VMWARE PIVOTAL CONTAINER SERVICE

EN BREF

VMware® Pivotal Container Service (PKS) est une solution de conteneur basée sur Kubernetes et de niveau production, dotée de fonctions avancées de gestion du réseau, d'un registre de conteneur privé et de fonctions de gestion complète du cycle de vie. PKS simplifie radicalement le déploiement et l'exécution de clusters Kubernetes, afin de vous permettre d'exécuter et de gérer des conteneurs à grande échelle, sur des Clouds publics autant que privés.

PRINCIPAUX AVANTAGES

- Éliminer les processus fastidieux de déploiement et de gestion grâce au provisionnement à la demande, à des fonctionnalités d'évolutivité, à l'application de correctifs et à la mise à jour de clusters Kubernetes via une simple interface CLI ou API.
- Accéder à la dernière version la plus récente de Kubernetes et assurer une compatibilité constante avec Google Kubernetes Engine (GKE).
- Garantir la haute disponibilité des composants Kubernetes (nœuds maîtres, de travail, etcd) avec le déploiement de mises à niveau, des bilans d'intégrité et l'autoréparation de l'infrastructure virtuelle sous-jacente.
- Simplifier la mise en réseau des conteneurs et renforcer la sécurité grâce à VMware NSX®, en fournissant la haute disponibilité, le provisionnement automatisé, la micro-segmentation, un contrôleur d'entrée, l'équilibrage de charge et des règles de sécurité.
- Déployer des clusters Kubernetes pour les applications sans état et avec état.
- Sécuriser les déploiements d'applications grâce à un registre de conteneurs d'entreprise intégré associé à des analyses de vulnérabilité, à la signature des images et à des capacités d'audit.

Qu'est-ce que Pivotal Container Service (PKS) ?

PKS est une solution de conteneurs dédiée permettant de rendre Kubernetes opérationnel pour les entreprises et les fournisseurs de service multicloud. Elle simplifie radicalement le déploiement et la gestion des clusters Kubernetes, avec la prise en charge des opérations de Jour 1 et de Jour 2. Grâce à ses capacités renforcées de niveau production, PKS assure le déploiement de vos conteneurs depuis la couche applications jusqu'à la couche de l'infrastructure.

PKS intègre des fonctions de production essentielles telles que la haute disponibilité, l'évolutivité automatique, les bilans d'intégrité et l'autoréparation des VM sous-jacentes, ainsi que la mise à niveau en continu des clusters Kubernetes. Grâce à une compatibilité constante avec GKE, PKS fournit la version la plus récente de Kubernetes, de sorte que les développeurs disposent des dernières fonctionnalités et des derniers outils disponibles. PKS s'intègre également avec VMware NSX-T pour la mise en réseau avancée des conteneurs, en fournissant notamment la micro-segmentation, un contrôleur d'entrée, l'équilibrage de charge et des règles de sécurité. Grâce à un registre privé intégré, PKS sécurise l'image des conteneurs au moyen d'analyses de vulnérabilité, de la signature des images et de capacités d'audit.

PKS présente Kubernetes dans sa forme native sans ajouter de couches d'abstraction ou d'extensions propriétaires, ce qui permet aux développeurs d'utiliser l'interface CLI native de Kubernetes qu'ils connaissent le mieux. PKS peut être facilement déployé et rendu opérationnel via Pivotal Operations Manager, ce qui permet de déployer PKS en s'appuyant sur un modèle opérationnel commun à l'échelle de multiples abstractions IaaS telles que vSphere et Google Cloud Platform.

Architecture Pivotal Container Service

PKS s'appuie sur Kubernetes, BOSH, VMware NSX-T et Project Harbor pour constituer un service de conteneur de niveau production et hautement disponible qui s'exécute sur VMware vSphere® et les Clouds publics. Avec des fonctions d'intelligence intégrée et d'intégration, PKS associe tous ces modules open source et commerciaux pour offrir un produit simple d'utilisation, garantissant ainsi aux clients qu'ils disposent de l'environnement de déploiement et de gestion de Kubernetes le plus efficace possible.

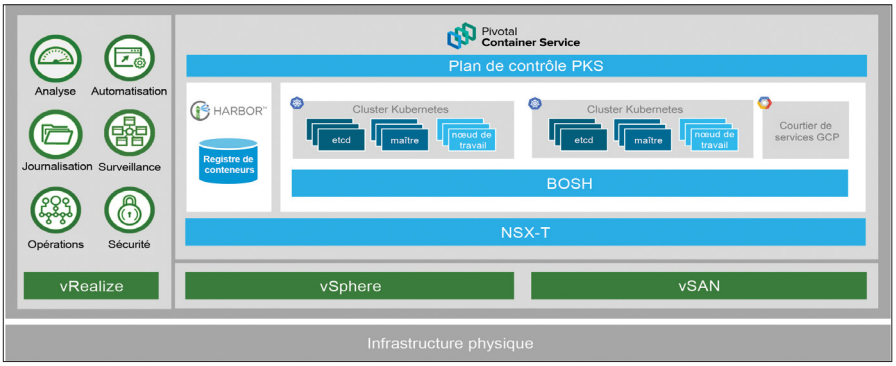

Figure 1. VMware Pivotal Container Service s'utilise conjointement avec le SDDC de VMware pour fournir une solution globale

CERTIFICATION KUBERNETES

Certifié par l'organisme Cloud Native Computing Foundation® (CNCF) dans le cadre de son programme de certification de conformité logicielle de Kubernetes, PKS permet aux clients d'exécuter des applications en étant assurés que leur déploiement a passé avec succès tous les tests du CNCF et est conforme à la spécification de la communauté. Comme un nombre croissant d'organisations adopte Kubernetes, un produit certifié comme PKS assure la portabilité, l'interopérabilité et la cohérence entre différents environnements.

Kubernetes

Kubernetes est une « structure d'orchestration » de conteneurs open source. Un conteneur regroupe une application et ses dépendances dans un objet distribuable (image de conteneur) autorisant la portabilité à l'échelle de multiples environnements, de façon à simplifier le développement et le déploiement de logiciels. Kubernetes orchestre ces conteneurs de façon à gérer et automatiser l'utilisation des ressources, le traitement des défaillances, la disponibilité, la configuration, l'évolutivité et l'état souhaité de l'application. Lorsqu'une application et ses services s'exécutent dans des conteneurs sur un cluster distribué de machines virtuelles, Kubernetes orchestre tous les éléments fluctuants de manière à ce qu'ils fonctionnent de manière synchronisée et optimise ainsi l'utilisation des ressources de calcul tout en conservant l'état souhaité d'une application.

BOSH

BOSH est un outil open source dédié à l'ingénierie, qui simplifie le déploiement et la gestion du cycle de vie des grands systèmes distribués. Il permet aux développeurs d'assurer le suivi des versions, le packaging et le déploiement des logiciels d'une manière simple, homogène et reproductible. BOSH prend en charge des déploiements dans différents environnements IaaS, tels que VMware vSphere, Microsoft Azure, OpenStack, Google Compute Platform (GCP) et Amazon Web Services EC2 (AWS EC2). BOSH a également été utilisé pour déployer et gérer avec succès la plate-forme Cloud Foundry depuis son lancement.

VMware NSX-T

VMware NSX-T fournit des fonctionnalités de mise en réseau avancée des conteneurs et de sécurité pour les clusters Kubernetes, notamment la micro-segmentation, un contrôleur d'entrée, l'équilibrage de charge et des règles de sécurité. Cette solution offre l'ensemble des services réseau des couches 2 à 7 requis pour la mise en réseau au niveau des pods. Avec l'intégration de NSX-T dans PKS, les entreprises sont en mesure de déployer rapidement des réseaux en appliquant la micro-segmentation et la virtualisation de réseau à la demande au niveau des conteneurs et des pods.

Project Harbor

Harbor est un serveur de registre de classe d'entreprise open source qui stocke et distribue les images Docker dans un registre privé derrière votre pare-feu. Outre la prise en charge du contrôle d'accès basé sur les rôles et de LDAP (Lightweight Directory Access Protocol) / AD (Active Directory), Harbor offre aux entreprises des fonctions d'analyse des vulnérabilités des images de conteneur et de réplication d'image basée sur des règles, ainsi que des services de gestion et d'audit.

Plan de contrôle PKS

Principal composant de PKS, le plan de contrôle est l'interface en libre-service chargée du déploiement à la demande et de la gestion du cycle de vie des clusters Kubernetes. Son interface API permet l'utilisation en libre-service des clusters Kubernetes. L'API envoie des requêtes à BOSH qui automatise la création, la mise à jour et la suppression des clusters Kubernetes (demandes des utilisateurs).

Principales fonctionnalités de Pivotal Container Service

Gestion et automatisation du cycle de vie complet

PKS assure la gestion du cycle de vie et l'automatisation pour Kubernetes, ce qui accélère et facilite les déploiements, l'évolutivité, l'application de correctifs et les mises à jour. PKS est doté d'une interface de ligne de commande simple fondée sur l'action et d'une interface API publique qui prend en charge de nombreux cas d'usage via le cycle de vie de Kubernetes. Avec PKS, les administrateurs peuvent déployer plusieurs clusters Kubernetes en quelques minutes. De simples appels de CLI ou d'API facilitent également l'extensibilité des clusters Kubernetes. Le même mécanisme de PKS simplifie également l'application de correctifs et la mise à jour de clusters Kubernetes, ce qui garantit que vos clusters bénéficient toujours des dernières mises à jour de sécurité et de maintenance. L'utilisateur peut rapidement supprimer les clusters s'il n'en a plus besoin.

Haute disponibilité

PKS offre des fonctionnalités essentielles taillées pour la production, qui garantissent un temps disponible maximal pour les charges de travail s'exécutant dans vos clusters Kubernetes. La solution surveille en continu l'intégrité de l'ensemble des instances de VM sous-jacentes, et recrée des VM si des nœuds sont défaillants ou ne répondent plus. PKS gère également le processus de mise à niveau en continu d'un parc de clusters Kubernetes sans interruption de service des charges de travail applicatives.

Mise en réseau et sécurité avancées des conteneurs

NSX-T fournit à PKS un réseau automatisé et software-defined pour les interfaces des conteneurs et les pods Kubernetes. Les services d'équilibrage de charge NSX-T sont basés sur un cluster NSX Edge™ hautement disponible et entièrement redondant, de sorte qu'en cas de défaillance d'un équilibreur de charge, le trafic bascule automatiquement sur un autre équilibreur. Ces services d'équilibrage de charge sont entièrement intégrés aux architectures Kubernetes Ingress et LoadBalancer. NSX ajoute la micro-segmentation NSX pour faciliter l'isolation des charges de travail. Les espaces de nommage Kubernetes peuvent être isolés les uns des autres, et les règles de gestion réseau dictent l'organisation du trafic lié aux espaces de nommage Kubernetes.

Grâce à PKS, n'importe quel éventail de règles dans NSX peut être appliqué à la mise en réseau des conteneurs. Des outils opérationnels et de dépannage tels que Traceflow et un outil de mise en miroir des ports et de connexion par port peuvent également être utilisés pour satisfaire les exigences de mise en réseau des applications conteneurisées.

Registre de conteneurs sécurisé

PKS fournit un registre de conteneurs de niveau entreprise avec des services avancés et sécurisés. Le registre de conteneurs PKS inclut le contrôle des accès et la gestion des utilisateurs avec l'intégration RBAC et AD/LDAP, qui garantit un niveau approprié d'autorisation et d'accès pour les images de conteneurs. Il propose également des fonctions de sécurité telles qu'un service de gestion des images pour fiabiliser les contenus des éditeurs, qui peuvent signer les images dans le cadre de leur transfert et empêcher la récupération des images non signées. Avec le registre privé de PKS, les utilisateurs peuvent détecter les vulnérabilités des images de conteneur et limiter ainsi le risque de violations de la sécurité liées aux images corrompues.

Compatibilité Constante avec Google Kubernetes Engine (GKE)

Ce logiciel est développé sur la base de la version principale de Kubernetes. Il propose la version la plus récente de Kubernetes à vos développeurs. Vous assurez ainsi une compatibilité constante avec les versions de Kubernetes gérées par GKE, de sorte que les développeurs ont à leur disposition les derniers correctifs et fonctionnalités pour les environnements vSphere et GKE. En outre, sans ajouter de couche d'abstraction propriétaire au-dessus de Kubernetes, PKS présente Kubernetes dans sa forme native, ce qui permet aux développeurs ou aux outils de développement d'interagir avec Kubernetes via l'interface Kubernetes native, et de garantir la portabilité des charges de travail entre vSphere et GKE.

Stockage persistant

PKS permet aux clients de déployer des clusters Kubernetes pour les applications sans état et avec état. La solution prend en charge le plug-in de stockage vSphere Cloud Provider qui est inclus dans Kubernetes au moyen du projet Project Hatchway. Ceci permet à PKS de prendre en charge les primitives de stockage Kubernetes telles que Volumes, Persistent Volumes (PV), Persistent Volumes Claims (PVC), Storage Class et Stateful Sets sur les solutions de stockage vSphere, et d'ajouter des fonctions de stockage de niveau entreprise telles que Storage Policy Based Management (SPBM) avec VMware vSAN™ aux applications Kubernetes.

Mutualisation

Afin d'isoler les charges de travail et de garantir la confidentialité, PKS prend en charge des instances multiples pour les différentes branches d'activité des entreprises. De multiples utilisateurs au sein de ces branches d'activité sont en mesure d'utiliser leurs propres clusters Kubernetes. En outre, grâce à la micro-segmentation NSX-T, les espaces de nommage Kubernetes peuvent être sécurisés pour plusieurs équipes au moyen d'un cluster partagé.

Multicloud

PKS prend en charge le déploiement multicloud à l'aide de BOSH. Grâce à PKS, vous pouvez déployer des applications conteneurisées avec une solution Kubernetes on premise sur vSphere, ou dans un Cloud public tel que Google Cloud Platform.

LISTE DES FONCTIONS DE PKS	
Fonction	Avantages
Provisionnement à la demande	• Accélère le déploiement des clusters Kubernetes • Élimine les étapes manuelles des déploiements de clusters Kubernetes • Limite les erreurs et accélère le retour sur investissement
Évolutivité à la demande	• Ajuste facilement la capacité du cluster • Élimine les étapes manuelles et les erreurs • Optimise l'utilisation des ressources
Application de correctifs à la demande	• Centralise et accélère l'application de correctifs et la mise à jour de multiples clusters Kubernetes • Garantit l'actualisation et la protection des clusters Kubernetes
Mises à niveau en continu	• Limite les temps d'indisponibilité des charges de travail par la mise à niveau en continu d'un parc de clusters Kubernetes
Bilans d'intégrité automatique et autoréparation	• Évite les problèmes grâce à une surveillance proactive de l'intégrité de tous les nœuds • Garantit le niveau de réactivité souhaité des services applicatifs en recréant des nœuds en cas de défaillance
Mise en réseau et sécurité avancées des conteneurs	• Augmente la productivité des équipes de développement et des opérations en simplifiant la gestion du réseau et en renforçant la sécurité • Optimise la mise en réseau native des conteneurs, en fournissant notamment le provisionnement automatique, la micro-segmentation, un contrôleur d'entrée, l'équilibrage de charge et des règles de sécurité
Registre de conteneurs sécurisé	• Réduit les violations de la sécurité grâce à une protection renforcée des conteneurs • Simplifie la gestion de l'image des conteneurs et renforce la sécurité via la réplication d'image, le contrôle d'accès basé sur les rôles, l'intégration AD/LDAP, les services de gestion, les analyses de vulnérabilité et les fonctions d'audit
Compatibilité constante avec Google Container Engine (GKE)	• Permet d'augmenter la productivité des développeurs en leur permettant de bénéficier des derniers outils et fonctions Kubernetes • Garantit la portabilité des charges de travail entre les environnements vSphere on premise et GKE

EN SAVOIR PLUS

Pour en savoir plus sur Pivotal Container Service, consultez la page PKS sur https://cloud.vmware.com/pivotal-container-service.

LISTE DES FONCTIONS DE PKS	
Fonction	Avantages
Prise en charge native de Kubernetes	• Présente Kubernetes dans sa forme native sans extensions propriétaires, ce qui évite la dépendance vis-à-vis d'un fournisseur • Permet d'augmenter la productivité des développeurs en leur offrant l'interface CLI native de Kubernetes et la prise en charge du langage YAML
Distribution Kubernetes certifiée par l'organisme CNCF	• Conforme aux spécifications de la communauté • Assure la portabilité, l'interopérabilité et la cohérence entre différents environnements cross-cloud
Mutualisation	• Fournit aux utilisateurs leurs propres clusters Kubernetes • Sécurise les charges de travail entre les locataires et garantit la confidentialité
Stockage persistant	• Déploie des clusters Kubernetes pour les applications sans état et avec état • Prend en charge le plug-in de stockage vSphere Cloud Provider au moyen du projet Project Hatchway
Multicloud	• Optimise le déploiement des charges de travail dans les environnements multicloud grâce à une interface cohérente pour déployer et gérer Kubernetes sur vSphere et sur Google Cloud Platform

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.com/fr