

VMware NSX® Advanced Load Balancer™ (Avi Networks)

多雲負載平衡、原生應用程式安全、可延展的容器入口
方案與分析

主要優勢

- 服務佈建速度加快 90%
- 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%

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
- 容器入口閘道
- 全域伺服器負載平衡 (GSLB)
- 即時應用程式分析
- 隨選應用程式自動擴充

應用程式服務加速實現業務靈活性

「遠端優先」已成為許多組織機構的常態，不僅是為了保護遠端員工的安全，也藉此確保以前所未有的速度維持業務續航力。我們執行業務及處理日常工作的方式經歷如此劇烈轉變，因此在不同環境提供應用程式的這種需求變得越來越迫切，不論時區或尖峰使用狀況為何。尤其是現行環境更講究彈性、機動性與靈活性，而傳統的基礎架構已經無法以安全可靠的方式交付應用程式。容器、API 和分析工具的興起，正是基礎架構擺脫以應用裝置為基礎的方法限制，蛻變為可組合、自動化與智慧化型態的良機。現代化企業需要隨選、可快速部署且易於使用的多雲解決方案，在地端和雲端環境中實現一致的應用程式交付。

軟體負載平衡器

VMware NSX Advanced Load Balancer (Avi Networks 提供) 採用軟體定義架構來區隔中央控制平台 (Avi 控制器) 與分散式資料轉發平台 (Avi 服務引擎)。NSX Advanced Load Balancer 是 100% 以 REST API 為基礎，因此完全可自動化，並與應用程式交付的持續整合 / 持續交付管道順暢整合。Avi 控制器是整個系統的「大腦」，在分散式資料轉發平台扮演單一智慧監控、管理與控制點的角色。Avi 服務引擎代表功能完整的企業級負載平衡器、網頁應用程式防火牆 (WAF) 與分析，可兼顧流量管理和應用程式安全性，同時從流量傳輸中收集即時分析數據。Avi 控制器以封閉迴路式遙測為基礎，提供全面的觀察力及呈現可運用的洞悉見解，以便根據應用程式監控、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、客戶洞悉等資料制定決策。請參閱圖 1。

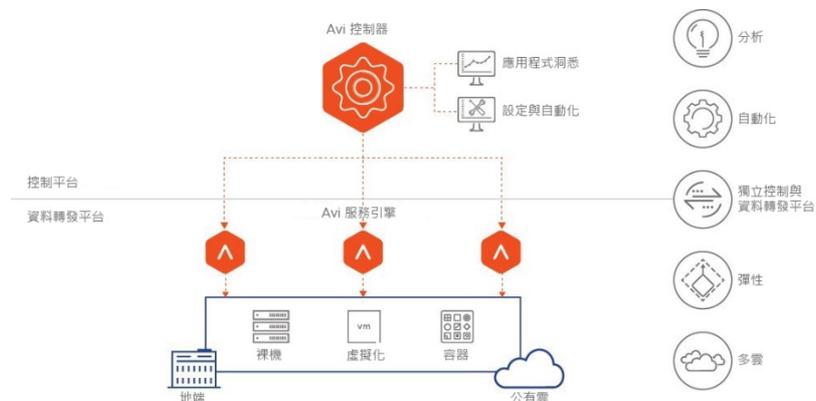


圖 1：NSX Advanced Load Balancer 高階架構

WAF iWAF 提供安全性洞悉

在安全性方面，Avi 的智慧型網頁應用程式防火牆 (iWAF) 採用分散式網頁應用程式安全性架構，除了透過封閉迴路式分析，也運用應用程式學習模式強制落實安全性，此模式涵蓋 OWASP CRS 保護，並支援 PCI DSS、HIPAA 與 GDPR 等合規規定，以及簽章式偵測。iWAF 的最佳化安全性管道搭配主動式安全性模式，可讓耗用大量資源的作業發揮最大效率。Avi Pulse 雲端服務即時饋送最新威脅消息，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控制面板 (Avi App Insights) 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 Avi Pulse 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

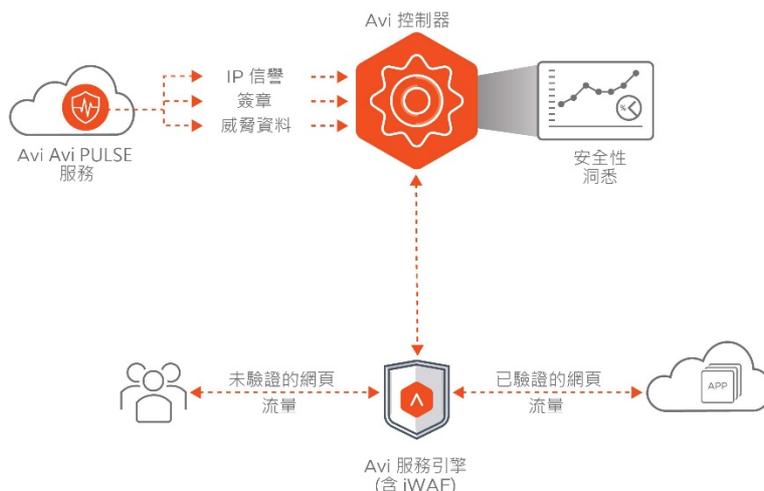


圖 2：iWAF 網頁應用程式安全性洞悉

Kubernetes 入口服務

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已然不合時宜。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，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管理流量及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、企業級容器入口流量管理、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
- 持續整合 / 持續交付以及藍綠 / 金絲雀

部署安全性與觀察性

- WAF
- 驗證
- 接受清單 / 封鎖清單
- 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

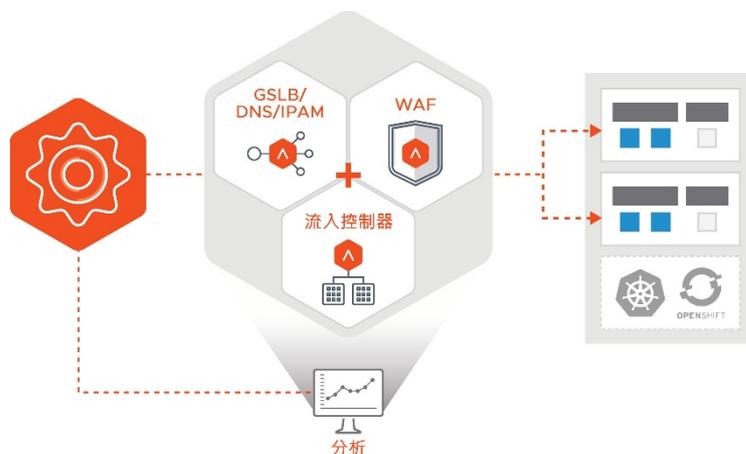


圖 3：Avi Kubernetes 流入服務



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

- 在數秒內佈建虛擬 IP (VIP)
- 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
- 透過應用程式交付自動化達成完整的生命週期管理
- 無須手動執行個別應用裝置設定



簡化作業可降低成本

彈性的負載平衡與恰如其份的容量避免過度佈建

- 沒有過度佈建的容量，也不需要持續重新整理、升級和維護個別硬體應用裝置
- 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
- 在高效能 Intel x86 伺服器上執行軟體定義的負載平衡作業，不需要自訂的主動-待命硬體
- 不必重新設定即可跨多雲環境提供穩定一致的應用程式服務



在數秒內迅速解決問題

透過如 Google 搜尋般的能見度掌握網路交易，以快速進行疑難排解

- 藉由應用程式運作狀況分數快速瞭解網路概況
- 提供端對端往返時間與各網路躍點之間的延遲情形
- 即時日誌記錄、記錄及重播流量事件
- 針對效能、安全性與終端使用者體驗提供精密的洞悉
- 執行「指向並按一下」動作即可進行應用程式疑難排解，不需要黑箱



彈性的自動擴充和高效能

根據即時流量使用分析導向的自動化作業進行隨選垂直擴充或縮減

- 自助式佈建可因應持續應用程式交付
- 持續整合 / 持續交付支援隨選負載平衡和應用程式自動擴充
- 服務引擎故障自動復原
- 自動針對網路、雲端和應用程式環境進行程式編寫
- 全面支援多雲，包括與 Azure、AWS、Google Cloud Platform 混合的地端部署環境

1. 《Avi Vantage 的商業價值：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)
2. VMware Data Integrated Customer Engagement (DICE) Tool (VMware 資料整合式客戶參與度 (DICE) 工具)
3. Principled Technologies 公司的《負載平衡基準測試報告》(Load Balancing Benchmark Report)

支援的平台		系統效能與規模	
VMware	vCenter、VMware NSX、VMware Cloud on AWS	系統總流量上限	10 Tbps
OpenStack	Queens、Rocky、Stein、RH OSP、Keystone v3	連線數上限	每秒 1 億
裸機	RHEL、CentOS、Ubuntu、Oracle Enterprise Linux、Cisco CSP (NFV 應用裝置)	同時連線數上限	100 億
容器	Kubernetes、OpenShift、Amazon EKS、AKS、GKE	HTTP 請求數上限	每秒 2 億
公有雲	Microsoft Azure、Amazon Web Services (AWS)、Google Cloud Platform (GCP)、IBM Cloud、Oracle Cloud	SSL TPS (2k RSA) 上限	1,000 萬
SDN	Cisco ACI/APIC、VMware NSX、Nuage VSP、Juniper Contrail	SSL TPS (SEC256r1 ECC) 上限	3,000 萬
IPAM / 網域名稱系統 (DNS)	Avi DNS、Azure DNS、Azure DNS 私人區域、AWS Route 53、Infoblox、自訂 DNS 整合	租戶數 (共用的資料轉發平台) 上限	無限制
自動化	Ansible、Terraform、Swagger、Python SDK、Go SDK、vRealize Orchestrator (vRO)、原生 REST API	租戶數 (隔離的資料轉發平台) 上限	200
監控	Splunk、Cisco Tetration、Cisco AppDynamics、Graphite、Datadog、Logstash、Elasticsearch、InfluxDB、Syslog、Prometheus、Zabbix	Avi 服務引擎數上限	200

功能	描述
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
預測性自動擴充	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、OpenShift/Kubernetes、VMware Cloud on AWS (由客戶管理)
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	網頁應用程式防火牆 (WAF) 採用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訊
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
整合式容器服務	Kubernetes 服務包含可延展平台上的入口服務、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



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com 11073 台北市信義區松仁路 100 號 38 樓之一台北南山廣場辦公大樓 電話 +886-2-3725-7000 傳真 +886-2-3725-7010 www.vmware.com/tw

Copyright © 2020-2021 VMware, Inc. 版權所有。本產品係受美國及國際之版權及智慧財產權相關法律保護。VMware 產品係受 <http://www.vmware.com/tw/download/patents.html> 上所列之一或多項專利的保護。VMware 係 VMware, Inc. 及其子公司在美國和其他管轄區域的註冊商標或商標。此處所提及的所有其他標誌和名稱，可能分別為其相關公司的商標。u07.20。文件編號：vmw-ds-temp-word-103-proof 5/19