發掘其資料的全部潛力。
4. **AI 首選轉型（AI-First Transformation）**：最後一步是全面實施 AI 首選策略，這不僅僅涉及技術的應用，還包括文化和營運模式的轉變。

Citizens Bank 的數位化和 AI 應用

Citizens Bank 是一家主要在美國經營的銀行，其案例展示了如何透過數位化和 AI 來加速金融服務的創新，從而為客戶提供更便捷、更個性化的服務，列述如下：

數位化服務

Citizens Bank 通過推出數位點對點銷售經驗和線上服務平台，使客戶能夠隨時隨地進行銀行業務操作，從而提高了客戶體驗的便捷性和滿意度。

利用 AI 提升決策制定

Citizens Bank 利用 AI 技術來分析客戶資料，從而提供更加個性化的金融產品和服務。例如，AI 技術幫助銀行優化了房屋淨值貸款（HELOC）的審批流程，將審批時間從數週縮短到數天，大大提高了效率和客戶滿意度。

AI 驅動的創新金融產品

透過 AI 分析和機器學習，Citizens Bank 能夠開發出符合客戶需求的新金融產品，如即時貸款批准和個性化的財務規劃建議，進一步加強了其市場競爭

力。

這兩個案例展示了不同行業如何透過雲端轉型和 AI 技術的應用來推動業務創新、提高運營效率並加強客戶關係。BP 和 Citizens Bank 的經驗為希望透過技術轉型實現業務增長和效率提升的企業提供了寶貴的參考。

結語

AI 和生成式 AI 為企業帶來了前所未有的機遇，但同時也伴隨著挑戰。企業必須建立清晰的商業策略、加強資料治理，並不斷探索新的業務模式和合作機會。透過持續的創新和適應，企業能夠在 AI 時代中脫穎而出，成為各自行業的領導者。

補充：Citizens Bank 介紹

Citizens Bank 是一家美國的商業銀行，擁有深厚的歷史背景和廣泛的業務範圍。這家銀行的起源可以追溯到 1828 年，在賓夕法尼亞州的普羅維登斯市成立，最初是作為一家小型社區銀行開始其業務的。經過近兩個世紀的發展，Citizens Bank 已經成長為在美國具有顯著影響力的金融機構之一。

在規模方面，Citizens Bank 是美國最大的銀行之一，擁有豐富的客戶基礎和廣泛的分行網絡。它在多個州設有分行，尤其是在新英格蘭地區和中大西洋地區，提供各種銀行服務和金融解決方案。此外，Citizens Bank 也是一家上市公司，其股票在紐約證券交易所交易。

在業務範圍方面，Citizens Bank 提供廣泛的金融服務，包括個人銀行業務、商業銀行業務、財富管理和資產管理服務。對於個人客戶，它提供儲蓄帳戶、支票帳戶、信用卡、住房貸款和個人貸款等服務。對於商業客戶，Citizens Bank 提供商業貸款、信用線、現金管理和貿易融資服務。此外，它還為客戶提供投資和退休計劃服務，以幫助他們達成長期的財務目標。

參考網址

https://www.citi.com/

資料驅動

導讀

資料驅動對於智慧電網和電力公司而言，意義重大，尤其是在混合雲環境中更是如此。資料驅動的方法不僅能夠提高電網的效率和可靠性，還能夠幫助電力公司更好地管理和預測能源需求，從而優化能源分配和減少浪費。

在混合雲環境下，電力公司能夠利用雲計算的彈性和擴展性來處理和分析大量的資料。這些資料來自於各種來源，包括智能計量設備、感測器、天氣預報以及用戶消費模式等。通過對這些資料的深入分析，電力公司不僅能夠即時響應電網狀態的變化，還能夠預測未來的趨勢和挑戰，從而進行更有效的規劃和決策。

此外，資料驅動的方法還支持電力公司在可持續性和環保方面的努力。通過分析能源消耗資料和二氧化碳排放資料，公司能夠識別減少能源消耗和減少環境影響的機會。這不僅有助於滿足政府和消費者對於環保的要求，也有助於提高企業的社會責任形象和市場競爭力。

One data platform for reporting, analytics, and ML (FSI317)

在摩根大通針對報告、分析和機器學習開發的統一資料平台項目中，我們看到了如何利用雲技術，特別是 AWS，來應對金融服務行業中的資料處理和分析挑戰。通過實施這一平台，摩根大通成功地提升了資料處理的效率和可靠性，實現了資料質量的顯著改善。這一變革不僅加快了資料上線的速度，也增強了公司在資料分析和機器學習領域的能力，從而在競爭激烈的金融市場中保持領先。

Using AI for ESG reporting and data-driven decision-making (SUS204)

這場演講展示了如何利用 AI 技術來改善 ESG（環境、社會和治理）報告的流程，並利用資料驅動的方法來支持決策制定。通過 AWS 的 AI/ML 服務，企業能夠提高 ESG 報告的效率和準確性，同時實現對相關資料的即時監控和分析。這不僅有助於企業更負責任地做出決策，也支持了企業在可持續性目標上的進展。

JPMorgan Chase：One data platform for reporting, analytics, and ML (FSI317)

摩根大通分享了他們一個集報告、分析和機器學習於一體的統一資料平台。本場演講深入探討摩根大通如何應對業務挑戰，並通過上雲實現業務轉型。

圖說：演講者正在介紹 J.P. Morgan Asset Management，突出了三個關鍵點：該公司的定位，成長的驅動因素，以及它們獨特之處難以被複製。具體來說，她提到公司管理著 2.9 萬億美元的資產，擁有超過 1200 名投資專業人士和 600 多種投資策略。這些都顯示了公司的規模、專業知識和多樣性。

摩根大通資產管理的核心：資料與創新

摩根大通資產管理部門是全球最大的資產管理公司之一，管理著 2.9 萬億美元的資產。該公司依靠其 1,200 名投資專業人員，為全球各大市場的客戶提供服務，範圍涵蓋大型機構、資產所有者到零售中介和財務顧問。在這樣一個多元化的客戶基礎中，資料和對資料的文化是業務的核心。

摩根大通每年投入 150 億美元於技術和資料，支持近 6 萬名工程師，以推動業務的持續創新和競爭力。資料平台 AM IQ 的建立，正是為了滿足不同用戶群的需求，從銷售團隊到市場團隊，再到客戶本身，每個人都依賴於平台提供的資料來驅動決策。

面臨的挑戰與上雲的驅動力

摩根大通資產管理在業務擴展過程中遇到了多重挑戰，主要集中在基礎設施擴展、新策略快速部署以及建立一個能夠支持多種業務的多功能平台上。隨著業務的不斷增長和多樣化，現有的基礎設施難以滿足日益增長的資料處理需求，而傳統的基礎設施擴展方式又過於耗時且不夠靈活。此外，快速部署新策略以應對市場變化成為另一大挑戰，這要求平台能夠迅速適應新的業務需求並支持新服務的快速上線。

上雲提供了解決這些挑戰的一個有效途徑，因為雲技術以其規模彈性、部

署速度和高度靈活性而著稱，能夠迅速應對業務需求的變化。然而，金融行業的嚴格監管要求對雲服務的選擇和使用提出了額外的限制，這意味著摩根大通在進行上雲時不得不在遵守監管要求和實現技術創新之間尋找平衡，做出相應的妥協和調整。

架構與技術挑戰

摩根大通資產管理的資料平台架構旨在從根本上解決這些挑戰，通過整合 AWS 提供的多項服務，包括 S3、EMR 和 Redshift，構建了一個強大而靈活的資料處理和分析平台。這個架構支持從內部和外部來源每天攝取數千個資料集，處理數十億條記錄，並生成多達 6,000 份報告，從而滿足了業務對資料處理能力和報告生成需求的增長。

為了提升資料質量和流程的可靠性，摩根大通開發了一系列內部工具和框架，這些工具和框架對 AWS 的原生組件進行了增強和補充。其中包括一個資料攝取框架，用於簡化從多樣化資料源攝取資料的過程，以及一個基於規則的資料處理引擎，使得業務用戶和資料工程師可以通過簡單的配置來定義和運行複雜的資料處理流程。

成果與啟示

通過這個先進的資料平台，摩根大通資產管理不僅大幅削減了成本，提高了業務響應速度，還增強了創新能力。平台的成功部署大大縮短了新資料上線的時間，從之前的幾周甚至幾個月縮短到了幾小時，這使得業務團隊能夠快速響應市場變化，驗證和推廣新策略和產品。更重要的是，這個平台確保了資料處理過程的質量和可靠性，為業務決策提供了堅實的資料支持。

這一成就不僅展示了雲技術在金融服務行業中的應用潛力，也為其他企業提供了寶貴的經驗：在面對基礎設施擴展、新策略部署和多功能平台建設等挑戰時，通過上雲和內部創新可以有效提升業務的敏捷性和創新能力。摩根大通資產管理的案例證明，即使在嚴格監管的行業中，通過巧妙設計和技術創新也能夠實現上雲的成功，為企業帶來長遠的業務價值。

Using AI for ESG reporting and data-driven decision-making (SUS204)

在這次演講主題為「運用 AI 於 ESG 報告和資料驅動的決策制定」。本次演講由 Aditi Suresh，AWS 全球專家組織的可持續性專家，以及 Brian Rowe，Rehrig Pacific 公司資訊安全與 IT 部門的總監，共同主持。Rehrig Pacific 公司是廢物回收和供應鏈解決方案領域的行業領導者。在本文將重點闡述他們如何透過 AI 技術改善 ESG（環境、社會和治理）報告流程，並展示 AWS 的 AI/ML（人工智能/機器學習）功能如何在此過程中發揮關鍵作用。

圖說：ESG 報告包括了多種非財務因素。ESG 代表環境（Environmental）、社會（Social）和治理（Governance），這三個元素被視為公司可持續性和社會責任的關鍵方面。

ESG 報告的挑戰與趨勢

隨著全球對於企業可持續性的關注日益增加，ESG 報告已成為企業透明度和責任的關鍵指標。然而，傳統的 ESG 報告過程面臨著多項挑戰，包括資料收集的繁瑣、資料質量的不一致性以及缺乏統一的報告框架。此外，隨著相關法規和標準的不斷演進，企業在遵循最新規定和最佳實踐方面也面臨壓力。

AI 在 ESG 報告中的角色

AI 技術，特別是機器學習和深度學習，提供了一種革新性的方法來克服傳統 ESG 報告中的挑戰。通過自動化資料收集和處理、提高資料質量和一致性，以及能夠快速適應不斷變化的報告要求，AI 技術為 ESG 報告帶來了前所未有的效率和準確性。

AWS AI/ML 在 ESG 報告中的應用

AWS 提供了一系列先進的 AI/ML 服務，幫助企業實現更高效、更準確的 ESG 報告。這些服務包括但不限於 Amazon Textract（用於自動化文件處理和資料提取）、Amazon SageMaker（用於構建和訓練機器學習模型）、以及 Amazon Kendra（一種智能搜尋服務，可從分散和非結構化的資料源中快速獲得答案）。

實踐案例：Rehrig Pacific 公司的 ESG 報告之旅

Rehrig Pacific 公司的 ESG 報告之旅展現了一家擁有 110 年歷史的家族企業如何透過先進的 AI 技術和 AWS 的協助，徹底轉型其環境、社會與治理（ESG）報告流程。以下是這趟旅程的關鍵階段和成果：

公司背景與文化

Rehrig Pacific 公司最初從事木材產品的製造，隨著時間的推移，轉型成為一家塑膠產品製造商。儘管業務範圍和材料發生了變化，但公司一直堅持可持續性和循環利用的理念。作為一家技術驅動的公司，Rehrig Pacific 致力於透過創新解決方案，提升供應鏈和廢物回收行業的可持續性。

ESG 報告的挑戰

Rehrig Pacific 面臨著 ESG 報告的多項挑戰，包括手動資料收集的低效率、資料質量的不一致性，以及缺乏即時分析能力。這些挑戰導致公司難以準時準確地完成 ESG 報告，並限制了根據這些報告做出及時決策的能力。

資料自動化與 AWS 的應用

為了解決這些問題，Rehrig Pacific 決定採用 AWS 的 AI/ML 服務，包括 Amazon Textract 用於自動化文件處理和資料提取，Amazon SageMaker 用於構建和訓練機器學習模型，以及其他服務來提高資料處理的效率和準確性。這些技術的應用使得公司能夠自動化以前需要大量手動工作的過程，從而提高效率並降低錯誤率。

合作夥伴的角色

在這一轉型過程中，Rehrig Pacific 與 FlexZero 合作，後者是一家專門提供 ESG 報告解決方案的 AWS 合作夥伴。FlexZero 的平台使 Rehrig Pacific 能夠更有效地收集和處理 ESG 相關資料，並提供即時分析和看法，幫助公司更好地理解其運營對環境的影響。

實現成果

通過轉型其 ESG 報告流程，Rehrig Pacific 實現了多項重要成果，包括：

1. **資料收集自動化**：自動化過程減少了手動資料輸入的需要，從而提高了資料收集的效率和準確性。
2. **即時分析與看法**：通過 AWS 的 AI/ML 服務，Rehrig Pacific 能夠即時分析 ESG 資料，並根據這些資料做出更加負責任和資料驅動的決策。
3. **可持續性目標的進展**：自動化和即時分析使公司能夠更有效地追踪其對可持續性目標的進展，並及時調整策略以達成這些目標。

未來展望

Rehrig Pacific 計劃進一步深化其與 AWS 和 FlexZero 的合作，以探索更多利用 AI 和機器學習改善 ESG 報告和可持續性管理的機會。公司將繼續尋找新的方法來減少其運營的環境影響，並通過創新和技術提高整個供應鏈的可持續性。

補充：Rehrig Pacific 公司介紹

Rehrig Pacific 公司是一家專注於提供物流解決方案的公司，特別擅長製造可持續和創新的包裝和物流產品。該公司成立於 1913 年，擁有超過 100 年的歷史，最初是以生產木製製品開始其業務，隨著時間的推移，逐步轉型為塑料產品的製造和創新包裝解決方案的提供者。

Rehrig Pacific 的業務範圍廣泛，覆蓋了多個市場和行業，包括飲料、乳製品、烘焙、農業、食品服務、零售、環境以及供應鏈物流等領域。公司致力於開發和生產各種塑料包裝容器、托盤、垃圾桶和回收桶等產品，這些產品不僅耐用且環保，還能提高客戶的供應鏈效率和可持續性。

Rehrig Pacific 公司在創新方面有著深厚的積累，不斷地採用先進的技術和材料來改善和優化其產品設計。公司還提供定制化的解決方案，以滿足特定客戶的獨特需求，幫助他們解決物流和供應鏈中的挑戰。

在全球化的背景下，Rehrig Pacific 也擴展了其國際業務，擁有多個製造設施和銷售辦公室，服務於全球各地的客戶。公司的目標是通過其創新的產品和服務，推動行業發展，並為實現更加可持續和高效的全球供應鏈作出貢獻。

參考網址

https://www.rehrigpacific.com/

韌性

導讀

在當今數位化迅速發展的時代，「韌性」已成為智慧電網、電力系統、電力公司以及能源產業不可或缺的關鍵。韌性指的是在面對各種預料之外的事件時，如自然災害、網絡攻擊、人為錯誤等，組織能夠迅速恢復正常運作的能力。這不僅涉及到技術層面的恢復能力，還包括組織、流程、人員以及資訊系統的應對機制。

在資訊系統的領域，韌性特別關注於保護和恢復關鍵的 IT 基礎設施和資料，以確保即使在遭遇重大打擊時，系統仍能繼續運行或迅速恢復。這包括備份和災難恢復計劃、多重資料中心策略、雲端服務的彈性以及網絡安全防護措施。這些措施的目的是保證即使在面對如網絡攻擊這樣的數位威脅時，電力和能源系統的關鍵操作也不會中斷。

AWS Resilience Partners Best practices to create a resilient organization (PEX210)

本場演講由來自 AWS 的 Ashu 主講，他分享了建立組織韌性的最佳實踐，並強調了 AWS 韌性能力認證對於確保業務連續性的重要性。演講中，Cigna 的案例展示了如何通過正式的韌性計劃來提升系統穩定性，而 Deloitte 則分享了其在技術韌性領域的專業服務，包括戰略制定、操作模型確立以及災難恢復計劃的實施。

Building a practice to optimize your customer’s resilience journey (PEX208)

這場由 Steph Rowan 和 Diego Dalmolin 主持的演講，深入探討了如何建立和優化客戶的彈性旅程。演講強調了彈性的定義、其對於在 AWS 上運行工作負載的客戶的重要性，以及 AWS 合作夥伴在協助客戶面對彈性挑戰中的關鍵作用。演講中提到，建立彈性實踐需要考慮多個方面，包括評估、可觀察性、DevOps 實踐、微服務架構、多可用區和多地區部署，以及災難恢復策略。AWS 為合作夥伴提供了一系列的程序和工具，以支持開發針對客戶需求的彈性解決方案。

Capital One: Achieving resiliency to run mission-critical applications (FSI314)

這場演講由 Capital One 的高級解決方案架構師 Steve Mirman、資深副總裁 Sharmila Ravi，以及卡片技術副總裁兼首席架構師 Kathleen deValk 共同主持。他們分享了 Capital One 如何在轉向雲端過程中實現關鍵任務應用程式的韌性。重點在於雲原生、多區域部署和先進的容錯機制的應用，以及所謂

的「細胞架構」，這是一種新的微服務架構方法，旨在提高性能和一致性。此外，演講還涉及了控制平面的重要性和一次實際的故障案例分析，特別是 2021 年 12 月 AWS Route 53 服務的故障，這對 Capital One 是一次重要的學習經歷。

Data protection and resilience with AWS storage (STG215-R)

在「STG215-R：資料保護與 AWS 儲存的彈性」演講中，講者探討了資料保護和彈性的重要性，並展示了 AWS 如何支援企業確保其資料的安全和可用性。演講強調了資料在當今數位時代的關鍵作用，以及面對資料量爆炸性增長時，如何保護這些資料免受各種威脅的挑戰。AWS 透過提供一系列工具和服務，如 AWS Backup、AWS Elastic Disaster Recovery 和 AWS Resiliency Hub，幫助企業實現資料的高可用性和災難恢復能力，從而支援企業的資料彈性策略。

Gain confidence in system correctness & resilience with formal methods (ARC315)

在這場演講中，Ankush Desai 與 Bikash Behera 探討了如何透過形式方法來增強系統正確性與韌性。他們介紹了 P 框架，這是一種 AWS 內部用於推理系統正確性的工具，也對 AWS 客戶開放，以便應用於自己的工作負載。演講強調了分佈式應用程式設計的挑戰，尤其是需要滿足的特定規範或要求，如可擴展性、高吞吐量、可用性以及正確性屬性。P 框架允許開發者以狀態機形式表達系統設計，並透過 P 檢查器探索所有可能行為，以確保設計滿足所需的規範。此外，演講透過實例展示了如何使用 P 模型來驗證系統的正確性和韌性，強調了形式方法在識別和修正系統設計中難以發現的缺陷的重要性。

Practice like you play: How Amazon scales resilience to new heights (ARC316)

這場演講深入探討了亞馬遜 Prime Video 如何透過預測性和非預測性事件的訓練與實驗，提升工程團隊的韌性。演講介紹了建立運營準備分數、自動化負載測試、故障注入服務和持續學習等策略，旨在提升團隊對不可預測事件的應對能力。運營準備分數是衡量系統和服務韌性的量化方法，涵蓋了部署安全、程式碼覆蓋率、運營準備完成度和錯誤更正行動等方面。自動化負載測試幫助團隊建立操作肌肉記憶，定期模擬高流量事件以確保系統在高壓力下的表現符合預期。

Resilience lifecycle: A mental model for resilience on AWS (ARC312)

在「ARC312：AWS 上的韌性生命週期」這場演講中，Clark Richey 和來自 Vanguard 的 Stacey Brown 及 Yoni 分享了在 AWS 上建立和維持應用韌性的心得。演講中介紹了 AWS 的韌性生命週期模型，這是一套旨在幫助企業系統化

提高應用韌性的框架。此模型強調了設定目標、設計與實施、響應與學習、評估與測試，以及運營等五個階段。透過這個模型，企業可以在設計架構、管理服務配額、部署程式碼以及管理資料備份等方面做出明智的選擇，從而建立更強韌的應用。Vanguard 的案例提供了在雲端環境中建立和維持高度韌性應用的實踐經驗和啟示。

Resilient architectures at scale: Real-world use cases from Amazon.com (ARC305)

「ARC305：Amazon.com 的大規模韌性架構實戰案例」演講中，分享了 Amazon 如何建立大規模的韌性架構。透過細胞化架構的概念，Amazon 將系統分割成多個獨立單元或「細胞」，每個細胞獨立處理部分工作負載，大大降低了單點故障的影響。此外，透過解耦的設計，各個微服務可以獨立進行創新和疊代，提高系統的靈活性和速度。混沌工程和負載測試被用於評估系統韌性，通過主動尋找和改善潛在弱點來提高可靠性。此外，持續的監控和度量確保了系統即使在高負載下也能保持高可用性。

Using zonal autoshift to automatically recover from an AZ impairment (ARC309)

「ARC309：使用區域自動切換自動從可用區故障中恢復」演講中，Deepak Sury 和 Gavin McCullagh 深入解析了 AWS 的 Zonal Autoshift 功能如何提升服務的可靠性和故障恢復能力。這項功能能夠在某個可用區發生故障時，自動識別問題並將流量無縫切換到其他健康的可用區，確保服務的持續運行。技術實現依賴於 AWS 的高級路由能力和健康檢查機制，實現高度自動化和智能化的故障恢復，有效應對硬故障和灰色故障，從而保證系統整體的韌性和穩定性。

AWS Resilience Partners Best practices to create a resilient organization (PEX210)

在這個數位化快速發展的時代，企業面臨的挑戰與日俱增，尤其在持續提供穩定的服務和處理突發事件。這場演講，由 Ashu 領銜，他負責全球合作夥伴團隊的韌性領導，與來自 Cigna 和 Deloitte 的 Steve 和 Nitin 一同探討如何構建一個韌性企業的最佳實踐。

韌性的定義與重要性

韌性（Resilience）是指在面對各種意料之外的事件時，組織能夠迅速恢復正常運作的能力。這包括應對網絡攻擊、人為錯誤、未經授權的第三方訪問等情況。在當今這個要求 "永遠在線、永遠可用" 的雲計算時代，這一點尤其重要。AWS 通過推出 AWS 韌性能力認證，對合作夥伴在建立韌性最佳實踐和運營韌性 AWS 工作負載方面的能力和經驗進行了認證，進一步強調了韌性在業務運營中的核心地位。

Cigna 的韌性之旅

Steve 介紹了 Cigna 努力提升韌性的過程，作為一家全球性的健康服務公司，其韌性之旅反映了對系統穩定性的不懈追求，尤其是在關鍵時刻為數以百萬計的客戶提供服務的能力。在這個旅程中，Cigna 設立了一個正式的韌性計劃，這個計劃涵蓋了從設計思維到災難恢復的各個方面，確保在面對各種挑戰時，如網絡攻擊、人為錯誤或系統故障，公司能夠快速回應並恢復正常運營。為了加強這一計劃，Cigna 選擇與 Deloitte 合作，利用後者在技術韌性領域的專業知識和經驗。

Deloitte 的韌性服務

Nitin 介紹了 Deloitte 提供的技術韌性服務涵蓋了從戰略制定到操作模型的確立、架構缺陷的識別和補救、韌性測試和可觀測性的增強，以及災難恢復計劃的實施。Deloitte 的方法論著重於理解和應對當今技術環境中的複雜性和不斷變化的挑戰，特別是在客戶對系統可用性要求越來越高的背景下。透過對 Fortune 500 客戶的服務，Deloitte 累積了大量的案例經驗，這些經驗不僅幫助客戶應對技術中斷，還幫助他們在面對潛在危機時保持業務運營的連續性。

韌性的指導原則

圖說：Cigna 和 Deloitte 在韌性建設方面遵循的指導原則包括：

Integrate defensively（防禦性整合）：假設所有依賴可能變慢或不可用，並保護應用程式免受影響。

Test completely（全面測試）：證明您的應用程式能夠如設計的那樣處理慢速或不可用的依賴關係。

Deploy pessimistically（謹慎部署）：假設每次應用程式更改都會失敗，並採取措施以限制其影響。

Run cautiously（謹慎運行）：運行可按需擴展以滿足需求的應用程式副本，但需在定義的限制範圍內。

Observe obsessively（專注觀察）：當應用程式失敗時，作為第一個知道的人，並擁有確定原因所需的資料點。

Recover urgently（迅速恢復）：有效使用可觀測性資料來確定恢復應用程式所需的行動。

Update frequently（頻繁更新）：通過保持應用程式依賴性最新，降低安全漏洞和缺陷的暴露風險。

韌性實踐的實施

Cigna 和 Deloitte 採取了一系列措施來實施這些韌性原則，包括：

建立 SRE 運營模型：確定關鍵垂直領域的關鍵 SRE，並分配其角色和責任。

進行故障模式分析（FMA）：通過評估應用程式架構來識別可能的故障模式並記錄它們。

創建可靠性指南：編制一個包含系統設計模式、部署模式和可觀察性模式的韌性模式目錄。

進行混亂測試和遊戲日活動：通過引入錯誤來測試系統、人員和流程對這些情況的反應。

提供韌性培訓：確保所有相關人員都了解其在韌性方面的角色和責任，並提供必要的知識和工具來支持這些努力。

透過這些實踐的實施，Cigna 能夠強化其系統的韌性，確保即使在面對挑戰時也能保持業務連續性和客戶滿意度。這不僅提高了系統的穩定性，還增強

了公司對未來潛在威脅的準備程度。

面向未來的韌性建設

演講的結尾部分討論了如何將這些韌性建設措施擴展和持續改善，包括應用韌性認證過程和通過持續教育和文化建設來加強組織的韌性意識。Cigna 和 Deloitte 的這次合作展示了通過明確的戰略、堅固的合作夥伴關係和持續的創新如何有效地提高組織的韌性。

補充

Cigna 簡介

Cigna 是一家全球性的健康服務公司，其業務範圍涵蓋健康保險、生命保險以及各種醫療服務和相關產品。公司致力於提供創新的健康解決方案，以滿足個人、家庭和企業客戶的需求。Cigna 的服務範圍廣泛，不僅包括傳統的醫療保險覆蓋，還涉及健康管理、行為健康、牙科保險、殘疾和人壽保險以及醫療補助計劃。通過其全球性的網絡，Cigna 為超過 180 個國家和地區的客戶提供服務，致力於提高人們的健康水平、幸福感和安全感。

Deloitte 簡介

Deloitte 提供專業服務的全球性組織之一，其業務範圍包括審計、諮詢、財務諮詢、風險管理、稅務和相關服務。Deloitte 致力於提供優質的專業服務，幫助客戶在復雜多變的全球市場中取得成功。作為四大會計事務所之一，Deloitte 擁有廣泛的行業知識和深厚的技術專長，為來自不同行業的客戶提供量身定制的解決方案。Deloitte 的網絡遍及全球，擁有來自各個國家和地區的專業人士，通過合作提供創新和有效的業務策略，幫助客戶應對挑戰，抓住機遇。

Building a practice to optimize your customer’s resilience journey (PEX208)

這場演講是由 Steph Rowan 和 Diego Dalmolin 共同主持，為我們提供了關於如何建立和優化客戶的彈性旅程的深入看法。本文旨在概述這場演講的要點，並進一步探討如何在 AWS 生態系統內實現和提高系統彈性。

彈性的定義和重要性

彈性是指一個系統在面對基礎設施或服務中斷時能夠恢復的能力。這不僅包括滿足需求和緩解由錯誤配置或暫時性問題引起的中斷，還包括通過設計、運營和恢復的最佳實踐來最小化停機時間的持續時間和影響。對於 AWS 上的客戶工作負載而言，彈性是一項共享責任，類似於安全性，AWS 負責雲的彈性，而客戶或其合作夥伴則負責雲內的彈性。

市場需求與客戶挑戰

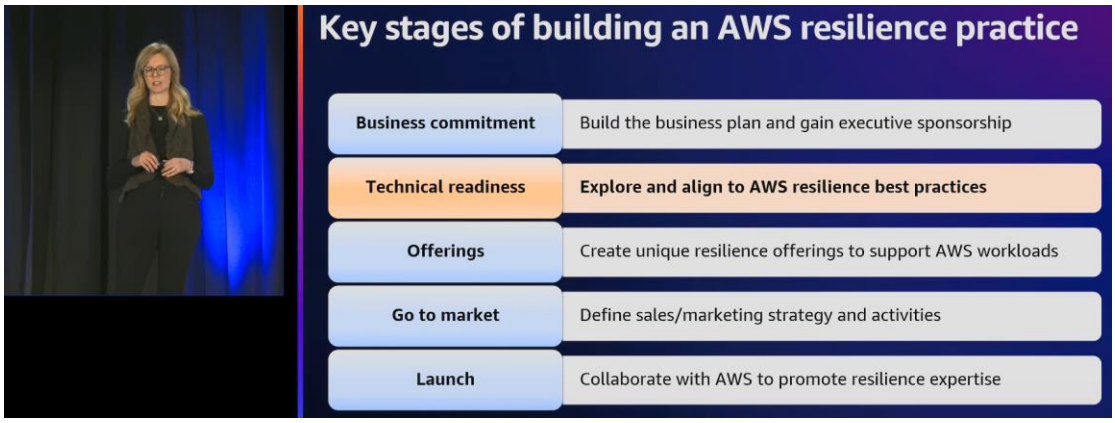
隨著組織越來越多地採用應用程式和市場解決方案來進行日常運營，對彈性的需求也在不斷增長。客戶面臨著滿足其應用程式和網站始終可用的期望、處理遠程團隊和複雜分佈式系統的挑戰，以及遵守新的行業和地區法規的壓力。此外，考慮到 AWS 提供的廣泛服務套件，客戶在維護對這些服務的了解並確保它們共同實現最佳成果方面面臨著挑戰。

合作夥伴的角色

AWS 合作夥伴在幫助客戶應對彈性挑戰方面發揮著關鍵作用。無論是通過遷移和設計關鍵應用程式、創建運營手冊、規劃災難恢復策略，還是通過管理基礎設施和應用程式、管理補丁和更新以及進行持續的安全性和災難恢復評估，合作夥伴都在支持客戶的彈性需求。

建立彈性實踐

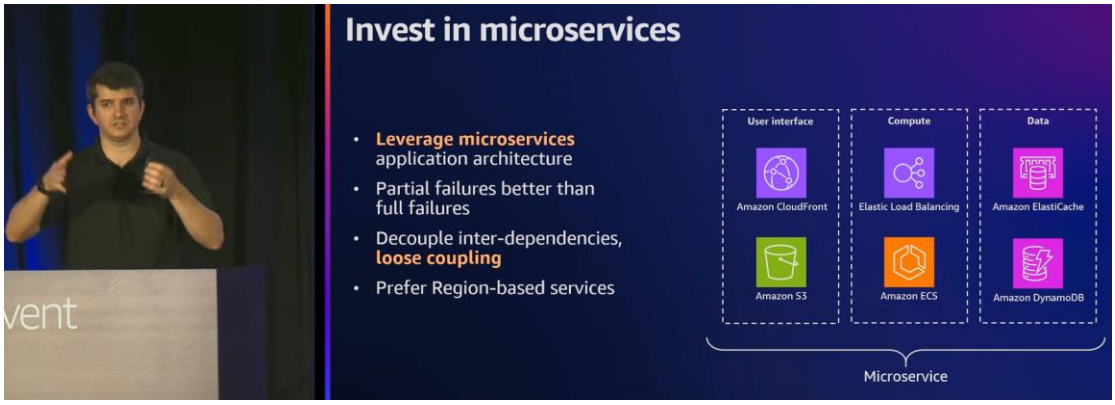
AWS 為合作夥伴提供了一系列程序和工具來支持建立彈性實踐，這包括業務承諾、技術準備、構建產品、市場推廣和推出階段。合作夥伴可以利用 AWS 的指導、工具和支持來開發針對客戶需求的彈性解決方案。



圖說：Rowan 介紹了建立 AWS 復原性實踐的關鍵階段：從商業承諾開始，構建商業計劃並獲得高層支持；技術準備階段，探索並遵循 AWS 的復原性最佳實踐；提供階段，創建支持 AWS 工作負載的獨特復原性方案；上市階段，定義銷售/市場策略和活動；以及最後的發布階段，與 AWS 合作以推廣復原性專長。

技術原則與最佳實踐

彈性的實現涉及到多個方面，包括評估、可觀察性、DevOps 實踐、微服務架構、多可用區和多地區部署以及災難恢復策略。這些技術原則和最佳實踐有助於設計高可用性和可恢復性的應用程式，並通過有效的運營管理來維持這些系統的彈性。



圖說：Dalmolin 強調了將微服務作為一種值得投資的技術架構。圖片右側的子彈文本列出了一系列與微服務相關的建議和原則，包括：1. 利用微服務應用程式架構。2. 相對於完全故障，部分故障更好。3. 解耦內部依賴，實現鬆耦合。4. 優先選擇基於區域的服務。

AWS 服務與支持

AWS 提供了一系列服務來支持彈性建設，包括 AWS Resilience Hub 和 AWS Elastic Disaster Recovery（DRS）。這些服務使合作夥伴能夠評估客戶的彈性需求、識別潛在的弱點、提供建議以提高彈性，並實施有效的災難恢復策略。

總之，隨著對於系統彈性的需求不斷增加，AWS 及其合作夥伴在提供強

大、靈活且可靠的解決方案方面發揮著關鍵作用。通過遵循最佳實踐、利用 AWS 的廣泛服務和工具，以及專注於客戶的特定需求，合作夥伴可以在彈性旅程中為客戶提供重要的支持。

補充

在當今這個數位化快速發展的時代，企業面臨著前所未有的挑戰和機遇。在這個背景下，建立和維持系統彈性成為了確保業務連續性和客戶滿意度的關鍵因素。AWS re:Invent 2023 的演講中，Steph Rowan 和 Diego Dalmolin 深入探討了如何在 AWS 生態系統內建立彈性實踐，並分享了一系列技術原則和最佳實踐。

建立彈性實踐

建立彈性實踐是一個全面的過程，涉及從業務承諾到技術實施的各個方面。AWS 為合作夥伴提供了一個結構化的框架，以支持這一過程：

1. **內部共識**：這是建立彈性實踐的起點，要求合作夥伴內部團隊對於提升彈性有共同的理解和承諾。這包括確定業務目標、資源分配和彈性的戰略地位。
2. **技術準備**：技術準備階段關注於為團隊提供必要的工具和知識，以從技術角度支持彈性實踐。這包括對 AWS 服務的深入了解、彈性設計原則的培訓，以及與彈性相關的銷售和市場策略的準備。
3. **建立產品**：在這一階段，合作夥伴將開發具體的彈性解決方案和服務，為客戶提供量身定制的彈性架構。AWS 提供了一系列工具和資源來支持合作夥伴在這一過程中的創新和開發。
4. **市場推廣**：這一階段涉及到定義銷售策略和市場推廣計劃，以將合作夥伴的彈性解決方案推向市場。AWS 提供適合的服務和工具，幫助合作夥伴有效地傳達其彈性服務的價值主張。
5. **推出**：最後，合作夥伴將推出其彈性服務，並與 AWS 密切合作，共同開發商機並支持客戶的彈性需求。這個階段的成功取決於合作夥伴與 AWS 之間的緊密協作和持續的客戶支持。

技術原則與最佳實踐

為了實現和維持系統的彈性，遵循一系列技術原則和最佳實踐是至關重要的。Diego Dalmolin 在演講中分享了以下幾點：

1. **評估和可觀察性（Observability）**：從評估客戶的業務需求和彈性目標開始，並建立一個全面的可觀察性框架，以即時監控系統狀態並及時響應。
2. **DevOps 實踐**：通過實施不可變部署、金絲雀部署和自動化測試等 DevOps 最佳實踐，提高系統的穩定性和可靠性。
3. **微服務架構**：採用微服務架構來提高系統的靈活性和可擴展性，使得單一組件的失敗不會影響整個系統的可用性。

4.**多可用區和多地區部署**：利用 AWS 的全球基礎設施，在多個可用區和地區部署應用和資料，以提高容錯能力和災難恢復能力。

5.**災難恢復策略**：根據業務需求和風險容忍度，設計和實施適當的災難恢復策略，從簡單的備份和恢復到熱備災和多地區主動-主動部署等不同級別的策略。

通過這些技術原則和最佳實踐，AWS 的合作夥伴可以為客戶提供高度彈性的解決方案，確保其業務連續性和長期成功。隨著技術環境的不斷變化，持續學習和適應這些最佳實踐將是合作夥伴成功的關鍵。

Capital One Achieving resiliency to run mission-critical applications (FSI314)

Capital One 的高級解決方案架構師 Steve Mirman 在這場演講中聚焦於如何在重視韌性的環境中運行關鍵任務應用程式。Capital One 的資深副總裁 Sharmila Ravi 和卡片技術副總裁兼首席架構師 Kathleen deValk 共同分享了他們如何設計和操作以提高韌性。

Sharmila 首先講述了 Capital One 轉向雲端的旅程，以及他們如何將自己定位為一家技術公司而非僅僅是金融機構。她強調了在雲端環境中實現韌性超出客戶期望的重要性，並介紹了 Capital One 如何從頂層結構著手，將韌性融入業務團隊、產品團隊以及架構中。Sharmila 分享了 Capital One 在卡片技術領域的架構設計，強調了系統的複雜性以及在設計韌性方面所面臨的挑戰。

接著，Kathleen 深入探討了如何通過雲原生、多區域部署和先進的容錯機制來提高系統的韌性。她講述了一些具體的韌性設計案例，如如何利用全球表格和 DynamoDB 來處理依賴於主幹網的系統，以及如何在處理信用卡交易時應用主動/主動模式以提高性能和一致性。除此之外，Kathleen 還介紹了所謂的"細胞架構"，這是一種新的微服務架構方法，旨在通過在單一"細胞"內執行端到端的調用鏈來提高性能和一致性。

Kathleen 還強調了控制平面的重要性，並分享了一次實際的故障案例，該案例涉及到 AWS 的 Route 53 服務。這次事件發生在 2021 年 12 月，當時 Route 53 遇到了問題，導致了系統錯誤和可用性問題。這個案例對 Capital One 來說是一次重要的學習經歷，特別是對於 Kathleen 來說，因為這是她加入公司後遇到的第一次重大故障。

圖說：Kathleen 討論控制平面的重要性，指出如果控制平面宕機，自動化將失敗，如果失去可視性，則無法進行故障排除。圖片中的道路標誌暗喻了開始學習和改善的旅程，激勵觀眾對 AWS 的控制平面有深入的理解和持續的改善。

Route 53 故障：Route 53 的下線導致了廣泛的系統錯誤，AWS 和 Capital One 都觀察到了這些錯誤。這引起了雙方的合作，共同診斷問題並尋找解決方案。

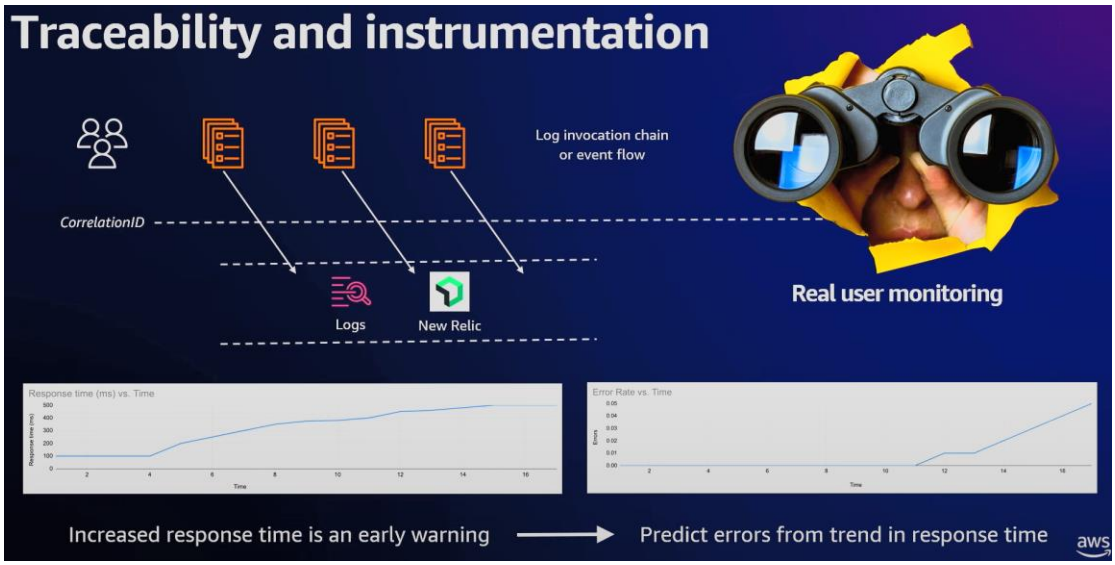
發現的問題

監控系統的局限：一些監控系統不是多區域配置的，因此受到了 Route 53 故障的影響。這導致了對系統狀態的可見性受到限制。

內部部署系統受阻：Capital One 的某些 CI/CD（持續整合和持續部署）管道在美國東部運行，依賴於該地區的 AWS API。由於 Route 53 問題，這些 API 的可靠性受到影響，導致無法有效地強制執行故障轉移。

控制平面的脆弱性：由於 Route 53 的問題，更新 DNS 條目以幫助重新路由到次要區域的能力受到了影響。手動更新是可能的，但 DNS 快取的傳播延遲（約 15 到 20 分鐘）使得這些更改難以立即生效。

從中學到的經驗



圖說：這張簡報展示了如何利用跟蹤和儀表監測來改善應用性能和用戶體驗。通過使用 CorrelationID 跟蹤日誌調用鏈或事件流，並結合日誌和 New Relic 這樣的工具來分析資料。實際用戶監測是通過觀察人物形象和望遠鏡表示的。圖表顯示，響應時間的增加是一個早期警告信號，這有助於從響應時間的趨勢中預測錯誤，從而在問題影響用戶體驗之前進行預防性維護。

加強監控和可見性：強化監控系統，使其跨多個區域運行，以增加對於系統狀態的可見性和控制能力，即使在單一 AWS 服務遇到問題時也是如此。

建立冗餘的部署系統：確保 CI/CD 管道和其他關鍵的內部部署工具在多個 AWS 區域中有冗餘設置，以防止單點故障影響操作能力。

深入理解底層依賴：深入了解系統依賴的工作原理，特別是那些像 Route 53 這樣的基礎設施服務，以便在設計系統時能夠考慮並規劃這些依賴可能出現的故障模式。

提高重試策略的智能性：AWS 的報告指出，由於客戶端的重試行為增加了系統負擔，這是一個意料之外的行為。Capital One 從中學到需要改善重試機制，

避免在系統壓力時期造成額外的負擔。

持續改善和學習：這次故障強調了持續改善和從每次事件中學習的重要性。Capital One 將從這次故障中獲得的看法納入其持續的架構和運營優化中，以提高整體的韌性和可靠性。

透過這次故障案例的分享，Kathleen 強調了在雲基礎設施和服務中實現高韌性的復雜性，以及作為技術組織在設計、監控和應對潛在故障時必須考慮的多個方面。

補充

Capital One 是一家位於美國的金融服務公司，以其創新和客戶導向的金融產品而聞名，特別是在信用卡、銀行業務、貸款和儲蓄產品方面。公司以技術驅動的策略著稱，旨在通過數位化轉型和雲端採納來重新定義金融服務行業的標準。

Capital One 的技術轉型

在過去的幾年中，Capital One 一直在積極轉型成為一家技術公司，將自己從傳統的金融服務提供商轉變為技術先驅。這一轉型的核心是全面採納雲計算技術，特別是通過與 Amazon Web Services（AWS）的合作，Capital One 成為了採用雲端服務的領先金融機構之一。公司不僅將其基礎設施遷移到雲端，還在開發和部署應用程式時採用了雲原生方法。

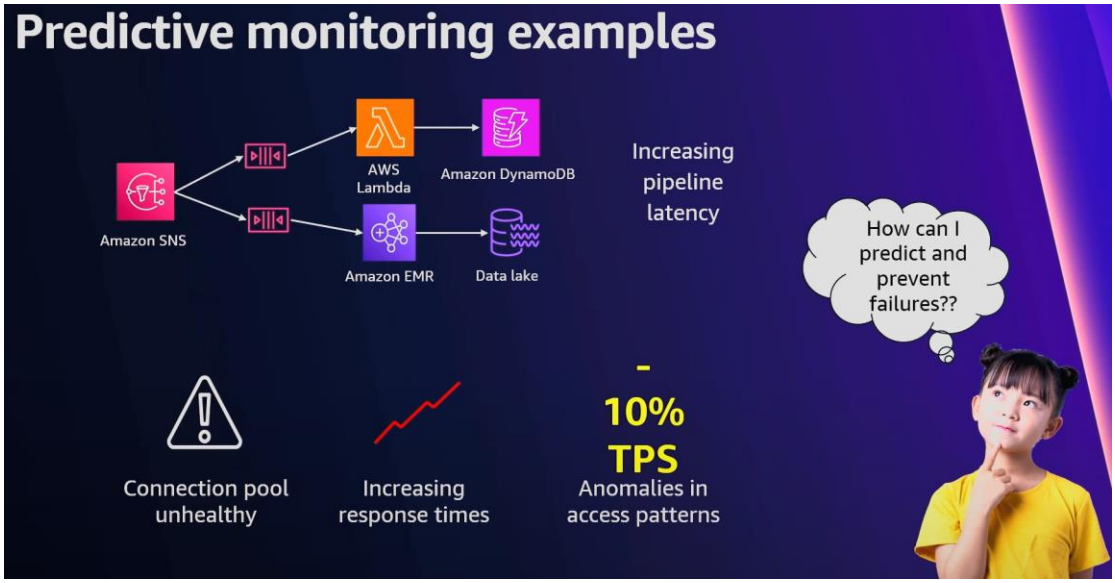
卡片技術的創新

卡片技術是 Capital One 技術創新的一個關鍵領域，涵蓋了信用卡和簽帳金融卡產品的開發、運營和維護。這一領域專注於提高交易處理的效率和安全性，增強客戶體驗，並通過利用資料分析和機器學習來創新金融產品和服務。卡片技術的創新包括即時欺詐檢測、個性化客戶服務、以及支持各種支付技術，如無接觸支付和移動支付解決方案。

韌性和卡片技術

在這場演講中，Kathleen deValk 詳細介紹了 Capital One 如何在其卡片技術領域提高系統韌性。這包括了在多個 AWS 區域和可用區（AZ）中部署服務以實現高可用性，採用微服務架構以提高系統的靈活性和可擴展性，以及實施復雜的故障轉移和自動恢復機制以確保即使在面臨基礎設施故障時也能維持業務連續性。

此外，卡片技術團隊還專注於使用先進的監控和可觀測性工具來提早檢測潛在問題，並通過實施混沌工程和持續的壓力測試來進行預防性故障演練。這些策略和實踐使 Capital One 能夠在高度競爭的金融服務市場中保持領先地位，為其客戶提供無與倫比的服務質量和可靠性。



圖說：這張圖展示了預測監控的幾個範例，以及它們在提前識別並防止系統失敗方面的重要性。我們可以看到幾個 AWS 服務組成的工作流程，並指出了三個潛在的問題信號，這些問號代表了可能會導致系統失效的指標：(1)連接池不健康：這可能表示基礎的服務（如資料庫）無法有效地管理連接，導致系統性能下降或者中斷。(2)響應時間增加：如果服務對請求的響應時間變長，這可能暗示系統正在承受越來越多的負載，或者出現了性能瓶頸。(3)TPS（每秒交易次數）異常增加 10%：這顯示出訪問模式出現了異常，可能是由於不正常的用戶行為，或者是系統本身的問題。

Data protection and resilience with AWS storage (STG215-R)

在 AWS re:Invent 2023 的「STG215-R：資料保護與 AWS 儲存的彈性」演講中，講者深入探討了資料保護和彈性的重要性，並展示了 AWS 如何支援企業確保其資料的安全和可用性。

資料的重要性與挑戰

在當今的數位時代，資料已成為企業最寶貴的資產。它不僅支撐了日常業務運作，還是決策制定的關鍵依據。然而，隨著資料量的爆炸性增長，如何保護這些資料免受各種威脅，包括人為錯誤、系統故障、自然災害等，成為企業面臨的一大挑戰。

AWS 的資料彈性策略

AWS 提供了一系列工具和服務，幫助企業實現資料的高可用性和災難恢復能力。這些策略包括：

高可用性(High Availability)：透過設計可在單一組件故障時依然保持運作的應用程式，以達到極高的服務可用性。AWS 的多可用區部署就是一種常見的高可用性策略。

災難恢復(Disaster Recovery, DR)：針對整個區域故障的情況，制定恢復計劃。這包括了確定恢復點目標(Recovery Point Objective, RPO)和恢復時間目標(Recovery Time Objective, RTO)，以及選擇適合的災難恢復策略，例如冷備份、熱備份、多站點活躍/活躍部署等。

AWS 的資料保護工具

AWS 提供了多種資料保護工具，以支援企業的不同需求：

AWS Backup：一個集中管理的服務，支援跨多個 AWS 資源的資料備份，幫助企業輕鬆遵守法規要求並實現資料的彈性。

AWS Elastic Disaster Recovery：提供快速、可靠的災難恢復解決方案，幫助企業在災難發生時迅速恢復業務運作。

AWS Resiliency Hub：幫助企業評估和改善其在 AWS 上運行的應用程式的彈性，確保業務連續性和資料保護。

實際案例與策略

高可用性設計實例

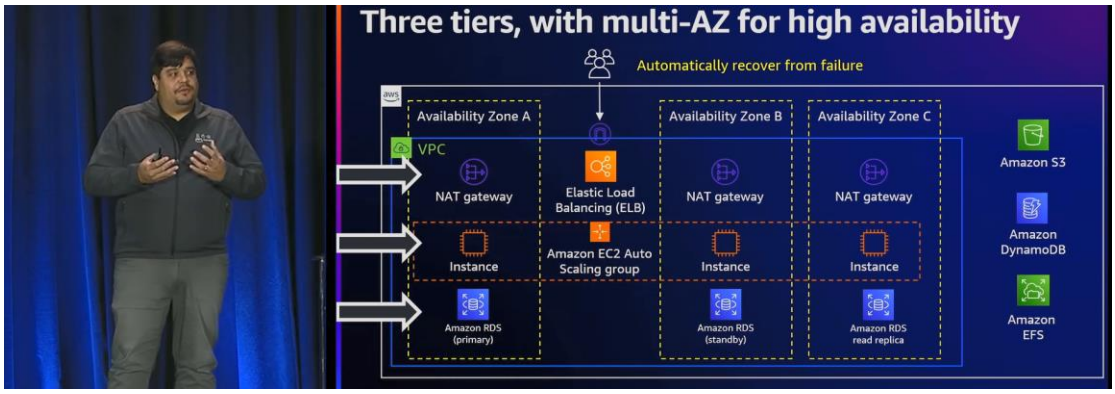
案例背景：一家全球範圍的電商平台需要確保其在線交易系統終年無休，即使在高峰期也要保持服務的穩定性和可用性。

策略實施

多可用區部署：該公司將其關鍵服務部署在多個 AWS 可用區中，即使某個可用

區發生故障，系統也能自動切換到其他健康的可用區，保障服務不中斷。

自動擴展：利用 AWS 的自動擴展服務，根據實際流量自動調整計算資源，確保在用戶訪問量激增時能迅速提供足夠的處理能力。



圖說：這幅圖片顯示了一個高可用性（High Availability, HA）的三層架構，部署於 Amazon Web Services（AWS）上，利用多個可用區（Multi-Availability Zones, AZs）來提高系統的耐用性和穩定性。從左至右分別是以下組件：

(1)**虛擬私人雲（VPC）**：所有資源都在 AWS 的 VPC 內部署，這是一個隔離的網絡空間，允許用戶在 AWS 雲中定義自己的虛擬網絡。

(2)**NAT 閘道器（NAT Gateway）**：在每個可用區中都設置了 NAT 閘道器，以允許私有子網中的實例能夠與因特網通信，而不允許外部直接訪問這些實例。

(3)**實例（Instances）**：AWS EC2 實例分佈在不同的可用區中，這些實例通過自動擴展組（Auto Scaling group）進行管理，以便根據負載自動擴展或縮小。

(4)**彈性負載平衡器（ELB）**：ELB 位於架構的前端，用於分發進入流量到多個 EC2 實例，以實現負載平衡和故障轉移。

(5)**關聯式資料庫服務（RDS）**：圖片中顯示了兩種 RDS 的部署方式：一個是主要的資料庫（primary），另一個是在不同可用區的備用資料庫（standby），以及一個讀取副本（read replica）。

(6)**簡單儲存服務（S3）**：提供高可用性和高擴展性的物件儲存，常用於備份和儲存大量的非結構化資料。

(7)**DynamoDB**：一個快速且靈活的 NoSQL 資料庫服務，用於處理需要快速且一致性的讀寫能力的大量資料。

(8)**彈性檔案系統（EFS）**：為應用提供了一種簡單、伸縮性強的檔案儲存服務。

整體上，這個架構為應用提供了自動從失敗中恢復的能力，透過跨多個物理位置的資源複製和負載平衡，增強了整體系統的穩健性。這種配置尤其適用於那些對停機時間和資料丟失非常敏感的應用。

災難恢復策略實例

案例背景：一家金融機構需要確保其交易系統即使在遭遇自然災害或其他重大故障時也能迅速恢復。

策略實施

跨區域災難恢復：該金融機構在不同的 AWS 地理區域設置了災難恢復站點，一旦主要站點不可用，就能迅速切換到災難恢復站點，保障關鍵業務的連續性。

RPO 和 RTO 設定：通過明確設定恢復點目標（RPO）和恢復時間目標（RTO），該機構能夠根據業務需求和風險承受度，制定出合適的資料備份和恢復策略。

綜合策略應用實例

圖說：這幅圖片呈現了不同的災難恢復策略，每種策略都以恢復點目標（RPO）和恢復時間目標（RTO）為特徵，並列出了其應用情境、成本和操作方式的概覽。這是為了幫助組織理解在遇到意外事件時如何恢復其 IT 系統和資料。從左到右，策略依據恢復速度和成本增加：
每種策略的選擇取決於組織對於服務中斷和資料損失的容忍度，以及他們願意為確保持續性和恢復力投入的資金。这些策略展示了從最基本的備份與恢復，到最先進的多站點活動/活動配置之間的恢復能力和成本的逐步增加。

策略	RPO/RTO	描述	成本
備份與恢復	數小時	用於低優先級案例；災難發生後提供所有 AWS 資源；災難發生後恢復備份	$
駕駛燈	數十分鐘	資料保持活躍，服務保持閒置；災難發生後配置一些 AWS 資源並擴展	$$
溫備份	數分鐘	始終運行，但規模較小；適用於業務關鍵性服務；災難發生後擴展 AWS 資源	$$$
多站點活動/活動	即時	零停機時間；幾乎零資料損失；用於任務關鍵型服務	$$$$

案例背景：一家國際新聞媒體公司需要確保其新聞發布系統在全球範圍內的高可用性和資料一致性。

策略實施

多站點主動-主動架構：通過在多個 AWS 區域部署主動-主動（Active-Active）架構，確保全球用戶都能獲得快速響應和最新內容。

資料同步與一致性：利用 Amazon DynamoDB 的全球表功能，實現資料的即時同步和一致性，無論用戶訪問哪個地區的服務，都能獲取到最新的新聞內容。

這些案例展示了企業如何結合 AWS 的多種服務和特性，根據自身業務需求和風險評估，設計出既能保障資料安全又能提高業務彈性的解決方案。通过這些策略，企業不僅能夠提高系統的可用性和穩定性，還能在面對突發事件時迅速恢復，保障業務的持續運營。

結論與建議

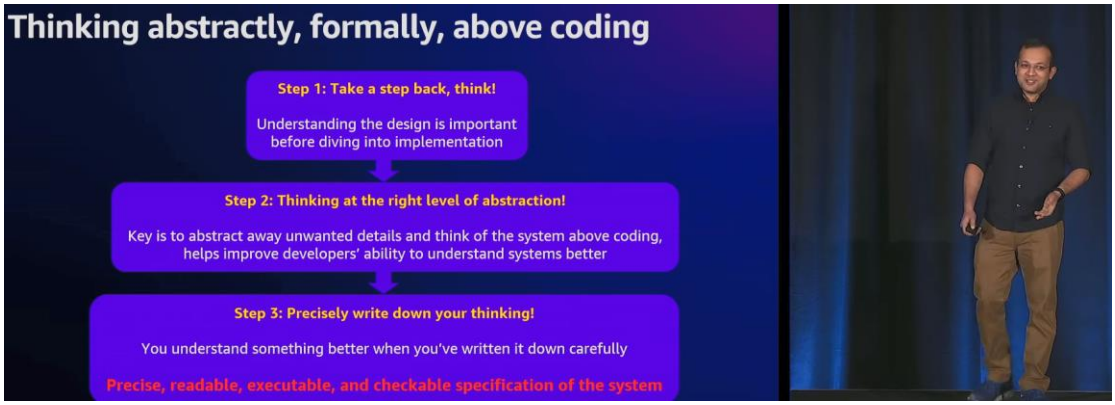
確保資料的保護和彈性是企業在數位轉型過程中必須面對的挑戰。透過 AWS 的強大工具和服務，企業可以根據自身的需求和業務重要性，制定並實施適合的資料保護策略。此外，AWS 的共享責任模型強調，客戶也需要承擔起保護其在 AWS 上運行應用程式的責任，這包括配置適當的備份計劃和安全設置。

隨著技術的不斷進步和威脅的日益增加，持續評估和改善資料保護策略將是企業確保長期成功的關鍵。AWS 提供的教育資源和專業指導，將助力企業在這一旅程上取得成功。

Gain confidence in system correctness & resilience with formal methods (ARC315)

在本次演講中，Ankush Desai 與 Bikash Behera 共同探討了如何通過形式方法增強系統正確性與韌性的信心。他們向觀眾介紹了 P 框架，這是一種在 AWS 內部用於推理系統正確性的工具，並且也對 AWS 客戶開放，以便他們能夠在自己的工作負載中應用這些技術。

本次演講的核心觀點在於，分佈式應用程式的建構極具挑戰性，需要精確地滿足一系列特定的規範或要求，如可擴展性、高吞吐量、可用性以及正確性屬性，如一致性。為了在分佈式系統中滿足這些規範，系統設計必須考慮到各種非確定性因素，如節點失敗、網絡分區、消息丟失等。因此，系統設計必須是組合式的，包含多個互相交互的服務、組件和協議。



圖說：這張圖片展示的是演講者介紹的三個思考系統設計的階段，強調在正式編碼之前的抽象、形式化思考過程。這三個步驟如下：

步驟 1：退後一步，思考！

瞭解設計在深入實施之前是重要的。這個階段是關於從宏觀的角度來理解系統設計的重要性。

步驟 2：在正確的抽象層次上思考！

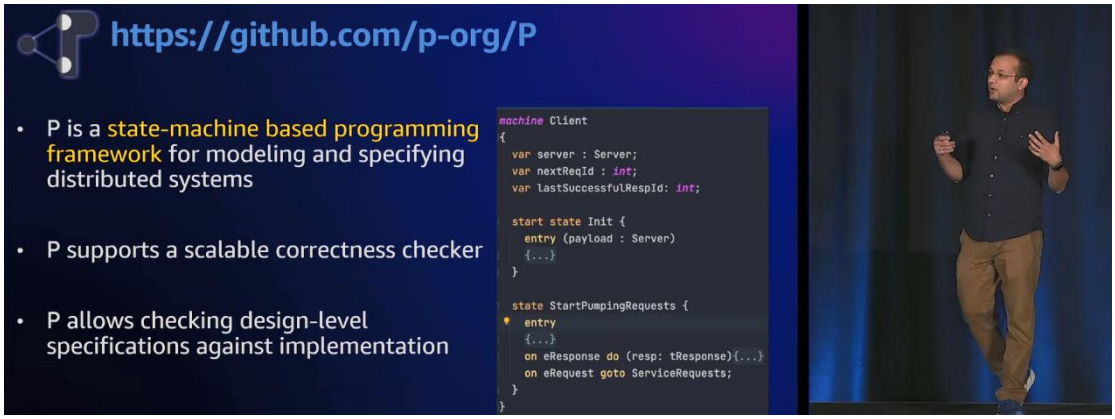
關鍵是要抽象掉不必要的細節，並在編碼之上思考系統，這有助於開發人員更好地理解系統。

步驟 3：準確記錄下你的思考！

當你仔細書寫下來時，你對某件事的理解會更好。這一步涉及到將思考過程轉化為精確、可讀、可執行且可檢查的系統規範。

這張圖片突顯了在實際開始編碼之前，對系統進行周全思考的重要性，這樣做可以提高系統設計的質量並降低後期錯誤修正的成本。

形式方法的引入，作為開發過程中的一個額外的安全措施，可以幫助開發者早期發現設計層面的邏輯錯誤，從而降低在開發過程後期發現這些錯誤的成本和努力。Ankush 介紹了 P 框架，這是一種用於應用形式方法於分佈式系統和應用程式的工具，它允許開發者以狀態機的形式表達系統設計，並通過 P 檢查器探索系統的所有可能行為，以確保設計滿足所需的規範。



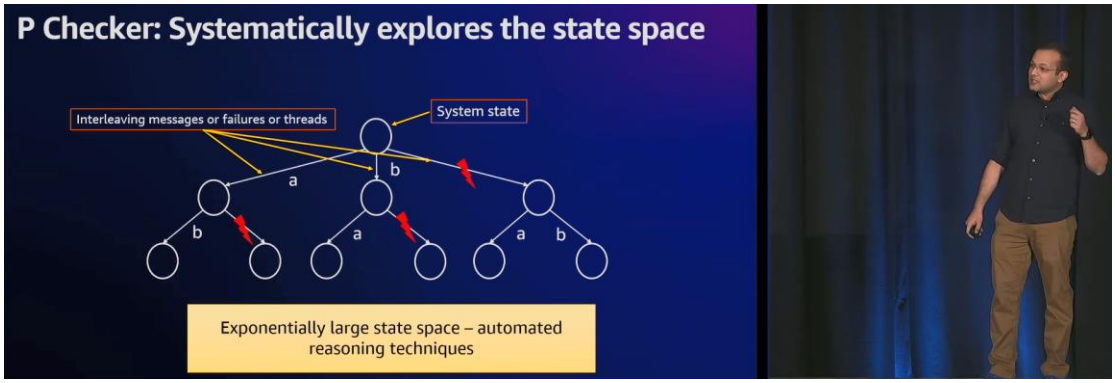
P 編程框架是一種基於狀態機的編程框架，用於建模和指定分布式系統：

P 是一個狀態機基礎的編程框架，適用於對分布式系統進行建模和規範。

P 支持一個可擴展的正確性檢查器。

P 允許檢查設計級別的規範與實施情況的對應性。

Bikash 進一步闡述了如何將 P 框架應用於 AWS 客戶的工作負載中，並以交易處理系統為例，展示了如何使用 P 模型來驗證系統的正確性和韌性。他強調了形式方法的一個核心概念，不變性，這是系統始終需要滿足的預期。透過模擬各種測試情境，包括標準處理、混沌工程和災難恢復，Bikash 展示了 P 模型如何幫助識別並修正系統設計中難以發現的缺陷。



圖說：簡報有如下內容

P Checker： 它是一種工具，用於探索分布式系統設計的所有可能狀態，從而檢查系統是否符合給定的規範。

系統狀態探索： 圖示顯示了一個樹狀結構，其中節點表示系統的狀態，而分支表示可能的事件或動作（如 a 或 b），這些事件導致系統狀態的變化。紅色閃電形圖標表示可能的故障或錯誤。

交錯消息或故障或線程： 這表明 P Checker 能夠處理系統中發生的異步事件，如消息傳遞、故障或多線程操作的交錯。

指數級大的狀態空間： 標註提到使用自動推理技術來處理可能非常龐大的狀態空間。這種技術可以幫助分析和驗證那些在實際操作中可能難以通過手工測試來探索的複雜系統行為。

最後，Ankush 和 Bikash 共同強調，雖然 P 框架提供了一種強大的工具，但最重要的是開發者在設計階段進行抽象思考的過程本身。他們鼓勵觀眾將形式方法和 P 框架整合到自己的開發流程中，以提高開發分佈式應用程式的信心和效率。

本次演講不僅為參與者提供了有關如何利用形式方法來增強系統設計正確性和韌性的實用知識，而且通過實例展示了這些方法和工具在實際應用中的強大功能。通过這次分享，參與者得以深入理解分佈式系統設計中的關鍵挑戰，以及如何通過系統化的方法和工具來克服這些挑戰。

補充

1. CAP 理論

CAP 理論是分佈式系統設計的一個基本原則，指出在面對網絡分割（Partition tolerance）時，系統不能同時滿足一致性（Consistency）和可用性（Availability）的全部要求。

一致性（Consistency）：系統中的所有節點在同一時間看到的資料是相同的。

可用性（Availability）：系統每個請求都能在有限時間內得到回應，無論回應是成功還是失敗。

分**區容錯性（Partition tolerance）**：系統能夠在任何網絡分區故障中繼續運行。

2. 最終一致性與強一致性的差別

強一致性：系統在更新資料後，任何後續的訪問都將立即看到最新的資料。這意味著系統必須在資料更新和讀取操作之間保持嚴格的一致性。

最終一致性：系統保證只要沒有新的更新，資料最終會變得一致。這意味著更新後，系統可能會在一段時間內返回舊資料，但最終會達到一致狀態。

3. P 框架是什麼？

P 框架是一種用於分佈式系統的形式化驗證工具，它提供了一種基於狀態機的高級編程語言，使得開發者能夠以通信狀態機的形式表達他們的系統設計。P 框架特別適用於那些需要嚴格推理系統正確性和韌性的複雜分佈式應用。

4. P 框架的價值

設計階段的系統驗證：P 框架允許開發者在實際程式開發之前就驗證系統設計的正確性，從而提早發現和修正潛在的設計錯誤。

提高系統韌性：通過模擬各種失敗情況和非確定性行為，P 框架幫助確保系統能夠在面對真實世界挑戰時保持穩定和可靠。

促進深入理解系統行為：使用 P 框架強迫開發者進行抽象和形式化的思考，從

而更深入地理解系統的行為和交互。

5. **應用 P 框架的案例**

Amazon S3 一致性協議：Amazon S3 團隊使用 P 框架來驗證其從最終一致性到強一致性轉變的協議設計，確保在各種失敗模式下都能維持一致性保證。

交易處理系統驗證：Bikash Behera 利用 P 框架建模和驗證了一個包含多個微服務和通過隊列通信的交易處理系統。這一過程不僅揭示了設計中的潛在問題，還指導了如何增強系統的韌性和可靠性，特別是在面對隨機失敗和災難恢復情況時的行為。

Practice like you play How Amazon scales resilience to new heights (ARC316)

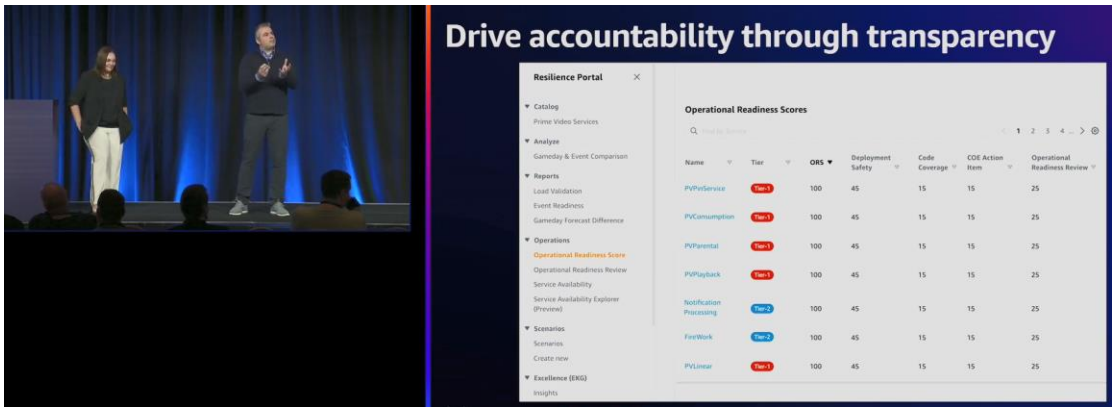
在這場演講中，我有幸聽到了亞馬遜 Prime Video 團隊如何將運動團隊的訓練策略應用於提升其服務的韌性。這個過程不僅令人著迷，也提供了一個極佳的示範，說明了如何在不斷變化的環境中保持服務的高效和穩定。

Laurent 和 Olga，來自 AWS 和 Prime Video 的兩位資深專家，向我們揭示了一套創新的方法，一本韌性劇本，旨在讓工程團隊像頂尖運動隊伍一樣訓練和準備。這本劇本中蘊含的策略和技巧，已經幫助 Prime Video 成功地應對了連續兩年獨家直播周四夜足球賽的挑戰，並將觀眾數量增加了 26%。

一個值得注意的比喻是，Olga 將工程團隊準備應對高峰負載的過程，與運動員準備超級杯大賽的方式進行了比較。這種比較不僅生動形象，也強調了在壓力之下表現出色所需的策略性思維和持續訓練的重要性。

他們的講述深入介紹了 Prime Video 如何透過「全球思考，本地行動」的策略來規劃和執行其全球活動。這一策略強調了在全球範圍內制定共同目標和計畫的同時，也賦予各地團隊足夠的靈活性來因地制宜地執行任務。

一、運營準備分數：量化韌性的關鍵指標



圖說：這張圖片展示了「Resilience Portal」中的「操作準備分數（Operational Readiness Scores）」。這些分數用來評估不同服務的準備情況，包括「部署安全（Deployment Safety）」、「程式碼覆蓋率（Code Coverage）」、「COE 行動項（COE Action Item）」以及「操作準備評論（Operational Readiness Review）」。各個方面的得分。這展示了對於服務健壯性與準備情況的透明度和責任追究的重視。

運營準備分數是一種衡量系統和服務韌性的量化方法。這一分數基於四個支柱：部署安全、程式碼覆蓋率、運營準備完成度和審查以及錯誤更正行動。

部署安全：這涉及到自動回滾、藍綠部署、漸進式發布等策略，以確保新程式碼的部署不會對現有系統造成不利影響。

程式碼覆蓋率：高質量的測試覆蓋率是確保程式碼質量和系統穩定性的重要因素。包括單元測試、整合測試和端到端測試在內的全面測試策略，可以揭露潛在問題。

運營準備完成度和審查：這包括確保所有系統組件都準備就緒並且經過徹底審查，從安全性到性能都要考慮在內。

錯誤更正行動：當系統出現問題時，快速準確地定位並修復這些問題是至關重要的。這需要一個有效的錯誤追蹤和解決機制。

透過對這些領域的持續評估和改善，團隊可以提高系統的整體韌性，從而更好地應對各種挑戰和變化。

二、自動化負載測試：建立操作肌肉記憶

自動化負載測試是一種強大的工具，用於模擬高流量條件下系統的行為，從而提前發現潛在的性能瓶頸和穩定性問題。這種測試可以幫助團隊建立所謂的「操作肌肉記憶」，即在真實世界的高壓環境下自動和直覺地做出反應。透過定期的自動化負載測試，團隊可以：

確保系統能夠處理預期的最高負載

在安全的環境中識別和解決問題，而不會影響實際的用戶體驗。

提高團隊對系統行為的理解，從而在出現問題時快速做出反應。

透過自動化的負載測試，團隊可以定期模擬高流量事件，以確保系統在高壓力下的表現符合預期。Prime Video 每週在每個區域進行三次這樣的測試，這有助於團隊熟悉正常和異常流量模式，並及時發現並解決潛在問題。

三、故障注入服務：實踐非預測性事件的應對

故障注入服務（如 AWS 的 Fault Injection Simulator）允許團隊在受控環境中主動引入各種故障（例如網絡延遲、系統資源耗盡等），以評估系統在面對真實世界故障時的反應和恢復能力。這種做法有助於團隊：

1. 理解系統在面對意外事件時的行為。
2. 驗證和改善災難恢復計劃和故障轉移策略。
3. 提升系統的整體韌性，減少未來潛在故障的影響。

故障注入服務（FIS）允許團隊在受控環境中模擬各種故障情況，如資源耗盡、網絡延遲或服務中斷。通過在開發和生產環境中執行這些實驗，團隊可以評估其系統的恢復能力和容錯能力。

四、持續學習與改善：從實踐中獲取看法

韌性不是一個靜態的目標，而是一個需要持續努力和改善的過程。透過持續的學習和改善，團隊可以不斷提高系統的韌性。這包括：

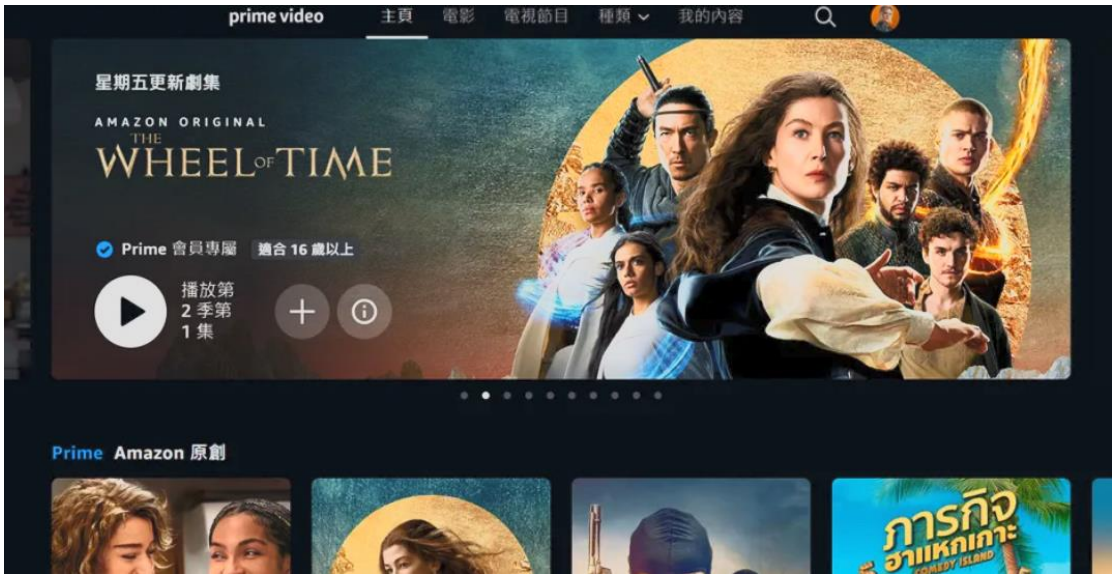
定期進行事後分析（Post-Mortem Analysis）：從每次故障中學習，並將這些學習轉化為具體的改善措施。

更新和維護文檔：包括運營手冊和緊急應對計劃，以確保團隊成員在需要時能夠快速找到並遵循正確的程序。

鼓勵開放和無責任的文化：使團隊成員在出現問題時能夠毫無保留地分享信息和看法，從而加快問題的解決速度並促進團隊間的學習。

持續的學習和改善是提高系統韌性的核心。透過定期的回顧演講和故障分析，團隊可以從每次事件中學習，並將這些學習轉化為改善措施。這種持續的疊代過程有助於團隊預測和應對未來的挑戰。

補充



亞馬遜 Prime Video 是亞馬遜公司旗下的一項流媒體視頻服務，提供各種電影、電視劇、紀錄片以及原創內容給全球範圍內的觀眾。自從推出以來，它已經成為 Netflix、Hulu 等其他流媒體平台的強有力競爭者。

主要特色

1. **豐富的影視庫**：Prime Video 擁有包括好萊塢大片、獨家原創劇集、流行電視節目、經典電影以及各種語言的國際內容。
2. **原創內容**：亞馬遜投入大量資源製作原創內容，包括得到觀眾和評論家好評的劇集和電影，如《透明家庭》（Transparent）、《高堡奇人》（The Man in the High Castle）以及《了不起的麥瑟爾夫人》（The Marvelous Mrs. Maisel）等。
3. **運動直播**：除了電影和電視節目，Prime Video 還提供運動賽事的直播服務，包括但不限於美國足球（NFL）的 Thursday Night Football、ATP 巡迴賽等，豐富了它的內容類型。

4.**高品質的觀看體驗**：支援 4K 和 HDR 視頻質量，為用戶提供高質量的觀看體驗。

5.**跨平台支持**：用戶可以在各種設備上觀看 Prime Video，包括智能電視、遊戲機、智能手機、平板電腦和網絡瀏覽器等。

6.**Prime 會員特權**：亞馬遜 Prime 會員不僅可以享受 Prime Video，還包括免費的快速運送、音樂流媒體服務、電子書借閱服務等多項福利。

Resilience lifecycle: A mental model for resilience on AWS (ARC312)

這場演講由 Clark Richey 主講，揭示了如何在 AWS 上建立和維持應用程式韌性的心法。此外，Vanguard 的 Stacey Brown 和 Yoni 分享了他們如何實踐這些理念，確保其全球投資管理業務的穩固與可靠。

韌性等於收益

Clark 首先指出，韌性直接關聯於企業的收益。根據 Gartner 的研究，一旦應用程式發生故障，無論其功能多麼先進，都將對公司造成經濟損失。IDC 的估計更是驚人，僅僅是計劃外的停機時間，就會使財富 1000 強企業每年損失 15 到 25 億美元。除了這些直接損失外，應用程式的不可用還會對企業的聲譽造成長期的負面影響。

AWS 的韌性共享責任模型

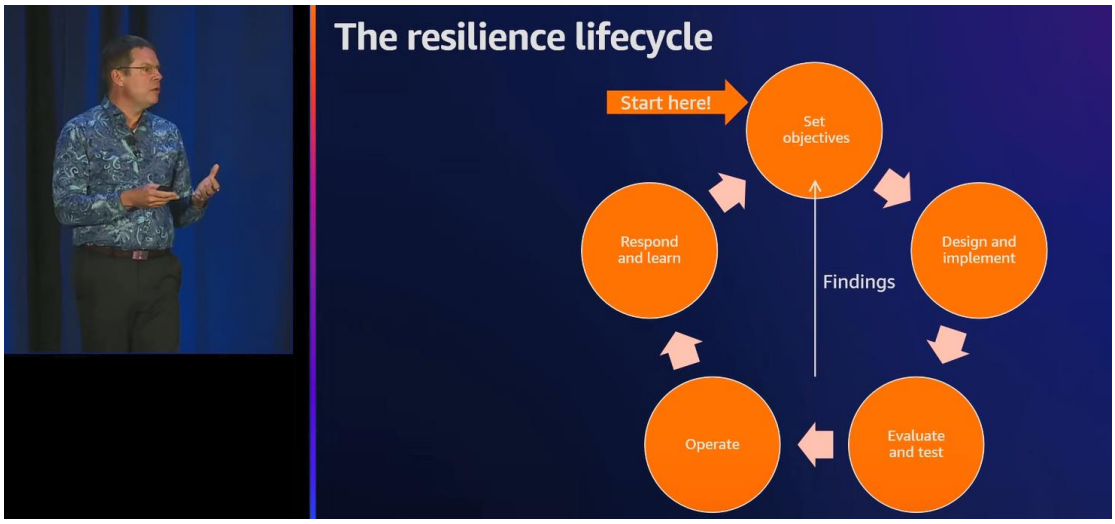
在 AWS 的生態系統中，韌性建構基於一個共享責任模型。AWS 承擔確保雲端基礎設施的韌性，包括區域、可用區以及全球基礎設施的穩健。而客戶則需負責在雲端中構建韌性強大的架構，包括設計選擇、資料備份、故障管理等。

分佈式系統的挑戰

Clark 強調，轉移到雲端雖帶來靈活性和成本效益，但同時也帶來了分佈式系統的複雜性和挑戰。確保這樣一個系統的可觀察性和管理多個組件之間的交互影響是一項艱巨的任務。

AWS 的彈性生命週期模型

AWS 的彈性生命週期模型是一套旨在幫助企業系統化地提高應用彈性的框架。這個模型強調了 AWS 的共享責任模型，在其中，AWS 負責雲端的彈性，而客戶則需負責雲端內的彈性。這意味著客戶需要在設計架構、管理服務配額、部署程式碼以及管理資料備份等方面做出明智的選擇，以建立彈性的應用。



彈性生命週期的五個階段

1. **設定目標**：這是確定業務對應用彈性需求的階段，通常涉及確定恢復點目標（RPO）和恢復時間目標（RTO）。
2. **設計與實施**：在這個階段，企業將根據設定的目標來設計和實施他們的系統架構，包括選擇合適的 AWS 服務和遵循最佳實踐指南。
3. **響應與學習**：當系統發生事件時，如何快速有效地響應並從中學習，以避免未來同樣的問題，是這個階段的重點。
4. **評估與測試**：這個階段包括在部署前後對系統進行測試，以確保其滿足彈性目標。這可能包括性能基準測試、負載測試和混沌工程實驗。
5. **運營**：在這個階段，重點是監控系統的運行狀態，並透過合成流量和告警系統來提前識別潛在問題。

Vanguard 的彈性之旅

Vanguard 作為一家全球投資管理公司，在 AWS 雲端上實施彈性生命週期模型的經驗極為豐富且具啟發性。透過對其實施過程的深入剖析，我們可以獲得關於如何在雲端環境中建立和維持高度彈性應用程式的寶貴看法。

組織架構與運作模式

Vanguard 首先建立了一個跨功能團隊，包括架構、工程、生產保障和運營團隊，以端到端的視角來審視彈性生命週期。這種組織架構的設計確保了從設計、部署到運營的每個階段都能夠共享知識和經驗，並且能夠從每次事件中學習和改善。

圖說：Vanguard 建立了一個韌性團隊，從而創造一個持久的企業結構。它把過程分成了四個階段：

1. **定義 (Define)**：此階段由「韌性架構辦公室」負責，主要工作是建立韌性架構和發展相關模式。
2. **賦能 (Enable)**：由「軟件工程辦公室」負責，涉及管道工程、混沌工程和測試工程等方面的工作，旨在賦予軟件開發流程以更高的韌性。

3. **保障（Assure）**:「生產保障辦公室」則關注於韌性治理、運營智能以及變更與發佈管理，以確保產品和服務的可靠性。

4. **運營（Operate）**：最後，「生產與運營管理」聚焦於日常運營，包括主要事件管理、問題管理和運營活動，保證組織能夠順利運作。

從反應式到主動式

Vanguard 的轉變過程從反應式管理到主動和預防性管理，這一點尤為關鍵。他們意識到，雖然過去在彈性方面有所改善，但這些改善往往是零散和反應式的。因此，Vanguard 著手建立一個企業級的架構，將所有團隊在彈性方面的努力整合起來，從而實現統一和系統化的改善。

標準、模式與工具

為了支持這一轉變，Vanguard 確立了明確的彈性標準和模式，並且開發了一系列工具來幫助工程師和開發人員遵循這些標準和模式。這些工具包括：

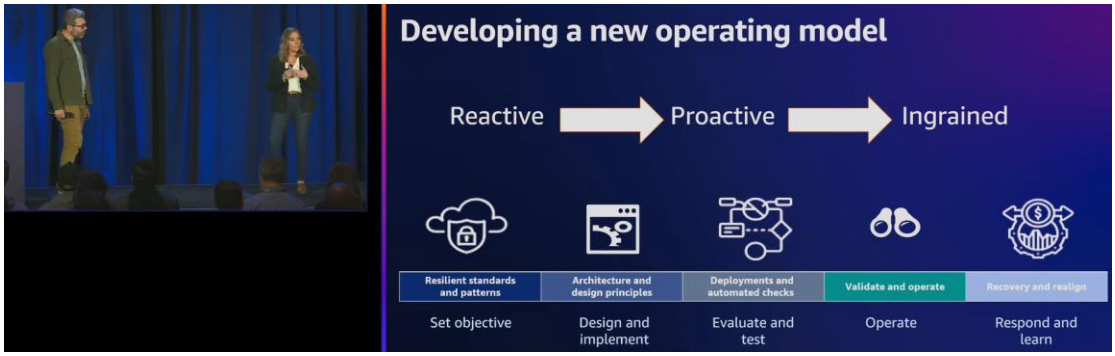
性能測試服務（PTAS）：基於 Locust 開發的控制平面，可以應對極大的負載，幫助團隊理解系統在高負載下的表現。

混沌工程工具：用於模擬可能發生的系統失效，幫助團隊預先理解和準備應對潛在的失效情況。

觀測性增強：引入分佈式追蹤技術，顯著降低了故障檢測和修復的時間。

策略引擎：使用開放標準如 Rego 和 OPA 來確認業務流程的遵循度，並在開發過程的早期階段即可發現不符合彈性標準的地方。

文化和培訓



圖說：這幅圖顯示了 Vanguard 組織營運模式的演進，從反應式（Reactive）到主動式（Proactive），最終到根深蒂固（Ingrained）。每個階段下都有相應的活動和策略：

1. **反應式**：在這個階段，組織主要是對問題做出反應。設定目標是這一階段的關鍵，涉及建立韌性標準和模式。
2. **主動式**：轉變為主動模式意味著在問題發生之前進行預防。這涉及設計和實施合理的架構和設計原則，以及在部署過程中進行自動檢查，以確保系統能夠抵抗未來的故障。
3. **根深蒂固**：這一階段表示韌性已經深入到組織的運營和文化之中。這包括在日常運營中驗證系統的穩健性，以及在問題發生時進行快速的恢復和重新校準。

Vanguard 認識到，僅僅有工具和流程是不夠的，建立一個重視彈性的文化同樣重要。因此，他們改革了變更和發布管理流程，將 SRE（Site Reliability Engineering）實踐融入到培訓課程中，並且創立了一個彈性冠軍網絡來促進知識和最佳實踐的共享。

成果與未來方向

Vanguard 的這一系列努力帶來了顯著的成果：提高了系統的可靠性和連續性，同時減少了重大事件的發生，並且大幅降低了平均故障修復時間（MTTR）。未來，Vanguard 計劃進一步提高工具和標準的易用性，加強觀測性，並且持續優化彈性實踐。

Vanguard 在 AWS 上實施彈性生命週期模型的經驗強調了跨功能合作、持續改善和文化建設的重要性。對於其他企業而言，Vanguard 的經驗提供了一個寶貴的參考，特別是對於那些正在尋求在雲端環境中提高應用彈性的企業。

結論

彈性不是一個一勞永逸的目標，而是一個需要持續努力和改善的過程。AWS 的彈性生命週期模型提供了一個框架，幫助企業系統地提高他們在雲端的應用彈性。Vanguard 的經驗教訓強調了跨功能團隊合作的重要性，以及將彈性整合到開發生命週期中的重要性。對於希望在雲端環境中提高應用彈性的企業來說，這些看法無疑是寶貴的。

補充

Vanguard 是一家全球領先的投資管理公司，以其廣泛的共同基金和 ETFs（交易所交易基金）而聞名於世。成立於 1975 年，由投資界的傳奇人物約翰·博格（John C. Bogle）創立，Vanguard 以其成本低廉、以投資者為中心的理念而著稱。該公司總部設在美國賓夕法尼亞州的馬倫，是世界上最大的共同基金提供商之一，也是第二大 ETF 提供商。

投資者擁有的結構

Vanguard 獨特之處在於其所有權結構。與傳統的投資管理公司不同，Vanguard 屬於其基金持有人，這意味著投資者不僅擁有他們在 Vanguard 基金中的投資，實際上也是公司本身的擁有者。這種結構有助於確保公司的利益與投資者的利益一致，並且通常導致更低的管理費用和更高的回報率。

產品與服務

Vanguard 提供廣泛的投資產品，包括共同基金、ETFs、個人退休帳戶（IRA）、退休計劃服務以及其他金融規劃和諮詢服務。其產品覆蓋了多種資產類別，包括股票、債券、貨幣市場基金和平衡基金，滿足不同投資者的需求和風險承受能力。

投資哲學

Vanguard 堅信長期投資、分散化投資和低成本投資的重要性。公司以提供低成本的指數基金而聞名，這些基金旨在追蹤市場指數的表現，而不是試圖超越市場。約翰·博格是指數基金的先驅之一，他認為大多數主動管理的投資基金在長期內很難持續戰勝市場平均水平，特別是在扣除管理費用後。

全球影響力

隨著全球投資市場的發展，Vanguard 已將其業務擴展到世界各地，包括亞洲、歐洲和澳大利亞等地。該公司不僅服務於個人投資者，也為機構投資者、財務顧問和退休計劃提供服務。Vanguard 在全球投資管理領域的影響力日益擴大，其低成本投資理念也影響了整個行業的定價結構和投資策略。

總體來說，Vanguard 以其投資者優先的理念、低成本的產品和堅實的投資表現，成為了全球投資者值得信賴的合作夥伴。

Resilient architectures at scale Real-world use cases from Amazon.com (ARC305)

韌性架構的重要性

在當今的技術環境中，韌性架構是確保企業系統可靠並能夠應對各種故障和負載波動的關鍵。從 Amazon.com 的經驗中，我們學到了設計、測試和運營韌性系統的重要性。這些案例展示了如何通過隔離故障、自動擴展、解耦架構和深入監控來實現高可用性和可擴展性。

設計韌性：細胞化架構和解耦

透過細胞化架構，Amazon 將其系統分割成多個獨立的單元或"細胞"，每個細胞都能獨立地處理一部分工作負載。這種方法大大降低了單點故障對整體系統的影響，提高了容錯能力。同時，解耦的設計使得各個微服務可以獨立進行創新和疊代，從而加速開發流程並提高整體系統的靈活性。

測試韌性：混沌工程與負載測試

Amazon 透過混沌工程和負載測試來評估其系統的韌性。混沌工程，特別是通過 AWS 故障注入服務，允許團隊在控制的環境中引入故障，從而發現潛在的弱點並加以改善。這種主動尋找故障的方法，有助於提前識別並解決問題，進一步提高系統的可靠性。

運營韌性：度量和監控

為了保持系統的韌性，持續的監控和度量至關重要。Amazon 使用跨帳戶 CloudWatch 觀察性解決方案來集中監控其多元化的服務和應用程式。這種集中化的方法不僅提高了故障檢測的效率，還加快了故障排除過程，確保即使在高負載下系統也能保持高可用性。

結論

從 Amazon.com 的真實案例中，我們可以看到建立韌性架構需要從設計、測試到運營的全面考量。透過細胞化架構、混沌工程和全面監控，可以建立一個既靈活又可靠的系統，即使在面對不可預測的故障和負載變化時也能保持穩定運行。對於追求創新和可持續發展的 IT 專業人士而言，這些洞察提供了寶貴的指導和靈感。

補充

在探討建立大規模韌性架構的過程中，從設計、測試到運營每一步都充滿了挑戰和機遇。以下將深入探討細胞化架構、混沌工程與度量監控這三大主題，並闡述其技術細節與實踐要點。

設計韌性：細胞化架構和解耦

細胞化架構是一種將大型系統分割成多個小型、獨立運作的單元（細胞）的設計模式。每個細胞包含了完成特定功能所需的所有資源，如計算、儲存和網絡組件，並且與其他細胞隔離。這種隔離確保了當一個細胞遇到故障時，不會影響到其他細胞的運作，從而降低了系統整體的故障範圍（Blast Radius）。

在細胞化架構中，關鍵的技術考量包括細胞之間的路由策略、資料共享與同步機制以及細胞內部的資源管理。例如，路由策略可以基於特定的業務規則（如用戶地理位置或請求類型）來決定請求應該被導向哪個細胞。

解耦則是另一個關鍵概念，指的是系統中各部分之間的依賴關係最小化。在微服務架構中，每個服務都獨立於其他服務運作，只通過明確定義的 API 與其他服務交互。這種設計使得各個服務可以獨立開發、部署和擴展，從而提高了系統的靈活性和可維護性。

測試韌性：混沌工程與負載測試

混沌工程是一種通過主動引入故障來檢測系統韌性的實踐方式。這包括故意終止服務實例、模擬網絡延遲或斷開、製造資源耗盡情況等。透過這些實驗，團隊可以驗證系統的容錯和自我恢復能力，並在安全的環境中學習如何應對真實世界的故障情況。

負載測試則是指模擬高流量條件下系統的行為，以確定系統的性能瓶頸和擴展能力。透過持續增加請求率直至系統達到其極限，團隊可以評估系統在高負載情況下的表現，並進行必要的優化。

運營韌性：度量和監控

在現代雲計算環境中，有效的監控和度量是確保系統韌性的關鍵。這包括從基礎設施層面到應用層面的全面監控，並使用即時資料分析和可視化工具來洞察系統狀態。

跨帳戶 CloudWatch 觀察性解決方案允許組織集中收集和分析來自多個 AWS 帳戶和服務的監控資料。這使維運團隊可以在單一界面中查看和關聯來自整個組織的日誌、指標和追蹤資料，從而更快地識別和解決問題。

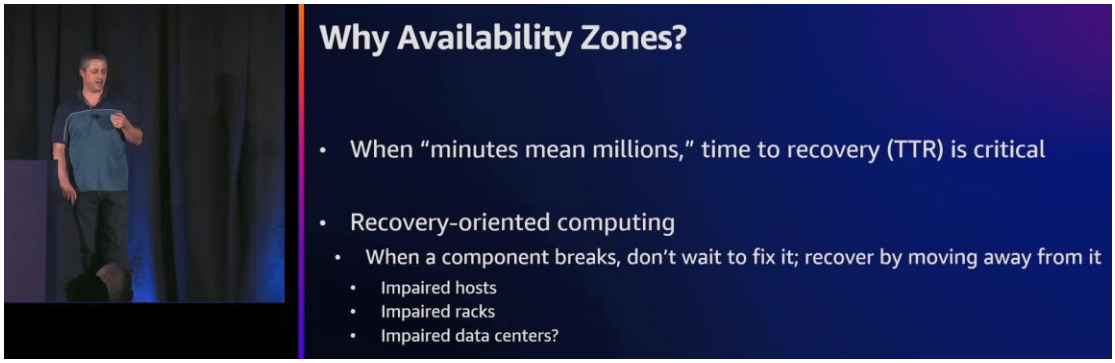
透過這些策略和技術，組織可以建立一個既靈活又韌性強的系統，能夠有效地應對各種挑戰，保障業務的持續運營。

Using zonal autoshift to automatically recover from an AZ impairment (ARC309)

在這場演講中，Deepak Sury 和 Gavin McCullagh 分享了關於如何利用區域自動轉移功能來自動從一個可用區的故障中恢復的深入看法。本次演講不僅提供了對 AWS 可用區的全面理解，還介紹了一項名為「區域自動轉移」的新功能，旨在幫助用戶在發生可用區故障時自動恢復服務。

AWS 的可用區設計哲學

AWS 的全球基礎設施由眾多可用區（AZ）構成，每個可用區都包含一個或多個物理上隔離的資料中心，但在網絡連接上保持緊密聯系。這種設計旨在實現高度的可靠性和故障隔離，使客戶能夠在不同的可用區中部署冗餘的應用副本，從而提高業務連續性和應對單點故障的能力。



圖說：Gavin 談到了亞馬遜網站和 AWS 在早期對可靠性的追求，並解釋了為什麼在遇到故障時快速恢復如此關鍵。他用“分鐘意味著百萬美元”來形容在繁忙時期，如節假日購物季，即時恢復的重要性。他還介紹了“恢復導向計算”的概念，強調在故障發生時快速切換到冗餘系統的重要性，而不是試圖修復損壞的部分。

區域自動切換（Zonal Autoshift）的創新之舉

Zonal Autoshift 是 AWS 為進一步提升應用韌性而推出的一項功能。當某個可用區發生故障時，這項功能能夠自動識別問題並將流量無縫切換到其他健康的可用區，從而確保服務的持續運行和最小化對終端用戶的影響。

技術實現

Zonal Autoshift 的實現依賴於 AWS 的高級路由能力和健康檢查機制。當 AWS 的監控系統檢測到某個 AZ 的異常指標時，如網絡延遲增加、錯誤率升高或系統資源不可用等，Zonal Autoshift 會被觸發，自動調整路由策略，將新的流量請求導向其他正常運作的 AZ。

自動化和智能化

Zonal Autoshift 的一大亮點在於其高度的自動化和智能化。系統無需人工干預，即可即時響應可用區的變化，確保流量在各個 AZ 之間的平滑轉移。這不僅大幅提高了故障恢復的速度，也降低了因人為操作錯誤導致的風險。

圖說：演講者正總結有關“區域轉移”的部分內容，這是一種在地理上分散的雲計算策略，用於在不同的區域之間轉移負載和資源。這通常用於提高可用性和恢復力，尤其是在面對單一資料中心或區域故障時。

應對硬故障和灰色故障

在雲計算環境中，硬故障和灰色故障是兩種常見的故障類型。硬故障如硬碟損壞或伺服器完全宕機等，相對容易被系統偵測和恢復。而灰色故障，如網絡延遲或服務響應不穩定等，則更為隱蔽且難以處理。

Zonal Autoshift 正是為了更好地應對這些挑戰而設計。通過細致的監控和智能的流量管理，即使是灰色故障也能被及時識別和緩解，確保系統的整體可靠性和性能。

實務應用和挑戰

實際部署 Zonal Autoshift 時，需要考慮多種因素，包括如何設計適應性強的應用架構、如何確保資料一致性和事務完整性、以及如何平衡成本和性能等。此外，還需要進行廣泛的測試，以確保在各種故障情景下系統都能正常運作。

可持續性及成本效益

導讀

在面對全球氣候變遷和資源有限的挑戰下，可持續性和成本效益已成為智慧電網、電力系統和電力公司不可或缺的考量因素。可持續性不僅涉及環境保護，也關係到長期經營的穩定性和社會責任。對於這些企業而言，實現能源效率的提升和二氧化碳排放的減少，是達成可持續發展目標的關鍵步驟。此外，成本效益的追求促使企業探索創新的技術和管理方法，以最佳化營運成本和提高能源使用效率。這不僅能夠增強企業的市場競爭力，也是對抗能源危機和環境變遷的重要策略。

Improving your AWS cost reporting (COP203)

在「Improving your AWS cost reporting」這場演講中，演講者深入介紹了 AWS 針對成本報告和管理所提供的一系列新功能和最佳實踐。藉由展示如何有效利用 AWS 計費與成本管理控制台的改善、成本探索器的擴展功能，以及新的資料導出體驗等工具，演講者向 IT 專業人士指出了如何更精確地追踪和控制雲端支出。此外，透過應用程式註冊庫與成本管理的整合以及 AWS Billing Conductor 的創新使用，這場演講不僅提升了成本效率和透明度，也強調了策略性資源分配在雲端經濟學中的重要性。

Saving on AWS If not, what are you waiting for (COP218)

這場演講由 Rahul Subramaniam 主持，他從雙重視角出發，分享了如何在 AWS 上實現成本節約的實用策略。通過分析 EC2、S3 等 AWS 資源的低利用率問題，Rahul 揭示了許多企業在雲端資源管理中存在的浪費。他提出了一系列解決方案，包括利用最新的實例、採用智能分層策略，以及部署自動化工具，如 CloudFix，來提高資源利用效率。這場演講不僅強調了成本節約的重要性，也指出了透過持續的努力和策略調整來實現長期成本優化的必要性。

Sustainable compute: Reducing costs and carbon emissions with AWS (CMP212)

在這場演講中，講者透過攀岩的比喻，強調了在雲計算中實現資源有效利用的重要性。AWS 的可持續性承諾，特別是其轉向 100%再生能源的目標，為企業提供了減少碳足跡的機會。Spot 實例和 Graviton 處理器的介紹，展示了如何在保持高性能的同時，降低營運成本和減少環境影響。Adobe 案例研究進一步證明了轉移到更節能處理器的長期效益，包括顯著的成本節約和減少二氧化碳排放。

Understanding the measurable value of the cloud (GDS103)

該演講深入探討了企業轉向雲端的多重益處。除了直接的成本節約外，上雲還帶來了業務敏捷性、運營韌性和員工生產力的提升。通過分析真實案例，如 Adobe 的上雲故事，演講者強調了雲端服務對於支持業務成長和適應快速變化市場條件的關鍵作用。

Optimizing TCO for business-critical analytics (ANT209)

本場演講聚焦於如何為關鍵業務分析優化總體擁有成本。講者探討了建立有效資料策略、選擇適當的分析工具和架構的重要性，並強調了利用 AWS 服務如 Glue、Redshift 和 S3 智能分層來降低成本的策略。Expedia 的案例研究提供了一個實際的範例，展示了如何通過管理雲基礎設施中的資料來實現成本和效率的最佳化。

Reinvent your cloud strategy: Optimize performance & cut cloud costs (CON326)

在這場演講中，Snap 公司分享了他們如何通過雲端策略的優化來改善服務並降低成本。特別是透過 Granulate 技術的應用，Snap 實現了即時的性能優化和資源分配，大幅提升了運營效率並降低了雲端支出。

Building your green future today: Unlocking secrets to sustainability (COP229)

這場演講強調了當前技術和企業界在實現可持續發展方面所扮演的關鍵角色。講者探討了技術創新如何推動能源效率和減少環境足跡，並強調了可持續性作為未來業務競爭優勢的重要性為了滿足您的要求。

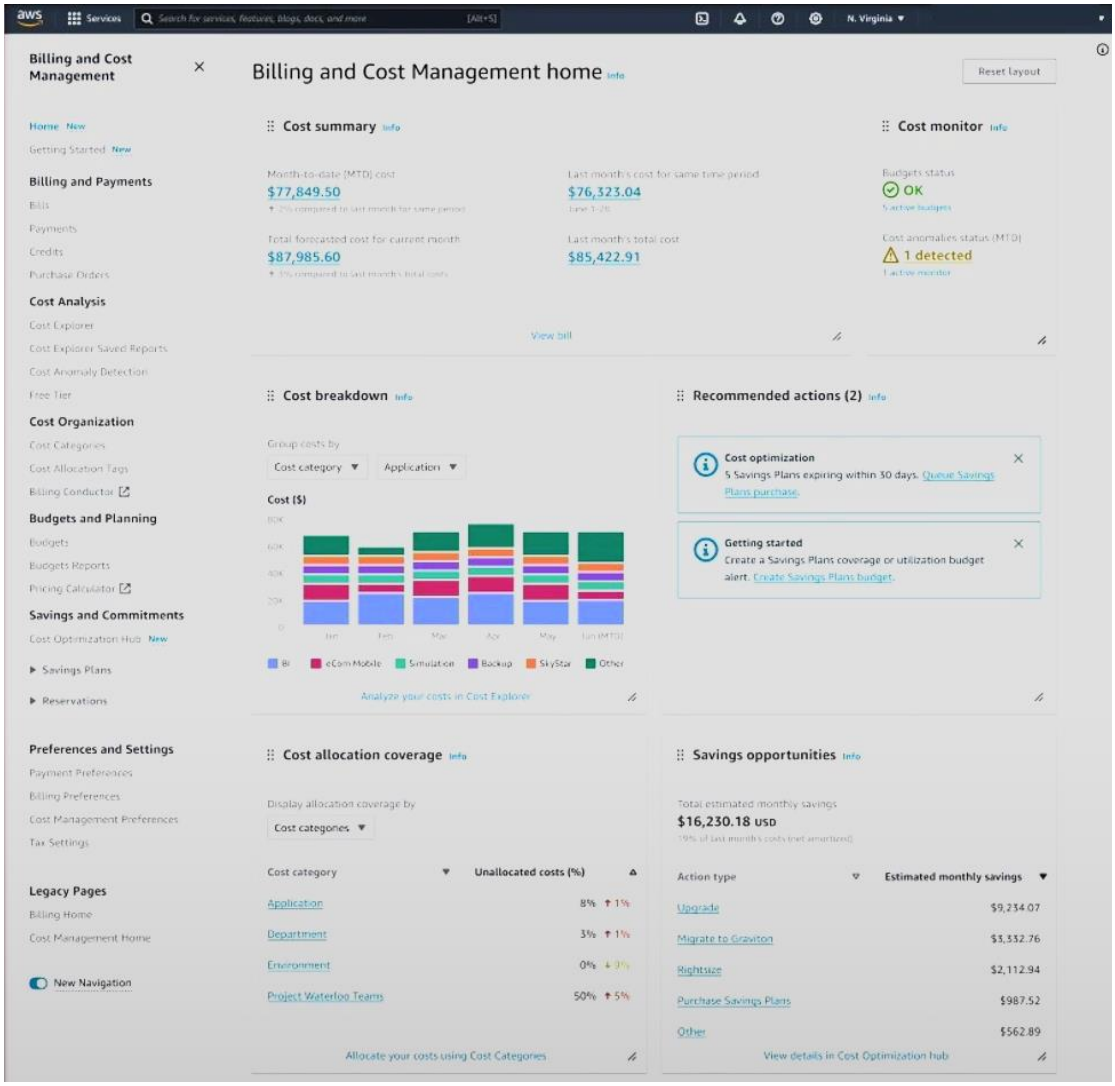
這些演講對於智慧電網、電力系統和電力公司來說，提供了寶貴的參考價值和學習機會。從中，我們可以得知，透過創新技術和策略的應用，不僅可以達到節能減碳的目標，也能實現成本的有效控制和業務的持續增長。未來趨勢可能會更加重視綠色能源和智能技術的融合，推動電力行業向更加可持續和高效的方向發展。對於智慧電網、電力系統和電力公司而言，制定以資料為驅動的經營策略，投資於先進的能源管理和分析工具，並積極探索再生能源和智能網絡技術的應用，將是實現長期成功的關鍵。

Improving your AWS cost reporting (COP203)

在這場演講中，我有幸聽到了 Bowen Wang 和 Matt Berk 分享關於如何改善 AWS 成本報告的深刻看法。隨著雲端運算成為企業運營的不可或缺部分，精確且即時的成本管理已成為各組織不可忽視的重要任務。

首先，講者指出，"你無法改善你無法測量的"，這話在雲成本管理中尤其關鍵。正確且詳細的成本報告不僅讓利害關係人能夠做制定更有效的成本管控政策或發現成本優化機會，更是推動組織向前邁進的關鍵。

然而，面對市場上琳瑯滿目的成本報告解決方案，如何選擇最適合自己需求的服務？AWS 提供了一系列工具和服務，旨在幫助用戶從各個角度獲取成本和使用資料，從而提供全面的成本透明度。這些工具包括新推出的 AWS Billing and Cost Management 控制台首頁，它為用戶提供了一個統一的儀表板，以便於獲取和分析成本資料。



圖說：AWS Billing and Cost Management 控制台的截圖，包括了如下幾個部分：

成本總結(Cost summary)：顯示了迄今為止本月的成本、預測的本月成本以及上月同期的成

本。

成本監控(Cost monitor)：提供了預算狀態和成本異常監控。

推薦行動(Recommended actions)：包括成本優化建議，如節約計劃的購買。

成本分解(Cost breakdown)：按成本類別或應用程式分組成本，並提供柱狀圖進行視覺化展示。

成本分配覆蓋率(Cost allocation coverage)：展示了成本類別下的分配和未分配成本。

節約機會(Savings opportunities)：提供了估計的月度節約金額和相應的行動類型，例如升級或遷移至 Graviton。

此外，AWS Cost Explorer 的更新使得歷史資料的保留時間延長，並提供了更細緻的資源層級資料，使用戶能夠進行更深入的成本分析。這些功能的改善意味著組織現在可以更容易地進行年度比較分析，並對特定 AWS 服務的使用情況有更清晰的了解。

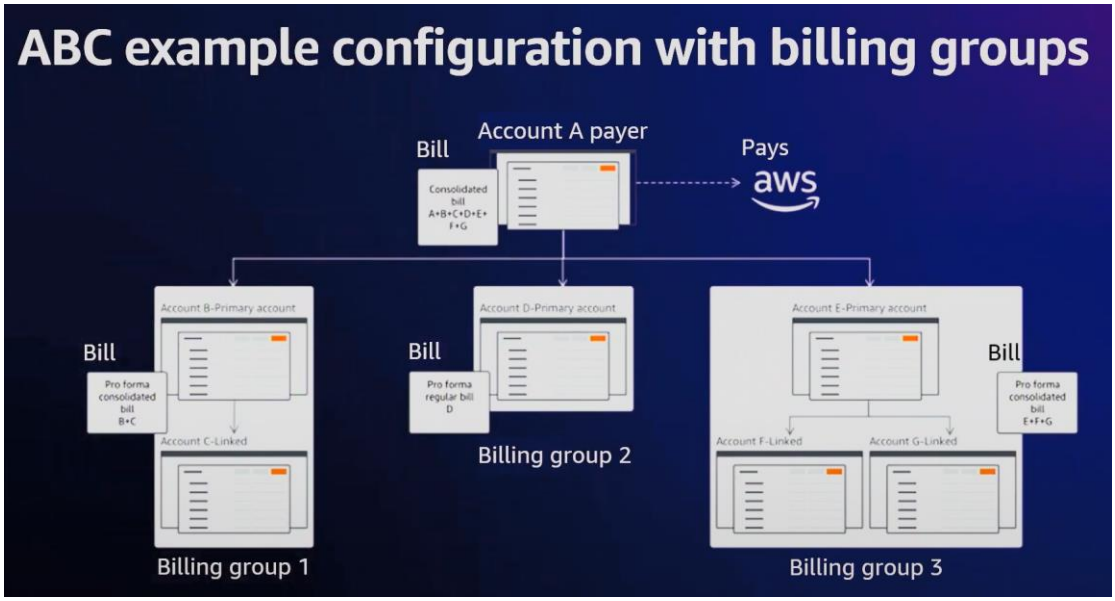
圖說：這張圖片顯示了如何利用 AWS 的 Cost Explorer 視覺化呈現 AWS 的使用成本。

左邊的圖表顯示了過去 12 個月的成本趨勢（Trailing 12-month view），展示了每個月的成本變化，有助於追踪和分析長期成本趨勢。

右邊的圖表則突出了按購買選項分類的成本（Filter by purchase options），比如按需（On Demand）、儲蓄計劃（Savings Plans）和預留（Reserved），讓使用者能夠了解不同購買選項對總成本的貢獻。

兩個圖表上方都顯示了總成本($289,739.52)和平均每月成本($24,144.96)，而右側圖表還顯示了購買選項的數量。這些資料可以幫助用戶做出成本效益分析和預算決策。在視覺化工具的幫助下，用戶可以更直觀地理解成本結構，並識別降低成本的機會。

在成本分配方面，AWS 提供了基於標籤和規則的方法，讓用戶可以根據業務需求靈活地分配成本。此外，AWS Billing Conductor 提供了一種方法，允許用戶根據自己的計費規則來展示和回收成本，這對於實現透明的內部計費和成本分配至關重要。



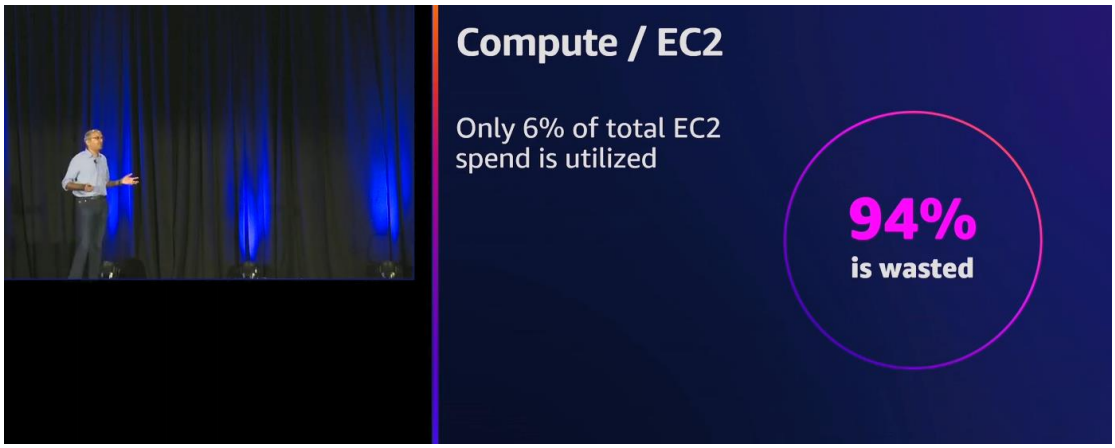
圖說：這幅圖片展示了使用 AWS Billing Conductor（ABC）進行計費配置的範例，其中包含了多個計費組。圖片說明了一種結構，在這種結構中，不同的 AWS 帳戶被整合到單獨的計費組內，並由一個主帳戶（Account A payer）負責支付費用。每個計費組都有一個主要帳戶，該帳戶接收關於其下聯結帳戶的形式化合併帳單。這種配置使得管理計費更加清晰，也方便按不同的業務單位或項目將成本分配到正確的部門。例如，計費組 1 可能代表了部門 B 和 C 的成本，計費組 2 代表了部門 D，而計費組 3 則包含了 E、F 和 G 部門的成本。這種方法為組織提供了靈活性，以根據不同的計費需求或內部計費結構定制和管理成本。

最後，正確設置並持續追踪關鍵績效指標(KPIs)是評估雲端財務管理實踐成效的重要手段。透過與業務成果指標相關聯的 KPIs，組織可以更有效地衡量雲端投資的實際價值，並持續優化其雲端策略。

透過這次分享，Bowen Wang 和 Matt Berk 不僅提供了一套全面的工具和策略，更重要的是，他們強調了持續改善和適應變化的重要性。隨著技術的進步和組織需求的變化，有效的雲成本管理策略應該是動態的，能夠支持組織實現其長遠目標。對於任何希望最大化其雲端投資回報的組織而言，掌握這些實踐和工具是成功的關鍵。

Saving on AWS If not, what are you waiting for (COP218)

在這場關於 AWS 成本最佳化的專題演講中，由 CloudFix 的 CEO 兼一大企業集團的 CTO，Rahul Subramaniam 親自主講。這場精彩的演講不僅分享了他們從管理約 40,000 個 AWS 帳戶中獲得的經驗和看法，還提出了實用的優化策略。



Rahul 指出，在 EC2（Amazon Elastic Compute Cloud）的使用上，僅有 6%的總開銷被實際利用，而有高達 94%被浪費。這強調了在雲計算資源管理方面的一個重要問題，即存在大量的資源未被充分使用，導致成本上的極大浪費。這個資料可以成為推動企業進行成本優化和資源管理改善的有力論點。

首先，Rahul 提到 AWS 上的大部分開支集中在 EC2 服務上，佔總帳單的 40%，但驚人的是，EC2 實例的平均利用率僅為 6%。這意味著有大量的資源被浪費，尤其是在開發和測試環境中。此外，S3 服務中有超過 90%的物件在整個生命週期中只被訪問一次，顯示出在資料儲存方面存在著巨大的浪費。

在網絡配置方面，Rahul 強調了預設配置可能導致的高額成本，尤其是當應用程式和部署規模擴大時。例如，EC2 實例與 S3 間的預設流量是通過互聯網進行的，會產生額外的出口流量費用，而透過適當的 VPC 設定可以將這部分成本降至零。

Rahul 也分享了一些關於如何有效實現成本節約的看法。對於 EC2 來說，除了常規的大小調整之外，還有兩種不那麼常見但非常有效的策略：現代化和重構。現代化指的是將實例更新至最新的世代，而重構則涉及更改實例類型以利用性能更高或成本更低的選項。在儲存方面，他建議清理閒置資源，啟用 S3 的智能分層，並將 GP3 作為默認卷類型。

在網絡優化方面，他提醒我們注意閒置的彈性 IP 和 NAT 閘道，並建議使用 VPC 端點來優化 AWS 內部的流量。此外，對於那些需要托管靜態內容的用戶，Rahul 推薦使用 S3 配合 CloudFront，這不僅成本更低，還能提供更好的性能和可靠性。

最後，Rahul 強調了實施成本優化策略時遇到的挑戰，並提出了一些解決方案，如採用自動化工具、建立對成本負責的文化，以及定期復查和調整策

略。他還特別推薦了 CloudFix 這一工具，它能夠幫助自動實施 AWS 推薦的許多成本優化措施，讓開發團隊能夠專注於他們的核心工作，同時保持雲成本的最優化。

透過這場深入的分享，Rahul 不僅提供了具體的資料和策略來指導 AWS 用戶如何更有效地管理他們的雲資源，也強調了持續監控和優化的重要性，以確保在快速變化的技術環境中保持成本效益。對於每一位 AWS 用戶來說，這不僅是關於節省開支的問題，更是關於資源效率和可持續發展的問題。

技術細節說明

Subramaniam 在演講中提到了針對 AWS 資源的多個優化策略，這些策略旨在幫助企業降低成本，提高效率。以下是對他提到的一些主要策略的詳細說明：

EC2 優化

1. EC2 現代化：

將現有的 EC2 實例更新到最新一代，以利用更高的性能和更低的成本。舊一代的實例相比新一代通常會更貴且性能較差。

例如，將 M4 實例更新到 M5 或 M6，可以獲得更好的性能和更高的網絡帶寬，同時降低每小時的成本。

2. 重定型（Retyping）：

將實例從一種類型轉換到另一種類型，特別是考慮從 Intel 或 AMD 轉換到 Graviton（ARM 架構）。Graviton 實例在性能和成本效益上可能提供顯著優勢。

3. 權限調整（Rightsizing）：

根據實際使用情況調整 EC2 實例的大小。這涉及到評估 CPU、內存、磁盤 I/O 和網絡 I/O 的使用情況，並選擇最適合工作負載需求的實例大小。

使用 AWS Compute Optimizer 工具來獲取基於使用模式的權限調整建議。

S3 優化

智能分層（Intelligent Tiering）：

啟用 S3 智能分層，根據對象訪問模式自動將資料移動到成本更低的儲存層。這樣可以在不影響資料可訪問性的情況下實現成本節省。

網絡設置優化

避免使用默認配置：

調整和優化 VPC 和 NAT 閘道配置，避免不必要的資料通過公共互聯網傳輸，從而節省出口流量費用。

使用 VPC 端點來保持 AWS 服務間的流量在 AWS 內部，減少資料傳輸費用。

儲存優化

1.刪除閒置資源：

定期審查和刪除未使用的 EBS 卷和 S3 對象，以避免持續支付不必要的儲存費用。

2.GP3 卷：

將 EBS 卷從 GP2 遷移到 GP3，以利用更低的成本和相等或更好的性能。

RDS 優化

1.閒置資源管理：

刪除未使用的 RDS 實例，特別是在開發和測試環境中，這些環境中的閒置資源尤其多。

2.無伺服器化（Serverless）：

考慮使用 Aurora Serverless 資料庫，這樣可以根據負載自動調整容量，避免支付未使用的固定容量的成本。

3.權限調整和重定型：

與 EC2 相似，RDS 實例也應該根據實際需要進行調整和可能的重定型，以確保成本效益。

AWS Compute Optimizer

AWS Compute Optimizer 是一項由 Amazon Web Services 提供的服務，旨在幫助用戶優化他們的 AWS 計算資源，以提高性能並降低成本。它使用機器學習來分析歷史使用資料，並基於這些資料為 EC2 實例、Auto Scaling 組、EBS 卷、Lambda 函數和其他 AWS 資源提供優化建議。

主要功能

1.權限調整建議：

Compute Optimizer 評估您當前的 AWS 資源配置和使用情況，並提供有關如何更改資源大小（例如 EC2 實例類型）以提高性能和成本效率的建議。

2.實例類型推薦：

根據您的使用模式和需求，推薦更適合您工作負載的 EC2 實例類型，可能包括不同的計算、記憶體和網絡帶寬選項。

3.EBS 卷性能改善：

Compute Optimizer 可以分析您的 Amazon EBS 卷使用情況，並建議配置更改以提高儲存效率和性能。

4.Lambda 函數優化：

對於 AWS Lambda 函數，Compute Optimizer 會評估函數配置和使用情況，並提供記憶體大小調整建議，以優化性能和成本。

5.安全性和無風險：

提供的建議基於過去的使用情況，並考慮到避免性能降低，從而確保建議的

實施不會對應用程式的正常運行造成風險。

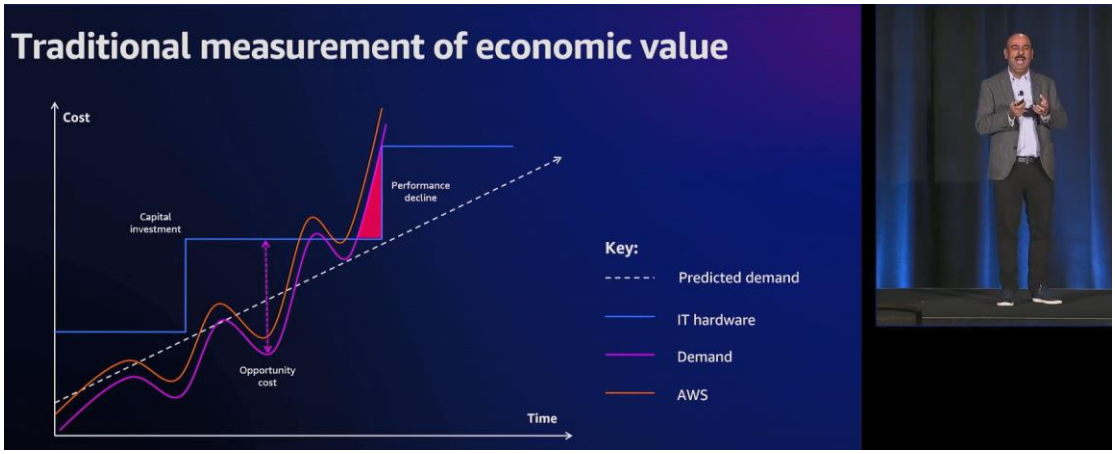
使用方式

使用 AWS Compute Optimizer 前，需要在 AWS 管理控制台中啟用該服務。
啟用後，它會自動開始分析支持的資源，這可能需要一些時間來收集足夠的使用資料。分析完成後，您可以在 AWS Compute Optimizer 控制台中查看針對各個資源的建議。
使用者可以根據這些建議進行手動調整，或者使用其他 AWS 服務和自動化工具來應用這些變更。

好處

成本節省：通過更有效地使用資源，降低不必要的開銷。
性能提升：確保資源配置最適合當前工作負載，從而提高應用程式性能。
簡化管理：自動化的分析和建議減少了手動監控和調整資源配置的需求。
定製化建議：基於您特定使用情況的個性化建議，而不是一般性的最佳實踐。

Understanding the measurable value of the cloud (GDS103)



圖說：Pranav Bhushan 解釋傳統衡量經濟價值的模式。成本隨著時間的推移呈現了三個階段的變化：

1. 資本投資（Capital investment）在初期，IT 硬件投資導致成本急劇上升。
2. 機會成本（Opportunity cost）隨著需求的不確定性，如果需求預測不準確，可能會有遺失收益的機會成本。
3. 性能下降（Performance decline）隨著時間的推移，傳統 IT 硬件的性能可能會下降，需要更多的投資來維持或更新系統。

圖中有三條曲線：虛線代表預測需求（Predicted demand），藍色實線代表 IT 硬件的成本（IT hardware），而橙色實線代表在 AWS 雲端平台上的成本（AWS）。從圖形可以看出，使用 AWS 的成本隨時間呈現較為平穩的增長，相比之下，傳統 IT 硬件成本在初期較高，且會因性能下降而需要進一步投資。

使用 AWS 雲端服務可以減少初期的資本投資，且可以更靈活地應對需求變化，避免機會成本的損失，並降低隨著時間造成的性能下降問題。

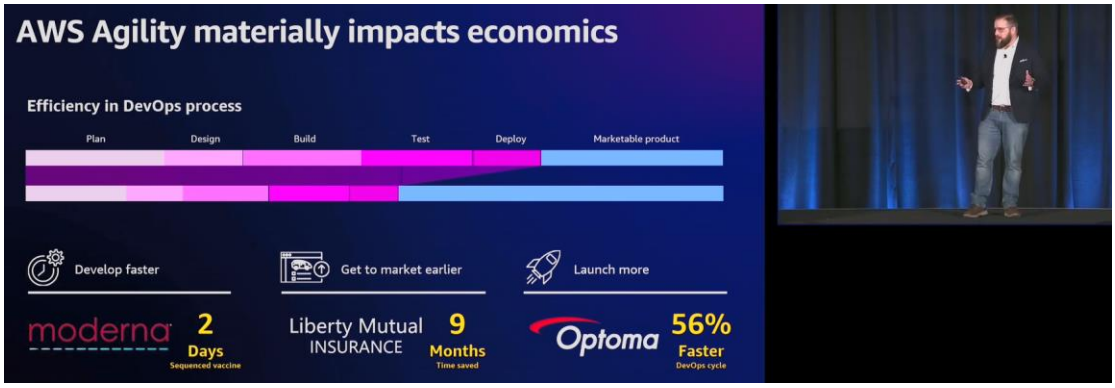
在這場演講中，Pranav Bhushan、Erik Satre 和 Sridhar Ayala 共同探討了上雲的可衡量價值。他們不僅深入剖析了企業在考慮上雲時應評估的關鍵績效指標（KPI），還分享了 Adobe 等公司的真實案例，展示了上雲如何在業務敏捷性、運營韌性、員工生產力和成本節約方面帶來顯著價值。

演講的開場由 Pranav Bhushan 揭幕，他強調了上雲對企業的重要性，並介紹了 AWS 在全球範圍內如何協助客戶評估上雲的財務效益。他通過一個親身經歷的故事，生動地描繪了在傳統 IT 架構下購買硬件、等待交付的繁瑣過程，以及這一過程如何延遲了項目進度並對業務造成影響。相對於此，雲端服務如 AWS 提供的靈活性和即時可用性，為企業帶來了前所未有的運營效率。

接著，Pranav 引入了一項由 IDC 執行的研究，這項研究顯示企業從雲端獲得的價值遠超單純的成本節約。根據這項研究，雲端帶來的價值可以分為四大類：成本節約、員工生產力、運營韌性和業務敏捷性，其中業務敏捷性佔了最大比重，達到 55%。這一發現挑戰了許多企業過分關注 IT 硬件成本節約的傳統

觀念，促使他們重新評估上雲的全面價值。

Erik Satre 深入探討了如何在業務案例中納入這些非成本類的經濟價值，並通過具體案例，如 Moderna 和 Liberty Mutual Insurance，展示了企業如何通過提高 DevOps 流程效率、加快產品上市時間等方式從上雲中獲益。



圖說：Erik Satre 說明 AWS 的敏捷性如何對經濟產生重大影響，特別是在 DevOps 過程中提升效率。從規劃、設計、構建、測試到部署階段，一直到產品可上市銷售，AWS 的敏捷性使得整個過程更加高效。簡報中的三個案例突顯了 AWS 加速開發的具體成效：

1. Moderna：在短短 2 天內完成了疫苗的序列化工作，展示了 AWS 在處理大規模高性能計算工作負載時的速度和效率。
2. Liberty Mutual Insurance：透過利用 AWS 服務，將一個預計 12 個月開發的產品開發時間縮短至 3 個月，節省了 9 個月的時間，從而更快地進入市場。
3. Optoma：發現在 AWS 上進行 DevOps 流程比在本地環境快 56%，這使得他們能夠更快地推出新的軟件版本，並且在相關活動上實現了 35%的成本節省。

Erik Satre 強調了 AWS 在加速開發和上市時間方面的優勢，並且具體展示了在不同企業和領域中這種敏捷性如何轉化為實際的經濟效益。

Sridhar Ayala 分享了 Adobe 如何通過與 AWS 雲端經濟學團隊合作，對其 GPU 工作負載進行了全面的價值分析，最終決定將工作負載遷移到 AWS。這一決策不僅基於成本考量，還充分考慮了業務敏捷性、市場需求和供應能力、以及專注於核心競爭力的重要性。Sridhar 強調了制定業務案例時考慮全面因素的重要性，包括風險評估和對業務關鍵績效指標的影響。

總結來說，這場演講不僅提供了深入的洞見和策略，幫助企業評估上雲的全面價值，還通過真實案例展示了這些策略如何在實際中被成功應用。企業可以從中獲得寶貴的經驗，以更全面、更戰略性的視角評估上雲，從而最大化其在雲端旅程中的投資回報。

具體案例

在這場演講中，提到了幾個具體案例，這些案例展示了企業如何通過上雲實現顯著的業務價值。以下是對這些案例的詳細說明：

PBS

作為一家美國的媒體和娛樂公司，PBS 通過 330 個電視台向 1 億觀眾提供娛樂和教育內容，其中有 3200 萬觀眾是在線觀看。PBS 遷移到 AWS 後，利用 Amazon Personalize 為觀眾提供個性化的內容推薦，從而減少了客戶流失率，提高了免費訂閱者轉為付費訂閱者的轉換率，並實現了 50%的流媒體錯誤降低，從而提升了觀眾的參與度。

Netflix

Netflix 是一家在 190 個國家向 1 億訂閱者提供內容的在線內容提供商。Netflix 面臨的挑戰是如何將交易郵件和促銷郵件發送給客戶，而不被互聯網服務提供商作為垃圾郵件阻擋。通過使用 Amazon Simple Email Service，Netflix 能夠將發送郵件的域分散到多個 IP 地址上，從而避免了郵件被屏蔽的問題，並實現了 99%的客戶收件箱放置率。

ISV 客戶群體

在對 2000 名 AWS 客戶進行的基準調查中，100 名來自獨立軟體供應商(ISV)行業的客戶報告說，他們平均看到交易量增加了 98%，能夠支持資料總量增加 93%。

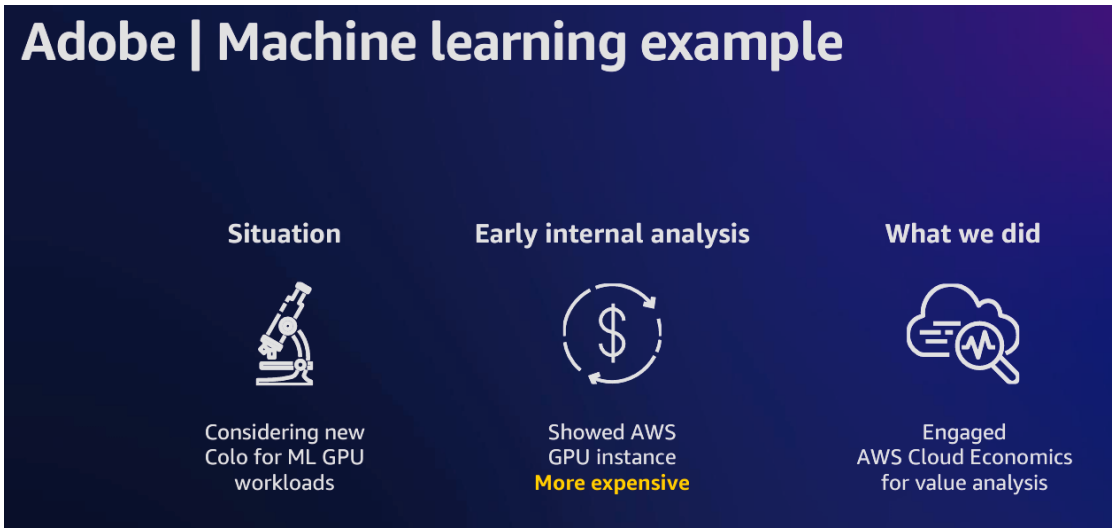
Salesforce

Salesforce 在 2016 年選擇 AWS 作為其首選雲提供商，並且在上雲後見證了數字營銷解決方案的 25%增長。Salesforce 面臨的挑戰是，每當它想要進入新的地理市場時，都需要等待 6 個月的時間來建立新的資料中心，以滿足資料居住要求。通過轉移到 AWS，Salesforce 能夠利用 AWS 在這些地理位置的現有區域，從而將啟動時間從 6 個月縮短到 4 小時，並在每個新地理區域中僅用 6 周就推出新產品。

Adobe

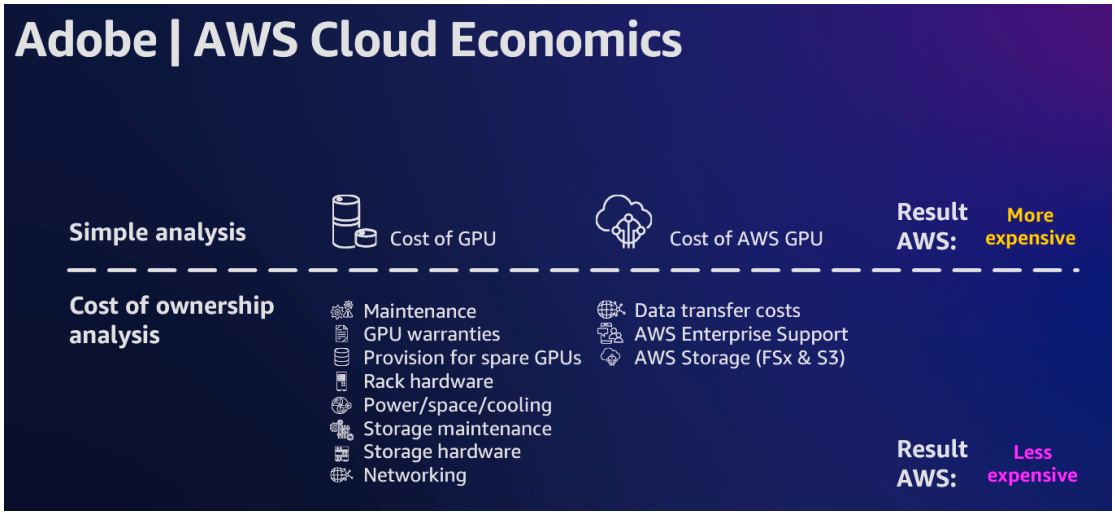
Adobe 的案例是一個深入探討上雲對企業價值產生重大影響的實例。在這個案例中，Adobe 面臨著決定是否將其機器學習 GPU 工作負載遷移到 AWS 雲端的挑戰。這個過程涉及多個階段，包括初步分析、成本擁有權分析和經濟價值分析，最終導致 Adobe 選擇將工作負載遷移到 AWS。

初步分析



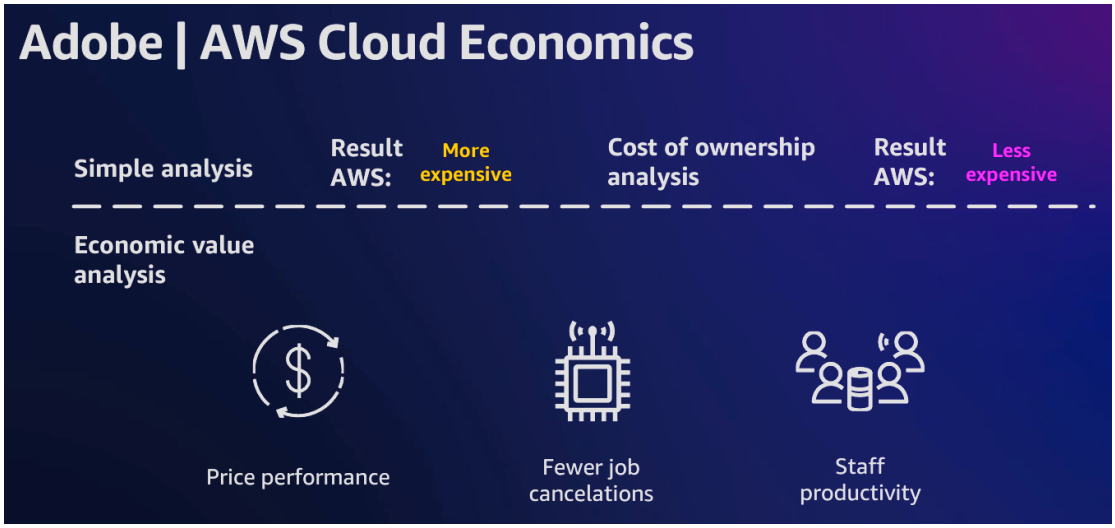
Adobe 最初的分析顯示，將 GPU 工作負載遷移到 AWS 的成本看似高於在內部或共位設施（Colo）中自行管理這些工作負載。這主要基於硬件成本的直接比較。

成本擁有權分析



隨後，Adobe 與 AWS 的雲端經濟團隊合作，進行了更全面的成本擁有權（TCO）分析。這個分析考慮了更多相關成本，包括維護、GPU 保修、備用 GPU 的準備、機架硬件、功率/空間/冷卻、儲存維護和硬件、網絡等因素。同時，也考慮了 AWS 端的資料傳輸成本、企業支持和儲存成本。這一全面分析顯示，AWS 的總成本略低，使選擇變得更加接近。

經濟價值分析



進一步的分析聚焦於 AWS 遷移的經濟價值，包括價格性能比、工作取消和延遲的減少以及員工生產力的提高。這些因素表明，儘管 AWS 的直接成本可能更高，但其提供的額外價值使得總體經濟效益更加有利。

決策與執行

考慮到時間至市場、預期的需求增長以及對可靠規模化能力的需求，Adobe 決定將其機器學習 GPU 工作負載遷移到 AWS。這一決策不僅基於成本分析，還基於能夠使 Adobe 團隊專注於其核心競爭力和創新而非基礎設施管理的戰略考量。

這些案例不僅展示了上雲如何幫助企業提升業務敏捷性、提高運營效率和員工生產力，還強調了在制定上雲策略時考慮全面因素的重要性。這些成功故事提供了有力的見證，說明企業如何通過上雲實現其業務目標和增長願景。

Optimizing TCO for business-critical analytics (ANT209)

隨著雲端技術的快速發展和企業資料量的爆炸式增長，有效管理雲端成本已成為許多組織面臨的一項重大挑戰。這場演講的主講者 Adam Driver 和 Kevin Lewis，分享了他們的專業看法和建議，幫助企業最大化雲端投資的回報，特別是在商業分析領域。

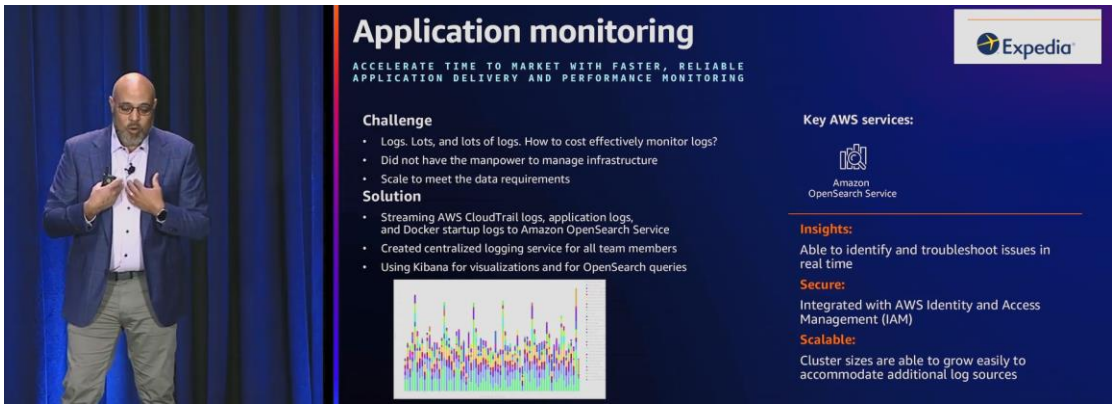
演講一開始，Adam Driver 引用了一篇 Forbes 文章，著重討論了轉移到雲端的隱藏成本及其對 IT 預算的影響。文章強調了企業在雲端轉型過程中可能遇到的過度支出問題，以及如何通過精細化的優化策略來尋找並減少這些不必要的開支。

隨後，他們提到了 Gartner 的一項預測，指出到 2025 年，公有雲計算的支出將超過 IT 支出的一半。這一資料突顯了雲計算在當代企業運營中的重要性，同時也突出了管理和優化雲端支出的迫切需求。

為了幫助企業應對這些挑戰，講者介紹了五大關鍵策略，主要針對如何優化企業的雲端成本和提高業務效率。這些策略包括：

1. **發展良好的資料策略**： 確立一套清晰的資料管理框架，包括資料收集、處理、儲存和分析的準則。這有助於減少重複工作，提高資料質量和利用率。
2. **選擇正確的工具**： 根據企業的具體需求和目標選擇合適的雲端服務和工具。選擇適當的工具不僅能提高工作效率，還能幫助企業節省成本。
3. **利用自動化服務進行優化**： 利用自動化技術減少手動操作，提高運營效率和穩定性，從而實現成本優化。
4. **整合到企業的資料治理架構**： 將上述策略融入到企業現有的資料治理架構中，確保技術和業務流程的一致性，以支持成本效益和業務價值的最大化。
5. **持續監控和評估**： 實施持續的監控和評估機制，以跟踪成本優化措施的效果，及時調整策略以應對變化的業務需求和市場環境。

Expedia 的案例研究



圖說：Kevin Lewis 介紹了應用監控系統的挑戰和解決方案，目的是通過更快、更可靠的應用交付和性能監控來加速產品上市時間。挑戰包括了大量的日誌資料處理、人力資源不足以及需要擴展以滿足資料要求。解決方案則是使用了 Amazon OpenSearch Service 來流轉 AWS CloudTrail 日誌、應用日誌和 Docker 啟動日誌，並創建了一個為所有團隊成員提供的集中式日誌記錄服務，同時使用了 Kibana 進行視覺化和 OpenSearch 查詢。幻燈片還強調了使用此系統帶來的洞察力，即能夠即時識別和排查問題，其安全性得益於與 AWS 身份和訪問管理（IAM）的整合，以及其可擴展性，指出集群大小可以輕鬆增長以容納更多的日誌來源

Expedia 面臨的挑戰是如何高效地管理來自 AWS 服務、非 AWS 服務以及內部系統的大量日誌資料。隨著資料量的爆炸性增長，傳統的日誌管理方法變得不再可行，這對於快速識別和解決問題至關重要。為了解決這一挑戰，Expedia 採取了以下步驟利用 Amazon OpenSearch 和 Kibana 實現高效的日誌監控和分析：

整合日誌資料源

Expedia 需要收集來自多個來源的日誌，包括 AWS 服務（如 Amazon EC2、Amazon S3 等）、非 AWS 服務以及他們自己的內部應用系統。他們通過各種整合和日誌轉發機制將這些日誌資料匯聚到一個中央位置。

利用 Amazon OpenSearch 處理和儲存日誌

Expedia 選擇 Amazon OpenSearch 作為其日誌資料的處理和儲存解決方案。OpenSearch 是一個可擴展的全文搜索和分析引擎，非常適合處理大量日誌資料。它可以即時索引、搜索和分析資料，從而加快問題識別和解決的過程。

使用 Kibana 進行資料可視化和分析

Kibana 是一個開源的資料可視化平台，與 OpenSearch 緊密整合。Expedia 利用 Kibana 提供的豐富的圖表、圖形和儀表板功能，對日誌資料進行可視化，從而使維運團隊能夠直觀地了解系統狀態、監控趨勢和迅速識別異常。

自動化和優化

為了管理日誌資料的爆炸性增長並提高效率，Expedia 實施了多種自動化和優化策略。這包括自動化日誌收集和處理流程、使用 Amazon OpenSearch 的自動擴展功能以適應資料量的變化，以及優化索引策略以提高搜索效率。

提高問題識別速度

通過上述步驟，Expedia 能夠大幅度提高問題識別和解決的速度。即時日誌分析和高效的資料可視化使得維運團隊能夠迅速定位問題根源，從而縮短系統故障的解決時間，提高系統的整體穩定性和可靠性。

通過這樣的實踐，Expedia 成功地應對了日誌資料管理的挑戰，不僅提高了維運效率，還確保了系統的高可用性和性能。這一案例展示了如何通過利用雲服務和先進的分析工具來優化大資料處理和分析的過程。

補充

AWS Glue、Amazon Redshift、Amazon EMR 和 Amazon S3 智能分層是 AWS 提供的幾項強大的雲服務，它們共同支持了資料處理、儲存和分析的各個方面。

AWS Glue

AWS Glue 是一項完全管理的 ETL（提取、轉換和加載）服務，使得準備和加載資料變得簡單。它可以自動發現使用者的資料，並在 AWS 的儲存和資料庫服務間儲存關聯的元資料。Glue 提供一個圖形界面來創建資料轉換邏輯，也可以直接編寫程式碼。它還能自動生成轉換程式碼，並且可以按需或定時運行 ETL 工作流，從而簡化了資料整合過程。

Amazon Redshift

Amazon Redshift 是一個完全管理的、具有高性能的資料倉儲服務，它允許您輕鬆地分析所有資料使用 SQL 和現有的商業智能工具。它使用列式儲存和大規模並行處理技術來提高查詢性能，適合處理大量資料和復雜的查詢。Redshift 支持從各種資料源載入和直接查詢資料，包括 AWS 內部的服務如 S3、DynamoDB 等。

Amazon EMR

Amazon EMR（Elastic MapReduce）是一個雲服務，用於處理大量資料。它利用開源框架，如 Apache Hadoop、Spark、HBase 和 Presto 等，提供了一個叢集環境來處理、分析和轉換資料。EMR 可以處理和分析儲存在 Amazon S3 或其他分佈式文件系統中的資料。它支持即時分析、機器學習、資料轉換等多種使用情境，並能根據需要動態調整計算資源。

Amazon S3 智能分層

它自動將資料移動到最符合資料訪問模式的儲存層。例如，它可以將經常訪問的資料保留在可快速訪問的層，而將很少或從未訪問的資料移動到成本更低的層。這一智能層級選擇基於機器學習算法，無需進行復雜配置或標籤，從而簡化了資料的生命週期管理。

這些服務組合在一起提供了一套全面的資料管理和分析工具，使得企業能夠有效地收集、儲存、處理和分析來自各種來源的大量資料，從而驅動商業洞見和決策制定。

Building your green future today Unlocking secrets to sustainability (COP229)

這場演講中不僅回顧了人類如何從 300 年前的蒸汽引擎發明一路發展到今天面臨的碳足跡問題，也提出了當前環境挑戰的嚴峻性，以及我們如何透過技術和創新來對抗這些挑戰。

首先，演講者提到，過去 300 年間，從蒸汽引擎到電力、再到內燃機的發明，人類不斷燃燒化石燃料來創造能源，這促進了工業革命並帶來了繁榮。然而，這也導致了當前我們面臨的全球二氧化碳排放問題。每 20 分鐘，世界將增加 140 萬公噸的二氧化二氧化碳排放，這不僅威脅到數百人的安居樂業，還導致生物多樣性的快速流失。

傳統的解決方案，如大規模植樹，已被證實在當前情況下不切實際。這要求我們必須尋找新的方法來解決這個問題。演講者強調，作為技術社群的一分子，我們擁有利用創新來降低能源消耗和二氧化碳排放的機會，即使這只是全球年能源消耗的一小部分（0.006%）。

值得鼓舞的是，全球已有約一半的 2000 大公司宣布了減少碳足跡的承諾，並設定了淨零目標。然而，企業在實現這些目標的過程中面臨諸多挑戰，包括法規遵守、供應鏈管理，以及如何將符合性措施轉化為對公司收益的直接貢獻等問題。

演講者建議，企業應該改變現有的應對策略，將焦點從僅僅符合法規要求轉向如何通過可持續性措施來提高運營效率、產品市場接受度和降低 IT 成本等。這不僅能夠幫助企業在短期內見到投資回報，同時也能在長期內建立起競爭優勢。

其中一個案例是 HCLTech 的淨零智能運營（NIO）平台，它能夠在不同的情境中部署，從製造業到資料中心，提供即時的能源監測和分析。這個平台通過 AI 和數位孿生技術，使企業能夠預測和規劃減碳行動，從而實現更有效的能源使用和減少碳足跡。

除了 NIO 外，演講中還提到了其他幾個解決方案，如 HCLTech 的 My Product Carbon Monitor 和 Green IT 資料中心框架，這些工具幫助企業在產品設計、資料中心運營等方面實現可持續性目標。

圖說：演講者介紹 HCLTech NIO 解決方案，這是一個集合資料收集、分析優化、測量和報告的平台。其特點包括：

收集功能，包含超過 100 種協議支持關鍵績效指標（KPIs）和關鍵系統的 API 整合。

分析和優化工具，如互相比較、標準化、預測、情境分析，以及使用人工智能提供的看法和視覺化。

測量方面，涵蓋了工資、福利、環境、社會治理（WAGES）資料、能源消耗和二氧化二氧化碳排放量，以及特定於行業的績效指標。

報告功能，支援可持續性範疇 1、2、3 的報告，符合合規報告模板，以及針對重資產的儀表板。

最後，演講者強調，可持續性不僅是企業應對法規的手段，更是實現下一代競爭優勢和促進成本節約的關鍵。透過這些創新的解決方案，企業可以在追求綠色發展的同時，也保證了業務的持續增長和繁榮。

這場演講不僅提供了對當前環境挑戰的深刻洞察，也展示了技術和創新如何成為實現可持續未來的強大工具。對於致力於綠色轉型的企業而言，這是一場啟發性的分享，為我們提供了行動的方向和靈感。

補充

Net Zero Intelligent Operations、My Product Carbon Monitor 和 Green IT 資料中心框架是 HCLTech 為了幫助企業達成可持續性目標而開發的解決方案。下面將對每個解決方案進行介紹：

Net Zero Intelligent Operations (NIO)

NIO 是一個平台，旨在幫助組織即時收集和分析企業範圍內的能源資料，以便監測、評估和減少能源消耗和二氧化碳排放。該平台通過獨特的互比性和標準化方法，能與所有 IT 系統、OT 系統和智能資產進行通信，為組織提供統一的能源使用視圖。利用數字孿生技術和人工智能，NIO 能更精確地發現差距和機會，大幅減少優化能源消耗所需的時間和努力。

My Product Carbon Monitor

這是一個平台，專為幫助企業在新產品設計階段考慮可持續性而開發。它整合了材料資料庫中的資料點、可用替代材料以及與這些材料相關的加工和製造過程的能源消耗資料。該平台使企業能夠在模擬器中調整工藝流程、選擇替代材料，並在工程決策時權衡成本與可持續性之間的關係，從而設計出更可持續的產品。

Green IT 資料中心框架

這個框架旨在幫助組織優化其資料中心的運營，實現能源效率和減少二氧化碳排放。它包括採用虛擬化技術、優化計算和儲存使用、遵循綠色採購原則，以及過渡到使用再生能源。該框架不僅有助於減少碳足跡，還能為企業節省營運成本。

可持續金融

可持續金融是指在金融服務業中整合環境、社會和治理（ESG）標準的實踐，旨在促進可持續發展目標的實現。這種金融方式鼓勵投資於那些對社會和環境有積極影響的項目和公司，同時考慮長期的金融回報和風險。可持續金融關注點包括綠色能源投資、負責任的投資決策、提高金融產品和服務的透明度等。

HCLTech

HCLTech 是一家全球性的資訊科技（IT）服務公司，提供廣泛的服務，包括數位化解決方案、工程服務、軟體開發和業務流程外包等。HCLTech 致力於通過創新技術幫助客戶實現業務轉型，同時也重視可持續性和企業社會責任。公司開發了多種解決方案和平台，以支持企業在可持續性轉型中面臨的挑戰。

SF360

SF360 平台是 HCLTech 推出的一個專門針對可持續金融領域的解決方案。這個平台旨在幫助銀行和金融機構管理和評估其投資組合的碳足跡，並支持它們在融資項目時做出更加負責任和可持續的決策。SF360 通過整合相關的碳足跡資料和可持續性指標，使金融機構能夠對現有和未來的投資進行風險評估，並確保其投資策略符合可持續發展目標。此外，這個平台還幫助金融機構應對日益嚴格的法規要求，提高其可持續性報告的準確性和透明度。

合規

導讀

在當今數位化轉型的浪潮中，智慧電網和電力公司越來越依賴雲端技術來提升運營效率、加強資料分析能力並提供更好的客戶服務。在這個過程中，合規和審計的重要性不斷提升。對於這些公司而言，採用混合雲架構不僅需要技術上的轉變，同時也要確保所有操作都符合行業標準、國家法律和國際規範。

合規性確保了智慧電網和電力公司的資料管理、隱私保護以及營運過程遵循正確的法律和標準，從而保障客戶的利益和公司的信譽。而審計則提供了一個機制，用於檢查和驗證合規性措施的有效性，確保風險管理措施得到恰當實施，並及時發現和糾正潛在問題。這對於保持企業的競爭力、避免法律風險並提升客戶信任至關重要。

隨著雲端技術的不斷進步，智慧電網和電力公司能夠利用更加先進的合規和審計工具，如自動化合規性檢查、即時風險評估以及深度學習驅動的異常檢測系統，來加強其混合雲環境的治理。這不僅可以提升運營效率，還能夠在保障安全和合規的同時，為公司帶來更大的業務靈活性和創新機會。

Demonstration of what’s new with AWS governance and compliance (COP348)

此演講展示了 AWS 治理與合規性工具的最新進展，包括 AWS Control Tower 的數位主權特性，AWS Config 的新增功能，以及 CloudTrail Lake 的增強功能。這些更新旨在提升企業管理雲端資源的能力並確保遵守法規要求，對信息工程師和企業具有實際意義。

How to customize AWS compliance and auditing services (COP209)

這場演講通過 Arctic Wolf 的案例展示了如何根據企業特定需求自定義 AWS 合規與審計服務。演講深入探討了 AWS 的合規與審計工具，如 AWS Control Tower、AWS Config 等，並強調了這些工具對於實現資料保護與基礎設施安全的重要性。

What’s new with AWS governance and compliance (COP340)

這場演講詳細介紹了 AWS 治理和合規性的新進展，包括 AWS Control Tower、AWS Config 和 CloudTrail Lake 的新功能，以及資料主權的關鍵問題。這些更新強化了企業在雲環境中的治理能力，並提升了合規性管理的效率。

Demonstration of what’s new with AWS governance and compliance (COP348)

AWS 針對其治理與合規性工具推出了一系列創新功能，旨在提升企業對雲端資源的管理能力，並確保其遵守日益嚴格的法規要求，這些創新功能包含 AWS Control Tower 的數位主權特性、AWS Config 的新增功能以及 CloudTrail Lake 的增強功能。

首先，AWS Control Tower 引入了「數位主權」特性，這是一個重要的更新，它加入了 246 個控制項目，旨在幫助全球企業符合特定地區的資料主權法規。這一特性允許企業在 AWS 環境中實施更細緻的控制，例如，基於組織單位級別拒絕或允許對特定 AWS 區域的訪問。這一變革不僅加強了資料治理的能力，也為跨國公司在遵守地區性法規方面提供了重要的支持。

接著，AWS Config 的新功能，包括資源排除和定期記錄設置，為企業提供了更大的靈活性，以根據其特定需求定制資源追蹤和合規性評估。資源排除功能特別適用於那些有臨時工作負載需求的情境，允許企業在不影響整體合規性狀態的情況下，暫時忽略某些資源的追蹤。此外，定期記錄功能為低活動或特定監控需求的帳戶提供了一種有效的資源配置快照方法。

此外，AWS Config 引入的自然語言處理查詢能力，使得非技術背景的用戶也能夠使用平易近人的語言來構建和執行查詢，這大大降低了使用高級查詢功能的門檻。透過將自然語言查詢轉化為 SQL 語句，AWS Config 提升了用戶檢索和分析資訊的效率，這對於加快決策過程和提高運營效率至關重要。

最後，CloudTrail Lake 的增強功能，特別是支持透過 Athena 進行的聯合查詢，為企業提供了更強大的資料分析和可視化工具。這使得用戶能夠將 CloudTrail Lake 的資料與 Athena 中的其他資料源進行關聯，從而實現更深入的資料洞察和分析。這項功能的增強，不僅提高了資料可視化的能力，也為企業在安全性、合規性和運營效率方面的決策提供了有力支持。

How to customize AWS compliance and auditing services (COP209)

在這場演講中，Brad Gilomen 與 Suchita Verma 共同發表了一場關於如何根據企業特定需求自定義 AWS 合規與審計服務的深入演講。此次演講不僅深入剖析了 AWS 提供的靈活性與客製化能力，更透過 Arctic Wolf 公司的 Todd Snyder 分享了實際應用案例，展現了如何利用 AWS 服務保障客戶資料的安全與解決業務運營上的挑戰。

AWS 的合規與審計服務，例如 AWS Control Tower、AWS Config、AWS Security Hub 與 AWS CloudTrail 等，為企業提供了一套強大的工具組，支援企業在雲環境中實現資料保護與基礎設施安全。這些工具不僅提供了豐富的安全性與合規性檢測功能，更允許企業根據自身政策與需求進行細緻的服務調整，實現精準的風險管理。

Todd Snyder 分享了他所屬的公司 Arctic Wolf 的案例，展示了一家專注於網絡安全服務的公司如何利用 AWS 的多元化服務來強化其安全架構，保護客戶免受網絡威脅。以下是該案例的詳細探討：

安全監控與資料收集

Arctic Wolf 部署了一系列的硬件傳感器與軟體掃描器於客戶的網絡環境中，這些設備負責持續監控網絡流量並收集各類安全相關資料。透過這些資料，Arctic Wolf 能夠獲得寶貴的洞察，及時識別並應對潛在的安全威脅。

跨雲平台整合

在當今多雲環境下，Arctic Wolf 的服務不僅局限於單一雲平台，而是跨越多個雲服務提供商，收集與整合來自不同雲平台的安全資料。這種跨平台的資料整合能力，使得 Arctic Wolf 能夠為其客戶提供全面的安全監控與威脅檢測服務。

第三方合作夥伴整合

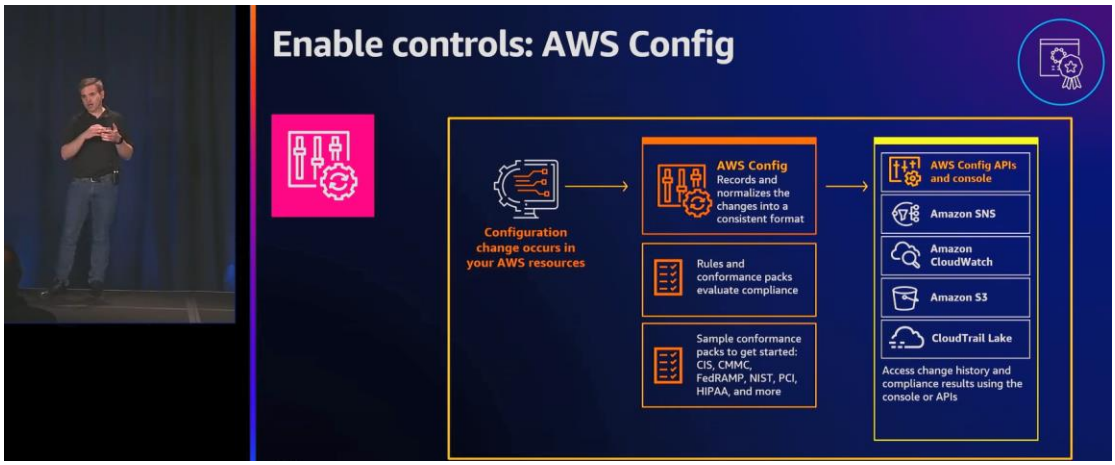
Arctic Wolf 通過與數百家第三方安全服務提供商的緊密合作，進一步擴大了其資料收集與分析的範圍。這些合作夥伴的整合不僅豐富了 Arctic Wolf 的安全資料庫，也增強了其對最新安全威脅的應對能力。

大規模資料處理

Arctic Wolf 每日需要處理約 4.5 萬億個安全事件，這要求公司擁有強大的資料處理能力。透過使用 AWS 的多項服務，如 Amazon S3、Amazon EC2、Amazon Redshift 等，Arctic Wolf 能夠有效地儲存、處理並分析龐大的資料集，確保能夠及時檢測並應對安全威脅。

安全與合規性管理

Arctic Wolf 在 AWS 環境中管理所有核心的安全與合規性服務，包括但不限於 AWS CloudTrail、AWS Config、AWS Security Hub 和 IAM Access Analyzer。這些服務使得 Arctic Wolf 能夠持續監控與評估其雲環境的安全狀態，並確保符合相關的合規要求。



圖說：Todd Snyder 說明透過 AWS Config 將 AWS 資源的變更標準化成一致的格式。

它透過規則和合規性套件評估合規性。

提供一些範例合規性套件來幫助使用者開始使用，這些套件適用於各種合規標準，如 CIS、CMMC、FedRAMP、NIST、PCI、HIPAA 等。

使用者可以透過 AWS Config API 和控制台、Amazon SNS、Amazon CloudWatch、Amazon S3 和 CloudTrail Lake，存取變更歷史記錄和合規性結果。

圖說：這張圖片介紹了 AWS Audit Manager 這個服務，它是用於內部審計的工具，允許用戶持續審計其 AWS 使用情況，從而簡化風險評估和合規性工作。過程包括以下步驟：

選擇一個框架 (Select a framework)：用戶可以選擇一個預建的框架，其中包括控制項，或者創建自己的定制框架。

定義範圍 (Define the scope)：指定在特定區域內需要評估的帳戶和服務。

啟動評估以持續收集證據（Activate the assessment to continuously gather evidence）：Audit Manager 進行自動化的證據收集，並可以進行控制審查，或委派給資源所有者進行驗證。

識別根本原因（Identify root causes）：過濾和分組資料以深入研究不合規的原因。

生成報告（Generate reports）：創建審計準備好的評估報告，並附上證據的鏈接。

身份與訪問管理

管理 AWS 中的訪問控制對 Arctic Wolf 來說至關重要，尤其是在管理數百名開發人員、多個團隊以及眾多服務的身份與訪問權限方面。透過精細的身份訪問管理（IAM）策略與設定，Arctic Wolf 確保了其服務與資料的安全性，防止了未經授權的訪問與潛在的安全風險。

透過這些策略與措施，Arctic Wolf 不僅能夠有效地保護客戶的資料安全，同時也能夠應對快速變化的安全挑戰，展現了其在雲環境下的安全與合規能力。此案例為資訊工程師提供了一個實際的範例，展示了如何利用 AWS 的各項服務與功能來構建一個安全、可靠且符合合規要求的雲基礎設施。

除了介紹客戶案例,演講還著重討論了如何通過自定義設置與優化策略,提升 AWS 服務的成本效益與運作效能。能。例如，透過 AWS Control Tower 的區域拒絕設置與 AWS Config 的事件選擇器功能，企業可以在保障安全與合規的同時，有效控制營運成本。

此外，隨著 AWS 不斷推出新功能，如 CloudTrail Lake 的增強等，企業需要不斷評估這些新服務與現有流程的整合方式，以及如何在成本與功能間取得最佳平衡。

綜上所述，這場演講不僅提供了豐富的技術看法與實踐案例，更為聽眾提供了一個關於如何利用 AWS 服務實現更高效、更安全的合規與審計管理的寶貴參考。隨著雲計算技術的不斷進步，這些知識與經驗將為企業在數位轉型之路上提供重要的指導與支持。

How to customize AWS compliance and auditing services (COP209)

在這場演講中，Brad Gilomen 與 Suchita Verma 共同發表了一場關於如何根據企業特定需求自定義 AWS 合規與審計服務的深入演講。此次演講不僅深入剖析了 AWS 提供的靈活性與客製化能力，更透過 Arctic Wolf 公司的 Todd Snyder 分享了實際應用案例，展現了如何利用 AWS 服務保障客戶資料的安全與解決業務運營上的挑戰。

AWS 的合規與審計服務，例如 AWS Control Tower、AWS Config、AWS Security Hub 與 AWS CloudTrail 等，為企業提供了一套強大的工具組，支援企業在雲環境中實現資料保護與基礎設施安全。這些工具不僅提供了豐富的安全性與合規性檢測功能，更允許企業根據自身政策與需求進行細緻的服務調整，實現精準的風險管理。

Todd Snyder 分享了他所屬的公司 Arctic Wolf 的案例，展示了一家專注於網絡安全服務的公司如何利用 AWS 的多元化服務來強化其安全架構，保護客戶免受網絡威脅。以下是該案例的詳細探討：

安全監控與資料收集

Arctic Wolf 部署了一系列的硬件傳感器與軟體掃描器於客戶的網絡環境中，這些設備負責持續監控網絡流量並收集各類安全相關資料。透過這些資料，Arctic Wolf 能夠獲得寶貴的洞察，及時識別並應對潛在的安全威脅。

跨雲平台整合

在當今多雲環境下，Arctic Wolf 的服務不僅局限於單一雲平台，而是跨越多個雲服務提供商，收集與整合來自不同雲平台的安全資料。這種跨平台的資料整合能力，使得 Arctic Wolf 能夠為其客戶提供全面的安全監控與威脅檢測服務。

第三方合作夥伴整合

Arctic Wolf 通過與數百家第三方安全服務提供商的緊密合作，進一步擴大了其資料收集與分析的範圍。這些合作夥伴的整合不僅豐富了 Arctic Wolf 的安全資料庫，也增強了其對最新安全威脅的應對能力。

大規模資料處理

Arctic Wolf 每日需要處理約 4.5 萬億個安全事件，這要求公司擁有強大的資料處理能力。透過使用 AWS 的多項服務，如 Amazon S3、Amazon EC2、Amazon Redshift 等，Arctic Wolf 能夠有效地儲存、處理並分析龐大的資料集，確保能夠及時檢測並應對安全威脅。

安全與合規性管理

Arctic Wolf 在 AWS 環境中管理所有核心的安全與合規性服務，包括但不限於 AWS CloudTrail、AWS Config、AWS Security Hub 和 IAM Access Analyzer。這些服務使得 Arctic Wolf 能夠持續監控與評估其雲環境的安全狀態，並確保符合相關的合規要求。

身份與訪問管理

管理 AWS 中的訪問控制對 Arctic Wolf 來說至關重要，尤其是在管理數百名開發人員、多個團隊以及眾多服務的身份與訪問權限方面。透過精細的身份訪問管理（IAM）策略與設定，Arctic Wolf 確保了其服務與資料的安全性，防止了未經授權的訪問與潛在的安全風險。

透過這些策略與措施，Arctic Wolf 不僅能夠有效地保護客戶的資料安全，同時也能夠應對快速變化的安全挑戰，展現了其在雲環境下的安全與合規能力。此案例為資訊工程師提供了一個實際的範例，展示了如何利用 AWS 的各項服務與功能來構建一個安全、可靠且符合合規要求的雲基礎設施。

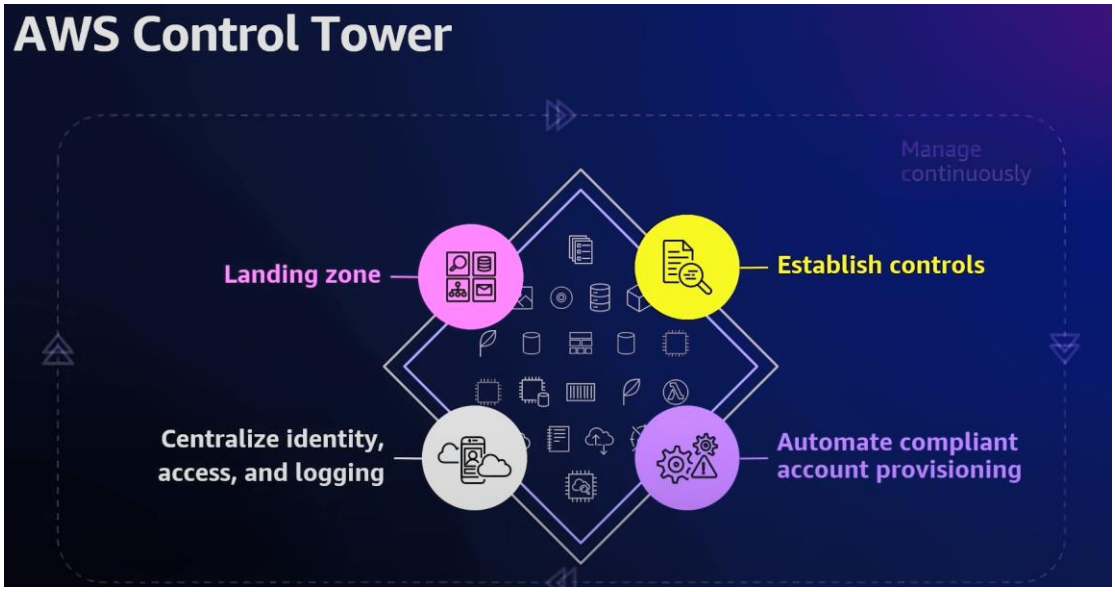
除了介紹客戶案例外，演講中還著重討論了如何通過自定義設置與優化策略，提升 AWS 服務的成本效益與運作效能。例如，透過 AWS Control Tower 的區域拒絕設置與 AWS Config 的事件選擇器功能，企業可以在保障安全與合規的同時，有效控制營運成本。

儘管 AWS 提供了強大的合規與審計工具，企業在自定義與調整這些工具以滿足特定需求時，仍可能面臨專業知識與資源的挑戰。此外，隨著 AWS 不斷推出新功能，如 CloudTrail Lake 的增強等，企業需要不斷評估這些新服務與現有流程的整合方式，以及如何在成本與功能間取得最佳平衡。

What’ s new with AWS governance and compliance (COP340)

隨著企業愈加依賴雲端技術推動業務發展，雲端治理和合規性管理成為了確保企業資訊安全與合規性的重要環節。此次演講探討了 AWS 在雲端治理與合規性領域的最新發展，特別是針對 AWS Control Tower、AWS Config、CloudTrail Lake 以及 AWS Audit Manager 和 AWS Artifact 等工具的更新，這些進展為企業提供了更強大的工具來管理和優化其雲端資源。

AWS Control Tower 的創新之旅



圖說：這張圖展示的是 AWS Control Tower 的核心功能框架。AWS Control Tower 是一種服務，用於設置和管理多帳戶 AWS 環境的治理。從圖中可以看出，它包含以下幾個主要組件：

登陸區(Landing Zone)：作為在雲中設置新用戶環境的基礎，規定了使用哪些區域、帳戶應該如何看起來等。

集中化身份、訪問和日誌管理(Centralize identity, access, and logging)：這涵蓋了身份管理、訪問權限和日誌信息的集中管理，以便對所有雲資源進行一致性監控和管理。

建立控制措施(Establish Controls)：這涉及建立合規性和治理控制措施，確保雲環境符合組織的政策和標準。

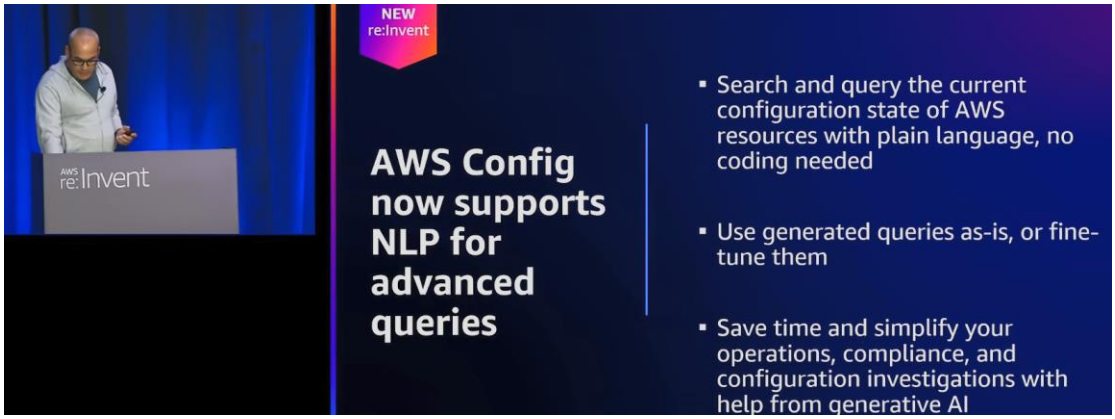
自動合規帳戶配置(Automate compliant account provisioning)：這是指自動創建新的帳戶，並根據事先設定的登陸區設置確保帳戶即時符合合規性要求。

持續管理(Manage continuously)：這代表了一個持續的管理過程，Control Tower 將持續監控環境並對配置進行即時更新，以保持合規性和治理最佳實踐。

AWS Control Tower 作為一站式的雲端治理解決方案，旨在為企業提供自動化和規範化的雲端環境設置。通過引入新的 API 功能，企業現在可以程式化地創建、更新和管理其登陸區（Landing Zones），從而實現更高效的資源部署和治理。例如，一家跨國企業希望快速擴展其在亞洲的業務，借助 AWS

Control Tower 的 API，該企業能夠迅速在多個 AWS 區域建立統一規範的雲端環境，並確保這些環境遵循企業的安全和合規政策。

AWS Config 與 CloudTrail Lake 的進階應用



演講者正在講解 AWS Config 現在支援自然語言處理（NLP）來進行高級查詢的新功能。這項功能讓用戶可以使用平常語言來搜索和查詢 AWS 資源的配置狀態，而無需編寫程式碼。用戶可以使用生成的查詢作為即時使用，或者進行微調以適應特定需求。這樣可以節省操作時間，並簡化運營、合規性和配置調查的過程，這些都得益於生成式 AI 的幫助。這顯示了 AWS 如何通過創新技術進一步提升用戶體驗並優化雲服務的管理。

AWS Config 的資源排除功能和定期記錄能力，使得企業能夠更靈活地管理其資源的配置和變更歷史。比如，一家金融服務公司需要嚴格監控其核心交易系統的配置變更，但對於一些非核心的開發和測試環境則不需要如此嚴格的監控。通過 AWS Config，該公司可以針對不同類型的資源設定不同的監控策略，既保證了關鍵系統的安全性，又避免了不必要的監控成本。

演講者在介紹 AWS CloudTrail Lake，這是一個用於大規模管理安全和審計資料的 AWS 服務：

Capture（捕獲）：指的是收集 AWS 資源的活動和變更的能力。

Store & aggregate（儲存與匯總）：指的是將捕獲的資料進行儲存和匯總，便於進行分析。

Analyze（分析）：提供資料分析能力，以理解和評估安全性和合規性。

CloudTrail Lake 有三個關鍵優勢：

Turn-key solution（一站式解決方案）：提供示例查詢以幫助用戶快速開始使用。

No time spent on ETL（無需花時間進行 ETL）：資料已經過優化，準備好直接進行查詢。

Immutable storage（不可變儲存）：為用戶提供只讀訪問，保證資料的不可更改性和安全性。

CloudTrail Lake 的非 AWS 資料源支援與 Athena 的零 ETL 分析整合，為企業提供了一個強大的安全和運營分析平台。舉例來說，一家電商平台希望分析其用戶行為資料與系統安全日誌之間的相關性，以識別潛在的安全風險。通過 CloudTrail Lake，該平台能夠將來自其網站的用戶行為日誌與 AWS 資源的安全事件日誌進行關聯分析，從而有效地識別並應對安全威脅。

AWS Audit Manager 與 AWS Artifact 的合規功能

演講者正在介紹 AWS Audit Manager 這個服務，這是一個幫助組織評估其控制措施有效性的工具。流程圖解釋了 AWS Audit Manager 的工作流程：

Review, customize, or create framework（評估、自定義或創建框架）：這可能涉及審查現有的控制框架，根據特定需求進行自定義，或者從頭開始創建一個新的框架。

Define scope of assessment（定義評估範圍）：在這一階段，將界定哪些資源和服務需要被納入評估過程中。

Activate assessment to continuously gather evidence（啟動評估以持續收集證據）：這個步驟意味著開始評估流程，以定期收集與配置、安全性和合規性相關的資料和信息。

Conduct control reviews（執行控制審核）：在這裡，進行定期的控制審查，以確保所有控制措施都在正確實施，並根據需要進行調整。

Generate audit-ready reports（生成審計準備報告）：最終，該服務能夠生成詳細的報告，這些報告為審計準備就緒，有助於展示合規性和控制措施的有效性。

AWS Audit Manager 的最佳實踐框架為企業提供了一套預定義的合規性檢查清單，使得企業能夠更系統地管理其合規性證據和審計報告。以一家需要符合 GDPR（一般資料保護條例）的歐洲科技公司為例，該公司可以利用 AWS Audit

Manager 提供的相關框架，自動化收集和管理其 GDPR 合規性證據，大大簡化了**合規性審計的流程，並降低了合規性風險。**

AWS Artifact 則為企業提供了即時訪問 AWS 服務合規性報告的能力，這對於需要向監管機構或客戶證明其雲端服務合規性的企業來說至關重要。例如，一家提供醫療健康服務的公司，需要證明其使用的 AWS 服務符合 HIPAA（健康保險流通與責任法案）的要求。通過 AWS Artifact，該公司可以輕鬆獲取 AWS 服務的 HIPAA 合規性報告，並將這些報告作為其合規性證據的一部分。

自動化

導讀

在當今的數位化時代，數位自動化對於智慧電網和電力公司的重要性日益突顯。隨著能源需求的增加和再生能源來源的整合，電力系統的維運變得越來越複雜。智慧電網透過即時資料分析和通信技術，能有效管理和分配電力，確保供電的可靠性和效率。此外，電力公司越來越依賴混合雲解決方案來處理巨量資料，提高維運效率並降低成本。

數位自動化在此過程中扮演著關鍵角色，它使電力公司能夠自動化其許多日常維運，從而減少人為錯誤，提高反應速度和服務質量。例如，通過自動化系統，電力公司可以即時檢測和解決網絡問題，自動調整能源分配以應對需求變化，並即時監控和維護電網健康。這不僅提高了電網的穩定性和可靠性，也為消費者提供了更經濟高效的服務。

此外，數位自動化還為電力公司帶來了更好的資料洞察力和決策支持，使它們能夠更精準地預測電力需求，優化產能規劃和資源分配。在面對極端天氣條件或突發事件時，自動化系統可以迅速調整維運策略，確保電力供應的連續性和安全性。

因此，對於智慧電網和電力公司而言，投資於數位自動化技術不僅是提升維運效率和服務質量的途徑，也是實現長期可持續發展的關鍵策略。隨著技術的進步和數位化轉型的加速，數位自動化將繼續在智慧電網的發展和電力行業的創新中發揮著不可或缺的作用。

Centralize your operations (COP320)

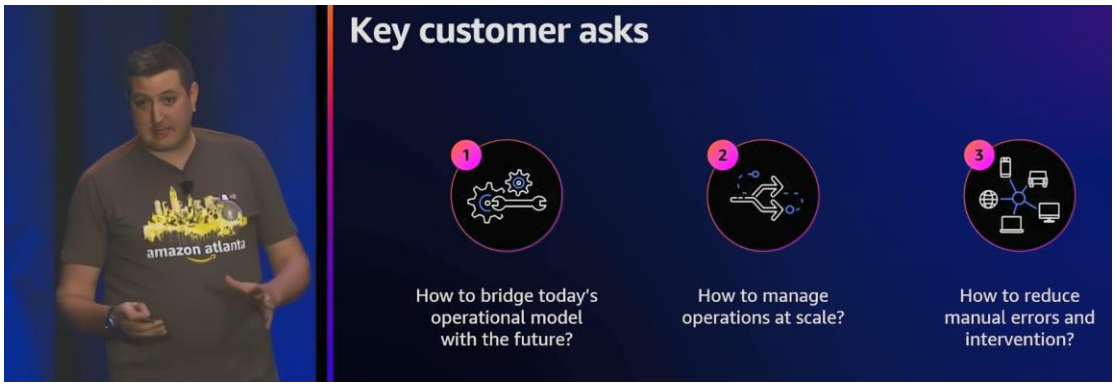
此演講強調了在雲計算環境下集中維運管理的重要性，尤其是通過 AWS 服務。它突出了處理大規模維運（如補丁管理）中自動化的需求，並討論了 MuleSoft 利用 AWS 進行自動化、高效和安全維運的方法。主要策略包括自動化補丁管理、低環境測試、使用 AWS Parameter Store 儲存補丁信息、定義資源組和維護窗口、逐步應用補丁，以及監控和回滾機制，旨在最小化服務中斷並優化維運效率。

Real-life automation and security best practices from the field (COP228)

此演講深入探討了雲環境中自動化和安全的實際方面，強調了雲遷移、安全實踐、組織轉型以及 AI 和 ML 在安全領域的應用。它呈現了行業專家對克服網絡安全挑戰的看法，強調了雲遷移中安全優先的方法，以及 DevOps 和 DevSecOps 的變革性角色。討論還突出了自動化中可觀察性和可見性的重要性，以提高安全操作的敏捷性。

Centralize your operations (COP320)

在這場精彩演講中，來自 AWS 和 MuleSoft 的專家們分享了他們在中心化維運管理方面的深入看法和實踐經驗。隨著企業紛紛轉向雲端，如何有效管理激增的資源與服務，成為了一大挑戰。



圖說：在運營管理方面的三大關鍵需求。這些需求包括：

如何將當今的營運模式與未來連接起來？ 這涉及如何平滑地過渡從當前運營實踐到能夠應對未來增長和變化的模型。

如何在大規模下管理運營？ 當業務擴展到需要跨多個帳戶和地區運營時，如何保持運營的高效性和可管理性。

如何減少手動錯誤和介入？ 探尋自動化策略，以減少人為失誤並提高效率，尤其是在繁瑣的手動過程中。

自動化運營的必要性

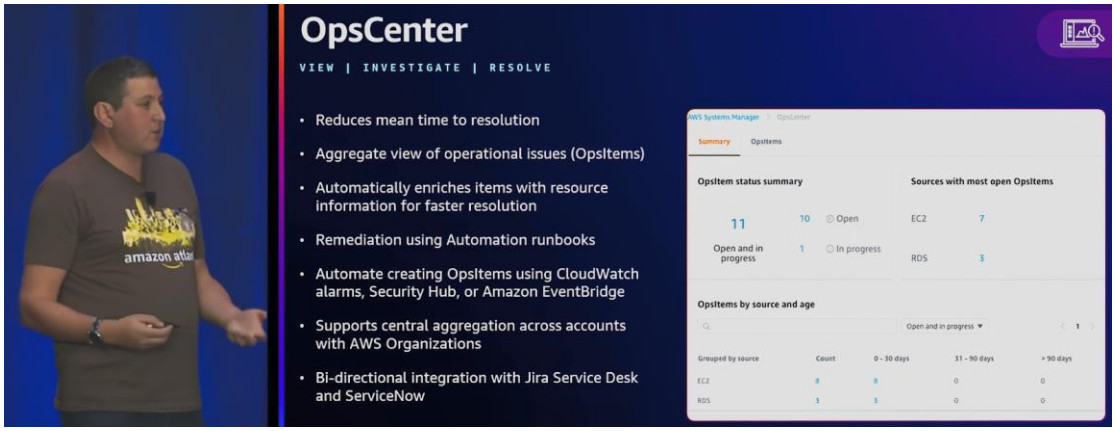
Erik Weber 在開場白中強調了中心化運營管理的重要性。他講述了企業在雲端旅程初期可能只有少量的 EC2 或 Lambda 實例，但隨著業務的擴展，這些數字可能迅速躍升至上萬。此時，初期使用的管理工具可能難以負荷如此龐大的規模，這就需要更加自動化和中心化的運營管理方法來應對。

圖說：演講者介紹了如何通過 AWS 的一系列工具來自動化跨不同環境的操作。展示了如何整合改變管理、事件管理、事件處理以及節點管理來實現自動化，並利用 AWS Config、Amazon

CloudWatch、AWS CloudTrail、Amazon DevOps Guru、AWS Security Hub 和 Amazon EventBridge 等服務來支持配置、可觀察性、安全性和合規性資料的收集和管理。簡報顯示了在 AWS 雲環境、內部部署、邊緣計算以及多雲環境中的自動化操作的結構，以及 AWS Systems Manager 在其中所扮演的角色，包括使用它的多個特性，如 Change Manager、OpsCenter、Incident Manager、Explorer、Inventory、Patch Manager、Session Manager 等。

跨帳戶與地區的資源管理

Erik 進一步探討了跨帳戶和地區管理資源所面臨的挑戰。在 AWS 的世界裡，企業往往會有多個帳戶和在多個地區部署資源，這使得獲取單一 EC2 實例的狀態變得極為複雜。這裡的關鍵在於如何實現資源的集中管理和視圖，以便更有效地監控和維運。

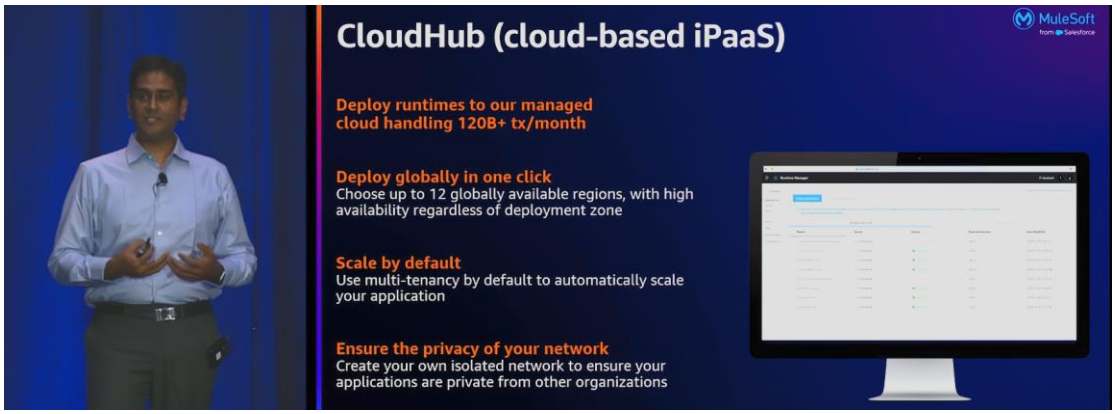


圖說：演講者強調了 OpsCenter 在維運管理中的價值。OpsCenter 被用來減少解決問題的平均時間，提供操作問題的綜合視圖，並自動豐富資源信息以加快問題解決。通過自動化 runbooks 進行補救，並能自動創建 OpsItems 來應對 CloudWatch 告警、Security Hub 或 Amazon EventBridge 事件。它支持通過 AWS Organizations 跨帳戶的中心聚合，並與 Jira Service Desk 和 ServiceNow 有雙向整合。右邊的屏幕截圖顯示了 OpsCenter 的一個操作界面，概述了當前開放和進行中的操作項目的狀態摘要，並按源和年齡分類這些項目。

節點管理與自動化

隨後，Erik 介紹了 AWS 在節點管理方面的解決方案，特別是對於那些仍然需要管理物理伺服器或虛擬機的情境。無論是完全服務化的架構，還是仍舊依賴於一定數量的伺服器節點，AWS 提供了一系列工具和服務來幫助企業實現在規模上的自動化管理。

實踐案例：MuleSoft 的自動化運營



圖說：這張幻燈片上的演講者正在介紹 MuleSoft 的 CloudHub，這是一種基於雲的整合平台即服務（iPaaS）。CloudHub 的主要功能包括：

部署執行時環境到 MuleSoft 管理的雲平台，每月處理超過 120 億次交易。

一鍵在全球範圍內部署應用，用戶可以選擇高達 12 個全球可用的地區，並保證高可用性。

預設即具備規模擴展能力，默認使用多租戶架構自動擴展應用。

確保網絡隱私，創建隔離的網絡以保證與其他組織的應用程式隱私。

MuleSoft 面臨的主要挑戰是管理其龐大的、遍及全球的 EC2 實例庫，這些實例支撐著每月約 1200 億次的交易。每個月都會有新的自定義 AMI（Amazon Machine Image）發布，客戶需要在特定時間內更新這些 AMI，若未按時更新則會被強制升級。這一流程中的一個關鍵挑戰是如何在不重啟客戶實例、不中斷服務的情況下，對這些實例進行安全補丁更新。

自動化補丁管理解決方案

MuleSoft 的解決方案聚焦於利用 AWS 服務來自動化補丁管理過程。這個流程分為幾個主要步驟：

AMI 遷移和訂閱：從 Linux 1 遷移到 Linux 2，並為每個新的 AMI 訂閱 Amazon Linux 內核即時補丁服務，確保可以即時應對安全漏洞。

補丁掃描和分類：在低環境中掃描識別出的補丁，進行分類並在測試環境中進行嚴格測試，以確保補丁不會破壞 MuleSoft 提供的服務。

利用 SSM 參數儲存：將經過測試和分類的補丁資訊儲存在 SSM 參數儲存中，按 AMI 和帳戶組織補丁資訊。

自動化補丁應用：利用 AWS Systems Manager 的 Run Command 功能，根據儲存在 SSM 參數儲存中的補丁資訊，自動向符合條件的 EC2 實例應用補丁。這一過程由 Scheduled Maintenance Windows 控制，確保補丁按計劃順序應用，同時監控補丁應用的狀態並將反饋發送到 Amazon SQS 隊列。

實踐成果

這一自動化補丁管理解決方案為 MuleSoft 帶來了顯著的成效：

高效的補丁管理：能夠在短時間內（約 4 至 6 小時）自動對數千甚至數萬個 EC2 實例進行補丁更新，顯著提高了運營效率。

無中斷服務：通過 AWS 內核即時補丁服務和精細控制的補丁應用流程，實現了在不重啟客戶實例的情況下更新安全補丁，無中斷地保障了服務連續性和穩定性。

自動化與規模化：這一流程的自動化程度高，易於擴展，適用於大規模 EC2 實例庫，特別適合需要在全球範圍內管理大量雲端資源的企業。

Real-life automation and security best practices from the field (COP228)

這是一場關於實際自動化和安全最佳實踐的精彩講座。這場演講涵蓋了雲端安全、自動化策略、組織變革以及 AI 和 ML 在安全領域的應用等多個重要方面。在此，我將詳細闡述演講中討論的關鍵點和實踐建議，以供大家參考和實踐。

首先，Aidan Walden 強調了上雲和安全實踐的重要性。他分享了 Fortinet 與客戶合作的經驗，特別強調了安全整合、雲端存取的安全性以及通過整個雲端部署生命周期推動自動化的重要性。Fortinet 專注於讓雲端安全易於消費，這一點對於企業實現雲端最大效率至關重要。

演講中還介紹了幾位專家，包括來自 Mount Wave Ventures 的 Roger Cressey，他分享了他在公共部門和私營部門解決網絡安全政策和風險管理挑戰的豐富經驗。此外，Vince Wang 和 Ali Bidabadi 分別就 Fortinet 在雲產品營銷、雲合作夥伴聯盟以及雲諮詢實踐方面的領導作用進行了闡述。

從組織變革的角度來看，雲端轉型不僅僅是技術的轉變，更涉及到組織結構、技能評估和工作流程的重組。DevOps 和 DevSecOps 的採納成為推動組織轉型的基石。演講還強調了 AI 和 ML 工具在雲端安全中的潛力，尤其是在加速威脅檢測和應對方面。

Ali Bidabadi 討論了大型組織在雲端實施方面的共同關切，特別是在進行上雲和安全策略制定時。他強調了從一開始就發展安全藍圖的重要性，以避免之後重新設計的需要。他也提到了在雲端環境中安全機制的差異性，特別是在網絡平面更加民主化的背景下。

談到自動化，Roger Cressey 指出，自動化的關鍵在於可觀察性和可見性。只有當能夠全面監控資源時，自動化才能有效提升安全操作的敏捷性。他分享了政府機構如何通過部署工具將應對時間從手動的一小時降低到幾秒鐘的案例。

在討論到雲安全的資料湖等話題時，強調了如何處理大量警報和信號的挑戰。成功的企業正通過歸一化資料和提供上下文來克服資料量挑戰，使安全運營人員能夠更有效地理解和行動。

最後，關於 AI 和 ML 在安全領域的應用，雖然存在許多炒作，但這些技術在提高威脅檢測、響應速度和縮小攻擊範圍方面確實提供了實質性的好處。然而，也需要注意 AI 和 ML 的應用並非萬能，其效果很大程度上取決於資料的質量和系統的訓練。

總結來說，雲端安全和自動化最佳實踐的核心在於從組織結構和流程的角度進行全面考慮，並且充分利用 AI 和 ML 等技術的潛力。透過建立安全藍圖、重視資料的可觀察性和可見性，以及採用靈活的安全策略，企業可以有效地保護自己在雲端環境中的資源和資料。

資訊安全

導讀

在當今數位化和互聯化的時代，智慧電網和電力公司面臨著前所未有的網絡安全挑戰。隨著操作技術（OT）和資訊技術（IT）的融合，以及物聯網設備的大量應用，電力系統的攻擊面不斷擴大，使其成為網絡犯罪分子的主要目標。一旦關鍵的電力基礎設施遭到入侵或破壞，不僅會導致大規模的停電事故，更可能對國家安全和社會穩定造成嚴重影響。

因此，對於智慧電網和電力公司而言，建立全面的網絡安全防禦體系至關重要。這不僅需要採用先進的安全技術和工具，如入侵檢測和防禦系統、安全資訊和事件管理（SIEM）等，還需要在組織內部培養一種濃厚的安全意識和文化。通過實施零信任安全模型、加強身份和訪問管理、定期開展安全培訓和演練等措施，電力公司可以從人員、流程和技術等多個維度來增強其網絡韌性。

此外，電力公司還需要建立完善的威脅情報體系和安全運營中心（SOC），以實現對各類安全事件的即時監測、分析和響應。通過利用大資料分析、機器學習等技術，SOC 可以從海量的安全日誌和網絡流量中及時發現可疑活動，並根據預定義的事件響應流程進行處置，從而最大限度地減少網絡攻擊造成的損失和影響。

在應對供應鏈攻擊、內部威脅等新興安全風險方面，電力公司還需要加強與上下游合作夥伴的協作，共同提升產業鏈的整體安全水平。通過制定嚴格的安全標準和評估機制，定期開展合作夥伴的安全審計和風險評估，電力公司可以有效識別和管控供應鏈中的潛在風險點。

總之，網絡安全已成為智慧電網和電力公司實現可持續發展的重中之重。唯有將安全融入到數位化轉型的各個環節之中，並通過不斷創新和完善安全策略來適應日新月異的威脅形勢，電力行業才能構建起一張萬無一失的安全網，為國家能源安全和人民生活質量提供堅實的保障。

Building a comprehensive security solution with AWS security services (SEC226)

本場演講深入探討了如何利用 AWS 的安全服務構建全面的安全解決方案，以應對複雜的多向量網絡威脅。通過 DBS 銀行的實際案例，講者生動地展示了 AWS 安全工具的強大威力和靈活的整合能力，為企業提供了寶貴的實踐借鑒。

Customize and contextualize security with AWS Security Hub (SEC242)

這場演講重點介紹了 AWS Security Hub 的新特性和自定義功能，幫助企業實現更加精細化和情境化的安全管理。通過中央配置和發現豐富化等創新，企業能夠更高效地管理其雲端資源的安全狀態，並從容應對不斷變化的合規要

求。

Defense in depth: Securely building a multi-tenant generative AI service(SEC334)

在這場演講中，亞馬遜的資深工程師分享了如何運用深度防禦原則，在 CodeWhisperer 客製化服務中構建多層次的安全防線。通過精心設計的訪問控制、資料隔離和創新技術的應用，CodeWhisperer 為企業提供了一個安全可靠的生成式 AI 平台。

Introducing GuardDuty ECS Runtime Monitoring, including AWS Fargate (SEC239)

這場演講重點介紹了 GuardDuty 對 ECS 和 Fargate 容器環境的即時監控能力，幫助企業及時檢測和應對容器層面的安全威脅。通過智能化的異常行為分析和高效的代理部署，GuardDuty 為容器環境提供了一道堅實的安全防線。

Streamlining security investigations with Amazon Security Lake (SEC234)

本場演講深入探討了如何利用 Amazon Security Lake 來簡化安全調查流程，讓企業能夠高效地管理和分析海量的安全日誌和事件資料。SEEK 公司的實際案例充分展示了 Security Lake 在打通資料孤島、提高安全運營效率方面的巨大價值。

Sustainable security culture: Empower builders for success (SEC211)

這場演講從文化和人性化管理的角度切入，分享了如何在組織內部構建可持續的安全文化。通過心理安全的營造、同理心的培養和賦能機制的建立，企業可以充分調動員工的安全積極性，形成一支富有激情和專業度的安全團隊。

The AWS data-driven perspective on threat landscape trends (SEC236)

在這場演講中，AWS 安全專家結合海量的第一手資料，深入剖析了當前網絡威脅態勢的發展趨勢。從 GuardDuty 的內部視角和 Shield 團隊的外部觀察，演講者全面展示了 AWS 在威脅情報和安全防禦方面的創新實踐，為與會者提供了獨特的洞見。

Building a comprehensive security solution with AWS security services (SEC226)

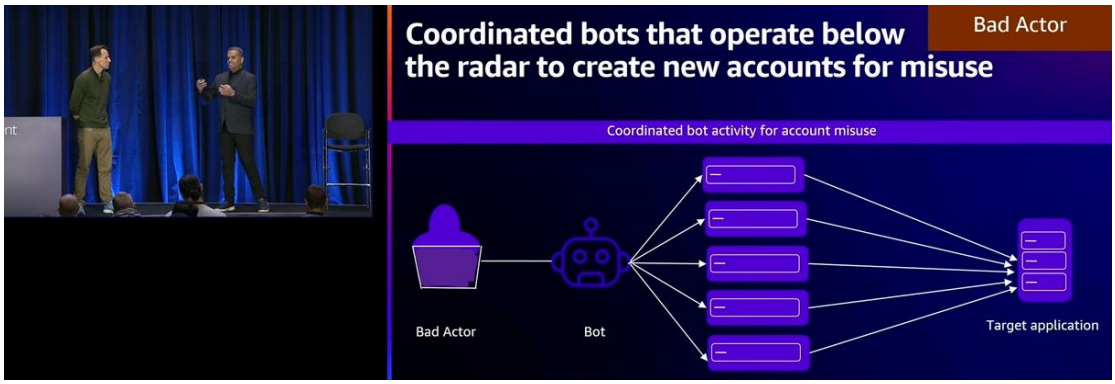
在這場演講中，AWS 安全領域的專家 Mun Hossain 和來自 DBS 銀行的 Abiram Subramanian 共同探討了如何構建全面的安全解決方案，利用 AWS 的安全服務來對抗多向量威脅並提升企業安全防禦。這場深入的討論涵蓋了從威脅偵察、攻擊模擬到實際案例分享，旨在向企業展示如何有效整合 AWS 的安全工具和服務來加固他們的雲端環境。

多向量威脅下的安全挑戰

在當今數位化快速發展的時代，企業面臨的安全威脅日益複雜多變。Mun Hossain 指出，根據 Neustar 的報告，77%的攻擊是多向量攻擊，這種攻擊策略結合了兩種或更多的工具和方法，針對網絡和應用資源。這種攻擊的複雜性使得企業必須部署大量的安全工具和資源來防禦，但這種做法往往帶來了更多的問題，如資源分散和安全工具之間的協同問題。

角色扮演：攻防實戰

為了更直觀地展示多向量攻擊的防禦過程，Mun 和他的同事 Michael Leighty 進行了一場別開生面的角色扮演，模擬了從基礎的偵察攻擊到高級的 SQL 注入和 DDoS 攻擊等一系列攻擊情境。在這場攻防對抗中，AWS 的安全服務如 Network Firewall、WAF 和 Shield Advanced 發揮了關鍵作用，有效阻止了攻擊者的嘗試，展現了 AWS 安全工具強大的保護能力和靈活的應對策略。



圖說：簡報內容顯示了一種協同機器人(bot)的活動，它們在偵測範圍以下運作以創建新的帳戶進行濫用。在圖的左側，有一個標記為“Bad Actor”的象徵圖，這代表了惡意行為者。這位惡意行為者通過一個中間的機器人，控制了多個創建帳戶的過程。每一條從機器人延伸出的線都指向了一組代表可能被濫用的目標應用程式帳戶。這種機器人的活動是協調一致的，旨在不被安全系統察覺的情況下進行帳戶濫用，這通常涉及到繞過傳統的安全檢查，如 IP 速率限制或行為分析。

DBS 銀行的現實案例分享

DBS 銀行是一家位於亞洲的領先金融服務集團，以新加坡為總部，並在整個亞洲擁有廣泛的業務。隨著數位化轉型的加深，DBS 銀行在雲端安全方面遇到了一系列挑戰和需求，特別是在安全運營的擴展、資料外泄風險的預防以及事件響應的自動化方面。

安全運營的擴展挑戰

DBS 銀行在 AWS 雲端上運行多種工作負載，包括計算、儲存和分析等服務。隨著在雲端的業務規模擴大，銀行需要一套能夠跨多個 AWS 帳戶和地區有效工作的安全控制機制。尤其是對於出站流量的管理，銀行需要確保所有的雲端資源都能在一個安全的環境下進行資料傳輸，同時預防如勒索軟體、命令與控制活動和零日攻擊等威脅。

資料外泄風險預防

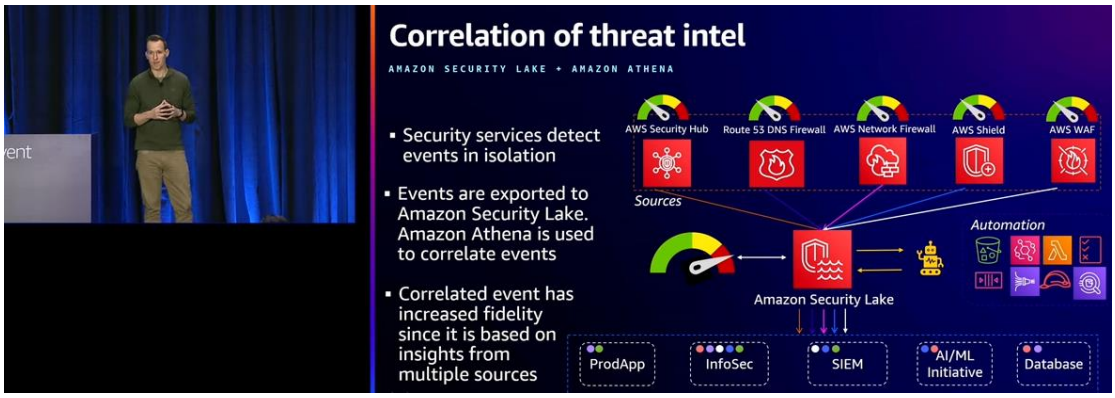
對於金融機構而言，資料的安全至關重要。DBS 銀行致力於監控和控制資料的外部移動，需要能夠精確地識別和預防未經授權的資料訪問和傳輸，特別是對於儲存在 S3 桶中的敏感資料。

事件響應自動化

傳統的事件響應過程往往依賴於手動操作，這不僅耗時且易於出錯，還會增加操作人員的負擔。DBS 銀行希望通過自動化的方式來提高事件響應的速度和準確性，從而快速緩解潛在的安全威脅。

解決方案和實施

DBS 銀行選擇了一種結合了 AWS 多種安全服務的整合解決方案，這包括 Amazon GuardDuty、IAM Access Analyzer、Network Access Analyzer 和 AWS Config 等。這些服務共同作用於提高對雲端環境中潛在威脅的可見性，並通過 AWS Security Hub 將安全警報集中起來，進行分析和處理。



這張圖描述了如何進行威脅情報的關聯分析。安全服務獨立檢測到事件後，這些事件被匯出到 Amazon Security Lake，並利用 Amazon Athena 來進行事件關聯。關聯後的事件因基於多重來源的洞察而具有更高的準確度。該流程整合了多個來源，如 AWS Security Hub、Route 53 DNS Firewall、AWS Network Firewall、AWS Shield 以及 AWS WAF，最後通過安全湖到達自動化處理，這包括產品應用、資訊安全團隊、安全資訊與事件管理系統（SIEM）、人工智慧/機器學習倡議和資料庫。

為了實現事件響應的自動化，DBS 銀行採用了 AWS 的 Step Functions 和 Lambda 函數來設計自動化的工作流。這些工作流基於 Security Hub 中的警報自動觸發相應的緩解措施，如更新 Network Firewall 的規則或調整 IAM 策略，從而快速有效地應對安全事件。

成效與收穫

通過實施這套整合的安全解決方案，DBS 銀行不僅提高了其雲端環境的安全性，還大大提升了安全運營的效率。自動化的事件響應減少了手動操作的需求，使安全團隊能夠更加專注於策略和架構的優化。此外，跨不同安全工具和團隊的協同工作也變得更加流暢，有助於形成一個更加統一和高效的安全防禦體系。

結語和行動呼籲

這場精彩的討論不僅提供了對抗多向量威脅的深入看法，也展示了通過 AWS 安全服務建立強大防禦的實際案例。對於任何希望加強其雲端環境安全的企業來說，AWS re:Invent 2023 的這場會議無疑提供了豐富的資源和靈感。Mun Hossain 在會議的最後強調，通過持續學習和運用 AWS 提供的安全工具，企業可以更好地預防和應對日益複雜的網絡威脅，保護他們的數位資產不受侵害。

Customize and contextualize security with AWS Security Hub (SEC242)

隨著雲端安全性的日益重要，AWS 在此次大會上推出了一系列安全中樞（Security Hub）的新功能，旨在提供更高的自定義性和上下文化，幫助企業更快更好地採取行動應對安全威脅。Dora Karali 和她的團隊介紹了這些創新功能，其中包括中央配置和發現豐富化，這些功能旨在讓企業能夠更有效地管理和反應於安全警報。

圖說：圖中展示了安全團隊面臨的挑戰，這些挑戰包括：

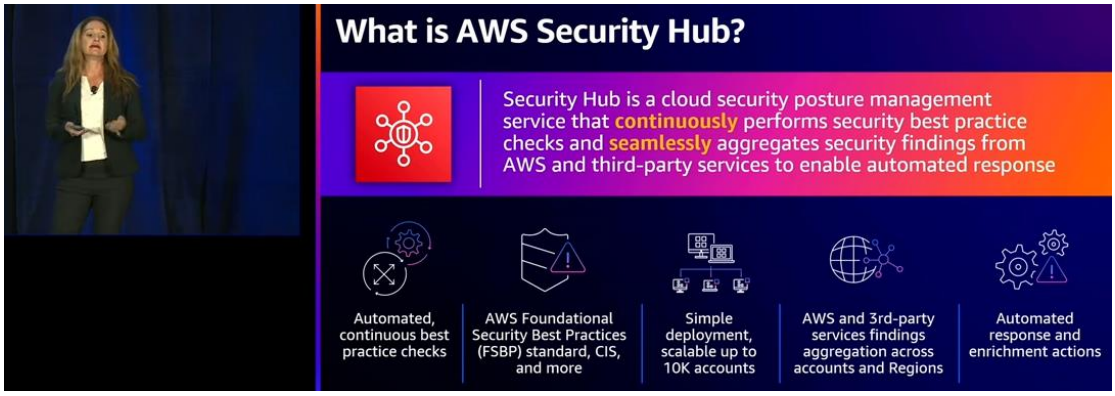
缺乏可見性 ：安全團隊難以看到安全風險及其影響。

規模調整 ：需要根據組織的需求，調整安全措施以適應擴展。

多重安全警報來源 ：安全警報來自多個源頭，增加了管理的複雜性。

過多警報 ：安全警報太多，且缺乏足夠的上下文以作出快速響應。

在這個快速發展的雲端世界中，企業面臨著一個共同的挑戰：如何在快速擴展的同時，確保資源的安全與合規？AWS 的答案是提供一個全面的安全管理平台，Security Hub。自 2019 年推出以來，Security Hub 一直致力於為客戶提供一個統一的安全態勢視圖，讓安全團隊可以集中管理來自 AWS 本身及第三方服務的安全發現。



圖說：演講者概述了 AWS Security Hub 的角色，它是一個雲安全姿態管理服務。它持續進行

安全最佳實踐檢查，並聚合來自 AWS 和第三方服務的安全發現，以實現自動化響應。其主要功能包括：自動化的持續最佳實踐檢查；AWS 基礎安全最佳實踐（FSBP）標準、CIS 等；可擴展至 10K 帳戶的簡便部署；跨帳戶和區域的發現聚合；以及自動化響應和增強行動。

透過這次更新，AWS 引入了「中央配置」功能，為企業提供了一個強大的工具，使其能夠在整個組織中統一安全控制的設置。這意味著企業可以根據自己的安全政策和標準，自定義 Security Hub 的安全檢查和控制。更重要的是，這些自定義設置可以一次性跨帳戶和區域應用，從而極大地簡化了配置過程，並確保了安全設置在整個組織中的一致性和遵循性。這不僅提高了配置的效率，也加強了組織對安全態勢的控制。

「發現豐富化」功能的引入，則進一步提高了安全團隊對安全警報的處理能力。透過自動添加有關資源的豐富上下文信息，如應用程式名稱、資源標籤和帳戶名稱等，安全團隊能夠更快速地定位到具體的問題資源，並根據資源的重要性、所屬應用程式或相關業務單位，作出更加精確和有針對性的反應。這種豐富化的信息不僅加快了問題的識別和處理速度，還提高了整體的安全管理效率。

隨著 AWS 持續增加新的控制和標準，擴展對更多 AWS 資源類型的支持，Security Hub 正在變得更加強大和全面。這意味著企業可以依靠 Security Hub 來維護更廣泛的雲端資源安全，使其成為一個真正的安全管理中心。此外，AWS 通過舉辦激活日和提供訂閱安全中樞公告的方式，鼓勵用戶更好地利用這些工具和資源，以加強自身的雲端安全防護。這些活動和資源不僅有助於用戶了解如何有效地設置和運用 Security Hub，也促進了 AWS 安全社區的發展和知識共享。

總之，AWS 推出的 Security Hub 新功能，為企業提供了一個更加靈活、上下文豐富的安全管理工具。透過這些創新，AWS 正在幫助企業建立一個更加堅固、可靠的雲端安全防線。隨著安全威脅的日益複雜，擁有如此強大的工具無疑是每個企業邁向更安全雲端之旅的關鍵。

Defense in depth: Securely building a multi-tenant generative AI service(SEC334)

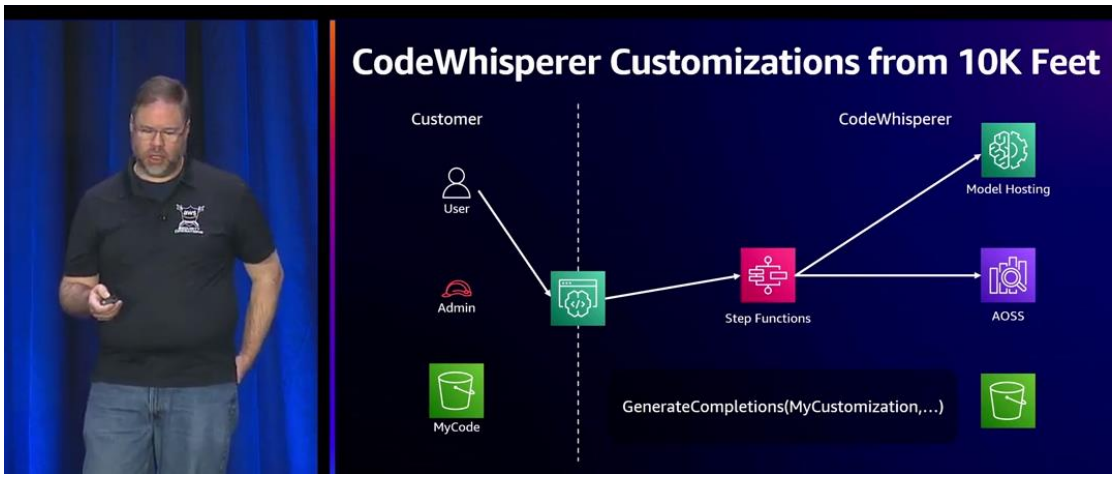
在 AWS re:Invent 2023 的一場名為「多維防禦：安全建構多租戶生成式 AI 服務」(SEC334) 的演講中，亞馬遜的資深工程師 Eric Brandwine 分享了如何在他們新推出的生成式 AI 服務「CodeWhisperer 客製化」中實踐深度防禦的概念。在這篇文章中，我們將探討 Eric 如何將安全建構視為一種藝術，並將其與攝影技術相比較，從而揭示出安全機制的多維度特性。

安全性的藝術：從攝影到程式碼

Eric 將自己對攝影的熱情與對電腦技術的熱愛結合在一起，透過攝影技術中的挑戰來比喻安全建構的複雜性。例如，他提到了如何通過拼接多張照片來創建全景圖，這不僅需要處理圖片的對齊和畸變問題，還要考慮到最終圖像的投影方式。類似地，建立一個安全的 AI 服務也需要在多個層面上進行精細的調整和優化，以確保從不同角度的安全性。

多維度防禦策略

Eric 介紹了「瑞士起司模型」來說明安全防禦的概念，這個模型強調通過多層保護來增加防禦的深度。他將這一概念應用到 CodeWhisperer 客製化服務中，闡述了一系列從員工訪問控制到加密技術的安全措施。每一項措施都像是起司中的一片片，共同作用來阻擋潛在的安全威脅。



圖說：演講者正在介紹 CodeWhisperer 自定義功能的高層次架構。在左側是客戶，包括一般用戶和管理員，他們擁有自己的程式碼庫。客戶透過一個稱為 Step Functions 的 AWS 服務與 CodeWhisperer 進行交互。這個過程涉及到程式碼生成建議（GenerateCompletions），這些建議是從客戶提供的自定義程式碼（MyCustomization）中產生的。右側是 CodeWhisperer 的 Model Hosting 部分，以及 Amazon OpenSearch Serverless（AOSS），它們負責處理和提供程式碼補全的功能。整個過程體現了 AWS 服務如何通過雲端解決方案支援客戶自定義他們的編碼環境。

對抗內外部威脅

Eric Brandwine 特別強調了 CodeWhisperer 客製化服務如何應對內外部威脅的策略。這些威脅包括來自外部的惡意攻擊者，可能會嘗試利用服務的漏洞來達到其不法目的；內部惡意人員，可能是被收買或擁有其他動機的員工，他們利用自己的訪問權限來造成損害；以及無意的安全疏漏，這可能源於員工的失誤或系統的不完善。

針對這些威脅，Eric 提到了一系列防護措施。首先是定期更新和修補軟件，這是基礎但至關重要的安全措施，可以確保系統不會因為已知漏洞而受到攻擊。其次，對員工訪問進行限制和監控，確保只有需要訪問權限的員工才能訪問敏感資訊，同時通過日誌和審計跟蹤員工的行為。最後，Eric 特別強調了多因素認證（MFA）的重要性，這是一種通過要求兩種或以上的驗證方式來增強帳號安全性的方法，大大降低了密碼被破解或員工憑證被盜用的風險。

創新技術的應用

在深度防禦的實踐過程中，Eric 展示了若干創新技術的應用，以增強 CodeWhisperer 客製化服務的安全性和效能。

一個顯著的例子是 Forward Access Sessions（FAS）。這項技術允許服務在獲得客戶明確授權的情況下，才能訪問其 S3 儲存桶中的資料。FAS 通過創建一次性或有時間限制的認證，確保訪問權限是臨時的且嚴格受控，這大大減少了潛在的資料泄露或未經授權訪問的風險。

另一項關鍵技術是 Amazon OpenSearch Serverless，這是一種無伺服器的搜索和分析服務，可以儲存、索引和檢索大量資料。在 CodeWhisperer 客製化服務中，利用 OpenSearch Serverless 不僅提高了資料處理的效率和靈活性，而且通過對每個客戶使用獨立的資料集合和加密鑰匙，進一步強化了資料隔離和安全性。

文化與機制：安全建構的雙翼

Eric 最後強調，建立安全的 AI 服務不僅需要先進的技術和嚴密的機制，還需要培養一種將安全視為核心價值的文化。透過教育和訓練，以及創建一套既能自動化也能持續進化的安全檢測和應對流程，可以確保隨著團隊成員的變化和技術的發展，服務的安全性仍然能夠得到保障。

通過這場精彩的演講，Eric 不僅分享了建立一個安全 AI 服務的實踐經驗，更重要的是，他向我們展示了將技術創新與深層文化理念結合的力量。這一過程證明了，即使面對日益複雜的安全挑戰，通過持續的努力和創新，我們仍能構建出既安全又強大的技術解決方案。

Introducing GuardDuty ECS Runtime Monitoring, including AWS Fargate (SEC239)

在今天的技術領域中，容器技術已經成為雲計算環境中不可或缺的一部分，尤其是在微服務架構和無服務（serverless）計算方面。AWS ECS（Amazon Elastic Container Service）提供了一個高度可擴展、高性能的容器管理服務，讓用戶可以在 AWS 雲上輕鬆運行、停止和管理 Docker 容器。而 Fargate，作為 ECS 的一個重要組成部分，為用戶提供了一種無需管理伺服器即可運行容器的方式。然而，隨著容器技術的普及，它們也面臨著和傳統虛擬機相同的安全威脅，例如密碼挖礦、服務拒絕攻擊等。因此，AWS 引入了 GuardDuty ECS 即時監控功能，旨在提升 ECS 和 Fargate 環境中的安全性。

在圖片中，演講者正介紹 Amazon ECS（Elastic Container Service）的巨大規模和其在 AWS 服務中的應用。提到的要點包括：

每週啟動超過 22.5 億個 Amazon ECS 任務。

每秒處理數以萬計的 API 請求。

在全球範圍內，ECS 服務遍佈於 32 個 AWS 地區和 102 個可用區。

超過 65% 的新 AWS 容器客戶選擇使用 ECS。

GuardDuty 是一項智能威脅檢測服務，可以持續監控異常活動和未經授權行為，從而幫助保護 AWS 帳戶和工作負載。通過引入對 ECS 的即時監控，AWS 旨在解決容器環境中獨特的安全挑戰，如容器逃逸、惡意軟件感染以及基於容器的供應鏈攻擊等。

圖說：圖片中展示了 Amazon GuardDuty 服務的概述，強調其在 AWS 生態系統中的普及和重要性。主要信息包括：

數以萬計的客戶跨行業和地理位置使用 Amazon GuardDuty。

這項服務保護了數百萬個帳戶，其中包括超過五億個 EC2 實例和數百萬個 S3 儲存桶。

超過 90% 的排名前 2000 的 AWS 客戶使用 Amazon GuardDuty。

從安全管理員到應用開發者，GuardDuty 的即時監控都提供了簡單而強大的工具，以保障 ECS 和 Fargate 環境的安全。對於安全專家來說，這意味著可以在整個 AWS 組織範圍內，輕鬆啟用並管理即時監控，而無需深入了解其底層運作原理。而對於應用開發者而言，他們可以專注於創建和運行應用，同時確保這些應用是在一個安全的環境中運行。

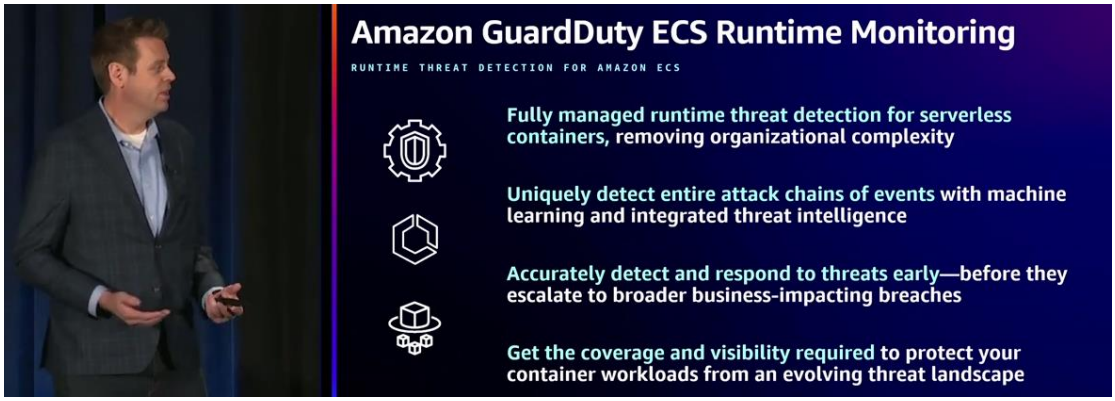
AWS 在 GuardDuty 上不斷創新，通過機器學習、威脅情報和複雜的狀態分析來提升威脅檢測的準確性和效率。這些技術的結合使 GuardDuty 能夠識別出複雜的威脅行為，包括但不限於文件無形執行、惡意域名查詢和高級持久性威脅（APT）。

隨著對 ECS 和 Fargate 的即時監控的引入，AWS 為容器環境提供了更加精細和深入的安全監控能力。不僅如此，通過簡化代理的部署和管理，AWS 確保了安全措施的實施既不會對性能產生負面影響，也不會增加用戶的管理負擔。這些代理基於 EBPF（Extended Berkeley Packet Filters）技術，能夠在不影響容器性能的前提下，提供對運行時環境的深入洞察。

AWS GuardDuty ECS 即時監控的引入，不僅展現了 AWS 在雲安全領域的持續創新和領導，也為 ECS 和 Fargate 用戶帶來了一層額外的保護，使他們能夠更加自信地在 AWS 雲上構建和部署容器化應用。隨著技術的不斷進步，AWS 將繼續提供先進的工具和服務，以幫助用戶應對不斷變化的安全挑戰，確保他們的雲環境安全可靠。

Streamlining security investigations with Amazon Security Lake (SEC234)

在這場演講中，安全專家們集結一堂，共同探討如何透過 Amazon Security Lake 加強安全調查的效率。Matt，AWS 偵測與回應服務的全球市場負責人，首先向我們介紹了包括 GuardDuty、Security Hub、Inspector、Macie、Detective 在內的六項相關安全服務，並特別提到了新推出的 Amazon Security Lake。



圖說：圖片中演講者正在介紹 Amazon GuardDuty ECS 運行時監控服務，它為 Amazon ECS 提供了運行時威脅檢測。它的主要特點包括：

為無伺服器容器提供全面管理的運行時威脅檢測，減少了組織的複雜性。

利用機器學習和整合的威脅情報，獨特地檢測整個攻擊事件鏈。

能夠準確地早期檢測和響應威脅，在它們升級為影響更廣業務的安全漏洞前。

提供了所需的覆蓋範圍和能見度，保護容器工作負載免受不斷變化的威脅風險。

這項新服務的誕生，源於 AWS 對客戶在建立安全資料湖時面臨的挑戰的深刻洞察。AWS 始終以客戶為中心，對客戶需求的敏銳洞察促使其創建了 Security Lake，旨在集中和標準化整個企業環境中的安全相關日誌，不僅支援 AWS，也延伸至混合雲和多雲環境，為長期保留提供了可靠解決方案，並大大增加了分析服務的選擇自由。

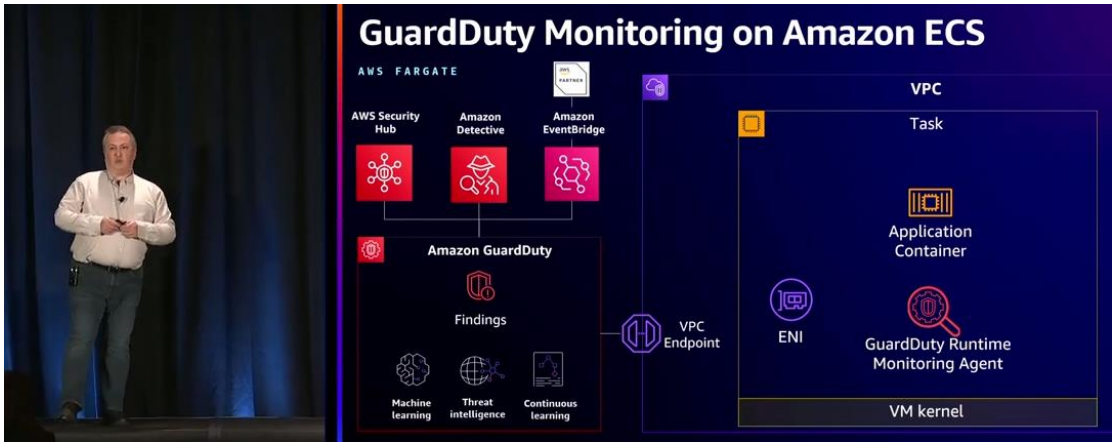
Matt 強調，現代資料策略的關鍵在於擁有共通的架構。為了實現這一目標，AWS 聯手 Splunk 和其他 18 家企業共同創立了開源項目 OCSF（Open Cybersecurity Schema Framework），致力於標準化和模板化安全相關資料，這對 Security Lake 的建立至關重要。

SEEK，作為澳洲、新西蘭以及東南亞領先的在線招聘市場平台，在 AWS re:Invent 2023 上分享了他們如何利用 Amazon Security Lake 來解決安全日誌和事件資料管理的挑戰。

首先，Andrew 指出，隨著 SEEK 業務的快速發展，安全團隊需要處理的日誌量驚人，而且安全工具的多樣性進一步加大了管理難度。SEEK 過去嘗試過使

用共通信息模型（CIM）來標準化日誌資料，但並未取得預期的成效。在此背景下，SEEK 開始尋找更有效的安全日誌管理方案。

在 2022 年，SEEK 已開始著手設計一個安全資料湖來統一管理和分析安全日誌。而 Amazon Security Lake 的推出，讓 SEEK 看到了一個既能滿足其當前需求又具有未來擴展性的解決方案。Security Lake 的設計原則與 SEEK 的需求高度契合，尤其是在分離關注點、性能優化和操作效率方面。



圖說：Andrew 在展示一個介紹 Amazon ECS 上的 GuardDuty 監控的架構圖。這張簡報展示了 Amazon GuardDuty 在 AWS Fargate 環境中的工作流程。從左至右，架構圖解釋了如何從應用容器中收集發現（Findings），這些發現是通過機器學習、威脅情報以及持續學習得出的。收集到的資料會透過 VPC 端點發送，並通過彈性網絡接口（ENI）進行處理。這些發現可以整合到 AWS Security Hub、Amazon Detective 和 Amazon EventBridge，從而為 AWS 客戶提供一個全面的安全監控和響應解決方案。圖片底部有 AWS 的標誌以及版權信息表明這是一項 AWS 服務。

SEEK 通過 Security Lake 整合了各種原生 AWS 資料源，如 VPC Flow Logs、CloudTrail、Security Hub 以及 DNS 日誌，並且還將來自合作夥伴的資料，比如 CrowdStrike 和 Netskope，以及自定義資料源整合到了安全資料湖中。這不僅讓 SEEK 能夠淘汰一些舊有的資料收集自動化流程，還為他們提供了之前未有的 DNS 日誌可視化能力。

SEEK 在 Security Lake 中的應用不限於安全分析。例如，當一個工程團隊需要確定一個特定 VPC 中 NAT 閘道流量異常高的原因時，他們就利用 Security Lake 中的 DNS 和 VPC 流量日誌來快速定位問題。這一點展示了 Security Lake 的應用範圍遠不止於安全領域，還可以支援雲運營和工程問題的解決。
Andrew 分享了兩個具體的安全事件調查案例，展示了 Security Lake 在實際操作中的價值。第一個案例是針對 Amazon GuardDuty 報告的一次未授權訪問事件。透過 Security Lake，SEEK 安全團隊能夠快速確認該事件是由於一個舊的威脅 IP 重新分配所致，而非真正的安全事件。第二個案例涉及對某個高級持續

性威脅（APT）的調查。SEEK 通過 Security Lake 快速搜索整個 AWS 環境中所有帳戶和地區的日誌，找到了一台與惡意 IP 通信的主機，最終確認這是一次虛驚。

最後，Andrew 展望了 SEEK 使用 Security Lake 的未來，計劃將更多的資料源整合進來，並擴展到更加主動的安全用例，如威脅狩獵和攻擊路徑映射等。SEEK 的案例充分證明了 Amazon Security Lake 不僅能幫助企業解決當前的安全日誌和事件資料管理問題，還為未來提供了擴展和創新的可能性。SEEK 的案例特別突出了 Security Lake 在應對大量日誌資料和提高查詢效率方面的優勢，以及它如何使 SEEK 得以發現並應對之前無法察覺的安全威脅。這些實際應用案例為參與者提供了豐富的啟示，不僅限於安全團隊，也包括基礎架構團隊，讓參與者了解到 Security Lake 的多面性和強大功能。

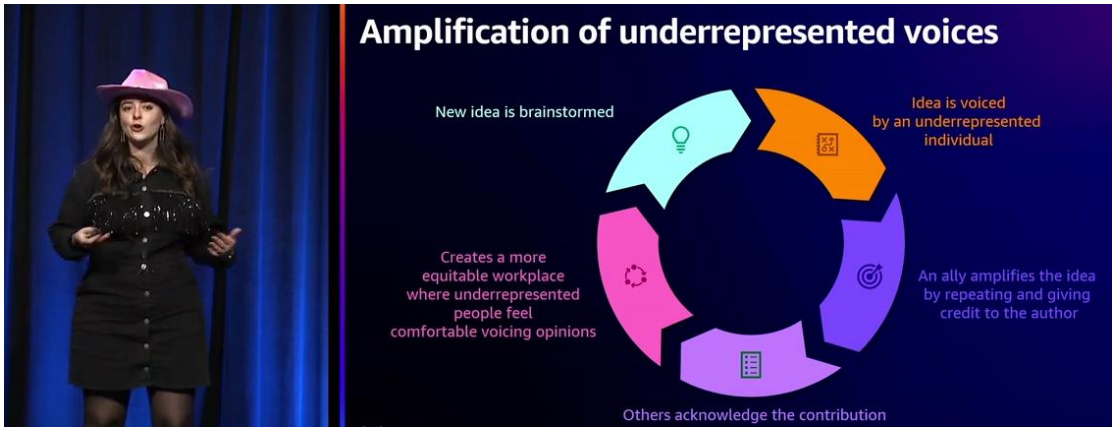
Sustainable security culture: Empower builders for success (SEC211)

在這場演講中，Hart Rossman 和 Sarah Currey，分享了他們豐富的經驗和看法，探討了如何在組織中建立一種持續的安全文化。他們的演講不僅僅是關於技術的深入解析，更多的是關於人性化的管理和領導策略，以及如何通過包容性和同理心來賦能團隊成員，從而使他們成為安全領域的冠軍。

首先，Sarah 談到了許多組織在建立安全文化時遇到的挑戰，比如安全架構師的短缺，或是團隊成員缺乏雲計算技能。她強調，透過實踐策略來賦予建設者更大的能力是非常關鍵的。Hart 則分享了一些關於如何將安全文化融入業務運營中的故事，強調了向董事會報告和讓組織內的不同團隊理解安全重要性的重要性。

圖說：Sarah 正在講述一個安全文化的發展藍圖，講述了從將安全植入業務運營的核心，到建立心理安全的基礎，再到構建一個對升級問題友好的安全文化，最終賦予構建者成為安全冠軍的能力。這是一個漸進的過程，旨在逐步增強組織的安全態勢，同時確保團隊成員感到被支持並被賦權。

他們接著談到了心理安全的基礎，即創建一個團隊成員可以毫無顧慮地提出想法、承擔風險並表達擔憂的環境。Sarah 透過分享自己在 AWS 初期的一個故事來強調這一點，這個故事展示了正面反饋和同儕支持對於鼓勵團隊成員積極參與和改善安全措施的重要性。



圖說：Sarah 說明如何在組織中增強那些未充分代表的聲音的過程。

這個流程圖的四個階段分別是：

1.New idea is brainstormed（新想法的集思廣益）：這指的是在團隊或會議中提出新想法的階段。

2.**Idea is voiced by an underrepresented individual（來自未充分代表的個體的想法）**：這一階段強調一個通常在討論中可能被忽略或未被充分聽取的個體提出想法。

3.**An ally amplifies the idea by repeating and giving credit to the author（盟友通過重述並歸功於原作者來放大這個想法）**：此處展示了一個盟友（或者支持者）的角色，他們通過公開承認和重述來強調這個想法，從而支持那些未被充分代表的聲音。

4.**Others acknowledge the contribution（其他人確認這份貢獻）**：這一階段是指其他團隊成員認可並接受這個想法，從而確保原始提出者得到應有的認可。

整體而言，這幅圖提供了一種增強未充分代表群體在職場上發聲的方法，旨在創造一個更平等的工作環境，讓所有人都感到舒適地表達自己的意見。這樣的流程有助於確保所有員工，不論背景或身份，都能夠被聽見並獲得認可。

他們還討論了如何減少團隊成員的燒盡感，例如通過時間友好的會議安排和有效的項目交接來實現這一目標。此外，透過 AWS Security Guardians 計劃，他們展示了如何將不是安全角色的建設者賦能為安全冠軍，這不僅提高了安全意識，還幫助減少了中等和高優先級的安全發現。

圖說：Security Guardians 是受過訓練、具有安全意識的亞馬遜員工，他們自願成為其團隊的安全冠軍。他們與同事合作，做出明智的安全決策，確保安全且準時的產品發布。他們還充當 AppSec 功能的擴展，擴大安全意識並提供強有力的反饋機制。

Hart 強調了持續教育的重要性，無論是通過每周的安全業務會議，還是透過正式的培訓和指導計劃，都能夠幫助團隊成員不斷提升自己在安全領域的技能和知識。他們最後強調了“反向指導”(reverse mentoring)的概念，這是一種讓經驗豐富的領導者從團隊中的新成員那裡學習的方法，這不僅能促進跨代溝通，還能增加組織內的創新和多樣性。

總而言之，Hart 和 Sarah 的演講不僅分享了建立持續安全文化的策略和實踐，更重要的是強調了以人為本的管理和領導方式對於促進團隊成員成長和發展的重要性。透過包容性、同理心和賦能，任何組織都能夠培養出一支既專業又充滿激情的安全團隊。

The AWS data-driven perspective on threat landscape trends (SEC236)

這場名為 "資料驅動觀點下的威脅景觀趨勢" 的演講，由 Amazon GuardDuty 團隊的 Ryan Holland 和 Shield 威脅研究團隊的 Paul 共同呈現，他們以豐富的經驗和深入的分析，為我們繪製了一幅網絡安全的全景圖。

這場演講不僅探討了高層次的趨勢，還深入了解了 AWS 從 GuardDuty 和網絡邊界的角度觀察到的現象。演講的核心在於介紹 AWS 如何進行威脅研究，包括建立分析系統以找出趨勢，以及如何利用這些情報設計防禦措施以保護網絡的可用性。這一切都基於一個使命：使 AWS 成為一個對惡意行為者來說不具吸引力的目標。通過增加攻擊者的成本和難度，AWS 希望為在其平台上運行工作負載的每一位用戶創造一個更安全的環境。

Paul 深入介紹了 DDoS 攻擊的趨勢，特別是應用層攻擊如何變得更加普遍。這種攻擊的增長不僅體現在數量上，也體現在攻擊的創新性上，迫使 AWS 不斷革新以應對這些挑戰。為了有效應對這些攻擊，AWS 追踪了 DDoS 基礎設施，並通過維護一個涉及惡意行為者 IP 地址的黑名單來提供防護。這個策略出乎意料地有效，因為它利用了 AWS 龐大的網絡，使得即使是最活躍的攻擊者也難以持續不斷地更換其攻擊基礎設施。

MadPot 是 AWS 用來收集全球威脅情報的一個複雜系統。透過在全球部署超過 10,000 個感應器，AWS 每天能夠攔截超過 1 億次的潛在威脅互動。這些資料不僅豐富了 AWS 對於當前威脅景觀的了解，也為其安全策略提供了堅實的基礎。實際上，從 MadPot 系統部署新的感應器開始，平均僅需 3 分鐘就會有攻擊嘗試發生，這一資料點突顯了網絡空間的危險性和無處不在的威脅。

圖說：Paul 指出，AWS 全球部署了超過 10,000 個感測器，每天觀察超過 1 億個潛在的威脅互動，並將其中 500,000 個活動每日歸類為惡意行為。這強調了 AWS 在全球範圍內監控和分析網絡威脅活動的能力，這些資料幫助 AWS 改善其安全性能，並為客戶提供了更高水準的保護。

Ryan Holland 則從 GuardDuty 的視角分享了 AWS 如何檢測和回應客戶帳戶內的威脅。GuardDuty 透過分析多種日誌來源，如 EC2 流量日誌、DNS 日誌和 CloudTrail 日誌，來識別潛在的威脅行為。Ryan 分享了一個關於如何識別和反應於 EKS 集群中的錯誤配置的實際案例，這個案例清楚地展示了 AWS 如何通過

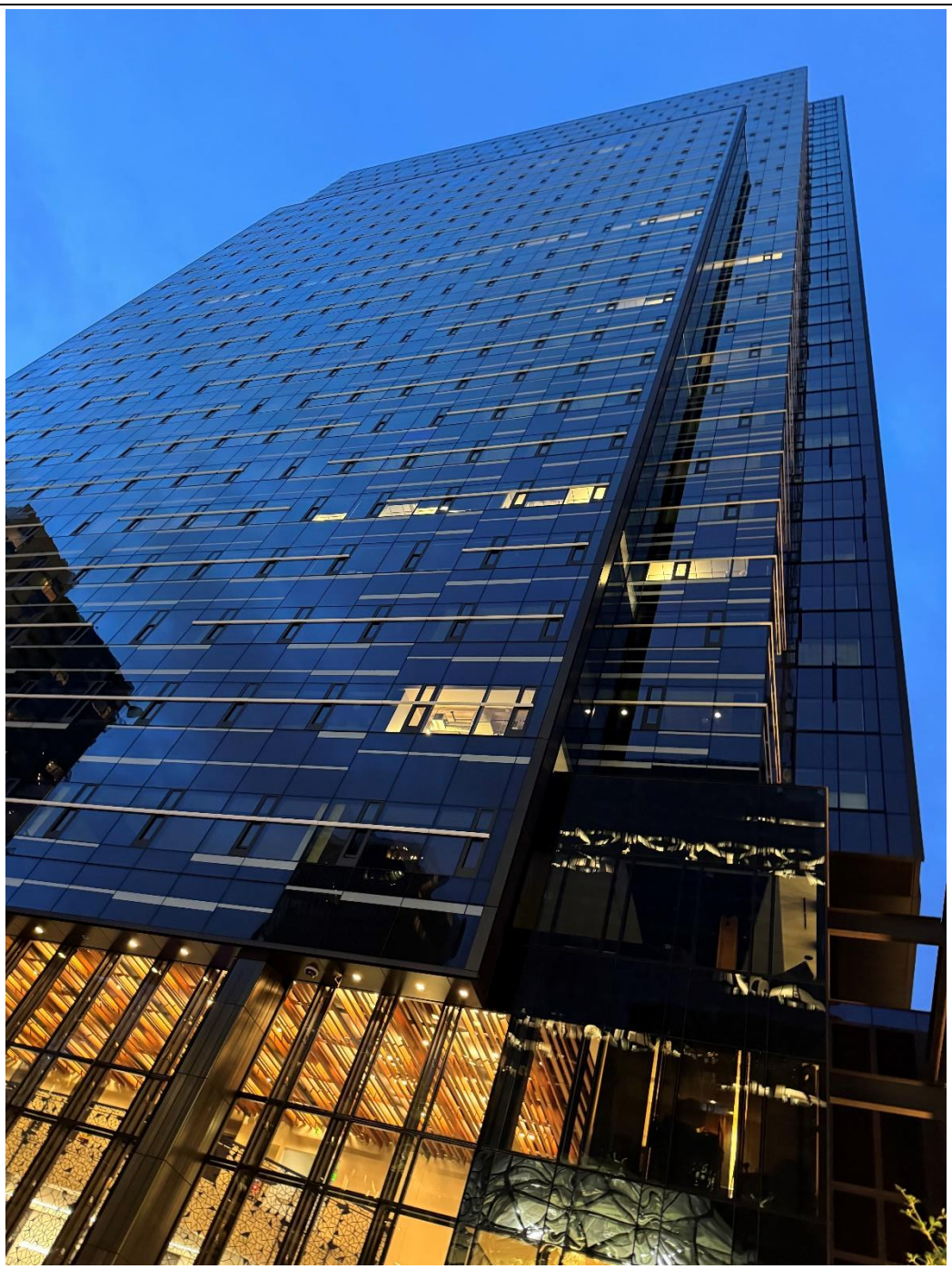
一系列的檢測結果指導客戶糾正安全漏洞。

Ryan 介紹 AWS 從 2017 年到 2023 年的威脅偵測和監控能力演進。從最初專注於 EC2 流量日誌和 DNS 日誌，擴展到包含 CloudTrail、S3 資料事件、EKS 審計日誌、RDS 登錄事件、Lambda 流量日誌和即時事件。使用威脅情報、TTP 檢測演算法、機器學習異常檢測和惡意軟件檢測，AWS 已經發展出 164 種不同的發現類型，並通過 AWS Security Hub、Amazon Detective、Amazon EventBridge 和 AWS 合作夥伴等服務提供客戶警告和洞察。

演講的結尾強調了 AWS 的努力不僅僅是為了保護自己的網絡，更是為了整個互聯網的安全作出貢獻。通過與互聯網上的其他參與者合作，AWS 致力於清除惡意基礎設施，提高攻擊者的成本，從而使得針對 AWS 網絡的攻擊變得不再具有吸引力。

這場演講不僅提供了對當前威脅趨勢的深入理解，還展示了 AWS 在保護其客戶免受這些威脅影響方面所採取的先進和多層次的方法。對於在 AWS 上運行關鍵業務負載的企業和個人而言，這是一個令人鼓舞的訊息：在 AWS 的保護之下，他們可以更安心地進行創新和業務拓展。

參訪 AWS 西雅圖總部



圖說：AWS 西雅圖 day 1 辦公室外觀

圖說：合影留念

圖說：主題式討論及分享

圖說：視訊交流

圖說：西雅圖 AWS 總部 The Spheres

心得與建議事項

這次參加 AWS re:Invent 2023，不僅開拓了我在雲端技術方面的視野，也讓我深入了解了混合雲架構和雲治理在電力行業中的重要性。以下是我這次參訪的主要心得與建議：

1.加速雲端轉型，建立電力行業的雲端卓越中心（CCoE）

電力公司應積極擁抱雲端技術，透過建立 CCoE 來推動和管理雲端採用策略。CCoE 可以幫助電力公司制定長遠的雲端採用策略，確保雲端採用遵守相關法規和標準，控制雲端支出，並推動人工智慧、機器學習等先進技術在智慧電網中的應用。

2.利用 AI 和資料驅動來優化電網運營和決策

台電應充分利用 AI 和資料分析技術來提高電網運營效率和可靠性。透過對電網資料的深入分析，電力公司可以更好地預測和管理能源需求，優化能源分配，並識別節能減碳的機會。同時，AI 技術如生成式 AI 也可應用於 ESG 報告和資料驅動的決策制定，提高企業的可持續性表現。

3.強化韌性，建立高可用且可恢復的智慧電網

隨著電網複雜性的增加，電力公司必須建立起高度韌性的資訊系統來應對各種挑戰。這包括採用細胞化架構設計、進行混沌工程測試、實施跨區域災難恢復策略等。同時，應加強對關鍵系統的即時監控，利用機器學習進行異常檢測和故障預測，從而最大限度地減少停電時間和服務中斷。

4.追求可持續發展，提高能源效率和減少碳足跡

透過採用雲端技術，電力公司可以優化 IT 基礎設施，減少不必要的能源消耗。同時，透過 AI 和資料分析，電力公司可以更精準地預測能源需求，優化能源分配，並找出節能減碳的機會。

5.加強合規性管理，確保資料安全和隱私保護

在數位化轉型的過程中，電力公司必須嚴格遵守相關法規和標準，特別是在資料安全和隱私保護方面。透過採用 AWS 提供的合規與審計服務，如 AWS Control Tower、AWS Config 等，電力公司可以加強其雲端環境的治理和合規性管理，確保關鍵資料和系統的安全性。

6.推動維運自動化，提高效率和服務質量

電力公司應積極採用自動化技術來簡化日常維運工作，減少人為錯誤，提高系統可靠性。透過 AWS 提供的自動化工具和服務，如 AWS Systems Manager，電力公司可以實現跨環境的自動化操作，如補丁管理、事件處理等。同時，企業應重視自動化中的可觀察性和可見性，利用 AI 和 ML 技術來加速問題識別和響應。

7.打造台電生成式 AI 先導平台

透過建立生成式 AI 先導平台，台電可以提高運營效率、優化決策制定、改善客戶服務等方面大幅精進。首先，台電可以利用生成式 AI 技術來輔助強化電

力調度和能源管理。通過對歷史資料和即時資料的深度學習，AI 系統可以生成精准的電力需求預測模型，幫助台電更好地平衡供需關係，減少能源浪費。同時，生成式 AI 還可以模擬各種極端天氣和故障情景，為電網的韌性設計提供有力支持。其次，生成式 AI 可以賦能台電的客戶服務和互動。透過自然語言處理和對話生成技術，AI 系統可以提供智慧化的客戶諮詢和問題解答，大大提高服務效率和質量。此外，生成式 AI 還可以根據客戶的用電行為和偏好，生成個性化的能源使用報告和節能建議，提升客戶體驗和滿意度。再者，台電可以運用生成式 AI 來輔助決策制定和策略規劃。透過對能源市場、技術趨勢、政策法規等海量信息的分析和知識萃取，AI 系統可以生成洞察報告和決策建議，為管理層提供有力支持。同時，生成式 AI 還可以模擬不同決策方案的效果，幫助台電選擇最佳的發展路徑。 最後，建立生成式 AI 先導平台還可以促進台電在能源生態中的創新合作。通過開放平台的建設，台電可以與學術界、創業公司等展開廣泛的技術交流與協作，共同探索生成式 AI 在智慧電網、綠色能源等領域的創新應用，引領能源行業的數位化轉型。

總之，數位化和智慧化轉型已成為電力行業的必然趨勢。AWS re:Invent 2023 為我們提供了寶貴的學習機會，讓我們深入了解了雲端技術、AI、資料分析等前沿領域的最新發展與應用。台電作為台灣電力行業的領導者，應積極擁抱變革，加速雲端轉型步伐，建立高度韌性和可持續的智慧電網，為台灣的能源未來贏得先機。