# VMware NSX® Advanced Load Balancer™

多雲應用程式服務：負載平衡、應用程式安全性、容器流入與分析

## 主要優勢

- 服務佈建速度加快 97%
- 透過應用程式運作狀況分數、應用程式分析、安全性和客戶洞悉，在數秒內迅速解決問題
- 透過隨選應用程式擴充，以及針對地端或雲端上任何裸機伺服器、虛擬機或容器提供支援，將 TCO 降低 30%
- 單一授權

## 包含的內容

在單一平台提供下列功能

- 第 4 層至第 7 層負載平衡
- 網頁應用程式防火牆 (WAF)
- 容器流入
- 全域伺服器負載平衡 (GSLB)
- 即時應用程式分析
- 透過客戶自行管理或軟體即服務等方式，進行隨選的應用程式自動延展

## 使用應用程式服務加速實現業務靈活性

現代化企業需要隨選、可快速部署且易於使用的應用程式交付解決方案，以在地端和雲端環境中實現多雲一致性。多雲和微服務正大舉帶動業務的 IT 靈活性。舊版基礎架構往往缺乏彈性和靈活性，而這兩者是安全且可靠交付應用程式所必備的條件。容器、API 和可觀察性的崛起，則提供大好良機，可讓基礎架構擺脫以應用裝置為基礎的方法限制，並蛻變為可組合、自動化與智慧化的型態。

### 平台功能

VMware NSX Advanced Load Balancer 是一款軟體定義架構，可區隔中央控制平台 (控制器) 與分散式資料轉發平台 (服務引擎)。NSX Advanced Load Balancer 具備完善的 REST API，可完全自動化，並與應用程式交付的 CI/CD Pipeline 順暢整合；這款經過精心打造的統一平台，能滿足現行數位化轉型環境的多項業務 IT 需求。NSX Advanced Load Balancer 致力於呼應應用程式在彈性、安全性和易於管理作業的訴求，不僅可透過隨選方式來水平擴充應用程式，還能偵測錯誤，使其成為可容錯且能自行修復的應用程式基礎架構。

這些功能都可透過封閉迴路式監控流程自動化，以提供自動執行的作業管理模式。進階分析 / 可觀察性能實現最佳化的應用程式交付，並運用內容感知的應用程式和 API 安全性，為應用程式交付作業及其資料提供保護。安全性原則會透過 PULSE 雲端服務的即時威脅更新，以保持最新狀態。

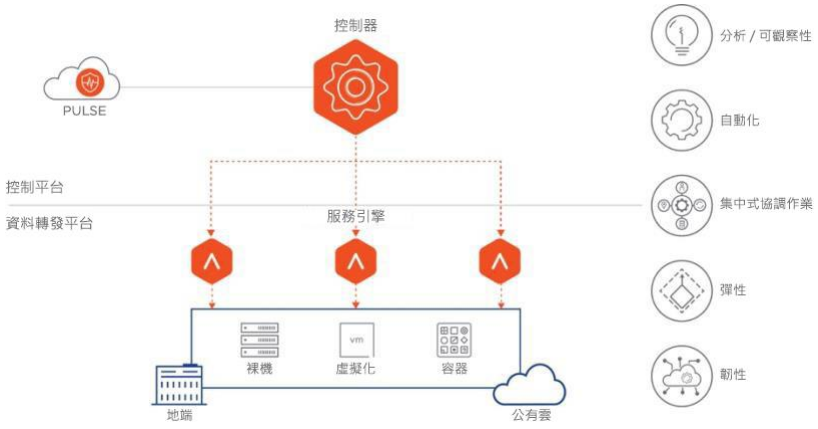


**圖 1**：高階架構

## 本機與全域負載平衡

在 VMware NSX Advanced Load Balancer 的使用情境中，控制器是整個系統的「大腦」，負責在企業級負載平衡、應用程式安全性、容器流入與分析中，擔任具有智慧、管理與控制能力的單一控制點角色。控制器會提供以封閉迴路式遙測為基礎的決策自動化，並根據應用程式監控、端對端時程安排、可搜尋的流量日誌記錄、安全性洞悉、日誌記錄洞悉、客戶洞悉等資料，呈現可運用的洞悉見解。隨附雲端服務的 NSX Advanced Load Balancer包含 PULSE 雲端服務，能為中央授權、安全性摘要和主動式支援等作業功能，提供持續的即服務使用模式。請參閱圖 1。

## 應用程式和 API 安全性

在網頁應用程式和 API 保護方面 (WAAP)，NSX Advanced Load Balancer 備有網頁應用程式防火牆 (WAF)、機器人管理，以及採用分散式網頁應用程式安全性架構的 API 保護。客戶可透過封閉迴路式分析，以及涵蓋 OWASP CRS 保護、合規規定 (PCI DSS、HIPAA 和 GDPR) 支援和簽章式偵測的應用程式學習模式，以強制落實安全性。WAF 的最佳化安全性 Pipeline 搭配主動式安全性模式，能讓耗用大量資源的作業發揮最大效率。PULSE 雲端服務可透過即時饋送提供最新的威脅更新，包括 IP 信譽、機器人偵測、簽章等資訊，並透過先進的安全性分析、偵測與強制執行模式，自動將誤報情形降至最低。即時應用程式安全性洞悉與分析功能，則可在具備端對端能見度的單一儀表板中，針對效能、終端使用者與安全性事件提供可運用的洞悉見解。請參閱圖 2。

### 重要功能

- 只要簡單的「指向並按一下」動作，即可執行中央控制的安全性原則
- 高效能的負載式自動水平擴充架構可彈性擴充
- 針對流量傳輸與規則相符情形提供精密的安全性洞悉，以建立精確原則
- 透過雲端服務提供自動化威脅更新
- 即時應用程式安全性洞悉與分析
- 保護應用程式免於 DDoS 攻擊與 OWASP 十大威脅的侵害

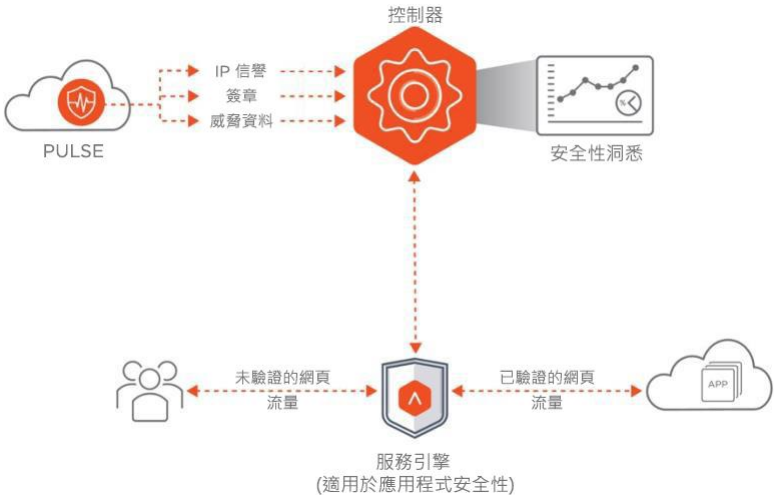


**圖 2：**適用於網頁應用程式的安全性洞悉

## Kubernetes 流入服務

相較於以微服務為基礎的現代化應用程式架構，以應用裝置為基礎的負載平衡解決方案，早已不合時宜。部署於 Kubernetes 叢集的容器化應用程式需要可延展的企業級解決方案，才能執行負載平衡、全域和本機流量管理、服務探索、監控 / 分析與安全性作業。然而，解決方案不能是多頭馬車，不應由平台團隊自行建置互不相通的產品，再加以拼湊而成。採用 Kubernetes 的企業，需要透過雲原生方法來管理流量並提供應用程式網路服務。對於現代化的容器式應用程式，NSX Advanced Load Balancer 提供一套經過整合的容器服務，包括雲原生、可延展、企業級容器流入流量管理、動態服務探索與安全性。請參閱圖 3。

### 重要功能

流量管理與服務探索

- 本機與全域負載平衡
- 網域名稱系統 (DNS) / IPAM / 電路斷路
- 運作狀況監控
- TLS 終止、憑證管理 / 自動化
- CI/CD 以及藍綠 / 金絲雀部署

安全性與可觀察性

- WAF
- 驗證
- 允許清單 / 拒絕清單
- 速率限制
- 偵測 / 削弱 DOS 攻擊
- 應用程式與基礎架構效能指標
- 交易追蹤與精細的日誌記錄

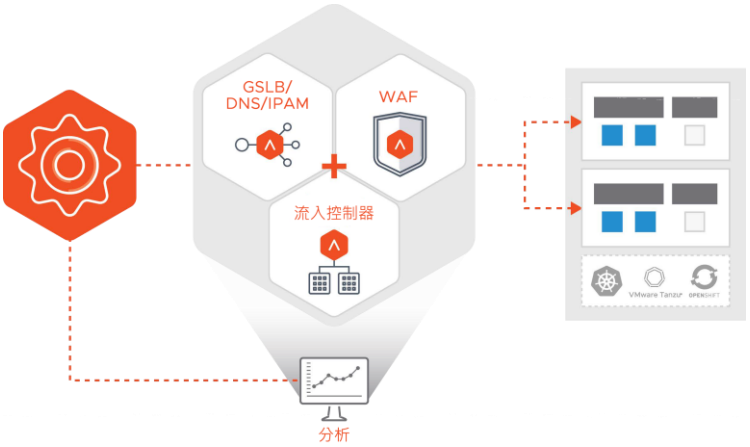


**圖 3**：Kubernetes 流入服務

## NSX Advanced Load Balancer 使用情境和商業網路

### 通用解決方案

NSX Advanced Load Balancer 經過精心設計，可運用在不同情境中。當中提供適用於多雲環境的平台，可藉由單一管理主控台因應各種環境。網頁應用程式安全性會透過解決方案關鍵元件的形式交付，以保護應用程式和資料。這項技術經過精心設計，能運用在傳統應用程式和容器微服務等項目上。

這款解決方案整合了多款 VMware 解決方案，包括 VMware Cloud Foundation、vCenter、Aria、Horizon VDI、Workspace One、NSX 和 vSphere 等。針對電信環境，NSX Advanced Load Balancer 則採用整合 VMware Telco Cloud Platform (TCP) 的設計，以支援 IPv6 和電信專用需求。


## 自動化佈建與自助式服務實現靈活性

透過個別應用程式負載平衡服務，進行自動化虛擬服務佈建

- 在短短數秒內完成應用程式佈建
- 利用 REST API 達成完全自動化，進而在藍綠與金絲雀部署中支援更快推出應用程式，也讓開發營運團隊能透過自助式入口網站處理工作
- 利用集中化原則簡化作業


## 簡化作業可降低成本

彈性的負載平衡與恰如其分的容量，可避免過度佈建

- 彈性的訂閱式授權模式可免除靜態容量
- 透過集中管理的簡化作業降低營運成本
- 不必重新設定，即可跨多雲環境提供一致的應用程式服務


## 在數秒內迅速解決問題

透過近乎即時的能見度掌握網路交易，快速進行疑難排解

- 藉由應用程式運作狀況分數，迅速瞭解網路概況
- 提供端對端往返時間與各個躍點之間的延遲情形
- 即時日誌記錄，用來記錄並重播流量和安全性事件

[1] IDC 公司《VMware NSX Advanced Load Balancer 的業務價值：使用新一代應用程式交付的企業研究》(The Business Value of Avi Vantage: A Study of Enterprises Using Next-Generation Application Delivery)

| 效能 - 單一服務引擎的觀察結果 | | |
|---|---|---|
| | 裸機伺服器 (24 合心) 配備 xl710 (40 Gbps) | 使用服務引擎做為 vCenter 虛擬機 (6C / 6GB) |
| SSL (EC) 連線上限 | 每秒 50K | 每秒 12K |
| SSL (RSA 2K) 連線上限 | 每秒 18K | 每秒 4000 |
| HTTP 請求數上限 | 每秒 700K | 每秒 185K |
| L4 TCP 連線上限 | 每秒 400K | 每秒 130K |
| SSL 總流量上限 | 38 Gbps | 10 Gbps |
| 租戶數 (共用的資料轉發平台) 上限 | 無限制 | 無限制 |
| 租戶數 (隔離的資料轉發平台) 上限 | 200 | 200 |
| 每一叢集的服務引擎上限 | 200 | 200 |

| VMware 整合 | | |
|---|---|---|
| vCenter | Google Cloud VMware Engine | Aria Automation (vRealize Automation) |
| VMware NSX | Oracle Cloud VMware Service | Aria Automation Orchestrator (vRealize Orchestrator) |
| VMware Cloud on AWS | VMware Tanzu | Aria Operations (vRealize Operations) |
| VMware Cloud Foundation (VCF) | VMware Horizon | Aria Operations for Networks (vRealize Network Insight) |
| Azure VMware Solution | vCloud Director (vCD) | Aria Operations for Logs (vRealize Log Insight) |

| 協力廠商整合 | 附註 |
|---|---|
| OpenStack | Queens、Rocky、Stein、RH OSP、Keystone v3 |
| 裸機 | RHEL、CentOS、Ubuntu、Oracle Enterprise Linux |
| 公有雲 | Microsoft Azure、Amazon Web Services (AWS)、Google Cloud Platform (GCP)、IBM Cloud、Oracle Cloud |
| 容器 | Kubernetes、Tanzu、Rancher、OpenShift、Amazon EKS、AKS、GKE |

| 協力廠商支援平台 | 附註 |
|---|---|
| 自動化 | Ansible、Terraform、Python/Java/Go SDK、vRO 外掛程式 |
| 分析 / 監控 | Splunk、Cisco Tetration、Cisco AppDynamics、Graphite、Datadog、Logstash、Elasticsearch、InfluxDB、Syslog、Prometheus、Zabbix |
| IPAM / 網域名稱系統 (DNS) | 網域名稱系統 (DNS)、Azure DNS、Azure DNS 私人區域、AWS Route 53、Infoblox、自訂網域名稱系統 (DNS) 整合、自訂 IPAM 整合 |

| 類別 | 功能 |
| --- | --- |
| 企業級負載平衡 | TLS 1.3 支援、SSL 終止、預設閘道、GSLB、網域名稱系統 (DNS)、Wildcard VIP 與其他第 4 層至第 7 層服務 |
| 多雲負載平衡 | 智慧型流量路由跨多個站點以及跨私有雲或公有雲，全域伺服器負載平衡作業支援指引站點和追隨站點的金絲雀型升級 |
| 應用程式效能監控 | 精密的日誌記錄可監控效能、記錄及重播網路事件 |
| 預測性自動延展 | 根據即時流量模式進行應用程式與負載平衡器擴充 |
| 雲端連接器 | VMware、SDN 控制器、OpenStack、AWS、GCP、Azure、Linux Server Cloud、VMware Cloud on AWS、Google Cloud VMware Engine、Azure VMware Solution (客戶自行管理) |
| 分散式應用程式安全性結構 | 利用來自分散式服務 Proxy 的精密應用程式洞悉，即時保護網頁應用程式 |
| 應用程式安全性 | 機器人管理 (技術預覽)、適用於 WAF 的主動式安全性模式和學習模式 |
| SSO / 用戶端驗證 | 後端 HTTP 應用程式採用 SAML 2.0 驗證與授權 |
| 自動化與可程式化的能力 | 以 REST API 為基礎的解決方案可加速應用程式交付，透過自助式入口網站將自動化從網路延伸到開發人員 |
| 應用程式分析 | 從即時提供數百萬個資料點的分散式負載平衡架構，取得即時遙測資料 |
| 集中式管理與升級 | 原則式管理，以及可透過彈性升級選擇性升級資料轉發平台 |
| 網路通訊協定支援 | BGP、RHI 與 ECMP、BFD、IPv6、VLAN 與主幹連線、VRF 感知、Radius 和 SIP |
| 整合式容器服務 | Kubernetes 服務包含可延展平台上的流入服務、WAF、GSLB、網域名稱系統 (DNS) / IPAM，可支援多叢集、多站點和多可用區域容器叢集 |
| 中央授權和能見度平台 | 透過集中式雲端服務控制所有雲端服務授權，並提供完整的全域和控制器儀表板 |



文件編號：vmw-ds-temp-uslet-word-2021 8/21