



雲端走向務實

基礎設施在雲端（1）

無限擴充的雲端平台、服務與應用宇宙，已成為業務與 IT 營運的基本要素。但那些令人擔憂的問題該如何處理？

文／Eric Knorr 譯／Nica

雲端不再是某個遙遠又獨立的地方。Amazon、Microsoft 與 Google，在全世界雲端資料中心，維護驚人遼闊的伺服器，成千上萬的SaaS供應商亦是如此。但它們提供的這些雲端與服務，已變得與客戶在地營運息息相關，成為時下近乎所有企業IT財產不可或缺的元素。

這種混合交織的型式很多。對新手而言，Amazon、Microsoft 與 Google可以藉由將託管伺服器機台存放在你資料中心裡的型式，取用它們的部份平台，預先載入啟動相同的公有雲軟體。這些在地雲前哨，有些還能提供存取雲端母艦裡存放的完整服務。

企業資料中心也改變策略，朝向虛擬化、容器化、極度可擴充的雲端模式。以Dell、HPE與Lenovo為例，就提供依使用付費硬體的雲端基礎架構軟體的在地雲產品，超額配置為企業提供隨時增加容量的內部空間。

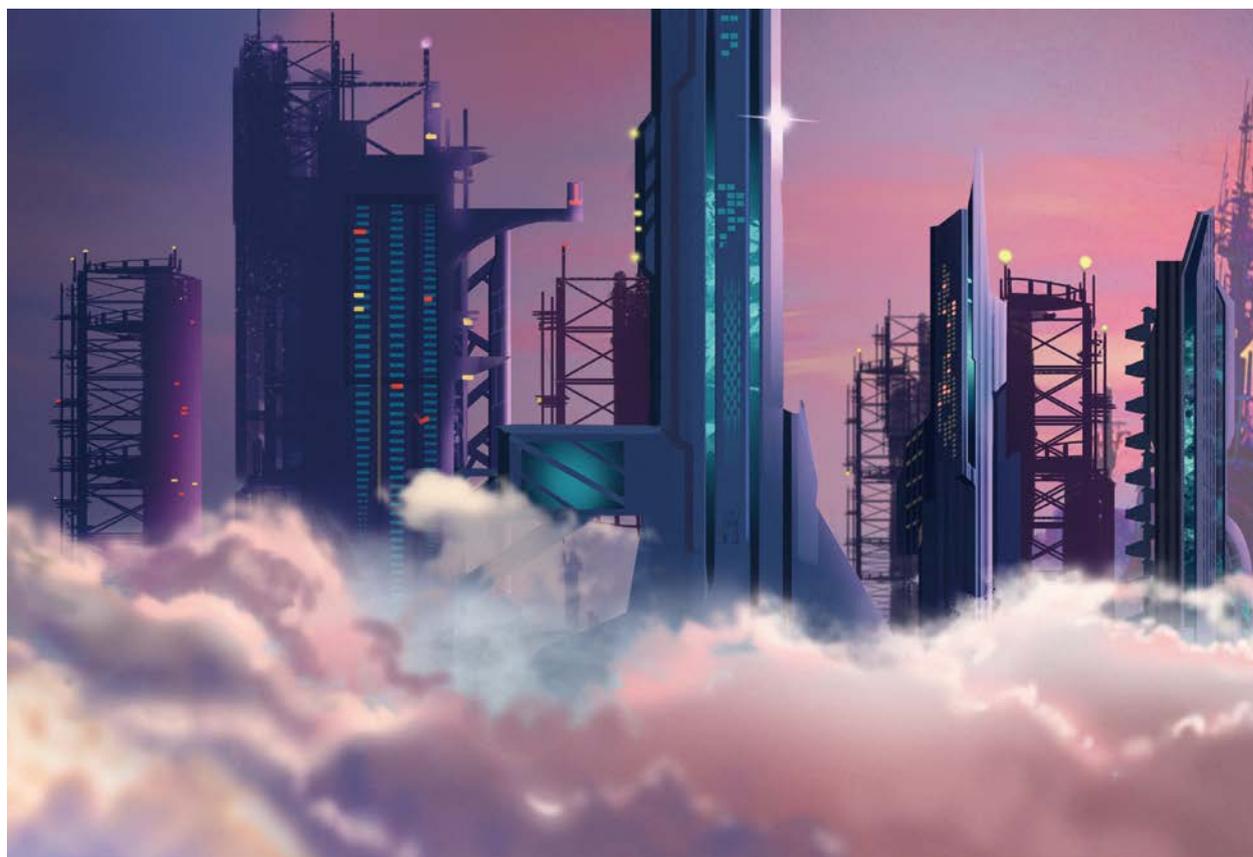
同時，這三大雲端巨擘已著手開展邊際運算，提供迷你雲解決方案，傳遞地理位置堪稱遙遠的交

通樞紐、醫療設備、製造業工廠等等的運算能力與服務，削減雲端延遲。

「混合雲」是在地雲與公有雲無限組合的總稱。本專題我們將深入瞭解混合雲運算的複雜狀況，並將重點放在解決管理這些服務與基礎架構的複雜矩陣所帶來的挑戰。過程中，我們會強調「無法抗拒」的雲端服務：一開始讓雲端三大巨擘如此誘人的那些。這幾篇文章如下：

- 混合雲的重重阻礙如何應對？(CIO)
- 新架構需要新的效能監控工具（Network World）
- 如何解決混合雲的五大資安挑戰（CSO）
- 難以抗拒的十六個雲端革新（InfoWorld）
- 選擇SaaS管理平台（Computerworld）

雲端已成為現代運算模式：敏捷、可擴充、滿是API可用的服務，足以與功能強大、特製應用串接。雲端已不是遠在天邊，它已經成為一切的基礎。



混合雲的重重阻礙如何應對？

基礎設施在雲端（2）

公有雲混搭在地雲火速成為許多企業選擇的架構，但這些企業往往容易落入常見陷阱。

文／Bob Violino 譯／Nica

許多企業正漸漸移往混合世界：無論是新興工作場所模式的混合還是雲端環境。就後者而言，私有與公有雲服務的混合，為企業組織提供在不斷變化的業務環境裡所尋求的靈活性。

2021年八月由研究調查公司Gartner所作的一份報告指出，混合、多重雲端與邊際運算環境「正逐步成長，並為新分散式雲端模式奠定基礎」。該公司預測，終端使用者在公有雲服務的花費將於2021年達3,960億美元，並於2022年成長22%，達到4,820億美元。到了2026年，該公司預測公有雲的花費將超過整體企業IT支出的45%，遠遠超越2021年的少於17%。

同時，也越來越多私有雲的採用。研究調查公司 Global Industry Analysts 預測，提供私有雲服務的全球市場，將從2020年的49億，到2026年攀升到132億美元，在此期間以複合年成長率18%的速度增長。

儘管部份企業可能選擇只用私有雲或只用公有雲，但混合似乎特別吸引絕大多數的公司企業。

「混合雲逐漸成為目前看到所有企業中最具主導地位的架構之一。」顧問諮詢公司 Deloitte Consulting 負責人 Nicholas Merizzi 如此表示。「混合雲讓企業依自有優先順序，彈性訂定通往雲端改革路線。」

顯然，企業組織發現混合雲處理方式的潛在優

勢。不過它們也得做好萬全準備面對可能的阻礙。

以下介紹這些企業可能面臨的一些挑戰，以及該如何克服這些問題。

1. 操作複雜度

Merizzi表示，混合雲基本上就必須維護與管理兩套緊密整合但又各自獨立的生態系統，這就造就了一個複雜的操作環境。

「利用多種相異技術平台平行運作的環境，往往為監控、資安與產品支援這類範疇帶來持續不斷的營運複雜性。」Merizzi表示。確保操作處理程序與工具，在公有雲與在地私有雲皆適用，越來越難。

「舉例來說，雲端資安與『在地』系統，使用的可能是不同的工具套件。」Merizzi表示。同樣地，從這個環境到另一個環境，底層基礎架構從儲存裝置到運算能力也有諸多差異。而且，提升員工處理這些各異工具與環境的技能時，也會有風險與效率的挑戰。

Merizzi表示，要讓複雜度的障礙降到最低，企業組織應注重推動私有與公有雲平台所有技術的通用性。這指的是，擁有可以從在地環境延展到公有雲的工具，同時維持相同的操作體驗。

Deloitte的客戶「正尋求能在所有混合雲環境運作，具可觀察性與點對點應用追蹤的軟體解決方

案。」Merizzi表示。「企業組織必須提升更高的營運能見度，並透過功能強大的儀器量測系統內部狀態。」

堪薩斯州威奇托市正在實行一套更能有效監控該市各種不同IT環境——包括雲端服務的軟體。

「隨著混合網路複雜度大大提升，可用以支援這些狀況的軟體與應用也變得更加精良。」該市資訊長 Michael Mayta 如此表示。「以全球的觀點實施，並『藉由』套用自動化這類的各種技術管理這些網路時，」這可能做得到。

2. 高漲的成本

若企組組織不能謹守管理底層資訊的紀律，同時維護在地私有雲與公有雲環境，可能導致明顯的成本超支。

「許多企業在混合環境下開出兩套帳本，」包括內部私有雲與外部公有雲的財務，Merizzi表示。「部份情況下，團隊甚至使用不同的工具程式評估它們的財務。」他表示。「這導致CIO難以用整合的角度檢視與推測公司財務狀況。」

現代化與操作化系統後，無法關閉或退役在地資產，擴大這項風險，Merizzi表示。「我們看到這些成本超支浮現在許多連結處，包括網路線路與軟體憑證。」他表示。

要減少這類問題，Deloitte建議建置企業級雲端現代化辦公室，著重多個領域：包括財務整合與資產退役。整合多重環境的財務帳本，可提供企業層面的財務概觀，Merizzi表示。同樣地，建立退役處理程序，有助於解放不使用的資產，降低整體花費成本，他表示。

資源管理工具有助於維持成本控制。「沒有統

一、集中的多重雲端管理平台，集團就無法真切感受到他們的成本分析與相關決策，」電腦硬體廠商Lenovo資深副總裁暨CIO Arthur Hu表示。

「我們為使用者提供對資源利用、帳單與開支預測具清楚能見度的成本規劃工具，解決這個問題。」Hu如此表示。「還為這些工具補充智慧型資源最佳化與精簡建議，協助達成最佳成本效益的目標。」

3. 缺乏一致性策略

雲端模式很誘人，許多企業組織可能被佈署公有雲與私有雲所吸引，卻未真正考慮他們希望達到的目標，也未確切規劃如何達成目標。這將可能引發混亂、導致受挫與成本超支。

「好的雲端策略，絕對是從清楚概述昂貴、複雜的混合雲解決方案價值/商業案例開始。」IT研究與諮詢公司 Info-Tech Research Group 雲端與核心基礎架構分析師暨研究調查主管 Jeremy Roberts

表示。

「檢視你的預期收益。」Roberts表示。「為何要混用？看看你的環境。哪些工作負載能從混合架構上獲益？如何獲益？別只是為了想做而做。」

Roberts經手過的一間企業審慎考量過混合佈署。「當我們談過更多企業目標與動能後，得出的結論是它們對管理私有雲沒那麼有興趣，而是傾向於著重SaaS訂閱式軟體優先、多重雲佈署、充分利用多個公有雲而不是公有/私有雲。」他表示。

理由是，就企業組織整體目標來看，同時管理公有雲與私有雲及它們之間的相互操作，所需的額外開銷與努力並不值得，Roberts表示。

「對於法規要求，強制必須在本地（公司內

混合雲的挑戰

1. 操作複雜度。
2. 高漲的成本。
3. 缺乏一致性策略。
4. 改變心態。
5. 缺乏標準或確立的實作。
6. 市場混亂。

部)保有部份資料/工作負載的企業組織來說,情況可能有所不同,又或者企業所需的執行效能只能從當地服務取得、但又希望享有公有雲與私有雲固有特性帶來的優勢。」Roberts表示。

4. 改變心態

Hu表示,就像大部份技術移轉一樣:移往混合雲環境必須克服的最大阻礙之一便是必須改變心態。

「我們必須確保企業相信移轉到混合雲環境的價值。」Hu表示。即便IT部門都必須接受這樣的想法,他表示。「我們必須從本身開始,IT一開始無法完全相信這是正確方向。但很快就改變了。」

Lenovo從經由混合基礎架構,試用部份「lighthouse」應用程式,做為開始,馬上能夠展現明確的價值,Hu表示。「工程部份的產出提升了65%,這歸因於雲端平台與工具程式所啟動的敏捷實作。一旦看見顯著價值,就能順利向企業其餘同仁『鼓吹』,而我們也會持續展現令人驚艷的成果。」

5. 缺乏標準或確立的實作

儘管雲端服務已行之有年,但大規模移往混合雲基礎架構,對多數企業組織而言仍是陌生領域。Hu表示:「因為這對Lenovo而言是全新版圖,我們深知必須為移往雲端建立清楚標準,並提供最佳實作。」

為解決這個問題,該公司發佈了條列清楚的指導方針,說明如何針對私有雲、公有雲或混合雲,選擇正確的雲端代管環境。「我們將這樣的選擇,成為每套應用的企業架構審查的一部份。」Hu如此表示。

該公司還制定「5-R遷移處理(5-R Migration Approach)」,協助應用擁有者依應用程式現有架構狀態為基礎,確認最佳路徑。內容包括重新代管(rehost,直接重新佈署到雲端)、重構(refactor,修改架構適應雲端)、修訂(revise,在不動架構前提下修改或延展現有程式碼)、重建(rebuild,拋棄現有技術,從頭開始開發),或者替換

(replace,現有應用退役,採用替代解決方案)。

此外,Lenovo還開發應用級最佳實作供集團參考,Hu如此表示。

6. 市場混亂

「廠商的選擇與管理,乃當代企業移往混合雲最棘手的項目之一。」研究調查公司IDC的專用暨混合雲基礎架構研發總監Chris Kanaracus如此表示。

「因為選擇很多雖然是好事,但雜訊比持續飆高。」Kanaracus表示。「我們擁有公認領導性超大規模的AWS、Microsoft與Google。但像Oracle這樣的新秀,在成本與功能上的積極作為,正逐步擴大市佔率。」

其他像Cisco、VMware、HPE與IBM這類選擇,則是「轉向混合雲市場。」Kanaracus表示。「他們發現了提供在地雲與混合雲邊緣元件,與超大規模三巨頭協同合作的機會。但超大規模三巨頭也想要這樣的商機,AWS Outposts、Azure Stack與Google Anthos即為證明。」

再者,電信業者與代管服務廠商逐漸走向整合,Kanaracus表示。「從CIO的角度來看,就有相當多要構思與管理的不地方了。成本監控與管理已成為混合雲的關鍵,未來要處理的層面只會更廣。無論大型小型的眾多廠商都渴望參與。CIO的選擇很多,因此可能引發混亂、造成失誤。在這個領域上的投資嚴陣以待非常重要。」

新架構需要新的效能監控工具

基礎設施在雲端 (3)

從多重網路的多個裝置提取效能資料的平台，有助於提升混合雲執行效能與修復問題。

文／Ann Bednarz 譯／Nica

隨著公司企業將更多工作放在雲端上，網路團隊發現雲端能見度不等同於企業在地資源所能達到的程度，網路效能監控現在變得更複雜了。

遷移至雲端，採用非企業所有的基礎架構，且大規模流行病引發遠端工作的強烈需求，加速了移往雲端的動作，相關的非在地環境也增加了。佈署在雲端原生基礎架構上、以容器為基礎的應用，進一步提升網路能見度的複雜性。基於這些理由，企業需要能夠監控的工具程式：不只是監控資料中心與廣域網路（WAN），還包括網際網路、SaaS應用與眾多供應商的公有雲操作。

「僅36%網路營運專家深信，他們的網路管理工具能夠做到像管理在地網路那樣管理雲端網路。」Enterprise Management Associates (EMA) 研發副總裁 Shamus McGillicuddy 表示。「同時，一般企業將40%的網路流量歸類在雲端。這是極大的劣勢。」

這種顯見的鴻溝是如何產生的？當企業開始將工作負載佈署到雲端上，網路團隊通常處於觀望。

「問題之一就在於，網路基礎架構團隊在雲端環境中不見得擁有在地網路上相同的授權。」McGillicuddy表示。「多數時候，採用雲端是由應用團隊或業務線所主導，他們視雲端為IT的替代品，沒有必要擴展。」

「雲端中擁有較多授權的團隊，不見得認為網

路監控是重要的事。他們對應用程式的執行效能監控更有興趣。」McGillicuddy表示。「他們認為舊時代基礎建設監控這種事，不值得投入預算。」

公司企業如何看待雲端中網路工程師的角色，會讓一切變得不同，網路能見度暨效能管理廠商 Kentik 產品經理 Dan Rohan 如此表示。

「在我們開始探討關於監控雲端的前兩三年，我不認為有太多網路工程師關心這一點，」Rohan 表示。隨著雲端佈署漸趨成熟，公司企業已越來越難瞭解雲端成本、效能與控制，它們體認到必須將部份架構回復原狀，此時突然，網路工程師又能再度發揮所長了。

當今網路效能管理工具能作什麼

典型雲端廠商網路極度複雜。「穿越你的ISP到雲端廠商之間可能得跳過15個網路節點（hop）並非特例，可能先是本地電信營運商，接著再來可能是第一級電信營運商。之後還要再通過雲端供應商裡的另外30個網路節點。」AppNeta總裁暨執行長 Matt Stevens 如此表示。「總共十幾二十個網路節點的日子如今已暴增到四、五十個 Layer 3 網路節點。每個節點都做點事拖慢你的效能。」

網路複雜度與日俱增，潛在問題亦然，Stevens 表示。「當你有許多員工執行著眾多應用，而這些應用被代管在許多來源位置，無論那是私有的資料

中心、企業組織試圖像雲端那樣運作的虛擬資料中心、完全公有雲，還是某些介於這之間的东西——混用IT終極定義，每增加一個變數，複雜度就會『呈指數型』增長。」

網路團隊轉向廠商求助。據EMA指出，有57%的網路團隊得到專屬工具程式，終結雲端——網路間能見度的鴻溝。

該研究調查公司預期，提供雲端監控的網路效能管理工具透過以下方式結合：

- 收集佈署在雲端中虛擬網路元素的指標。
- 收集由雲端廠商提供的流量事件記錄檔與其他遠距測量數據。
- 收集雲端中封包流量這類網路流量資料。
- 分析針對SaaS服務的合成網路流量。

傳統網路管理工具被設計成監控資料中心或企業內部網路中，路由器與交換器的健全狀態，但雲端帶來不同的挑戰，Rohan表示。「網路工程師的腦袋裡沒有『雲端基礎架構』的思維，因為雲端成長太快、而且也不是由他們所建置，它一直都是個挑戰，因為它是雲端。因此，網路工程師們就是從諸如此類的障礙做為起點。」

他們需要不同的工具解決這些突然冒出來的問題：應用程式團隊無法讓新的雲端應用與企業在地資料庫溝通，或與另一個雲端應用整合，諸如此類。

「網路團隊只能開始使用這些只是從 AWS API 或其中一個雲端廠商API撈資料的工具。」而這並不能告訴我連結失敗。也不能告訴我為何事情無法正常運作。Rohan說道：「所以從這裡開始：我們認為，在這個雲端時代，對網路人真正有幫助的是協助回答這些橫跨複雜網路拓撲的連結性問題。」

Kentik的工具，為網路工程師提供當下網路狀況，「他們所接手的事務。」Rohan表示。「這麼做有助於工程師視覺化網路的流動：好的和壞的。然後便可以說：『好，若我們在這安裝中繼閘道器，接著在這配對連結…』，工程師以自己的網路技術，確實利用我們的工具，讓網路獲得控制。」

雲端能見度的網路指標

遠端遙測資料可揭示混用雲狀態，包括來自各種網路：資料中心、WAN、網際網路、雲端、行動網路、邊界網路，以及各類網路元件：實體與虛擬設備及專屬或雲端原生裝置的所有資料。

資料來自資料中心元件、雲端基礎架構（例如服務網格、傳輸閘道與入口閘道）、網際網路基礎架構、校區裝置、傳統WAN路由器與交換器、SD-WAN閘道器與物聯網終端等等。遠端遙測型態則含括網路裝置（NetFlow、J-Flow、sFlow、IETF的IPFIX這類流量收集通用標準）、雲端廠商虛擬私有雲流量事件記錄、SNMP式裝置遙測，以及經由syslog 或 SNMP trap 傳送的事件通知等等，所輸出的流量資料。

EMA指出，除了網路流量與封包這類被動監控資料外，網路團隊漸漸轉向利用主動監控技術，例如基本的ping測試與第七級合成監測，提升傳統基礎架構與流量封包監控指標。該研究調查公司發現，有21%網路團隊正利用合成流量封包工具，進行持續的網路可用性與效能監測。

這並非是指公司企業之前沒有監控這些網路與設備，而是，目標在於提供含括各式網路協調一致的監控、對報告結果的整合檢視，以及能夠以自動化流程的方式整合分析結果。工具化正超越核心基礎架構監控，提供更貼近應用層級的檢視，以及對終端使用者體驗應用執行效能的瞭解。

誰銷售網路效能管理工具？

網路執行效能管理的產品佈局相當齊全。廠商包括Accedian、AppNeta、Cisco-ThousandEyes、cPacket Networks、Kentik、LogicMonitor、ManageEngine、Riverbed與SolarWinds。EMA發現，沒有一家廠商可以含括所有要項，大部份工具都是互補而非競爭，典型IT組織會利用到四至十項工具，進行網路監控與問題修復。

研究調查公司Gartner在其網路效能監控市場指南（Market Guide for Network Performance Monitoring）中表示，對在地環境而言理想的工具，

隨著企業組織增加混用程度而越來越沒有效率。即便有些廠商能夠提供橫跨在地與雲端環境兩者的能見度，但因資料傳輸需求與網路差異之故，這仍然深具挑戰，因為它們無法都透過相同的角度檢視，Gartner表示。

根據針對尋求網路效能管理工具的企業所提出的建議中，Gartner建議公司企業應「放棄在雲端中使用與在地環境相同監控處理方式的念頭，尤其是封包擷取與分析的部份。專注在提供API或實際網路流量資料這類雲端原生功能支援的廠商。」

人工智慧協助網路問題修復

需要分析的遠端遙測資料永遠不缺。現代網路監控工具的差別在於能夠權衡效能，將發現結果置於有前因後果的環境下，回答網路團隊的提問。

「轉向混用雲，問題其實不在於『它能不能運作？功能是好的還是壞的？』現在是：『慢』即為新的『壞』」AppNeta的Stevens表示。例如，使用者不會打電話表示無法連結到Salesforce。他們會抱怨Salesforce裡的script跑太慢，影響他們的工作能力。

他表示，「無論佈署何種架構，我們都要為企業組織提供可供瞭解的能見度。『這是我要的效能。這是我得到的效能。這之間差異太大所以必須採取行動，還是可以將它暫放一邊，先處理其他問題？』」

這就是人工智慧派上用場的地方。有越來越多工具支援以人工智慧為基礎的分析，這是為找出網路資料模式所設計，從中依過去的異常偵測與根本原因分析導出結論。

「我們不只要告訴你有問題，還要讓你知道哪裡有問題。知道何以如此，提供補救的建議，還能提供信心指數」，也就是提議的補救措施是否有用的量化數字，Stevens表示。

擁有可以讓網路團隊賴以瞭解問題，並為補救措施排列優先順序的工具，可以讓IT在企業進行重大業務改革專案之際擁有可信度，Stevens表示。

「這是牽涉很多人的大型專案，IT受邀成為業務夥伴。」

在職涯中與網路廠商與企業IT網路合作超過

三十年的資深系統網路工程師 Scott Bulger，已在兩間大型企業中使用AppNeta技術至少三年。

Bulger表示：「雲端基礎架構的能見度最低，所以能夠追蹤點對點封包漏失、抖動【譯註：語音封包規律性】與延遲、進入服務供應商雲端再回來的能力，可為你提供自主權與告知雲端供應商「我們有封包漏失」的正確性。你會證據確鑿，無可辯駁。」

Bulger最在意的指標是封包漏失。以TCP/IP為基礎的網路設計上就是容許漏失，「但有個臨界點：大概4%或5%，視拓撲而定，在那個點上漏失開始會被注意到，而且會影響終端使用者。所以，些許漏失是可接受的，但重大漏失，或長期時間損耗，就會有影響。」他表示。

整體而言，網路能見度工具，不僅有助於識別問題，還能全然避免效能問題。「這些平台，能在問題影響客戶前，讓你看見問題。」Bulger表示。

不過，從被動轉為主動態度並不容易。「若你的DevOps或客戶服務模式光支援立即性問題就已飽合，你很難有足夠的立場告訴他們：『這裡有地方出了點問題，但若我們不做點什麼，它的問題會更大。』」Bulger表示。

他表示：「我們需要一個將主動補救措施放在首要位置的企業文化。經理人要全然接受這樣的想法並毫不猶豫投入資金。」

如何解決混合雲的五大資安挑戰

基礎設施在雲端(4)

混合雲環境不僅提升資安團隊複雜度、降低能見度，還需要採用不同的事件紀錄與監控處理方式。

文／Bob Violino 譯／Nica

對越來越多的企業組織而言，IT環境已包括公有雲服務、私有雲與在地自建的混合基礎架構，而後者在混用環境裡所佔比例越來越低。

過去兩年，雲端服務使用激增，這樣的趨勢沒有減緩的徵兆。2021年四月由研究調查公司Gartner所作的預測指出，全球在公有雲服務上的花費，2022年將成長23%。

報告指出，容器化、虛擬化與邊緣運算這類新興技術，將更接近主流並刺激雲端支出。SaaS訂閱式軟體仍保有最大市場區隔。

企業選擇混用滿足企業目標，而不是只佈署一種雲端服務。混合雲端模式可為企業營運帶來絕佳彈性。企業可依需求上下調整容量，可以在大量雲端服務上移進移出資料與工作負載。混合雲也帶來網路資安風險：擱置不處理將引發重大損失。

本文將介紹資安主管與團隊在處理混合雲模式將面臨的五大挑戰，並說明如何解決。

一、複雜度增加、能見度減少

隨著企業佈署更多公有雲服務並增加私有雲能力，從管理與資安角度來看，企業IT環境更加複雜了。若不採取行動監控服務的使用狀況，企業無法瞭解這個環境下發生的一切。

「混合雲環境自然引發更多複雜度，它就是有這麼多『門窗』要鎖上、有更多安全性維護 — 修補

程式等等要實施。」研究調查公司International Data Corp. (IDC)專用暨混合雲基礎架構/服務研發主管Chris Kanaracus表示。「我們見過太多『像是』公有雲儲存容器設定不當的人為失誤引發資料外洩，而受到高度矚目的媒體故事。」

定義標準、認證與最佳實作，協助保障雲端運算環境安全的雲端安全性聯盟(CSA)便舉出：不當組態與不適切的變更管控，加上有限的雲端使用能見度，已成為2020年雲端運算的頭號威脅。

大量雲端服務意謂著企業組織處理安全性的方式需要改變。「雖然選擇混合雲環境為企業組織帶來選擇與彈性，但這也代表IT領導者必須重新評估安全性實作，研究必須如何調整。」線上數據搜尋工具Elastic的CISO Mandy Address如此表示。「你無法保護看不到的東西」這句話在混合雲架構上尤其適用。「混合公有與私有雲或基礎架構，會增加複雜度、提高企業風險。」取得能見度與控制，對保障分散式系統安全而言，至關重要。

二、知識與技術的鴻溝

已有充份數據資料證明網路資安技能嚴重短缺。許多企業組織苦於尋找填補各種角色的人才，但確認並雇用對雲端也瞭解的安全性專家，又是另一項全然不同的挑戰。這種雲端資安知識差距，可能令企業面臨風險，必須在為時已晚前找到方法填

補缺口。

方式之一就是提供內外部訓練。諮詢顧問公司Deloitte風險與財務諮詢網路雲端主管暨負責人Vikram Kunchala表示，在業務線、網路領導者與團隊、培訓與人力資源間，協調一致的處理方式，開發課程與多型態訓練方式，持續提升可支援複雜混合雲環境的技能。

重點在於，許多非技術型企業與非雲端服務廠商，也在競爭相同雲端人才資源，Kunchala表示。「因此，僱用人才是項挑戰，『企業』不應僅仰賴這個選項。開發訓練課程，讓現有員工提升技能或取得全面技能，可以在這方面有所幫助。」

強而有力的治理是混合雲環境另一項關鍵，Kunchala表示。具備定義完善的職責基準與營運模式能減輕疑慮，實現有效管理。「監控指標，可以為各個資安團隊效能與控制實施的有效性提供能見度。」

CISO與其他資安領導者「必須考量人力資源與技能使用的效率。」Andress表示。「混合雲環境下，資安團隊可能必須學習兩個或兩個以上的雲端服務資安功能。」

三、資安責任移轉

環繞著邊界安全性、基礎架構與虛擬化的管控責任，移轉到公有雲體系裡的雲端廠商，因此瞭解資安共享責任模式的改變非常重要，Kunchala表示。

「企業組織試圖將私有雲控制與技術堆疊擴展至公有雲，這種作法在某些情況下行不通。」他表示。「沒有清楚定義混合雲系統下的『職責安排基準』與/或操作模式，等於留下空間給未緩解威脅與未處理功能，阻礙企業組織擴展與滿足營運目標。」

儘管瞭解與遵循因使用雲端服務而來的共享職責模式很重要，但並非所有企業都這麼做。「公有雲公司使用的共享職責模式，是許多企業仍設法努力謹記在心的事。」Kanaracus表示。

四、網路保護配置不當

網路安全是企業組織不斷受到質疑的重點領域，因為廠商支援私有雲的現有工具，在公有雲上

可能不適用，Kunchala表示。「企業組織利用容器順利在混合雲裡轉換與管理，但並未充份瞭解服務網格與API安全性這類細微差異『可能』導致容器可能感染，進而遭到不當利用。」

大部份以公有雲為基礎的資安工具廠商會支援私有雲環境，Kunchala表示。「但傳統廠商專為企業在地私有雲所建置的工具程式，可能就無法擴展或提供針對公有雲的完整功能。」他表示。「廠商分析很重要，而且應該將完整需求與所有已確認方案執行一遍。」

五、分散的事件紀錄與監控功能

在混合雲環境下，事件記錄來源散佈在整個企業內部自建系統、公有雲系統、廠商工具與雲端原生服務，Kunchala表示。「識別事件記錄遠端遙控『並』建置監控指標是關鍵。」企業需要有針對營運與功能級別的關鍵績效指標(KPIs)，以及向執行層報告的關鍵風險指標(KRIs)，他表示。

「然而，事件記錄與監控功能的成熟需要一至兩年的時間，必須採取許多執行步驟與處理事件記錄的工具，進而為多重來源建立關係，得出定義指標。」Kunchala表示。終極目標是依執行高層所需，開發客製化報告控制面板，協助高層瞭解雲端服務的殘留風險與影響，他表示。同時，營運團隊也能獲得全面性的進階持續性威脅完整能見度。

難以抗拒的十六個雲端革新

基礎設施在雲端(5)

實支實付訂價模式背後，是公有雲充滿了最新穎、最優異的開發、devops，以及更快建置更聰明應用的人工智慧工具。

文／Martin Heller 譯／Nica

講到公有雲，通常首先想到財務：將工作負載從近乎飽容量的資料中心，移往雲端，可降低資本支出(CapEx)，但會增加營運支出(OpEx)。這點可能吸引CFO，也可能不，但開發人員、營運人員或兩者結合的devops(開發營運)，絕對感興趣。

對他們來說，雲端運算提供的許多機會，是必須購買新伺服器硬體才能得到的新軟體或企業級軟體套件無法提供的。必須花六個月在企業內部佈署在雲端有時只需十分鐘。必須通過重重管理階層簽署才能建置的企業內部服務，在雲端用信用卡消費就能完成。

不只是時間與便利性問題。雲端還能做到更高效的軟體開發，通常這代表更快切入市場。雲端也能進行更多實驗，讓軟體品質更好。

再者，雲端真正的革新是能提供即時性優勢進而解決企業內部運算長期以來的問題。本文將介紹十六項極具競爭力的雲端功能。

01. 依需用運算實例

需要在企業內部自有伺服器裡建置新資料庫？你得先排隊，再花上幾個月準備，或是幾年。若你可以容忍在企業內部的虛擬機器(VM)，不用實體伺服器，可以使用VMware或類似技術，可能只需等待幾個禮拜。不過若想在公有雲建立伺服器實例，花十五分鐘就可以備妥馬上運作、依需求調整大小，

之後在不需要使用的時候關閉。

02. 預建虛擬機器映像檔

能載入你選定作業系統的虛擬機器是很方便的，不過接著還是必須安裝與授權所需的應用程式。能載入你所選定的作業系統與應用程式皆已備妥的虛擬機器，是無價的。

03. 無伺服器服務

「無伺服器」代表一項服務或一段程式碼，依需求短暫執行，通常是為了回應某個事件，不需要運作在專屬VM下。若服務屬於無伺服器，通常就不需要擔心底層伺服器，由雲端供應商維護的資源池指派資源。

今日每家主流公有雲皆提供無伺服器服務，通常會具備自動擴充、內建高可用性與依價值付費(pay-for-value)帳單模式的功能。若想要無伺服器應用但不想鎖定任何特定公有雲，可使用Kubeless這類廠商原生無伺服器框架，需要的只有Kubernetes叢集。

04. 依需用容器

容器，是輕量級的可執行軟體元件，比虛擬機器精簡許多。容器將應用程式碼與函式庫這類相依性元素打包，共享主機機器的作業系統核心，可以

十六項極具競爭力的雲端功能：

01. 依需使用運算實例
02. 預建虛擬機器映像檔
03. 無伺服器服務
04. 依需使用容器
05. 預建容器映像檔
06. Kubernetes 容器編排
07. 自動擴充伺服器
08. 行星級資料庫
09. 混合服務
10. 可擴充機器學習訓練與預測
11. 雲端 GPUs、TPUs 與 FPGAs
12. 預訓練人工智慧服務
13. 客製化人工智慧服務
14. 監控服務
15. 分散式服務
16. 邊緣運算

在 Docker Engine 或 Kubernetes 服務上執行。依需執行容器具備依需執行虛擬機器所有優勢，所需資源更少而且成本更低。

05. 預建容器映像檔

Docker 容器是 Docker 映像檔的可執行實例，由 Dockerfile 指定。Dockerfile 的內容包含建置映像檔的指令，且通常以另一個映像檔為基礎。例如，內容含有 Apache HTTP Server 的映像檔可能是以 Ubuntu 映像檔為基礎。你可以在 Docker 登錄裡尋找預先定義的 Dockerfiles，再建立自己專屬的。可以在本機安裝的 Docker 下執行 Docker 映像檔，或在任何支援容器的雲端執行。有了預先建置的虛擬機器映像檔，就能

使用 Dockerfile 快速啟動完整應用，不同於虛擬機器映像檔的是，Dockerfiles 具有廠商中立性 (vendor-agnostic)。

06. Kubernetes 容器編排

Kubernetes (K8s) 是一套容器化應用的自動佈署、擴充與管理的開放源碼系統。K8s 以 Google 內部「Borg」技術為基礎。K8s 叢集由稱為節點 (node) 的工作機器組成，執行容器化的應用。工作節點託管內含應用的 pod，控制面板管理工作節點與 pod。K8s 在任何地方都能執行且無限擴展。所有主流公有雲皆提供 k8s 服務，也可以在自有的開發主機上執行。

07. 自動擴充伺服器

不需要容器化你的應用，然後在 Kubernetes 下執行它們以便在雲端裡自動擴充。多數公有雲都允許自動擴充虛擬機器，並依使用量啟動 (停用) 服務：增/減實例或擴大/縮減實

例大小。

08. 行星級資料庫

主要公有雲與多間資料庫廠商皆實施全球級分散資料庫，這些資料庫擁有能讓作業更有效率的資料結構、冗餘互連與分散式共識演算法，並達到五個九的可靠度 (99.999% 正常運作時間)。雲端特定的例子有 Google Cloud Spanner (關聯式)、Azure Cosmos DB (多重模式)、Amazon DynamoDB (鍵值與文檔模式)、Amazon Aurora (關聯式)。廠商的例子則包括 CockroachDB (關聯式)、PlanetScale (關聯式)、Fauna (關聯式/無伺服器)、Neo4j (圖形)、MongoDB (文檔模式)、DataStax Astra

(列儲存)與Couchbase Cloud(文檔模式)。

09. 混合服務

已在資料中心大量投資的企業，通常希望將現有應用與服務延展到雲端上，而不是用雲端服務取代。所有主要雲端廠商如今都有提供達成此目標的處理：無論是利用特定混合服務(例如跨越資料中心與雲端的資料庫)，還是連結公有雲的企業內部伺服器與邊緣雲端資源，通常稱混合雲。

10. 可擴充機器學習訓練與預測

機器學習訓練，尤其是深度學習，通常需要使用長達數小時至數周的可觀運算資源。此外，每次機器學習預測則需使用數秒的運算資源，除非進行大量批次預測。一般來說，利用雲端資源會是完成模組訓練與預測最便利的方式。

11. 雲端GPU、TPUs與FPGAs

精準訓練需要使用大量模組與大型資料庫的深度學習，通常使用CPU叢集往往需要一周以上。GPU、TPUs與FPGAs可以大量縮減訓練時間，並且將它們放在雲端上，有需要時便能輕鬆取用。

12. 預訓練人工智慧服務

許多人工智慧服務利用預先訓練模組順利運作，例如語言轉換、文字轉語音與圖形識別。所有主要雲端服務皆提供以穩健模式預先訓練的人工智慧服務。

13. 客製化人工智慧服務

預先訓練人工智慧服務在某些情況下無法確切達到你的需求。遷移學習僅訓練現有模式頂層少數神經網路層，可提供比從頭訓練模組相對快速的客製化服務。當然，所有主要雲端服務廠商皆提供遷移學習，只是名稱有所不同。

14. 監控服務

所有雲端都支援至少一項監控服務，以利用戶設定需要監控的雲端服務。監控服務通常以圖形化

控制面板的方式顯示，還可以設定異常通知及異常效能指標。

15. 分散式服務

資料庫並非得益於分散式運作的唯一服務。重點在於延遲。若運算資源離管理的資料或處理程序太遠，傳送與接受指令及資訊的時間會太長。若在回饋迴路中延遲太嚴重，迴路就容易失控。若機器學習與資料間延遲太高，執行訓練時間就會過長。為解決這個問題，雲端服務供應商提供連結性應用可延展服務到客戶資料中心(混合雲)，或接近客戶廠區樓層(邊緣運算)。

16. 邊緣運算

將分析與機器學習帶到地理上靠近機器與其他真實世界物件(物聯網, IoT)的位置，帶來了專屬設備，像是帶有GPU與感測器的微型運算裝置，與支援它們的基礎架構，例如邊緣伺服器、自動化平台與內容傳遞網路。最終，這些全會連回雲端，但在邊緣執行分析的能力，大幅減少傳送至雲端的資料量，也降低了延遲。

下次，當你聽到對雲端支出的疑慮時，或許可以提出這十六項優勢之一，或找到其中一個有助於你或你團隊的雲端功能。我們探討的這些雲端革新任一皆可證明使用上的合理性。總的來看，好處令人難以抗拒。