VMWARE® PKS

概览

VMware® PKS 是一个基于 Kubernetes 的生产级容器解决方案，具备高级网络连接、专有容器镜像仓库和完整的生命周期管理功能。VMware PKS 从根本上简化了 Kubernetes 集群的部署和运维，使您可以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过程。
- 访问 Kubernetes 的最新稳定版本并获得与 Google Kubernetes Engine (GKE) 的持续兼容性。
- 通过多可用区支持和多主控主机支持，并针对底层虚拟基础架构执行滚动升级、运行状况检查和自动修复，为 Kubernetes 组件（master 节点、worker 节点和 etcd 节点）提供高可用性。
- 使用 VMware NSX-T 简化容器网络连接和提高安全性，从而提供高可用性、自动调配、微分段、入口控制器、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镜像仓库安全地进行应用部署，包括漏洞扫描、镜像签名和镜像审核。
- 通过与 Wavefront by VMware 和 vRealize Log Insight 现成集成，提供监控、日志记录和分析功能，从而提升运维效率。

什么是 VMware PKS?

VMware PKS 是一种容器解决方案，专为多云企业和服务提供商高效实施 Kubernetes 而构建。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，VMware PKS 能够很好地执行从应用层到基础架构层的各种容器部署。

VMware PKS 内置关键生产功能，如高可用性、自动扩展、运行状况检查，以及 Kubernetes 集群的自我修复和滚动升级。 VMware PKS 能与 GKE 持续兼容，提供了 Kubernetes 的最新稳定版本，因此开发人员可以使用最新的功能和工具。此外，它还与 VMware NSX-T 集成，以实现高级容器网络连接，以及微分段、入口控制器、负载均衡和安全策略。通过集成的专有镜像仓库，VMware PKS 运用漏洞扫描、镜像签名和审核来保护容器镜像。

VMware PKS 不添加任何抽象层或专有扩展层，以原生形式展现 Kubernetes，这使开发人员可使用他们最熟悉的原生 Kubernetes CLI。VMware PKS 可以通过 Pivotal Operations Manager 轻松部署和高效运转，该管理器允许通过一个通用的运维模式跨多个 IaaS 抽象工具（如 VMware vSphere®、Google Cloud Platform (GCP) 和 Amazon Web Services (AWS) EC2）部署 VMware PKS。

VMware PKS 体系架构

VMware 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运行时，可在 vSphere 和公有云上运行。凭借内置的智能和集成功能，VMware 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。

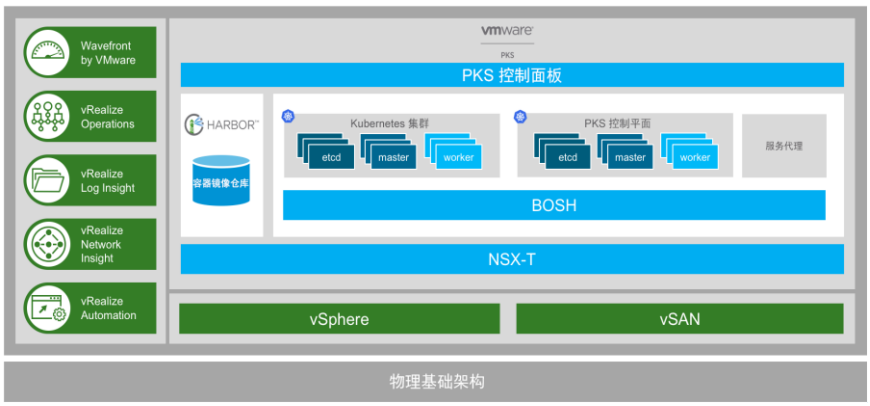

图 1. VMware PKS 与 VMware SDDC 协作以提供全面的解决方案。

KUBERNETES 认证

VMware PKS 获得了 Cloud Native Computing Foundation® (CNFC®) 的 Kubernetes 软件一致性认证计划认证，客户可以放心地运行应用，因为其部署已通过测试套件中的各项测试并且符合社区规范。随着越来越多的企业采用 Kubernetes，像 VMware PKS 这样经过认证的 Kubernetes 产品可确保不同环境之间的可移动性、互操作性和一致性。

Kubernetes

Kubernetes 是一个开源容器编排框架。Kubernetes 可以编排容器，以便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并使相关操作自动化。对于应用及其服务均在分布式虚拟机集群上的容器中运行的容器化应用，Kubernetes 可为其编排所有移动块，以便它们同步运行，从而优化计算资源的使用并使应用保持理想状态。

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软件版本管理、打包和部署。BOSH 可跨不同 IaaS 支持部署，例如 VMware vSphere、Amazon Web Services EC2 (AWS EC2)、Microsoft Azure、Google Compute Platform (GCP) 和 OpenStack，并且 BOSH 自问世以来，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、入口控制器、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 VMware 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 是值得信赖的云原生镜像仓库，它以提供能够信心十足地管理和提供容器镜像的云原生环境为使命，可对内容进行存储、签名和扫描。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 还为企业提供容器镜像漏洞扫描、基于策略的镜像复制以及公证和审核服务。

VMware PKS 控制平面

作为 VMware PKS 的一个关键组件，控制平面是负责对 Kubernetes 集群执行按需部署和生命周期管理的自助服务界面。它提供了一个 API 界面，并支持自助使用 Kubernetes 集群。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。

VMware PKS 的主要功能

完整的生命周期管理和自动化

VMware 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 VMware 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，VMware 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

VMware PKS 提供关键的生产级功能，以确保在 Kubernetes 集群中运行的工作负载达到最长的正常运行时间。借助多可用区和多主控主机/etcd 支持，它大幅提升了在生产环境中运行关键工作负载的 Kubernetes 集群的高可用性。

此外，VMware PKS 持续监控所有底层虚拟机实例的运行状况，并在出现有故障或无响应的节点时重新创建虚拟机。它还管理一批 Kubernetes 集群的滚动升级流程，使集群升级不会导致应用工作负载停止运行。

高级容器网络连接和安全性

NSX-T 为 VMware 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-T 还添加了微分段，以满足工作负载的隔离要求。使用 NSX-T，您可以部署 Kubernetes 集群，以便每个集群的节点可以位于单独的子网上。这样，可以更加轻松地创建安全策略，以便在 Kubernetes 集群之间以及 Kubernetes 命名空间内部实现网络流量隔离。现在，网络管理员可以快速识别流量的性质（源于/流向 Kubernetes 节点或 pod），并确定网络流量属于哪个 Kubernetes 集群。

通过 VMware PKS，各种 NSX 策略均可应用于容器网络连接。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生产级网络连接要求。

安全容器镜像仓库

VMware PKS 为企业级容器镜像仓库提供安全先进的服务。VMware PKS 容器镜像仓库能够借助 RBAC 和 AD/LDAP 集成来执行用户管理和访问控制，这可确保针对容器镜像为用户提供适当级别的授权和访问权限。它还提供了一些安全功能。例如镜像公证服务可让发布者在推送过程中对镜像进行签名，并能防止用户提取未签名的镜像，从而确保内容的可信度。借助 VMware PKS 的专有镜像仓库，用户还可以扫描容器镜像以查找漏洞，从而降低与受影响容器镜像相关的安全漏洞风险。

与 Google Kubernetes Engine (GKE) 始终兼容

VMware PKS 是使用主线 Kubernetes 开发的，为您的开发人员提供 Kubernetes 的最新稳定版本。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 的最新功能和补丁。此外，VMware PKS 不在 Kubernetes 上添加任何专有抽象层，以原生形式展现 Kubernetes，让开发人员或开发工具能够使用原生 Kubernetes 界面与 Kubernetes 进行交互，并使工作负载能够在 vSphere 和 GKE 之间轻松移动。

持久存储

VMware PKS 允许客户为无状态和有状态的应用部署 Kubernetes 集群。它通过 Project Hatchway 支持 vSphere Cloud Provider 存储插件。如此一来，VMware PKS 便可支持 vSphere 存储中的 Kubernetes 存储基元，包括卷（如持久性卷 (PV)）、持久性卷申领 (PVC)、存储类和有状态集等，还可为基于 Kubernetes 的应用引入企业级存储功能，例如由 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，VMware PKS 支持企业内多个业务线使用多个租户。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，使用共享集群的多个团队可保护其各自的 Kubernetes 命名空间。

多云服务

VMware PKS 既支持本地部署模型，也可部署在云服务提供商环境中。通过 VMware PKS，您可使用 Kubernetes 在 vSphere 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 和 Amazon Web Service (AWS) EC2）上。

集成 vRealize Log Insight 以执行日志管理和分析

VMware PKS 提供了与 VMware vRealize® Log Insight™ 的现成集成，可提供容器平台核心层的可见性，从而能够通过智能数据标记提供精确的追溯和监控功能。VMware PKS 可使用可搜索标记（如集群、pod、命名空间和容器）来聚合、标记所有日志并将其发送到 Log Insight。对于与 Log Insight 的集成，将使用 Operations Manager 集中进行管理。它允许对传输中日志数据进行 SSL 加密，以及施加日志限制以防 Log Insight 端点的数据丢失或溢出。

与 Wavefront by VMware 集成以执行 Kubernetes 分析、监控和警报功能

VMware PKS 内置与 Wavefront® by VMware® 的集成，以便实现 Kubernetes 的全面可见性。VMware PKS 与 Wavefront 的集成可提供可自定义的分析驱动型高级仪表盘和警报功能。它使 SRE、DevOps 和开发人员团队能够实时查看 Kubernetes 集群、节点、pod，乃至各个容器的运行状况、性能及资源利用率。Wavefront 还可以针对 Kubernetes KPI 发出警报，这些警报可以配置为通过电子邮件、PagerDuty 或其他 DevOps 工具发送给所选接收方。

VMware PKS 功能特性列表	
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
自动执行运行状况检查和自我修复	• 主动监控所有节点的运行状况，避免出现问题 • 通过重建出现故障/无响应的节点来确保应用服务的理想响应能力
多可用区	• 通过将集群节点跨多个可用区平均分布并支持 Kubernetes 故障域来提升集群高可用性 • 使企业能够将 Kubernetes 部署到安置区，以满足特定的数据关联性、监管和性能要求
多主控主机/etcd	• 通过将多个主控主机部署到多个可用区来应对任何可用区或主控节点发生故障的情形，从而提升 Kubernetes 管理平面的高可用性。 • 自动创建负载均衡器以便跨多个 API 服务器分布 API 请求。通过运行状况监控，API 请求将仅路由到正常运行的节点，而 BOSH 则负责修复没有响应的节点。
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，提高开发人员和运维人员的工作效率 • 优化原生容器网络连接，包括自动调配、微分段、入口控制器、负载均衡和安全策略

了解更多

要了解有关 VMware PKS 的更多信息，请访问 VMware PKS 页面，网址为：
https://cloud.vmware.com/vmware-pks

安全的容器镜像仓库	• 通过增强容器安全性最大限度地减少应用漏洞。 • 通过镜像复制、RBAC、AD/LDAP 集成、公证服务、漏洞扫描和审核，简化容器镜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 • 允许工作负载在本地 vSphere 环境和 GKE 之间移动
原生 Kubernetes 支持	• 通过为开发人员提供原生 Kubernetes CLI 和全面的 YAML 支持来提高开发人员的工作效率 • 以原生形式展现 Kubernetes，不添加专有扩展，防止局限于一家供应商
经 CNCF 认证的 Kubernetes 分发版	• 符合社区规范 • 确保不同云环境之间的可移动性、互操作性和一致性
企业身份认证	• 在 VMware PKS 控制平面级别与现有 LDAP 集成，以实现集群创建、扩展和更新 • 在下至 Kubernetes 集群级别与现有 LDAP 系统集成，以简化使用原生 Kubernetes RBAC 进行凭证管理的过程
多租户	• 为各用户提供他们自己的 Kubernetes 集群 • 在租户之间隔离工作负载并提供隐私保护
持久存储	• 为无状态和有状态的应用部署 Kubernetes 集群。 • 支持通过 Project Hatchway 成为 Kubernetes 组成部分的 vSphere Cloud Provider 存储插件。
多云服务	• 在 vSphere、GCP 和 AWS 上运行 • 通过提供一个一致的界面来部署和管理 Kubernetes，从而优化多云环境中的工作负载部署
与 Wavefront by VMware 集成	• 支持实时了解在 Kubernetes 集群中运行的容器化应用的运行状况和性能 • 允许开发人员和 DevOps 人员执行 APM（应用性能监控和管理）
与 vRealize Log Insight 集成	• 具备有行动指导意义的仪表盘、分析和范围更广的第三可方延展性，因而可提供高度可扩展的日志管理功能。 • 提供深入的运维可见性和更快速的故障排除。

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 北京市朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-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