# 使用 VMWARE ENTERPRISE PKS 在 VMWARE vSPHERE 上部署容器的主要原因

在这个广泛使用移动银行、手机购物、互联汽车和物联网的时代，您可以利用容器和 Kubernetes 的强大功能来推动快速实现数字化转型。您的自定义应用可以体现企业的创新，为客户的生活增添姿彩并扰乱竞争对手的业务。

自定义应用可以实现创收、提升品牌识别度、促进与业务的互动并创造精致的客户体验。在这一环境下，有三项技术可以推进应用发展。凭借轻型打包和移动性特征，容器可以加快软件开发。微服务可为应用提供所需的模块化体系架构，以便随时更改和按需扩展。Kubernetes 可编排容器化应用以自动执行部署和管理。

然而，Kubernetes 只是完整体系中的一层，负责将容器投入企业级生产。为满足企业级运维的需求并避免再创建另一个 IT 孤立小环境，该体系需要具备网络连接、安全性、存储、维护、可持续性、监控和可管理的基础架构。

VMware® Enterprise PKS 从根本上简化了 Kubernetes 集群的部署和运维，让您可以轻松安全地在 VMware vSphere® 上大规模运行容器。由于 VMware Enterprise PKS 与 VMware 基础架构和工具集成，您可以同时管理传统应用和现代应用。借助这一通用的集中式管理平面，您可以提前制止创建孤立小环境并简化容器化应用的管理，从而在自己的业务不受影响的情况下扰乱竞争对手的业务。

## 简易性

简易性是 VMware Enterprise PKS 的核心。VMware Enterprise PKS 的体系架构与 vSphere 紧密集成并使用 BOSH 来隐藏管理 Kubernetes 的复杂性，自然可简化 Kubernetes 集群的部署和运维。

该体系架构的两个部分赋予了 VMware Enterprise PKS 简易性：VMware Enterprise PKS 控制平面和 BOSH。控制平面提供了一个自助服务 API 接口，可用于按需部署 Kubernetes 集群并管理其生命周期。控制平面 API 将请求提交给 BOSH，BOSH 会自动创建和删除 Kubernetes 集群。

此外，VMware Enterprise PKS 的简易性与容器的固有简易性相结合，可以简化容器化应用以及运行这些应用的 Kubernetes 集群的维护和更新。

## 安全性

容器化应用需要保证全体系的安全性。云原生体系中遍布威胁和安全风险，而且容器与任何其他计算机技术一样，会遭到来自各种攻击途径的攻击。编排系统未获得充分的保护会带来额外一层风险，这种风险嵌入在快速发展的复杂技术中。

在无法将容器与现有安全系统和数据中心集成的情况下，为了满足容器化应用和编排系统的安全要求，您可能需要冒着极大的风险并付出高昂成本来构建自定义安全组件或集成。

### VMWARE ENTERPRISE PKS 概览

VMware Enterprise PKS 提供了一个高度可用的生产级 Kubernetes 平台，该平台具有来自 VMware NSX® Data Center 的高级网络连接、安全镜像仓库以及基于 BOSH 的生命周期管理功能。该解决方案从根本上简化了 Kubernetes 集群的部署和运维，以便您可以在 VMware vSphere 上大规模运行、编排、保护和维护容器。

### 主要优势

- 快速按需调配 Kubernetes 集群
- 通过滚动升级、运行状况检查和自动修复，为 Kubernetes 组件提供高可用性
- 使用包括微分段、负载均衡和安全策略在内的高级容器网络连接功能
- 通过漏洞扫描和镜像签名来保护容器镜像
- 通过监控、日志记录和分析提高运维效率

### 建立强大的安全边界

容器不是微型虚拟机，容器也不会像虚拟机那样建立安全边界。NIST 的“Application Container Security Guide”（NIST 特别出版物 800-190）的一个重要暗示就是要在虚拟机上运行容器化应用。

“尽管容器可以提供很高的隔离程度，但不会提供像虚拟机一样清晰和具体的安全边界。由于多个容器共享同一内核，并且可以在一台主机上以截然不同的功能和权限运行，所以，它们之间的隔离程度远低于 hypervisor 为虚拟机提供的隔离程度。”- 来源：NIST Application Container Security Guide。

VMware Enterprise PKS 可为虚拟机和 Kubernetes 单元提供统一的策略层，从而帮助保护整个体系内容器的安全。VMware Enterprise PKS 可扫描容器镜像以查找漏洞，并为已知镜像签名以表示它们可信任。VMware Enterprise PKS 可连接到您构建的身份验证和访问控制系统，如 Active Directory 和 LDAP。VMware Enterprise PKS 可与 Wavefront® by VMware® 等监控和日志记录工具集成。此外，通过与 NSX 结合使用，VMware Enterprise PKS 可支持应用微分段以保护容器化应用的安全。


图 1：VMware Enterprise PKS 保护整个云原生体系的容器。

## 避免 IT 孤立小环境

多个基础架构孤立小环境会导致团队、工具和流程的重复。最终，团队会无法在单个平台上专注于推动创新，而是白费力气做重复工作。

从头开始构建云原生体系可能会创建另一个 IT 孤立小环境，而且该环境成本高昂且复杂。另一个孤立小环境将偏离 IT 的使命，IT 正面临着提高敏捷性、缩短新应用和服务的销售就绪时间、快速采用新服务以及控制成本的压力，还需确保这一切不会导致复杂性和风险增加。这些是推动采用云原生技术的几个主要目标。这里有一点讽刺意味：如果实施会创建额外孤立小环境的云原生体系，可能会削弱云原生技术的重要优势。

VMware Enterprise PKS 可以基于现有 VMware 基础架构实施云原生体系。它不会创建另一个 IT 孤立小环境。反而，您可以使用大多数用于管理传统应用的 VMware 工具（如 VMware vRealize® Suite）并以大致相同的方式来管理容器化应用。

这一切都将在单个平台、单个环境中继续进行。因此，借助 VMware Enterprise PKS，您可以在整个体系（而非另一个孤立小环境）中实现一致的基础架构和运维。

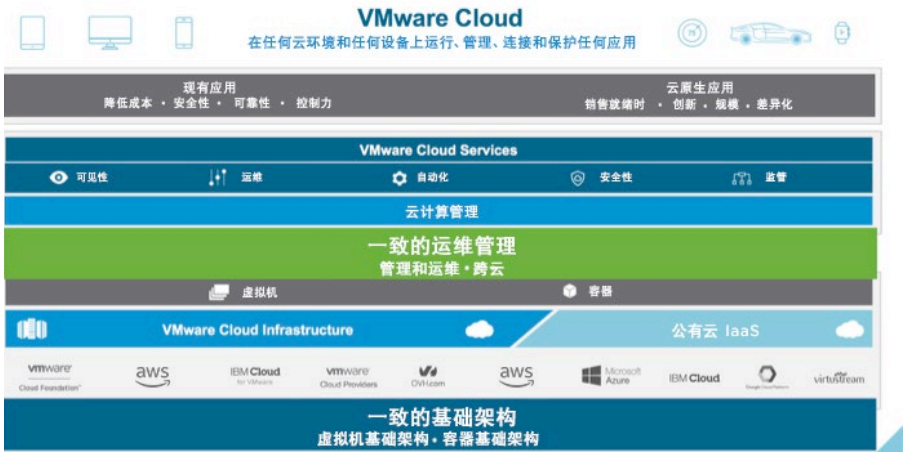


图 2：在使用 VMware Enterprise PKS 的 VMware SDDC 中的虚拟机上运行容器，可以在始终如一的基础架构上实现一致的运维管理。

## 利用对 vSphere 的现有投资

构建可扩展且灵活的基础架构以促进云原生应用的开发和部署可能是一项操作复杂、实施困难且成本高昂的任务。

经济高效地采用容器的快速途径是将现有虚拟化基础架构转变为灵活、可扩展且经过现代化改造的数据中心，从而能够部署云原生应用以及继续托管传统应用。

以下正是 VMware Enterprise PKS 大显身手之处：它可以将对 vSphere 和 VMware vCenter® 的现有投资转变为底层基础架构，并支持在该基础架构上运行容器以及使用 Kubernetes 来管理这些容器。此外，如果您使用 Active Directory 或 LDAP 进行身份验证和访问控制，则可以将 VMware Enterprise PKS 与这些系统集成，以便经济高效地提供安全保护。

VMware Enterprise PKS 可以实施这样一个体系架构，能够促进顺畅、快速且响应敏捷的开发和部署，同时保持原有系统的安全性、性能和经济效益。

## 多云移动性

容器和 Kubernetes 是有助于实现移动性的技术。容器的打包将应用从机器中分离，让开发人员能够决定部署应用的位置和方式。此外，Helm 等工具可以为预先配置、自定义、可重现且可管理的 Kubernetes 资源生成资源包。容器的移动性与 Kubernetes 的强大功能相结合，为您提供了云独立性。

为支持移动性，VMware Enterprise PKS 公开原生 Kubernetes、实施通用的运维模式、保持与 Google Kubernetes Engine 的持续兼容性并成为经认证的 Kubernetes 发行版。

VMware Enterprise PKS 以原生形式公开 Kubernetes，而不添加任何抽象层或专有扩展层，这样开发人员便可使用原生 Kubernetes CLI 和 API。

VMware Enterprise PKS 可以通过 Pivotal Operations Manager 进行部署，该管理器提供一个通用的运维模式，支持跨多个 IaaS 抽象工具（如 vSphere 和 Google Cloud Platform）实施 VMware Enterprise PKS。无论是本地部署环境还是跨多个云环境，VMware Enterprise PKS 的运维功能都可为您提供可见性、自动化和安全性，让您可以恰当运维容器化应用。

此外，VMware Enterprise PKS 还保持与 Google Kubernetes Engine (GKE) 持续兼容，确保开发人员获得最新稳定的 Kubernetes 版本、功能特性和工具。

VMware Enterprise PKS 已由 Cloud Native Computing Foundation (CNCF) 通过其 Kubernetes 软件一致性认证计划进行认证。此认证使您能够自信地运行应用，确信 Kubernetes 部署已通过 CNCF 测试套件的测试并符合社区规范。随着越来越多的企业采用 Kubernetes，像 VMware Enterprise PKS 这样经过认证的 Kubernetes 产品可确保公有云、私有云和混合云之间的可移动性和互操作性。

## 可管理性

VMware Enterprise PKS 与其他几种技术相结合，提供了一个完整的云原生体系，使您可以轻松管理容器镜像、Kubernetes 集群、容器网络连接以及底层基础架构。

Harbor 是一个开源容器镜像仓库，随 VMware Enterprise PKS 一起提供，可用于管理容器镜像。Harbor 的作用包括将容器镜像安全地存储在本地专有镜像仓库中，扫描镜像以查找漏洞，以及为镜像签名以表示它们可信任。

BOSH 与 VMware Enterprise PKS 集成，旨在简化 Kubernetes 的管理。BOSH 以一致且可重现的方式对 Kubernetes 进行打包、版本管理和部署，以节省时间并减少手动工作。当 BOSH 部署 Kubernetes 集群时，Kubernetes 控制平面的每个核心组件都会实例化为一个虚拟机实例。BOSH 可以监控 Kubernetes 控制平面的运行状况并修复故障虚拟机，无需人工干预。BOSH 还可自动执行修补、升级、停用和重新部署 Kubernetes 的流程。

VMware NSX 会在 Kubernetes 中自动实施容器网络连接。您可以使用微分段快速部署虚拟网络，而且这些网络可通过运维工具和 Traceflow 等故障排除实用程序轻松进行管理。

当 PKS 使用 vSphere 为 Kubernetes 提供底层基础架构时，您可以使用经验证的 VMware 技术（如 vCenter）来管理基础架构。对系统组件、容器和 Kubernetes 集群的监控由 vRealize Suite 和 Wavefront by VMware 来处理。

## 采用集成式存储选项以实现数据持久性

VMware Enterprise PKS 与 VMware vSAN 集成，可以将可扩展且持久的软件定义的存储延展到在 Kubernetes 上运行的容器化应用。通过将 vSphere 设置为 Kubernetes 的云服务提供平台，您可以创建持久性卷并指定存储类。通过利用 vSAN 进行持久性存储，便无需为有状态的容器化应用查找和连接存储解决方案。

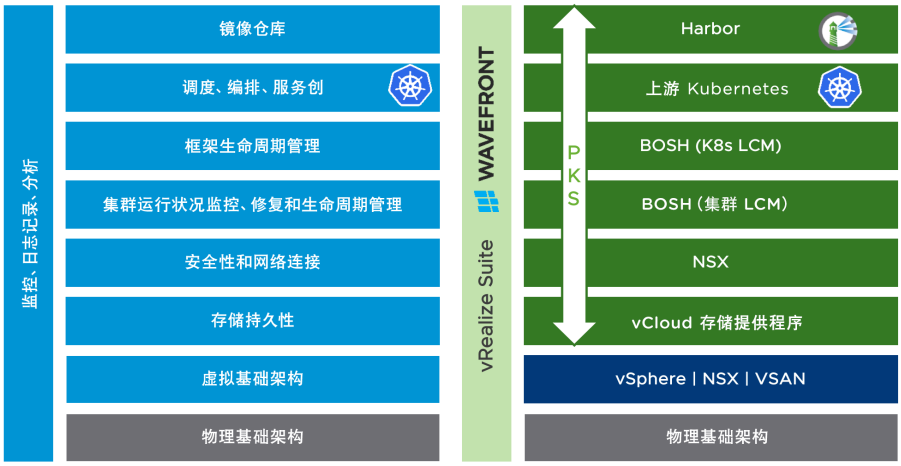


图 3：VMware Enterprise PKS 基于 VMware vSphere 交付完整的云原生体系。

## 总结

VMware Enterprise PKS 的简易性、功能、生命周期管理和自动化提供了一个安全的完整体系解决方案，从而帮助您节省时间、减少工作量和降低成本。

**详细了解**
**VMWARE ENTERPRISE PKS**
要了解 VMware 如何帮助客户运行和管理云原生应用，请访问：

cloud.vmware.com

**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