VMWARE PIVOTAL CONTAINER SERVICE

概览

VMware® Pivotal Container Service (PKS) 是一个基于 Kubernetes 的生产级容器解决方案，并配备高级网络连接、专有容器注册表和完整的生命周期管理功能。PKS 从根本上简化了 Kubernetes 集群的部署和运维，以便您可在私有云和公有云上大规模运行和管理容器。

主要优势

- 通过简单的 CLI 或 API 按需调配、扩展、修补和更新 Kubernetes 集群，从而消除冗长的部署和管理流程。
- 访问最新稳定的 Kubernetes 版本并获得与 Google Kubernetes Engine (GKE) 的持续兼容性。
- 通过滚动升级、运行状况检查和底层虚拟基础架构的自动修复，为 Kubernetes 组件（master 节点、worker 节点和 etcd 节点）提供高可用性。
- 使用 VMware NSX® 简化容器网络连接和提高安全性，可提供高可用性、自动调配、微分段、传入控制器、负载均衡和安全策略。
- 为无状态和有状态的应用部署 Kubernetes 集群。
- 通过集成的企业容器注册表安全地进行应用部署，包括漏洞扫描、映像签名和映像审核。

Pivotal Container Service (PKS) 是什么?

PKS 是一种容器解决方案，专为多种云环境的企业和服务提供商构建，以让 Kubernetes 高效运转。凭借初始和后续的运维支持，它从根本上简化了 Kubernetes 集群的部署和管理。通过强化的生产级功能，PKS 能够很好地胜任从应用程序层到基础架构层的容器部署。

PKS 内置关键产品功能，如高可用性、自动扩展、底层 VM 的运行状况检查和自我修复，以及 Kubernetes 集群的滚动升级。PKS 能与 GKE 持续兼容，提供最新的稳定 Kubernetes 版本，因此开发人员可以使用其最新的功能和工具。它还与 VMware NSX-T 集成，以实现高级容器网络连接，包括微分段、ingress controller、负载均衡和安全策略。通过集成的专有注册表，PKS 运用漏洞扫描、映像签名和审核来保护容器映像。

PKS 不添加任何抽象层或专有扩展层，以其原生形式展现 Kubernetes，这使开发人员可使用他们最熟悉的原生 Kubernetes CLI。PKS 可以通过 Pivotal Operations Manager 轻松部署和高效运转，该管理器允许一个通用的运维模式跨多个 IaaS 抽象工具（如 vSphere 和 Google Cloud Platform）部署 PKS。

Pivotal Container Service 体系结构

PKS 以 Kubernetes、BOSH、VMware NSX-T 和 Project Harbor 为基础构建，形成一种高度可用的生产级容器服务，这种服务可在 VMware vSphere® 和公有云上运行。凭借内置的智能和集成功能，PKS 将所有的开源和商用模块连接在一起，为客户提供了一种易于使用的产品，确保客户体验到最有效的 Kubernetes 部署和管理。

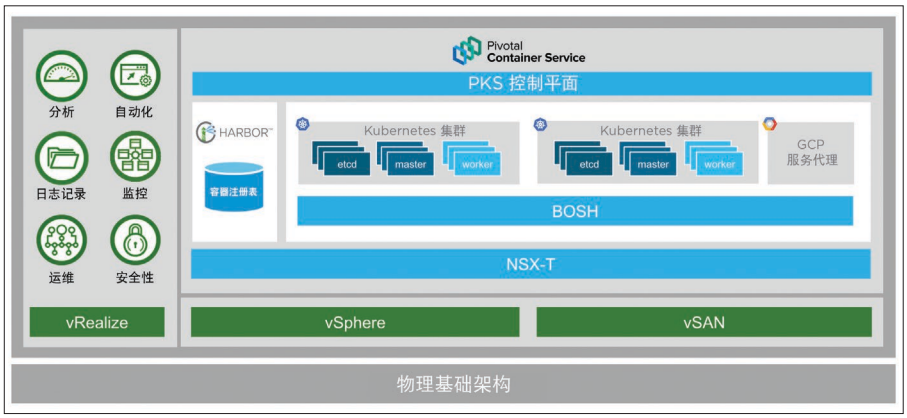

图 1. VMware Pivotal Container Service 与 VMware SDDC 合作以提供全面的解决方案

KUBERNETES 认证

由 Cloud Native Computing Foundation® (CNCF) 在 PKS 的 Kubernetes 软件一致性认证计划中认证，PKS 的部署已通过 CNCF 测试套件并符合社区规范，从而让客户可放心使用。随着越来越多的组织采用 Kubernetes，像 PKS 这样经过认证的 Kubernetes 产品，确保了不同环境之间的可移动性、互操作性和一致性。

Kubernetes

Kubernetes 是一个开源的容器编排框架。容器将应用及其依赖关系打包到一个可分发的构件中（容器映像），这个构件可移动到多个环境中，从而简化软件的开发和部署。Kubernetes 编排这些容器，以自动化管理应用的资源利用、故障处理、可用性、配置、可扩展性和理想状态。作为一个自身的服务在分布式虚拟机集群上的容器中运行的应用，Kubernetes 编排所有移动块，以便它们同步运行，优化计算资源的使用并保持应用的理想状态。

BOSH

BOSH 是一款用于发布工程的开源工具，可简化大型分布式系统的部署和生命周期管理。它使开发人员能够以一致且可重现的方式轻松进行版本管理、打包和部署。BOSH 可跨不同 IaaS 支持部署，例如 VMware vSphere、Microsoft Azure、OpenStack、Google Compute Platform (GCP) 和 Amazon Web Services EC2 (AWS EC2)，并且自 BOSH 建立以来，它已成功用于部署和管理 Cloud Foundry 平台。

VMware NSX-T

VMware NSX-T 为 Kubernetes 集群提供高级容器网络连接和安全功能，如微分段、ingress controller、负载均衡和安全策略。它提供 pod 级网络连接所需的第 2 层到第 7 层的全套网络服务。通过在 PKS 中集成 NSX-T，企业可以快速部署网络，为容器和 pod 提供微分段和按需网络虚拟化。

Project Harbor

Harbor 是一个开源的企业级注册表服务器，用于在防火墙后的专用注册表中存储和分发容器映像。除了提供 RBAC（基于角色的访问控制）、LDAP（轻型目录访问协议）/AD (Active Directory) 支持外，Harbor 还使企业能够进行容器映像漏洞扫描、基于策略的映像复制以及公证和审核服务。

PKS 控制平面

作为 PKS 的一个关键组件，控制平面是负责 Kubernetes 集群的按需部署和生命周期管理的自助服务接口。它提供了一个 API 界面，并支持 Kubernetes 集群的自助使用。API 将请求提交给 BOSH，BOSH 根据用户请求自动创建、更新和删除 Kubernetes 集群。

Pivotal Container Service 的核心功能

完整的生命周期管理和自动化

PKS 为 Kubernetes 提供生命周期管理和自动化，这使部署、扩展、修补和更新变得简单快捷。它提供了一个简单而基于操作的命令行界面和一个面向公众的 API，该 API 在 Kubernetes 的整个生命周期内可运用于多种用户场景。借助 PKS，IT 管理员可以在几分钟内部署多个 Kubernetes 集群。通过简单的 CLI 或 API 调用也可以轻松完成 Kubernetes 集群的扩展。通过相同的机制，PKS 使修补和更新一个或多个 Kubernetes 集群变得更容易，确保您的集群始终与最新的安全和维护更新保持同步。如果不再需要集群，用户可将其快速删除。

高可用性

PKS 提供关键的生产级功能，以确保在 Kubernetes 集群中工作负载的最长正常运行时间。它持续监测所有底层 VM 实例的运行状况，并在出现故障或无响应节点时重建 VM。它还管理一批 Kubernetes 集群的滚动升级流程，使集群得以升级，而不会出现应用工作负载的停止运行。

高级容器网络连接和安全性

NSX-T 为 PKS 配备了一个用于容器界面和 Kubernetes pod 的自动化软件定义网络。NSX-T 负载均衡的服务位于一个高度可用、完全冗余的 NSX Edge™ 集群上，因此如果一个负载均衡器停止运行，流量会自动转移到另一个负载均衡器。这些负载均衡服务与 Kubernetes Ingress 和 LoadBalancer 结构全面集成。NSX 添加了微分段，以满足工作负载的隔离需求。每个 Kubernetes 命名空间可彼此隔离，而网络策略可以指定流量如何在 Kubernetes 命名空间之间及内部移动。

通过 PKS，NSX 中的各种策略均可应用于容器的网络连接。操作工具和故障排除实用程序，如：Traceflow、端口镜像和端口连接工具，也可用于满足容器化应用的产品网络连接要求。

安全容器注册表

PKS 为企业级容器注册表提供安全先进的服务。PKS 容器注册表包括实现 RBAC 和 AD/LDAP 集成的用户管理和访问控制，确保为容器映像提供适当级别的授权和访问权限。它还提供一些安全功能（如映像公证服务），通过让发布者在推送和防止未签名映像被提取的过程中，对映像进行签名，以确保其内容的可信度。借助 PKS 的专有注册表，用户可以扫描容器映像以查找漏洞，从而降低与受污染容器映像相关的安全漏洞风险。

与 Google Kubernetes Engine (GKE) 始终兼容

PKS 是使用主线 Kubernetes 开发的，为您的开发人员提供最新版本的稳定 Kubernetes。它确保了与 GKE 支持的 Kubernetes 版本的持续兼容性，因此企业开发人员可使用 vSphere 和 GKE 上的最新功能和补丁。此外，在 Kubernetes 上不添加任何专有抽象层的情况下，PKS 以其原生形式公开 Kubernetes，让开发人员或开发工具通过使用本地 Kubernetes 接口与 Kubernetes 进行交互，并使工作负载在 vSphere 和 GKE 之间轻松转移。

持久存储

PKS 允许客户为无状态和有状态的应用部署 Kubernetes 集群。它通过基于 Project Hatchway 技术的 vSphere Cloud Provider 插件来提供存储功能。如此一来，PKS 便可支持 vSphere 存储中的 Kubernetes 存储基元，如卷、持久性卷 (PV)、持久性卷声明 (PVC)、存储类和状态集等，还可为基于 Kubernetes 的应用引入企业级存储功能，如由 VMware vSAN™ 提供的基于存储策略的管理 (SPBM)。

多租户

为了隔离工作负载并确保隐私，PKS 支持企业内多个业务线的多个租户。来自不同业务线的不同用户可使用他们自己的 Kubernetes 集群。此外，通过 NSX-T 微分段，多个团队可使用一个共享集群保护他们的 Kubernetes 命名空间。

多种云环境

PKS 通过 BOSH 支持多种云环境部署。通过使用 PKS，您可使用 Kubernetes 在 vSphere 上本地部署容器化应用，或将容器化应用部署在公有云（如：Google Cloud Platform）上。

PKS 功能列表	
功能特性	**优势**
按需调配	• 加快 Kubernetes 集群的部署 • 不再需要手动部署 Kubernetes 集群 • 最大限度减少错误并缩短价值实现时间
按需扩展	• 轻松扩展集群容量 • 消除手动步骤和错误 • 优化资源利用率
按需修补	• 集中并加速修补和更新多个 Kubernetes 集群 • 使 Kubernetes 集群保持最新性和安全性
滚动升级	• 通过滚动升级成批 Kubernetes 集群，最大限度地减少工作负载的停机时间
自动运行状况检查和自我修复	• 避免出现主动监控所有节点的运行状况的问题 • 通过重建失败/无响应的节点来确保应用服务的理想响应能力
高级容器网络连接和安全性	• 通过简化网络连接管理并增强安全性，提高开发人员和操作人员的工作效率 • 优化本地容器网络连接，包括自动调配、微分段、ingress controller、负载均衡和安全策略
安全容器注册表	• 通过增强的容器安全性最大程度地减少应用漏洞 • 通过映像复制、RBAC、AD/LDAP 集成、公证服务、漏洞扫描和审核，简化容器映像管理并增强安全性
与 GKE 始终兼容	• 通过允许开发人员访问最新的 Kubernetes 功能和工具来提高开发人员的工作效率 • 允许工作负载在 vSphere 环境内部和GKE之间移动
原生 Kubernetes 支持	• 以原生形式展现 Kubernetes，不添加专有扩展，防止供应商锁定 • 通过为开发人员提供原生 Kubernetes CLI 和全面的 YMAL 支持来提高开发人员的工作效率
CNCF 认证的 Kubernetes Distro	• 社区规范合规性 • 确保跨云的不同环境之间的可移动性、互操作性和一致性
多租户	• 为个人用户提供他们自己的 Kubernetes 集群 • 保护租户之间的工作负载并提供隐私空间

了解更多

要了解有关 Pivotal Container Service 的更多信息，请访问 PKS 页面 https://cloud.vmware.com/pivotal-container-service。

PKS 功能列表	
功能特性	**优势**
持久存储	• 为无状态和有状态的应用部署 Kubernetes 集群 • 通过 Project Hatchway 支持 vSphere Cloud Provider 存储插件
多种云环境	• 通过提供一致的界面在 vSphere 和 Google Cloud Platform 上部署和管理 Kubernetes，优化多种云环境中的工作负载部署

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京办公室 北京朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：86-10-5976-6300 传真：86-10-5976-6302
中国上海办公室 上海市淮海中路 333 号瑞安大厦 804-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101 www.vmware.com/cn