



# 中華電信—軟體定義雲端資料中心解決方案

## 1. 簡介

### 1.1 專案背景

近年因雲端服務的普及與技術演進快速，在「基礎架構即服務 (IaaS)」與平台即服務 (PaaS)」的發展過程中，開放原始碼的雲端運算軟體專案 OpenStack 崛起，扮演關鍵的角色。OpenStack 開放式軟體架構的優點為提供使用者低成本、高靈活度，且不被軟硬體廠商綁定的特色。對於企業而言，若要自行建置及管理維運私有雲環境，選擇商用產品提供的平台需額外負擔授權費用，於是許多企業開始考慮強調開放原始碼的 OpenStack。隨著雲端服務的普及，企業目前所面對的是多種雲端服務同時存在的環境，不再只是從公有雲、私有雲當中擇一使用，而是要同時考量如何能夠彼此搭配，而 OpenStack 就具備這種開放式的架構，雖然 OpenStack 成長的腳步飛快，但面臨的挑戰也不少，例如原生 OpenStack 核心尚欠缺一些多租戶應用場域所需的供裝、營運、維護、異動所需的機制與功能，因此原生 OpenStack 用於企業自建私雲的比例偏高。

軟體定義網路 (Software-Defined Network ; SDN) 與網路功能虛擬化 (Network Functions Virtualization ; NFV) 基於彈性的資料傳輸與簡化的管理架構，被視為是下一波網路改革的熱門技術，也是多個國際標準組織與電信營運商紛紛投入研究的領域。SDN 是將網路的控制層和資料層分離，由控制層做中央管控，透過軟體來定義控制不同廠牌的 SDN Switch，讓 SDN Switch 單純做資料的傳輸，大幅簡化網路的管理工作。SDN 與 NFV 的共同點是藉由雲端運算與虛擬化的技術增強網路功能部署的靈活性，節省大量 OPEX 的支出，對營運商來說可按需求提供頻寬、透過 Policy 的動態調度與彈性的服務鏈 (Service Chain) 進行服務的管理。而藉由 SDN 與 NFV 的整合，營運商可提供用戶 Layer1 至 Layer7 的服務應用，滿足用戶的多樣需求。

OCP (Open Compute Project) 為 Facebook 於 2011 年推動的開放式計畫，此計畫公開 Facebook 資料中心的伺服器、儲存系統等硬體規格與建置標準，初期成員主要是雲端服務業





者，目標是致力開放資料中心硬體規格，用以讓供應商能設計出更有效率（尤其是電源）的基礎架構以及更易於擴充規模與維護管理的資料中心。至今近 6 年的發展時間，其高能效的能源使用效率（PUE）已獲得更多資料中心及其他雲服務業者的關注，同時也吸引了電信供應商的加入。目前 OCP 正式成員已超過 200 家，包括資訊硬體供應商以及資料中心營運商。OCP 發展初期，主要是依 Facebook 的需求修改，以導入成本低等特性吸引用戶採用，而由於其開放的特性，更多資料中心營運商及電信運營商也都可提出自己所想的架構，這將大大考驗設備供應商的客製化能力，在因應資訊產業快速變動的環境，硬體供應商必須提昇模組化的產品設計功力，同時也必須加強彈性的管理能力，整廠輸出方面也要兼顧全球營運需求，這對廠商是新一波的挑戰。

隨著企業 IT 朝向雲端轉型需求愈趨旺盛，造就近年來 OpenStack 高速增長的榮景，同時驅使儲存系統邁向分散式、雲端化、開源化，使「軟體定義儲存」議題轉趨熾熱，也讓 Ceph 開放原始碼平台躍為 SDS 市場首選。軟體定義的儲存（Software-defined storage）具備橫向擴充的儲存架構且支援各種儲存方案，包括私有雲和混合雲的建置（包含支援區塊式儲存、物件式儲存、檔案系統層級儲存），日後要支援更多類型的儲存環境，也能繼續延伸。Ceph 的優點非常多，在 OpenStack 應用環境下固然相當熱門，然而，若應用在企業級的資料中心環境，仍有不少部分需要改良。例如在儲存效能部分，Ceph 採開放式架構，然而本身能否提供最佳儲存效能，則需要進一步調校。但由於能同時支持多種儲存形式、規模與容量易於擴展、高可用性等優勢，Ceph 已成為許多人建置 OpenStack 環境時搭配的儲存系統首選。

## 1.2 案例特點

本案採用供裝平台是選擇開源的雲平台 OpenStack，它支持多種虛擬化環境如 KVM、Xen、VMware 等，並且其服務組件都提供了 API 接取，便於二次開發。OpenStack 通過各種補充服務提供基礎設施即服務 Infrastructure-as-a-Service（IaaS）的解決方案。每個服務都提供便於集成的應用程式接口 Application Programming Interface（API）。OpenStack 邏輯架構如圖 1-1（出自 Cloudscaling Group, Inc）：



# OpenStack (m)Architecture Slide

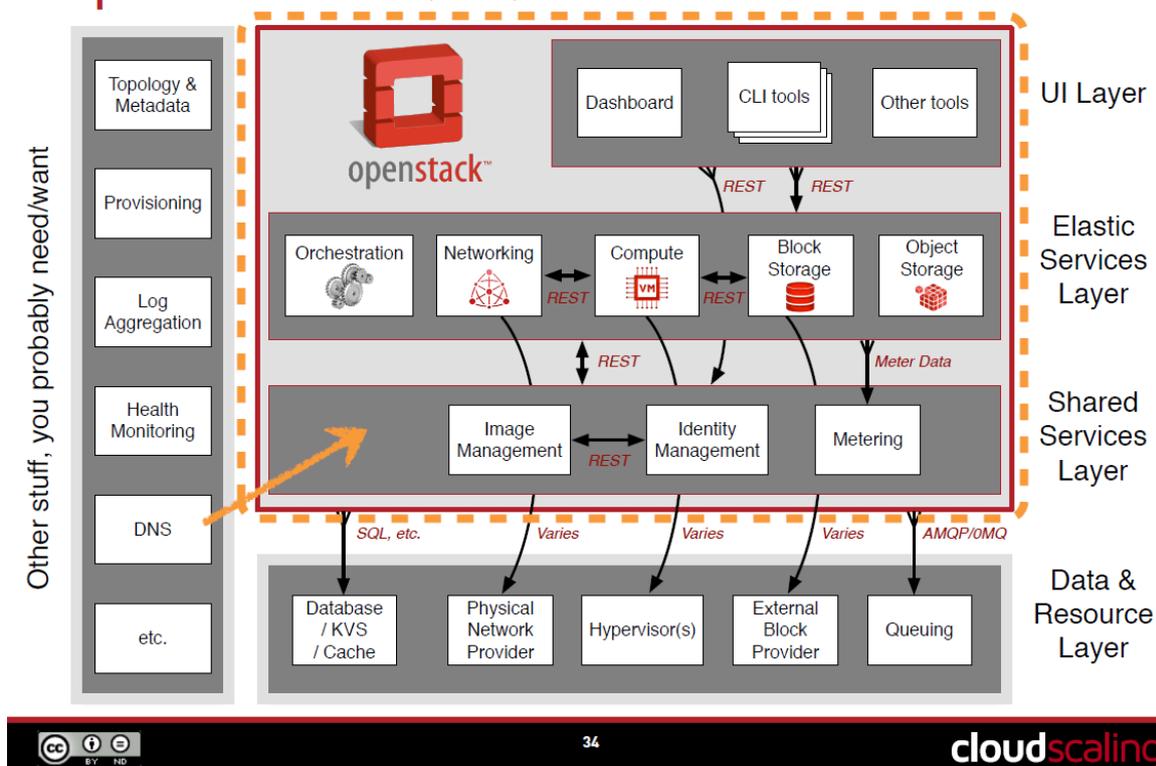


圖 1-1：OpenStack 邏輯架構

資料來源：Cloudscaling Group

OpenStack 本身是一個分布式系統，不但各個服務可以分布部署，服務中的組件也可以分布部署。這種分布式特性讓 OpenStack 具備極大的靈活性、伸縮性和高可用性。OpenStack 的各個服務之間通過統一 REST 風格的 API 調用，實現系統元件界面的彈性。另本案採模組化的方式進行建置，延續 OpenStack 水平擴充之能力，依據使用量視需進行水平擴增。單一區域 (Region) 最高可容納 200 台之實體主機提供服務，並透過多區域的概念進行建置，兩個區域即可達到 400 台實體主機之規模。

原生 Openstack 核心欠缺不少多租戶應用場域所需的供裝、營運、維護、異動所需的機制與功能。本案針對使用者體驗、營維等需求研發並提供營運完整優質服務，包含具備集中管控



多機房服務供裝、多資源池管理、NFV 生命週期管理、簡化管理複雜度與維持一致性的防火牆設定、虛實資源統整管理、擴充與 SDN 網路拓撲等友善的使用者操作介面與營運商等級的營維管理工具。雲端資源管理與服務示意圖如圖 1-2：

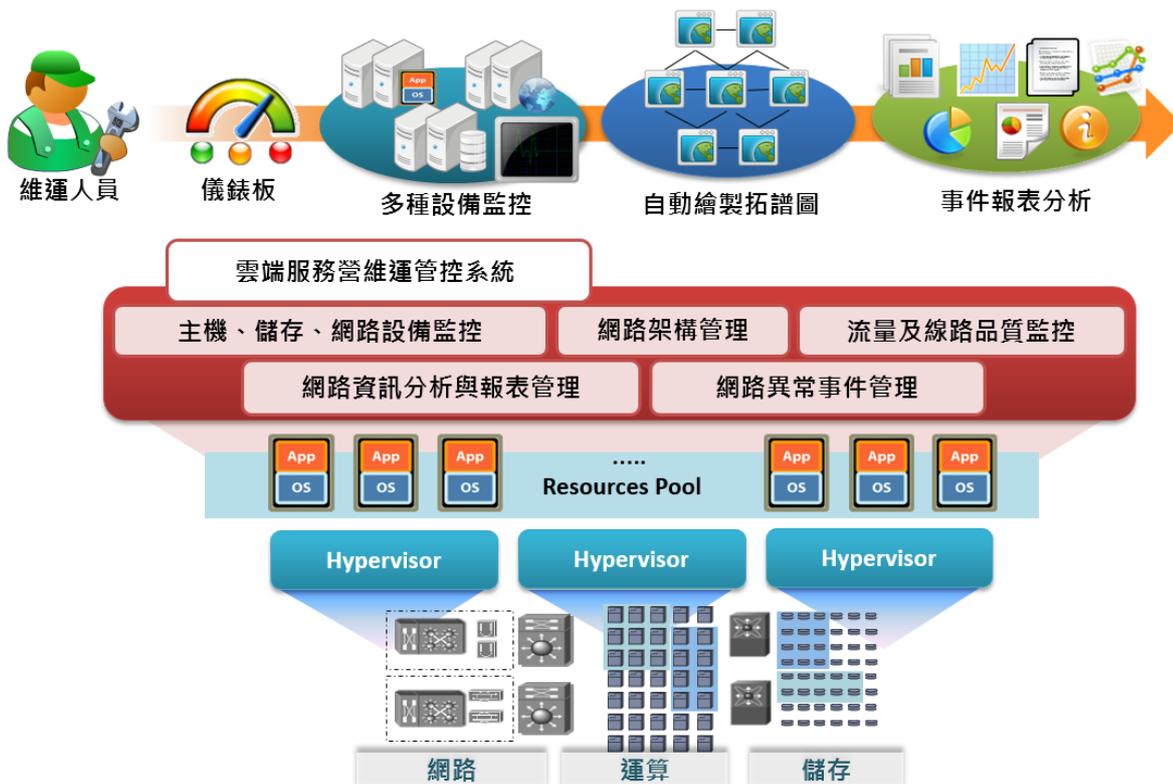


圖 1-2：雲端資源管理與服務示意圖

資料來源：中華電信

## 2. 需求分析

IDC 預測到 2020 年，全球整體的雲端 IT 基礎架構支出達到 595 億美元，年成長率為 13.1%，另外，進一步觀察公有雲和私有雲的變化，預期全球雲端服務供應商將花費 384 億美元在 IT 基礎建設上，以提供公有雲服務，另外，在私有雲的 IT 基礎建設支出則將達到 211 億美元。

雲端技術的應用為企業帶來的好處包括提升 IT 資源的使用率、提高 IT 部署的靈活性、縮短系統供應作業時間、符合節能減碳之環保潮流，吸引企業投入資金採用雲端技術的解決方





案，而帶來莫大的潛在商機。而經過這十多年多來的發展，雲端運算已邁入成熟期，開源陣營儼然已成為商用方案的第三勢力。現在雲端服務追求的是技術與服務能量的提升，為了不讓雲端服務被單一商用軟體鎖定（vendor lock-in），尋求自主與採用開源是必要的，而 OpenStack 則是目前最熱門、活躍的一個雲端開源陣營的解決方案，各大廠包含虛擬運算、網路、儲存等領域都積極參與其中。OpenStack 技術市場預估將從 2014 年 8.83 億美元，成長到 2018 年 33 億美元，CAGR 達 39%。目前 OpenStack 平台經過多次改版已日趨穩定，功能也逐漸齊全，許多企業已建置 OpenStack 提供企業內部運作環境，甚至進一步提供外部客戶應用服務，其中不乏知名大型業者如美國電信商 AT&T、消費電子零售商 Best Buy、線上購物網站 PayPal、跨國零售企業 Walmart、Cisco 線上會議服務 WebEx、美國有線電視提供商 Comcast、南美洲最大拍賣網站 Mercadolibre 等等，業已遍及超過 168 個國家、超過 500 個機構採用。

軟體定義資料中心（Software Defined Data Center）在企業 IT 數位轉型浪潮中，扮演技術升級關鍵角色，推升相關商機蓬勃發展。根據統計，2016 年全球 SDDC 市場規模達 256 億美元，預估 2021 年可上看 832 億美元，年複合成長率 26.5%。相較於傳統資料中心，在虛擬環境中，軟體定義資料中心（SDDC）可快速建置一個全新的應用環境並提供一個整合性解決方案，能同時支援傳統企業應用並佈署新型態的雲端服務。透過其帶來的技術變革，資料中心整體使用率得以提升，並提高生產力，進一步降低資本支出及營運成本。同時可在數分鐘內即刻因應業務需求，配合既定的政策，快速佈署應用服務。

軟體定義資料中心（Software Defined Data Center）興起，將伺服器、儲存與網絡等虛擬化，可有效降低成本與管理的複雜度。若再將其服務內容進行資料整合、系統軟體化自動管理，以減少 IT 提供服務和資源給使用者端的時間，是企業 IT 轉型目標，也是企業營運最急迫的任務。



### 3. 解決方案

#### 3.1 總體技術架構

本案係建置一個以開源、軟體定義為主的雲端資料中心環境，以 OpenStack、SDN（Software Defined Network）、SDS（Software Defined Storage），結合 OCP 綠能伺服器等相關技術，提供雲端產業之軟硬體發展環境。

本案提供一完整的發展解決方案，包含雲服務應用、雲端服務平台、雲端作業系統、SDN 網路、OCP 綠能、儲存管理系統、網路管理系統等，整體系統架構示意如圖 1-3 所示：

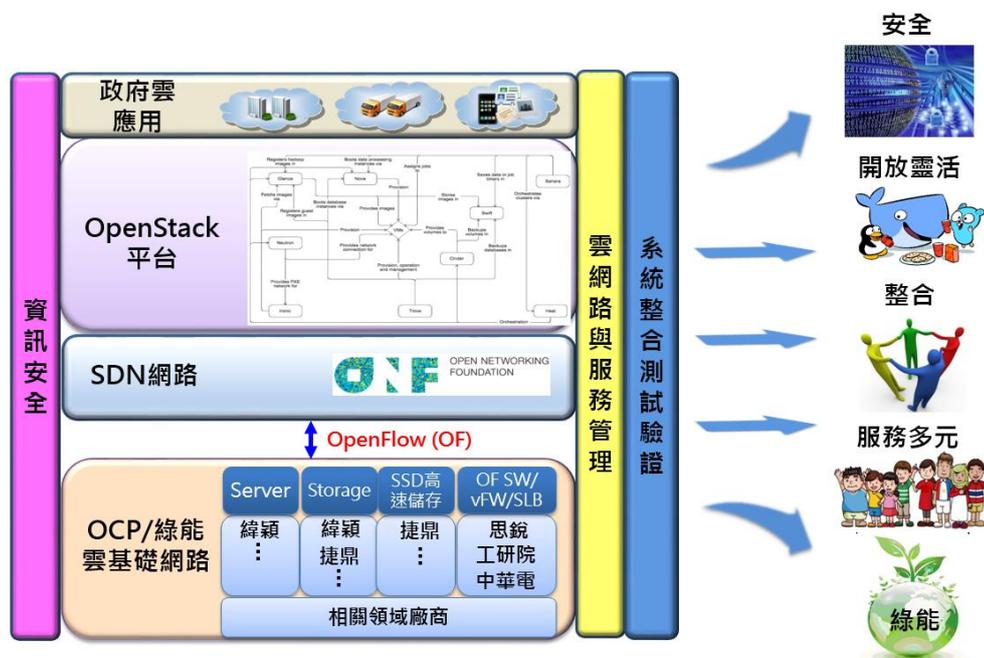


圖 1-3：整體系統架構示意圖

資料來源：中華電信

#### 3.2 具體技術方案

本案架構具體技術方案分述如下：

##### 3.2.1 雲端作業系統



雲端作業系統以 OpenStack 為基底進行整合開發，其整合架構如圖 1-4 所示，並分別描述

說明：

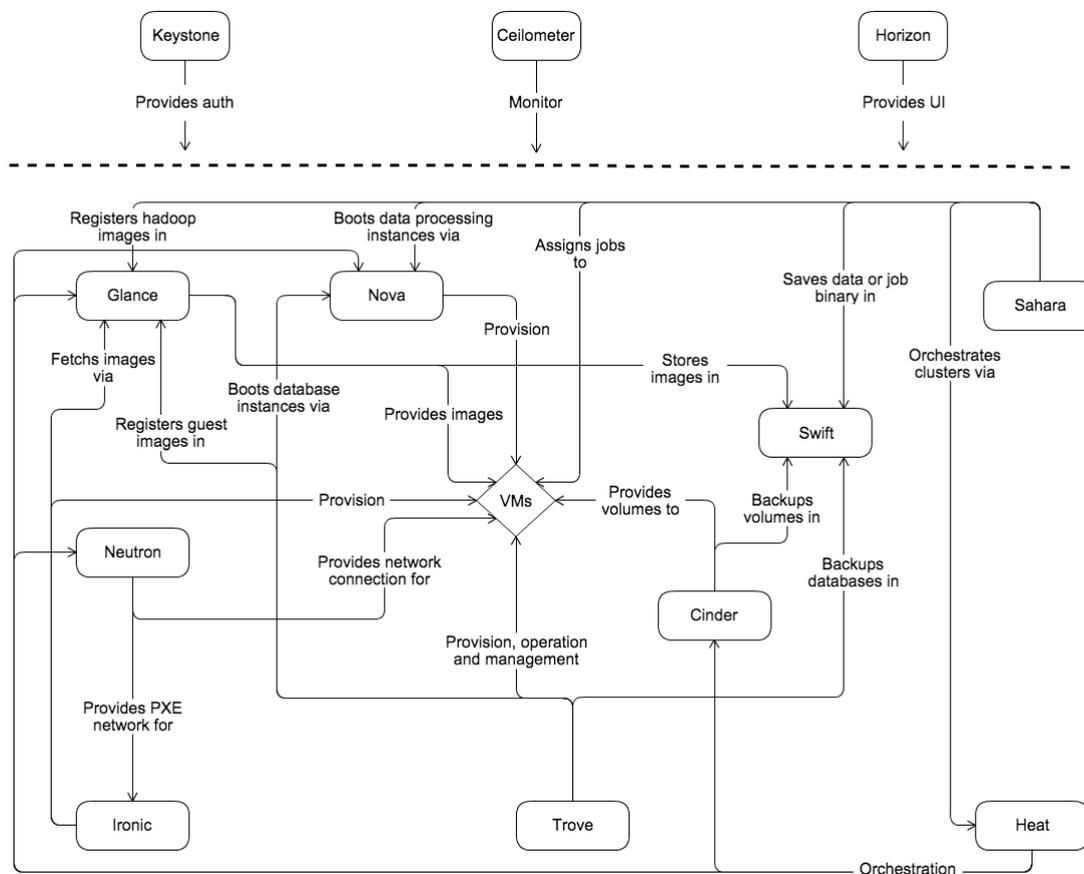


圖 1-4：雲服務平台整合架構圖

資料來源：OpenStack

採 OpenStack 作為佈建的環境平台，以 MaaS 結合 JuJu 快速佈建主要服務元件具高可靠度的作業環境，並整合以 SDN 為主體的第二層網路管理服務及實體資料中心管理系統，進行實體設備的裝置管理。Kilo 版本主要套件包括：Nova, Neutron, Cinder, Swift, Glance, Ceilometer, Heat, Horizon, Keystone, Trove, Sahara, Ironic，相關功能摘要如下：

- Nova：主要提供運算服務，管理實體資源與虛擬資源間的配置，其支援的虛擬化技術包括KVM, VMware及XEN，此外，它也支援LXC。
- Neutron：主要提供網路服務，透過API來管理的網路架構系統。





- Cinder：主要提供區塊儲存服務，除了提供本地端儲存資源服務外，它可支援的儲存架構包括Ceph, CloudByte, Coraid, EMC及自行研發的儲存管理。本案主要提供Cheetah及Ceph，提供分散式的儲存架構。
- Swift：主要提供物件儲存服務，使用者可透過API進行存取，可存放非結構化的資料；此外，可以透過swift的邏輯，確保資料被複製與分布在不同設備上。
- Glance：主要提供硬碟或伺服器的映像檔尋找、註冊以及服務交付等功能。
- Ceilometer：主要提供資料監控服務，藉由監控與收集CPU、網路等資源使用情況作為量測的基準，提供計價並可與Heat整合作為虛擬機自動生成的依據。
- Heat：主要提供一個以模板為基礎的架構，使用者可以藉由此模板建立如虛擬映像實體（Instance）、浮動IP位址、安全群組（Security Group）或是使用者等OpenStack各種資源。
- Horizon：主要提供圖形化的網頁管理介面，讓管理人員可以查看目前的規模與狀態，並且，藉由此介面能夠統一存取、部署與管理所有雲端服務所使用到的資源。
- Keystone：主要提供 OpenStack的身分認證系統，具有中央目錄，能查看使用者可存取服務項目，並提供了多種驗證方式，包括使用者帳號密碼、Token以及類似AWS的登入機制。
- Trove：主要提供各個服務一個具延展性且可靠的雲端資料庫服務（Database-as-a-Service）。
- Sahara：主要提供Hadoop佈署與管理的架構。
- Ironic：主要提供裸機佈署功能，本案是採Ubuntu Canonical所提供的MaaS作為裸機佈署。
- 支援HA備援運行架構。



- 
- 支援運行管理超過250個以上高密度實體伺服器節點之設計架構（具可管理超過10,000台以上VM之服務架構）。
  - 支援VM live migration，實體機故障時可於10分鐘內移轉完成。

### 3.2.2 雲端服務平台

- 提供單一用戶入口依需自主申租佈署虛擬私雲平台，申租與管理各項雲服務，如：虛擬機、儲存空間、防火牆、負載平衡、跨虛擬私雲之用戶服務監控儀表板等。
- 提供單一維運入口進行多機房整合資源管理，提供資源使用分析、使用量計費、障礙派工、供裝異常維運機制、（跨）機房資源使用Dashboard等。

### 3.2.3 儲存管理系統

- 儲存管理系統包含Deduplication（去重複）、Replication、Snapshot（快照）、Local/Remote Backup/Restore、多複本管理、遠端快照與備份還原等功能。
- 災難復原計畫對IaaS營運商而言是一個重要的營運功能，在本案中，災難復原計畫包括備份與復原的程序及兩個重要指標，包括：復原點目標（Recovery Point Objective, RPO）與復原時間目標（Recovery Time Objective, RTO）。其中RPO定義了發生災難事件時可接受的最大可容忍資料遺失。RTO定義了最大可容忍時限。若使用者選擇儲存型態為DMS Volumes的VMs，其Volumes已經受到完整的保護；其中Volume replication保證每一個block都至少有2份以上且儲存在不同data node；而local snapshot與remote snapshot的技術保證volume可以藉由backup policy進行本地端或遠地端的備份；因此，我們可以將volume經由local restore或remote restore還原至指定的時間。故以volume層次，其RPO，我們可以回復至上次最後一次的備份點；其RTO，因為只有volume回復，故其相對應的虛擬機down time時間非常短，但整體營運未受影響。

### 3.2.4 網路管理系統





不同於傳統資料中心網路架構是採用 Layer 2 交換器和 Layer 3 路由器的典型組合，本案在不需額外硬體支援下，可整合現有的乙太網路交換器、SDN Switch 及 Open vSwitch (OvS) 提供 SDN 服務，藉此滿足雲端資料中心擴充性、快速故障轉移及多租戶的需求。相關功能摘要如下：

- 提供多租戶虛擬網路隔離功能，同時透過NFV技術來導入軟體式網路功能，提供用戶防火牆及負載平衡等網路功能服務。
- 支援線路與交換機備援。
- 提供實體網路拓樸與實體網路即時流量資訊。
- 提供虛擬網路拓樸與虛擬網路即時流量資訊。
- 提供同虛擬網路中的虛擬機網路即時流量資訊。
- 管理者可觀察每個虛擬機的網路封包。
- 整合NFV及SDN技術，使用者可快速建立虛擬私雲並開通網路。
- 提供管理者整合管理虛實SDN網路、VNF等管理功能。

### 3.3 解決方案特點

本案架構與解決方案具備以下特點：

- 提供完善的虛實資源統整管理與彈性的運算、儲存、網路等虛實資源管理。
- 多元的服務自動開通，支援多類虛擬私雲服務，依需自主快速建置專屬虛擬私雲。
- 無縫的應用系統整合交付，結合DevOps持續交付流程，自動化整測、更版、部署並監控運作情形，實現應用系統快速交付。
- 彈性的虛擬私雲網路架構，以SDN技術設計標準化網路架構，具備彈性擴充的特性，能動態開通網路服務。



- 可靠的網路資安防護方案，虛擬私雲網路彼此隔離，搭配軟體式防火牆增強資安保護。整合OpenFlow通訊技術，管控虛擬、實體交換器，強化虛擬化平台資安防護。
- 穩定的異地備份備援機制，整合備援方案，提供檔案、應用軟體層級備份備援。
- 主動的虛實資源整合監控，完整事件關聯分析，掌握資源異常潛在影響服務範圍、完善資安稽核機制，存錄各式資源、服務等異動事件，有效預防不當的操作行為。
- 完善的障礙處理回覆流程與線上問題受理，結合企業人事組織進行障礙處理作業、事件告警規則設定、稽催、升級通報等功能。

## 4. 總結

### 4.1 經濟/社會效益

本案相關重要成果與效益分項說明如下：

#### (1) 雲端管理系統

植基於 Openstack 及其它各類開源方案，整合軟體運算、軟體網路（SDN、NFV）、軟體儲存（SDS）與 Container 管理等關鍵技術，提供資料中心 IT Infra 及自動化協作、營管機制。同時研發原生 Openstack 核心所欠缺的多租戶應用場域、供裝、營運、維護、異動等相關機制與功能，並完成與下層 SDN 網路的整合，提升軟硬體資源使用效率及應用佈署彈性，增進企業 Business Agility 並節降營運成本。

#### (2) OCP 與節能發展

OCP 硬體提供了許多優點，同時也定義了新的管理方式。本案整合 OCP 機櫃、機箱、主機、電源等管理單元，提供單一監控儀表讓管理者可以快速掌控機房軟硬體的的健康狀況。並且利用蒐集的資料發展自我診斷、修復與海量資料分析，為全自動化雲端資料中心建立基礎。在執行本案期間，獲得完整的服務流程經驗，得到有效導入 OCP 方法與成功案例。提供給公部





門及雲端服務供應商更多的選擇性，提高軟硬體廠商的競爭力。透過 OCP 的導入，使得資料中心 PUE 降低至 PUE1.5 以下。

### (3) 整合驗證與技術驗證

本案測試多款伺服器、儲存設備、SDN 網路交換器與雲端平台，並完成相關功能性與非功能性品質驗證作業，並將通過的設備，實際運用於目前專案的環境中。本案並提供相關建議與結果給廠商，請廠商依照相關建議進行修正，並清楚掌握每個設備所需的規格與效能。本計畫完成設備與平台的互聯整合性驗測，且通過相關安全性驗測。本案之整合驗證平台建置架構如下圖 1-5：

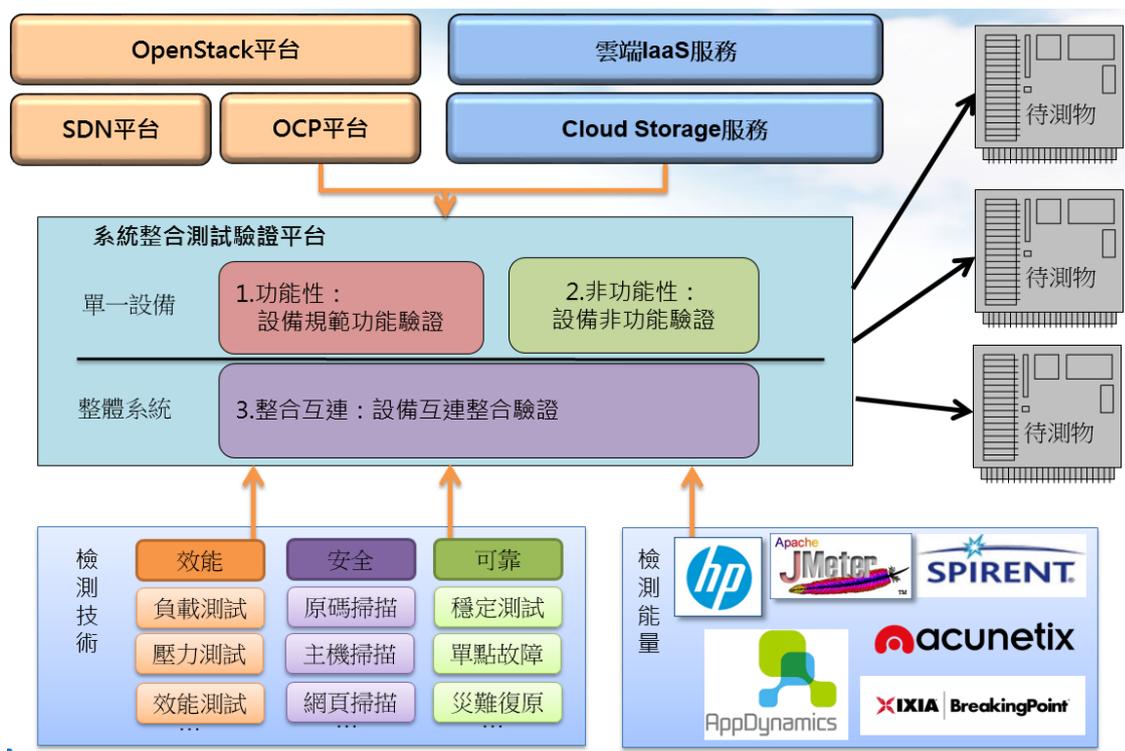


圖 1-5：整合驗證平台架構

資料來源：中華電信

本案完成整體服務驗證規劃與執行，包含 IV&V、第三方驗證、使用者驗證、跨地區案場、多樣態服務、SLA 六大部份。並透由中華電信研究院測試中心與財團法人資訊工業策進會（簡



稱資策會) IaaS 雲端特性驗測來提昇本案產品力與強化服務品質。產品於開發完成後進行第三方之產品獨立驗證與確認測試 IV&V (Independent VER&VAL)，並依據 ISO/IEC25010 品質指標及 CMMI 流程規範，設計出測試執行流程，規範相關單位於適當的時間點進行審查，為本案平台品質作分析及把關。相關驗證包含功能性測試、易用性測試、安全性測試、效能性測試、可靠性認證等測試。

#### (4) 成果發表

本案參與 WCIT 2017 世界資訊科技大會展覽，帶動技術創新與社會效益。透過參展，展示中華電信與合作夥伴長期深耕雲端的相關基礎建設及研發之成果，加強與全球資通訊產業之交流與合作，推廣及行銷資通訊產品，展現國際競爭力。

本案亦提昇相關產業研發能量並建立完善的制度，透過自主雲端服務之技術能力，提升研發能量，透過整合採用 Openstack、SDN (Software-defined networking)、DFS (Distributed File Systems) 等各領域之技術，提供雲端服務與營維機制，應用於不同領域案場。

## 4.2 用戶評價回饋

本案完成整體服務驗證規劃與執行，包含 IV&V、第三方驗證、使用者驗證、跨地區案場、多樣態服務、SLA 六大部份。

本案於第三方驗證部分通過資策會第三方雲端服務 IV&V 驗證測試，驗測面向涵蓋 VM 管理功能、網路管理、儲存管理、部署管理、可靠度、資安防禦、操作反應時間、使用者介面 (UI)、API、計費管理、服務管理、資安服務等 12 大面向。在使用者體驗之設計與操作亦獲得好評。

在 SLA 部分，為強化服務驗證的廣度、持續度與多樣性，本案團隊積極協助與完成公部門導入多個正式系統，滿足多樣態、跨地區需求。相關系統與案場均通過各單位所訂定的服務面向及平台面向測試。目前平台的 SLA 持續維持 100%。





### 4.3 總結

本案植基於 Openstack 及其它各類開源方案，整合軟體運算、軟體儲存 (SDS) 與 Container 管理等關鍵技術，提供資料中心 IT Infra 及自動化協作、營管機制。

本案之資料中心也透過導入 SDN 軟體式網路技術，提供 SDN 動態供裝及設定網路路徑功能，也整合多種 SDN 增值網路服務，包含網路流量監控分析、網路多路徑分流、虛擬網路服務 NFV 串鏈 (Service Chain) 等網路功能，透過完整緊密結合 SDN 與 NFV 使資料中心成為新世代 SDDC (Software Defined Data Center)，可滿足雲端資料中心五個特性與七大項需求。規劃之架構係在基礎設施建構上搭配綠能機房設施與經過 ISO 50001 認證之完善能源管理，並建置一套完備的雲端服務營維運管控系統以服務遞送、資源統合協作、服務監控與管理等三大面向之架構規劃，搭配資安服務，提供服務水準保證，完整涵蓋 (1) 資料中心基礎服務需求、(2) 建置用戶服務管理系統、(3) 虛擬化資源動態調配及統合管理服務、(4) 監控及告警服務、(5) 維運管理等需求。

中華電信多年來致力台灣社會資通訊發展及服務，並獲得多項肯定，除為台灣最大家電信業者外，亦為台灣擁有最多最快速骨幹網路、最多光纖網路、最多國際海纜、最多 IDC 資料中心機房據點及服務能量之業者。中華電信於 2016 年啟用之中華電信雲端資料中心，是台灣最新且最大之 IDC 機房，符合 TIA-942-A Rated 3/Rated 4，可供企業作為混合雲架構之用。

中華電信可協助企業進行 SDN 網路規劃，並利用 SDN 技術提供多種 IDC 機房間連線服務及 IDC 內網路架構。

中華電信在 SDDC 上之發展，可作為企業私有雲之運作核心，搭配既有之 hicloud 公有雲服務，成為可因應各式資訊應用服務需求之混合雲架構。

