VMWARE PIVOTAL CONTAINER SERVICE

AUF EINEN BLICK

VMware® Pivotal Container Service (PKS) ist eine produktionsoptimierte Container-Lösung auf Basis von Kubernetes, die neben erweiterten Netzwerkfunktionen und einer privaten Container-Registry auch umfassendes Lebenszyklusmanagement bietet. PKS vereinfacht die Bereitstellung und den Betrieb von Kubernetes-Clustern radikal, sodass Sie Container skalierbar in Private und Public Clouds ausführen und verwalten können.

DIE WICHTIGSTEN VORTEILE

- Kein zeitaufwändiger Bereitstellungs- und Managementprozess mehr: Eine einfache CLI oder API ermöglicht das bedarfsorientierte Bereitstellen, Skalieren, Patchen und Aktualisieren von Kubernetes-Clustern.
- Zugriff auf das neueste stabile Kubernetes-Release und dauerhafte Kompatibilität mit Google Kubernetes Engine (GKE)
- Hochverfügbarkeit für Kubernetes-Komponenten (Master, Worker, etcd-Knoten) durch unterbrechungsfreie Upgrades, Systemdiagnosen und Selbstreparatur der zugrunde liegenden virtuellen Infrastruktur
- Unkomplizierte Container-Netzwerke und höhere Sicherheit mit VMware NSX®: Sie erhalten Hochverfügbarkeit, automatisiertes Provisioning, Mikrosegmentierung, Ingress-Controller, Lastausgleich und Sicherheitsrichtlinien.
- Bereitstellung von Kubernetes-Clustern für zustandsfreie und zustandsgebundene Anwendungen
- Sichere Anwendungsbereitstellungen mit einer integrierten Container-Registry für Unternehmen, die Schwachstellenprüfung, Image Signing und Auditprozesse umfasst

Was ist Pivotal Container Service (PKS)?

PKS ist eine speziell entwickelte Container-Lösung zum Operationalisieren von Kubernetes für Multi-Cloud-Unternehmen und Serviceanbieter. Der Service unterstützt Tag-1- und Tag-2-Abläufe und vereinfacht das Bereitstellen und Verwalten von Kubernetes-Clustern in erheblichem Umfang. Mit stabilen Funktionen für die Produktionsumgebung verwaltet PKS die gesamte Container-Bereitstellung vom Anwendungs-Layer bis zum Infrastruktur-Layer.

PKS integriert entscheidende Produktionsfunktionen wie Hochverfügbarkeit, automatische Skalierung, Systemdiagnosen und Selbstreparatur der zugrunde liegenden VMs sowie unterbrechungsfreie Upgrades der Kubernetes-Cluster. PKS ist dauerhaft mit GKE kompatibel und stellt das neueste stabile Kubernetes-Release bereit, sodass Entwickler stets die neuesten Funktionen und Tools zur Hand haben. Zudem bietet die Integration in VMware NSX-T erweiterte Netzwerkfunktionen für Container, darunter Mikrosegmentierung, Ingress-Controller, Lastausgleich und Sicherheitsrichtlinien. Mithilfe einer integrierten privaten Registry wird das Container-Image in PKS durch Schwachstellenprüfung, Image Signing und Auditprozesse abgesichert.

PKS präsentiert Kubernetes in seiner ursprünglichen Form ohne zusätzliche Abstrahierungsebenen oder proprietäre Erweiterungen. So können Entwickler die native CLI von Kubernetes verwenden, mit der sie bereits umfassend vertraut sind. PKS lässt sich mit Pivotal Operations Manager einfach bereitstellen und operationalisieren. Anhand eines gemeinsamen Betriebsmodells kann PKS zudem über mehrere IaaS-Abstrahierungen wie vSphere und Google Cloud Platform hinweg bereitgestellt werden.

Architektur von Pivotal Container Service

PKS bildet auf Basis von Kubernetes, BOSH, VMware NSX-T und Project Harbor einen produktionsoptimierten und hochverfügbaren Container-Service für VMware vSphere® und Public Clouds. Durch intelligente Funktionen und Integration verknüpft PKS sämtliche Open Source- und kommerziellen Module. So entsteht ein unkompliziertes Produkt, mit dessen Hilfe Kunden Kubernetes mit maximaler Effizienz bereitstellen und verwalten können.

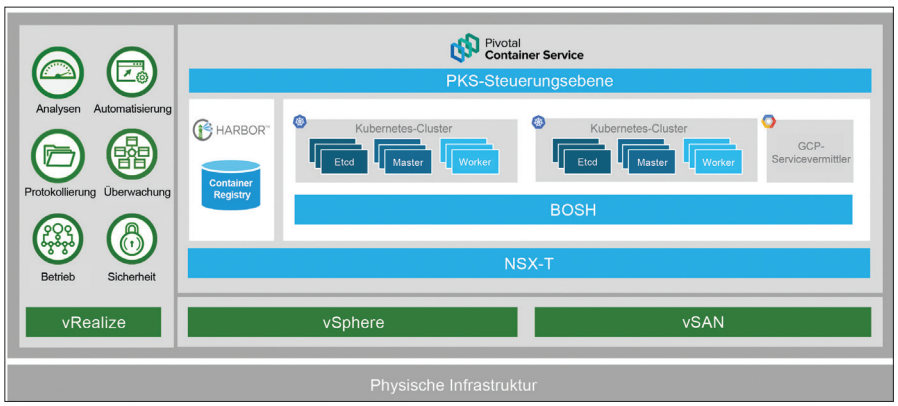

Abbildung 1: VMware Pivotal Container Service und VMware SDDC bilden zusammen eine umfassende Lösung

KUBERNETES-ZERTIFIZIERUNG

PKS wurde durch die Cloud Native Computing Foundation® (CNCF) im Rahmen des Kubernetes Software Conformance Certification-Programms zertifiziert. Deshalb können Kunden beim Ausführen von Anwendungen sicher sein, dass ihre Bereitstellung die CNCF-Tests bestanden hat und mit den Spezifikationen der Community kompatibel ist. Angesichts der zunehmenden Nutzung von Kubernetes in immer mehr Unternehmen sorgt ein zertifiziertes Kubernetes-Produkt wie PKS für Portabilität, Interoperabilität und Konsistenz zwischen verschiedenen Umgebungen.

Kubernetes

Kubernetes ist ein Open Source-Framework zur Orchestrierung von Containern. Mit Containern werden Anwendungen und ihre Abhängigkeiten in ein verteilbares Artefakt (Container-Image) paketiert, sodass sie über mehrere Umgebungen hinweg portierbar sind. Software kann so effizienter entwickelt und bereitstellt werden. Kubernetes orchestriert diese Container und ermöglicht das Verwalten und Automatisieren von Ressourcenauslastung, Fehlerbehebung, Verfügbarkeit, Konfiguration, Skalierbarkeit und dem gewünschten Zustand der Anwendung. Wenn eine Anwendung und ihre Services in Containern auf einem verteilten Cluster virtueller Maschinen ausgeführt werden, orchestriert Kubernetes alle beweglichen Elemente, sodass sie synchron arbeiten. Die Computing-Ressourcen werden auf diese Weise optimal genutzt und der gewünschte Zustand der Anwendung aufrechterhalten.

BOSH

BOSH ist ein Open Source-Tool für die Release-Entwicklung, das die Bereitstellung und das Lebenszyklusmanagement von umfangreichen verteilten Systemen vereinfacht. Mit BOSH können Entwickler Software ohne viel Aufwand einheitlich und reproduzierbar versionieren, paketieren und bereitstellen. BOSH unterstützt Bereitstellungen vieler verschiedener IaaS-Anbieter, darunter VMware vSphere, Microsoft Azure, OpenStack, Google Compute Platform (GCP) und Amazon Web Services EC2 (AWS EC2). Zudem wird es seit der Ersteinführung zum Bereitstellen und Verwalten der Cloud Foundry-Plattform verwendet.

VMware NSX-T

VMware NSX-T stellt erweiterte Netzwerk- und Sicherheitsfunktionen für Container in Kubernetes-Clustern zur Verfügung, darunter Mikrosegmentierung, Ingress-Controller, Lastausgleich und Sicherheitsrichtlinien. Hinzu kommen sämtliche Layer-2- bis Layer-7-Netzwerkservices, die für Pod-Level-Netzwerke benötigt werden. Mit der Integration von NSX-T in PKS können Unternehmen schnell Netzwerke mit Mikrosegmentierung und bedarfsorientierter Netzwerkvirtualisierung für Container und Pods bereitstellen.

Project Harbor

Harbor ist ein Open Source-Registry-Server der Enterprise-Klasse, der Docker-Images in einer privaten Registry hinter der Firewall speichert und verteilt. Er bietet eine rollenbasierte Zugriffssteuerung und unterstützt LDAP (Lightweight Directory Access Protocol)/AD (Active Directory). Darüber hinaus erhalten Unternehmen mit Harbor eine Schwachstellenprüfung für Container-Images, eine richtlinienbasierte Image-Replikation sowie Notary- und Auditing-Services.

PKS-Steuerungsebene

Die Steuerungsebene ist eine zentrale Komponente von PKS. Diese Self-Service-Oberfläche dient der bedarfsorientierten Bereitstellung und dem Lebenszyklusmanagement von Kubernetes-Clustern. Über ihre API-Schnittstelle können Kubernetes-Cluster als Self-Service genutzt werden. Die API sendet Anfragen an BOSH. Damit werden Erstellung, Aktualisierung und Löschung von Kubernetes-Clustern den Anfragen der Anwender entsprechend automatisiert.

Hauptfunktionen von Pivotal Container Service

Lebenszyklusmanagement und Automatisierung von A bis Z

PKS bietet Lebenszyklusmanagement und Automatisierung für Kubernetes. Bereitstellung, Skalierung, Patching und Aktualisierung werden so zum Kinderspiel. PKS verfügt über eine einfache aktionsbasierte Befehlszeilenschnittstelle (CLI) und eine öffentliche API, die viele Anwendungsbereiche während des Lebenszyklus von Kubernetes unterstützt. Mit PKS benötigen IT-Administratoren zur Bereitstellung mehrerer Kubernetes-Cluster nur wenige Minuten. Außerdem lassen sich Kubernetes-Cluster mit einfachen CLI- oder API-Aufrufen skalieren. Patching und Aktualisierung von einem oder mehreren Kubernetes-Clustern gestalten sich mit PKS einfacher, da beides auf dem gleichen Mechanismus basiert. Die Sicherheits- und Wartungs-Updates der Cluster sind daher immer auf dem neuesten Stand. Werden die Cluster nicht mehr benötigt, können sie kurzerhand gelöscht werden.

Hochverfügbarkeit

PKS stellt mit entscheidenden Produktionsfunktionen eine maximale Betriebszeit für Workloads auf Kubernetes-Clustern sicher. Der Service überwacht laufend den Zustand aller zugrunde liegenden VM-Instanzen und erstellt VMs neu, falls Knoten ausgefallen sind oder nicht reagieren. Zudem steuert er den unterbrechungsfreien Upgrade-Prozess für eine Reihe von Kubernetes-Clustern, damit diese ohne Ausfallzeit der Anwendungs-Workloads aktualisiert werden können.

Erweiterte Netzwerk- und Sicherheitsfunktionen für Container

NSX-T stellt automatisiertes Software-Defined Networking für Container-Schnittstellen und Kubernetes-Pods in PKS bereit. Die NSX-T-Services für den Lastausgleich befinden sich in einem hochverfügbaren, vollständig redundanten NSX Edge™-Cluster. Fällt ein Load Balancer aus, wechselt der Datenverkehr automatisch zu einem anderen Load Balancer. Diese Lastausgleichsservices sind vollständig in Kubernetes Ingress- und LoadBalancer-Konstrukte integriert. NSX erfüllt die Isolationsanforderungen von Workloads durch Mikrosegmentierung. Die einzelnen Kubernetes-Namespaces können isoliert werden und der Datenverkehr zwischen und innerhalb von Kubernetes-Namespaces lässt sich mithilfe von Netzwerkrichtlinien steuern.

Mit PKS kann jede der zahlreichen Richtlinien in NSX auf Container-Netzwerke anwenden. Betriebstools und Fehlerbehebungsprogramme wie Traceflow sowie Tools zur Port-Spiegelung und Port-Verbindung können eingesetzt werden, um die Produktionsanforderungen für Netzwerke mit Container-Anwendungen zu erfüllen.

Sichere Container-Registry

PKS bietet eine Container-Registry der Enterprise-Klasse mit sicheren, erweiterten Services. Die Container-Registry von PKS beinhaltet Anwendermanagement und Zugriffskontrolle mit RBAC und AD/LDAP-Integration, wodurch sachgerechte Zugriffsberechtigungen für Container-Images sichergestellt werden. Sicherheitsfunktionen wie der Notary-Service für Images gewährleisten die Vertrauenswürdigkeit von Inhalten. Publisher können Images während des Push-Vorgangs signieren und damit verhindern, dass unsignierte Images abgerufen werden. Anwender können Container-Images mit der privaten Registry von PKS auf Schwachstellen überprüfen und das Risiko von Sicherheitsverletzungen durch kontaminierte Container-Images minimieren.

Dauerhafte Kompatibilität mit Google Kubernetes Engine (GKE)

PKS wurde mithilfe von Mainline Kubernetes entwickelt und stellt das neueste stabile Kubernetes-Release für Entwickler bereit. PKS sorgt für kontinuierliche Kompatibilität mit Kubernetes-Versionen, die von GKE unterstützt werden. So haben Entwickler im Unternehmen stets die neuesten Funktionen und Patches für vSphere und GKE zur Hand. Darüber hinaus präsentiert PKS Kubernetes in seiner ursprünglichen Form ohne zusätzliche, proprietäre Abstrahierungsebenen. Entwickler oder Entwicklungs-Tools können über die native Kubernetes-Schnittstelle mit Kubernetes interagieren und Workloads lassen sich schnell zwischen vSphere- und GKE-Umgebungen portieren.

Persistenter Storage

Mit PKS können Kunden Kubernetes-Cluster für zustandsfreie und zustandsgebundene Anwendungen bereitstellen. PKS unterstützt das Storage-Plug-in vSphere Cloud Provider, das über Project Hatchway zu Kubernetes gehört. Damit kann PKS Storage-Primitive von Kubernetes unterstützen. Dazu gehören Volumes, persistente Volumes (PV), Persistent Volumes Claims (PVC), Storage-Klassen und Stateful Sets für vSphere-Storage. Kubernetes-basierte Anwendungen erhalten zudem Storage-Funktionen der Enterprise-Klasse wie Storage Policy Based Management (SPBM) mit VMware vSAN™.

Mandantenfähigkeit

Zur Isolation von Workloads und Wahrung des Datenschutzes unterstützt PKS Mandantenfähigkeit für viele Geschäftsbereiche im Unternehmen. Anwender unterschiedlicher Geschäftsbereiche können jeweils ihre eigenen Kubernetes-Cluster verwenden. Außerdem lassen sich Kubernetes-Namespaces mithilfe der NSX-T-Mikrosegmentierung über einen gemeinsam genutzten Cluster für mehrere Teams sichern.

Multi-Cloud

PKS unterstützt Multi-Cloud-Bereitstellung über BOSH. PKS bietet die Möglichkeit, containerbasierte Anwendungen mit Kubernetes intern über vSphere oder in Public Clouds wie Google Cloud Platform bereitzustellen.

FUNKTIONEN VON PKS	
Funktion	**Vorteile**
Bedarfsorientiertes Provisioning	• Schnellere Bereitstellung von Kubernetes-Clustern • Manuelle Schritte der Bereitstellung von Kubernetes-Clustern entfallen • Minimale Fehler und schnellere Wertschöpfung
Bedarfsorientierte Skalierung	• Einfaches Skalieren der Cluster-Kapazität • Manuelle Schritte und Fehler entfallen • Optimierte Ressourcenauslastung
Bedarfsorientiertes Patching	• Zentralisiertes und schnelleres Patching und Aktualisieren von mehreren Kubernetes-Clustern • Kubernetes-Cluster sind stets sicher und auf dem neuesten Stand
Unterbrechungsfreie Upgrades	• Minimale Ausfallzeiten für Workloads durch das unterbrechungsfreie Upgrade einer Reihe von Kubernetes-Clustern
Automatische Systemdiagnose und Selbstreparatur	• Eine proaktive Zustandsüberwachung aller Knoten verhindert Probleme • Garantiert die gewünschte Reaktionsfähigkeit von Anwendungsservices durch Wiederherstellung ausgefallener/nicht reagierender Knoten
Erweiterte Netzwerk- und Sicherheitsfunktionen für Container	• Höhere Produktivität von Entwicklern und Abläufen durch vereinfachtes Netzwerkmanagement und höhere Sicherheit • Optimierte native Netzwerkfunktionen für Container wie etwa automatisches Provisioning, Mikrosegmentierung, Ingress-Controller, Lastausgleich und Sicherheitsrichtlinien
Sichere Container-Registry	• Minimale Sicherheitsverletzungen durch Anwendungen dank höherer Container-Sicherheit • Einfacheres Management der Container-Images und höhere Sicherheit durch Image-Replikation, RBAC, AD/LDAP-Integration, Notary-Services, Schwachstellenprüfung und Auditprozesse
Dauerhafte Kompatibilität mit GKE	• Höhere Produktivität von Entwicklern durch Zugriff auf die aktuellsten Kubernetes-Funktionen und -Tools • Workloads sind zwischen der internen vSphere-Umgebung und GKE portierbar
Native Kubernetes-Unterstützung	• Präsentation von Kubernetes in seiner ursprünglichen Form ohne proprietäre Erweiterungen und Anbieterbindung • Höhere Produktivität von Entwicklern durch Zugriff auf native Kubernetes-CLI und uneingeschränkte YMAL-Unterstützung

WEITERE INFORMATIONEN

Weitere Informationen zu Pivotal Container Service finden Sie auf der PKS-Seite unter https://cloud.vmware.com/pivotal-container-service.

FUNKTIONEN VON PKS	
Funktion	Vorteile
CNCF-zertifizierte Kubernetes-Distribution	• Kompatibel mit den Spezifikationen der Community • Cloudübergreifende Portabilität, Interoperabilität und Konsistenz zwischen verschiedenen Umgebungen
Mandantenfähigkeit	• Einzelne Anwender erhalten eigene Kubernetes-Cluster • Sichere Workloads zwischen Mandanten sowie Datenschutz
Persistenter Storage	• Bereitstellung von Kubernetes-Clustern für zustandsfreie und zustandsgebundene Anwendungen • Unterstützung des Storage-Plug-ins vSphere Cloud Provider über Project Hatchway
Multi-Cloud	• Optimierte Workload-Bereitstellung in Multi-Cloud-Umgebungen dank einer einheitlichen Oberfläche für die Bereitstellung und das Management von Kubernetes auf vSphere und Google Cloud Platform

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Freisinger Str. 3 85716 Unterschleißheim/Lohhof Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de