VMWARE ENTERPRISE PKS

AT A GLANCE

VMware® Enterprise PKS is a production-grade Kubernetes-based container solution equipped with advanced networking, a private container registry, and full lifecycle management. VMware Enterprise PKS radically simplifies the deployment and operation of Kubernetes clusters so you can run and manage containers at scale on private and public clouds.

KEY BENEFITS

- Eliminate lengthy deployment and management processes with on-demand provisioning, scaling, patching and updating Kubernetes clusters via simple CLI or API.
- Access the latest stable Kubernetes release from the open source community
- Provide critical enterprise features for running production workloads such as high availability, rolling upgrades, health-checks and auto-healing of the underlying virtual infrastructure
- Simplify container networking and increase security with VMware NSX-T™.
- Deploy Kubernetes both on prem on vSphere and in public clouds
- Deploy Kubernetes clusters for both stateless and stateful applications
- Secure application deployments with an integrated enterprise container registry with vulnerability scanning, image signing and auditing.
- Improve operational efficiency with monitoring, logging, and analytics through out-of-box integration with Wavefront by VMware and vRealize Log Insight.

What is VMware Enterprise PKS?

VMware Enterprise PKS is a purpose-built container solution to operationalize Kubernetes for multi-cloud enterprises and service providers. It significantly simplifies the deployment and management of Kubernetes clusters with day 1 and day 2 operations support. With hardened production-grade capabilities, VMware Enterprise PKS takes care of your container deployments from the application layer all the way to the infrastructure layer.

VMware Enterprise PKS is built-in with critical production capabilities such as high availability, auto-scaling, health-checks, as well as self-healing and rolling upgrades for Kubernetes clusters. It provides the latest stable Kubernetes release so developers have the latest features and tools available to them. It also integrates with VMware NSX-T for advanced container networking including micro-segmentation, ingress controller, load balancing and security policy. Through an integrated private registry, VMware Enterprise PKS secures container image via features such as vulnerability scanning, image signing and auditing.

VMware Enterprise PKS exposes Kubernetes in its native form without adding any layers of abstraction or proprietary extensions, which lets developers use the native Kubernetes CLI that they are most familiar with. VMware Enterprise PKS can be easily deployed and operationalized via Pivotal Operations Manager, which allows a common operating model to deploy VMware Enterprise PKS across multiple IaaS abstractions like VMware vSphere®, Google Cloud Platform (GCP), Amazon Web Services (AWS) EC2, and Azure.

VMware Enterprise PKS Architecture

VMware Enterprise PKS builds on Kubernetes, BOSH, VMware NSX-T, and Project Harbor to form a production-grade, highly-available container runtime that operates on vSphere and public clouds. With built-in intelligence and integration, VMware Enterprise PKS ties all these open source and commercial modules together, delivering a simple-to-use product for customers, ensuring the customers have the most efficient Kubernetes deployment and management experience possible.

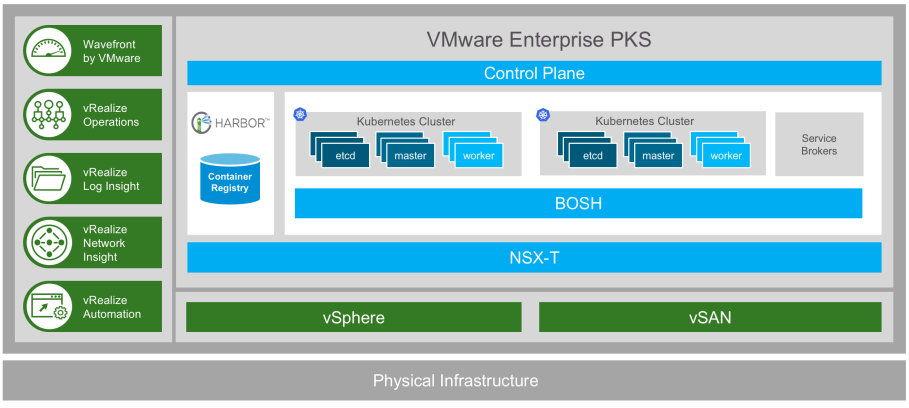

Figure 1. VMware Enterprise PKS works with the VMware SDDC to provide a comprehensive solution.

KUBERNETES CERTIFICATION

Certified by the Cloud Native Computing Foundation® (CNCF®) in its Kubernetes Software Conformance Certification program, VMware Enterprise PKS lets customers run applications with the confidence that their deployment has passed test suites and is compliant with the community's specification. As more organizations adopt Kubernetes, a certified Kubernetes product like VMware Enterprise PKS ensures portability, interoperability, and consistency between different environments.

Kubernetes

Kubernetes is an open source container orchestration framework. Kubernetes orchestrates containers to manage and automate resource utilization, failure handling, availability, configuration, scalability, and desired state of the application. As an application and its services run in containers on a distributed cluster of virtual machines, Kubernetes choreographs all the moving pieces so they operate in a synchronized way to optimize the use of computing resources and to maintain an application's desired state.

BOSH

BOSH is an open source tool for release engineering that simplifies the deployment and lifecycle management of large distributed systems. It allows developers to easily version, package, and deploy software in a consistent and reproducible manner. BOSH can support deployments across different IaaS, such as VMware vSphere, Amazon Web Services EC2 (AWS EC2), Microsoft Azure, Google Compute Platform (GCP), and OpenStack, and it has been used to successfully deploy and manage Cloud Foundry platform since its inception.

VMware NSX-T

VMware NSX-T provides advanced container networking and security features for Kubernetes clusters such as micro-segmentation, ingress controller, load balancing and security policy. It provides the complete set of Layer 2 through Layer 7 networking services that is needed for pod-level networking. With NSX-T integration in VMware Enterprise PKS, enterprises can quickly deploy networks with micro-segmentation and on-demand network virtualization for containers and pods.

Project Harbor

Harbor is a trusted cloud native registry that stores, signs, and scans content, with the mission of providing cloud native environments the ability to confidently manage and serve container images. In addition to providing RBAC (Role-Based Access Control), LDAP(Lightweight Directory Access Protocol)/AD (Active Directory) support, Harbor enables enterprises with container image vulnerability scanning, policy-based image replication, as well as notary and auditing services.

VMware Enterprise PKS Control Plane

A key component of VMware Enterprise PKS, the control plane is the self-service interface responsible for the on-demand deployment and lifecycle management of Kubernetes clusters. It provides an API interface that enables self-service consumption of Kubernetes clusters. The API submits requests to BOSH which automates the creation, update, and deletion of Kubernetes clusters based on user requests.

Key Capabilities of VMware Enterprise PKS

Full lifecycle Management and Automation

VMware Enterprise PKS provides lifecycle management and automation for Kubernetes, making deployments, scaling, patching, and updating quick and easy. It provides a simple action-based command line interface and a public facing API that supports multiple use cases through the lifecycle of Kubernetes. With VMware Enterprise PKS, IT admins can deploy multiple Kubernetes clusters in minutes. Scaling Kubernetes clusters can also be done easily via the simple CLI or API calls. Patching and updating one or more Kubernetes clusters are also made easier by VMware Enterprise PKS through the same mechanism, making sure your clusters always keep pace with the latest security and maintenance updates. If the clusters are no longer required, the user can quickly delete them.

High Availability

VMware Enterprise PKS provides critical production-grade capabilities to ensure maximum uptime for workloads running in your Kubernetes clusters. With multi-AZ and multi-master/etcd support, it significantly improves high availability of your Kubernetes clusters running critical workloads in production.

In addition, VMware Enterprise PKS continuously monitors the health of all underlying VM instances, and recreates VMs when there are failed or unresponsive nodes. It also manages the rolling upgrade process for a fleet of Kubernetes clusters, allowing clusters to be upgraded with no downtime for application workloads.

Advanced Container Networking and Security

NSX-T equips VMware Enterprise PKS with an automated, software-defined network for container interfaces and Kubernetes nodes and pods. With NSX-T, all the networking components such as load balancers, edge routers, firewalls both on the edge nodes and between workloads deployed across multiple clusters are automatically deployed. You get logical segmentation between the clusters and individual namespaces for better network security and isolation.

Each networking service supported by NSX-T is deployed in a highly available, fully redundant mode, if one of these services fail, NSX-T automatically switches over to another logical instance of the same component.

VMware Enterprise PKS also supports Kubernetes deployment with multiple edge routers selectable on a per cluster basis, which provides complete isolation and autonomy for tenants. With network profile, VMware Enterprise PKS allows advanced network configurability. For example, Kubernetes clusters can be deployed with either small, medium or large load balancers optimized for scale and throughput requests . And Kubernetes Nodes and Pods can be deployed in either NAT or No-NAT mode, allowing customers to choose between saving precious IP address space using the NAT'ed mode, or improving traceability and visibility of the workload traffic using the No-NAT mode.

With VMware Enterprise PKS, any of the wide range of policies in NSX can be applied to container networking. Operational tools and troubleshooting utilities such as Traceflow, port mirroring and port connection tool can also be used to fulfill the production networking requirements for containerized applications.

Secure Container Registry

VMware Enterprise PKS provides an enterprise-grade container registry with secure, advanced services. VMware Enterprise PKS container registry includes user management and access control with RBAC and AD/LDAP integration, which ensures proper level of authority and access for container images. It also offers security features such as image notary service to enable content trust by letting publishers sign the image during pushing and prevent the un-signed image from being pulled. With VMware Enterprise PKS' private registry, users can also scan container images for vulnerabilities to mitigate the risk of security breaches related to contaminated container images.

Latest Stable Upstream Kubernetes

VMware Enterprise PKS is developed using mainline Kubernetes and delivers the latest stable Kubernetes release to your developers so they can use the latest features and patches from the community. In addition, without adding any proprietary abstraction layer on top of Kubernetes, VMware Enterprise PKS exposes Kubernetes in its native form, letting developers or your development tools interact with Kubernetes using the native Kubernetes interface, and also making workloads readily portable between different clouds.

Persistent Storage

VMware Enterprise PKS allows customers to deploy Kubernetes clusters for both stateless and stateful applications. It supports the vSphere Cloud Provider storage plugin through Project Hatchway. This allows VMware Enterprise PKS to support Kubernetes storage primitives for volumes such as, Persistent Volumes (PV), Persistent Volume Claims (PVC), Storage Classes and Stateful Sets on vSphere storage, and also brings in enterprise-grade storage features like Storage Policy Based Management(SPBM) with VMware vSAN™ to Kubernetes-based applications.

Multi-Tenancy

To isolate workloads and ensure privacy, VMware Enterprise PKS supports multi-tenancy for multiple lines of business within an enterprise. Different users from different lines of business are able to use their own Kubernetes clusters. Additionally, with NSX-T micro-segmentation, Kubernetes namespaces can be secured for multiple teams using a shared cluster.

Multi-Cloud

VMware Enterprise PKS is supported in an on prem deployment model as well as being deployed on cloud providers. With VMware Enterprise PKS, you can deploy containerized application with Kubernetes on-premises on vSphere, or on public clouds such as Google Cloud Platform, Amazon EC2, and Microsoft Azure.

vRealize Log Insight Integration for Log Management and Analytics

VMware Enterprise PKS comes with out-of-box integration with VMware vRealize® Log Insight™ to provide visibility into the core layers of the container platform, allowing pinpoint traceability and monitoring by intelligent data tagging. VMware Enterprise PKS aggregates, tags, and ships all logs to Log Insight with searchable tags such as cluster, pod, namespace and container. Log Insight integration is centrally managed with Operations Manager. It allows SSL encryption of log data in transit, as well as log limiting/throttling to prevent overflow or loss of data to the Log Insight endpoint.

Wavefront by VMware Integration for Kubernetes Analytics, Monitoring and Alerting

VMware Enterprise PKS delivers built-in integration with Wavefront® by VMware® for complete visibility into Kubernetes. The VMware Enterprise PKS Wavefront integration offers sophisticated, customizable analytics-driven dashboards and alerts. It gives SREs, DevOps, and developer teams real-time visibility into the health and performance of Kubernetes clusters, nodes and pods down to individual containers and their resource utilization.Wavefront can also alerts on Kubernetes KPIs, which are configurable to send to chosen alert targets whether by email, PagerDuty or other DevOps tools.

VMware ENTERPRISE PKS FEATURE LIST	
Key FEATURES	**BENEFITS**
On-demand provisioning	• Accelerates the deployment of Kubernetes clusters • Eliminates manual steps for deploying Kubernetes clusters • Minimizes mistakes and shortens time-to-value
On-demand scaling	• Scales up and down the cluster capacity easily • Eliminates manual steps and mistakes • Optimizes resource utilization
On-demand patching	• Centralizes and speeds up patching and updating of multiple Kubernetes clusters • Keeps Kubernetes clusters up-to-date and secure
Rolling upgrades	• Minimizes workload downtime by rolling upgrading a fleet of Kubernetes clusters
Automatic health check and self-healing	• Prevents issues with proactive monitoring of the health of all nodes. • Ensures desired responsiveness of the application services by recreating failed/unresponsive nodes
Multi-AZ	• Improves high availability of the clusters by evenly spreading the cluster nodes across multiple AZs and support Kubernetes failure-domains • All NSX-T networking services are deployed in a fully redundant mode • Enables enterprises to target Kubernetes deployments into a placement zone to meet particular data affinity, governance and performance requirements
Multi-Master/etcd	• Improves the high availability of the Kubernetes management plane by deploying multiple masters into multiple AZs to address any AZ outage or master nodes outage. • Automatically creates load balancers to distribute API requests across multiple API servers. With health check monitoring, API requests get routed to only the healthy nodes, while BOSH takes care of resurrection of the unresponsive nodes.
Advanced container networking and security	• Increases developer and ops productivity by simplifying networking management and enhancing security • Optimizes native container networking including automatic provisioning, micro-segmentation, ingress controller, load balancing and security policies • Achieves better tenant isolation by supporting multiple Tier 0 routers

LEARN MORE

To find out more about VMware Enterprise PKS, visit VMware PKS page at https://cloud.vmware.com/vmware-enterprise-pks

Secure container registry	• Minimizes application breaches with enhanced container security • Simplifies container image management and enhances security through image replication, RBAC, AD/LDAP integration, notary services, vulnerability scanning, and auditing.
Latest Stable Kubernetes Release	• Enhances developer productivity by letting developers access the most up-to-date Kubernetes features and tools • Allows workloads to be portable between environments
Native Kubernetes Support	• Increases developer productivity by offering them the native Kubernetes CLI and full YAML support • Exposes Kubernetes in its native form with no proprietary extensions to prevent vendor lock-in
CNCF Certified Kubernetes Distro	• Complies with the community's specification • Ensures portability, interoperability and consistency between different environments cross-clouds
Enterprise Authorization	• Integrates with existing LDAP at VMware Enterprise PKS control plane level in terms of cluster creation, scale and update. • Integrates with existing LDAP system down to the Kubernetes cluster level to simplify credential management with native Kubernetes RBAC
Multi-tenancy	• Provides individual users with their own Kubernetes clusters • Secures workloads between tenants • Provides complete network traffic isolation and autonomy for tenants to bring their own IP address ranges
Persistent Storage	• Deploys Kubernetes clusters for both stateless and stateful applications. • Supports vSphere Cloud Provider storage plugin which is part of Kubernetes through Project Hatchway.
Multi-cloud	• Runs on vSphere, GCP, Amazon EC2 and Azure. • Optimizes workload deployment in multi-cloud environments by providing a single consistent interface to deploy and manage Kubernetes
Integration with Wavefront by VMware	• Offers real-time visibility into the operations and performance of containerized applications running in the Kubernetes clusters • Allows developers and devops to do APM (Application Performance Monitoring & Management)
Integration with vRealize Log Insight	• Delivers highly scalable log management with actionable dashboards, analytics, and broad third-party extensibility. • Enables deep operational visibility and faster troubleshooting

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.