出國報告（出國類別：實習）

雲端治理相關實務研習

服務機關：台灣電力股份有限公司

姓名職稱：謝欣宸　主管（系統軟體一）

派赴國家/地區：美國　拉斯維加斯

出國期間：113 年 12 月 1 日至 113 年 12 月 9 日

報告日期：114 年 2 月 4 日

摘要

為規劃本公司未來建置混合雲之多雲環境，強化資通安全，建立完善的雲端治理，提升資訊服務之效能、安全及品質，推動數位轉型及達成經營策略目標，前往美國研習雲端治理相關實務。

美國亞馬遜網路服務公司（Amazon Web Services, AWS）為世界級公有雲端服務提供者，市佔率為全球第一名，提供超過 200 種雲端服務，其服務之用戶橫跨多個不同國家及各種產業，本次出國實習為前往美國拉斯維加斯參加該公司舉辦之「AWS re:Invent 2024」大型雲端服務研討交流活動，透過參與最新的雲端運算服務發表、產業實務應用演講等，學習在雲端運算及生成式人工智慧蓬勃發展且快速變遷的時代，AWS 如何做到雲端治理及資通安全防護，並思考如何應用於本公司，以利推動雲端治理，達成經營策略目標。

目錄

一、目的

依據本公司 113 至 117 年經營策略所制定之十大策略：(1) 確保穩定供電、(2) 強化電網韌性、(3) 確保財務永續、(4) 邁向淨零排放、(5) 營造友善環境、(6) 推動數位轉型、(7) 精進用戶服務、(8) 落實職業安全、(9) 提升人力價值及(10) 深化社會責任，本公司為推動第六項策略數位轉型，目前正在建設遠信雲端資料中心與彰化雲端資料中心，預計將於 114 年啟用彰化雲端資料中心、115 年啟用遠信雲端資料中心，並規劃利用雲端資料中心建置智慧電網大數據分析運用，提高再生能源發電預測之精準度，使電力調度更加快速且精準反應，同時搭配光纖通訊網路提供資訊智慧化線上服務，達成確保穩定供電、精進用戶服務之策略目標。

為規劃本公司未來混合雲之營運及治理框架，強化資通安全，並進行混合雲管理平台建置，以擘劃未來集團化經營之雲端服務藍圖，強化競爭力及提高資訊服務品質，使未來提供的雲端服務能夠實現預期效益，進而成為本公司穩定發展的基石，雲端治理是其中的關鍵性因素，透過良好的雲端治理，本公司可以確保雲端服務治理框架、資訊安全、法規遵循以及有效的風險管理，同時提高內部協作和溝通效率。

依據市場研究機構 Synergy Research Group 於 2024 年第 2 季全球公有雲市佔率調查報告，三大公有雲端服務提供者中，第一名為 Amazon Web Services（以下簡稱 AWS）以 32%的市佔率領先，第二名為 Microsoft Azure 市佔率 23%，第三名為 Google Cloud 市佔率 12%，這三家公有雲端服務提供者的市佔率合計達到 67%。AWS 作為全球公有雲服務之領導企業，舉辦「AWS re:Invent 2024」科技大

會，有最新的雲端運算服務發表、科技發展趨勢、產業實務應用演講、大型科技展覽等活動，邀請來自世界各地之雲端服務從業人員報名參加，透過研討、分享、討論與交流，共同學習與成長，強化企業核心競爭力。

本次出國實習目標為參加「AWS re:Invent 2024」大型雲端服務研討交流活動，並聚焦參加雲端治理相關的研討會，以研習 AWS 雲端治理實務，達成本公司經營策略目標。

二、實習內容

(一) 最佳化雲端工作負載

這場演講分享如何使用 AWS 建置最佳化雲端工作負載（Cloud Workload），這位專家說明有三個階段：設計與建立階段（Design and Build）、營運階段（Operate）與進化階段（Evolve）。

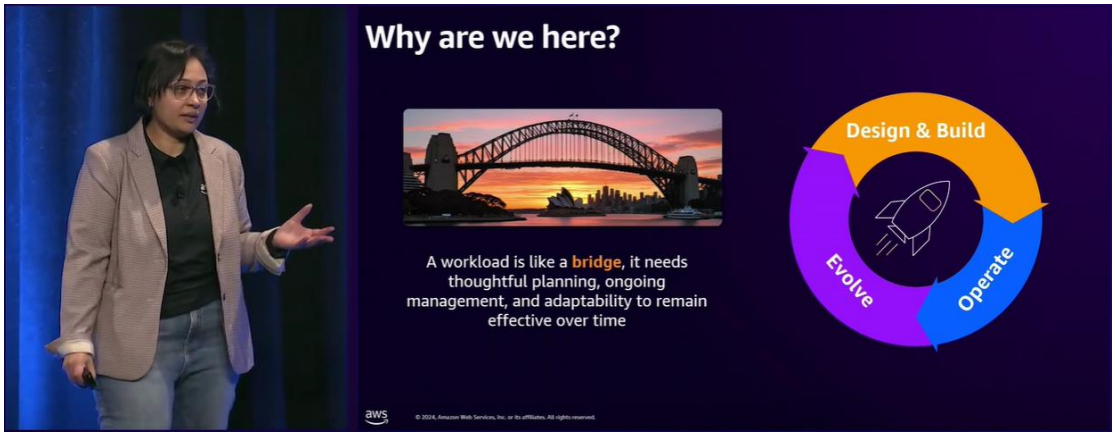

圖 1

在設計與建立階段，需要花一些時間，進行全面且完整的規劃，將整個雲端工作負載，建立穩定的架構基礎，同時也要考量到整個雲端工作負載的資通安全，以利保護資訊系統內的組織營運資料、機敏資料及個人資料。

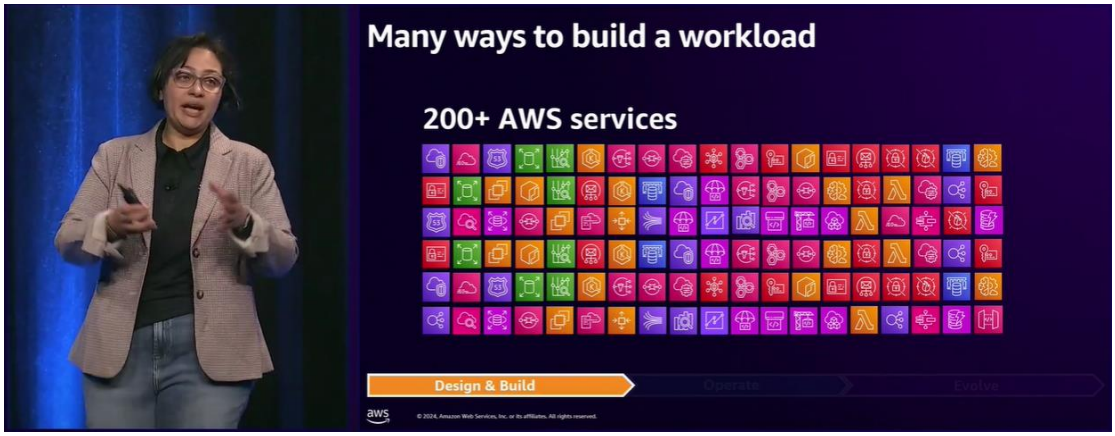

圖 2

AWS 有超過 200 多種雲端服務，並且雲端服務之間可以靈活的互相交換使用，因此可以選擇不同的服務來建立雲端工作負載，代表著完全不同的雲端服務架構，可以選擇基於伺服器（Based on Server）、無伺服器（Serverless）、或容器（Container）的架構。

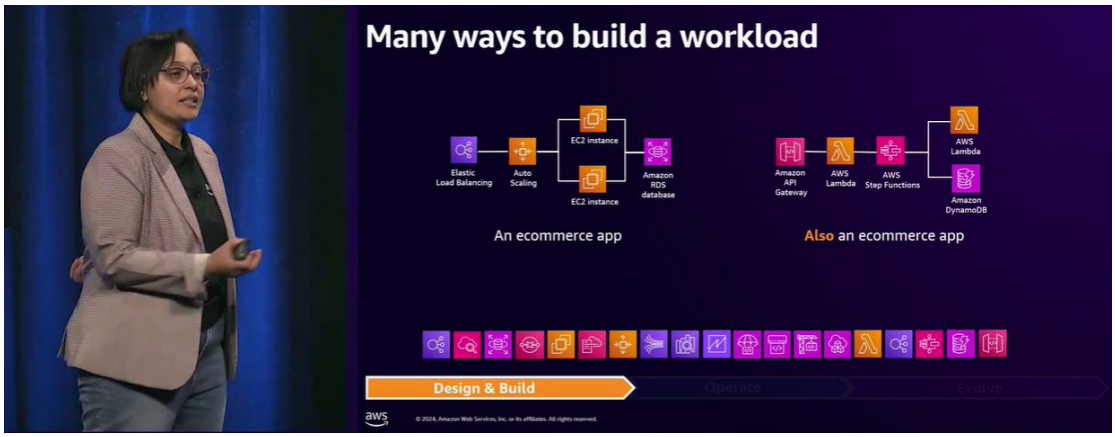

圖 3

以建立電子商務網站為例，可以選擇基於伺服器的架構，使用 AWS 的 Elastic Load Balancing、EC2 和 RDS 等雲端服務；也可以選擇無伺服器的架構，使用 AWS 的 API Gateway、Lambda、DynamoDB 等雲端服務；透過不同的雲端工作負載架構，達成相同的業務目標。

圖 4

在建立雲端工作負載時，需要設計雲端架構，並且考量六大主

要能力，包含：安全性、可靠性、成本、營運、效能與可持續性。安全性需要採取一些控制措施來保護雲端工作負載，避免惡意人士透過資安弱點進行攻擊，或是允許未經授權的資料存取。效能與可靠性可以確保雲端工作負載的運算資源，可以做到精確分配，並得以保持高效能的運作，如果忽然發生異常情形或是軟硬體的故障狀況，能夠快速地恢復營運，達成營運持續的目標。在營運部分需要持續執行與監控雲端工作負載，並且確保可以在保護資訊安全的前提下，維持高效能的方式運行。在成本與可持續性部分，追求建立的雲端工作負載不只是讓企業可以花費最小的雲端服務費用，更可以於環境保護方面做到企業社會責任。

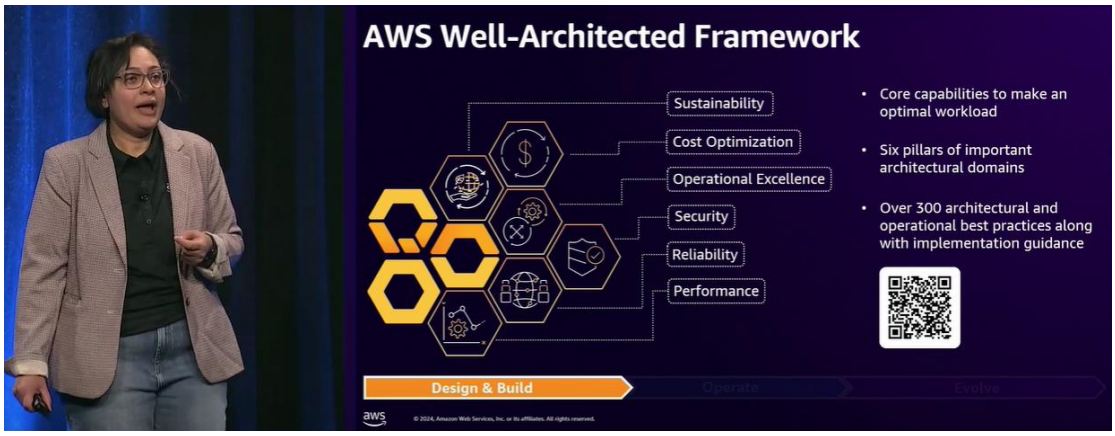

圖 5

為了在雲端工作負載追求達成上述六大主要能力，最佳解決方案為使用 AWS 的「Well-Architected Framework」雲端服務框架，這是 AWS 提供的用以協助雲端服務架構師，依據 AWS 的最佳實務來建立雲端工作負載。AWS 服務全球來自多個不同產業領域的企業客戶，具有相當豐富的雲端實務經驗。在永續發展、成本最佳化、卓越營運、安全性、可靠性與效能上，都有 AWS 提供的設計原則與最佳實務建議。

以營運電子商務網站作為範例，如果依據規定需要保存用戶操作紀錄 3 年，可以將用戶在網站上的操作紀錄發送到 AWS CloudWatch 進行監控，也可以將操作紀錄作為檔案上傳到 AWS S3 儲存桶，在可以達成相同功能目標的情形下，上傳到 AWS S3 可以更有成本優化的效益，因此使用 AWS Well-Architected Framework 進行最佳化雲端工作負載的設計非常重要。

在營運階段，需要針對雲端工作負載進行持續的監控，隨時進行弱點掃描、弱點修補與軟體更新，以維持雲端工作負載的最佳化效能與安全性。隨著持續運作雲端工作負載及業務需求的持續改變，使用到的 AWS 雲端服務數量可能會越來越多、越來越複雜，會使得維護人員越來越難以掌控與管理，因此在使用 AWS 雲端服務時，建立一套可以提供雲端資源配置狀態的統一視覺化管理工具非常重要，可以確保持續與 AWS 最佳實務保持一致。

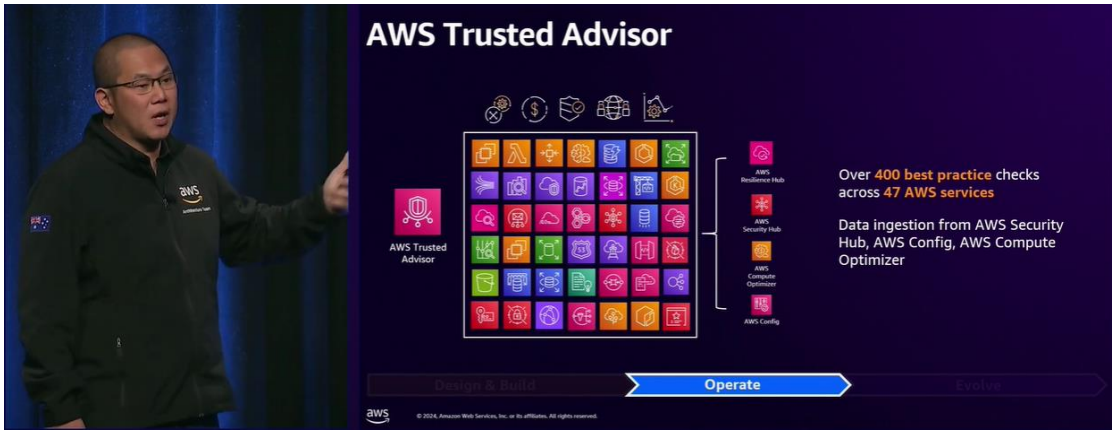

圖 6

AWS 提供 Trusted Advisor 雲端服務，可以持續檢查所有雲端資源的配置狀態，將所有的雲端資源配置與超過 400 個最佳實務與橫跨 47 個 AWS 雲端服務進行比較，並且和 AWS Security Hub、AWS Config、AWS Compute Optimizer 雲端服務進行資料整合，提供統一

的視覺化管理工具，呈現所有資源的配置狀態。

AWS Trusted Advisor 可以和 AWS EventBridge 整合，使得在進行雲端治理時，如果雲端工作負載監控到一些系統營運事件，可以透過自動觸發程式的方式來執行相關作業，例如：使用 AWS Lambda 或 AWS Systems Manager 執行程式。如此一來，除了持續監控以掌握雲端工作負載的現況之外，更可以自動化採取行動，達成妥善維護的快速反應能力。

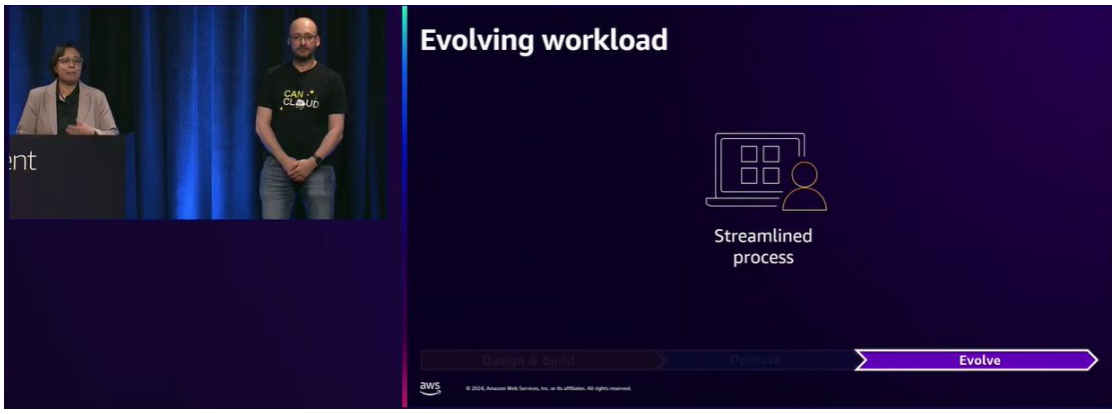

圖 7

在進化階段，在持續營運雲端工作負載到一段較長期的時間之後，需要追求減少工程師或維護人員所花費的人力時間，減少人為操作的失誤風險，並且提升雲端工作部門的工作效率。在生成式人工智慧快速發展的時代，可以使用生成式人工智慧精簡作業流程，提升工作效率及降低失誤發生的風險，努力將工作效率與工作品質達成平衡。

最後，實務上雲端工作負載會隨著企業組織變動、來自外部環境的壓力、政策的改變、新的業務需求、採用新的雲端服務等情形而隨時變動，因此需要定期執行 AWS Well-Architected Framework 確保雲端工作負載可以保持雲端治理的最佳實務。

(二) 多雲環境管理

多雲環境（Multi-cloud Environment）是指在多個雲端環境中運作工作負載，在多個雲端環境中營運會增加額外的成本與複雜度。

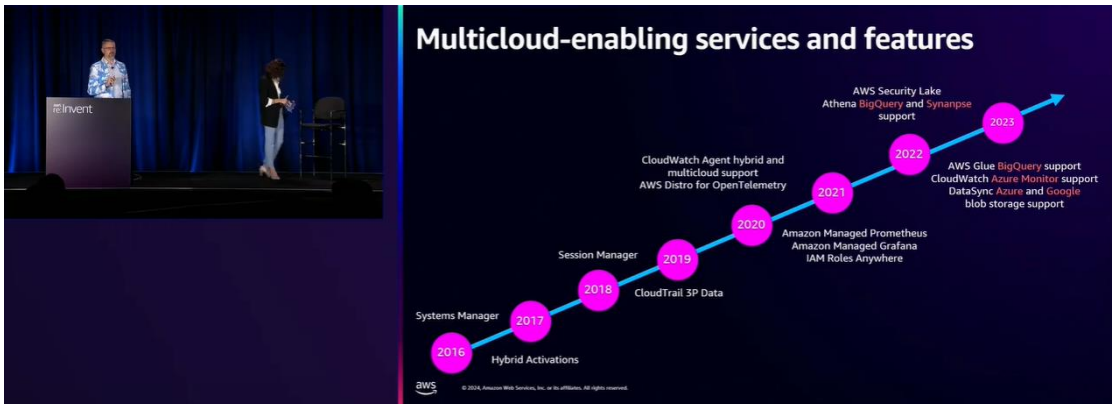

圖 8

AWS 從 2016 年起陸續推出多雲及混合雲的解決方案，使用戶可以採用 AWS 服務，整合本地端及其他雲端服務供應者（例如：Microsoft Azure）的平台或服務，以滿足多雲環境之用戶營運管理需求。

圖 9

首先專家說明需要多雲環境管理的情境，專家舉例業界常見的使用案例，原本有一家公司（Octank）在一個雲端平台上營運，之

後收購了另外一家公司（North Wind），而該公司是使用另外一個不同的雲端平台，因此需要決定，是否需要遷移這些雲端工作負載，以及處理合規要求。

圖 10

因為被收購的公司（North Wind）有一些既有的用戶協議，要求該公司繼續在原本的雲端工作負載運作，原本也有使用許多原生服務，重新架構並且搬遷雲端工作負載其實不太具有意義，還會失去既有員工的專業技能與知識，會產生需要額外進行員工培訓、教育訓練等人事成本，這就是多雲環境管理的意義，因為多雲代表有許多雲端工作負載與工具，企業需要將管理流程精簡、簡化及達成一致性。

多雲環境可以透過 AWS Systems Manager 服務存取本地端、AWS 或其他雲端服務平台之伺服器，且這些伺服器可以大量同時運行。

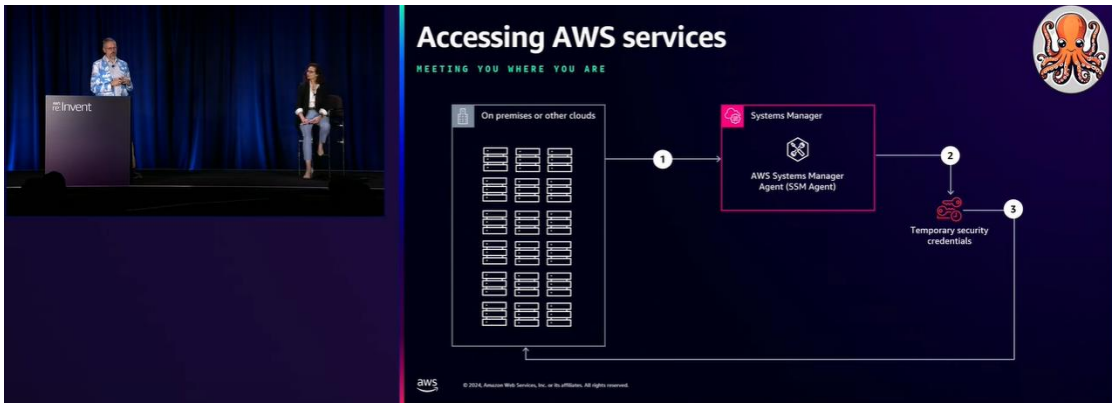

圖 11

使用 AWS Systems Manager 並且在本地環境或其他雲端服務平台之伺服器安裝 AWS Systems Manager Agent 代理軟體，並且將 Token 儲存在本地端的檔案系統內，這些 Token 可以對應到 AWS IAM 角色，再經由一些操作設定，即可透過 AWS Systems Manager 管理多雲環境之伺服器。

接下來將進行 AWS 實際操作說明的部分，首先進入 AWS 控制台。

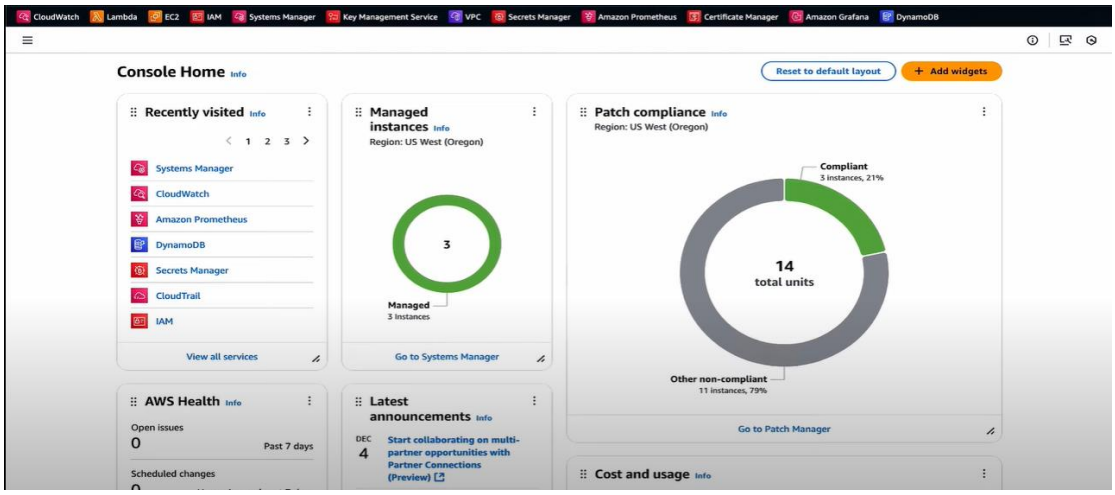

圖 12

可以點選進入 AWS Systems Manager 功能頁面：

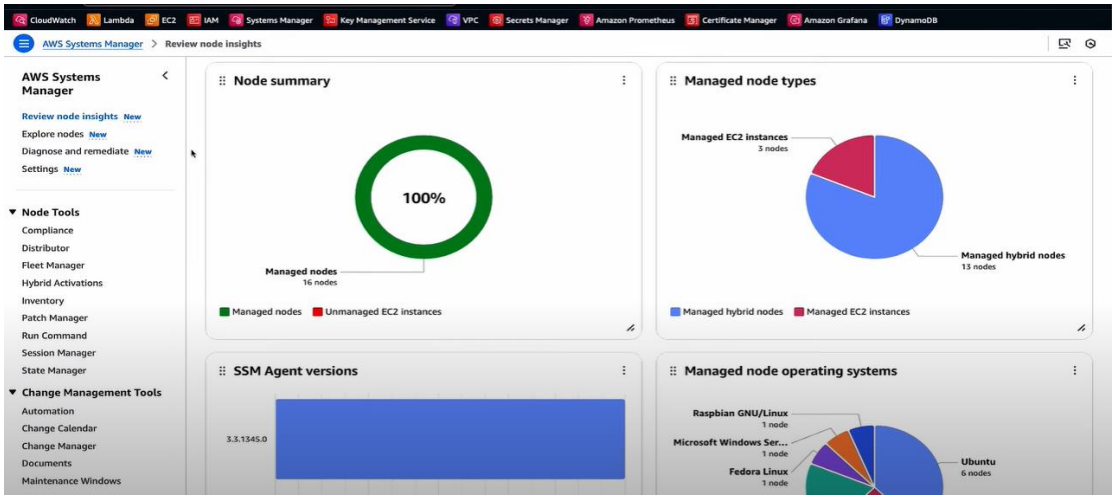

圖 13

為了示範 AWS Systems Manager 可以整合不同雲端服務平台之伺服器，在 Microsoft Azure 建立一個新伺服器之後，回到 AWS Systems Manager 的 Hybrid Activations 功能，點選 Create activation 按鈕。

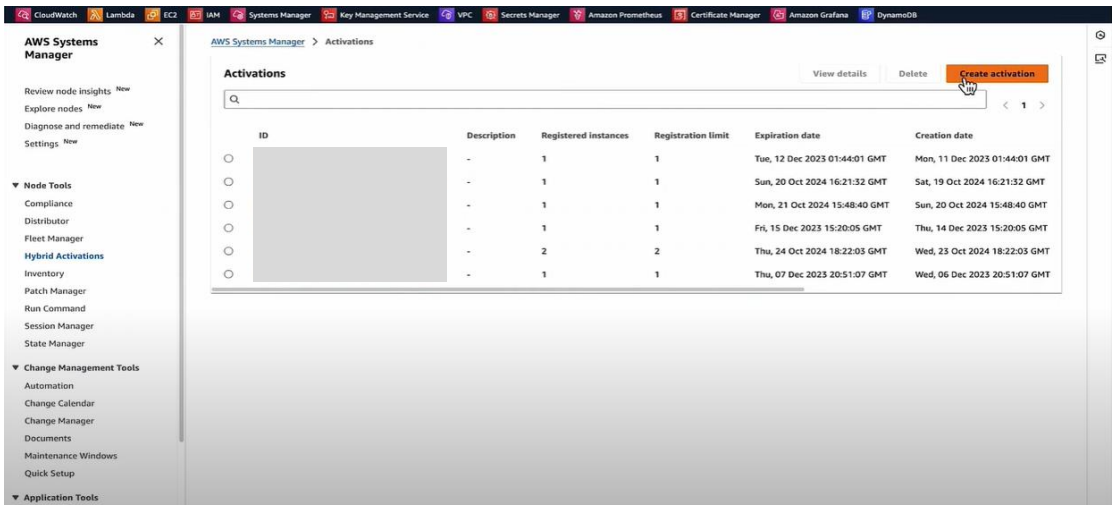

圖 14

操作完成之後，可以取得啟動碼及 ID，用於執行遠端存取。

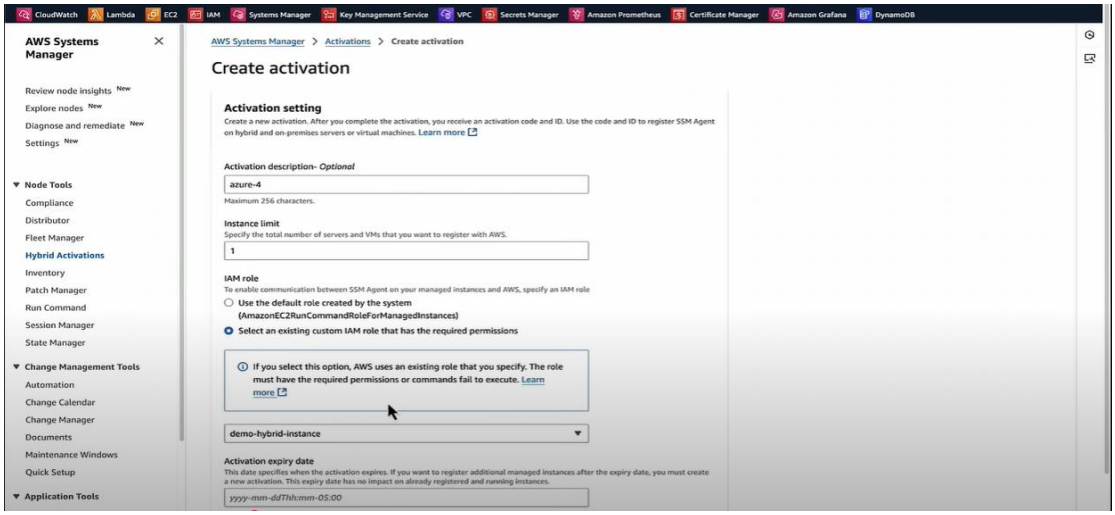

圖 15

登入在 Microsoft Azure 的伺服器，執行啟用 AWS Systems Manager Agent 的程序。

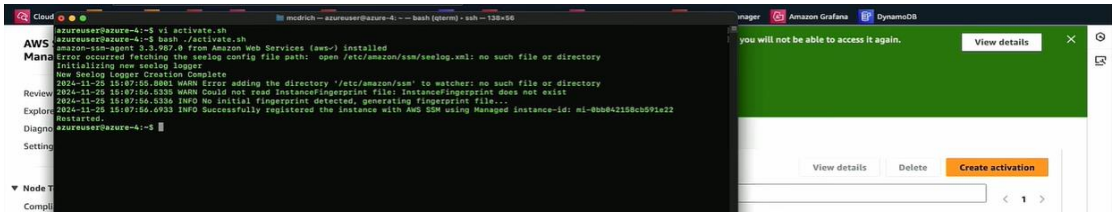

圖 16

回到 AWS Systems Manager，進入 Fleet Manager 功能頁面，即可看見新增的 Microsoft Azure 伺服器作為節點（Node）。

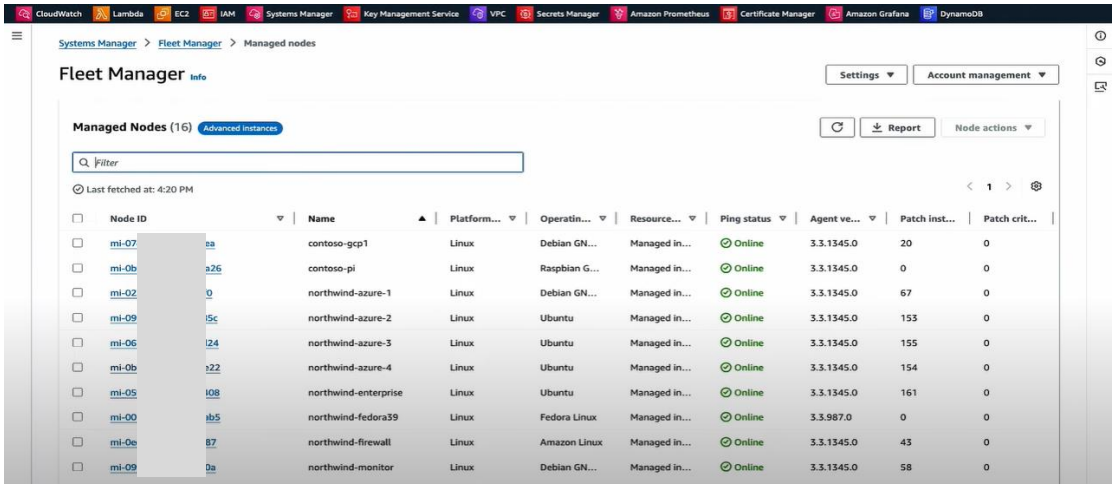

圖 17

點擊伺服器節點名稱，可以很快速的查詢該伺服器內的內容。

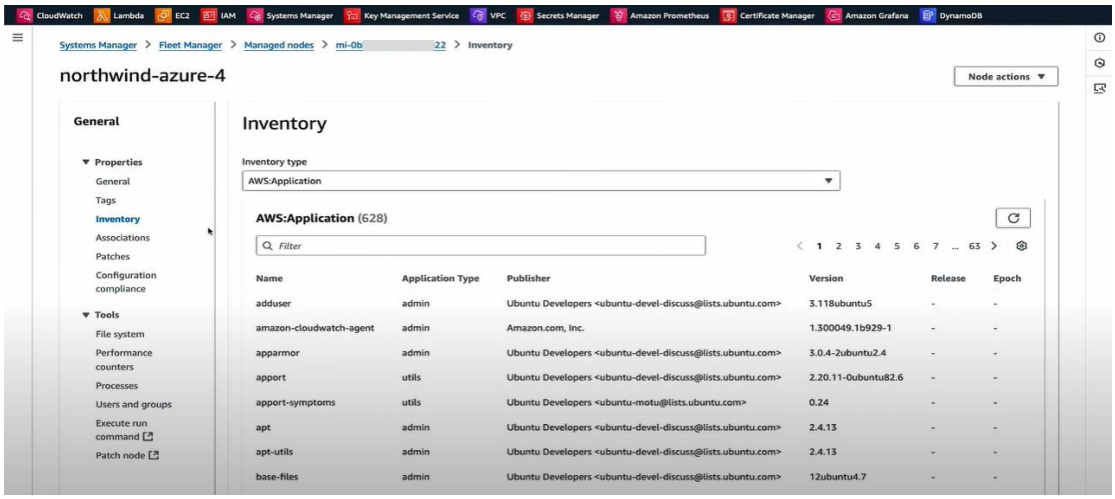

圖 18

如果有搜尋特定檔案的需求，輸入關鍵字搜尋（例如：bash），可以快速找到檔案，方便管理。

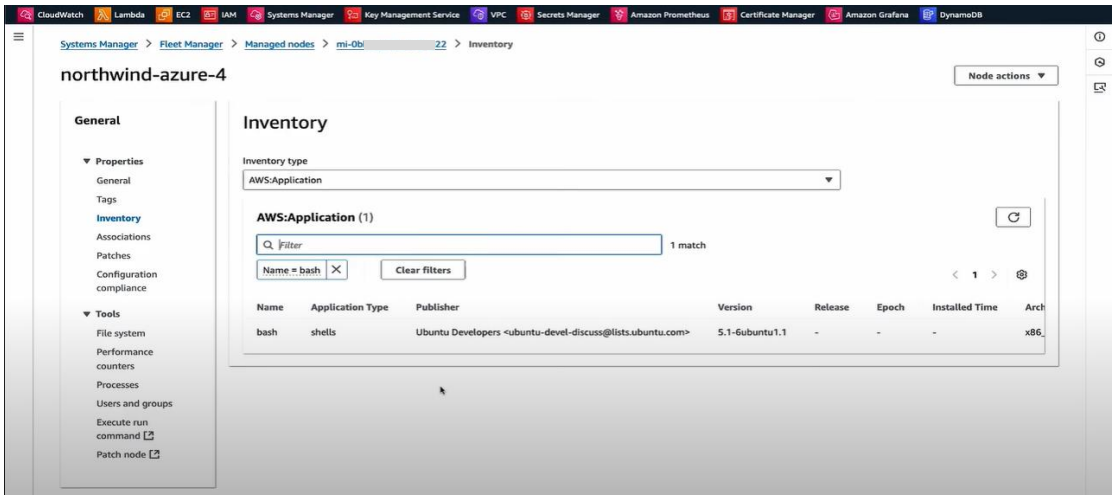

圖 19

如果想要透過 AWS Systems Manager 下載或上傳檔案到特定伺服器，進入 File system 頁面，可以快速達成。

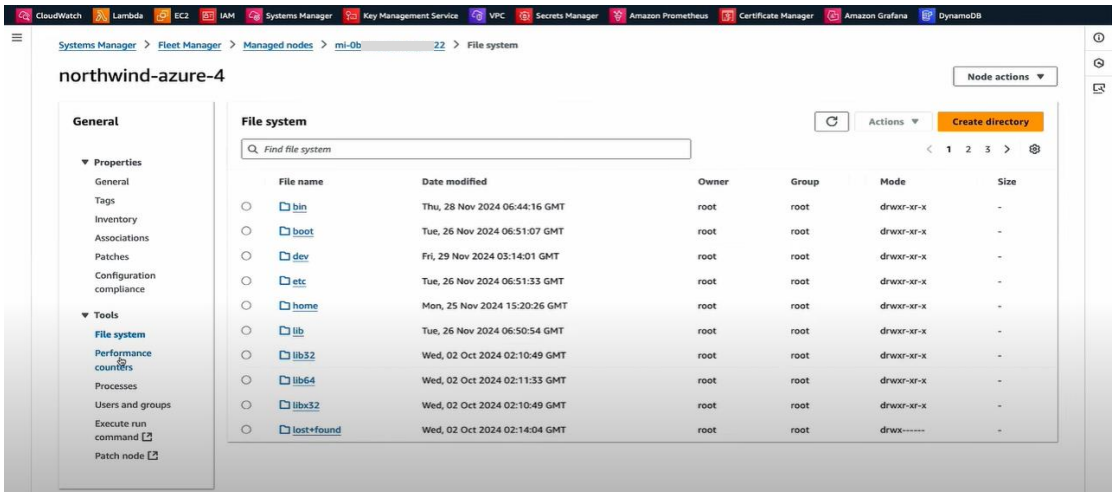

圖 20

透過 AWS Systems Manager 的 Performance counters 頁面，可以查詢伺服器之效能計數器，快速了解伺服器即時的運作情形，包含：CPU 使用率、磁碟輸入及輸出、網路頻寬、記憶體使用量等。

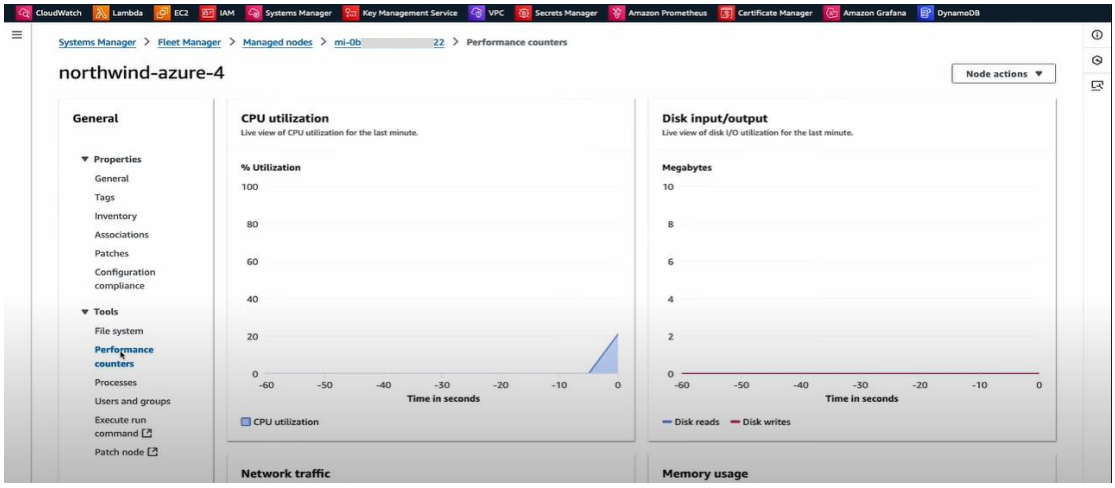

圖 21

如果發現有特定程序異常，可以透過網頁操作，進入 Process 頁面，點選想要終止執行的程序，點擊 Terminate process 按鈕即可終止程序，快速解決異常問題。

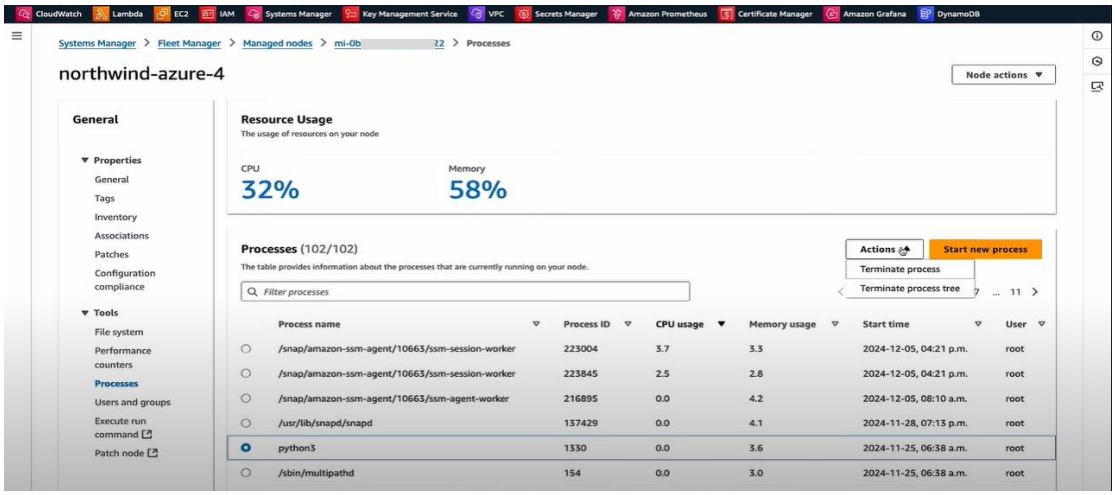

圖 22

使用 AWS Systems Manager 的 Patch Manager 功能，可以快速修補伺服器的補丁（Patch），並且支援發佈到多台伺服器。在多雲環境中，營運數量龐大的伺服器，同時需要針對舊版軟體進行補丁升級以降低資通安全風險時，此功能相當實用。

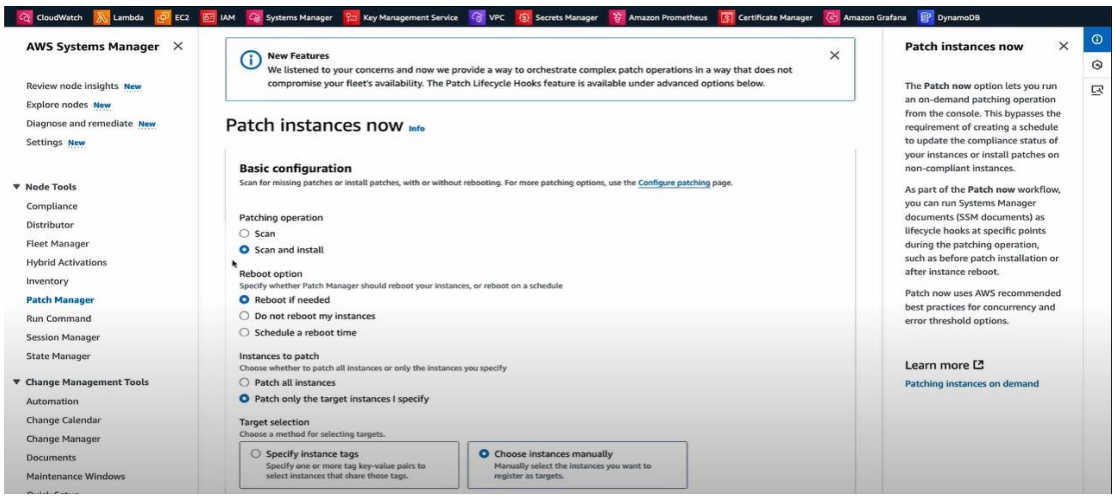

圖 23

下圖為安裝補丁成功之畫面：

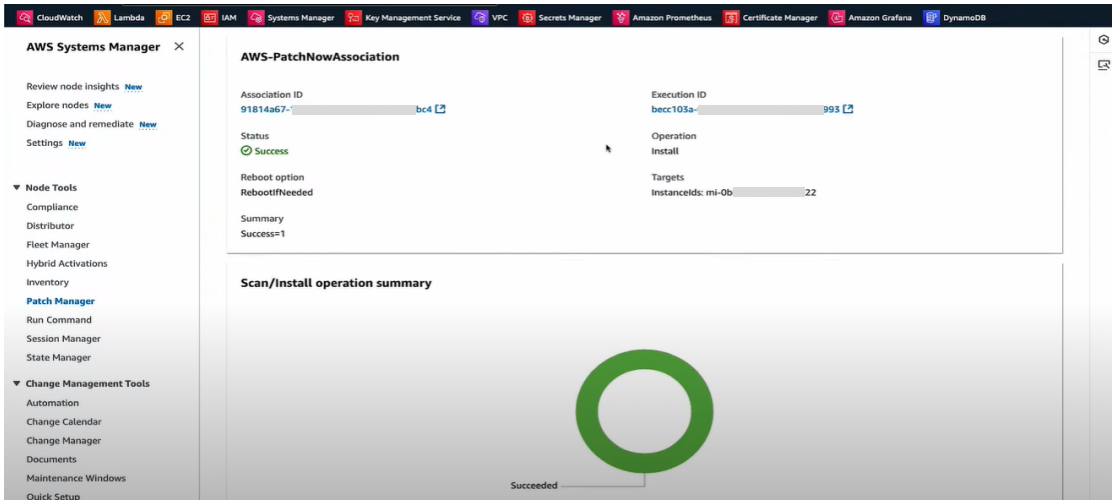

圖 24

使用 AWS Systems Manager 可以透過開發與執行程序腳本，達成自動化維運的功能。AWS 提供視覺化的設計介面，方便開發自動化程序腳本，下圖為範例。

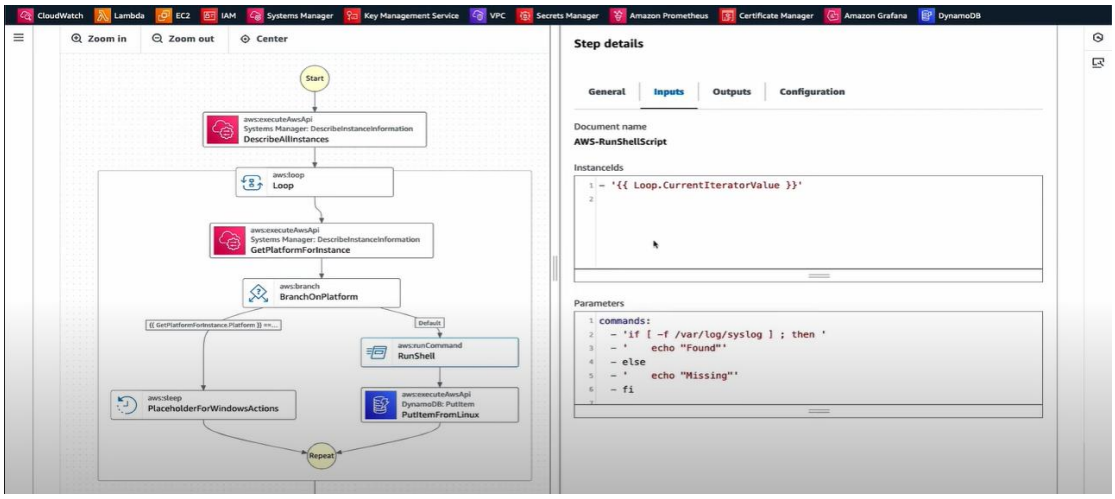

圖 25

在這個自動化程序腳本中，是想要在大量伺服器的多雲環境中，逐台伺服器搜尋符合特定名稱的檔案，並且將搜尋結果儲存到 AWS DynamoDB 資料庫，以利系統管理員快速取得搜尋結果，並進行後續行動，下圖為點擊 Execute automation 按鈕以執行自動化程

序。

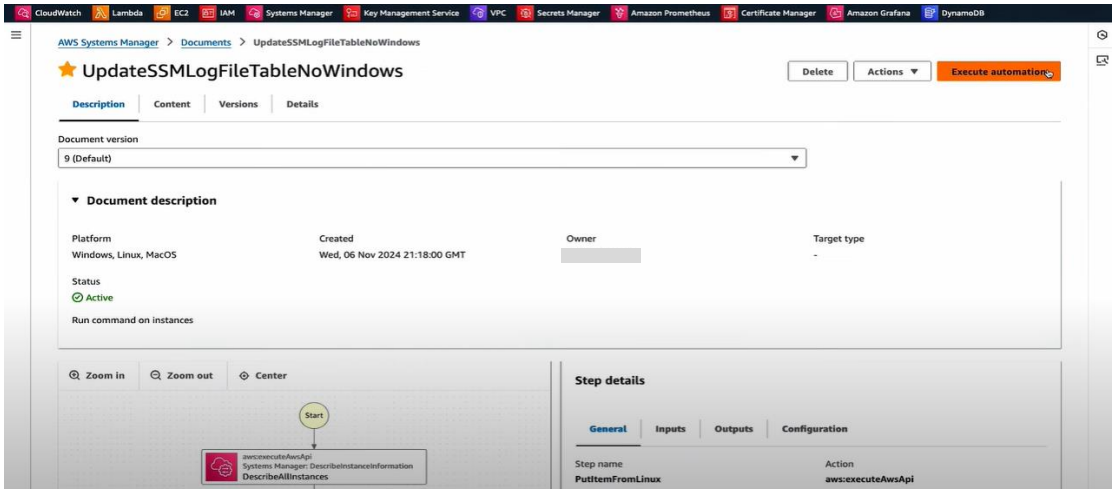

圖 26

前往 AWS DynamoDB 資料庫服務，進入 Explore items 功能頁面，可以快速查詢執行結果。

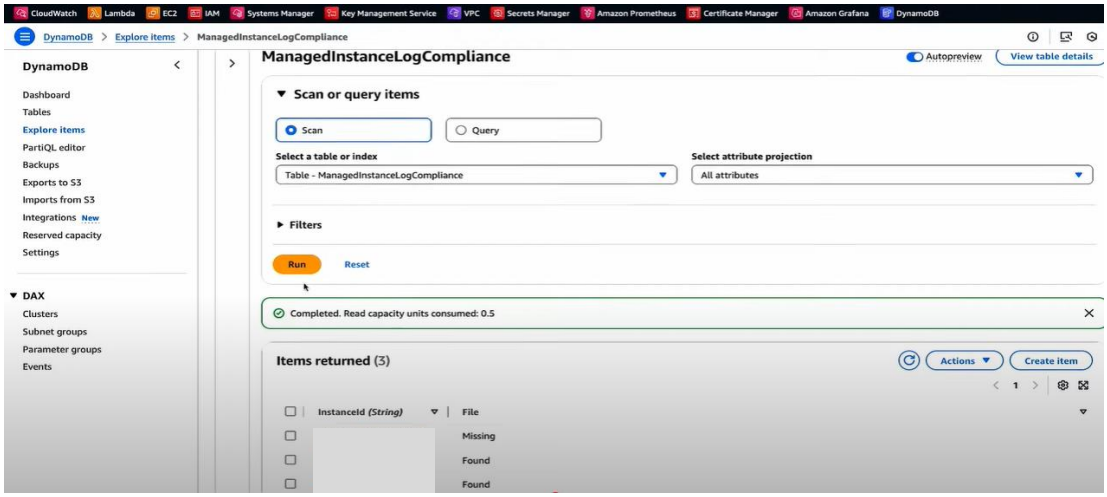

圖 27

AWS Systems Manager 的自動化功能，很適合用於需要每台伺服器固定執行程序的情境，方便進行多雲環境的營運管理。

為了控管伺服器執行及操作紀錄，可以將伺服器的所有操作紀錄整合到 AWS CloudWatch 監控服務。

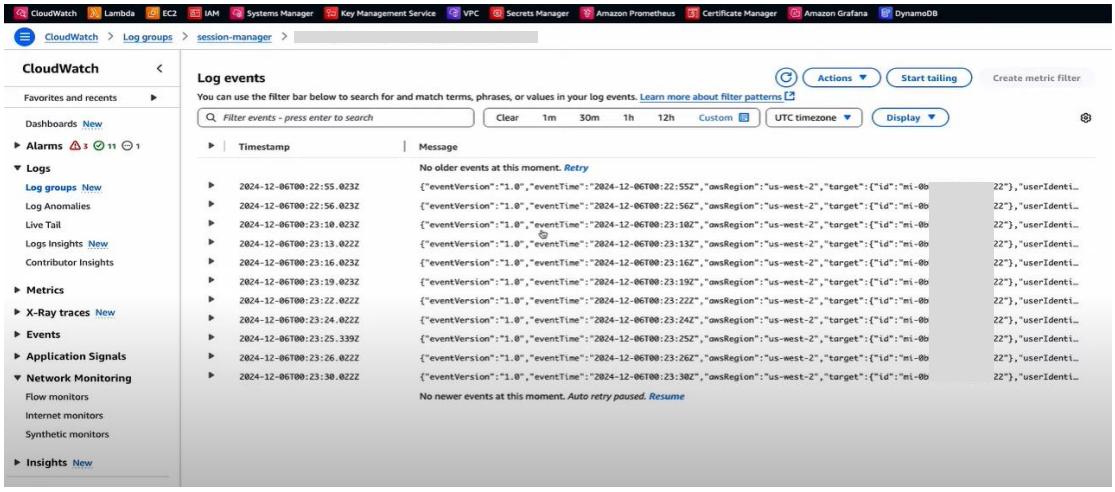

圖 28

在 AWS CloudWatch 服務的 Log events 頁面，會將收集到的操作紀錄，依據時間完整排列，點擊可以呈現完整的紀錄內容。

在 AWS CloudWatch 服務內，有提供網際網路天氣地圖（Internet weather map）的功能，可以呈現世界各地之網際網路供應者是否出現網路連線問題，快速掌握營運現況，如下圖：

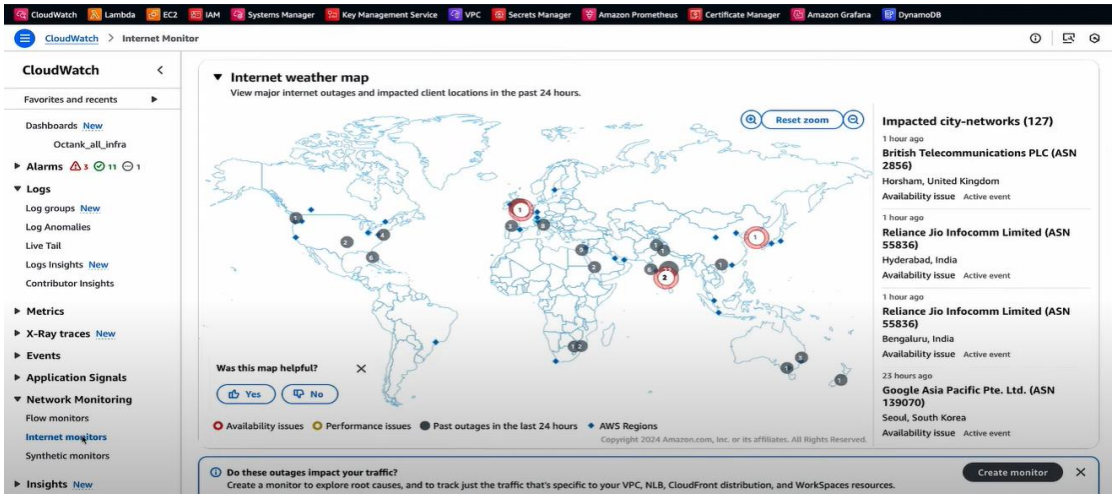

圖 29

在目前產業實務中，每個雲端服務提供者都有自己的儀表板，甚至本地環境也有企業自行開發設計的儀表板，在多雲環境中，可

以使用 AWS CloudWatch 服務，達成整合儀表板的優勢，讓系統管理人員不需要在本地端或其他雲端服務供應者網站之間頻繁切換，提升工作效率，下圖為 AWS CloudWatch 服務之儀表板。

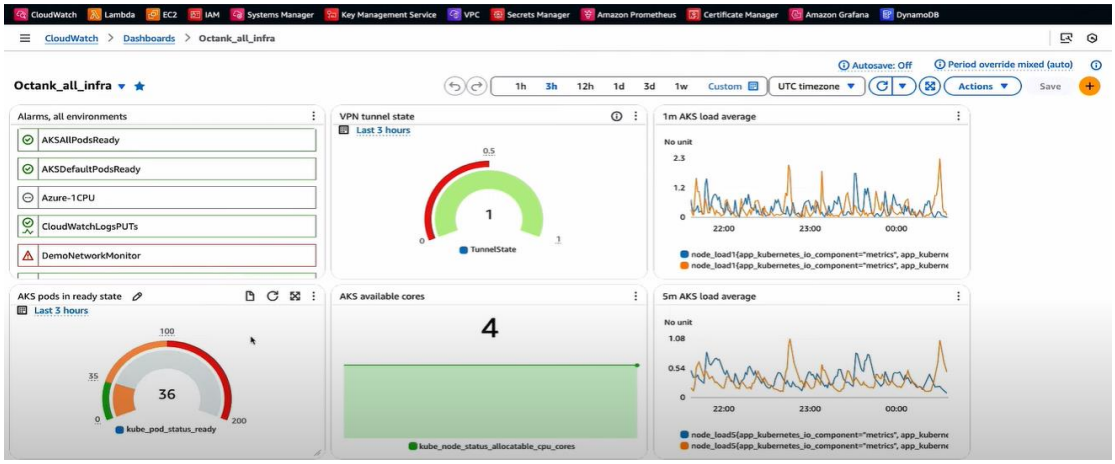

圖 30

透過 AWS CloudWatch 服務的 CloudWatch settings 功能，可以點擊 Create data source 按鈕，建立其他雲端服務供應者作為資料來源。

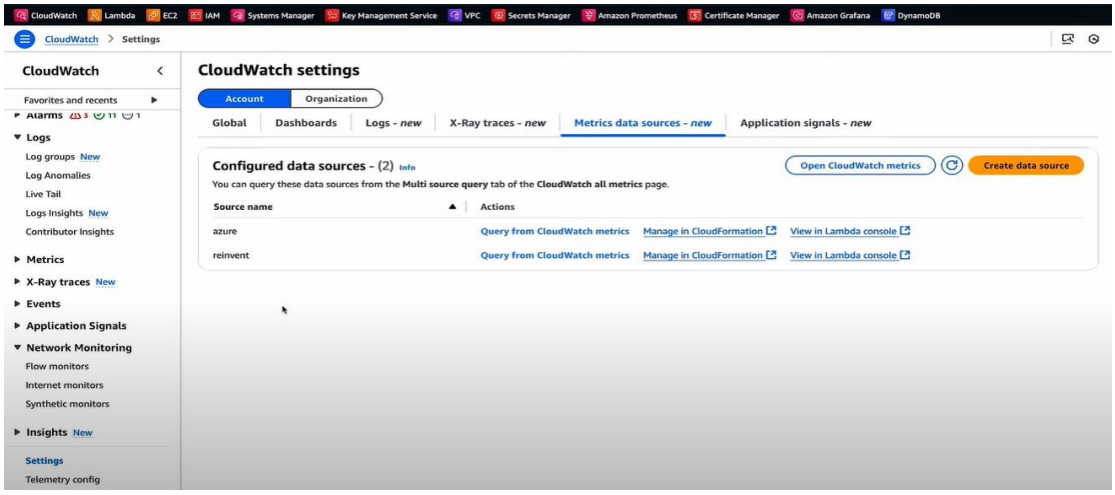

圖 31

下圖為資料來源類型，可以選擇 Azure Monitor 建立監控 Microsoft Azure 的伺服器。

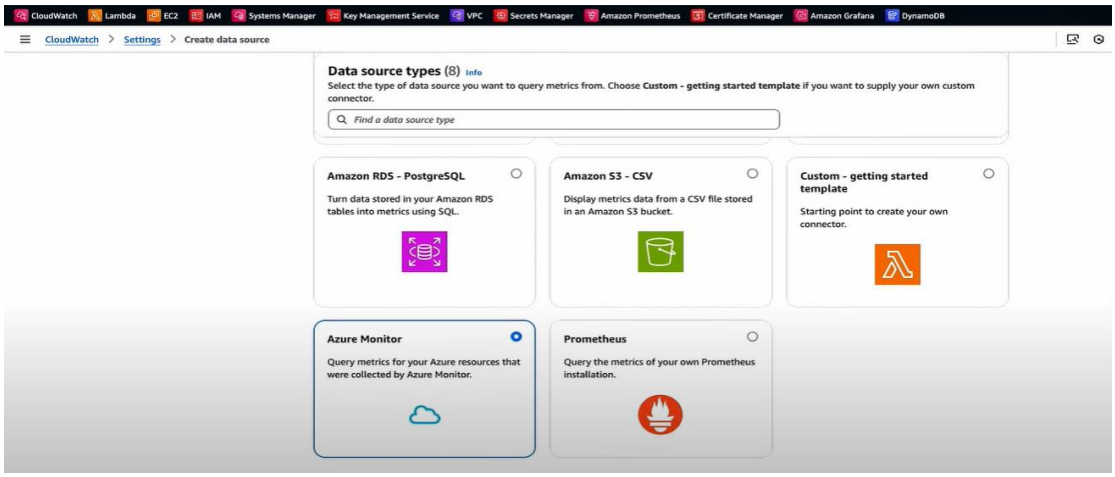

圖 32

在設定 Azure Monitor 資料來源的過程中，輸入 ID 與金鑰，即可設定完成。設定完成之後，可以透過 AWS CloudWatch 的 Metrics 功能頁面，看見來自 Microsoft Azure 伺服器的 CPU 使用率儀表板（如下圖），滿足多雲環境管理的需求。

圖 33

如果想要將資訊服務運作狀態，呈現給業務單位人員或管理階層等非資訊技術人員，AWS CloudWatch 支援整合 Grafana 儀表板工具，可以不需要進入 AWS 控制台，也可以透過瀏覽器呈現資訊服務儀表板。

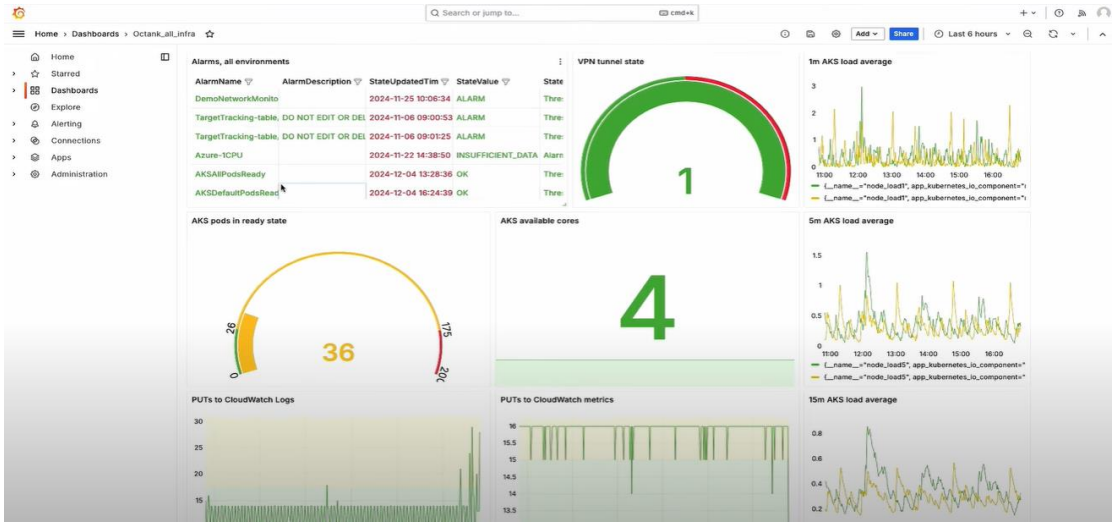

圖 34

在多雲環境的營運管理中，可以透過 AWS Systems Manager 與 AWS CloudWatch 服務，將來自本地端或其他雲端服務供應者的伺服器資訊，快速整合至單一服務儀表板，並且可以執行自動化程序腳本，面對營運非常大量伺服器的混合雲環境，也可以很方便的進行管理，並且可以逐一於所有的伺服器執行，快速進行補丁更新、搜尋特定檔案等，以強化資通安全防護能力，達成多雲環境之雲端治理。

(三) 雲端身分安全

圖 35

在資訊科技快速發展的時代，雲端身分安全（Cloud Identity Security）面臨六大挑戰，分別是：(1) 雲端服務與混合雲環境的爆炸性成長、(2) 缺乏存取權限的視覺化管理工具、(3) 跨系統的權限管理非常多變化且複雜、(4) 過度授權與安全風險、(5) 傳統的身分安全解決方案的缺點、(6) 非人類身分的大量成長。

在「雲端服務與混合雲環境的爆炸性成長」方面，目前業界實務上，通常大多數企業使用的雲端平台不會只有一個，而是會有好多個雲端平台同時運作，而每個不同的雲端平台都在各自儲存資料、管理資料及監控資料，並且有各自不同的安全性及存取權限設定方式。

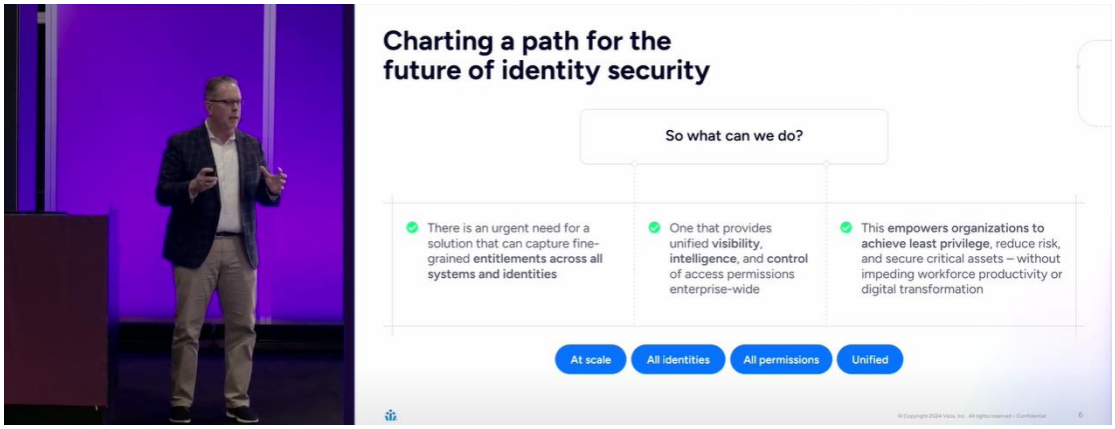

圖 36

在「缺乏存取權限的視覺化管理工具」方面，因為每個業務資料，事實上只有業務單位主管才會了解如何依據資料特性決定存取權限，但是業務單位主管可能並不會知道如何設定 AWS 的存取權限，甚至企業內部可能使用多個各自不同的雲端服務平台，而每個平台的存取權限設定方式都各自不同（例如：AWS 有 107 個存取權限設定、ServiceNow 有 45 個、Snowflake 有 67 個等），只有資訊專業人員能夠懂得雲端服務平台的存取權限功能意義，但是資訊專業人員並不會深入了解資料特性，因此在業界實務上，需要支援跨雲端平台的視覺化智慧管理工具，使得業務單位主管能夠很方便且快速的自行決定每個業務資料的存取權限。

在「跨系統的權限管理非常多變化且複雜」方面，因為每個雲端服務平台的存取權限設定概念、邏輯、功能選項等都不同，並且各家雲端服務為了保持競爭優勢，會持續調整及更新存取權限功能，使得功能操作越來越複雜，因此需要將多個雲端服務平台的存取權限設定方式統一且正規化。

在「過度授權與安全風險」方面，在一家企業中，往往賦予員工太多超過他們執行實際上工作所需要的存取權限，因為為了加快專案推動進度，直接給所有的權限可以更簡單、更方便。專家說明，一般員工通常擁有超過他們工作所需要的 8 至 10 倍的存取權限，存取權限有三個要素：人員、可以存取的物件、可以做到哪些動作。最小權限原則是存取權限的完美目標，但是很少有企業可以真的達成。

在「傳統的身分安全解決方案的缺點」方面，目前市場上有許

多解決方案可以設定哪些人員可以進入哪些雲端平台，但是很少有解決方案可以限制這些人員進入雲端平台之後，可以執行哪些作業，因為身分與存取權限的本質是樹狀結構，建立在目錄、用戶與群組的基礎上運作，對於管理營運很有助益，但是不容易達成最小權限原則。以搭乘飛機為例，在機場內的所有安全檢查都是由美國運輸安全管理局 TSA 負責，但是一旦通過 TSA 的安全檢查，進入機場內部之後，可以選擇哪一架飛機、哪一個座位嗎？或是以入住飯店為例，進入飯店之後，可以進入任何的房間嗎？這是目前大多數身分解決方案的問題，專注於管控進入點的安全性，但是對於允許進入之後的操作行為控制卻相對缺乏。

在「非人類身分的大量成長」方面，目前資訊科技演進方向已經進入到 AI 時代，在企業透過 AI 快速提升工作效率、品質、競爭優勢的同時，也代表外部人員可以透過 AI 自動化的方式發送請求及存取資料，這是存取權限控制領域中的重要挑戰。

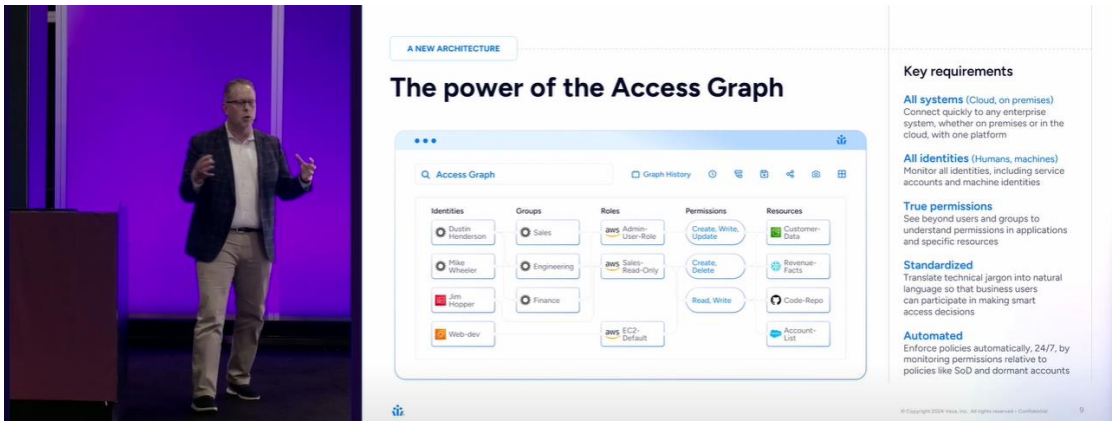

圖 37

專家分享依據他的實務經驗，提出「存取圖」（Access Graph）的資料模型，可以整合身分（Identity）、群組（Group）、角色（Role）、權限（Permission）與資源（Resource）。在存取圖的資料

模型中，是使用圖形資料結構來處理複雜的存取權限關聯，而不是使用傳統的樹狀資料結構或是關聯式資料結構。在企業內的員工，分散隸屬於不同的單位或部門，有各自不同的角色。身分是指每位實際上的人員；群組可以是依據單位或部門來設定群組；角色可以是設定為一定時間內、臨時短期所需要的存取權限，例如可能因為課長需要出差，基層同仁短期內需要擁有代理課長的權限，等到課長出差回來之後，代理課長的角色就會自動解除；權限是指實際上是否可以允許新增、刪除、修改、讀取的權限等；資源是指實際上可以存取哪些業務資料。

實際上一個企業內部可能會有多個資訊系統及雲端服務平台，存取圖是透過 API 連結多個系統及平台，有些可能是近期開發的也有些是舊的系統或平台，新開發的系統或平台通常可以直接使用 API 介接，舊的系統或平台可能要使用其他客製化程式的方式介接，提供統一的視覺化存取權限管理工具。

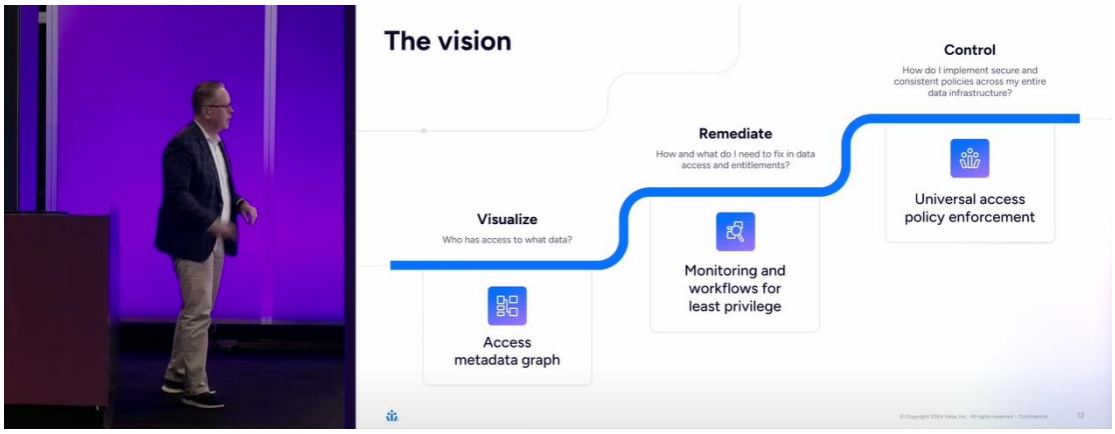

圖 38

有關雲端身分安全的發展方向，首先需要有智慧型且視覺化的存取權限管理工具，並且運用存取圖來知道是誰、可以在哪些時間內、存取哪些資料，接著需要持續監控並且依據業務需求，最好是

可以讓業務單位主管能夠可以直接針對每個業務資料自由的進行存取權限設定，依據最小權限原則設定存取權限，接下來因為企業內部執行業務往往使用多個資訊系統及雲端服務平台，需要橫向且跨系統的統一存取權限控制政策，如此才能做到良好的雲端身分安全治理。

(四) 雲端安全

圖 39

在生成式 AI 快速發展的時代，組織可以靈活運用 AI 快速提升工作效率，駭客也可以運用生成式 AI 快速生成惡意程式碼，提升惡意攻擊的效率，因此對於防禦者，需要學習如何利用生成式 AI 來快速提升防禦速度、能力及效率。

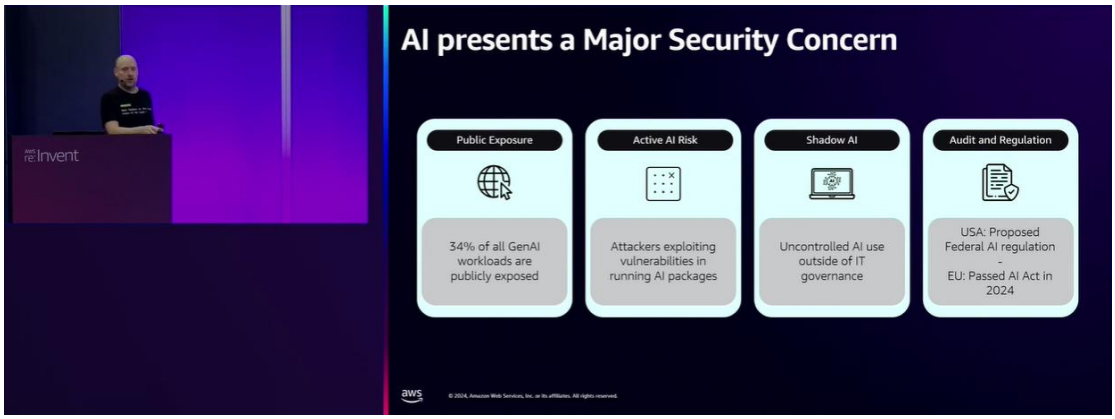

圖 40

在研究雲端工作負載的關鍵安全性問題時，發現有 4 項關鍵問題：(1) 公開暴露、(2) 主動風險、(3) 影子 AI、(4) 法規遵循。

「公開暴露」是指有許多 AI 使用的雲端工作負載是刻意對外公開的，也有些可能是不小心意外暴露在外。

「主動風險」是指駭客可以使用在雲端工作負載中，既有存在的弱點來入侵系統的前端或平台的內部。

「影子 AI」是指有些沒有經過完整授權的 AI 部署，因為沒有被發現也沒有在妥善的管理控制內，而沒有採取必要的安全檢查。

「法規遵循」是指使用 AI 需要符合當地政府的資通安全相關法規。

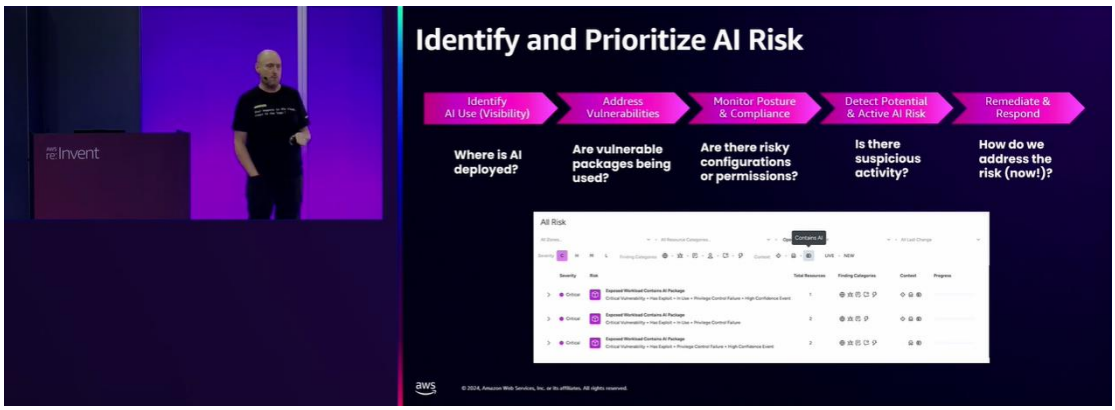

圖 41

為了保護雲端工作負載，有 5 項保護措施：(1) 視覺化、(2) 弱點掃描、(3) 配置管理、(4) 主動威脅偵測、(5) 快速回應。

「視覺化」是指可以利用視覺化智慧管理工具，自動偵測雲端工作負載的部署情形。

「弱點掃描」是指需要定期掃描雲端工作負載的弱點並且快速修補完成，以降低資通安全風險。

「配置管理」是指要可以採用 AWS 雲端工作負載的最佳實務建議，進行雲端資源的配置，以避免設定過多的存取權限，或是資源配置的錯誤。

「主動威脅偵測」是指需要有可以即時監控所有資安相關異常

攻擊活動的威脅偵測工具，例如：可以偵測是否有不明的程式、指令或連線正在執行。

「快速回應」是指需要在發生資安威脅的時候，可以在 10 分鐘之內快速採取行動的能力，以盡量減少對於組織的傷害。

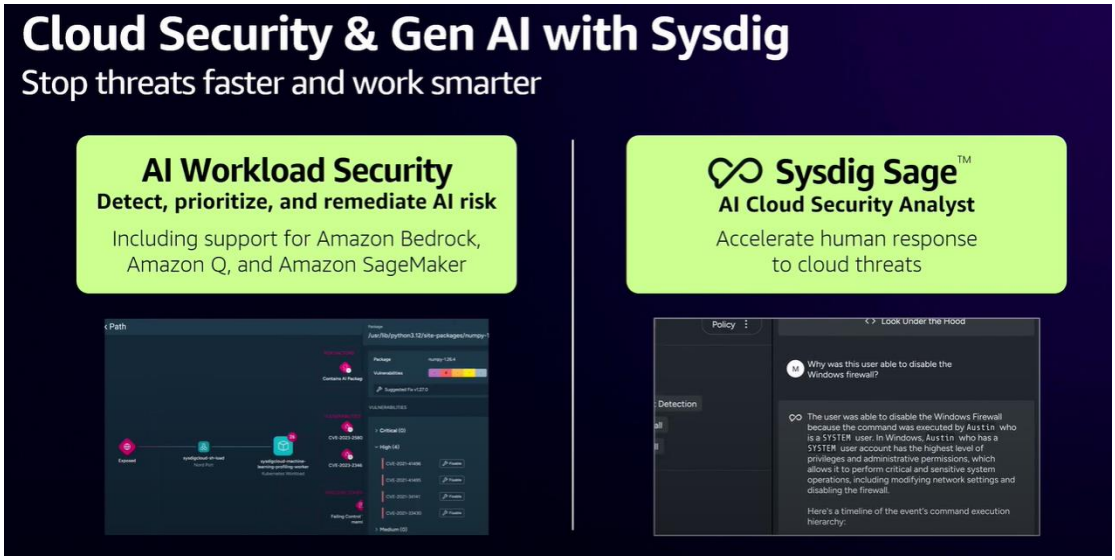

圖 42

使用 AI 可以快速進行攻擊偵測，並且針對攻擊威脅提供資訊人員相關的行動建議，AI 對於資安防護而言越來越重要，可以快速提升防禦能力。透過已經訓練好資安模型的生成式 AI，在快速偵測到攻擊威脅的同時，能夠快速找到關鍵的路徑與漏洞，並且能夠和資安人員進行溝通討論，提供即時指導的功能，協助企業能夠達成提升資安防護、快速防禦及反應能力。

(五) 雲端資料治理

雲端資料治理（Cloud Data Governance）是指在雲端環境中對資料進行管理、保護、監控、分析及確保合規性的一系列策略、流程與技術。隨著越來越多企業將資料存放於雲端，如何確保資料的完整性、安全性和合規性變得尤為重要。雲端資料治理的目的是確保企業在雲端儲存和處理資料時，能夠遵循適當的規範與政策，達到最大化的資料價值同時降低風險。

目前市面上有許多不同的雲端資料平台，每個雲端資料平台都有各自不同的安全模型，對於資料存取的保護方式，通常有三種方式：

(1) 資料表權限：控制使用者可以存取哪些資料表。

(2) 資料列權限：控制使用者可以存取哪些資料列。

(3) 資料欄權限：控制使用者可以存取哪些資料欄，以及欄位資料之遮罩顯示方式。

整理常見的雲端資料平台的安全模型，如下表：

表格 1

雲端資料平台	表	列	欄
Snowflake	提供角色的存取控制，依據角色授權，有繼承功能。	利用 SQL 定義使用者是否可以查詢特定資料列。	提供欄位遮罩功能，依據使用者改變資料顯示方式。

Databricks Unity Catalog	依據角色授權，無繼承功能。	提供資料列過濾功能。	提供欄位遮罩功能。
Amazon Redshift	依據使用者、群組、角色授予存取權限。	提供資料庫端控制使用者可以存取那些列(Row-Level Security)。	提供欄位遮罩功能。
AWS Lake Formation	提供 LF Grants 功能，整合 IAM 依據使用者或角色的存取權限。	提供資料列過濾功能。	提供欄位遮罩功能。

一家企業可能同時營運多個不同的雲端資料平台，在營運管理方面提升複雜度。這位專家提出「政策編排引擎」（Policy Orchestration Engine）的概念，運用人工智慧之資料治理整合軟體，一次性定義存取權限控制政策，自動將控制政策推送到各個不同的資料平台的安全模型，實現跨平台的統一存取控制，不需要處理不同資料平台的差異。

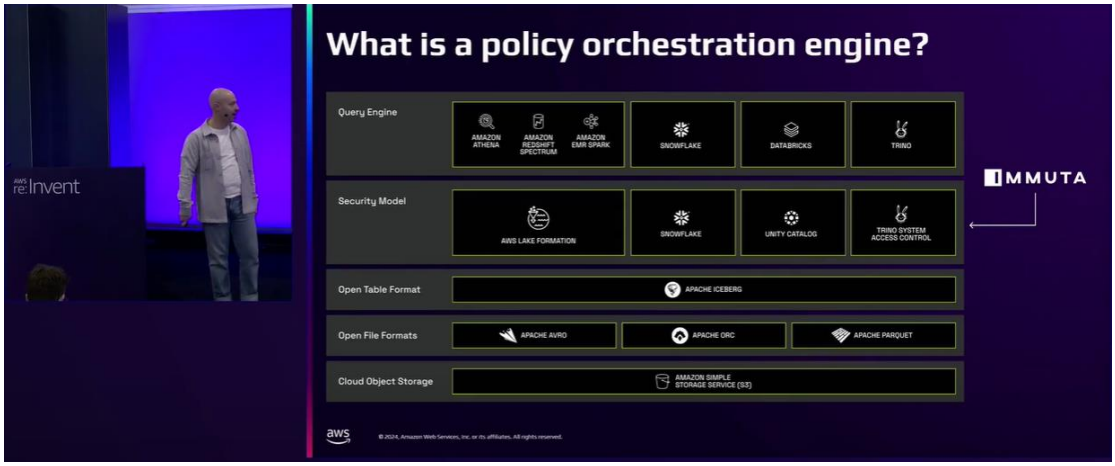

圖 43

利用政策編排引擎，可以達成三項優勢：

(1) 簡化存取權限管理，降低治理複雜度。

(2) 多平台環境的統一存取權限控制解決方案，不需要每個手動設定，避免人為疏失。

(3) 自動依據使用者屬性或資料屬性的改變進行動態更新。

因此在多雲環境或混合雲環境的資料治理，需要考量與建立跨雲端資料平台之統一存取控制方式，可以評估導入資料治理之整合套裝軟體，以降低營運複雜度、自動更新控制措施，達成跨平台之資料一致性與完整性。

三、 心得及建議

首先感謝本公司各位層峰長官的栽培，讓我有這份機會可以出國學習。我平常很少出國，這次是第一次前往美國，對於拓展我的視野以及國際觀很有助益。

圖 44

美國原本就是全球資訊科技、雲端運算與人工智慧發展的中心，在 AWS re:Invent 大會，整個活動會場分散在好幾個超大型飯店的會議室及舞廳等大型空間，活動場地幅員廣大，與會人員眾多，有來自世界上各個不同國家的人們共同以英文交流，更加可以體會匯聚來自世界各地的雲端從業專家，共同聚集在一起互相研討最新技術實務的震撼感。這是以往在台灣不曾有過的體驗，讓我體會到需要有國際觀的視野，不要只侷限在台灣，在資訊科技的專業領域中，要持續提醒自己不斷的跟隨著世界的科技浪潮，持續學習與充實自己的知識與技術能力。

圖 45

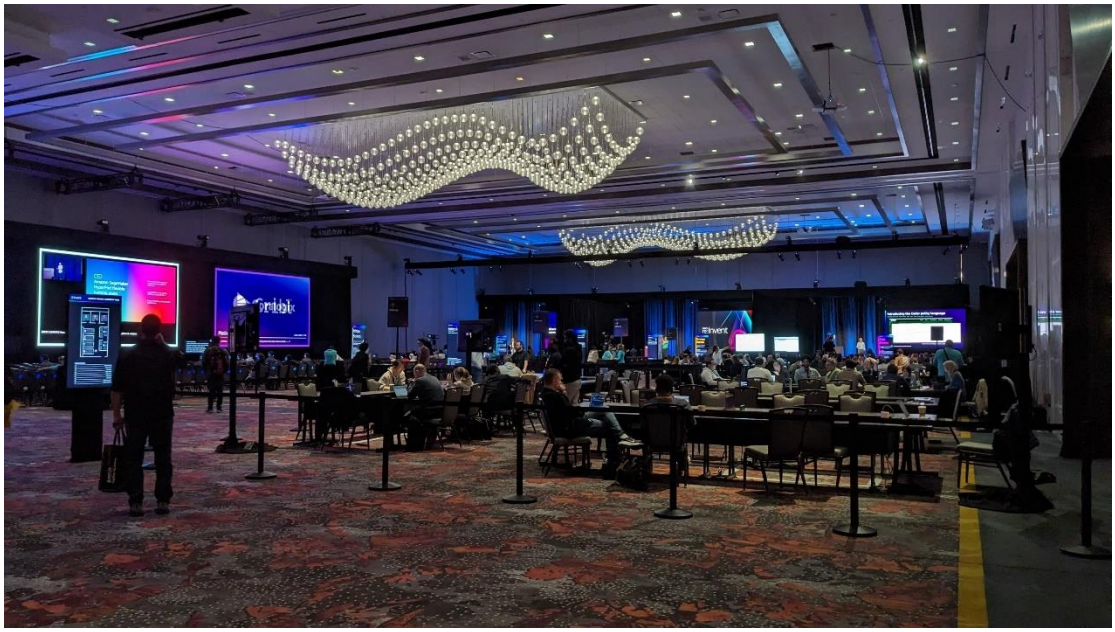

圖 46

在資訊科技的快速發展下，目前人們的生活往往是透過電腦或手機獲得資訊。企業想要行銷獲利、提供產品或服務、拓展市場、提升競爭優勢等，勢必會需要透過擁有自己的網站或 App 來達成，而建立實體資訊設備的成本很高（例如：需要建設機房、採購硬體設備、架設網路、資安防護等）以國營事業來說，如果要採購硬體

設備，需要處理預算、採購、驗收、維護、折舊、稽核等作業，在辦理業務的過程中需要相當多的人力時間與成本，如果可以使用 AWS 雲端服務，則不需要自行採購及維護硬體設備，並且可以達成高可用性（High Availability），使資訊人員只需要專注在開發或維護伺服器及其應用程式，甚至可以使用 AWS 的無伺服器解決方案，只需要專注在應用程式及資料庫即可，可以大幅度的減輕企業的人力成本壓力，並且讓資訊人員可以專注在處理真正重要的工作上，從而提升工作效率與資訊服務品質。

然而在雲端運算快速發展的時代，一間企業往往不只是會使用到一個雲端服務平台，可能同時使用 AWS、Microsoft Azure 與 Google Cloud 等，甚至也有自行建置的本地端私有雲，於是在多雲或混合雲環境中，如何做好雲端治理及資安防護，讓各個不同的公有雲及私有雲，能夠有完整的、統一且正規化的智慧型視覺化管理工具，需要可以讓很熟悉資料特性的業務單位同仁，能夠快速且直接的設定每個資料的存取權限，降低資訊單位同仁不了解業務特性的困境，達成最小權限原則的理想目標，並且提供整合性儀表板，使資訊主管及業務單位同仁可以快速掌控資訊服務的營運現況，提升快速反應及處理能力，變得相當重要。

在多雲或混合雲環境中，伺服器數量眾多且可能分散在本地端或是不同的雲端服務平台，並且通常會設置自動擴展功能，當面臨到效能不足的情形時，可以自動增加伺服器叢集，使得營運管理更加困難與複雜；處理資通安全事件時，可能需要在眾多的伺服器中，統一進行第三方軟體之版本升級或安裝補丁，或是盤點是否存在特定的檔案名稱，如果沒有自動化程序工具，僅靠維護人員手動執行，會相當耗時且沒有效益，難以管理。採用 AWS Systems

Manager 服務，可以在大規模的多雲或混合雲環境，快速修補安全性更新、安全連線及自動化執行客製程序等，並且將資料輸入 AWS CloudWatch 進行監控或是 AWS DynamoDB 資料庫進行後續處理，提升工作效率，強化資安防護，達成良好的雲端治理。

使用公有雲的雲端服務，自然是需要付費的，因此在雲端治理的領域中，需要進行良好的雲端財務管理，來控制成本費用。除了在符合業務目標的前提之下，透過精準有效的運算資源分配，努力降低成本支出之外，在執行雲端工作負載的過程中，也需要隨時監控系統服務，使用搭載人工智慧功能的自動化監控軟體工具，可以自動偵測威脅與惡意攻擊，自動歸納與整理，並且快速提供解決方案的建議，讓系統維護人員能夠快速地反應與處理，提升資訊安全防護能力、工作效率及將惡意攻擊的傷害降到最低；如果雲端工作負載有被惡意攻擊或是忽然發生故障的情形，也可以透過公有雲保障的高可用性，得以快速恢復正常服務運作，達成持續營運的目標。

本公司內部有多個資訊系統，每個資訊系統的開發時期都不一樣，在相當重視資通安全的時代，要能夠培訓資訊人員具備專業的資訊技術、熟悉各系統的存取權限控制措施、培養資安防護的專業技術，做好完善的安全性及達成最小權限原則，同時還要辦理許多採購或行政工作，相當不容易。目前在身分安全與存取權限管控方面，常常是需要針對各個資訊系統進行客製化的設定及處理，如果想要整合身分、群組、角色、權限和資源，是自行開發相關安全機制的話，實際上相當耗時且困難。AWS 作為世界級雲端服務提供者，提供超過 200 種雲端服務，涵蓋各個領域，包含運算、儲存、網路、安全性、資料庫、人工智慧等，在安全性的方面，提供很完

整的使用者身分、群組、角色、權限和資源的存取權限管理功能，並且採用高強度的資安標準，支援將各種雲端服務資源使用標籤進行分類，有完整的存取紀錄可以追蹤所有的使用者操作行為，提供同地與異地備援的高可用性及持續營運能力，採用 AWS 作為雲端服務的解決方案，可以很容易達成各種資通安全管理法規的要求，面對來自上級機關、公司內部及外部的資通安全稽核時，也可以很快速的通過稽核，使得本公司的資訊人員可以減少處理複雜且艱深的技術問題，全心專注在真正重要的業務工作上，追求達成公司的策略與績效目標。

牛頓說：「如果我能看得更遠，那是因為站在巨人的肩膀上。」建議本公司可以將需要動態調整運算資源、達成持續營運、需要符合最高等級資通安全相關規定的資訊系統，評估與考量採用 AWS 雲端服務，因為如果要委外或自行開發，所需要耗費的成本實在相當高，如果直接採用 AWS 雲端服務，AWS 提供既有的各種資通安全服務已相當完整，符合世界級的法規及標準，相當便利。在雲端治理的方面，AWS 作為全球雲端服務的領導者，提供應用人工智慧之自動化雲端治理的解決方案，建議針對 AWS 雲端工作負載需要定期使用 AWS Well-Architected Framework 進行雲端服務架構的審查作業，可以確保在營運、安全性、可靠性、效能、成本、永續發展的方面都可以達到世界級的最佳實務。

四、 參考資料

(一) Cloud Market Growth Stays Strong in Q2 While Amazon, Google and Oracle Nudge Higher

作者：Synergy Research Group

網址：

https://www.srgresearch.com/articles/cloud-market-growth-stays-strong-in-q2-while-amazon-google-and-oracle-nudge-higher