

在企業中採用軟體定義網路

透過可程式化的介面來虛擬化網路資源，我們能夠為 Intel 應用程式開發人員提供最佳的支援

執行概覽

Intel IT 採用軟體定義網路 (SDN)，提供隨選配置的網路資源和網路服務。透過可程式化的介面來虛擬化網路資源，我們能夠為講求效率和靈活度的內部客戶 (Intel 應用程式開發人員) 提供最佳的支援。這些客戶必須能夠迅速存取網路資源，並避免因網路組態和配置服務而造成瓶頸。

SDN 不但可以協助我們提高資料中心虛擬機器 (VM) 的商業價值，還可能實現下列優勢：

- 縮減網路配置時間
- 透過自助式的環境，有效簡化網路的配置程序
- 藉由提升網路管理效率，有效降低服務成本

SDN 產業最近提升了 SDN 元件的各項效能和可擴充性。過去這兩年來，我們一直在評估下列各項，以判斷部署 SDN 的效益：

- 定義哪些使用案例需要部署 SDN

- 測試與分析不同的 SDN 架構，以瞭解各個節點之間的資料流向
- 更新員工的角色和職責，屆時負責在自助式環境中建立網路的員工，他們可能不具備網路工程背景

我們將陸續採用 SDN 並在整個虛擬環境中部署，我們也會繼續評估如何運用 SDN 元件和架構，來為客戶排除網路服務的障礙，協助他們更快速且順利部署應用程式。

Sridhar Mahankali
雲端網路工程師，Intel IT

Sanjay Rungta
資深首席工程師，Intel IT

內容

執行概覽	1
商業挑戰	2
在我們的資料中心發展雲端事業：儲存、運算和網路	2
可預期之可編程虛擬網路的商業利益	2
解決方案	3
選擇 SDN 架構	3
重疊網路架構	4
變更安全性架構	5
變更角色和責任	5
初步結果	5
後續步驟	6
結語	7
相關資訊	7
英文字母縮寫	7

IT@INTEL

IT@Intel 計畫將透過組織內部同儕來與全世界的 IT 專業人員連結，並分享學習的課程、方法和策略。我們的目標很簡單：共同分享可創造商業價值和 IT 競爭優勢的 Intel IT 最佳準則。請立即造訪 <http://www.intel.com.tw/content/www/tw/zh/it-management/intel-it/intel-it-best-practices.html> 或與您當地的 Intel 代表聯繫以取得更多資訊。

商業挑戰

Intel IT 在 64 個資料中心運作約 55,000 部伺服器，支援 104,000 名以上的員工。¹ 十多年來，Intel IT 一直在虛擬化辦公室、企業和服務資料中心環境中的伺服器。

在 2000 年，佈建虛擬機器 (VM) 需要 90 天以上的時間。現今，我們可以隨需佈建 VM 以加速開發應用程式之業務單位 (BU) 的行銷。有 85% 以上的辦公室、企業和服務資料中心的工作負載都在 VM 上執行。然而，網路資源依舊有隨需佈建的瓶頸，尤其是在我們辦公室和企業資料中心內。因此，我們需要找解決方案來加速網路服務佈建，以提升業績表現。

在我們的資料中心發展雲端事業：儲存、運算和網路

如表 1 時間表圖解所示，我們可以將 Intel 對虛擬技術的使用回溯到 2000 年。在 2009 之前，只有 12% 的企業運算環境有虛擬化。在那段時間內，佈建 VM 需要 90 天以上的時間，而且虛擬化環境的穩定性時有變數。

¹ 為了定義「資料中心」，Intel 使用 IDC 的資料中心大小分類：「任何裝載伺服器和其他基礎架構元件，且大於 100 平方英尺的空間。」

在 2009 年，我們開始將大部分的辦公室和企業資料中心伺服器環境虛擬化。三年後的 2012 年，已有 75% 的企業運算環境虛擬化，可隨需進行運算佈建，可用性高達 99.7-99.9。2014 年開始之後 (85% 的企業運算環境虛擬化)，我們打算繼續虛擬運算、儲存和網路服務，以及支援這些服務的隨需佈建。這可幫助我們跟上大幅增加的 Intel 應用程式開發生態系統。

若使用在 SDN 模型之前所使用的舊型網路佈建模型，佈建網路需要四到六小時工作時間，若再加上開工停工、要求佈建網路衍生的待處理項目，以及其他複雜度等等，網路佈建流程可能需要 13 天時間才能完成。串聯其他應用程式登陸工作的延遲，例如安全設置、區域及全域負載平衡及網域名稱系統 (DNS) 組態。

為跟上需求大量增加的腳步，我們需要轉換為在辦公室和企業資料中心伺服器環境部署可編程的網路元件，如此就能隨需大量佈建。當利用虛擬 LAN (VLAN) 和虛擬路由及轉送 (VRF) 技術在實體網路上虛擬化某些特定網路資源時，這些技術本身並無可編程功能，而這偏偏是自動化和自助式服務所必需的。

表 1. 自 2000 年以來，我們從小量虛擬機器 (VM) 進展到 2010 年私有雲端到現今的混合雲端。

	2000-2009	2010	2012	2014+
	傳統主機代管	主流虛擬化	INTEL CLOUD 1.0	HYBRID CLOUD 2.0 融合式雲端服務
虛擬伺服器	12%	42%	75%	85%
佈建	90 天以上	10 天	隨需運算	隨需運算、網路和儲存
服務請求	手冊	手冊	部分隨需	完全自助式服務
可靠性	變數伺服器可靠性	99.7% VM 可靠性	99.7%-99.9% 可用性	99.9% 可用性

可預期之可編程虛擬網路的商業利益

將可編程網路服務元件整合到資料中心網路，有助於加強靈活度，簡化佈建流程，並且減少整體擁有成本 (TCO)。

- **靈活度。** 設定網路和佈建服務如負載平衡器和防火牆等，可能會使整體應用程式登錄程序產生瓶頸。有了可編程的虛擬網路，就可以從集中管理的主控台大幅佈建網路資源，或是利用 API 建置其他客製化自動流程。我們期待在沒有網管人員介入的情況下能隨需佈建大部分的資料中心網路服務。
- **簡單化。** 可隨需佈建的虛擬網路能減輕網管人員的負擔，讓我們的客戶能更輕鬆地為他們的應用程式開發工作製作和管理自己的網路。
- **TCO。** 可自動設定網路設備組態的虛擬網路，能夠減少手動設定個人網路元件的組態。我們希望這個網路可編程全域檢視有助於降低網路營運成本。

解決方案

圖 1 中所說明的軟體定義網路 (SDN) 能力，可協助我們將企業資料中心網路虛擬化，方式和將伺服器虛擬化很類似。SDN 將控制面從資料面切分出來，為網路啟用 SDN 部分提供集中式可編程介面。讓網路元件可編程後，SDN 會提供給較新的多租用戶共享模型及安全存取控制，加強可擴充性，並透過網路應用程式推動快速服務創新。

在企業資料中心網路中，我們一直在建造和採用以 OpenStack* 為基礎的私有雲端環境，提供了整合 SDN 元素的架構。OpenStack 的 Neutron API 可透過開放原始碼和專屬可編程網路元件來佈建、修改和刪除網路服務。

對業界而言，SDN 是相當新的功能，且持續在成熟當中。Intel IT 正在評估 SDN 是否會減少網路佈建時間、簡化佈建網路服務流程，以及降低服務成本。我們的評估重點在於測試及分析 SDN 控制器的效能。SDN 控制器是 SDN 的核心，能呈現每一租用戶網路的邏輯視圖，以及管理網路硬體和租用戶之間的流程控制。

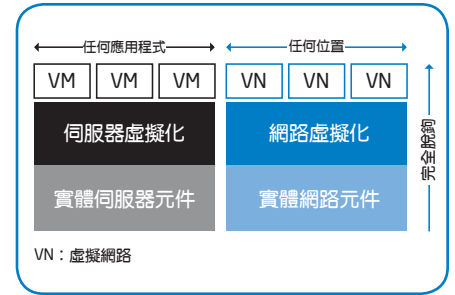


圖 1. 如同伺服器虛擬化作業與實體伺服器完全脫鉤 (decoupled) 建立多部虛擬機器 (VM)，網路虛擬化 (即軟體定義網路 (SDN)) 會從實體網路元件完全脫鉤成數個虛擬網路。

網路進展：從硬體鎖定到開放式軟體

當電腦網路開始普遍化後，只有少數幾個供應商製造硬體 (包括提供技術的矽晶片) 和軟體。如此一來，各公司便需要從不同的供應商採購硬體、軟體和服務才能佈建網路。

當相關產業益發成熟，有些供應商便開始將主力放在開發獨有的硬體組件。自此軟體市場開始大鳴大放，各協力廠商開始開發和擴充軟體功能。

當軟體定義網路 (SDN) 問世後，各公司就可以為軟體開發制定規範，使軟體更加開放。我們相信 SDN 能幫助排除侷限於特定供應商，同時又能簡化和自動化網路佈建程序。

選擇 SDN 架構

我們的評估顯示可用兩種方式實作 SDN。其中一種方式是使用 OpenFlow*，這種開放標準通訊介面允許直接存取及操控交換器轉送 table。另一種方式是使用重疊網路 (overlay network)，其包含建構在現有網路上之節點和邏輯連結。其所建立的網路服務在現有實體網路並無法使用，其中每一個邏輯連結可能是由基礎網路中的多個實體連結所組成。

OpenFlow 需要新的硬體來支援 OpenFlow 轉送 table。重疊網路不需要任何其他硬體，因此不需要投資新設備。此外，OpenFlow 有不同版本，不是所有的 SDN 控制器和網路硬體供應商都支援相同版本。當資料流可變更，且網路需要根據資料流的變動來重新編輯時，OpenFlow 便很適用。然而，我們沒有同質性硬體環境，且由於我們的來源和目標節點之間的資料流在建立後通常可預測，所以重疊模型能比 OpenFlow 模型提供我們更多價值。

從 2012 到 2013 年中，我們用多重架構測試四種 SDN 控制器，範圍從重疊架構到啟用 OpenFlow 的架構。測試準則包含網路頻寬和效能基準測試。圖 2 解說我們的測試系統。

我們分三階段執行測試：

- **階段 1：SDN 控制器效能問題。** 這個測試階段在 2012 年初時支援 SDN 概念的有效性，並且確認某些效能問題是我們測試過所有 SDN 控制器都會發生的問題。這些問題需要在我們採用技術之前先由業界共同解決。例如，一個沒有重疊網路之 10 Gigabit Ethernet (GbE) 網路的測試情境結果顯示了兩個 Hypervisor 上兩部 VM 的 9.39 Gbps 傳輸量。而使用重疊網路的相同設定則顯示只有 3.3 Gbps 傳輸量。在 Hypervisor 增加更多 VM 並不會使效能提升，這表示重疊驅動程式未進行最佳化。
- **階段 2：可擴充性難題。** 這個測試階段在 2012 年末和 2013 年初進行，雖然

傳輸量有增加，卻遇到可擴充性難題。我們發現架構無法隨著大量 VM 和資料流擴充。每一次通訊帶來新的資料流，卻沒有終止，造成通道數量也在大量 VM 間擴增。

- **階段 3：最佳化資料流。** 在 2013 年中進行的最後測試階段顯示，產品供應商已處理資料流擴增問題，而且軟體也更成熟和穩定。雖然不同供應商處理問題的方式各異，但都得到相同結果，就是每一部 VM 不需要傳播到其他 VM 就能維持通訊，且都會根據來源和目的位址將資料流的建立最佳化。

重疊網路架構

SDN 重疊網路組態提供資料中心最大價值的最佳化資料流。在 2013 年下半年，我們在生產環境中部署重疊網路。圖 3 解說高階 SDN 架構檢視。這種架構有三個主要元件，分別為 SDN 控制器、閘道器節點和 Hypervisor 節點，其可使用虛擬交換器連接 VM。

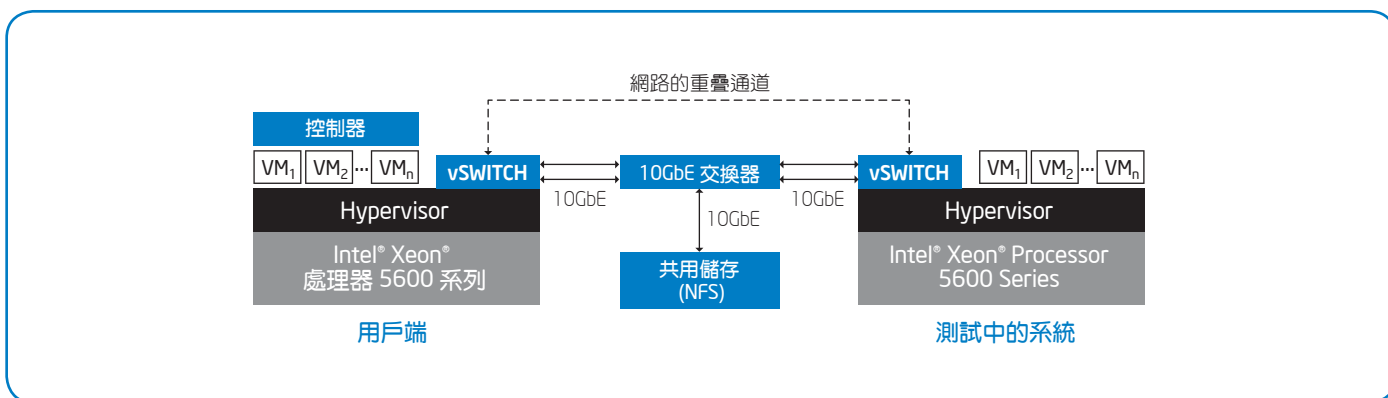


圖 2. Intel 的測試組態。在評估軟體定義網路 (SDN) 期間，我們使用重疊架構來測試及監測 SDN 控制器效能、可擴充性問題和資料流最佳化。

SDN 控制器

SDN 控制器可造就 SDN 網路，方法是將網路從硬體分離出來。控制器（其實就是一種軟體應用程式，不是硬體）主要負責管理應用程式和網路裝置之間的通訊。在大型實作中，會有一個以上的 SDN 控制器創造出 SDN 控制器叢集。

集中式主控台方法可製作出智慧型網路，具有最佳化的通訊資料流和自動化組態設定，以及從單一主控台檢視整體網路等特性。

- **最佳化資料流。**傳統網路具有從通訊資料流來源到其目的地的單一路徑。SDN 控制器可識別資料流的多重路徑，也可分割資料流跨多重節點的流量。SDN 控制器可根據來源和目的節點將特殊資料流的網路路徑最佳化。這些能力可提升網路效能和可擴充性。

- **自動化組態設定。**與傳統手動式一個裝置接著裝置設定的網路組態不一樣的是，SDN 控制器可節省時間，並藉由自動設定網路裝置組態提高組態準確度和一致性。當網路狀況發生變化時，用這個方法可輕易調整組態。最重要的是，SDN 控制器可將整個網路架構當成單一裝置一樣來管理。
- **檢視整體網路。**SDN 控制器的主控台提供網管人員整個網路的全域視野，可提高決策和管理效率。

SDN 控制器的可編程介面提供網管人員比傳統網路更大的網路流量控制權。例如，我們的安全性策略要求特殊伺服器的輸入流量須通過防火牆。而輸出流量並不會對安全造成威脅，因此不一定非得通過防火牆不可。在傳統網路中，要達到這麼細微的控制是很困難的。有了 SDN，非網路工程師的員工都能輕易為控制器編程，將輸

出流量重新導向為環繞防火牆。透過 SDN 控制器可在工作階段、使用者、裝置和應用程式層級套用這些策略。

閘道/服務節點

閘道節點提供整合 VLAN 的實體網路網狀架構與啟用 SDN 的雲端網狀架構的方式，這些都由 SDN 控制器設定和管理。閘道能力有助於整合兩個環境，允許啟用 SDN 的 Hypervisor 與非啟用 SDN 的網路通訊。服務的節點會處理 VM 之間的傳播、多點傳送和資料流建立。

HYPERVISOR 節點

Hypervisor 節點裝載 VM。如圖 3 所示，每一個 Hypervisor 節點執行虛擬交換器模組，是 SDN 控制器為租用戶建置虛擬網路之處。單一 Hypervisor 可裝載數個虛擬網路的 VM。策略控制由 Hypervisor 和 VM 之間的虛擬交換器管理。

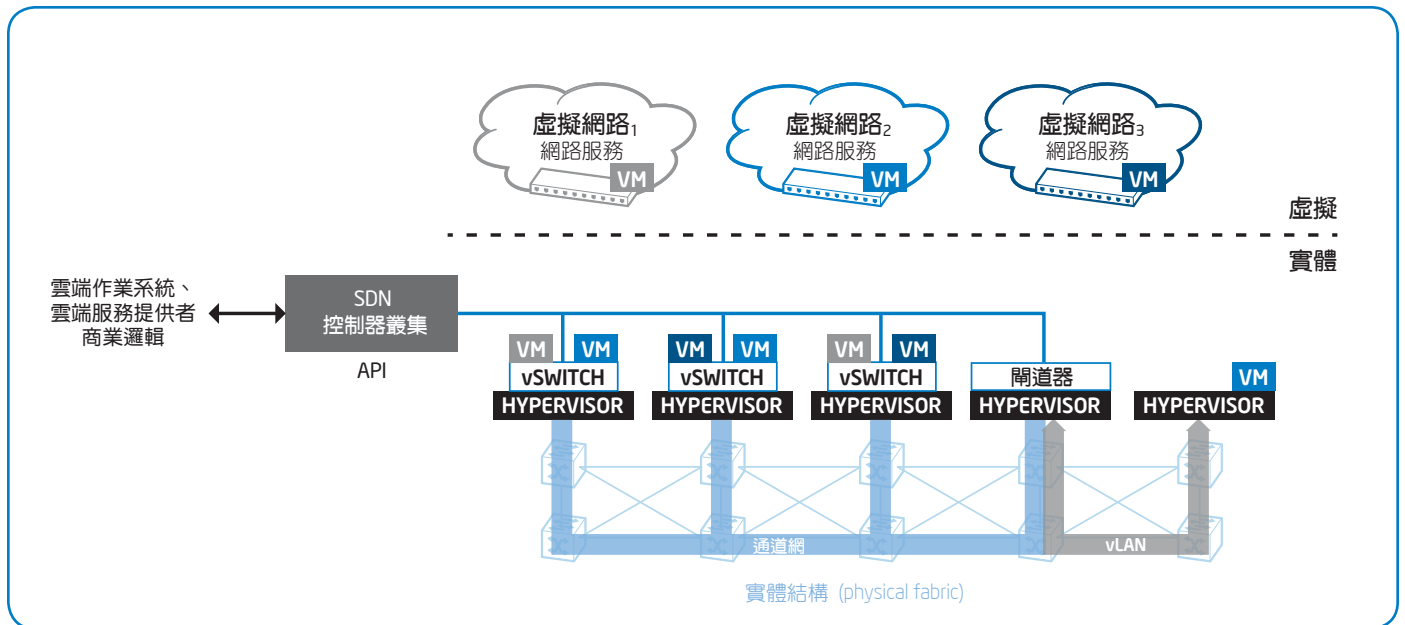


圖 3. 我們的重疊軟體定義網路 (SDN) 架構包含三種主要元件：SDN 控制器叢集、閘道器/服務節點，以及 Hypervisor 節點。最重要的是，SDN 控制器可將整個網路架構當成單一裝置來管理。

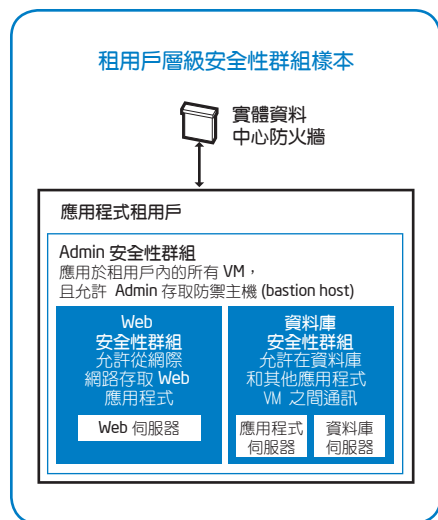


圖 4. 這個安全性群組模型描述結合 OpenStack* 私
有雲端環境與軟體定義網路 (SDN) 功能所提
供的網路存取控制彈性。

變更安全性架構

個人化 (Consumerization) 和其他產業趨勢是促使在網路的虛擬環境中佈建的應用程式增多的因素。傳統上大多使用網路分割和網路控制作為保護 VM 的主要機制。在舊式網路佈建模型中，我們仰賴整合型外部防火牆設備提供細微網路存取權以控制這些和應用程式。這類的功能性模型顯露出可擴充性、支援性和風險方面的困境。例如，在某些環境中，外部防火牆必須強制執行數以千計的安全性規則，如此反而造成安全性管理問題，並且有可能擴大安全缺口。

以 OpenStack 為主的私有雲端環境結合 SDN 能力，讓我們轉移到更分散且以租用用戶為重點的安全性架構。每一個應用程式租用用戶皆佈建在我們私有雲端上的私人虛擬網路。虛擬網路環境網路存取控制乃使用安全性群組在租用用戶的虛擬網路環境內管理。

安全性群組實質上是一組可在每一個租用用戶內部啟動的存取控制規則。有多組的安全性群組可套用到 VM 以定義該 VM 的網路安全性，如圖 4 之說明。

藉由在主機上強制使用應用程式租用用戶層級安全性群組，就能夠針對每一租用用戶落實更方便管理的存取控制規則，並以自助式服務方式管理那些規則。接著可使用實體防火牆設備來保護資料中心，此時便需要較小型且更方便管理的安全性規則。

變更角色和責任

在建立網路執行個體時，我們的網路、伺服器與運算團隊責任之間不會再硬性分離，而是合作無間。有了 SDN，曾在實體網路裝置上實作的網路功能，現在也可在虛擬網路上實作。因此，若要採用 SDN，必須將之前系統管理員和網管人員之間分離的技能結合在一起。

自助式服務的實際應用

軟體定義網路 (SDN) 可為非網管人員的員工將網路服務佈建打造成自助式服務活動。例如，Intel 的 IT 育成中心經理 Thomas Birch 利用 SDN 建立網路，讓 Intel 業務單位 (BU) 能夠啟動 Web 服務。

這個擷取畫面來自 Birch 用來管理所建立之網路的 Web 介面。針對這個使用案例，Birch 藉由建立網路規則來設定輸入連線到虛擬機器 (VM)。他看著 VM，判定其他 VM 可能因任何理由需要與這部 VM 通訊、部署和測試網路執行個體，這些全部都透過 Web 介面完成。

在採用 SDN 之前，Birch 必須要求網管人員進行所有網路服務佈建。此時，他做到了即時建立網路。Birch 表示，「在 SDN 之前，自動化有限，設定工作需要大量手動修改。我必須要求 IT 工程師開啟特定連接埠，並扮演中間人的角色...多虧有了 SDN 讓我控制住局勢。」



若要建立自助式服務網路，員工可使用 Web GUI 佈建虛擬網路執行個體。

為了彌補這個缺口，於是我們建立了雲端系統管理功能。每一團隊（網路、伺服器與運算）的代表，都有責任開發和運作雲端環境。這些代表彼此協作及分享技能。

負責佈建網路的員工有一定的學習進程，不一定需要具備網路技術背景。網路工作團隊可幫助這些員工了解一些基本概念和網路安全作法，之後就讓佈建 GUI 來引領他們學習。我們也建置直覺式應用程式環境範本，讓客戶能更輕鬆隨需佈建網路元件，並不需要知道太多網路知識就可做到。

初步結果

服務佈建時間已在改善中。SDN 提供之 SDN 控制器的全域網路檢視和自助式服務優點，可減輕網管人員為達到網路服務要求的服務等級協定 (SLA) 而產生的壓力。

SDN 可簡化網路佈建程序。建立網路需要一些訓練，尤其是網路工作經驗不多或完全沒經驗的員工。然而，在獲得網路工程師協助並有 SDN 管理應用程式工作經驗後，員工就能體會自助式服務方法的好處。他們期望能不受限制地支援各個業務單位，投入靈活的開發工作，而且能控管部署，也有能力進行即時部署和測試。

初始測試結果指出 SDN 可透過提升網路管理效率來降低服務成本。我們也可保留目前的基礎架構投資，降低對專屬硬體和專用設備的依賴。

後續步驟

到了 2014 年，我們將針對 2013 年初開始生產部署擴充重疊網路部署，我們也會繼續探索使用 OpenFlow 的方式以增加重疊網路的價值。

我們打算使用 API 來虛擬網路服務，如雲端環境內的負載平衡器和 Web 應用程式防火牆。我們將會監視這些功能對主機的 CPU 額外負荷，並在適當時機卸載處理程序至較低層級硬體或網路介面控制器 (NIC)。

雖然從 Hypervisor 環境移轉到 SDN 環境時會面臨許多挑戰，我們仍不遺餘力地尋找方法來簡化這個移轉作業。

從整合型安全模型進化到分散式安全模型時，我們需要監視可擴充性，尤其和主機限制有關部分。我們打算在任何適當時機卸載處理程序。

結語

SDN 虛擬雲端環境的網路，讓員工（而不是網路工程師）可以為重疊網路元件編程，如此我們就可以隨需大幅佈建網路。以往需要數天時間進行組態設定的網路服務，現在可以透過自助式服務方法即時完成。

我們知道的 SDN 優點如下：

- 更快的服務佈建
- 更簡單的自助式服務網路建立
- 降低服務成本

此外，我們能更加管控目前的基礎架構，降低對專屬硬體和專用設備的依賴。

相關資訊

請造訪 www.intel.com/IT 以尋找相關主題內容：

- 「Intel IT 因應企業轉型的資料中心策略」
- 「將資料中心的網路架構升級至 10 Gigabit (Gb) 乙太網路」

如需關於 Intel IT 最佳實務的詳細資訊，請造訪 <http://www.intel.com.tw/content/www/tw/zh/it-management/intel-it/intel-it-best-practices.html>。

英文字母縮寫

BU	業務單位
DNS	網域名稱系統
GbE	Gigabit 乙太網路
NIC	網路介面卡
SDN	軟體定義網路
SLA	服務層級協議
TCO	總擁有成本
VLAN	虛擬 LAN
VM	虛擬機器
VRF	虛擬路由和轉送

效能測試中使用的軟體與工作負載，可能只有針對 Intel® 微處理器的執行效能最佳化。效能測試 (例如 SYSmark® 與 MobileMark®) 使用特定的電腦系統、元件、軟體、作業及功能進行評量。這些因素若有任何變更，可能會導致不同的結果。考慮購買時，為了協助您充分評估，您應該參考其他資訊及效能測試，包括該產品結合其他產品使用時的效能表現。

組態：

伺服器 (測試中的系統)	<p>機型：Intel® S5520UR (Urbanna)</p> <ul style="list-style-type: none"> 處理器：Intel® Xeon® 處理器 X5680 @ 3.33 GHz (2 個通訊端，6 個核心/通訊端)，96 GB RAM，停用超執行緒 BIOS: S5500.86B.01.00.0060 網路卡：2 x Intel® Ethernet Server Adapter X520-2 連接 @ 10GbE 到 10GbE 交換器 網路驅動程式：ixgbe 2.0.84.8.2-10vmw-NAPI Hypervisor：VMware ESX* 5.1 RC (版本編號 716794) Guest VM 組態：1 vCPU, 4 GB RAM, RHEL 6.2 (2.6.32-220.el6.x86_64), vmxnet3 和 ixgbev, 24 VMs 大型交換器控制器 (Corona) - 測試版本
用戶端組態	<p>機型：Intel® S5520UR (Urbanna)</p> <ul style="list-style-type: none"> 處理器：Intel® Xeon® 處理器 X5670 @ 2.93 GHz (22 個通訊端，6 個核心/通訊端)，96 GB RAM，停用超執行緒 BIOS: S5500.86B.01.00.0060 網路卡：2 x Intel® Ethernet Server Adapter X520-2 連接 @ 10GbE 到 10GbE 交換器 網路驅動程式：ixgbe 2.0.84.8.2-10vmw-N Hypervisor：VMware ESX* 5.1 RC (版本編號 716794) Guest VM 組態：1 vCPU, 4 GB RAM, RHEL 6.2 (2.6.32-220.el6.x86_64), vmxnet3, 24 VMs
網路組態	<p>機型：Extreme Networks Summit* X650 10GbE交換器</p> <ul style="list-style-type: none"> 網路連線功能： <ul style="list-style-type: none"> 2 x Intel® Ethernet Server Adapter X520-2 連接 @ 10GbE (從伺服器) 2 x Intel® Ethernet Server Adapter X520-2 連接 @ 10GbE (從用戶端) 1 x 10 Gigabit Ethernet 控制器 IX1-SFP+ 連接 @ 10GbE (從 NetApp FAS6240)
儲存體組態	<p>NetApp FAS6240</p> <ul style="list-style-type: none"> 版本 8.0.1 P1 Intel® Xeon® 處理器 E5540 @ 2.53 GHz (8 proc), 48 GB RAM 512 GB 的 PAM-II NFS 儲存體 @ 10GbE
應用程式	Netperf* 2.5
使用的資料收集工具	<ul style="list-style-type: none"> 從 Netperf 擷取傳輸量 使用「esxstop」公用程式擷取 VMware ESX* 主機上的系統使用量

本報告中提供的資訊為一般準則而非特定指示。其中提供的建議 (包括可節省的成本) 是以 Intel 的經驗為根據，並僅供評估之用。Intel 不保證其他人將會取得類似的結果。

本文件提供的資訊與 Intel 產品有關。本文件並未透過禁反言或任何其他方式，授予任何明示或暗示之智慧財產權。除了 Intel 在這類產品的銷售條款與細則所提供的內容之外，Intel 不需負任何責任，此外，Intel 拒絕提供關於銷售及/或使用 Intel 產品之任何明示或暗示的保固，包括有關特定用途的適合性、適銷性，或是侵犯任何專利、版權或其他智慧財產權的責任或保固。

Intel、Intel 標誌、Intel Xeon、Look Inside 與 Look Inside 標誌均為 Intel 公司在美國及/或其他國家/地區的商標。

*其他名稱與品牌可能業經宣告為他人之財產。

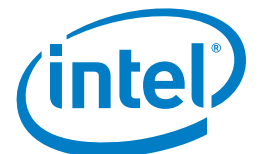
著作權 © 2014 Intel Corporation。版權所有。

印製於美國

♻️ 請回收資源

0914/WWES/KC/PDF

330118-001US



Look Inside.™