對第二版的讚譽

「這本書全面而深入地介紹了雲端運算的概念和實際運作機制。它不僅清楚的解釋了雲端的功能和架構，還說明了雲端對企業的影響。對於未來需要制定雲端運算的藍圖來說，這是一本很好的基礎讀物。」

——*Jo Peterson*，*Clarify360* 的雲端與安全副總裁

「這本書提供全面且深入研究的雲端運算指南，涵蓋了從雲端運算基礎到進階架構考量的廣泛主題。書中以清晰簡潔的文風撰寫，並提供大量寶貴的資訊和案例研究供參考。我強力推薦這本書給任何想要了解更多關於雲端運算的人。」

——*Jorge Blanco*，*Glumin* 企業再造與訓練部門總經理

「憑藉其全方位的洞察力和中立客觀的觀點，這本書在雲端運算複雜的世界中熠熠閃耀，成為指路明燈。作者強調如何做出與商業目標契合的明智決策，為成功採用這項革新科技奠定了基礎。透過引領潛在的危險和挑戰，本書使讀者能夠做出戰略性選擇，保護其組織免於潛在陷阱。從基本概念到實際考量，每章都提供了一個解鎖雲端運算全部潛力的路線圖。本書包含珍貴的案例研究、架構分析以及對服務品質指標和 *SLA* 的關注，是任何希望利用雲端運算的人不可或缺的資源。它作為雲端專業人士認證的重要基石，為進一步探索這個持續成長的領域奠定了良好的基礎。對於每一位具有前瞻性思維的專業人士來說，這是一本必備讀物。」

——*Valther Galván*，首席安全資訊官

「這本書是目前市面上最完整的雲端運算概念指南。它奠定了紮實的基礎，並逐步深入探討，內容涵蓋廣泛。書中穿插的案例研究與內容相輔相成，生動地展示了雲端運算的可能性和難題。」

——*Emmett Dulaney*，大學教授與作家

前言

David S. Linthicum

終於，一本關於雲端運算的使用手冊問世。

大多數企業都誤解了雲端運算。雖然不至於到「倒閉」的程度，但大多數企業最終得到的都是未經優化的雲端系統，無法達到股東預期的價值。

發生什麼事呢？大多數人將問題歸咎於過度炒作的技術、「雲端洗腦」以及太過倉促地遷移到雲端平台。但真正的答案是，合格的雲端運算解決方案設計師和建構者數量不足，供不應求。就連雲端銷售人員一開始也缺乏足夠的雲端專業知識提供客戶建議。

專業人員的經驗和資歷的累積並不容易，尤其是每次都需要設計客製化解決方案及複雜的新技術，當雲端「先驅」的需求很高，也很少有時間將技能傳授給其他人。

長久以來，我們一直假設只要某個東西有效，它就是最佳化的。未經優化的雲端部署方案會隨著時間降低企業價值。如果不斷重複這些錯誤，很快就會感受到雲端運算帶來的負面價值。

回顧 2008 年和 2009 年，當雲端運算的炒作首次出現在快速發展的科技市場時，時常可以看到雲端投資報酬率 10 倍的承諾。但大多數企業每投資一美元，最終的回報只有 0.5 美元，而非預期的 10 美元。

你可以這樣理解這個問題：從洛杉磯搭乘廉價航空的經濟艙飛往紐約，費用大約是搭乘私人飛機的 1%。兩種飛機都能讓你從 A 點到達 B 點，但太多的企業雲端就像包機一樣昂貴。與飛行成本一樣，雲端運算也提供許多折衷方案，可以在效率和成本之間取得令人滿意的平衡。這種平衡需要了解資料、安全性、營運和應用程式行為，這些都需要透過精心配置的雲端運算架構和實作技術來解決，才能建立最佳的解決方案。

遺漏的手冊

我們面臨的是教育問題，而不是技術問題。大多數企業利用他們從傳統技術平台理解的零星知識，勉強完成了最初的雲端實施。對於新興雲端運算技術的能力，存在太多廣泛的臆測。

當然，沒有單一資料來源可以提供關於「雲端」是什麼以及它能做什麼的所有知識。本書作為實用知識的來源脫穎而出，提供對雲端技術的全面理解，以及如何有效利用雲端技術，透過標準和進階的雲端架構概念來解決大多數業務問題。更確切地說，本書提供了你需要掌握的知識，以發掘最初承諾的雲端運算價值。

如同大多數優秀的使用手冊一樣，本書包含了作為「快速入門」指南的基礎知識，以及成功利用雲端機制的建議。Erl 進一步深入探討了只有透過經驗才能學到的進階概念。基礎知識足以讓你通過雲端工作面試。Erl 對於進階概念的討論超越了我們大多數雲端架構領域人士目前的認知。

我發現最吸引人的是，Erl 並未專注於特定的技術品牌，因為他了解這些技術會快速發展。好的解決方案始於概念。不幸的是，我們經常因為在流程中過早引入特定品牌的技術，而誤解了這些解決方案應該做什麼或應該是什麼。在設計和建構雲端運算解決方案時尤其如此。Erl 在討論中省略了品牌，使得本書中的概念更具實用性，並且適用於隨時間演進的不同的技術。

Erl 以教育家的熱忱，將其他人所理解的內容整合為有用的知識集合。閱讀本書，學習雲端運算的概念、設計、架構和其他進階概念，這些概念以邏輯的方式建構在其他概念之上。無論是雲端旅程的初學者，還是更進階的學習者，都能理解書中傳達的資訊。

這本手冊適用於所有程度和需求。在你自己的雲端運算旅程中，你可以多次參考這本手冊，以確保你做出正確的選擇。

終於，找到雲端運算的價值

我猜想你們大多數人之所以會閱讀本書，是因為你們已經見證了雲端運算未能達到預期效果，並且想知道如何解決這個問題。這是唯一一本結構良好且完整的指南，可以幫助你了解如何正確運用雲端運算。將本書中提出的概念轉化為最佳的解決方案，最大限度地提高企業回報價值。

本書旨在幫助你做出正確的選擇、理解做出這些選擇的原因，並確定最適合企業的選擇。如果說有一本涵蓋了進階和基礎概念的雲端運算使用手冊，那就是這本了。

它將幫助你更好地理解任何技術的正確應用及其在解決問題方面的有效性。的確，它能讓你避免掉入許多「兔子洞」，這些「兔子洞」可能會浪費時間，或者更有可能導致你做出錯誤的決定。

祝你運算愉快。

David S. Linthicum
作家、演講家、教育家和顧問

4.2 雲的特性

IT 環境需要具備特定的特性才能有效地實現遠端配置、具有擴充性和可計算使用量的 IT 資源。IT 環境成為有效的雲端環境需要確實具備以下特性。

以下特徵普遍存在於大多數雲端環境中：

- 按需求使用
- 隨時隨地存取
- 多租戶（和資源池）
- 彈性
- 可計算使用量
- 韌性

雲端服務供應商和消費者可以共同或自行評估這些特性，以衡量特定雲端平台的定位。雖然雲端服務和 IT 資源將繼承和表現出不同程度的個別特徵，但通常支援和採用度越高，產生的價值就越大。

按需求使用

雲端服務消費者可以單方面存取雲端 IT 資源並自主配置這些 IT 資源。一旦設定完畢，這些 IT 資源將在使用時自動配置，無須雲端服務消費者或供應商人工干預。這形成**按需求使用**的環境。這種特性也稱為「隨選自助服務」，它代表主流雲端環境中以服務和使用驅動的特性。

隨時隨地存取

隨時隨地存取是指雲端服務可以容易被存取的能力。為了隨時隨地存取的能力，雲端服務可能需要支援各種設備、傳輸協議、介面和安全技術。通常提供這種等級的存取服務需要雲端服務架構根據不同雲端服務消費者進行客製化。

多租戶和資源池

軟體程式的*多租戶*特性，即程式的一個實體能服務於不同的使用者（租戶），且每個租戶彼此隔離。雲端服務供應商透過採用多租戶模型（這種模型經常依賴虛擬化技術的使用）來將 IT 資源轉化為資源池，為多個雲端服務使用者提供服務。透過多租戶技術，可以根據雲端服務消費者的需求動態重新分配 IT 資源。

資源池允許雲端服務供應商將大規模的 IT 資源轉化為資源池，為多個雲端服務消費者提供服務。不同的物理和虛擬 IT 資源會根據雲端服務消費者需求動態重新分配，然後透過使用率統計來重複執行。資源池通常透過多租戶技術來實現，因此為多租戶特性中的一部分。更詳細的解釋請參考第 13 章的「資源池架構」小節。

圖 4.9 和 4.10 展示了單租戶和多租戶環境之間的區別。

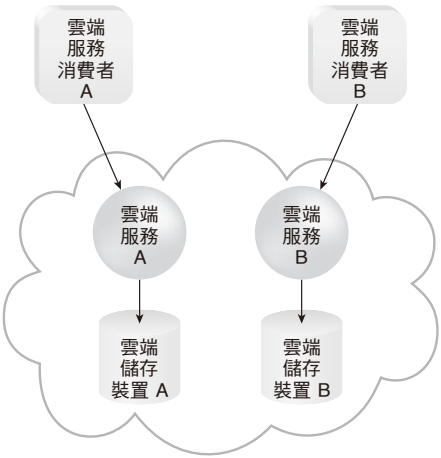


圖 4.9 單租戶環境，每個雲端使用者有個別的 IT 資源實體

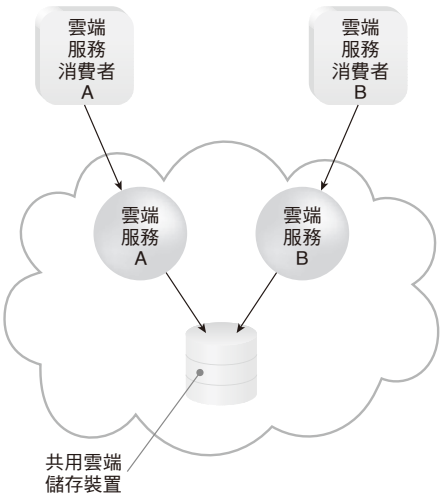


圖 4.10 在多租戶環境中，一個 IT 資源的實體，例如雲端儲存裝置可以服務多個雲端消費者

如圖 4.10 所示，多租戶允許多個雲端服務消費者使用相同的 IT 資源或實體，同時使用者不會知道該資源可能同時被其他人使用。

彈性

*彈性*是指雲端自動調整 IT 資源的能力，可根據運行時的狀況或由雲端服務消費者或供應商預先設定的需求擴展 IT 資源。彈性通常被認為是採用雲端運算的主要理由之一，因為它與「降低投資和對應的成本」效益密切相關。擁有龐大 IT 資源的雲端服務供應商可以提供最大的彈性範圍。

可計算使用量

*可計算使用量*的特性是指雲端平台追蹤 IT 資源使用情況（主要由雲端服務消費者使用）的能力。基於計算結果，雲端服務供應商可以只向雲端服務消費者收取實際使用過的 IT 資源費用，以及存取 IT 資源時的費用。在此情境下，可計算使用量與按需使用的特性密切相關。

可計算使用量不僅僅用於追蹤計費的統計數據，它還涵蓋 IT 資源監控和相關的使用狀況報告（同時適用於雲端服務供應商和消費者），因此可計算使用量的特性也適用於不收取使用費的雲端（例如在接下來的「雲端部署模型」小節中描述的私有雲端部署模型）。

韌性

韌性運算是一種將冗餘的 IT 資源實體分佈在不同的物理位置達到故障轉移的目的。可以預先配置 IT 資源以便在其中一個資源出現故障時，處理程序自動移交給另一個冗餘的實體。在雲端運算中，*韌性*的特性可以指同一雲端內（但位於不同物理位置）的冗餘 IT 資源，或跨越多個雲端的冗餘 IT 資源。雲端服務消費者可以透過利用雲端 IT 資源的韌性來提高其應用程式的可靠性和可用性（圖 4.11）。

4.3 雲端交付模型

*雲端交付模型*代表雲端服務供應商提供的特定預先封裝的 IT 資源組合。以下三種常見的雲端交付模型已廣泛被使用：

- 基礎架構即服務（IaaS）
- 平台即服務（PaaS）
- 軟體即服務（SaaS）

這三種模型之間涵蓋的範圍和關聯將在本章後面的「組合雲端交付模型」小節進行探討。

NOTE

雲端交付模型可以稱為雲端服務交付模型，因為每種模型都被歸類為不同類型的雲端服務產品。

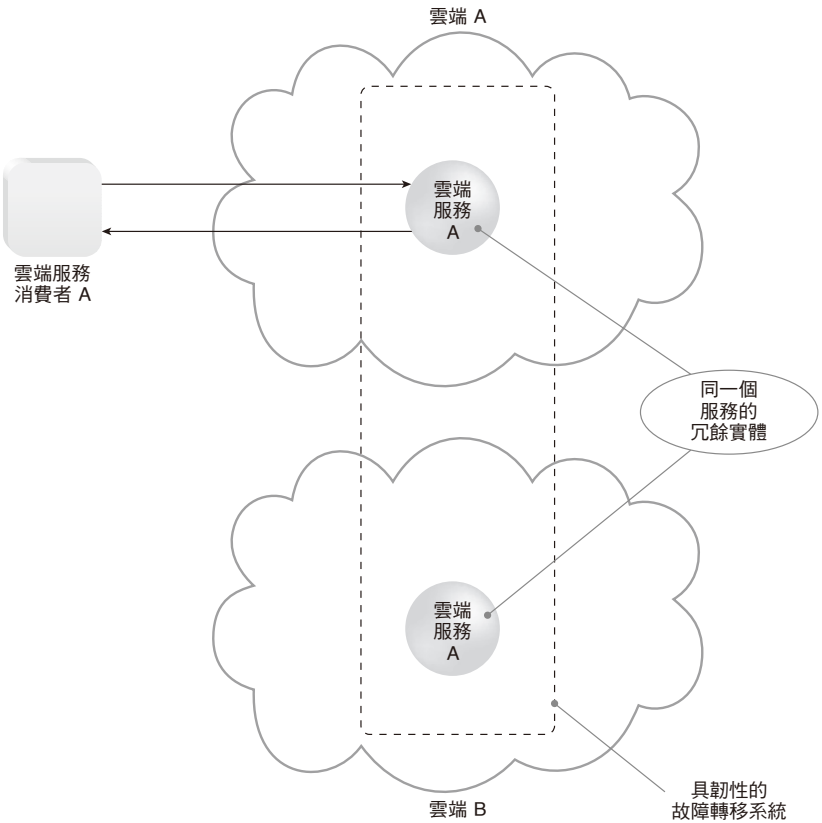


圖 4.11 具有韌性的系統在雲端 A 與 B 上同時運行雲端服務 A，當雲端 A 上故障時可以轉移到雲端 B 上的冗餘雲端服務 A

基礎架構即服務（IaaS）

基礎架構即服務（IaaS）的交付模型為一個獨立的 IT 環境，提供以基礎設施為中心的 IT 資源，透過雲端服務存取介面和工具進行管理。該環境可以包含硬體、網路、連線、作業系統和其他「原始」IT 資源。與傳統的託管或外包環境相比，IaaS 的 IT 資源通常會透過虛擬化將資源轉化為服務組和，簡化基礎架構運行時的擴展和客製化需求。

IaaS 環境的目標是為雲端服務消費者提供對雲端 IT 資源高度的配置、使用和控制權。IaaS 提供的 IT 資源通常不會預先設定好，因此管理責任直接落在雲端服務消費者身上，該模型適用於需要對建立的雲端環境擁有高度控制權的雲端服務消費者。

有時，雲端服務供應商會從其他雲端服務供應商購買 IaaS 服務來擴展自己的雲端環境。不同雲端服務供應商提供的 IaaS 產品上所提供的 IT 資源類型和品牌可能有所不同。IaaS 環境所提供的 IT 資源通常會以全新初始化的狀態提供服務。通常 IaaS 環境中的主要 IT 資源是虛擬伺服器。虛擬伺服器的使用方式通常是透過指定伺服器硬體需求（例如處理能力、記憶體和本地儲存空間）來租用，如圖 4.12 所示。

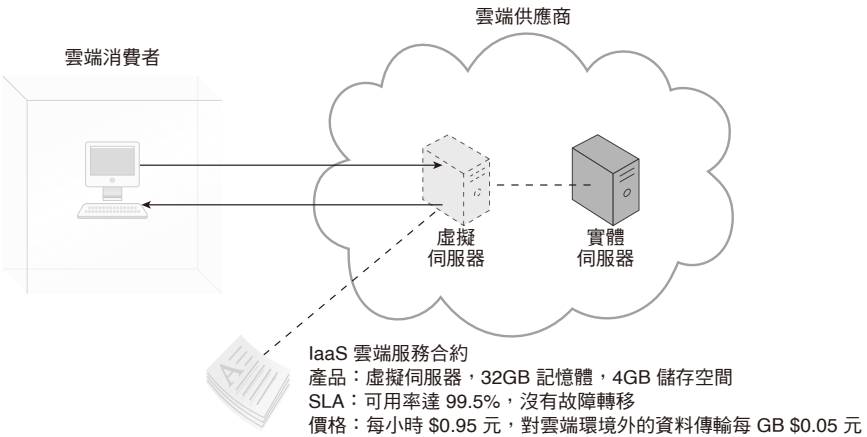


圖 4.12 雲端服務消費者使用 IaaS 環境中的虛擬伺服器。雲端服務供應商提供一個範圍內的使用合約，記載所提供的伺服器規格，例如容量，效能及可用率。

平台即服務（PaaS）

平台即服務（PaaS）交付模型為一個預先制定的「可立即使用」環境，通常包含已部署並配置的 IT 資源。更準確地來說，PaaS 主要由使用現成的環境來建立一套預封裝的產品和工具，用於支援客製化應用程式的整個交付生命週期。

雲端服務消費者使用和投資 PaaS 環境的常見原因包括：

- 雲端服務消費者希望達成可擴展性和經濟性的目的將內部部署環境擴展到雲端。
- 雲端服務消費者使用現成環境完全替代內部部署環境。
- 雲端服務消費者希望成為雲端服務供應商，並部署自己的雲端服務以供其他外部雲端服務消費者使用。

在現成平台中運作，雲端服務消費者可以避免配置和維護 IaaS 模型中提供的裸機基礎設施 IT 資源所帶來的管理負擔。相對的，雲端服務消費者對託管和提供平台的底層 IT 資源的控制權較低（圖 4.13）。

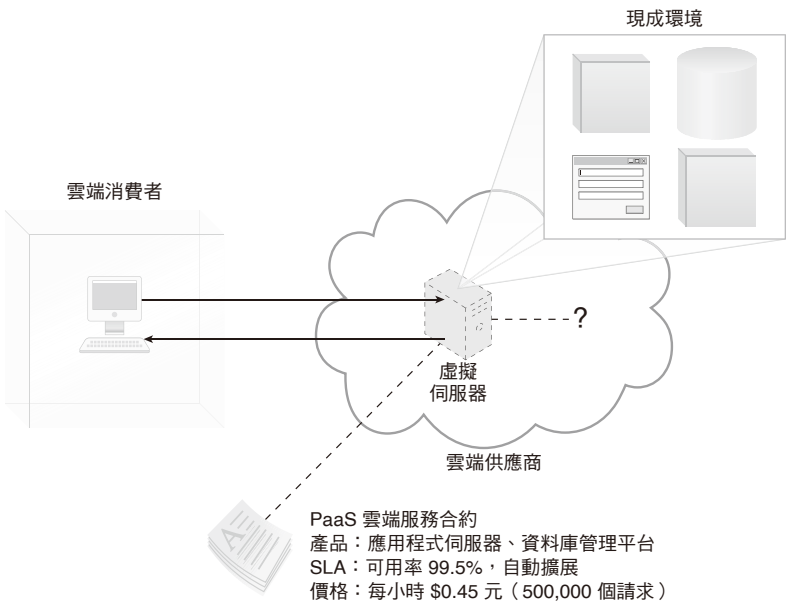


圖 4.13 雲端服務消費者存取 PaaS 的現成環境。問號為刻意呈現消費者並不知道雲端服務供應商的實作細節。

這章將介紹雲端環境上基本的資訊安全術語和概念，然後概述常見於公有雲環境的威脅和攻擊。第 10 章和第 11 章介紹的雲端安全和網路安全機制，並提供應對這些威脅的安全控制措施。

7.1 基本安全術語

資訊安全是由技術、手法、法規、行為等的複雜集合來保護電腦系統的存取權限和數據完整性。IT 安全措施是防禦來自使用者非蓄意的錯誤使用或惡意造成的威脅和干擾。

接下來的內容將定義雲端運算的基本安全術語並描述相關概念。

機密性

機密性（*Confidentiality*）是指訊息僅限授權方存取的特性（圖 7.1）。在雲端環境中，機密性主要指對傳輸和儲存資料的存取限制。

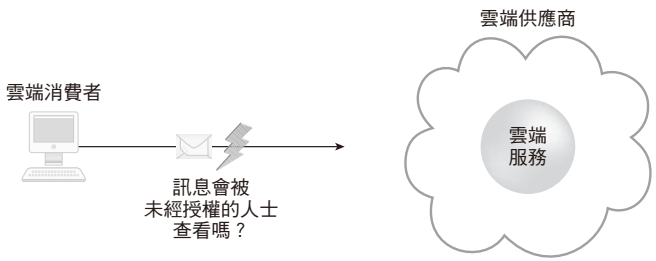


圖 7.1 雲端使用者發送給雲端服務供應商的訊息只有不被未經授權的第三方存取才會視為機密

完整性

完整性（*Integrity*）是指訊息不會被未經授權的人更改的特性（圖 7.2）。雲端數據完整性面臨一個重要問題是，雲端用戶是否可以保證發送到雲端服務的數據與雲端服務接收到的數據符合。完整性還可以擴展到雲端服務和雲端 IT 資源如何儲存、處理和取得數據。

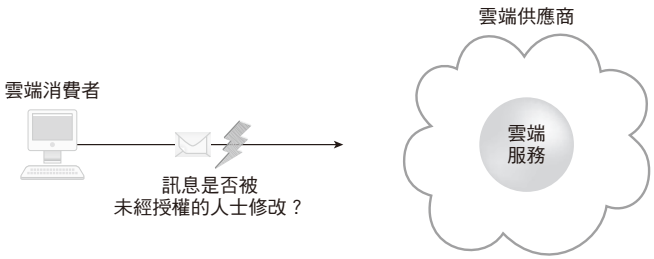


圖 7.2 雲端服務消費者發送給雲端服務供應商的訊息中途沒有被修改則視為具有完整性

可用性

可用性（*Availability*）是指在指定時間內可存取和使用的特性。在典型的雲端環境中，雲端服務可用性可能是雲端服務供應商和雲端營運商共同承擔的責任。雲端服務消費者使用的雲端解決方案可用性也由雲端服務消費者進一步承擔。

圖 7.3 描繪一個場景，展示了如何透過一系列安全技術來確保網際網路上資訊交換的機密性和完整性，以及含有私人資料的中央資料庫可用性。

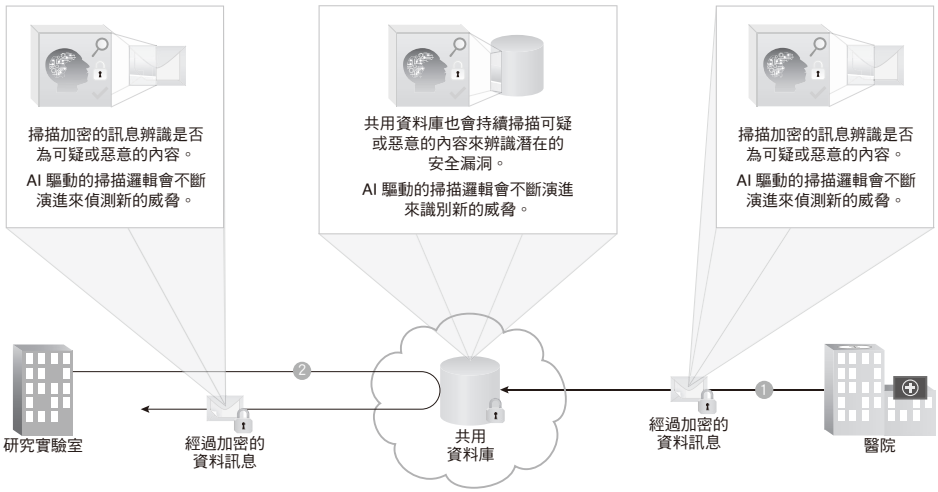


圖 7.3 醫院向雲端資料庫貢獻機敏醫療數據（1），該資料庫與會存取該數據（2）的研究機構共享。使用的網路安全技術透過加密提供機密性，並在運行環境掃描提供完整性，確保共用雲端資料庫持續保有安全性來提供可用性。

攻擊媒介和攻擊面

攻擊媒介（*attack vector*）是攻擊者用來利用漏洞的途徑。電子郵件附件、彈出視窗、聊天室和即時訊息都是攻擊媒介的例子。通常會利用人為錯誤或無知來選擇攻擊媒介。*攻擊面*（*attack surface*）是攻擊者可以用來存取系統或獲取資訊的攻擊媒介集合。

7.3 威脅來源

威脅來源（*threat agent*）是指能夠發動攻擊的實體。雲端安全的威脅可以來自內部或外部，可以是人類或軟體程式。接下來將介紹相應的威脅來源。圖 7.4 展示了威脅來源在漏洞、威脅、風險對安全政策和安全機制所建立的保護措施方面的作用。

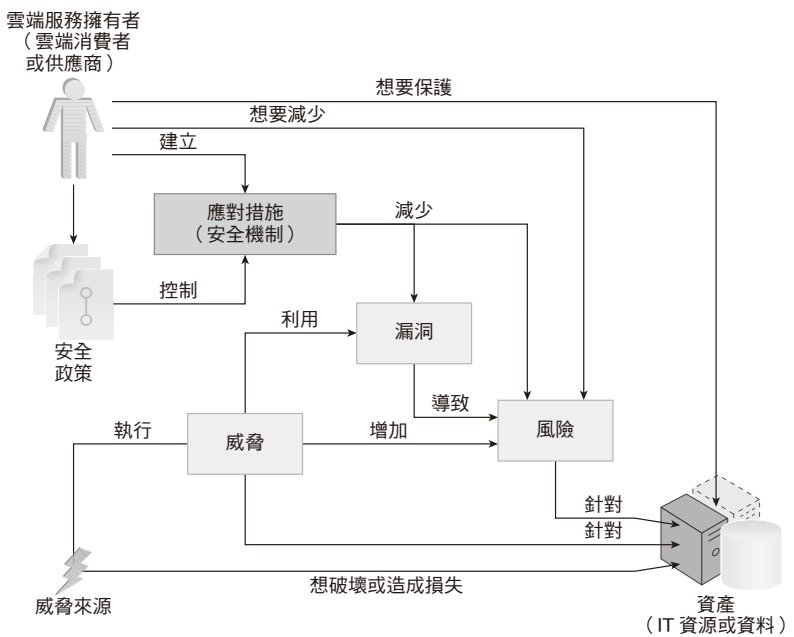


圖 7.4 安全政策跟機制如何應對威脅來源所造成的威脅，漏洞和風險

匿名攻擊者

匿名攻擊者（*anonymous attacker*）是非信任的雲端服務使用者，在雲端沒有權限（圖 7.5）。它通常利用外部軟體程式透過公共網路發起網路層的攻擊。當匿名攻擊者對安全政策和防禦措施的資訊有限時，會抑制他們制定有效攻擊的能力。因此，匿名攻擊者經常採取繞過用戶帳戶或竊取用戶憑證等行為，同時使用可以確保匿名性或需要消耗大量資源才能在法律上被起訴的方法。

圖 7.5 匿名攻擊者的圖示

惡意服務代理

惡意服務代理（*malicious service agent*）能夠攔截和轉發雲端環境內傳輸的網路流量（圖 7.6）。它通常以邏輯遭到破壞或具有惡意的服務代理（或偽裝成服務代理程式）的方式呈現。它也可能是可以遠端攔截並破壞訊息內容的外部程式。

圖 7.6 惡意服務代理的圖示

受信任的攻擊者

受信任的攻擊者（*trusted attacker*）與雲端使用者共享同一個雲端環境中的 IT 資源，並試圖利用合法憑證攻擊雲端服務供應商和其共享 IT 資源的雲端租戶（圖 7.7）。與匿名攻擊者（非信任）不同，受信任的攻擊者通常透過濫用合法憑證或竊取敏感和機密訊息，從雲端信任邊界內發動攻擊。

圖 7.7 受信任的攻擊者圖示

受信任的攻擊者（也稱為惡意租戶（*malicious tenants*））可以利用雲端 IT 資源進行各種攻擊，例如入侵弱認證流程、破解加密、發送垃圾郵件或發動常見攻擊，像是阻斷服務攻擊（denial of service）。

惡意內部人員

惡意內部人員（*Malicious Insider*）是雲端服務供應商相關的人為威脅來源。他們通常是當前或以前的員工或第三方供應商，可以進出雲端服務供應商的場所。此類威脅來源具有巨大的破壞潛力，因為惡意內部人員可能擁有存取雲端使用者 IT 資源的管理權限。

NOTE

代表一般形式的人為攻擊的符號是工作站結合閃電符號（圖 7.8）。這個通用符號並不代表特定的威脅來源，只表示攻擊是透過工作站發起的。

圖 7.8 圖示為代表利用工作站發起的攻擊，人類圖示並非必要的元素

7.4 常見威脅

本章節介紹了雲端環境中一些常見的威脅和漏洞，並描述了稍早提到的威脅來源的角色。

流量竊聽

流量竊聽（*Traffic eavesdropping*）是指傳輸到雲端或在雲端內（通常從雲端使用者到雲端服務供應商）的數據被動的被惡意服務代理攔截以進行非法資訊收集（圖 7.9）。此攻擊的目的是直接破壞數據的機密性，並可能破壞雲端使用者和雲端服務供應商之間的機密性。由於攻擊是被動的，短時間內不容易被檢測到。

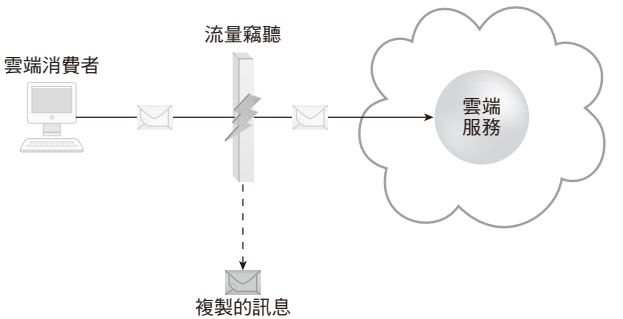


圖 7.9 一個位於外部的惡意服務代理程式執行流量竊取攻擊，攔截雲端使用者發送到雲端服務的訊息。該服務代理程式在訊息傳送至雲端服務之前複製了未經授權的訊息副本。

惡意中間人

惡意中間人（*malicious Intermediary*）威脅在於惡意服務代理攔截和篡改訊息，從而破壞訊息的機密性或完整性。它還可能會在訊息轉發到目的地之前插入有害資料。圖 7.10 展示了惡意中間人攻擊的一個常見範例。

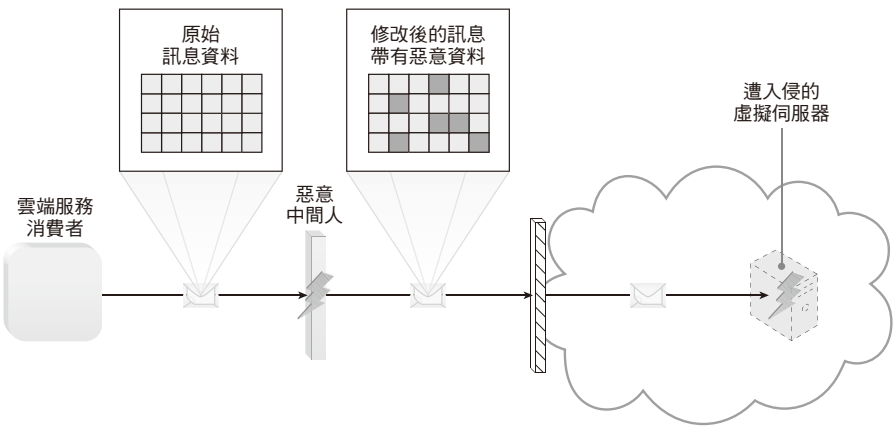


圖 7.10 惡意服務代理程式會攔截並修改雲端服務使用者傳送至運行在虛擬伺服器上雲端服務的訊息（未標示在圖中）。由於有害數據被包裝進訊息中，虛擬伺服器將會遭到入侵。

NOTE

雖然不常見，但惡意中間人攻擊也可以由惡意的雲端服務使用者程式發起。

阻斷服務

阻斷服務（*denial of service*，*DoS*）攻擊的目的是使 IT 資源過載以至於它們無法正常運行。這種形式的攻擊通常以下列方式發起：

- 使用捏造的訊息或重複的連線請求增加雲端服務的工作負載。
- 用大流量使網路過載，降低其反應能力並癱瘓其效能。
- 發送多個雲端服務請求，每個請求目的在消耗大量記憶體和處理資源。

成功的 DoS 攻擊會導致伺服器效能下降或故障，如圖 7.11 所示。

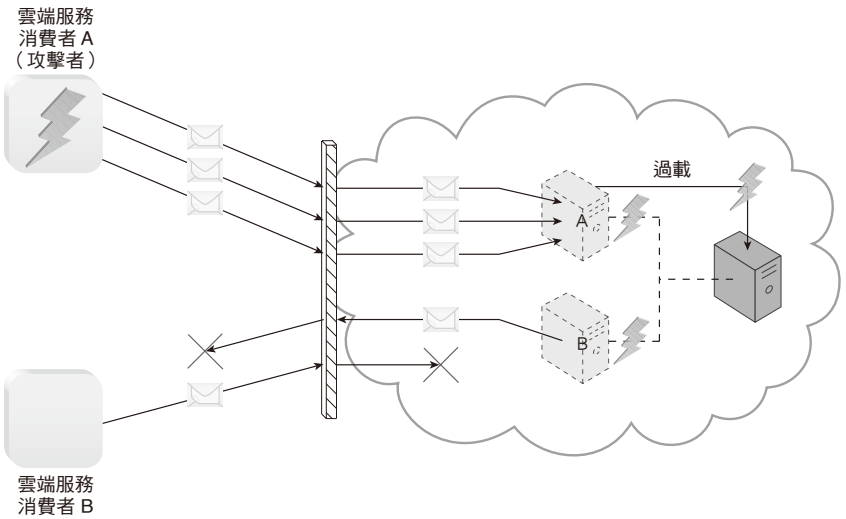


圖 7.11 雲端服務使用者 A 向位於虛擬伺服器 A 的雲端服務（未標示）傳送大量訊息。這樣會使底層實體伺服器的容量過載而導致虛擬伺服器 A 和 B 發生停機。導致合法雲端服務使用者（例如雲端服務使用者 B）無法與任何位於虛擬伺服器 A 和 B 的雲端服務通訊。

NOTE

服務阻斷攻擊（DoS）的常見變種是**分散式阻斷服務攻擊**（*distributed denial of service*，*DDoS*），攻擊者會使用大量被入侵的系統向目標網站或網路發起巨大流量，企圖使該網站或網路無法提供服務。

過度授權

過度授權（*insufficient authorization*）攻擊是指錯誤或授予過度的存取權限，導致攻擊者可以存取受保護的 IT 資源。攻擊者會取得通常只有受信任的使用者程式能使用的 IT 資源的直接存取權（圖 7.12）。

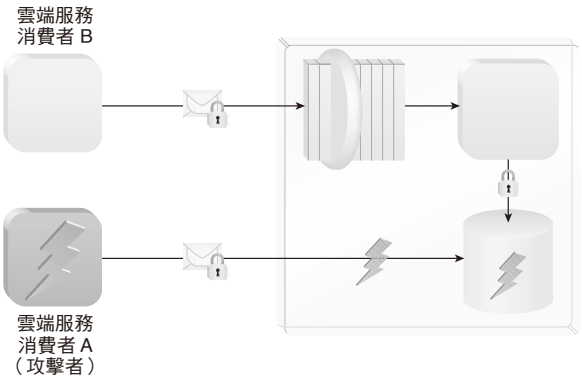


圖 7.12 雲端服務使用者 A 存取了一個原本設計只會被具有服務合約授權使用的網路服務（如同雲端服務使用者 B）進行存取。

這種攻擊的一種變體稱為**弱認證**（*weak authentication*），可能發生在使用弱密碼或共享帳戶來保護 IT 的資源。在雲端環境中，此類攻擊可能會產生重大影響，具體取決於攻擊者獲得的 IT 資源範圍和對這些 IT 資源的存取範圍（圖 7.13）。

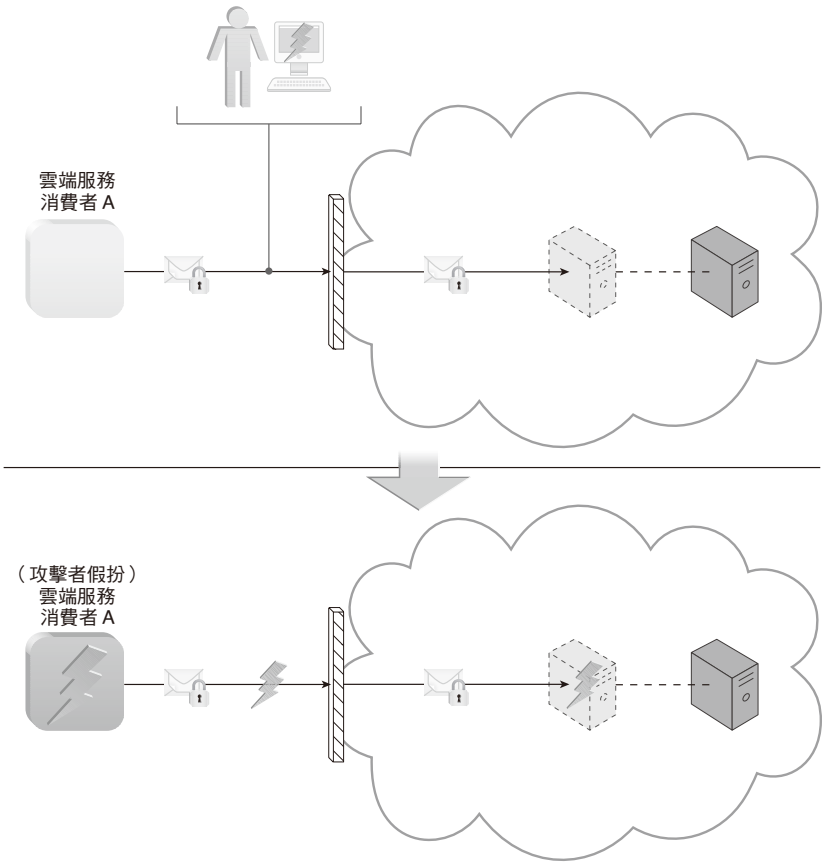


圖 7.13 一名攻擊者破解了雲端服務使用者 A 使用的弱密碼。惡意的雲端服務使用者程式（由攻擊者擁有）假冒雲端服務使用者 A 以存取雲端虛擬伺服器。

虛擬化攻擊

虛擬化讓多個雲端使用者能夠存取邏輯上隔離但共享底層硬體的 IT 資源。由於雲端服務供應商授權雲端使用者對虛擬化 IT 資源（例如虛擬伺服器）的管理權限，因此雲端使用者可能會濫用此存取權限來攻擊底層實體 IT 資源而產生風險。

本章描述以下基礎雲端架構模型：

- 工作負載分配
- 資源池
- 動態擴展
- 彈性資源容量
- 服務負載平衡
- 雲端彈性擴展
- 彈性磁碟配置
- 冗餘儲存
- 多雲端

每個架構通常都會有一些在第二部分提到過的雲端運算機制參與其中。

13.1 工作負載分配架構

IT 資源可以透過增加一個或多個相同的 IT 資源以及一個負載平衡器來實現水平擴展，負載平衡器擁有運作邏輯能夠在可用 IT 資源之間均勻分配工作負載（圖 13.1）。成立的**工作負載分配架構**取決於負載平衡演算法和運行時邏輯的複雜性，可以在一定程度上減少 IT 資源過度利用和利用不足的問題。

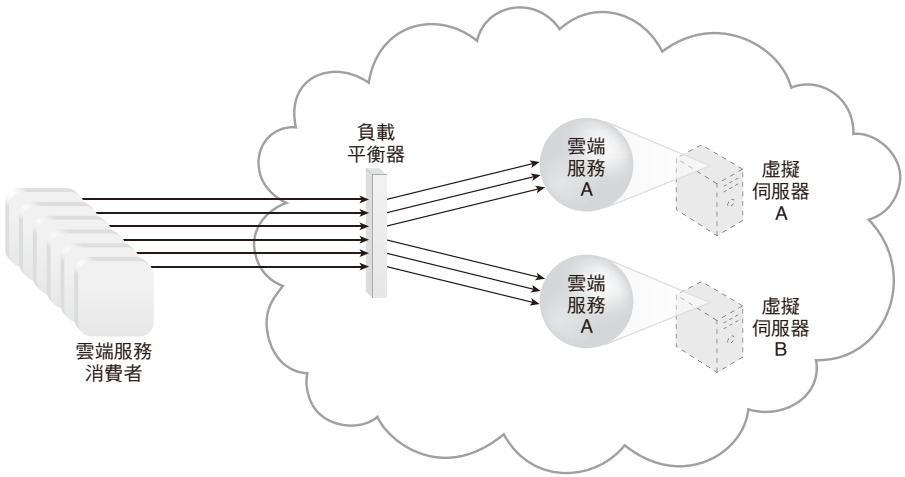


圖 13.1 雲端服務 A 的冗餘副本運行在虛擬伺服器 B。負載平衡器會攔截雲端服務使用者請求，並將它們導向虛擬伺服器 A 和 B，以確保平均分配工作負載。

這個基本架構模型可以應用於任何 IT 資源，工作負載分配功能通常用於支援分散式虛擬伺服器、雲端儲存裝置和雲端服務。考慮負載平衡的不同面向，特定 IT 資源的負載平衡系統通常會有一些架構上的特殊變體，例如：

- 本章後面介紹的服務負載平衡架構
- 第 14 章介紹的虛擬伺服器負載平衡架構
- 第 15 章描述的虛擬交換器負載平衡架構

除了基本的負載平衡器機制以及可以使用負載平衡的虛擬伺服器和雲端儲存裝置機制之外，下列機制也可以成為雲端架構的一部分：

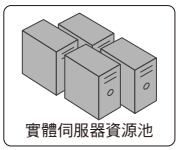
- **稽核監視器**：分配工作負載時，為了滿足法規要求，可能因為處理資料的 IT 資源類型以及所在的地理位置決定是否啟用稽核監視器。
- **雲端使用量監視器**：可以使用各種監視器來追蹤運作時的工作負載和資料處理。
- *Hypervisor*：執行的工作負載可能需要在 Hypervisor 與虛擬伺服器之間進行分配。

- **邏輯網路邊界**：邏輯網路邊界隔離雲端客戶的網路邊界，具體取決於工作負載的分佈方式和地點。
- **資源叢集**：處於主動 - 主動模式的叢集式 IT 資源通常用支援不同叢集節點之間的工作負載平衡。
- **資源複製**：此機制可以根據運行時工作負載分配需求產生虛擬化 IT 資源的新實例。

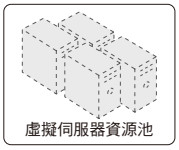
13.2 資源池架構

資源池架構使用一個或多個資源池，相同的 IT 資源分組並由系統自動維護且確保它們保持同步。

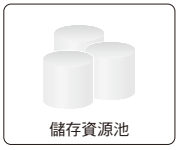
以下是常見的資源池範例：



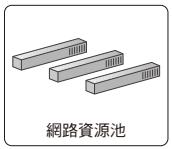
實體伺服器資源池：由具有網路連線的伺服器組成，已安裝作業系統和其他必要的應用程式，隨時可以使用。



虛擬伺服器資源池：通常使用雲端客戶在配置過程中，從幾種可用範本裡選擇一種進行配置。例如，雲端客戶可以設定一個擁有 4 GB RAM 的中階 Windows 伺服器資源池或一個擁有 2 GB RAM 的低階 Ubuntu 伺服器資源池。

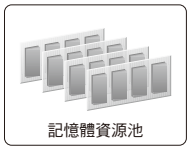


儲存資源池或雲端儲存裝置資源池：利用檔案儲存裝置或區塊儲存裝置組成，其中包含空的或裝滿的雲端儲存裝置。



網路資源池（或互連資源池）：由預先配置的不同網路設備連接組成。例如，可以建立一個虛擬防火牆設備或實體網路交換器資源池，用於冗餘連接、負載平衡或鏈路聚合。

***CPU* 資源池**：可隨時分配給虛擬伺服器，通常細分到單一處理核心。



實體記憶體資源池：可以在新建的實體伺服器或垂直擴展實體伺服器時使用。

每種類型的 IT 資源可以建立專用資源池，每個資源池可以組成更大的資源池，在這種情況下，每個獨立的資源池就成為更大資源池中的子資源池（圖 13.2）。

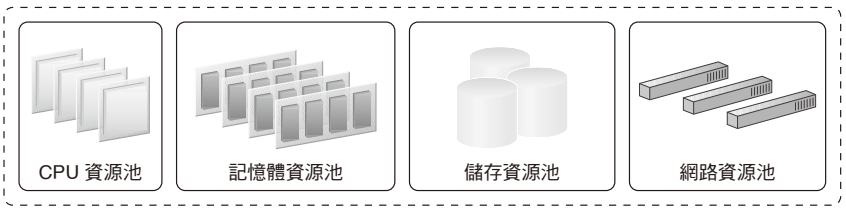


圖 13.2 資源池範例，由中央處理器、記憶體、雲端儲存設備和虛擬網路設備等 4 個子資源池所組成。

資源池可以變得非常複雜，可以為特定雲端客戶或應用程式建立多個資源池。可以建立階層架構來形成父資源池、同級資源池和巢狀資源池，以方便滿足各種需求（圖 13.3）。

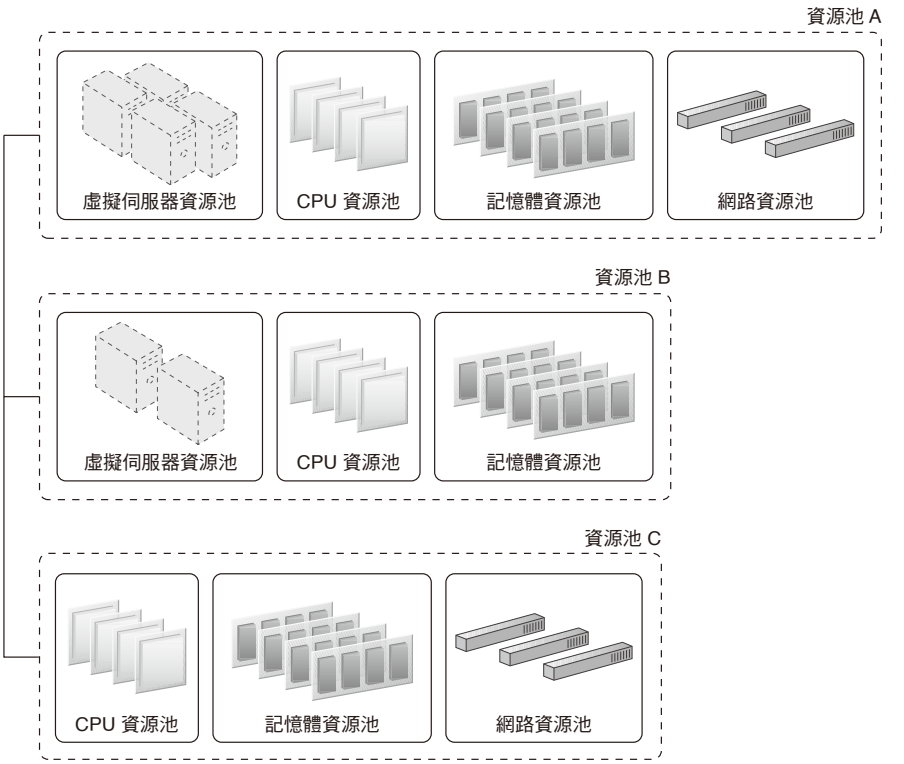


圖 13.3 可以從整個雲端共用的通用 IT 資源儲備中建立資源池 B 和資源池 C 的。而另一種替代方案是從分配給雲端客戶的較大資源池 A 中分割出來的同級資源池建立資源池 B 和資源池 C。

同級資源池通常來自於實體分組的 IT 資源，而不是分佈在不同資料中心的 IT 資源。同級資源池相互隔離，這樣每個雲端客戶只能存取各自的資源池。

在巢狀資源池模型中，較大的資源池被細分為較小的資源池，這些較小的資源池將相同類型的 IT 資源組合在一起（圖 13.4）。巢狀資源池可用於將資源池分配給同一雲端客戶組織中的不同部門或群組。

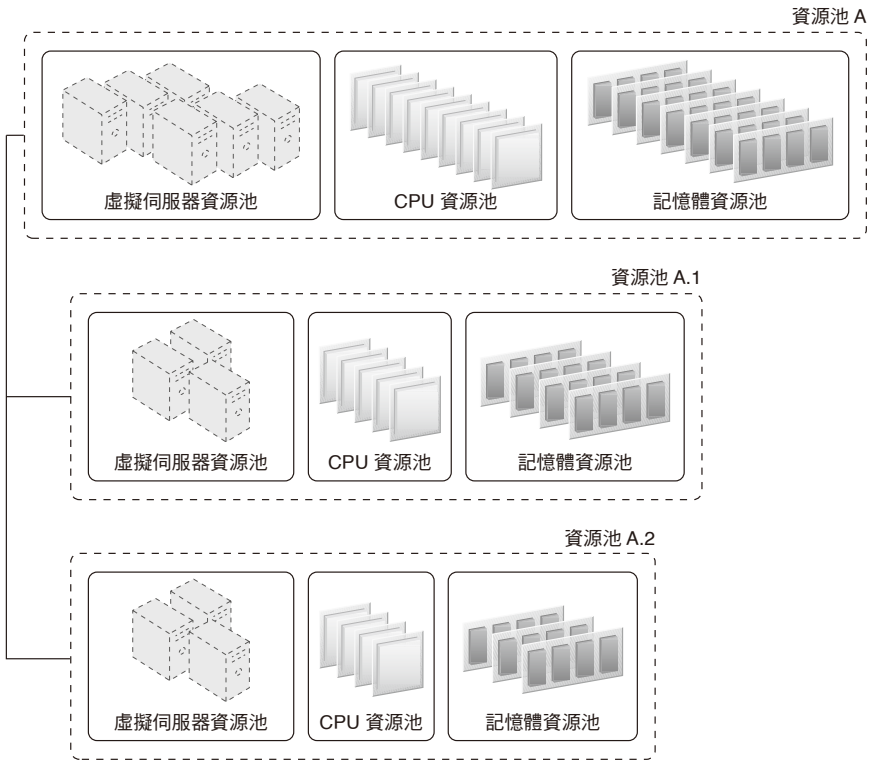


圖 13.4 巢狀資源池 A.1 和資源池 A.2 與資源池 A 包含相同的 IT 資源類型，但數量不同。巢狀資源池通常用來配置相同的雲端服務，需要使用相同類型的 IT 資源並快速透過相同配置產生實體。

定義好資源池後，可以從每個資源池中建立多個 IT 資源實例，並存放在記憶體中的「使用中」IT 資源池作為紀錄。

除了雲端儲存裝置和虛擬伺服器（這些都是常見的資源池機制）之外，下列機制也可以成為這個雲端架構的一部分：

- **稽核監視器**：此機制監控資源池使用情況，以確保遵守隱私和法規要求，尤其是資源池包含雲端儲存裝置或載入到記憶體中的資料時。

- **雲端使用量監視器**：各種雲端使用量監視器參與資源池 IT 資源和任何底層管理系統所需的運作追蹤和同步。
- *Hypervisor*：Hypervisor 機制除了運行虛擬伺服器（有時也運行資源池）之外，還負責為虛擬伺服器提供存取資源池的權限。
- **邏輯網路邊界**：邏輯網路邊界在邏輯上組織和隔離資源池。
- **按使用量計費監視器**：按使用量計費監視器會收集有關各個雲端客戶如何從各種資源池中分配和使用 IT 資源的使用和計費資訊。
- **遠端管理系統**：此機制用於與後端系統和程式互動，透過前端入口網提供資源池管理功能。
- **資源管理系統**：資源管理系統機制為雲端客戶提供管理資源池的工具和權限管理選項。
- **資源複製**：此機制用來為資源池產生新的 IT 資源實例。

13.3 動態擴展架構

動態擴展架構是一種觸發預先定義擴展條件時，會從資源池中動態分配 IT 資源的架構模型。動態分配資源可以根據使用需求的波動調整使用率，且無須人工介入即可有效回收不必要的 IT 資源。

自動擴容監聽器設有工作負載閾值，用來指示何時需要增加新的 IT 資源到運行中的工作負載中。此機制可以提供邏輯來確保根據個別雲端客戶的配置合約條款動態提供多少額外的 IT 資源。

以下為常用的動態擴展類型：

- **動態水平擴展**：根據負載的波動來擴展和縮減 IT 資源實例。自動擴容監聽器會監控請求的狀況並根據需求和權限向資源複製機制發出信號，啟動 IT 資源複製。
- **動態垂直擴展**：當需要調整單一 IT 資源的處理能力時，會對 IT 資源實例進行向上和向下的擴展。例如，可以對負載過重的虛擬伺服器動態增加記憶體，或者可以增加處理核心。
- **動態遷移**：將 IT 資源重新導向具有更大容量的主機。例如，資料庫可能需要從每秒 I/O 容量為 4 GB 的磁帶式 SAN 儲存裝置移至另一個每秒 I/O 容量為 8 GB 的磁碟式 SAN 存放裝置。

圖 13.5 至圖 13.7 展示了動態水平擴展的過程。

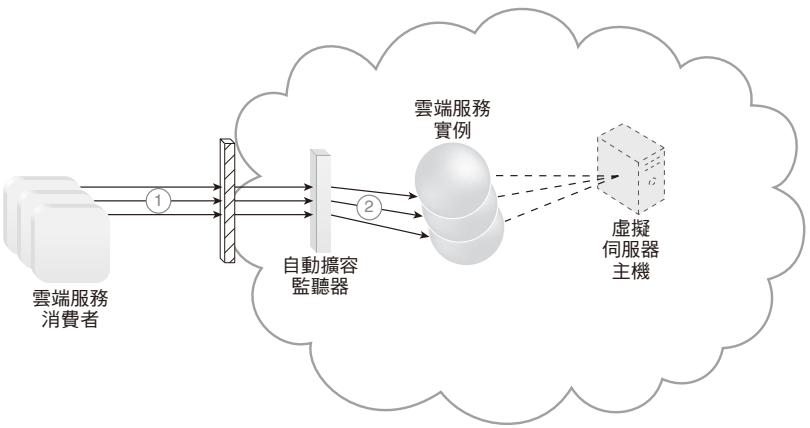


圖 13.5 雲端服務使用者正向雲端服務發送請求（1）。自動擴容監聽器會監控雲端服務，以確定是否超過預先定義的容量閾值（2）。

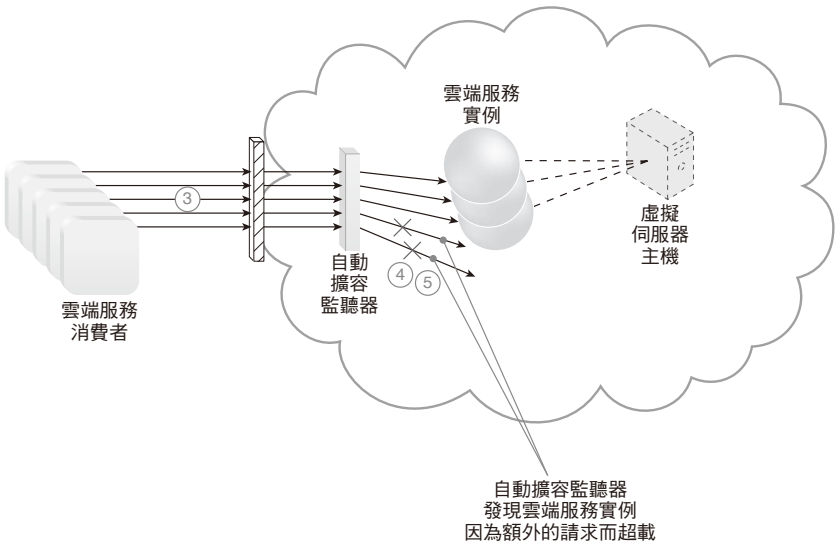


圖 13.6 雲端服務使用者發送的請求數量增加（3）。工作負載超過性能閾值。自動擴容監聽器會根據預先定義的擴展策略確定接下來要採取的措施（4）。如果認為雲端服務可以進行額外的擴展，則自動擴容監聽器會啟動擴展流程（5）。

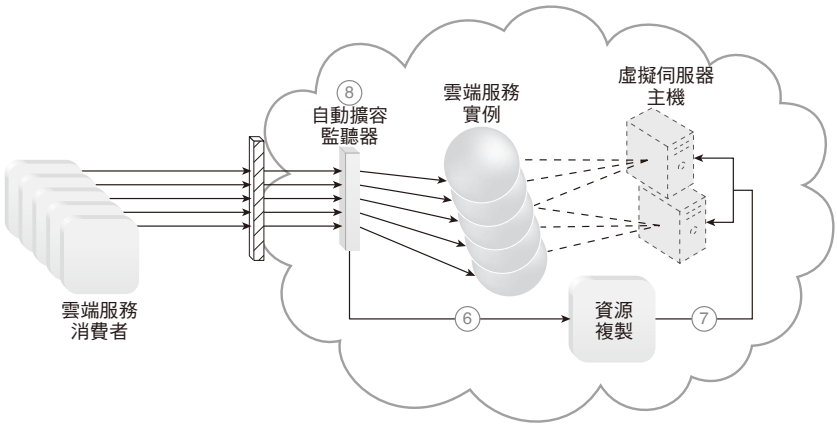


圖 13.7 自動擴容監聽器會向資源複製機制發送信號（6），該機制會建立更多雲端服務實例（7）。現在額外的負載已經得以處理，自動擴容監聽器會根據需要繼續監控和擴展 IT 資源（8）。