

# VMWARE PIVOTAL CONTAINER SERVICE

## INFORMACIÓN BÁSICA

VMware® Pivotal Container Service (PKS) es una solución de contenedores basada en Kubernetes para entornos de producción dotada de funciones de redes avanzadas, registro de contenedores privado y gestión completa del ciclo de vida. PKS simplifica radicalmente la implementación y el funcionamiento de los clústeres de Kubernetes con lo que le facilita la ejecución y la gestión de los contenedores según las necesidades en las clouds públicas y privadas.

## VENTAJAS PRINCIPALES

- Elimine los largos procesos de implementación y gestión mediante el aprovisionamiento según las necesidades, el escalado, la aplicación de parches y la actualización de clústeres de Kubernetes a través de una sencilla CLI o API.
- Acceda a la última versión estable de Kubernetes y obtenga una compatibilidad constante con Google Kubernetes Engine (GKE).
- Proporcione una alta disponibilidad a los componentes de Kubernetes (nodos maestro, esclavo y etcd) con actualizaciones continuas, comprobaciones del estado y recuperaciones automáticas de la infraestructura virtual subyacente.
- Simplifique las redes de contenedores y aumente la seguridad con VMware NSX®, proporcionando alta disponibilidad, aprovisionamiento automatizado, microsegmentación, controlador de entrada, equilibrio de carga y política de seguridad.
- Implemente clústeres de Kubernetes para aplicaciones con y sin estado.
- Proteja las implementaciones de aplicaciones mediante un registro integrado de contenedores empresariales que incorpore funciones de detección de vulnerabilidades, firma de imágenes y auditorías.

## ¿Qué es Pivotal Container Service (PKS)?

PKS es una solución de contenedor creada expresamente para hacer que Kubernetes sea operativo para empresas multicloud y proveedores de servicios. Simplifica considerablemente la implementación y la gestión de los clústeres de Kubernetes con operaciones iniciales y posteriores. Gracias a sus funciones reforzadas para entornos de producción, PKS lleva a cabo la implementación de contenedores desde la capa de aplicaciones hasta llegar a la capa de infraestructura.

PKS incorpora características de producción esenciales, como una alta disponibilidad, el escalado automático, las comprobaciones del estado y la recuperación automática de las máquinas virtuales subyacentes, así como las actualizaciones continuas de los clústeres de Kubernetes. Con una compatibilidad constante con GKE, PKS ofrece la última versión estable de Kubernetes para que los desarrolladores puedan disponer de las funciones y herramientas más recientes. Se integra también con VMware NSX-T para redes de contenedores avanzadas mediante la microsegmentación, el controlador de entrada, el equilibrio de carga y la política de seguridad. Mediante un registro privado integrado, PKS protege la imagen de contenedor a través de la detección de vulnerabilidades, la firma de imágenes y las auditorías.

PKS ofrece Kubernetes en su forma nativa sin añadir capas de desvinculación ni extensiones de propiedad reservada, lo que permite a los desarrolladores utilizar la CLI nativa de Kubernetes con la que están más familiarizados. PKS se puede implementar y utilizar fácilmente a través de Pivotal Operations Manager, lo que permite que un modelo operativo común implemente PKS en varias desvinculaciones de la infraestructura como servicio (IaaS), tales como vSphere y Google Cloud Platform.

## Arquitectura de Pivotal Container Service

PKS se basa en Kubernetes, BOSH, VMware NSX-T y Project Harbor para ofrecer un servicio de contenedores de alta disponibilidad para entornos de producción que se ejecuta en VMware vSphere® y las clouds públicas. Con funciones de inteligencia e integración incorporadas, PKS combina todos estos módulos de código abierto y uso comercial, para ofrecer a los clientes un producto fácil de usar y garantizarles la experiencia más eficiente posible de implementación y gestión de Kubernetes.

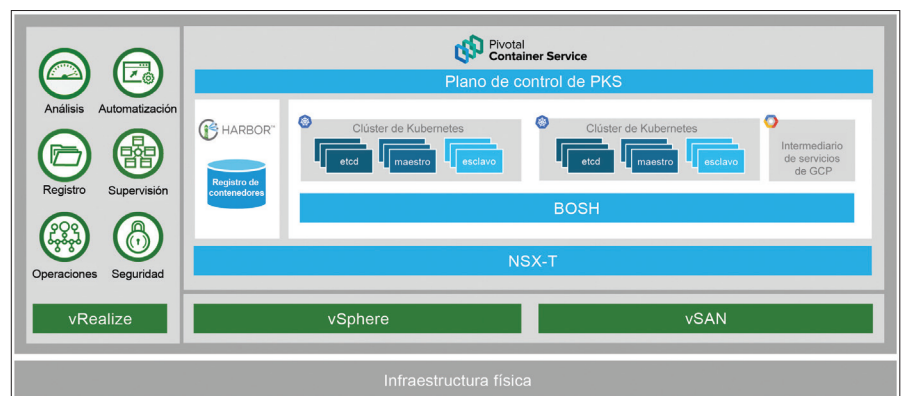


Figura 1. VMware Pivotal Container Service funciona con el SDDC de VMware para ofrecer una solución completa.

## CERTIFICACIÓN DE KUBERNETES



Con la certificación de Cloud Native Computing Foundation® (CNCF) en su [programa Kubernetes Software Conformance](#)

[Certification](#), PKS permite a los clientes ejecutar aplicaciones con la confianza de que su implementación ha pasado las pruebas de CNCF y cumple las especificaciones de la comunidad.

Y, a medida que el número de organizaciones que adoptan Kubernetes aumenta, los productos con certificación de Kubernetes, como es el caso de PKS, permiten garantizar la portabilidad, la interoperabilidad y la coherencia entre distintos entornos.

## Kubernetes

Kubernetes es un marco de coordinación de contenedores con código abierto. Los contenedores empaquetan las aplicaciones y sus dependencias en un elemento distribuido (imagen de contenedor) que proporciona portabilidad en varios entornos, optimizando el desarrollo y la implementación de software. Kubernetes coordina estos contenedores para gestionar y automatizar la utilización de los recursos, la gestión de fallos, la disponibilidad, la configuración, la escalabilidad y el estado deseado de la aplicación. Cuando una aplicación y sus servicios se ejecutan en contenedores en un clúster distribuido de máquinas virtuales, Kubernetes coordina todos los elementos involucrados para que funcionen de forma sincronizada y así optimizar el uso de los recursos informáticos y mantener el estado deseado de la aplicación.

## BOSH

BOSH es una herramienta de código abierto para ingeniería de versiones que simplifica la implementación y la gestión del ciclo de vida para grandes sistemas distribuidos. Permite a los desarrolladores gestionar versiones, empaquetar e implementar software de un modo fácil, coherente y reproducible. BOSH permite realizar implementaciones en distintas IaaS, como VMware vSphere, Microsoft Azure, OpenStack, Google Compute Platform (GCP) y Amazon Web Services EC2 (AWS EC2), y se ha utilizado para implementar y gestionar con éxito la plataforma Cloud Foundry desde su creación.

## VMware NSX-T

VMware NSX-T ofrece funciones de redes de contenedores avanzadas y seguridad para clústeres de Kubernetes, como la microsegmentación, el controlador de entrada, el equilibrio de carga y la política de seguridad. Proporciona el conjunto completo de servicios de red de capa 2 a capa 7 que se requiere para las operaciones de red a nivel de módulo. Con la integración de NSX-T en PKS, las empresas pueden implementar redes rápidamente con la microsegmentación y la virtualización de red según las necesidades para los contenedores y los módulos.

## Project Harbor

Harbor es un servidor de registro de nivel empresarial con código abierto que almacena y distribuye imágenes de Docker en un registro privado más allá de su cortafuegos. Además de proporcionar compatibilidad con RBAC (control de acceso basado en funciones), LDAP (protocolo ligero de acceso a directorios)/AD (Active Directory), Harbor proporciona a las empresas funciones de detección de vulnerabilidades de imagen de contenedor, replicación de imágenes basada en políticas, así como servicios de notaría y auditoría.

## Plano de control de PKS

El plano de control es un componente esencial de PKS, ya que se ocupa de las interfaces de autoservicio para la implementación según las necesidades y la gestión del ciclo de vida de los clústeres de Kubernetes. Ofrece una interfaz API que permite el autoservicio de los clústeres de Kubernetes. La API envía solicitudes a BOSH que automatiza la creación, la actualización y la eliminación de los clústeres de Kubernetes en función de las solicitudes de los usuarios.

## Funciones principales de Pivotal Container Service

### Gestión del ciclo de vida completo y automatización

PKS ofrece gestión del ciclo de vida y automatización en Kubernetes, facilitando y agilizando los procesos de implementación, escalado, aplicación de parches y actualización. Proporciona una sencilla interfaz de línea de comandos basada en la acción y una API pública que admite diversos casos de uso a través del ciclo de vida de Kubernetes. Con PKS, los administradores de TI pueden implementar varios clústeres de Kubernetes en solo unos minutos. El escalado de los clústeres de Kubernetes también se puede llevar a cabo fácilmente a través de llamadas a la CLI o API. PKS facilita además la aplicación de parches y la actualización de uno o varios clústeres de Kubernetes a través de estos mismos mecanismos, asegurándose de que los clústeres están siempre al día de las últimas actualizaciones en materia de seguridad y mantenimiento. Si el usuario ya no necesita los clústeres, puede eliminarlos rápidamente.

### Alta disponibilidad

PKS proporciona funciones para entornos de producción esenciales con el fin de garantizar un tiempo de actividad máximo en las cargas de trabajo que se ejecutan en los clústeres de Kubernetes. Supervisa continuamente el estado de todas las instancias de la máquina virtual subyacentes, y recrea las máquinas virtuales cuando se detectan nodos que fallan o no responden. También gestiona el proceso de actualización continua para un grupo de clústeres de Kubernetes, permitiendo la actualización de los clústeres sin tiempo de inactividad para las cargas de trabajo de las aplicaciones.

### Redes de contenedores avanzadas y seguridad

NSX-T proporciona a PKS una red automatizada definida por software para las interfaces de contenedores y los módulos de Kubernetes. Los servicios de equilibrio de carga que proporciona NSX-T se encuentran en un clúster de NSX Edge™ de alta disponibilidad y totalmente redundante, por lo que si un equilibrador de carga deja de funcionar, el tráfico automáticamente pasaría a otro equilibrador de carga. Estos servicios de equilibrio de carga están totalmente integrados con las estructuras de entrada y equilibrador de carga de Kubernetes. NSX añade la microsegmentación para satisfacer los requisitos de aislamiento de las cargas de trabajo. Es posible aislar los espacios de nombres de Kubernetes entre sí, y las políticas de red pueden especificar el modo en que puede desplazarse el tráfico entre los espacios de nombres de Kubernetes, así como dentro de cada uno de ellos.

Con PKS, se puede aplicar cualquiera de la amplia gama de políticas de NSX a las redes de contenedores. También se pueden utilizar herramientas operativas y utilidades para la solución de problemas (como Traceflow), y la herramienta de creación de reflejo de puertos y conexión de puerto para satisfacer los requisitos de las redes de producción para las aplicaciones contenedorizadas.

### Registro de contenedores seguro

PKS ofrece un registro de contenedores empresariales a través de servicios avanzados y seguros. El registro de contenedores de PKS incluye la gestión de usuarios y el control de acceso mediante la integración de RBAC y AD/LDAP, lo que garantiza un nivel adecuado de autoridad y el acceso a imágenes de contenedor. También ofrece funciones de seguridad, como el servicio de notaría de imagen que hace posible confiar en los contenidos, ya que permite firmar la imagen cuando se inserta y evita que se extraigan imágenes sin firma. Con el registro privado de PKS, los usuarios pueden examinar imágenes de contenedor para detectar vulnerabilidades con objeto de reducir el riesgo de vulneraciones de la seguridad relacionadas con imágenes de contenedor contaminadas.

### Compatibilidad constante con Google Kubernetes Engine (GKE)

PKS se ha desarrollado con la línea principal de Kubernetes y proporciona la última versión estable de Kubernetes a los desarrolladores. Garantiza una compatibilidad constante con las versiones de Kubernetes que GKE admite, por lo que los desarrolladores empresariales tienen a su disposición las últimas funciones y parches en vSphere y GKE. Asimismo, sin añadir ninguna capa de desvinculación de propiedad reservada a Kubernetes, PKS ofrece Kubernetes en su forma nativa, por lo que los desarrolladores o las herramientas de desarrollo pueden interactuar con Kubernetes mediante la interfaz nativa de Kubernetes, y las cargas de trabajo pueden transportarse entre vSphere y GKE.

### Almacenamiento persistente

PKS permite a los clientes implementar clústeres de Kubernetes para aplicaciones con y sin estado. Admite el complemento de almacenamiento vSphere Cloud Provider que forma parte de Kubernetes mediante [Project Hatchway](#). De este modo PKS puede admitir primitivas de almacenamiento de Kubernetes —como los volúmenes, los volúmenes persistentes, las notificaciones de volúmenes persistentes, la clase de almacenamiento y los conjuntos con estado— en el almacenamiento de vSphere, y también incorpora funciones de almacenamiento empresarial, como Storage Policy Based Management (SPBM) con VMware vSAN™ en las aplicaciones basadas en Kubernetes.

### Entorno multicliente

Para aislar las cargas de trabajo y garantizar la privacidad, PKS admite entornos multicliente para diversas líneas de negocio dentro de una empresa. Los distintos usuarios de las distintas líneas de negocio pueden utilizar sus propios clústeres de Kubernetes. Asimismo, con la microsegmentación que ofrece NSX-T, se pueden proteger los espacios de nombres de Kubernetes para los distintos equipos que comparten un mismo clúster.

### Entorno multicloud

PKS admite la implementación en entornos multicloud a través de BOSH. Con PKS, puede implementar una aplicación contenedorizada con Kubernetes a nivel local en vSphere o en las clouds públicas como Google Cloud Platform.

LISTA DE CARACTERÍSTICAS DE PKS	
Característica	Ventajas
Aprovisionamiento según las necesidades	<ul style="list-style-type: none"> <li>• Acelera la implementación de los clústeres de Kubernetes.</li> <li>• Elimina los pasos manuales para implementar los clústeres de Kubernetes.</li> <li>• Minimiza los errores y reduce la rentabilidad.</li> </ul>
Escalado según las necesidades	<ul style="list-style-type: none"> <li>• Adapta la capacidad del clúster de forma sencilla.</li> <li>• Elimina los pasos manuales y los errores.</li> <li>• Optimiza la utilización de recursos.</li> </ul>
Aplicación de parches según las necesidades	<ul style="list-style-type: none"> <li>• Centraliza y acelera la aplicación de parches y la actualización de varios clústeres de Kubernetes.</li> <li>• Mantiene al día los clústeres y los protege.</li> </ul>
Actualizaciones continuas	<ul style="list-style-type: none"> <li>• Minimiza el tiempo de inactividad de la carga de trabajo mediante la actualización continua de una flota de clústeres de Kubernetes.</li> </ul>
Comprobación del estado y recuperación automáticas	<ul style="list-style-type: none"> <li>• Evita problemas con la supervisión proactiva del estado de todos los nodos.</li> <li>• Garantiza el dinamismo deseado de los servicios de aplicaciones mediante la recreación de los nodos que fallan o no responden.</li> </ul>
Redes de contenedores avanzadas y seguridad	<ul style="list-style-type: none"> <li>• Aumenta la productividad de los desarrolladores y operadores simplificando la gestión de redes y mejorando la seguridad.</li> <li>• Optimiza las redes de contenedores nativas, como el aprovisionamiento automático, la microsegmentación, el controlador de entrada, el equilibrio de carga y las políticas de seguridad.</li> </ul>
Registro de contenedores seguro	<ul style="list-style-type: none"> <li>• Minimiza las vulneraciones de las aplicaciones mejorando la seguridad de los contenedores.</li> <li>• Simplifica la gestión de imágenes de contenedor y mejora la seguridad a través de la replicación de imágenes, RBAC, la integración de AD/LDAP, los servicios de notaría, la detección de vulnerabilidades y las auditorías.</li> </ul>
Compatibilidad constante con GKE	<ul style="list-style-type: none"> <li>• Aumenta la productividad de los desarrolladores dándoles acceso a las funciones y herramientas de Kubernetes más actualizadas.</li> <li>• Permite que las cargas de trabajo sean portátiles entre el entorno local de vSphere y GKE.</li> </ul>
Compatibilidad nativa con Kubernetes	<ul style="list-style-type: none"> <li>• Ofrece Kubernetes en su forma nativa sin extensiones de propiedad reservada para evitar la dependencia de los proveedores.</li> <li>• Aumenta la productividad de los desarrolladores ofreciéndoles la CLI nativa de Kubernetes y plena compatibilidad con YML.</li> </ul>

## MÁS INFORMACIÓN

Para obtener más información sobre Pivotal Container Service, visite la página de PKS en <https://cloud.vmware.com/pivotal-container-service>.

LISTA DE CARACTERÍSTICAS DE PKS	
Característica	Ventajas
Distribución de Kubernetes con certificado CNCF	<ul style="list-style-type: none"> <li>Cumple con la especificación de la comunidad.</li> <li>Garantiza la portabilidad, la interoperabilidad y la coherencia entre distintos entornos multicloud.</li> </ul>
Entorno multicliente	<ul style="list-style-type: none"> <li>Proporciona a cada usuario sus propios clústeres de Kubernetes.</li> <li>Protege las cargas de trabajo entre clientes y proporciona privacidad.</li> </ul>
Almacenamiento persistente	<ul style="list-style-type: none"> <li>Implementa clústeres de Kubernetes para aplicaciones con y sin estado.</li> <li>Admite el complemento de almacenamiento vSphere Cloud Provider mediante Project Hatchway.</li> </ul>
Entorno multicloud	<ul style="list-style-type: none"> <li>Optimiza la implementación de la carga de trabajo en entornos multicloud mediante una interfaz coherente para implementar y gestionar Kubernetes en vSphere y Google Cloud Platform.</li> </ul>

