# Enfoque en capas para la seguridad de los contenedores y de Kubernetes

Protección de los contenedores, desde el diseño hasta la implementación y la ejecución

## Índice




facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

## Introducción

Con el tiempo, los contenedores han logrado destacarse gracias a su capacidad para empaquetar las aplicaciones y sus dependencias en una sola imagen que se puede trasladar desde la etapa de desarrollo hasta las de prueba y producción. Estos permiten garantizar la consistencia entre los entornos y varios objetivos de implementación, como los servidores físicos, las máquinas virtuales (VM) y las nubes privadas o públicas. Gracias a los contenedores, los equipos pueden desarrollar y gestionar con mayor facilidad las aplicaciones que aportan agilidad a la empresa.

- **Aplicaciones:** con los contenedores, los desarrolladores pueden crear y trasladar fácilmente una aplicación y sus dependencias como una unidad. Su implementación se puede llevar a cabo en cuestión de segundos. En un entorno organizado en contenedores, el proceso de diseño de software es la etapa del ciclo de vida en la que el código de una aplicación se integra con las bibliotecas de tiempo de ejecución necesarias.
- **Infraestructura:** los contenedores representan los procesos aislados de las aplicaciones en el kernel compartido de un sistema operativo Linux®. Son más compactos, livianos y sencillos que las máquinas virtuales. Además, se pueden usar en diferentes entornos, desde plataformas on-premise hasta nubes públicas.

Kubernetes es la plataforma de organización en contenedores preferida de las empresas. Hoy más que nunca es fundamental garantizar la seguridad de los contenedores, ya que muchas empresas ejecutan sus servicios esenciales en ellos. En este artículo, se describen los elementos clave de seguridad para las aplicaciones en contenedores.

## Seguridad integral de los contenedores y de Kubernetes: capas y ciclo de vida

Proteger los contenedores es como proteger cualquier proceso de Linux en ejecución. Antes de implementar y ejecutar su contenedor, debe considerar la seguridad en todas las capas de la pila de soluciones. También es importante tener en cuenta la seguridad a lo largo de todo el ciclo de vida de la aplicación y del contenedor. Cabe destacar que la seguridad debe ser un proceso constante que se integra a todo el ciclo de vida de la TI, y que se extiende para responder a las nuevas amenazas y soluciones a medida que surgen. La Figura 1 muestra un enfoque integral para la seguridad de los contenedores.


Figura 1. La seguridad integral de los contenedores implica proteger el diseño, la implementación y el tiempo de ejecución, además de ampliar la seguridad con herramientas especializadas cuando sea necesario.

Con los contenedores, los desarrolladores pueden crear y trasladar fácilmente una aplicación y sus dependencias como una unidad. Además, le permiten aprovechar al máximo sus servidores porque posibilitan las implementaciones de aplicaciones de arquitectura multiempresa en un host compartido. Usted podrá implementar fácilmente varias aplicaciones en un solo host, y poner en marcha o detener los contenedores individuales según sea necesario. A diferencia de la virtualización tradicional, no necesita un hipervisor para gestionar sistemas operativos guest en cada máquina virtual, ya que los contenedores se encargan de virtualizar los procesos de sus aplicaciones, no el hardware.

Ciertamente, no es usual que las aplicaciones se distribuyan en un solo contenedor. Incluso las aplicaciones más sencillas suelen tener un frontend, un backend y una base de datos. Además, tal como se muestra en la Figura 2, la implementación en contenedores de aplicaciones modernas de microservicios implica la implementación de varios contenedores, a veces en el mismo host, y otras veces distribuidos en múltiples host o nodos.

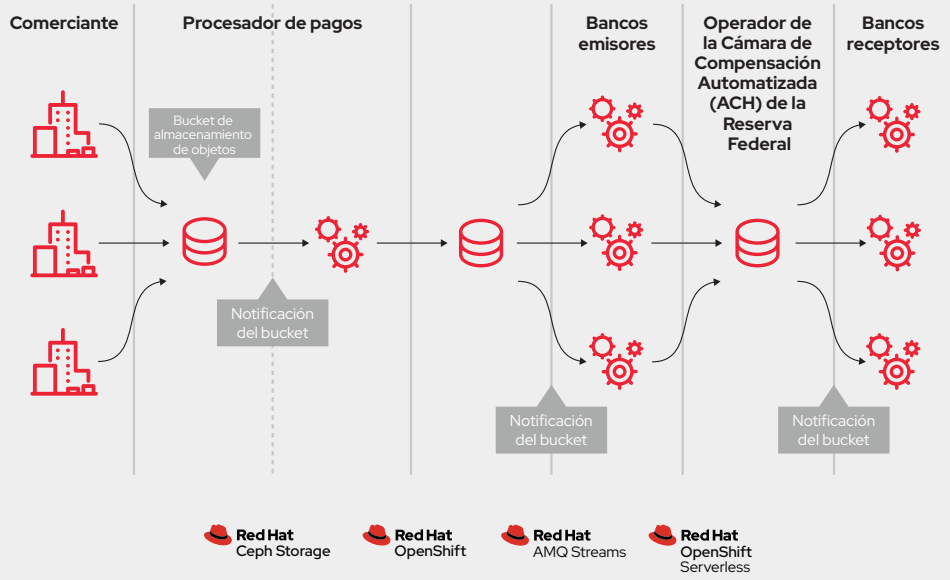


Figura 2. Los entornos de los contenedores pueden ser complejos y estar distribuidos en varios nodos.

Al gestionar la implementación de contenedores según sea necesario, debe tener en cuenta:

- Qué contenedores deben implementarse en qué hosts.
- Cuáles son los hosts que tienen más capacidad.
- Qué contenedores necesitan poder acceder a otros contenedores, y cómo harán para detectarse.
- Cómo controlar no solo el acceso a los recursos compartidos, como la red y el almacenamiento, sino también su gestión.
- Cómo supervisar el estado del contenedor.
- Cómo ajustar automáticamente la capacidad de las aplicaciones para satisfacer la demanda.
- Cómo habilitar la tecnología de autoservicio para desarrolladores y a la vez cumplir con los requisitos de seguridad.

Usted puede diseñar su propio entorno de gestión de contenedores, para lo cual deberá dedicar tiempo a integrar y gestionar los elementos individuales. O bien, puede implementar una plataforma de contenedores con funciones integradas de gestión y seguridad. Este enfoque permite que su equipo concentre sus energías en diseñar las aplicaciones que aportan valor empresarial, y no en volver a diseñar la infraestructura.

Red Hat® OpenShift® Container Platform ofrece una plataforma uniforme de Kubernetes empresarial para la nube híbrida que permite diseñar y ajustar las aplicaciones en contenedores. Para poder utilizar Kubernetes en toda la empresa, necesita funciones adicionales que le ayuden a incorporar la seguridad a sus aplicaciones, políticas automatizadas para gestionar la seguridad de la implementación de contenedores y funciones que le permitan proteger el tiempo de ejecución de estos.

## Incorpore la seguridad a sus aplicaciones

En el caso de las implementaciones en la nube, es fundamental que incorpore la seguridad a sus aplicaciones. Para proteger sus aplicaciones en contenedores deberá:

1. Usar el contenido del contenedor de confianza
2. Usar un registro de contenedores empresariales
3. Controlar y automatizar el diseño de contenedores
4. Integrar la seguridad al canal de la aplicación

### 1. Uso del contenido del contenedor de confianza

A la hora de gestionar la seguridad, lo que se encuentra dentro del contenedor es importante. Desde hace algún tiempo, las aplicaciones y las infraestructuras se componen de elementos a los que se puede acceder con facilidad. Muchos de ellos son paquetes open source, como el sistema operativo Linux, Apache Web Server, Red Hat JBoss® Enterprise Application Platform, PostgreSQL y Node.js. Las versiones en contenedores de estos paquetes también están disponibles, de manera tal que no tiene que diseñarlas usted mismo. Sin embargo, al igual que con los códigos que descarga de una fuente externa, usted debe conocer dónde se originaron los paquetes, quién los diseñó y si hay algún código malicioso en ellos. Pregúntese:

- ¿El contenido del contenedor pondrá en peligro mi infraestructura?
- ¿Hay algún punto vulnerable conocido en la capa de la aplicación?
- ¿Están actualizadas las capas del tiempo de ejecución y del sistema operativo en el contenedor?
- ¿Con qué frecuencia se actualizará el contenedor y cómo sabré cuando se llevará a cabo?

Durante años, Red Hat se ha encargado de empaquetar y ofrecer contenido confiable de Linux en Red Hat Enterprise Linux y en toda nuestra cartera de productos. Ahora, Red Hat distribuye ese mismo contenido empaquetado y confiable como contenedores de Linux. Gracias a la incorporación de imágenes de base universales de Red Hat, puede aprovechar la mayor confiabilidad, seguridad y rendimiento de las imágenes de contenedores de Red Hat, sin importar dónde se ejecuten los contenedores de Linux compatibles con la Open Container Initiative (OCI). Esto significa que puede diseñar una aplicación en contenedor en una imagen de base universal de Red Hat, trasladarla al registro que usted elija y compartirla.

Red Hat también proporciona una gran cantidad de imágenes y operadores certificados para distintos tiempos de ejecución del lenguaje, middleware, bases de datos y más, a través de Red Hat Ecosystem Catalog. Los contenedores y operadores certificados de Red Hat funcionan en cualquier lugar donde se ejecute Red Hat Enterprise Linux, desde los equipos sin sistema operativo hasta las máquinas virtuales y la nube, y cuentan con el soporte de Red Hat y de nuestros partners.

Red Hat supervisa de forma permanente el estado de las imágenes que distribuye. El índice de estado de los contenedores muestra el "grado" de cada imagen de contenedor, y detalla cómo deben coordinarse, utilizarse y evaluarse para satisfacer las necesidades de los sistemas de producción. La clasificación de los contenedores se basa en parte en la antigüedad y el impacto de las erratas de seguridad no aplicadas a todos los elementos de un contenedor, lo que proporciona una clasificación agregada de la seguridad que puede ser entendida tanto por los expertos en la materia como por los que no lo son.

Cuando Red Hat lanza actualizaciones de seguridad, como correcciones de runc CVE-2019-5736, MDS CVE-2019-11091 o VHOST-NET CVE-2019-14835, nosotros también rediseñamos nuestras imágenes de contenedores y las incorporamos al registro público. Los avisos de seguridad de Red Hat le advierten sobre cualquier problema detectado recientemente en las imágenes certificadas de los contenedores, y lo dirigen hacia la imagen actualizada para que usted pueda actualizar cualquier aplicación que la utilice.

Puede haber ocasiones en las que necesite contenido que Red Hat no ofrece. Le recomendamos usar las herramientas de análisis de contenedores que utilizan constantemente bases de datos actualizadas de puntos vulnerables, para asegurarse de tener siempre la información más reciente sobre los aspectos vulnerables conocidos cuando se emplean imágenes de contenedores de otras fuentes. Dado que la lista de puntos vulnerables conocidos cambia todo el tiempo, deberá verificar el contenido de sus imágenes de contenedores cuando las descargue por primera vez, y realizar un seguimiento del estado de los aspectos vulnerables de todas las imágenes aprobadas e implementadas, tal como Red Hat lo hace con sus imágenes de contenedores.

### 2. Uso de un registro de contenedores empresariales para acceder de forma más segura a las imágenes de contenedores

Claro está que sus equipos diseñan contenedores que ubican el contenido por encima de las imágenes públicas de contenedores que usted descarga. El acceso a las imágenes de contenedores descargadas y a las imágenes diseñadas internamente, y su posterior traslado, se deben gestionar de la misma manera en que se gestionan otros tipos de binarios. Hay una serie de registros privados que admiten el almacenamiento de imágenes de contenedores. Le recomendamos seleccionar un registro privado que le permita automatizar las políticas de uso de las imágenes de contenedores almacenadas en el registro.

Red Hat OpenShift incluye un registro privado que proporciona funciones básicas para gestionar sus imágenes de contenedores. El registro de Red Hat OpenShift proporciona controles de acceso basado en funciones (RBAC) que le permiten gestionar quién puede insertar y extraer imágenes de contenedores específicas. Además, admite la integración con otros registros privados que posiblemente ya esté usando, como Sonatype Nexus y Artifactory de JFrog.

Red Hat Quay está disponible como un registro empresarial independiente y ofrece varias funciones adicionales, como la replicación geográfica y activadores de creación de imágenes.

El proyecto Clair es un motor open source que impulsa al escáner de seguridad de la solución Red Hat Quay para que detecte puntos vulnerables en todas las imágenes dentro de ella. Red Hat OpenShift Container Security Operator se integra a Red Hat Quay para proporcionar un panorama completo del clúster con los aspectos vulnerables conocidos de sus imágenes implementadas en la consola de OpenShift.

### 3. Control y automatización del diseño de imágenes de contenedores

Poder administrar este proceso de diseño es fundamental para proteger la pila de software. La adhesión a la filosofía "diseñe una sola vez e implemente en cualquier lugar" garantiza que el producto del proceso de diseño sea exactamente igual a lo que se implementa en la etapa de producción. También es importante mantener la inmutabilidad de los contenedores, es decir, no aplicar parches en los contenedores que se están ejecutando, sino volver a diseñarlos e implementarlos.

Red Hat OpenShift proporciona una serie de funciones para la automatización de las compilaciones basada en eventos externos, como una forma de mejorar la seguridad de sus imágenes personalizadas.

- Los activadores de Red Hat Quay proporcionan un mecanismo para generar la compilación de un repositorio de Dockerfile a partir de un evento externo, como un webhook o la transferencia de contenido de GitHub, BitBucket o GitLab a un repositorio remoto.
- Source-to-image (S2I) es un marco open source que combina códigos fuente e imágenes de base (Figura 3). Este permite que sus equipos de desarrollo y de operaciones colaboren entre sí en un entorno de diseño reproducible. Cuando un desarrollador confirma los cambios en el código con Git y usa S2I, Red Hat OpenShift puede:
  - Activar el ensamblaje automático de una nueva imagen desde artefactos disponibles, como la imagen de base de S2I, y el código confirmado recientemente (mediante webhooks en el repositorio del código o algún otro proceso de integración continua [CI] automatizado).
  - Implementar de forma automática la imagen diseñada recientemente para probarla.
  - Trasladar la imagen probada a la etapa de producción e implementar automáticamente la nueva imagen a través del proceso de integración e implementación continuas (CI/CD).

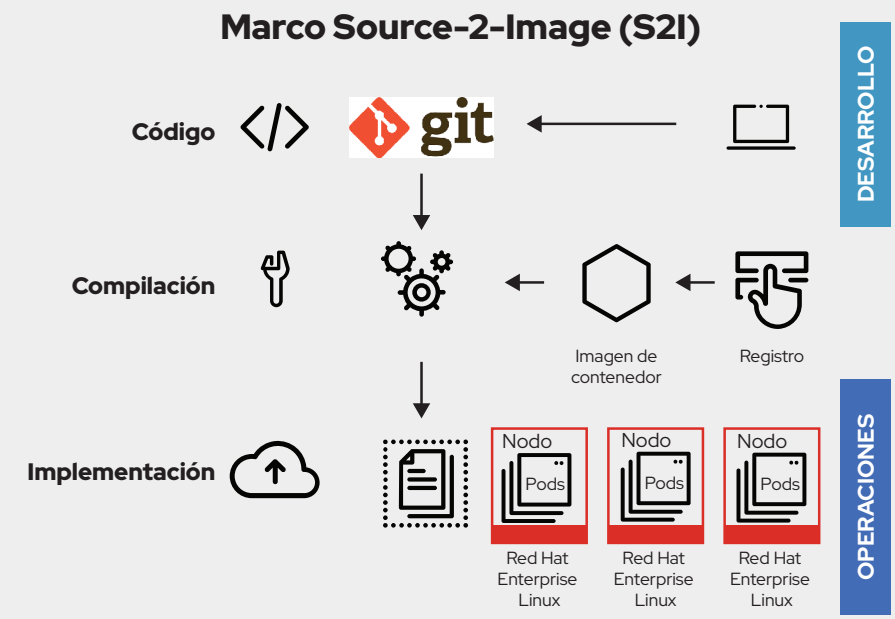


Figura 3. S2I es un kit de herramientas y un flujo de trabajo para diseñar imágenes de contenedores reproducibles y listas para ejecutarse a partir del código fuente.

- Los flujos de imágenes de Red Hat OpenShift pueden utilizarse para ver los cambios realizados en las imágenes externas implementadas en su clúster. Estos trabajan con todos los recursos originales disponibles en Red Hat OpenShift, como las compilaciones y las implementaciones, las tareas, los controladores de replicaciones o los conjuntos de réplicas. Al observar un flujo de imágenes, las compilaciones y las implementaciones pueden recibir notificaciones cuando se agregan nuevas imágenes, o si se modifican, y responder con el lanzamiento automático de una compilación o una implementación, respectivamente.

  Por ejemplo, analicemos una aplicación que está diseñada con tres capas de imágenes de contenedores: la capa base, la capa del middleware y la capa de la aplicación. Si Red Hat encuentra un problema en la imagen de base, se encarga de volver a diseñarla y de cargarla en el repositorio llamado Red Hat Ecosystem Catalog. Si los flujos de imágenes están habilitados, Red Hat OpenShift puede detectar los cambios en la imagen. En el caso de las compilaciones que dependen de esta imagen y que tienen activadores definidos, Red Hat OpenShift volverá a diseñar automáticamente la imagen de la aplicación incorporando la imagen de base fija.

  Una vez que se completa el proceso de compilación, la imagen personalizada que se actualizó se envía al registro interno de Red Hat OpenShift. Red Hat OpenShift detecta de inmediato los cambios en las imágenes de su registro interno y, en el caso de las aplicaciones con activadores definidos, implementa de forma automática la imagen actualizada, lo que garantiza que el código que se está ejecutando en la etapa de producción sea siempre idéntico a la imagen actualizada más recientemente. Todas estas funciones trabajan en conjunto para integrar la seguridad al proceso y al canal de CI/CD.

### 4. Integración de la seguridad al canal de la aplicación

Red Hat OpenShift incluye instancias integradas de Jenkins para la CI y Tekton, un canal de CI/CD de Kubernetes de última generación que funciona para los contenedores (incluso para los que no tienen servidor). Además, incluye API de RESTful sofisticadas que se pueden usar para integrar sus propias herramientas de diseño o de CI/CD, lo que incluye un registro de imágenes privado.

Una de las prácticas recomendadas para la seguridad de las aplicaciones consiste en integrar pruebas de seguridad automatizadas a su canal, incluidos el registro, el entorno de desarrollo integrado (IDE) y las herramientas de CI/CD.

**Registro:** las imágenes de contenedores se pueden y deben analizar en el registro de contenedores privado. Puede utilizar Red Hat Quay junto al escáner de seguridad Clair para informar a los desarrolladores sobre los puntos vulnerables nuevos que se vayan detectando. OpenShift Container Security Operator se integra a Red Hat Quay para proporcionar un panorama completo del clúster con los aspectos vulnerables conocidos de sus imágenes implementadas en la consola de OpenShift. Opcionalmente, el repositorio Red Hat Ecosystem Catalog ofrece varias soluciones externas y certificadas para el análisis de contenedores.

**IDE:** cuando el código se introduce por primera vez en el entorno de desarrollo integrado (IDE), los plugins del IDE de Red Hat Dependency Analytics proporcionan advertencias sobre los puntos vulnerables y consejos en relación con las correcciones de errores para las dependencias del proyecto.

**CI/CD:** las herramientas de análisis se pueden integrar con la CI para realizar un control en tiempo real de los aspectos vulnerables conocidos que catalogan los paquetes open source en su contenedor, notificarlo acerca de cualquier punto vulnerable conocido y brindarle información actualizada en relación con aquellos que se detectaron en paquetes escaneados anteriormente.

Además, el proceso de integración continua debe incluir políticas que indiquen las compilaciones con problemas detectadas por los análisis de seguridad, para que su equipo pueda adoptar las medidas adecuadas y resolver dichos inconvenientes a la brevedad.

Por último, le recomendamos que firme los contenedores diseñados de manera personalizada, para asegurarse de que no sean utilizados de forma indebida entre la etapa de diseño y la de implementación.

## Implementación: gestione la configuración, la seguridad y el cumplimiento de sus implementaciones

Para que la seguridad de sus implementaciones sea efectiva, no solo necesita proteger la plataforma de Kubernetes, sino también automatizar las políticas de implementación. Red Hat OpenShift incluye las siguientes funciones listas para usar:

1. Configuración de la plataforma y gestión del ciclo de vida.
2. Gestión de identidades y accesos.
3. Protección de los datos de la plataforma y del almacenamiento adjunto.
4. Políticas de implementación.

### 5. Configuración de la plataforma y gestión del ciclo de vida

En la auditoría de seguridad de Kubernetes de la fundación Cloud Native Computing Foundation (CNCF), que se publicó en el verano de 2019, se llegó a la conclusión de que la mayor amenaza a la seguridad de Kubernetes radica en lo complejo que resulta configurar y fortalecer sus elementos. Para poder superar este desafío, Red Hat OpenShift utiliza operadores de Kubernetes.

El operador es un método para empaquetar, implementar y gestionar aplicaciones creadas originalmente en Kubernetes. Actúa como un controlador personalizado que puede extender la interfaz de programación de aplicaciones (API) de Kubernetes con la lógica específica de la aplicación que se necesita para gestionarla. Cada elemento de la plataforma de Red Hat OpenShift está empaquetado en un operador y proporciona funciones automatizadas de configuración, supervisión y gestión para OpenShift. Los operadores individuales configuran directamente los elementos como los servidores de la API y la red definida por software (SDN) mientras que el operador de la versión del clúster gestiona varios operadores en toda la plataforma. Estos le permiten automatizar la gestión del clúster, incluidas las actualizaciones, desde el kernel hasta los servicios superiores de la pila.

Una de las características más importantes de las plataformas de contenedores es que permiten que los desarrolladores utilicen funciones de autoservicio, lo cual posibilita que sus equipos de desarrollo distribuyan con mayor rapidez y agilidad las aplicaciones diseñadas en capas aprobadas. Los equipos podrán acceder a un portal de autoservicio, que les brindará el control suficiente para fomentar la colaboración y, a su vez, proporcionar seguridad. La herramienta Operator Lifecycle Manager (OLM) ofrece un marco para que los usuarios del clúster de Red Hat OpenShift encuentren y utilicen los operadores que permiten implementar los servicios necesarios para habilitar sus aplicaciones. Gracias a esta herramienta, los usuarios pueden instalar y actualizar los operadores disponibles, como así también asignarles un control de acceso basado en funciones.

El operador denominado Compliance Operator de Red Hat OpenShift automatiza el cumplimiento de la plataforma con los controles técnicos que exigen los marcos de cumplimiento. Este operador permite que los administradores de Red Hat OpenShift describan el estado de cumplimiento deseado de un clúster, y les proporciona un panorama general de los problemas relacionados y de las formas de corregirlos. Además, evalúa el cumplimiento de todas las capas de la plataforma, incluidos los nodos que ejecutan el clúster. El operador File Integrity Operator también está disponible para realizar periódicamente verificaciones de la integridad de los archivos en los nodos del clúster.

### 6. Gestión de identidades y accesos

La gestión de identidades y el control de acceso basado en funciones (RBAC) son elementos esenciales de la plataforma de contenedores, debido a la gran cantidad de funciones en Kubernetes con las que cuentan los desarrolladores y los administradores. Las API de Kubernetes son clave para automatizar la gestión de los contenedores, según sea necesario. Por ejemplo, las API se utilizan para iniciar y validar las solicitudes, lo cual incluye la configuración y la implementación de pods y servicios.

La autenticación y autorización de la API es fundamental para proteger su plataforma de contenedores. El servidor de la API es un punto central de acceso y debe recibir el mayor nivel de control de seguridad posible. El plano de control de Red Hat OpenShift incluye la autenticación integrada a través del operador Cluster Authentication. Los desarrolladores, los administradores y las cuentas de servicio obtienen tokens de acceso de OAuth para realizar su propia autenticación en la API. Como administrador, puede configurar el proveedor de identidad que desee en el clúster, de manera que los usuarios puedan autenticarse antes de recibir un token. Se admiten nueve proveedores de identidad, entre ellos, los directorios del protocolo ligero de acceso a directorios (LDAP).

El RBAC detallado se habilita de forma predeterminada en Red Hat OpenShift. Los objetos del RBAC determinan si un usuario puede llevar a cabo una acción específica dentro de un clúster. Los administradores pueden usar los enlaces y las funciones del clúster para controlar los niveles de acceso al clúster de OpenShift y a los proyectos dentro de él.

### 7. Protección de los datos de la plataforma

Red Hat OpenShift refuerza Kubernetes de forma predeterminada para proteger los datos en tránsito. También incluye opciones para proteger los datos en reposo.

Para proteger los datos en tránsito de la plataforma, Red Hat OpenShift:

- Cifra los datos en tránsito mediante protocolos http, para que todos los elementos de la plataforma de contenedores se comuniquen entre sí.
- Envía todas las comunicaciones con el plano de control a través de la seguridad de la capa de transporte (TLS).
- Garantiza que el acceso al servidor de la API se base en tokens o en certificados X.509.
- Usa la cuota del proyecto para delimitar el daño que puede ocasionar un token malicioso.
- Configura el etcd con sus propios certificados y autoridad de certificación (CA). (En Kubernetes, el etcd almacena el estado maestro permanente, mientras que el resto de los elementos lo observan para detectar cambios y ajustarse al estado especificado).
- Rota los certificados de la plataforma de forma automática.

Para proteger los datos en reposo de la plataforma, Red Hat OpenShift:

- Cifra de manera opcional el almacén de datos del etcd y los discos de Red Hat Enterprise Linux CoreOS para brindar mayor seguridad.
- Ofrece la preparación de los Estándares Federales de Procesamiento de la Información (FIPS) para Red Hat OpenShift. El FIPS 140-2 es un estándar de seguridad del Gobierno de Estados Unidos que se utiliza para aprobar módulos criptográficos. Cuando se inicia Red Hat Enterprise Linux CoreOS en el modo FIPS, los elementos de la plataforma Red Hat OpenShift llaman a los módulos criptográficos de Red Hat Enterprise Linux.

Los contenedores son útiles para las aplicaciones con y sin estado. Red Hat OpenShift es compatible tanto con el almacenamiento efímero como con el permanente. Uno de los elementos clave para la seguridad de los servicios con estado es la protección del almacenamiento adjunto. Red Hat OpenShift es compatible con varios tipos de almacenamiento, lo que incluye los sistemas de archivos de red (NFS), Amazon Web Services (AWS) Elastic Block Stores (EBS), los discos permanentes de Google Compute Engine (GCE), Azure Disk, iSCSI y Cinder.

Además, Red Hat OpenShift Container Storage es un almacenamiento persistente definido por software que se encuentra integrado a Red Hat OpenShift Container Platform, y optimizado para esta plataforma. OpenShift Container Storage ofrece un almacenamiento permanente y con gran capacidad de expansión para las aplicaciones desarrolladas en la nube que requieren características como el cifrado, la replicación y la disponibilidad en todas las multicloud híbridas.

- Un **volumen permanente (PV)** puede montarse en un host de cualquier manera que sea compatible con el proveedor de recursos. Los proveedores tendrán distintas funciones, y los modos de acceso de cada PV se configuran con los modos específicos compatibles con ese volumen en particular. Por ejemplo, NFS admite múltiples clientes de lectura/escritura, pero un PV específico del NFS podría exportarse en el servidor como de solo lectura. Cada PV tiene su propio conjunto de modos de acceso que describen las funciones de ese volumen permanente específico, como ReadWriteOnce, ReadOnlyMany y ReadWriteMany.
- En el caso del **almacenamiento compartido** (p. ej.: NFS, Ceph y Gluster), la clave está en hacer que el volumen permanente (PV) del almacenamiento compartido registre su ID de grupo (gid) como una anotación en el recurso del PV. Cuando el pod solicite el PV, el gid registrado se añadirá a los grupos complementarios del pod y les dará acceso a los contenidos del almacenamiento compartido.
- En el caso del **almacenamiento en bloques** (p. ej.: EBS, discos permanentes de GCE y iSCSI), las plataformas de contenedores pueden usar las funciones de SELinux para proteger la raíz del volumen montado para los pods sin privilegios, de manera tal que el volumen montado sea propiedad del contenedor con el que está asociado y solo él pueda visualizarlo.

Claro está que usted debe aprovechar las funciones de seguridad disponibles en la solución de almacenamiento que eligió.

### 8. Automatización de la implementación basada en políticas

Un sistema de seguridad sólido incluye políticas automatizadas que se pueden usar para gestionar la implementación de contenedores y clústeres desde el punto de vista de la seguridad.

- Implementación de contenedores basada en políticas

Los clústeres de Red Hat OpenShift se pueden configurar para que permitan o denieguen la extracción de imágenes de registros específicos. En el caso de los clústeres de producción, una de las prácticas recomendadas consiste en permitir que las imágenes se implementen solo desde su registro privado.

El plugin del controlador de admisión Restricciones del contexto de seguridad (SCC) de Red Hat OpenShift define un conjunto de condiciones con las que un pod debe ejecutarse para ser aceptado en el sistema. Las **restricciones del contexto de seguridad** le permiten descartar privilegios de forma predeterminada, lo cual no solo es importante, sino también una de las mejores prácticas recomendadas. Estas restricciones garantizan que, de forma predeterminada, ningún contenedor con privilegios se ejecute en los nodos de trabajo de OpenShift. Desde el principio, se niega el acceso a los identificadores de los procesos y las redes del host.

Los usuarios con los permisos correspondientes pueden ajustar las políticas de SCC predeterminadas para ser más permisivos, si así lo desean.

Red Hat Advanced Cluster Management for Kubernetes ofrece **una gestión avanzada del ciclo de vida de las aplicaciones** mediante estándares abiertos que permiten implementar aplicaciones utilizando políticas de ubicación, las cuales se encuentran integradas a los controles de supervisión y los canales de CI/CD actuales.

- Gestión de varios clústeres basada en políticas

La implementación de varios clústeres puede ser útil para proporcionar la alta disponibilidad de las aplicaciones en todas las zonas de disponibilidad múltiples o para habilitar las funciones de gestión común de las implementaciones o migraciones en diversos proveedores de nube, como Amazon Web Services (AWS), Google Cloud y Microsoft Azure. Cuando gestione varios clústeres, sus herramientas de organización deberán proporcionar la seguridad que usted necesita en las diversas instancias implementadas. Como siempre, la configuración, la autenticación y la autorización son clave, como así también la capacidad para transmitir datos de forma segura a sus aplicaciones, donde sea que se ejecuten, y para gestionar las políticas de las aplicaciones en todos los clústeres. Red Hat Advanced Cluster Management for Kubernetes ofrece:

- **Gestión del ciclo de vida de varios clústeres,** que le permite crear, actualizar y destruir clústeres de Kubernetes de manera confiable y uniforme, según sea necesario.
- **Los riesgos y el cumplimiento del control basados en políticas,** que utilizan políticas para configurar y mantener la consistencia de los controles de seguridad de forma automática, de acuerdo con los estándares empresariales del sector. También puede especificar una política de cumplimiento que se aplique a uno o más clústeres gestionados.

## Proteja las aplicaciones en ejecución

Además de la infraestructura, es fundamental mantener la seguridad de las aplicaciones. Para proteger las aplicaciones en contenedores, se necesita:

1. Aislamiento del contenedor.
2. Aislamiento de la aplicación y la red.
3. Protección del acceso a la aplicación.
4. Capacidad de observación.

### 9. Aislamiento del contenedor

Para aprovechar al máximo la tecnología de empaquetado y organización de los contenedores, el equipo de operaciones necesita poder ejecutarlos en el entorno adecuado: un sistema operativo (OS) que pueda garantizar la seguridad de los contenedores en los límites (proteger el kernel del host de los escapes del contenedor y proteger los contenedores unos de otros).

Los contenedores son procesos de Linux con aislamiento y confinamiento de los recursos, que le permiten ejecutar aplicaciones ubicadas en espacios aislados en el kernel de un host compartido. Su estrategia para proteger los contenedores debe ser la misma que utiliza para proteger cualquier proceso en ejecución en Linux.

En la publicación especial 800-190 del NIST, se recomienda utilizar un sistema operativo optimizado para los contenedores para mayor seguridad. Red Hat Enterprise Linux CoreOS, el sistema operativo de base para Red Hat OpenShift, minimiza el entorno del host y lo ajusta a los contenedores para reducir la superficie de ataque. Red Hat Enterprise Linux CoreOS solo contiene los paquetes que necesita para ejecutar Red Hat OpenShift, y su espacio de usuario es de solo lectura. La plataforma se prueba, versiona y envía junto con Red Hat OpenShift, y se utiliza el clúster para gestionarla. La instalación y las actualizaciones de Red Hat Enterprise Linux CoreOS son automáticas y compatibles con el clúster. Además, admite la infraestructura que usted elija, ya que hereda la mayor parte del ecosistema de Red Hat Enterprise Linux.

Todos los contenedores de Linux que se ejecutan en una plataforma de Red Hat OpenShift están protegidos por potentes funciones de seguridad de Red Hat Enterprise Linux integradas a los nodos de Red Hat OpenShift. Para proteger los contenedores que se ejecutan en Red Hat Enterprise Linux, se utiliza lo siguiente: espacios de nombres de Linux, SELinux, Cgroups, funciones de Linux y modo de computación seguro (seccomp).

- Los espacios de nombres de Linux proporcionan los aspectos básicos del aislamiento de contenedores. Estos hacen que los procesos contenidos en el espacio de nombre parezcan tener su propia instancia de recursos globales. Además, proporcionan la abstracción necesaria para creer que uno ejecuta sus aplicaciones en su propio sistema operativo desde adentro de un contenedor.
- SELinux proporciona una capa adicional de seguridad para mantener los contenedores aislados unos de otros y del host. Permite que los administradores ejecuten los controles de acceso obligatorios (MAC) para cada usuario, aplicación, proceso y archivo. Además, actúa como una pared de ladrillos que impedirá que usted rompa la abstracción del espacio de nombre (ya sea por accidente o a propósito). SELinux disminuye los puntos vulnerables del tiempo de ejecución del contenedor, y las configuraciones adecuadas de SELinux pueden prevenir que los procesos del contenedor abandonen el aislamiento.

- Los Cgroups (grupos de control) delimitan, contabilizan y aíslan el uso de recursos (p. ej.: la CPU, la memoria, la E/S del disco y la red) de un grupo de procesos. Utilice los Cgroups para evitar que los recursos de su contenedor se superpongan con otro contenedor del mismo host. Estos también se pueden usar para controlar los seudodispositivos, los cuales son un vector de ataque conocido.
- Las funciones de Linux se pueden usar para inhabilitar los privilegios en un contenedor. Se trata de distintas unidades de privilegio que se pueden habilitar o deshabilitar de forma independiente. Estas le permiten, por ejemplo, enviar paquetes de protocolo de Internet (IP) sin procesar o realizar enlaces a puertos inferiores al 1024. Al ejecutar contenedores, se pueden dejar de lado varias funciones sin que esto afecte a la gran mayoría de las aplicaciones en contenedores.
- Por último, un perfil de modo de computación seguro (seccomp) se puede asociar con un contenedor para delimitar la cantidad de llamadas disponibles del sistema.

### 10. Aislamiento de la aplicación y de la red

La seguridad multiempresa es fundamental para el uso de Kubernetes en toda la empresa. Este tipo de arquitectura permite que diferentes equipos utilicen el mismo clúster, pero evita el acceso no autorizado a los entornos de los demás. Red Hat OpenShift admite dicha arquitectura a través de una combinación de espacios de nombres del kernel, SELinux, RBAC, espacios de nombres de Kubernetes (proyecto) y políticas de redes.

- **Los proyectos de Red Hat OpenShift** son nombres de espacios de Kubernetes con anotaciones de SELinux que aíslan las aplicaciones en los equipos, los grupos y los departamentos. Las funciones y los enlaces locales sirven para controlar quién tiene acceso a los proyectos individuales.
- **Las restricciones del contexto de seguridad** le permiten descartar privilegios de forma predeterminada, lo cual no solo es importante, sino también una de las mejores prácticas recomendadas. Estas restricciones garantizan que, de forma predeterminada, ningún contenedor con privilegios se ejecute en los nodos de trabajo de OpenShift. Desde el principio, se niega el acceso a los identificadores de los procesos y las redes del host.

La implementación en contenedores de aplicaciones modernas de microservicios implica implementar varios contenedores distribuidos en múltiples nodos. Estos microservicios tienen que detectarse y comunicarse entre ellos. Teniendo en cuenta la defensa de la red, necesita una plataforma de contenedores que le permita tomar un solo clúster y segmentar el tráfico para aislar, dentro de él, los diferentes usuarios, equipos, aplicaciones y entornos. También necesita herramientas para gestionar el acceso externo al clúster y el acceso desde los servicios del clúster a elementos externos. Para lograr el aislamiento de la red, se necesitan las siguientes propiedades clave:

- **Control del tráfico de entrada.** Red Hat OpenShift incluye CoreDNS para proporcionar a los pods un servicio de resolución de nombre. El enrutador de Red Hat OpenShift (HAProxy) respalda las entradas y las rutas para proporcionar acceso externo a los servicios que se ejecutan en el clúster. Ambos admiten las políticas de nuevo cifrado y de acceso directo: el "nuevo cifrado" implica descifrar y volver a cifrar el tráfico HTTP cuando se envía, mientras que el "acceso directo" implica que el tráfico pase de forma directa sin finalizar la seguridad de la capa de transporte (TLS).
- **Espacios de nombres de red.** El primer nivel de defensa de la red proviene de los espacios de nombres de la red. Cada conjunto de contenedores (conocido como "pod") obtiene su propia IP y su propio intervalo de puertos a los cuales enlazarse, lo que posibilita el aislamiento de las redes de los pods en el nodo. Las direcciones IP de los pods son independientes de la red física a la cual están conectados los nodos de Red Hat OpenShift.

- **Políticas de red.** Las redes definidas por software de Red Hat OpenShift utilizan políticas de red para brindar un control detallado de la comunicación entre los pods. El tráfico de red se puede controlar hacia un pod desde cualquier otro pod, en puertos y direcciones específicos. Cuando las políticas de red se configuran en el modo multiempresa, cada proyecto recibe su propia ID de red virtual y, por consiguiente, se aíslan entre sí las redes de los proyectos en el nodo. En el modo multiempresa (predeterminado), los pods que se encuentran en un mismo proyecto pueden comunicarse entre sí, pero los que pertenecen a espacios de nombres diferentes no pueden enviar paquetes a pods o servicios de otros proyectos, ni recibirlos de ellos.
- **Control del tráfico de salida.** Red Hat OpenShift también permite controlar el tráfico de salida de los servicios que se ejecutan en el clúster, ya sea por medio de métodos de enrutamiento o de firewalls. Por ejemplo, puede usar una lista blanca de direcciones IP para proporcionar acceso a una base de datos externa.

### 11. Protección del acceso a la aplicación

La protección de sus aplicaciones comprende la gestión del usuario de la aplicación y la autenticación y autorización de la API.

- **Control del acceso de los usuarios**

La función de inicio de sesión único (SSO) web constituye una parte fundamental de las aplicaciones modernas. Las plataformas de contenedores pueden incluir varios servicios en contenedores que los desarrolladores podrán utilizar a la hora de diseñar sus aplicaciones. El Inicio de sesión único de Red Hat es un lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0 o un servicio de federación, inicio de sesión único web y autenticación de OpenID Connect basado en el proyecto upstream Keycloak totalmente compatible y listo para usarse. El servicio de inicio de sesión único de Red Hat incluye adaptadores de clientes para Red Hat Fuse y Red Hat JBoss Enterprise Application Platform. Además, posibilita la autenticación y el inicio de sesión único web para las aplicaciones Node.js, y se puede integrar a los servicios de directorios de LDAP, lo que incluye Microsoft Active Directory y Red Hat Enterprise Linux Identity Management. El inicio de sesión único de Red Hat también se integra con proveedores de inicio de sesión sociales, como Facebook, Google y Twitter.

- **Control del acceso a las API**

Las API son un elemento fundamental de las aplicaciones compuestas por microservicios. Estas aplicaciones tienen múltiples servicios de API independientes, lo cual lleva a la proliferación de los extremos del servicio que requieren herramientas adicionales para su control. Le recomendamos que utilice una herramienta de gestión de API. Red Hat 3scale API Management le proporciona una variedad de opciones estándar para la autenticación y seguridad de la API, las cuales se pueden usar por separado o combinadas para emitir credenciales y controlar el acceso.

Las funciones de control de acceso disponibles en Red Hat 3scale API Management no se limitan a la seguridad y la autenticación básicas. Los planes de cuentas y aplicaciones le permiten restringir el acceso a extremos, métodos y servicios específicos, y aplicar políticas de acceso a grupos de usuarios. Los planes de aplicaciones le permiten establecer límites de frecuencia para el uso de las API y controlar el flujo de tráfico para los grupos de desarrolladores. Puede establecer límites por períodos para las llamadas entrantes a la API, a fin de proteger la infraestructura y mantener el flujo constante del tráfico. También puede activar de forma automática alertas por uso excesivo de las aplicaciones que alcanzan o exceden los límites de frecuencia, y definir el comportamiento de las aplicaciones que superan estos límites.

- **Protección del tráfico de la aplicación**

En la sección 10 del presente artículo, se explica cómo es posible proteger el tráfico de las aplicaciones con las opciones de entrada y salida del clúster. En el caso de las aplicaciones de microservicios, el tráfico de seguridad entre los servicios del clúster tiene la misma importancia. Se puede usar una red de servicios para proporcionar esta capa de gestión. El término "red de servicios" (service mesh) describe la red de microservicios que conforman las aplicaciones en una arquitectura de microservicios distribuidos, como así también las interacciones entre ellos.

La solución Red Hat OpenShift Service Mesh, la cual se basa en el proyecto open source Istio, agrega una capa transparente sobre las aplicaciones distribuidas actuales, para poder gestionar la comunicación entre los servicios sin que sea necesario realizar cambios en el código del servicio. Red Hat OpenShift Service Mesh utiliza un operador multiempresa para gestionar el ciclo de vida del plano de control, lo cual permite utilizar OpenShift Service Mesh por proyecto. Además, esta solución no necesita recursos de control de acceso basado en funciones que alcancen a los clústeres.

Red Hat OpenShift Service Mesh ofrece funciones de descubrimiento y equilibrio de carga, además de autenticación y cifrado entre servicios, recuperación de fallos, métricas y supervisión, los cuales son clave para la seguridad.

3scale Istio Adapter es un adaptador opcional que le permite etiquetar un servicio que se encuentra ejecutándose dentro de Red Hat OpenShift Service Mesh.

### 12. Capacidad de observación

La capacidad para supervisar y auditar un clúster de Red Hat OpenShift es un aspecto importante que permite proteger al clúster y a sus usuarios contra el uso inapropiado. Red Hat OpenShift incluye funciones integradas de supervisión y auditoría, así como una pila de registro opcional.

Los servicios de OpenShift Container Platform se conectan con la solución integrada de supervisión, la cual está compuesta por Prometheus y su ecosistema. Tiene a su disposición un panel de alertas. Los administradores del clúster pueden habilitar la supervisión para proyectos definidos por el usuario, si así lo desean. Las aplicaciones que se implementan en Red Hat OpenShift pueden configurarse para aprovechar los elementos de supervisión del clúster.

Una de las prácticas recomendadas de seguridad es la auditoría de eventos, la cual, por lo general, se requiere para cumplir con los marcos normativos. La función de auditoría de Red Hat OpenShift se diseñó básicamente utilizando un enfoque en la nube, el cual aporta centralización y resistencia. En Red Hat OpenShift, la auditoría de los hosts y los eventos se encuentra habilitada de forma predeterminada en todos los nodos. Esta solución brinda una flexibilidad increíble para configurar la gestión y el acceso a los datos de las auditorías. Para controlar la cantidad de información que se asienta en los registros de auditoría del servidor de la API, debe elegir el perfil de política de registro de auditoría que desea utilizar.

Las funciones de supervisión, auditoría y registro de datos están protegidas por el control de acceso basado en funciones. Los administradores de proyectos tienen a su disposición los datos del proyecto y los administradores de clústeres pueden acceder a los datos del clúster.

Como práctica recomendada, configure su clúster para que envíe todos los eventos de auditoría y registro a un sistema de gestión de eventos e información de seguridad (SIEM) para el análisis, la conservación y la gestión de la integridad. Los administradores pueden implementar el registro de clústeres para agregar todos los registros del clúster de Red Hat OpenShift, como los de auditoría del host y de la API, los de infraestructura y los de contenedores de aplicaciones. Los registros del clúster agregan estos registros desde todos los nodos del clúster y los guarda en un almacén predeterminado. Hay varias opciones disponibles que le permiten enviar los registros al SIEM que usted elija.

## Ampliación de la seguridad con un ecosistema sólido

Si desea mejorar aún más la seguridad de sus contenedores y de Kubernetes, o cumplir con las políticas actuales, puede optar por la integración con las herramientas de seguridad de terceros. Red Hat cuenta con un amplio ecosistema de partners certificados que ofrecen soluciones como:

- Gestión de acceso con privilegios.
- Autoridades de certificación externas.
- Soluciones de gestión de claves y almacenamientos externos.
- Herramientas de gestión de puntos vulnerables y de análisis del contenido de los contenedores.
- Herramientas de análisis del tiempo de ejecución de los contenedores.
- SIEM.

## Conclusión

Cuando implementamos aplicaciones y microservicios basados en contenedores, no solo debemos tener en cuenta la seguridad. Su plataforma de contenedores debe ofrecer una experiencia que funcione tanto para los desarrolladores como para el equipo de operaciones. Necesita una plataforma de aplicaciones basada en contenedores, centrada en la seguridad y de nivel empresarial que potencie la capacidad de los desarrolladores y los operadores, sin comprometer las funciones que necesita cada equipo, y que también mejore la eficiencia operativa y el uso de la infraestructura.

Red Hat OpenShift se basa en un núcleo de contenedores de Linux estándar y portátiles que ofrecen funciones de seguridad integradas, lo que incluye:

- Herramientas integradas de CI/CD y diseño para prácticas DevOps seguras.
- Una plataforma de Kubernetes reforzada y lista para la empresa con funciones integradas de gestión del ciclo de vida, cumplimiento y configuración.
- RBAC sólidos con integraciones a los sistemas de autenticación de la empresa.
- Opciones para la gestión de la entrada y salida del clúster.
- Red de servicios y SDN integradas con soporte para la microsegmentación de la red.
- Soporte para proteger los volúmenes de almacenamiento remoto.
- Red Hat Enterprise Linux CoreOS, con la capacidad para ejecutarse en contenedores según sea necesario y con aislamiento sólido.
- Políticas de implementación para automatizar la seguridad del tiempo de ejecución.
- Funciones integradas de supervisión, auditoria y registro.

Red Hat OpenShift proporciona también la mayor colección de marcos, servicios y lenguajes de programación compatibles (Figura 4). Red Hat Advanced Cluster Management for Kubernetes ofrece la gestión integrada de varios clústeres.

Red Hat OpenShift se puede ejecutar en OpenStack, VMware, equipos sin sistema operativo, AWS, Google Cloud Platform (GCP), Azure, IBM Cloud y cualquier plataforma que admita Red Hat Enterprise Linux. Además, Red Hat ofrece Red Hat OpenShift Dedicated para AWS y GCP como servicio de nube pública. Red Hat y Microsoft ofrecen en conjunto Azure Red Hat OpenShift. Red Hat y Amazon ofrecen en conjunto Red Hat OpenShift Service on AWS.

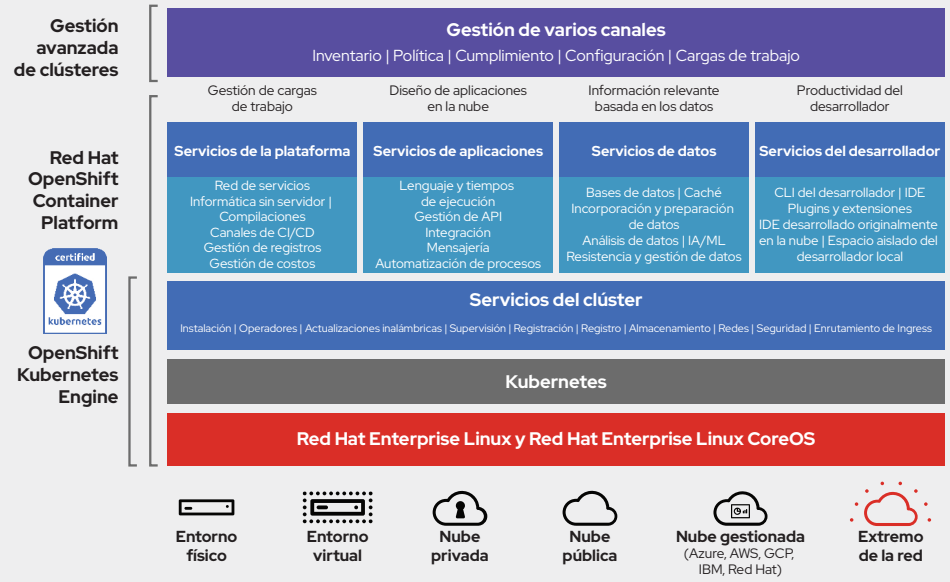


Figura 4. Red Hat OpenShift proporciona una pila de tecnología con todas las funciones en entornos físicos, virtuales, de nube pública y de nube privada.

Red Hat, como el proveedor líder de soluciones open source confiables para clientes empresariales durante casi dos décadas, ofrece el mismo nivel de confianza y seguridad para los contenedores mediante soluciones como Red Hat OpenShift Container Platform, Red Hat Advanced Cluster Management for Kubernetes y nuestra cartera de productos de Red Hat habilitados para contenedores.

## ACERCA DE RED HAT

Red Hat es el proveedor líder de soluciones de software de open source para empresas, que adopta un enfoque basado en la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Red Hat ayuda a los clientes a integrar aplicaciones de TI nuevas y existentes, desarrollar aplicaciones nativas de la nube, estandarizar en nuestro sistema operativo líder del sector y automatizar, proteger y gestionar entornos complejos. Sus servicios galardonados de soporte, capacitación y consultoría convierten a Red Hat en un asesor de confianza para las empresas de Fortune 500. Como partner estratégico de proveedores de nube, integradores de sistemas, proveedores de aplicaciones, clientes y comunidades de open source, Red Hat puede ayudar a las organizaciones a prepararse para el futuro digital.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

**ARGENTINA**
+54 11 4329 7300

**CHILE**
+562 2597 7000

**COLOMBIA**
+571 508 8631
+52 55 8851 6400

**MÉXICO**
+52 55 8851 6400

**ESPAÑA**
+34 914 148 800

**es.redhat.com**
**#F26463_1220**