

Optimización de la tecnología 5G con los contenedores en equipos sin sistema operativo

¿Por qué los proveedores de servicios de comunicación eligen esta arquitectura?

Tom Conklin, Ventas
para el extremo de la red,
América del Norte, Red Hat

Sanjay Aiyagari, Arquitecto
principal de soluciones, Red Hat

"Es posible mejorar la competitividad en el mercado si se avanza hacia la implementación de los contenedores en equipos sin sistema operativo, para prestar un servicio mejor y más innovador. El proceso consiste en pasar de las máquinas virtuales a los contenedores. Esto le permite incluir más aplicaciones en una infraestructura menor para reducir los costos, implementar los servicios en segundos y mantener el nivel de seguridad que requieren los clientes."

Anoop Agrawal

Director de ingeniería de
productos para MEC y SDN,
Verizon

Los proveedores de servicios de comunicación deben modificar su enfoque si quieren obtener los mismos beneficios relacionados con la escala que los proveedores de nube globales. La igualdad de rendimiento, eficiencia y agilidad se obtiene con la evolución de las máquinas virtuales (VM) en contenedores.

Sumario ejecutivo

La segunda ola de migraciones de las redes de telecomunicación a la nube está en curso. La primera, la virtualización de las funciones de red (NFV), disminuyó los costos gracias a que los elementos de red que anteriormente se basaban en los dispositivos se transfirieron al software, sin sacrificar la necesidad heredada de los gestores de elementos. Hoy en día, los proveedores de servicios de comunicación (CSP) están adoptando las arquitecturas y los contenedores creados en la nube para incrementar la eficiencia, el rendimiento, la resistencia, la seguridad y la agilidad. La arquitectura que prefieren ofrece ventajas considerables para sus casos de uso específicos y consiste en la implementación de los contenedores en equipos sin sistema operativo y sin una capa adicional de virtualización.

Este whitepaper destaca las ventajas de implementar los servicios 5G usando los contenedores en servidores sin sistema operativo, en lugar de hacerlo en máquinas virtuales (VM).

Contexto

A medida que las funciones de red comenzaron a trasladarse a la nube, algunos visionarios de los grandes CSP buscaron pasar directamente a los contenedores y dejar de implementar las funciones de red en máquinas virtuales. Red Hat también fue uno de los primeros partidarios de esta idea, ya que había notado el valor de Kubernetes cuando hacía grandes contribuciones a sus primeros lanzamientos. Sin embargo, el impulso del sector y algunas limitaciones de los contenedores para las redes de telecomunicaciones en aquel momento hicieron que [OpenStack®](#) y las máquinas virtuales se establecieran como la base de ese cambio. La mayoría de los CSP implementaron con éxito las funciones de red virtual (VNF) según la arquitectura de NFV del Instituto Europeo de Normas de Telecomunicaciones (ETSI) para prestar servicios en la actualidad. Las máquinas virtuales que ejecutan aplicaciones heredadas estarán en la red y en el espacio de TI de los CSP en el futuro inmediato. Sin embargo, la mayoría de las aplicaciones y los elementos 5G nuevos se implementarán usando los contenedores.

Actualmente, hay grandes cambios tecnológicos en curso. Las aplicaciones heredadas se están trasladando del antiguo diseño monolítico que mejor se adapta a las máquinas virtuales a los [microservicios](#). La metodología ágil y DevOps son las prácticas recomendadas para desarrollar y gestionar las aplicaciones hoy en día, y funcionan mejor cuando estas se diseñan utilizando elementos más pequeños e independientes. Con este enfoque, se puede desarrollar e implementar las funciones y las correcciones para cada componente de forma constante, sin afectar al resto de la aplicación. A veces, los CSP y sus proveedores necesitan la integración y distribución continuas (CI/CD) para admitir varios parches y actualizaciones cada año. Gracias al desarrollo ágil, pueden ofrecer un respaldo muchísimo mejor.

El listado de requisitos que originó la adopción de las máquinas virtuales ha disminuido con el paso del tiempo. Por ejemplo, una de las ventajas de utilizarlas era su compatibilidad con varios sistemas operativos guest. Hoy, este nivel de complejidad es innecesario. Linux® es el sistema operativo estándar para las aplicaciones de red. Además, si una nube es compatible con varios sistemas operativos, es más difícil reducir los aspectos vulnerables de la seguridad a medida que se descubren. Asimismo, ahora las funciones y las aplicaciones de red no suelen tener estado, así que no dependen tanto de su afinidad con el almacenamiento de red.

Hasta un 44 % de reducción del costo total de propiedad (TCO)¹

La investigación realizada por Red Hat y ACG demuestra que el TCO de una implementación 5G se puede reducir hasta un 44 % si se implementa una RAN virtualizada abierta en vez de tecnologías de RAN diseñadas con fines específicos. Esto motiva a los CSP para que adopten las tecnologías 5G en sus implementaciones.

En el futuro inmediato, las máquinas virtuales existirán en la red para las funciones actuales, pero la implementación de funciones nuevas en contenedores, incluido el núcleo de la 5G y la RAN, ofrece una ventaja muy importante.

Uno de los cambios que más se destaca en el mundo de las telecomunicaciones es la evolución a la tecnología 5G, tanto la red de acceso por radio (RAN) como el núcleo². Con ella, el CSP puede distribuir las funciones de red en las ubicaciones físicas que más le convengan al cliente y a la empresa. Ahora es posible distribuir las funciones de voz y del núcleo del paquete en las nubes públicas, los centros de datos centralizados o regionales, e incluso en las instalaciones del cliente. La RAN también está evolucionando gracias a la colaboración y la estandarización dentro de OpenRAN (O-RAN) Alliance y el proyecto OpenRAN, para respaldar las funciones que se alojan en los servidores comerciales listos para usarse, en vez de hospedarlas en el hardware propietario. Los elementos pueden encontrarse en diferentes lugares geográficos, pueden proporcionarlos varios proveedores, y pueden utilizar una infraestructura compartida entre los que componen el núcleo de las telecomunicaciones y las aplicaciones de valor agregado para los usuarios finales.

Los contenedores son ideales para estas mejoras, y su implementación en equipos sin sistema operativo ofrece grandes beneficios a los CSP. Respecto a las aplicaciones heredadas, puede que haya motivos para implementarlas en máquinas virtuales, pero para la tecnología 5G, estas últimas implican una segunda capa de complejidad, lo cual es innecesario e incluso contraproducente.

Eficiencia operativa

El aumento de la eficiencia es una de las principales ventajas de virtualizar una red de telecomunicaciones. Antes, cada servicio que se ofrecía a los clientes contaba con su propio segmento de tecnología, y lo mantenían distintos grupos que gestionaban capas individuales de tecnología, además de las operaciones de red y el soporte al cliente. Estas múltiples capas de organización desaparecen al colocar las diferentes funciones de red que conforman los servicios en la misma infraestructura de nube.

El paso de las máquinas virtuales a los contenedores no debe ser contraproducente para la eficiencia. Sin embargo, OpenStack y Kubernetes son dos áreas de especialización diferentes, y la implementación de los contenedores en máquinas virtuales agrega una capa de recursos a las arquitecturas NFV actuales, en lugar de simplemente reemplazarla. La complejidad aumenta notablemente cuando se expande el footprint de la red para incluir recursos de la nube pública y cientos de sitios remotos del extremo de la red. Kubernetes se ocupa de abordar dicha complejidad en los contenedores, ya que si se mantienen las máquinas virtuales en este entorno, se genera ineficiencia operativa y dificultades innecesarias. Los contenedores implementados en equipos sin sistema operativo son compatibles con todas las variantes de nube, pero las máquinas virtuales y las diversas plataformas que los admiten no. Como resultado, se necesita más personal para brindar soporte a las plataformas que reúnen máquinas virtuales y contenedores, y se requieren aún más especialistas para respaldar plataformas diferentes para las nubes públicas y privadas. Lo ideal sería usar una sola plataforma de organización en contenedores para ambos tipos de nube.

La adopción de funciones de red creadas en la nube (CNF) separadas puede representar una dificultad administrativa para la gestión y la garantía del ciclo de vida. Los microservicios que componen una aplicación no necesariamente están asociados físicamente entre sí en el mismo servidor ni en la misma ubicación. La gestión del ciclo de vida es más compleja sin una automatización considerable. Para aumentar la eficiencia, los CSP y los proveedores emplean cadenas de herramientas de DevOps, la metodología de CI/CD y, actualmente, la garantía de bucle cerrado. Sin embargo, la automatización requiere habilidades específicas que, además de ser costosas, escasean. Es importante que el CSP solicite un canal de CI/CD común para todos los proveedores siempre que sea posible.

Las actualizaciones y los parches se deben distribuir, probar e implementar de forma automática y uniforme. Cualquier complejidad adicional en la red provocará que se necesite más personal que escriba y actualice los recursos de automatización, y que las funciones que no pueden automatizarse se mantengan de forma manual. Esto presenta un obstáculo para los CSP al momento de intentar reducir los costos para mantener la competitividad y cumplir con las demandas de los clientes.

¹ ACG Research. "Ventajas económicas de la virtualización de la RAN en las infraestructuras de operadores móviles", patrocinado por Red Hat. Septiembre de 2019.

² 5G Americas. "5G and the cloud", diciembre de 2019.

Agilidad del servicio

Con la NFV, los CSP obtuvieron agilidad en el servicio y ahora pueden implementar y eliminar los servicios mucho más rápido que antes³. Asimismo, con la adopción de la tecnología 5G, pretenden abrir sus redes para que los terceros soliciten y preparen segmentos de sus redes para las aplicaciones integrales especializadas. Este tipo de servicio se publicará a través de las interfaces de programación de aplicaciones (API) norte, que permiten controlar el acceso de los terceros a los recursos de red. La velocidad a la que se ponen a disposición los servicios es fundamental para que los clientes se sientan satisfechos. Las máquinas virtuales demoran mucho más que los contenedores para ponerse en marcha. Si el cliente solicita un segmento con dos clics, probablemente deba esperar varias horas mientras se crea una instancia de este en forma de varias máquinas virtuales en diferentes ubicaciones de la red. Sin embargo, esta experiencia mejora con la implementación casi instantánea de un servicio basado en contenedores.

De cara al futuro, la velocidad de los contenedores en los equipos sin sistema operativo también posibilita la prestación de un servicio diferenciado en el extremo de la red. Un usuario final puede solicitar un servicio de valor agregado y hacer que se implemente en un nodo del extremo cercano según lo requiera. No es necesario que las cargas de trabajo residan de forma permanente en este tipo de nodos, así que quedan libres para alojar solo las aplicaciones más solicitadas. Por ejemplo, un suscriptor móvil que utiliza una aplicación de comunicación ultraconfiable y de baja latencia (URLLC) con gran ancho de banda y habilitada por 5G puede hacer que esta lo siga a medida que cambia su cercanía a los sitios del extremo de la red. Cuando se acercan a ellos, se crean instancias de las aplicaciones en segundos. Si los contenedores se implementan en máquinas virtuales, no se puede obtener este beneficio, ya que los recursos para todas las aplicaciones posibles deberían reservarse en el extremo de la red. Asimismo, se tendrían que crear instancias de las máquinas virtuales según se solicite, lo cual llevaría una cantidad de tiempo inadmisibles.

La agilidad del servicio con los contenedores ayuda a generar ganancias y libera los recursos que utilizaban los servicios eliminados con mayor rapidez. También permite que el CSP asuma ciertos riesgos para volverse más competitivo⁴. Estas ventajas se pueden aprovechar mejor cuando los contenedores se implementan en equipos sin sistema operativo.

Rendimiento

En las redes de telecomunicación, al igual que en la naturaleza, la evolución debe brindar beneficios. Debe resolver problemas, hacer que las empresas sean más competitivas y mejorar las oportunidades de continuidad. Por lo general, no se adoptan los cambios que aumentan los costos y disminuyen el rendimiento. Las redes de telecomunicación poseen requisitos de rendimiento específicos que hacen que la implementación de los contenedores en las máquinas virtuales implique un retroceso.

Con la NFV, uno de los mayores obstáculos para las aplicaciones con núcleo móvil y un subsistema multimedia de protocolo de Internet (IMS) era la tasa de interrupción que generaban las máquinas virtuales. Inicialmente, esto podía generar un deterioro de hasta el 20 % del rendimiento normal del servidor⁵, lo cual podía inhabilitar la virtualización de ciertas aplicaciones para los CSP que necesitaban un mayor rendimiento. Sin embargo, este ha mejorado notablemente gracias a que se ha centrado en la arquitectura y a los avances en la aceleración del hardware, como la virtualización de entrada y salida de raíz única (SR-IOV) y el kit de desarrollo de plano de datos (DPDK). La combinación de los contenedores y las máquinas virtuales vuelve a dificultar la tasa de interrupción. Si bien ya no genera una latencia informática considerable, la sobrecarga adicional de las máquinas virtuales reduce el rendimiento de entrada y salida (E/S) del nodo, en comparación con los contenedores implementados en equipos sin sistema operativo. Esta reducción es mucho mayor con las transacciones de E/S pequeñas que con las grandes. El tráfico de datos y de voz en una red de telecomunicaciones a veces está bastante fragmentado y consta de pequeñas transacciones.

³ Estudio de caso de Red Hat. "[Turkcell crea una nube unificada de telecomunicaciones utilizando la NFV de Red Hat OpenStack](#)", abril de 2020.

⁴ Esfandiari, Shirin. "[Bringing 5G-enabled services to life calls for cloud-native operations](#)". DevOps.com, 20 de agosto de 2019.

⁵ Liu, Ming, et al. "[Understanding the virtualization "Tax" of scale-out pass-through GPUs in GaaS clouds: An empirical study](#)". IEEE.org, febrero de 2015.

Hoy en día, las funciones de red con un uso intensivo de E/S son las que necesitan el mejor rendimiento, en vez de las que hacen un uso intensivo de la unidad central de procesamiento (CPU). Además, su rendimiento se puede ver afectado en gran medida si se implementan usando los contenedores en máquinas virtuales. El impacto puede llegar a ser hasta del 30 %, lo cual implica que más contenedores realicen el mismo trabajo⁶. Una mayor cantidad de ellos en las máquinas virtuales se traduce en más servidores y mayores costos.

Ventajas de la infraestructura

Antes de la NFV, el uso del hardware de red solía ser muy bajo en una carga normal. Estos sistemas eran redundantes y generaban un costo adicional. Las piezas de repuesto se almacenaban en las cercanías y aumentaban aún más los gastos. Se adaptó la capacidad para responder en los periodos de mayor actividad, y los costos diarios se mantuvieron iguales, independientemente de los días sumamente rentables o de menor demanda, en que disminuía su rentabilidad.

En teoría, la virtualización de varias VNF en la misma infraestructura mejoraría el uso de forma considerable. La adopción de una organización avanzada para la gestión del ciclo de vida podría eliminar la necesidad de repuestos y hardware redundante. La nube ofrecería una capacidad común para que todas las VNF se expandieran o se adaptaran a ella. Sin embargo, en la práctica, las VNF en ocasiones se han implementado en diferentes segmentos de hardware específicos de los proveedores. La separación era necesaria porque los CSP necesitaban que los proveedores mantuvieran el mismo rendimiento y tiempo de actividad para sus productos que el hardware heredado. Los segmentos todavía se diseñaban para admitir la capacidad máxima, ya que no se agrupaban los recursos de la nube para respaldar la disponibilidad del 99,999 % que necesitaban los CSP. Y, por lo general, se seguían implementando segmentos de hardware redundante para las aplicaciones que necesitaban alta disponibilidad. No siempre se lograba conseguir el aumento de la utilización prometido. Como resultado, solía haber varios gestores de la infraestructura virtual (VIM) de diferentes proveedores administrando las máquinas virtuales en distintos segmentos de tecnología dentro de la misma red.

Generalmente, los elementos del núcleo 5G y de la RAN se diseñan como funciones creadas en la nube que se ejecutan en los contenedores, debido a los métodos modernos de desarrollo de software y gestión del ciclo de vida. La arquitectura especificada por la 3rd Generation Partnership Project (3GPP) permite separar aún más las funciones que solían ser monolíticas en microservicios de diferentes proveedores y proyectos open source. Los CSP esperan que los proveedores compartan la infraestructura de nube, y las arquitecturas de software creadas en la nube permiten una coexistencia más aceptable de las soluciones de los proveedores, en comparación con lo que sucedió con la NFV y otras aplicaciones monolíticas comunes.

Los contenedores son excelentes para empaquetar los microservicios, y Kubernetes organiza las aplicaciones que forman estos últimos. Si los contenedores se implementan dentro de máquinas virtuales, los recursos para el almacenamiento, la informática y la memoria se utilizan para cada sistema operativo guest. Esos recursos se reservan sin conocer las necesidades de los contenedores que se implementarán eventualmente en cada máquina virtual. Por lo tanto, la utilización se mantiene baja, de forma similar a las redes heredadas. Los recursos se reservan para los periodos de mayor actividad, para que puedan respaldar un complemento entero de contenedores, pero la demanda no siempre coincide con los recursos reservados. Como sucede con las redes heredadas, cuando se adaptan las dimensiones de la máquina virtual para responder a los picos de tráfico, el uso normal de sus recursos es cercano al 20 %⁷. En el caso de los contenedores en equipos sin sistema operativo, los recursos no se reservan de la misma forma y se puede utilizar apenas un 20 % como contenedores en máquinas virtuales. Por ello, es posible incluir más contenedores en un servidor. En el caso de las máquinas virtuales, la baja utilización y la menor densidad de contenedores dan lugar a mayores gastos operativos y de capital, que resultan de la compra y la gestión de hardware adicional.

La optimización de los recursos es fundamental para las aplicaciones en el extremo de la red habilitadas por 5G. Entre ellos se encuentra la red, la RAN y las cargas de trabajo de aplicaciones empresariales implementadas cerca del cliente, para que se beneficie de la baja latencia y del ancho de banda previsible. Varios sitios del extremo de la red tienen limitaciones de espacio o del entorno, así que no hay lugar para hardware adicional.

⁶ Lettieri, Guiseppe, et al. "A study of I/O performance of virtual machines". The British Computer Society, vol. 61 N.º 6, 2018.

⁷ Liu, Ming, et al. "Understanding the virtualization "Tax" of scale-out pass-through GPUs in GaaS clouds: An empirical study". IEEE.org, febrero de 2015.

Asimismo, la cantidad de sitios genera una limitación de costos para cada uno de ellos y puede restringirlos a un solo servidor, ya que el valor total puede aumentar de forma descontrolada con rapidez. Por cada servidor del extremo de la red, las máquinas virtuales suman el elevado costo de todos los sistemas operativos guest al del host, que es el único necesario para los contenedores implementados en equipos sin sistema operativo. Esta última opción permite una mayor cantidad de tráfico y servicios de forma más eficiente, para aumentar los márgenes de ingresos y ganancias.

Seguridad

Una de las grandes ventajas para el CSP que implementa redes 5G y en el extremo de la red es la seguridad mejorada cuando se utilizan los contenedores en equipos sin sistema operativo. Con las redes 4G/LTE y NFV, los CSP implementaban y gestionaban relativamente pocos sitios de nube privada. La tecnología 5G brinda la posibilidad de tener arquitecturas más distribuidas, incluidas múltiples nubes públicas y quizás miles de pequeñas instancias de nube cercanas a las instalaciones de los clientes o incluso en ellas. Además, las aplicaciones que les ofrecen servicios de valor agregado pueden compartir las mismas instancias de nube con las funciones esenciales de la red. La combinación de la escalabilidad y la arquitectura multiempresa merece un análisis de seguridad. Existe un concepto erróneo generalizado que dice que las máquinas virtuales son necesarias para garantizar que una aplicación en contenedores no utilice los recursos que necesita otra. Otro concepto erróneo es que ofrecen un aislamiento seguro para las cargas de trabajo de distintos usuarios. En realidad, la seguridad forma parte de las funciones del sistema operativo (Linux), no del organizador (Kubernetes).

Cada máquina virtual se aísla en un nodo de la nube para que las cargas de trabajo dejen de ocupar los recursos de las otras. Cuando se utilizan para la NFV y las aplicaciones monolíticas, se configuran según los requisitos de las aplicaciones que se están ejecutando en ellas. Los contenedores implementados en máquinas virtuales pueden robarse los recursos de la misma forma que podrían hacerlo en los equipos sin sistema operativo si no se les controla de forma correcta. El aislamiento de las cargas de trabajo de los usuarios en máquinas virtuales diferentes también puede ocasionar que se reduzca su utilización. La solución frente a estos desafíos es Security-Enhanced Linux (SELinux), un elemento que forma parte de varias distribuciones de Linux. Se trata del módulo de seguridad del kernel que en principio diseñó la Agencia de Seguridad Nacional (NSA) de Estados Unidos, el cual permite que los administradores controlen las autorizaciones detalladas de acceso a los elementos del sistema operativo y el nodo. Las políticas de seguridad se establecen en el nodo, y luego, cada contenedor implementado en él adopta una política que protege sus propios intereses. Se debe activar SELinux en el sistema operativo guest para que brinde seguridad, incluso si los contenedores se encuentran en máquinas virtuales. No obstante, estas no son necesarias para protegerlos y solo se protegen de las demás máquinas virtuales. La implementación de una capa de estos sistemas puede tener un impacto negativo en la seguridad de la red de los CSP, dado que dificulta el cumplimiento.

Otro aspecto clave de la seguridad es el cumplimiento de las políticas de seguridad establecidas por el CSP, los usuarios de la red y los organismos reguladores. Para eliminar los posibles puntos vulnerables que encuentran los proveedores, las comunidades open source o el resto del sector, se deben supervisar y actualizar de forma constante el hardware, los sistemas operativos, los gestores de la infraestructura virtual, las aplicaciones, los scripts de automatización y otros elementos. A modo de ejemplo, suponga que opera una red 5G desde hace cinco años. Llegado ese momento, en la red habrá varias generaciones y, probablemente, varios proveedores de todos los elementos. Es necesario automatizar la ejecución constante de parches y la reparación habitual de desajustes respecto de las expectativas de seguridad. Como las máquinas virtuales agregan un sistema operativo guest que requiere mantenimiento, el cumplir con las normativas es mucho más complicado.

Es probable que algunos contenedores admitan servicios con acuerdos de nivel de servicio (SLA) específicos para la seguridad. La abstracción del hardware físico del contenedor en la forma de una máquina virtual dificulta la uniformidad de la seguridad y el rendimiento. Kubernetes no sabe en qué nodo específico de la nube se coloca un contenedor. Si no se puede asociar el hardware con el sistema operativo host para todos los contenedores, no se puede garantizar la seguridad de una carga de trabajo sujeta al cumplimiento de las normativas comerciales (por ejemplo, en el sector de las tarjetas de pago) o de la salud (por ejemplo, HIPAA). Es más sencillo configurar el cumplimiento de la seguridad y mantenerlo cuando los contenedores están implementados en equipos sin sistema operativo.

Conclusión

Las redes 4G/LTE y NFV necesitaban una cantidad relativamente pequeña de instancias de la nube privada para respaldar una red grande de telecomunicación. En la actualidad, la tecnología 5G trae un gran cambio. El CSP que desee beneficiarse de las funciones nuevas de estas redes, como la latencia baja y previsible, el gran ancho de banda y la arquitectura distribuida, podrá tener éxito de forma más sencilla si las implementa en contenedores que se ejecuten en equipos sin sistema operativo. Puede reducir los gastos de capital (CapEx) y operativos (OpEx), ser más ágil y competitivo, mejorar el rendimiento con un footprint más pequeño y ofrecer mayor seguridad de la red.

Gracias a que hay comunidades enteras centradas en encontrar soluciones para los desafíos del futuro, la tecnología de open source ofrece la ventaja de generar innovaciones y resolver los problemas con mayor rapidez. La elección de este tipo de tecnología implica que los CSP no dependen de un proveedor específico. Red Hat ofrece distribuciones sofisticadas de proyectos open source con funciones de valor agregado que permiten mejorar el uso y automatizar las tareas administrativas. Los CSP pueden diseñar sus redes 5G con las siguientes soluciones:

- [Red Hat® OpenShift®](#)
- [Red Hat Ansible® Automation Platform](#)
- [Red Hat AMQ](#)
- [Red Hat 3Scale API Management](#)
- [Compilación Quarkus de Red Hat](#), un tiempo de ejecución Java™ creado en Kubernetes

Red Hat ha ayudado a muchos CSP en todo el mundo a transformar sus redes en NFV. Como uno de los principales colaboradores de OpenStack, Kubernetes y muchos otros proyectos open source, contamos con amplia experiencia en la evolución de las arquitecturas de red de telecomunicaciones a servicios creados en la nube. Además, las funciones de red certificadas que ofrecen los partners del ecosistema de Red Hat le brindan opciones para que realice implementaciones con confianza. Obtenga más información sobre las [soluciones de telecomunicaciones de Red Hat](#).

Acerca de Red Hat

Red Hat es el proveedor líder mundial de soluciones de software open source para empresas, que ha adoptado un enfoque impulsado por 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 las aplicaciones de TI nuevas y actuales; desarrollar aplicaciones nativas de la nube; estandarizar nuestro sistema operativo líder del sector; y automatizar, proteger y gestionar entornos complejos. Sus servicios galardonados de asistencia, capacitación y consultoría convierten a Red Hat en asesor de confianza para las empresas de la lista Fortune 500. Como partner estratégico de proveedores de nube, integradores de sistemas, proveedores de aplicaciones, clientes y comunidades open source, Red Hat ayuda a las empresas a prepararse para el futuro del mundo digital.

Copyright© 2020 Red Hat, Inc. Red Hat, el logotipo de Red Hat, Ansible y OpenShift son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus filiales en Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en Estados Unidos y en otros países.

La marca denominativa de OpenStack y el logotipo de Square O Design, ya sea juntos o separados, son marcas comerciales o marcas comerciales registradas de OpenStack Foundation en Estados Unidos y en otros países, y se utilizan con el permiso de OpenStack Foundation. Red Hat, Inc. no está afiliada a OpenStack Foundation ni a la comunidad de OpenStack, y tampoco goza de su respaldo ni de su patrocinio. Java y todas las marcas comerciales y los logotipos que se basan en Java son marcas comerciales o marcas comerciales registradas de Oracle America, Inc. en Estados Unidos y en otros países.

Los CSP colaboran con Red Hat para ejecutar las funciones de red creadas en la nube en equipos sin sistema operativo, para obtener el mayor beneficio de sus implementaciones 5G.

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



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