規劃採用 NSX 時的作業轉型

實務中的最佳做法

指南

vmware®

目錄

簡介

本白皮書的對象主要針對雲端、網路與安全性高層主管和經理。對後述人員也會有幫助：在所屬組織參與實際運用 NSX 的架構設計、工程與作業經理和個別貢獻者。

網路虛擬化代表一項重大進展，能幫助組織實現速度、靈活性與安全性三大效益。其所提供的效益相當於或更甚於運算虛擬化在過去十年來所提供的效益。為了實現網路虛擬化的效益，建議組織先評估和執行一項涵蓋**人員**、**流程**與**技術**的運作計畫。

VMware 在此之前一直與既有的 NSX 客戶密切配合，以了解將網路虛擬化應用於生產環境的實際情況。我們對實際情況的了解與認識將幫助引領您完成 NSX 的評估、部署與實際運用。您與您的組織可以評估找出對您組織的特定情況最有助益的最佳做法，並善加利用。

雖然本白皮書涵蓋廣泛的最佳做法，但其實無論您的組織目前處於何種狀態，都只需最小程度的變動就能開始實際運用 NSX。實際運用 NSX 並不複雜，而且有明確的成功之道。

本指南分為三個主要部分，針對下列方面探討重要學習內容和最佳做法：

人員

網路虛擬化為組織提供潛力，能展現組織的實力，並將整個技術組織完成工作的方式轉型，藉此帶給組織重大效益。網路虛擬化也代表一項需要審慎考量的改變，以確保整個組織明確瞭解且一致配合。確保您有一個靈活的組織結構，而且有明確分工與分責的混合型團隊，將讓您能幫助您的組織與人員實現最大成果與價值。我們提供組織結構、內部參與和溝通策略，以及分工與分責的相關資訊和指引。

流程

網路虛擬化提供大量的機會，能藉由將整個應用程式生命週期中的手動流程自動化，全面提高生產力。定義出您如何佈建、管理和監控應用程式與服務的理想未來狀態，能讓您遠離不必要的既有流程和做法。我們將提供您關於如何思考自動化、流程管理、工具，以及一些常見使用情境的指引。

技術

網路虛擬化的一個主要優勢是將網路與安全性功能從底層實體基礎架構分離，並將這些功能抽象化到一個虛擬化層。這讓您能以更佳方式架設和管理您的基礎架構，持續往前邁進。我們將提供關於架構設計最佳做法、漸進式基礎架構實作的指引，以及定期推出新功能。

這些最佳做法的用意並非代表制式或「一體適用」的做法。您需要依照您組織特有的特性、目標與優先事項，挑選您認為會對您的組織產生助益的做法。請避免採用「一次全包」的做法。先從幾個部分小規模開始，然後隨著時間擴大到其他部分。

有些組織過早心滿意足，在真正達到最佳效能之前就停止這項虛擬化過程。因此，限制了組織能達到的成功範圍。所以，隨時牢記最終目標，並持續力求完善，直到達到最終目標。

人員

我們首先探討的主題是「人員」：也就是您的技術組織，以及組織中負責端對端提供應用程式與服務並加以管理的團隊和個人，是網路虛擬化成功實際運用與安全性的背後推手。

組織結構初始概念

網路虛擬化與 NSX 並不需要有特定類型的組織結構。最佳結構取決於您的組織特有的因素。已實際運用 NSX 的組織結構類型從傳統孤島式組織，到完全混合型與內置型雲端團隊皆涵蓋。也有介於純粹孤島式與完全混合型團隊之間的居中型團隊。

您的理想組織結構將取決於多項因素。在設計組織結構時，應考量下列因素：

- 不同領域和專業領域之間一致配合
- 價值流程的成熟度
- 技術領導的層級
- 人員的經驗與專業知識
- 作業經驗與熟練度
- 委外的使用
- 基礎架構與應用程式的數量
- 非全新或全新部署

我們的建議：設計一個混合型團隊組織結構

根據實務經驗，生產力最高的團隊都是緊密整合、高度協同合作，而且獨立自主。這類混合型團隊經證實工作效率更高、週期時間更短，有濃縮型和擴大型兩種意見迴路，而且更能分享知識與持續學習。此團隊的成員最好都在同一地點。

我們看到的成功組織結構是依照知識領域 (例如運算、儲存、網路與安全性)，以及依照分工領域 (例如架構設計、開發與整合、作業以及支援) 的團隊組成。在這兩種組織結構中，團隊都是負責實體與虛擬基礎架構。

隨著您將越來越多的基礎架構與應用程式從現有的企業網路移至雲端，人員配置也會隨之轉移。隨著時間推進，將會有越來越多的人員在雲端上作業，而在現有企業網路上作業的人員則會越來越少。所以，很重要的一點是擬定一項溝通與訓練計畫，幫助組織瞭解這項變遷以及新的工作機會，並為這些做好準備。同樣重要的是，您將需要與人員溝通清楚，無論他們是在現有企業網路或雲端上作業，每個人貢獻己力都是組織整體成功的必要條件。

配合共同的成功指標

組織的下一個重要考量因素是配合一項共同策略，其中有明確定義的最終目標、階段目標、指標與獎勵。您的團隊應有一個服務導向的方法，並集體負責整個服務提供的生命週期，從業務需求到運作一直到管理一個有 SLA 為據的高品質生產工作負載。

每個團隊都應有共同的成功指標，而這些指標是依據對您的組織最重要的因素所界定。例子包括：上市時間、對營收的影響、對市場需求的回應能力、創新率和/或客戶獲益與滿意度。最終目標應對外展現著重在業務與服務的使用者。

容許團隊擬定並追蹤自己的成功指標。但同時確保這些指標與最終目標和階段目標有關，並且與之配合一致。除了配合組織目標之外，關鍵績效指標也應為具體、明確、可量化和可衡量。無論團隊選擇哪些關鍵績效指標，都應力求簡單，而且先從一些容易瞭解且有意義的基本指標開始。

在選好您的關鍵績效指標之後，請設好基線並記錄您目前的績效狀態。然後定期追蹤並評估 (例如一般是每月一次或每季一次) 您邁向期望最終狀態的進展。請向團隊明確表明，這麼做的用意不是為了批判人員或過去的績效，而是為了提供證據，以證明團隊的成功以及持續為業務締造的新價值。這些指標也有助於讓績效考核與評量更有效、更具體，而且對個別人員更有意義。

營造負責敬業的組織文化

組織文化是成功達到網路虛擬化與安全性的重要基礎。具備支持軟體定義的資料中心原則的組織文化，是成功的關鍵。與其由執行高層或管理階層強制執行組織文化變革 (這種做法在根本上難度極高)，組織文化應該是從團隊內部透過共同的經驗、技能與價值觀而自然浮現。

藉由確立共同的成功指標，新的組織文化將會隨之出現，並自然地落地生根。此新組織文化的基礎將是基於一個明確且使用者導向的業務目標、共同承擔的職責與風險、更密切的協同作業與合作，以及互信互敬。

團隊：安全性與網路方面的專業人員共同合作

網路虛擬化的一個主要優勢是將網路與安全性功能從底層實體基礎架構分離，並將這些功能抽象化到一個虛擬化層。這項轉移引發了一些疑問，例如：「應由哪個團隊負責虛擬化管理程序中執行的虛擬網路與安全性？」以及「網路虛擬化會導致我的職責有何改變？」 在本節，我們會回答這些疑問。

由您的現有網路與安全性人員負責網路虛擬化與安全性。NSX 是基於需要有網路專業知識的網路概念與技術。所以，只要您的網路團隊具備必要的專業知識即可。需要有網路與安全性專業知識，才能設計、部署和運作虛擬網路，這和處理實體網路的方式一樣。

實體網路不會消失，只是變得更簡單、更容易管理。我們不建議將團隊與實體和邏輯網路劃清界線。為了幫助達到最快速度和最大靈活性，一個包含網路架構設計師、工程師和操作員的團隊應該同時負責實體底層與虛擬重疊。

但是，您還是可以選擇讓網路工程師更多專注在實體設備的裝載、堆疊與組態設定上，讓其他人員較多專注在虛擬重疊上。不過，所有這些人員都應屬於同一團隊。

網路專業領域職能 (例如架構設計師、工程師和操作員) 演變為包含網路虛擬化與安全性。大多數網路與安全性人員將需學習新事物，以增強他們的專業知識與技能。有了 NSX 之後，網路服務會在虛擬化管理程序層中執行。網路專業人員必須對於伺服器虛擬化，以及這對邏輯網路服務造成的影響有一定程度的瞭解。

人員方面最佳做法：訓練

在評估流程初期，第一優先事項就是確定每位人員都瞭解網路虛擬化的原則，並接受過 NSX 以及屬於雲端商業網路的 NSX 相關作業與管理工具等方面的訓練。VMware 提供多種訓練方式，包括實驗室實作、研討會與訓練課程。這些資源主要是針對沒有伺服器虛擬化背景的網路專業人員，但也適合想學習網路虛擬化的伺服器虛擬化專業人員。您也可以實行一項計畫，藉由提供領導機會給人員，讓他們以非正式方式教授最佳做法給其他團隊與小組，藉此確保團隊內與團隊間的知識分享與訓練。

其中一種加快學習的最佳方法是想出並展開小型試行專案與評估。納入涵蓋運算、儲存、網路與安全性的所有必要專業領域職能，也就是架構設計、工程與作業。

先從一個小型跨職能團隊開始

另一種低風險的建議方法是在您邁向網路虛擬化的進展過程中，先從一個小型跨職能團隊開始。如果您有能力從孤島式團隊轉為混合型團隊，可以隨著時間推進分階段進行這項轉型。我們看到最多的是兩種類型的跨職能團隊。選擇對您來說效果最好的模式：

新創團隊	專案團隊
如果長遠來看您有能力轉為混合型團隊，請採用新創團隊。新創團隊終究會成為組織結構/組織圖的常設單位。並且配置 100% 全時間專職於此團隊的全職員工。	如果長遠來看您沒有能力轉為混合型團隊，請採用專案團隊。專案團隊是在必要時成立和解散的團隊。此類團隊的成員屬於兼職性質，另有一個正式的隸屬團隊。我們已看到政府機構大多採用專案團隊。

此跨職能團隊一般是端對端負責某一應用程式堆疊或一組應用程式堆疊。此團隊應有運算、儲存、網路與安全性的專家。專業領域技能應涵蓋架構設計、工程與作業。此團隊必須有能力處理所有工作，從設計、開發、測試到部署以及持續的作業。(請參閱附錄的網路與安全性分工與分責說明。)

選擇第一個團隊的變革推動者

為初始團隊選出人員，分別擔任變革推動者、主題專家、技術宣導者和受敬重的領導者。找出大家都希望納入自己團隊的人員。這些人員必須懂得如何建立人際關係、敞開溝通管道，以及識別摩擦點，並將摩擦點減至最少。也應有領導特質，能鼓勵他人做出改變，同時以身作則。如果此團隊的成員不在同一地點，請在專案一開始讓成員聚在一起兩週。

此團隊的成員應該各自都有配合團隊目標的個人階段目標管理 (MBO)。例如，如果團隊某一成員花 50% 的工作時間在新創團隊上，這份工作就應該大約佔其 MBO 的 50%。這點或許看似昭然若揭，但我們曾看過一些情況是人員花在跨職能團隊的時間被當做業餘愛好般，而不是被正視為個人工作的核心部分。這不太可能會是成功之道。

人員方面最佳做法：避免臨時告知

不要等到您即將部署前，才臨時告知人員。已經發生過一些情況是在整個過程中太晚納入網路或安全性作業人員。因而導致專案大幅落後。作業人員將需要知道網路虛擬化與安全性會導致監控、警示與移難排解有何改變。以及他們的流程與工具必須有何改變，我們將在本文稍後探討這個部分。

慶祝成功和把握成長機會

延攬網路與安全性人員參與專案時，向他們說明這項專案對他們個人與工作發展有何潛在助益。隨著您將基礎架構虛擬化和自動化，您的網路與安全性人員將會有更多時間展開有建設性的新專案。他們就能專注在能為業務締造更高價值的策略性計畫。例如，與其進行 VLAN、負載平衡器或防火牆規則組態設定等平淡無奇的工作，他們能轉而設計能為業務增加價值的新服務：將跨領域流程自動化、進行增加彈性的設計、規劃容量，或進行其他有建設性的專案與計畫。

也應向人員說明，組織中有創新構想和前瞻思維的人將有機會為網路與安全性轉型貢獻己力。締造的成果將會有利於推動這項轉型的人，正如同過去大力倡導 IP 網路並因此大展鴻圖的人，以及最近的運算虛擬化。在這兩個案例中，新類型的管理員因此誕生，具備新的技能與知識。參與這項轉型將充實人員的專業能力，增加他們在就業市場的機會與價值。

鼓勵主動吸引服務使用者參與

另一個有效方法是鼓勵此團隊吸引服務使用者參與 (例如應用程式、業務與基礎架構擁有者)，藉此讓他們瞭解新功能。請這些使用者主動參與，瞭解他們的要求並取得他們的意見。他們會想知道功能與使用者經驗將會有何改變。以下舉出一些成功的吸引參與活動：

定期與使用者接觸：定期進行研討會，以提供最新資訊、掌握需求，並徵求意見。

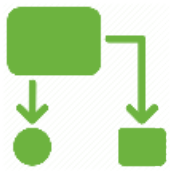
「展示成果，不要只說」：確立團隊開發和發行新功能的規律步調，並將此告知客戶，這會提升客戶參與度。

向全組織宣告成功會帶來正面效果

除了向獲選團隊成員和服務使用者宣傳此專案之外，向所有業務線或整個組織宣導此專案，也是個明智做法。目標在於吸引夠多的人支持此專案，並建立一個平台，作為執行工作的實際管道。分享關於此專案可締造業務與 IT 成果的有用案例。您也可以藉由結合簡報發表、討論會、文章、部落格貼文、社群媒體、電子郵件或示範影片等不同方式，來進行這項宣傳。參與此團隊的每個人員都應將自己視為此專案的宣導者。慶祝大小成功是高績效組織的代表特點，所以應將此視為技術變更管理上的重要最佳做法。

變更非易事：所以需要找到共識

我們都知道變更非易事。尤其在變更緩慢的部分與專業領域，或者在變更可能被視為對工作或生計造成潛在威脅的部分。這些因素可能導致對進步的抗拒。有些人員可能會積極對抗這項轉型。最佳因應方法是透過真誠溝通和宣導，以及支持組織的成功，來尋求對網路虛擬化潛力的共同理解。您需要展現公開、透明且樂意的態度，明確解釋並回答這些問題：「這對我有什麼助益？」「這對我們有什麼助益？」



流程

在本節，我們將解釋網路虛擬化對作業流程的影響、說明您應採取的步驟，進而剖析並瞭解您的現有流程，並提供一些建議，讓您瞭解如何改變您的流程與工具，以充分利用網路虛擬化與安全性。

清點並分析現有流程

網路虛擬化的一項重要價值主張是將與應用程式生命週期相關的典型手動流程自動化。這提供給您一個極佳機會，能全面評估您的現有流程，以判定這些流程應如何與網路虛擬化同步往前邁進。

重要訣竅：不要只是將全部現有流程與 NSX 網路虛擬化和安全性一同保留。這麼做會降低您原本可以達到的效益與成本節省程度。找出並瞭解您全部的現有網路與安全性流程。瞭解網路虛擬化對下列流程的影響：

- 應用程式佈建
- 組態設定管理
- 變更管理
- 容量管理
- 事件與問題管理

您需要瞭解這些流程目前如何端對端運作，以及可以如何透過自動化與協調作業予以簡化與精簡。您將發現可以大幅精簡現有流程或步驟，在某些情況下甚至可以省略。

在您完成徹底清點之後，請排定將這些網路與安全性流程自動化的優先順序。要快速看到效果，請著重在將高價值且低人力的流程自動化。請不要一次精簡太多流程；先選一個或兩個流程開始進行。

流程方面最佳做法：基準測試

在開始進行之前，必須進行基準測試。在您變更任何部分之前，先設好基線並記錄您的流程目前需要多久時間。然後，計算每個流程的所需人力與週期時間。將流程自動化之後，再進行一次相同測量。然後，您就可以進行比較，並發布您所達到的結果。瞭解效能將幫助團隊達成其階段目標 (例如減少佈建時間或偵測與隔離問題所需時間)，並幫助團隊為您的使用者確立適當的 SLA。

將佈建與管理自動化

一旦您清點並評估完成您的現有流程之後，下一個步驟是將您的應用程式或服務的佈建與管理自動化。組織使用網路虛擬化與 NSX 的固有自動化功能，以達到速度、標準化、一致性與可稽核性。自動化也會減少手動組態設定錯誤導致的停機與安全風險。自動化會提高開發與測試生產力、加快新應用程式的上市、提供一致的標準化組態設定，而且產生的錯誤較少，解決問題的速度更快。

雖然 NSX 不需要自動化工具，但大多數客戶會合併使用雲端自動化專用工具與 NSX API。這些工具與 API 是用於將 NSX 提供給虛擬網路的功能性服務 (即邏輯 L2 交換、L3 路由、負載平衡、防火牆保護與 Edge 服務) 的佈建與管理自動化。大多數組織使用 NSX 將多種服務自動化。

目前的典型情況：目前依然是用鍵盤與指令行介面 (CLI)，以手動方式將實體網路與 VLAN 佈建到專用硬體上。所以，網路變更正處於應用程式部署的關鍵路徑上。如您所知，這類部署可能得花上數天、數週或更長時間，直到網路連線、效能、可用性與安全性等方面萬事俱備。

透過 NSX 往前邁進：組織使用 NSX 將網路虛擬化與安全性的佈建、組態設定、管理與除役自動化。有了 NSX 之後，網路團隊不再需要設定眾多實體交換器的流量導向與網路組態設定，例如 VLAN、VRF、VDC、QoS、存取控制清單等。

一旦將實體網路的初始組態設定為底層網路之後，就不需再配合新應用程式部署的需求或不斷改變的應用程式需求而持續或經常重新設定。所有這類變更現在全都是透過自動化工具在邏輯網路空間內完成。

流程方面最佳做法：著重在 IT 自動化

我們建議您一開始先為 IT 建立自動化，讓他們能更快滿足服務請求。在 IT 自動化之後，您就可以新增一個自助服務入口網站與服務目錄，應用程式開發人員與品保工程師只要按一下按鈕就能存取完整環境。接著介紹 NSX 使用者使用的一些自動化工具。

工具考量事項

正如前文所述，您必須先找出、瞭解並記錄您想要自動化的工作與流程。這是關鍵步驟，因為不同的 IT 自動化工具 (例如雲端管理平台與協調工具) 提供不同的特色與功能。所有這些工具都需要一些學習與設置方面的前期投資，但之後產生的效益絕對值得。

首先介紹用於佈建、管理與協調網路基礎架構的 vRealize Suite 與 OpenStack。一開始請先將獨立分散的工作自動化，藉此熟悉這項工具。在您學會使用這項工具之後，您就可以轉而將工作流程自動化，即：在單一完整堆疊中佈建與一同管理應用程式和其網路與安全性的工作流程。任何網路自動化輔助工具的評估與操作，都應有網路操作員或雲端網路操作員參與其中。

組態設定標準化與自訂

組織可以使用範本與原則，將完整應用程式堆疊的運算、儲存、網路與安全性組態設定標準化。如果組織需要進行變更，可以直接修改範本，然後直接套用到生產環境。使用此範本的所有工作負載就會自動顯示這項變更。並會保留一份所有變更的記錄，供稽核與確認合規。

工程部門可以發布靜態和/或可自訂的組態設定。靜態環境一般用於通過生產認證的堆疊。而可自訂環境則是用於開發與測試沙箱。可自訂環境可以滿足 80% 以上的使用者需求，但是開發人員或品保工程師可以在必要時變更環境。可以將工作負載設定為使用新網路，或連到現有網路。

藍圖流程自動化範例

接著來看看可以將哪些工作自動化，以納入標準化的三層應用程式藍圖：

在此藍圖通過測試與驗證後，就可以將其公布到供使用者使用的服務目錄。使用者只要按一下服務項目與完整應用程式堆疊 (其連線、可用性與安全性等設定全部包含在內)，就能在幾秒內完成部署。

這項自動化服務比傳統沒有 NSX 的實體網路快了許多倍，以往通常需要耗時數天或數週才能完成部署。組織能避免因複雜的問題回報工作流程、變更審查與核准、備援需求搜尋與驗證，以及手動組態設定所導致的週期時間長與延遲。

流程方面最佳做法：角色型存取

在自助服務入口網站上依照業務角色實作角色型存取控制。您也應依照業務群組定義資源保留與配置原則、追蹤計費成本，並恪守服務層級 (SLA)。

讓安全性原則自動套用到群組

NSX 會以原生方式將許多原本在實體網路與安全性基礎架構上以手動方式執行的工作自動化。例如，NSX 提供多種新方式，可為虛擬化層上的虛擬機定義安全性原則，並將這些原則套用到這些虛擬機。

舊方法：依照舊方法，安全團隊是依據 IP 位址、連接埠與通訊協定手動建立規則。團隊最怕的「5-Tuple」管理夢魘。

新方法：依照新方法，安全性原則是依據安全性群組而建立。您可以定義一個包含一組虛擬機的安全性群組，然後依據這些工作負載的需求建立一個安全性原則。如果您新增另一個虛擬機到此群組，您不需進行任何手動調整，這個安全性原則就會自動套用到新的工作負載。也可以透過或改透過安全性標籤與環境定義，動態套用群組成員資格。NSX 的安全性原則可以包含例如防火牆保護、防毒保護與 IPS。

安全性群組可以是靜態或動態，透過程式設計可以在工作負載的任何任意中繼資料上啟動。例如，使用者群組身分識別、作業系統特性、虛擬機名稱與標籤，以及有病毒存在等。NSX 會自動依據虛擬化相關環境定義指定適當的安全性群組與原則，而非依據實體拓撲。

也會集中協調和管理預先核准的安全性原則，這會減少規則蔓延，並確保安全性原則獲得準確且一致的套用。這種新的自動化程度會大幅減少運作複雜度，以及管理所有工作負載安全性原則的支出。

每一個安全團隊都使用一個獨一無二的網路安全性應用裝置組合，以便符合自身環境的需求。除了 NSX 的分散式防火牆保護功能之外，組織也應運用此平台將 VMware 技術合作夥伴提供的進階網路安全功能自動化。

網路安全團隊經常面臨挑戰，要判定多家廠商所提供完全不相關的網路安全服務之間的關係並加以協調。NSX 讓團隊能輕鬆做到這點。NSX 會將網路服務分散至 vNIC 環境中，以形成適用於虛擬網路流量的服務邏輯管線。可以將協力廠商的網路服務接入至此邏輯管線，就可以在邏輯管線中使用實體或虛擬服務。企業可使用 NSX 建立原則，這類原則能運用 NSX 的服務接入、串接與導引功能，協助服務在此邏輯管線中執行。

NSX 平台提供的運作模式也有益於整合式安全性工具。此類整合會大幅提升佈建速度、管理效率與服務品質，同時維持伺服器、網路與安全團隊之間的職責分工。

透過與 Palo Alto Networks、Intel Security、Trend Micro、Symantec、Checkpoint 與其他幾家 VMware NSX 合作夥伴整合，提供了進階安全功能。

利用新穎工具建立應用程式層級能見度

虛擬化管理程序以理想且獨特的方式位於實體與虛擬環境交界上。因為 NSX vSwitch 會在每個封包進入和離開虛擬機時偵測到每個封包，所以能提供最高層級的能見度與環境定義。也可以判定應用程式、虛擬網路、實體網路與更多其他物件之間流動性關係的關聯性。

以下舉出一些範例情境，以示範 NSX 獨特的監控與疑難排解功能：

即時摘要	監控與疑難排解	偵錯
操作員可以選擇任一虛擬機的網路介面，就可以看到所有流程與其狀態的即時摘要。完全不需將完整封包擷取設定到某一遠端工具內，也不需過濾 IP 位址，才能搜尋該虛擬機。	透過 NSX 的中央指令行介面與中央 API，就能檢視虛擬網路的每個層面。這大幅簡化了監控與疑難排解作業，因為您不再需要苦思應該在網路的哪個位置尋找問題。而且，也不再需要為了進行疑難排解，而切換到不同主控台。	每個封包都是由 vSwitch 在軟體內處理，提供您比傳統網路上更大的能見度。您不需要存取 Guest 虛擬機，就可以建立綜合交易。可以將「追蹤流程」封包放入前饋管線內，以進行資料路徑上的精密問題偵錯 (例如限制性過高的存取控制清單原則)。

操作員已使用許多工具來管理和支援資料中心基礎架構。他們使用不同的工具來監控、疑難排解與變更管理作業。在網路虛擬化之後，沿用同一組現有工具就可以檢視邏輯網路。

即時監控工具在不斷改變的虛擬化環境中很重要，在這類環境中，基礎架構與應用程式會動態移轉於不同伺服器間，而且會自動重新設定網路。

流程方面最佳做法：工具

找出讓您能檢視虛擬與實體運算、儲存和網路基礎架構之間物件關係的 VMware 或協力廠商工具。基礎架構領域之間的相關性有助於快速縮小特定領域問題的範圍，並減少使用多種領域特定工具的需求。

最佳選項通常是新穎工具，例如 vRealize Operations、Arkin、Riverbed 與專為虛擬與實體環境所設計的其他工具。這些工具都提供包含拓撲、應用程式運作狀況、利用率與容量的端對端檢視畫面。

請記住，只用單一廠商的做法不見得隨時都能提供您最佳能見度。多種工具可能是提供最佳監控、警示與疑難排解的最佳選擇，正如目前您的實體網路同樣需要多種工具。例如，您可能使用不同的工具進行流量流程分析 (例如 SolarWinds、NetQoS)、封包分析 (例如 Wireshark、SteelCentral)，以及警示發布 (例如 Netcool、OpenNMS)。

虛擬網路提供與實體網路內相同層級的檢測工具，同樣是透過標準通訊協定 (例如透過簡易網路管理協定 (SNMP) 與 API 的封包與位元組統計數據、SPAN/L3 SPAN、NetFlow/IPFIX、連接埠鏡射和 Syslog)。這讓組織能在一開始先使用現有的監控、警示與疑難排解工具，之後再改用新穎工具，例如前述的新穎工具。

關於流程的結語

網路虛擬化與 NSX 讓您有很好的理由立即評估您目前的作業方式，並定義一個更好且更有效率的方式往前邁進。修正所有流程感覺上是件艱鉅任務：採用漸進式方法將您的流程自動化，就不會覺得無所適從。精實且持續的功能改善是往前邁進的極佳方式。

技術

在本節，我們將探討規劃、部署和實際運用網路虛擬化與 NSX 時的架構設計與基礎架構考量事項。也將討論微分段與災難復原的實際使用情境。

實體網路的設計以簡單為目標

有了 NSX 之後，實體網路架構的設計只是基於連線與效能考量。簡單的程度可能就像您目前已在使用的 L2 網狀架構，或以主幹式架構為基礎的 L3 網狀架構一樣。您可以一開始先用第一種架構，再逐漸改用第二種架構。

NSX 不會硬性規定 L2 界限的劃分位置。實體網路的組態設定變更應該會相對較不頻繁，因為實體網路只是提供主機之間的連線。這有助於避免手動組態設定錯誤。

將網路服務與拓撲從實體硬體分離，已讓 L3 主幹式網狀架構變得廣泛遍布。這讓您能用同一個邏輯網路、安全性與管理模式建立一個通用平台。

由於 NSX 會從實體拓撲抽將虛擬機所見的虛擬網路拓撲抽象化，因此在網路架構中進行變更會更為可行。NSX 讓網路設計師能更輕鬆改用主幹式架構，此架構使用架頂式 (Top-of-Rack) 交換器間無封鎖 ECMP 的 L3 路由。

底層實體網路可以獨立於虛擬網路自由發展，其架構是依據延展性、總流量與健全性標準而設計。單一裝置或連結故障不會影響應用程式連線。

ECMP L3 網狀架構設計提供組態設定統一性，並增強裝置互通性。硬體升級 (例如部署新的交換器) 可以從 NSX 分離，以避免影響正在您的虛擬網路上執行的工作負載。NSX 可以支援任何廠商的交換器，而且可以將它們互連在一起。

網路虛擬化重疊與主幹式架構結合，會帶來更大的彈性與營運效率、更有效率的頻寬使用以及延展性，能處理資料中心內與日俱增的橫向通訊量。而較小的 L2 廣播網域則會增加網路的穩定性。

以漸進方式實作網路虛擬化

NSX 網路虛擬化並非全有或全無的產品方案。NSX 虛擬網路不需要變更底層實體網路。網路虛擬化會與實體網路上現有的應用程式部署透明地共存。

技術部門擁有只將部分網路虛擬化的彈性，只需要將虛擬化管理程序的節點新增至 NSX 平台即可。此外，NSX 的軟體閘道或架頂式交換器 (也就是 VMware 合作夥伴提供的硬體) 提供順暢互連虛擬與實體網路的功能。這些元件可為連到虛擬網路的工作負載存取網際網路提供支援，或者直接將傳統虛擬區域網路和裸機工作負載連到虛擬網路。

技術方面最佳做法：先從單一專案開始

建議您以漸進方式推行網路虛擬化與安全性。我們建議您先從單一使用情境和單一應用程式組合開始。找出低風險/高回報的工作負載，以運用新功能。在您初次實作時，請選擇風險較低但有足夠複雜度的工作負載，以驗證 NSX 適合您的環境。

您選擇實作的使用情境會主要決定您應該為您的虛擬網路，將哪些 NSX 的功能型服務自動化。例如，如果您要將網路佈建自動化，可以先從邏輯 L2 交換、L3 路由和 Edge 服務開始自動化。如果您即將實作微分段，您應該從邏輯防火牆保護開始自動化。

定義一個策略與方法，以持續為您的客戶推出新的 NSX 特性與功能。確立一個規律的發行步調，讓業務部門能預先知道時程，並可以依之規劃他們的專案。您將發現，定期發行有助於提升使用者參與度、服務的採用和客戶滿意度。讓使用者主動採用服務，不要試圖以人為方式強迫廣泛採用。

技術方面最佳做法：研討會

與您組織中的業務和技術同事保持密切合作，是確保任何計畫 (包括網路虛擬化) 都能成功的絕佳方式。可以考慮舉辦使用者參與的定期研討會，以告知並教育相關人員有關目前發行的網路虛擬化與安全性服務，同時讓他們知道您的最新藍圖計畫。鼓勵應用程式與基礎架構擁有者與您協同合作，告訴您他們對未來發行版本的要求，以及對目前生產環境上的可用功能有什麼意見。

使用情境：依循應用程式界限分段

大多數 NSX 客戶在初期實作和實際運用的一個主要使用情境是微分段。微分段被視為最佳做法安全性架構已有很長一段時間。入侵者企圖非法侵入網路時，微分段能有效限制入侵者的移動，並防止資料遭盜用。然而，微分段在過去並未獲得廣泛使用。這是因為傳統實體網路的架構限制，使其難以被實際運用。

NSX 讓微分段在作業上變得可行。此平台提供原生隔離與分段功能。進階服務接入功能讓協力廠商的安全性應用裝置也能運用這個 NSX 運作模式。

無論是為了合規、減量或單純為了避免開發、測試和生產環境相互影響，大多數網路安全性皆以隔離作為基礎。虛擬網路依預設不僅與其他虛擬網路隔離，也與底層實體網路隔離，除非有特別規定必須將這些連在一起。操作員不需要處理實體子網路、VLAN、存取控制清單與防火牆規則。

分段主要與隔離相關，但也適用於多層虛擬網路中的分層。一般來說，網路分段是實體防火牆或路由器的功能，其設計在於允許或拒絕往返於各個網路區段或層之間的流量。例如，將 Web 層、應用程式層和資料庫層之間的路由器與防火牆流量分段。

現今的挑戰：傳統的分段設定流程不僅手動、耗時，而且很容易出現人為失誤，因此可能導致安全性漏洞出現。若要進行實作，需要具備有關裝置組態設定語法、網路定址、應用程式連接埠與通訊協定的特定專業知識。

網路虛擬化解決方案：NSX 是將安全性原則套用在虛擬化層上。所以，您可以將橫向流量繞道工具包丟掉。在封包還沒抵達第一個虛擬網路連接埠之前，就已完全透明地套用了安全性原則。由於在最初就已確保安全，所以對延遲敏感的橫向流量就能順著延遲最低的路徑，直接前往其目的地。

結合集中式控制與分散式服務實作，代表可以透過運作上可行的方式，將極精密的原則套用到每個虛擬介面。例如，三層應用程式中位於同一層的虛擬機可以與其他層通訊，但不可以彼此通訊。其實上，每個工作負載都有各自的安全保護。

NSX 讓您能依據高層級的業務結構 (例如應用程式、使用者或群組) 設定安全性原則，而不是依據低層級的基礎架構結構 (例如 IP 位址、應用程式連接埠與通訊協定)。能以更高的精準度、準確性，以及配合企業政策來套用安全性原則，完全不需透過人為解讀。

以工作負載行動力與復原能力為設計目標

傳統上，當 IT 移動應用程式時，實體網路拓撲與位址空間會要求 IT 變更 IP 位址。在有些情況中，IP 位址是以硬編碼方式編入應用程式內，因為需要修改程式碼並進行迴歸測試，所以成本更高。

NSX 讓您的工作負載不再受限於 VLAN 與 IP 位址設定，並讓工作負載在整個資料中心網狀架構內的行動力與配置不受限制。有了 NSX 之後，工作負載配置不再依賴特定位置上實體網路服務的實體拓撲與可用性。

無論實體存放的位置在哪裡，虛擬機所需要的一切網路功能都由 NSX 提供。工作負載可以在不同子網路、可用性區域或資料中心間移動自如，操作員完全不必為工作負載重設 IP。如果工作負載已移動，其所有的網路與安全性服務都會自動跟著移動，完全不需人為調整。

組織可使用 NSX 的工作負載行動力與配置功能進行下列事項：

- 加速佈建應用程式
- 將工作負載移轉到新的資料中心
- 更新或重新整理底層實體基礎架構

使用情境：透過網路虛擬化提高伺服器資源利用率

組織也可使用 NSX 取得同一資料中心內其他位置上或另一個資料中心內的可用伺服器容量。這會大幅提高伺服器資源利用率與整合率。所有這些使用情境都會大幅減少營運成本，並提高靈活性，為您在網路虛擬化與 NSX 上的投資增加整體價值。

在傳統網路拓撲中，每個叢集或 Pod 都有各自的伺服器容量。若要從另一個 Pod 或叢集存取網路，需要重新設定網路，不但耗時過長，而且容易發生人為錯誤。可用的伺服器容量也會白白浪費。我們有時將此稱為「暗處伺服器容量」，因為不容易觸及。事實上，傳統網路拓撲與設備的複雜度會限制技術部門更有效使用伺服器容量的能力。

NSX 讓您能延伸網路，以取得資料中心內任何位置上的可用容量。完全不需觸及您的現有實體基礎架構。如果您想新增虛擬機，例如新增到不同子網路的伺服器或可用性區域，只需叫出虛擬機，將其連接到您的邏輯交換器即可。即使這兩種工作負載會跨越實體網路上的多個子網路與可用性區域，它們現在仍相鄰位於第 2 層。

使用情境：災難復原

您也可以使用 NSX 補強現有的災難復原解決方案。使用傳統的網路方法時，為災難復原所運用的備份站點需要在成本與功能之間取得平衡。與其將網路拓撲與服務忠實地複製到第二個位置，大多數組織會選擇用「夠好的」解決方案了事。會採取這類折衷是為了減少成本，但卻導致功能不如他們的主要資料中心。

NSX 能提供零折衷的災難復原。NSX 讓您不只是擷取虛擬機的快照，而是能擷取完整應用程式架構的快照，連網路與安全性都包括在內。無論您將副本傳到任何硬體上維持備援的災難復原站點，功能都不會發生任何缺損。

發生災難時，只要叫出虛擬機，就能完成災難復原。虛擬機需要連到的網路早已在災難復原站點上執行。這樣您就能大幅減少您的復原時間目標，因為不再需要為工作負載與安全性應用裝置重新設定新的 IP 位址。

技術方面考量事項結語

網路虛擬化與 NSX 會為您的技術環境提供極大程度的新靈活性。這會讓許多能創造價值的使用情境變得可行。為了避免因為眾多可能性而不知如何下手，首先請著重在服務品質。然後擴大您最初使用情境的版圖。接著選擇第二種使用情境進行實際運用。只在您的團隊與使用者滿意服務品質之後，才提供新功能。

後續步驟

應將實際運用網路虛擬化與安全性視為一個旅程。在這旅程中，隨著您改用軟體定義的資料中心，並為業務創造更多價值，您的組織會日益成熟幹練。

您的組織和個別團隊成員將會有多種可用選項，能深入瞭解如何達到網路虛擬化與 NSX 提供的所有運作效益，以及 NSX 如何補強您 IT 部門的其他部分。

步驟一：學習

極佳的第一步驟就是提供學習機會給您的組織與個別人員。可以結合不同類型的教育與學習方式：包括正式方法 (例如研討會、訓練課程、實驗室實作、訓練計畫)，以及非正式方法 (例如共進午餐一同學習、指導、輔導)。為了獎勵學習，可以考慮將訓練與學習目標納入個人 MBO。

一開始，您的團隊可以先參與 VMware 的實驗室實作 (labs.hol.vmware.com)，以及透過 VMware Education (vmware.com/education) 提供的講師引導研討會與訓練課程。VMware 也提供著重在監控與疑難排解的 NSX 作業指南。

步驟二：轉型服務

聘請外部人員以客觀立場幫助您改用網路虛擬化與 NSX，將能大幅加快這項流程。VMware 提供「營運轉型」服務與研討會 (vmware.com/consulting)。例如：「網路即服務 (NaaS) 願景規劃」會幫助您清楚確定新網路與安全性運作模式的願景、最終目標與階段目標。「NaaS 探索」會幫助您確認您需要增強或建立哪些營運與組織功能，以落實這個新的運作模式，並達到預期目標與成果。

步驟三：簡單試行

瞭解 NSX 並看出可以如何加以實際運用的一個最佳方式，就是先用單一使用情境與一些工作負載開始生產試行。選擇風險較低但有足夠複雜度的工作負載，讓您能學到最多關於如何實際運用 NSX。

請聯絡您的 VMware 或合作夥伴客務專員，幫助您開始進行。

附錄

最終狀態效能特性

下表摘要出實際運用 NSX 後的人員、流程與技術方面的最終狀態特性。您可以用此作為您整個旅程的指南：

向量	目前/開始狀態	未來/最終狀態
組織結構	• 孤島式且界限僵化，需要重量級流程 • 請求程序非常正式 • 做完份內工作後就丟給別人 • 相互指責：非我即敵 • 最終目標、階段目標與獎勵各有不同且互不配合	• 混合型，有立即的互動 • 開放的溝通態度 • 採用濃縮型意見迴路 • 高度協同合作 • 有共同的目標與 KPI • 共同承擔風險與責任
人員	• 專門化技能 • 專業知識侷限在某一領域 • 使用指令行介面與指令碼 • 廣泛普及的知識 • 職涯成長有限 • 以硬體基礎架構為中心	• 跨領域以及專業領域技能 • 多種領域專業知識 • 使用 API 與自動化工具 • 持續學習 • 有機會透過策略專案對業務產生正面影響 • 以服務與應用程式為中心
流程	• 手動且容易出錯 • 問題回報系統繁瑣 • 需要協調與經驗傳承 • 複雜且有瓶頸 • 需要等候服務 • 營運成本高 • 以基礎架構為重	• 自動化、標準化、一致且方便稽核 • 發生手動錯誤的風險低 • 周轉速度快/有 SLA 為據 • 即時互動 • 營運成本降低 • 以服務或應用程式為重

向量	目前/開始狀態	未來/最終狀態
工具	• 舊版且領域特定 • 孤島式且工具種類多 • 檢測設備限用於實體 • 以基礎架構為重 • 難以隔離服務問題 • 個別元件有各自的指令行介面	• 工具新穎且跨領域適用 • 其設計同時適用於虛擬與實體檢測設備 • 以應用程式為重 • 整合式基礎架構與服務監控 • 容易隔離服務問題 • 透過集中式指令行介面與 API 存取檢測設備基礎架構
架構	• 有典型 3 層架構的限制 • 受限於工作負載 • 防火牆遇到瓶頸 • 核心超額分配 • 依賴連結效能 • 受限於位置的集中式服務	• 無封鎖 ECMP 主幹式網狀架構 • 具有分離與抽象化功能的重疊 • 工作負載可移植性與行動力 • 原生隔離與分段 • 延展性與彈性 • 分散式服務
基礎架構	• 實體，且底層變更緩慢 • 安全性受限於基礎架構 • 災難復原功能降低，只有「夠好的」程度 • 需要人為解讀原則 • 原則以基礎架構為中心 • 低層級的基礎架構結構 • 零散式管理 • 受限於硬體廠商 • 難以進行服務串接	• 虛擬，重疊變更處於動態 • 安全性以應用程式為重 • 災難復原零折衷 • 安全性原則為虛擬機可讀 • 原則以業務為中心 • 高層級的業務結構 • 集中化管理 • 價格/效能選擇 • 容易進行服務串接

雲端網路與安全性職務

下列說明將幫助您定義雲端網路與安全性人員的職務與職責。這些雲端職務是由「傳統」網路與安全性專業人員執行；也就是您團隊中的現成人員。

在中小企業中，一人負責執行兩種以上這類職務是很常見的情形。例如，一位網路工程師可能同時負責網路架構設計、開發和/或營運。並非所有組織都需要有不同的人員分別負責每一種這類職務。

而大企業中的情況則與上述恰好相反，常有多位人員負責相同/類似職務。例如，我們已看到許多跨國公司擁有數名雲端網路架構設計師或雲端網路工程師。

雲端網路職務

雲端網路架構設計師 (CNA) 負責依照服務型使用模式 (網路即服務) 開發端對端雲端網路架構，並擬定標準。CNA 須履行下列職責：

- 判定技術與營運的網路需求
- 設計滿足應用程式需求 (例如容量與效能) 的實體與邏輯網路
- 發展並驗證測試方法，以確保需求獲得滿足
- 引導雲端網路解決方案的規劃與實作

雲端網路工程師 (CNE) 負責網路服務與基礎架構低層級設計、網路功能開發與測試、容量佈建，以及網路組態設定定義。CNE 須履行下列職責：

- 確保滿足客戶需求與達到相關服務層級
- 將需求轉譯為邏輯藍圖與組態設定範本
- 設計、開發與測試例行工作 (例如整合、部署、監控與合規) 的自訂工作流程與指令碼
- 提供疑難排解協助給第 2 層級與第 3 層級支援、提議解決方案，並要求修正

雲端網路操作員 (CNO) 完全負責次要作業的所有層面、滿足應用程式作業需求 (例如效能與容量)，並維護雲端網路基礎架構、工具與平台。CNO 須履行下列職責：

- 執行並控制佈建、管理、監控、警示與疑難排解的自動化
- 主動監控雲端網路基礎架構，並在事件影響服務之前採取行動予以化解
- 進行疑難排解、根本原因分析、套用 CNE 提議的解決方案與修正
- 提供第 2 層級與第 3 層級支援，並管理事件、問題與向上提報

雲端安全性職務

雲端安全性架構設計師 (CSA) 完全負責架構、設計與支援雲端安全性基礎架構的所有層面。涵蓋範圍包括網路安全性虛擬化、自動化、協調作業與監控。CSA 須履行下列職責：

- 評估雲端基礎架構與應用程式的安全風險，並針對安全性策略與解決方案提供權威性指引
- 判定技術的安全性原則、流程，並稽核滿足雲端安全需求與達到此方面目標所需的功能
- 發展驗證測試方法，以驗證雲端安全性解決方案，並規劃與引導這類解決方案的實作
- 維持對威脅與風險移轉策略的透徹瞭解

雲端安全性工程師 (CSE) 負責將安全性原則轉譯為可稽核的安全性控制項。CSE 須履行下列職責：

- 設計並實作能落實雲端安全性控制項的實體與邏輯解決方案
- 協調雲端安全性流程 (控制、監控與稽核)，並將這些流程自動化
- 整合並實作能滿足需求並達到服務層級的雲端安全性服務與工具
- 參與向上提報、調查安全性缺口，建議並實作修正解決方案

雲端安全性操作員 (CSO) 負責瞭解、實作、強制執行、驗證並維護組織政策與風險評估需要的特定安全性控制項。CSO 須履行下列職責：

- 監控、偵測並分析安全性異常、漏洞與威脅
- 管理安全性記錄檔、確保符合記錄標準，並協助進行安全性稽核
- 調查、診斷並解決雲端安全性問題，以因應事件
- 實作針對漏洞的安全性解決方案與修正

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
台北市 110 信義路五段七號台北 101 大樓 57 樓 C 室 電話 +886-2-8758-2804 傳真 +886-2-8758-2708 www.vmware.com/tw