VMware Pivotal Container Service

요약 정보

VMware® Pivotal Container Service(PKS)는 고급 네트워킹, 프라이빗 컨테이너 레지스트리 및 전체 수명주기 관리 기능이 탑재된 운영 환경 수준의 Kubernetes 기반 컨테이너 솔루션입니다. PKS는 Kubernetes 클러스터의 구축 및 운영을 대폭 간소화하여 프라이빗 및 퍼블릭 클라우드에서 컨테이너를 규모에 맞게 실행 및 관리할 수 있게 해 줍니다.

주요 이점

- 간단한 CLI 또는 API를 통해 Kubernetes 클러스터를 온디맨드로 프로비저닝, 확장, 패치 적용, 업데이트하여 시간이 오래 걸리는 구축 및 관리 프로세스를 제거합니다.
- 안정적인 최신 Kubernetes 릴리스에 액세스하고 Google Kubernetes Engine(GKE)과의 지속적인 호환성을 확보합니다.
- 기반 가상 인프라의 연속적인 업그레이드, 상태 점검, 자동 복구를 통해 Kubernetes 구성 요소(마스터, 작업자, etcd 노드)에 고가용성을 제공합니다.
- VMware NSX®를 통해 고가용성, 자동화된 프로비저닝, 마이크로 세분화, 수신 컨트롤러, 로드 밸런싱, 보안 정책을 제공하여 컨테이너 네트워킹을 간소화하고 보안을 강화합니다.
- 애플리케이션의 상태 저장 여부에 관계없이 Kubernetes 클러스터를 구축합니다.
- 통합 엔터프라이즈 컨테이너 레지스트리의 취약점 검사, 이미지 서명, 감사 기능을 사용하여 애플리케이션 배포를 보호합니다.

Pivotal Container Service(PKS) 소개

PKS는 멀티 클라우드 기업 및 서비스 공급업체에 Kubernetes 운영 환경을 제공하는 맞춤형 컨테이너 솔루션으로, 1일 차 및 2일 차 운영 지원을 통해 Kubernetes 클러스터 구축 및 관리를 획기적으로 간소화합니다. 강화된 운영 환경 수준의 기능을 통해 PKS는 애플리케이션 계층에서 인프라 계층까지 컨테이너 배포를 완벽하게 처리합니다.

PKS에는 기반 가상 머신의 고가용성, 자동 확장, 상태 점검, 자가 복구 및 Kubernetes 클러스터의 연속적인 업그레이드 등 운영 환경을 위한 필수 기능이 내장되어 있습니다. GKE에 대한 지속적인 호환성을 통해 PKS는 안정적인 최신 Kubernetes 릴리스를 제공하여 개발자가 최신 기능 및 툴을 사용할 수 있도록 하고 또한 VMware NSX T와 통합되어 마이크로 세분화, 수신 컨트롤러, 로드 밸런싱, 보안 정책을 포함한 고급 컨테이너 네트워킹을 제공합니다. 통합 프라이빗 레지스트리를 통해 PKS는 취약점 검사, 이미지 서명, 감사 기능을 사용하여 컨테이너 이미지를 보호합니다.

PKS는 추상화 계층 또는 독자적인 확장을 추가하지 않고 Kubernetes를 기본 형식으로 노출시켜 개발자가 가장 익숙한 기본 Kubernetes CLI를 사용할 수 있도록 합니다. PKS는 vSphere 및 Google Cloud Platform 등의 여러 IaaS 추상화에 걸쳐 PKS를 구축하기 위한 공통 운영 모델을 제공하는 Pivotal Operations Manager를 통해 간단하게 구축 및 운영할 수 있습니다.

Pivotal Container Service 아키텍처

PKS는 Kubernetes, BOSH, VMware NSX-T, Project Harbor 기반으로 구축되어 VMware vSphere® 및 퍼블릭 클라우드에서 실행되는 운영 환경 수준의 고가용성 컨테이너 서비스를 실현합니다. 인텔리전스 및 통합 기능이 내장된 PKS는 이러한 모든 오픈 소스 및 상업용 모듈을 하나로 통합하여 간편하게 사용할 수 있는 제품을 고객에게 제공하여 고객이 가장 효율적으로 Kubernetes를 구축하고 관리할 수 있도록 합니다.

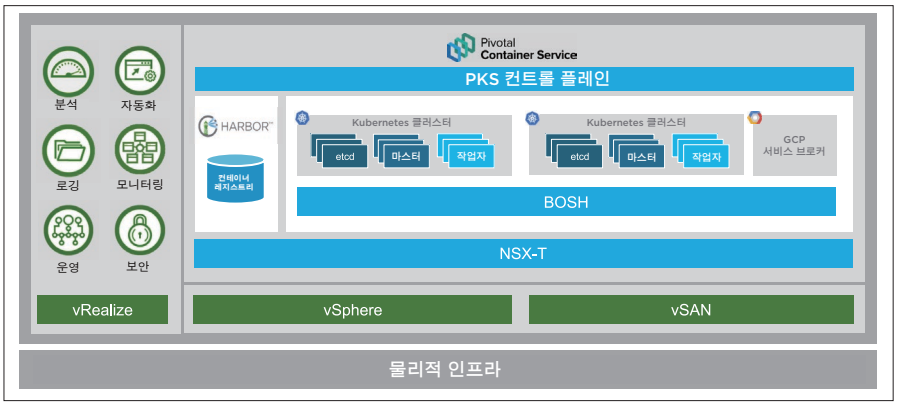

그림 1. VMware Pivotal Container Service는 VMware SDDC와 함께 포괄적인 솔루션을 제공

Kubernetes 인증

Cloud Native Computing Foundation®(CNFC) Kubernetes Software Conformance Certification 프로그램의 인증을 받은 PKS를 이용하면 고객은 CNCF 테스트를 통과한 구축과 커뮤니티 규격 준수를 통해 안심하고 애플리케이션을 실행할 수 있습니다. 점점 더 많은 조직이 Kubernetes를 도입함에 따라, PKS와 같은 인증된 Kubernetes 제품은 서로 다른 환경 간에 이동성, 상호 운용성, 일관성을 보장합니다.

Kubernetes

Kubernetes는 오픈 소스 컨테이너 조정 프레임워크입니다. 컨테이너는 애플리케이션 및 해당 종속성을 여러 환경에 걸쳐 이동성을 제공하는 배포 가능한 아티팩트(컨테이너 이미지)로 패키징하여 소프트웨어 개발 및 배포를 간소화합니다. Kubernetes는 이러한 컨테이너를 조정하여 애플리케이션의 리소스 활용도, 장애 처리, 가용성, 구성, 확장성 및 원하는 상태를 관리하고 자동화합니다. 애플리케이션과 해당 서비스가 가상 머신으로 구성된 분산형 클러스터의 컨테이너 안에서 실행되는 동안 Kubernetes는 컴퓨팅 리소스 사용을 최적화하고 애플리케이션을 원하는 상태로 유지하기 위해 모든 가변 요소를 동기화된 상태로 운영하도록 조정합니다.

BOSH

BOSH는 대규모 분산 시스템의 배포 및 수명주기 관리를 간소화하는 릴리스 엔지니어링을 위한 오픈 소스 툴이며, 개발자가 소프트웨어를 지속적이고 재현 가능한 방식으로 쉽게 버전 지정, 패키지화 및 배포하도록 지원합니다. BOSH는 VMware vSphere, Microsoft Azure, OpenStack, Google Compute Platform(GCP), Amazon Web Services EC2(AWS EC2) 등 서로 다른 IaaS 간 구축을 지원하고 출시 이래로 Cloud Foundry 플랫폼을 성공적으로 구축 및 관리하는 데 사용되어 왔습니다.

VMware NSX-T

VMware NSX T는 Kubernetes 클러스터에 마이크로 세분화, 수신 컨트롤러, 로드 밸런싱, 보안 정책 등의 고급 컨테이너 네트워킹 및 보안 기능을 제공하며 포드 수준 네트워킹에 필요한 완벽한 레이어 2-7 네트워킹 서비스를 제공합니다. PKS와 NSX-T의 통합을 사용하여 기업은 컨테이너와 포드의 마이크로 세분화와 온디맨드 네트워크 가상화를 통해 네트워크를 빠르게 구축할 수 있습니다.

Project Harbor

Harbor는 방화벽으로 보호되는 프라이빗 레지스트리에 Docker 이미지를 저장하고 배포하는 오픈 소스 기반의 엔터프라이즈급 레지스트리 서버입니다. Harbor는 RBAC(역할 기반 액세스 제어), LDAP(Lightweight Directory Access Protocol)/AD(Active Directory)를 지원할 뿐 아니라, 기업에 공증 및 감사 서비스와 컨테이너 이미지 취약점 검색, 정책 기반 이미지 복제 기능을 제공합니다.

PKS 컨트롤 플레인

PKS의 주요 구성 요소인 컨트롤 플레인은 Kubernetes 클러스터의 온디맨드 구축 및 수명주기 관리를 담당하는 셀프 서비스 인터페이스로 Kubernetes 클러스터의 셀프 서비스 사용을 지원하는 API 인터페이스를 제공합니다. API는 BOSH에 요청을 제출하여 사용자 요청에 따라 Kubernetes 클러스터의 생성, 업데이트, 삭제를 자동화합니다.

Pivotal Container Service의 주요 기능

전체 수명주기 관리 및 자동화

PKS는 Kubernetes에 수명주기 관리 및 자동화를 제공하여 빠르고 간편한 구축, 확장, 패치 적용, 업데이트를 실현하고 간단한 액션 기반 명령줄 인터페이스와 Kubernetes의 수명주기 전반에 걸쳐 다양한 사용 사례를 지원하는 개방형 API를 제공합니다. PKS를 통해 IT 관리자는 몇 분만에 여러 개의 Kubernetes 클러스터를 구축할 수 있습니다. 또한 간단한 CLI 또는 API 호출을 통해 Kubernetes 클러스터를 간편하게 확장할 수 있습니다. PKS를 통해 동일한 메커니즘으로 하나 이상의 Kubernetes 클러스터를 더욱 간편하게 패치 적용하고 업데이트할 수 있으므로, 클러스터의 보안 및 유지 보수를 항상 최신 상태로 유지할 수 있습니다. 사용자는 클러스터가 더 이상 필요하지 않은 경우 빠르게 삭제할 수 있습니다.

고가용성

PKS는 중요한 운영 수준 기능을 제공하여 Kubernetes 클러스터에서 실행 중인 워크로드의 가동 시간을 극대화합니다. PKS는 모든 기반 가상 머신 인스턴스의 상태를 지속적으로 모니터링하고 장애가 발생하거나 응답하지 않는 노드가 존재할 경우 가상 머신을 재생성합니다. 또한 전체 Kubernetes 클러스터의 연속적인 업그레이드 프로세스를 관리하여 애플리케이션 워크로드의 다운타임을 유발하지 않고 클러스터를 업그레이드할 수 있도록 합니다.

고급 컨테이너 네트워킹 및 보안

NSX-T는 컨테이너 인터페이스와 Kubernetes 포드를 위한 자동화된 소프트웨어 정의 네트워크를 PKS에 제공합니다. NSX-T 로드 밸런싱 서비스는 완전히 이중화된 고가용성 NSX Edge™ 클러스터를 통해 제공되므로, 하나의 로드 밸런서가 중단되면 트래픽이 자동으로 다른 로드 밸런서로 이동합니다. 이러한 로드 밸런싱 서비스는 Kubernetes 수신 및 로드 밸런서 구성과 완벽하게 통합됩니다. NSX는 마이크로 세분화를 추가하여 워크로드의 격리 요구 사항을 충족합니다. 각 Kubernetes 네임스페이스는 서로 격리되며 네트워크 정책을 통해 Kubernetes 네임스페이스 간에, 그리고 Kubernetes 네임스페이스 내에서 트래픽이 이동하는 방법을 지정할 수 있습니다.

PKS를 이용하면 NSX의 다양한 정책을 컨테이너 네트워킹에 적용할 수 있습니다. 또한 Traceflow, 포트 미러링 및 포트 연결 툴과 같은 운영 툴과 문제 해결 유틸리티를 사용하여 컨테이너형 애플리케이션의 운영 네트워킹 요구 사항을 충족할 수 있습니다.

컨테이너 레지스트리 보안

PKS는 엔터프라이즈급 컨테이너 레지스트리에 우수한 보안 서비스를 제공합니다. PKS 컨테이너 레지스트리는 RBAC 및 AD/LDAP 통합을 이용한 사용자 관리 및 액세스 제어를 포함하여 컨테이너 이미지에 적정 수준의 권한 및 액세스를 보장하며, 이미지 공증인 서비스 등의 보안 기능을 제공하여 게시자가 푸시 중에 이미지에 서명하도록 하고 서명하지 않은 이미지를 가져오지 못하게 차단하여 컨텐츠에 대한 신뢰를 구축합니다. PKS의 프라이빗 레지스트리를 통해 사용자는 컨테이너 이미지의 취약점을 검색하여 감염된 컨테이너 이미지와 관련된 보안 침해 리스크를 완화할 수 있습니다.

Google Kubernetes Engine(GKE)과의 지속적인 호환성

PKS는 메인라인 Kubernetes를 사용하여 개발되었으며 개발자에게 안정적인 최신 Kubernetes 릴리스를 제공합니다. PKS는 GKE가 지원하는 Kubernetes 버전과의 지속적인 호환성을 보장하기 때문에 기업의 개발자는 vSphere와 GKE 전반에서 최신 기능 및 패치를 사용할 수 있습니다. 또한 PKS는 Kubernetes에 독자적인 추상화 계층을 추가하지 않고 Kubernetes를 기본 형식으로 노출시켜 기본 Kubernetes 인터페이스를 이용한 Kubernetes와 개발자 또는 개발 툴과의 상호 작용을 지원하고 vSphere와 GKE 간에 워크로드를 손쉽게 이동할 수 있도록 합니다.

영구 스토리지

PKS를 통해 고객은 애플리케이션의 상태 저장 여부에 관계없이 Kubernetes 클러스터를 구축할 수 있습니다. PKS는 Project Hatchway를 통해 Kubernetes의 일부인 vSphere 클라우드 공급업체 스토리지 플러그인을 지원합니다. 이를 통해 PKS는 vSphere 스토리지에서 볼륨, 영구 볼륨(PV), 영구 볼륨 청구(PVC), 스토리지 계층, 상태 저장 세트 등의 Kubernetes 스토리지 기본 작업을 지원하고 Kubernetes 기반 애플리케이션에 VMware vSAN™을 통한 스토리지 정책 기반 관리(SPBM) 등의 엔터프라이즈급 스토리지 기능을 추가할 수 있습니다.

멀티 테넌시

워크로드를 격리하고 개인정보를 보호하기 위해 PKS는 기업 내 다양한 LOB(Line of Business)에서 멀티 테넌시를 지원합니다. 서로 다른 LOB의 다양한 사용자가 자신만의 Kubernetes 클러스터를 사용할 수 있습니다. 또한 NSX-T 마이크로 세분화를 통해 Kubernetes 네임스페이스를 보호하여 여러 팀이 공용 클러스터를 안심하고 사용할 수 있습니다.

멀티 클라우드

PKS는 BOSH를 통해 멀티 클라우드 배포를 지원합니다. PKS를 사용하면 vSphere를 통해 사내에 또는 Google Cloud Platform과 같은 퍼블릭 클라우드에 Kubernetes를 이용하여 컨테이너형 애플리케이션을 배포할 수 있습니다.

PKS 기능 목록	
기능	이점
온디맨드 프로비저닝	• Kubernetes 클러스터 구축 가속화 • Kubernetes 클러스터 구축 시 수작업 제거 • 오류 최소화 및 가치 실현 기간 단축
온디맨드 확장	• 간편하게 클러스터 용량 확장 • 수작업 및 오류 제거 • 리소스 활용도 최적화
온디맨드 패치 적용	• 한곳에서 여러 개의 Kubernetes 클러스터에 대한 패치 적용 및 업데이트를 더 빠르게 수행 • Kubernetes의 최신 상태 및 보안 유지
연속적인 업그레이드	• 전체 Kubernetes 클러스터에 연속적인 업그레이드를 적용하여 워크로드 다운타임 최소화
자동 상태 점검 및 자가 복구	• 모든 노드에 대한 사전 예방적 상태 모니터링을 통해 문제 방지 • 오류가 발생했거나 응답하지 않는 노드를 재생성하여 애플리케이션 서비스에 요구되는 응답성 확보
고급 컨테이너 네트워킹 및 보안	• 네트워킹 관리 간소화 및 보안 강화를 통해 개발자 및 운영 생산성 향상 • 자동 프로비저닝, 마이크로 세분화, 수신 컨트롤러, 로드 밸런싱, 보안 정책을 포함한 기본 컨테이너 네트워킹 최적화
컨테이너 레지스트리 보안	• 컨테이너 보안 향상을 통해 애플리케이션 침해 최소화 • 이미지 복제, RBAC, AD/LDAP 통합, 공증인 서비스, 취약점 검색, 감사를 통해 컨테이너 이미지 관리 간소화 및 보안 강화
GKE와의 지속적인 호환성	• 개발자에게 최신 Kubernetes 기능 및 툴을 제공하여 개발자 생산성 향상 • 사내 vSphere 환경과 GKE 간 워크로드 이동 구현
기본 Kubernetes 지원	• 독자적인 확장 기능 없이 Kubernetes를 기본 형식으로 노출시켜 벤더 종속 방지 • 개발자에게 기본 Kubernetes CLI 및 전체 YMAL 지원을 제공하여 생산성 향상
CNCF 인증 Kubernetes 배포	• 커뮤니티 규격 준수 • 서로 다른 클라우드 환경 간에 이동성, 상호 운용성, 일관성 보장
멀티 테넌시	• 개인 사용자에게 자체 Kubernetes 클러스터 제공 • 테넌트 간 워크로드 보안 및 개인 정보 보호 제공

자세한 정보

Pivotal Container Service에 대해 자세히 알아보려면 https://cloud.vmware.com/pivotal-container-service의 PKS 페이지를 방문하십시오.

PKS 기능 목록	
기능	이점
영구 스토리지	• 애플리케이션의 상태 저장 여부에 관계없이 Kubernetes 클러스터 구축 • Project Hatchway를 통해 vSphere 클라우드 공급업체 스토리지 플러그인 지원
멀티 클라우드	• vSphere 및 Google Cloud Platform 모두에 Kubernetes를 구축하고 관리하는 일관된 인터페이스를 제공하여 멀티 클라우드 환경에서 워크로드 배포 최적화

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
서울시 강남구 영동대로 517 아셈타워 13층 (우) 06164 e-메일: vmware_kr@vmware.com

Item No: 115301wf-vmw-ds-pivotal-container-service-pks-a4-106-final