

VMWARE PIVOTAL CONTAINER SERVICE

概觀

VMware® Pivotal Container Service (PKS) 是一項生產級 Kubernetes 容器解決方案，提供先進的網路、私有容器登錄工具，以及完整生命週期管理。PKS 能大幅簡化 Kubernetes 叢集的部署與作業，協助您大規模執行和管理私有雲與公有雲上的容器。

主要優勢

- 透過簡單的指令行介面或 API 進行 Kubernetes 叢集的隨選佈建、延展、修補與更新，以避免冗長的部署與管理程序。
- 存取最新且穩定的 Kubernetes 發行版本，並持續與 Google Kubernetes Engine (GKE) 相容。
- 運用漸進式升級、運作狀況檢查與自動修補底層虛擬基礎架構等方式，發揮 Kubernetes 元件 (主機、工作者與 etcd 節點) 的高可用性。
- 透過 VMware NSX® 簡化容器網路並提高安全性，以推動高可用性、自動化佈建、微分段、流入控制器、負載平衡與安全性原則。
- 可針對無狀態與具狀態應用程式部署 Kubernetes 叢集。
- 透過具備弱點掃描、映像簽名與稽核等功能的整合式企業容器登錄，確保應用程式部署安全無虞。

什麼是 Pivotal Container Service (PKS)?

PKS 是一款精心打造容器解決方案，旨在協助多雲企業與服務供應商充分運用 Kubernetes。PKS 能運用主要作業和次要作業支援，大幅簡化 Kubernetes 叢集的部署與作業。PKS 具備強化的生產級功能，可用來進行容器部署，讓您從應用程式層到基礎架構層，一路暢行無阻。

PKS 備有多項關鍵生產功能，包括高可用性、自動延展、運作狀況檢查與自行修補底層虛擬機器，以及 Kubernetes 叢集的漸進式升級。PKS 能持續相容於 GKE，以提供最新且穩定的 Kubernetes 發行版本，進而讓開發人員能坐擁最新的功能與工具。此外，當中整合了 VMware NSX-T，可構築先進的容器網路，一舉囊括微分段、流入控制器、負載平衡與安全性原則等功能。PKS 具備整合式的私有登錄機制，可透過弱點掃描、映像簽名與稽核等功能來確保容器映像安全無虞。

PKS 會以 Kubernetes 的原生型態加以公開，不會加入任何抽象層或專屬延伸功能，因此可讓開發人員使用他們最為熟悉的原生 Kubernetes 指令行介面。Pivotal Operations Manager 可運用常見的運作模式，將 PKS 部署至多個基礎架構即服務抽象層 (例如 vSphere 與 Google Cloud Platform)，以輕鬆部署與運用 PKS。

Pivotal Container Service 架構

PKS 是採用 Kubernetes、BOSH、VMware NSX-T 與 Project Harbor 為基礎所建置而成的生產級、高度可用容器服務，可於 VMware vSphere® 和公有雲上執行。PKS 內建智慧型功能與整合功能，可密切統整上述所有開放式原始碼與商用模組，以提供客戶簡單易用的產品，同時為客戶帶來最符合效率的 Kubernetes 部署與管理經驗。

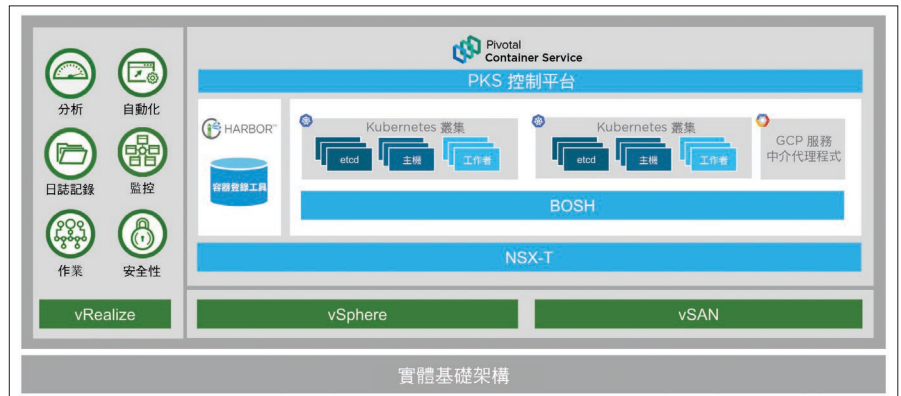


圖 1. VMware Pivotal Container Service 能與 VMware 軟體定義的資料中心搭配運作，以建構全方位解決方案

KUBERNETES 認證



PKS 通過 Cloud Native Computing Foundation® (CNCF) 的 Kubernetes Software Conformance Certification 計畫的認證，可讓客戶確信自身的應用程式部署

既符合 CNCF 測試套件的標準，也符合社群規格。鑑於採用 Kubernetes 的組織與日俱增，PKS 等通過 Kubernetes 認證的產品將有助於確保不同環境的可移植性、互通性與一致性。

Kubernetes

Kubernetes 是一款採用開放式原始碼的容器協調架構。容器會將應用程式及其相依項目封裝為可散發的成品（容器映像），以實現跨越多個環境的可移植性，進而簡化軟體的開發與部署作業。Kubernetes 會協調這些容器，以便管理資源利用、錯誤處理、可用性、設定、延展性與應用程式的目標狀態，並加以自動化。當應用程式及其服務在虛擬機分散式叢集的容器中執行時，Kubernetes 會編排所有移動元件，好讓這些項目能以同步化的方式運作，進而妥善運用運算資源，並維持應用程式的目標狀態。

BOSH

BOSH 是一款適用於發行版本工程的開放式原始碼工具，可簡化大型分散式系統的部署與生命週期管理作業。BOSH 可協助開發人員以一致且可重現的方式，輕鬆管理軟體版本、進行封裝並加以部署。BOSH 可支援不同基礎架構即服務的部署作業，例如 VMware vSphere、Microsoft Azure、OpenStack、Google Compute Platform (GCP) 與 Amazon Web Services EC2 (AWS EC2)，而且自問世以來，也於 Cloud Foundry 平台的部署與管理領域寫下卓越實績。

VMware NSX-T

VMware NSX-T 可為 Kubernetes 叢集構築先進的容器網路與安全功能，包括微分段、流入控制器、負載平衡與安全性原則。VMware NSX-T 可提供涵蓋第 2 層到第 7 層的完整網路服務，以滿足機組等級網路需求。由於 PKS 中已整合 NSX-T，因此，企業將可透過微分段功能迅速部署網路，並完成容器與機組的隨選網路虛擬化作業。

Project Harbor

Harbor 是一款採用開放式原始碼的企業級登錄伺服器，可在您的防火牆後方，透過私有登錄功能來儲存並散發 Docker 映像。Harbor 不僅提供角色型存取控制 (RBAC)、輕量級目錄存取協定 (LDAP)/Active Directory (AD) 支援，還可讓企業進行容器映像弱點掃描、原則式映像複寫，以及公證與稽核服務。

PKS 控制平台

控制平台為 PKS 的主要元件，這個自助介面會負責進行 Kubernetes 叢集的隨選部署與生命週期管理作業。當中的 API 介面可用來推動 Kubernetes 叢集的自助使用。該 API 會將要求提交至 BOSH，讓 BOSH 根據使用者要求來自動建立、更新與刪除 Kubernetes 叢集。

Pivotal Container Service 的主要功能

完整的生命週期管理與自動化

PKS 可進行 Kubernetes 的生命週期管理與自動化，進而加快部署、延展、修補和更新速度，並簡化這些作業。PKS 提供簡單的動作式命令行介面與公開的 API，可支援 Kubernetes 生命週期內的多種使用情境。只要使用 PKS，IT 管理員就能在短短數分之內部署多個 Kubernetes 叢集。此外，Kubernetes 叢集的延展作業也可透過簡單的命令行介面或 API 呼叫完成。使用 PKS，即可運用相同的機制完成一個或多個 Kubernetes 叢集的修補與更新作業，如此一來，您就能確保叢集可跟上最新安全性與維護更新的腳步。如果已不再需要叢集，使用者也可迅速加以刪除。

高可用性

PKS 提供眾多關鍵的生產級功能，可確保 Kubernetes 叢集中執行的工作負載能享有最大限度的不停機時間。PKS 會持續監控所有底層虛擬機執行個體的運作狀況，並在節點發生故障或無法回應時重新建立虛擬機。此外，PKS 也能管理多個 Kubernetes 叢集的漸進式升級流程，在應用程式負載無須停機的情況下升級叢集。

先進的容器網路與安全性

NSX-T 可為容器介面與 Kubernetes 機組提供自動化、軟體定義的網路，讓 PKS 如虎添翼。NSX-T 負載平衡服務位於高度可用且完整備援的 NSX Edge™ 叢集上，因此，如有任何負載平衡器發生故障，流量就會自動導向另一個負載平衡器。這些負載平衡服務都已與 Kubernetes Ingress 和負載平衡器結構完整整合。NSX 會新增微分段，以滿足工作負載的隔離需求。每個 Kubernetes 命名空間都可以彼此隔離，而網路原則也可指定流量將以何種方式在 Kubernetes 命名空間之間和之內移動。

有了 PKS，即可將 NSX 中的任何廣泛多樣的原則套用到容器網路。操作工具與疑難排解公用程式（例如 Traceflow、連接埠鏡射與連接埠連線工具），也可用來滿足容器化應用程式的生產網路需求。

安全的容器登錄

PKS 提供企業級的容器登錄機制，可享有安全且先進的服務。PKS 容器登錄備有透過 RBAC 與 AD/LDAP 整合進行的使用者管理與存取控制，可確保為容器映像提供適當的授權層級與存取權限。此外，當中也提供映像公證服務等安全功能，可讓發佈者於推送期間簽署映像，並避免擷取未簽署的映像，進而達到內容信任的目的。有了 PKS 的私有登錄，使用者就能掃描容器映像是否具有弱點，以降低受感染容器映像所帶來的安全性漏洞風險。

持續與 Google Kubernetes Engine (GKE) 相容

PKS 是使用主流的 Kubernetes 開發而成，可為您的開發人員提供最新且穩定的 Kubernetes 發行版本。PKS 確保與 GKE 支援的 Kubernetes 版本持續相容，好讓企業開發人員能在 vSphere 與 GKE 使用的最新功能與修補程式。此外，PKS 也會以原生形式公開 Kubernetes，不會在 Kubernetes 上方新增任何專屬的抽象層，因此，開發人員或開發工具都可使用原生的 Kubernetes 介面與 Kubernetes 進行互動，而工作負載也可於 vSphere 與 GKE 之間輕鬆移轉。

持續性儲存

PKS 可讓客戶針對無狀態與具狀態應用程式部署 Kubernetes 叢集。PKS 可透過 [Project Hatchway](#) 支援屬於 Kubernetes 的 vSphere 雲端供應商儲存外掛程式。正因如此，PKS 可支援多種 Kubernetes 儲存原始物件，例如 vSphere 儲存上的磁區、持續性磁區 (PV)、持續性磁區宣告 (PVC)、儲存類別與具狀態的集合，同時為 Kubernetes 架構的應用程式提供眾多企業級儲存功能，像是 VMware vSAN™ 隨附的 Storage Policy Based Management (SPBM)。

多租戶

PKS 可針對企業中的多個業務線提供多租戶支援，以達到隔離工作負載與確保隱私權等目的。不同業務線的使用者皆可使用專屬的 Kubernetes 叢集。此外，在 NSX-T 微分段的助陣下，即使讓多個團隊共用叢集，Kubernetes 命名空間依舊安全無虞。

多雲

PKS 可透過 BOSH 支援多雲部署。有了 PKS，您就能在 vSphere 上的內部部署或 Google Cloud Platform 等公有雲上，使用 Kubernetes 部署容器化的應用程式。

PKS 功能清單	
功能	優勢
隨選佈建	<ul style="list-style-type: none"> • 加快 Kubernetes 叢集的部署作業 • 不需使用手動步驟，就能部署 Kubernetes 叢集 • 盡可能減少錯誤，並縮短實現價值的時間
隨選延展	<ul style="list-style-type: none"> • 輕鬆延展叢集容量 • 不需要手動步驟，且可避免錯誤 • 最佳化資源使用率
隨選修補	<ul style="list-style-type: none"> • 集中進行多個 Kubernetes 叢集的修補與更新作業，並加快其速度 • 確保 Kubernetes 叢集的最新狀態且安全無虞
漸進式升級	<ul style="list-style-type: none"> • 漸進式升級多個 Kubernetes 叢集，將工作負載的停機時間降至最低
自動進行運作狀況檢查與自我修復	<ul style="list-style-type: none"> • 主動監控所有節點的運作狀況，以防範於未然 • 重新建立故障/沒有回應的節點，以確保應用程式服務能維持必要的回應能力
先進的容器網路與安全性	<ul style="list-style-type: none"> • 簡化網路管理作業並強化安全性，以提高開發人員與操作人員的生產力 • 實現最佳化的原生容器網路，一舉囊括自動佈建、微分段、Ingress 控制器、負載平衡與安全性原則等功能
安全的容器登錄	<ul style="list-style-type: none"> • 運用強化的容器安全性，將應用程式漏洞的風險降至最低 • 透過映像複寫、RBAC、AD/LDAP 整合、公證服務、弱點掃描與稽核，簡化容器映像管理並強化安全性
持續與 GKE 相容	<ul style="list-style-type: none"> • 協助開發人員存取最新的 Kubernetes 功能與工具，以強化自身的生產力 • 可在內部部署的 vSphere 環境與 GKE 之間移轉工作負載
原生 Kubernetes 支援	<ul style="list-style-type: none"> • 以原生方式公開 Kubernetes，且不加入任何專屬延伸，因此無需受限於廠商 • 為開發人員提供原生的 Kubernetes 指令行介面與完整的 YML 支援，以提高其生產力
通過 CNCF 認證的 Kubernetes Distro	<ul style="list-style-type: none"> • 符合社群規格 • 確保不同環境的跨雲可移植性、互通性與一致性
多租戶	<ul style="list-style-type: none"> • 為個別使用者提供專屬的 Kubernetes 叢集 • 確保租戶之間的工作負載安全，並提供隱私權

深入瞭解

若要進一步瞭解 Pivotal Container Service，請造訪 PKS 頁面：<https://cloud.vmware.com/pivotal-container-service>。

PKS 功能清單	
功能	優勢
持續性儲存	<ul style="list-style-type: none"> • 可針對無狀態與具狀態應用程式部署 Kubernetes 叢集 • 透過 Project Hatchway 支援 vSphere 雲端供應商儲存外掛程式
多雲	<ul style="list-style-type: none"> • 在 vSphere 與 Google Cloud Platform 上提供一致的介面來部署與管理 Kubernetes，進而在多雲環境中實現最佳化的工作負載部署

