
Las razones por las que su sistema operativo sigue siendo importante

Las ocho formas en las que Linux respalda los objetivos empresariales y de TI modernos



Índice

1

Su sistema operativo es esencial en la TI moderna

2

Ocho razones por las que su sistema operativo sigue siendo importante

3

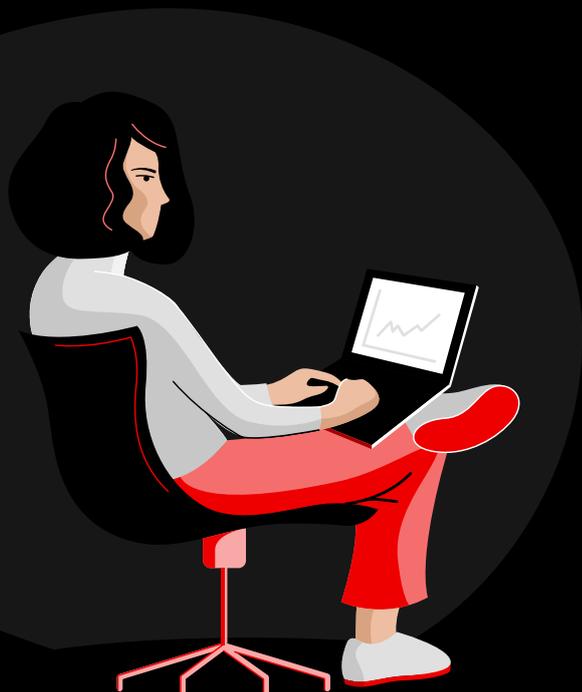
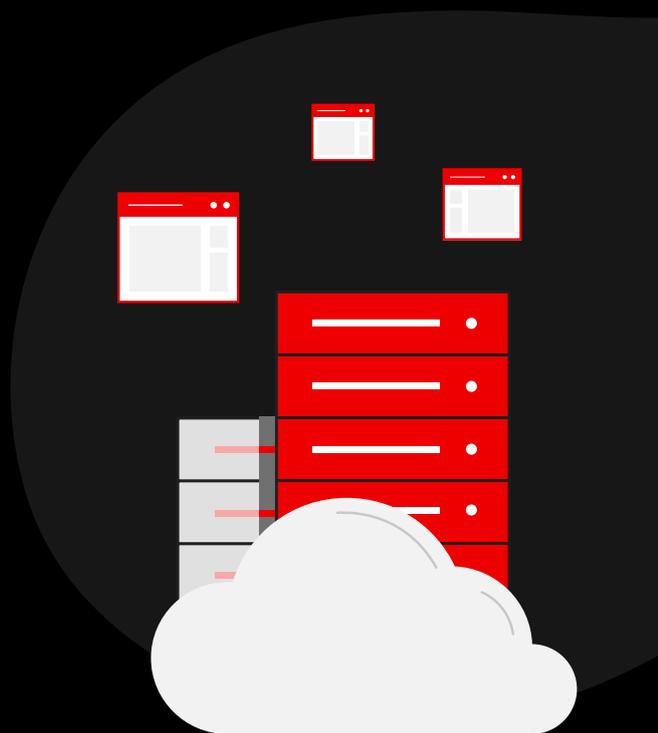
Aproveche el software open source

4

Simplifique la gestión del sistema operativo

5

Red Hat Enterprise Linux: un punto de partida para la TI moderna



Su sistema operativo es esencial en la TI moderna

Los sistemas operativos son esenciales para los entornos de TI desde que se desarrollaron,

en la década de los 50, y no han cesado de evolucionar para satisfacer las necesidades cambiantes de los consumidores. Los primeros sistemas operativos se centraban principalmente en el procesamiento por lotes y la programación sencilla de tareas, y ejecutaban una labor a la vez. La aparición de los sistemas de tiempo compartido, en los 60, permitió que varios usuarios interactuaran simultáneamente con una computadora. En consecuencia, las décadas siguientes fueron testigo del surgimiento de sistemas operativos como UNIX, que aportaron modularidad y portabilidad a los entornos informáticos.

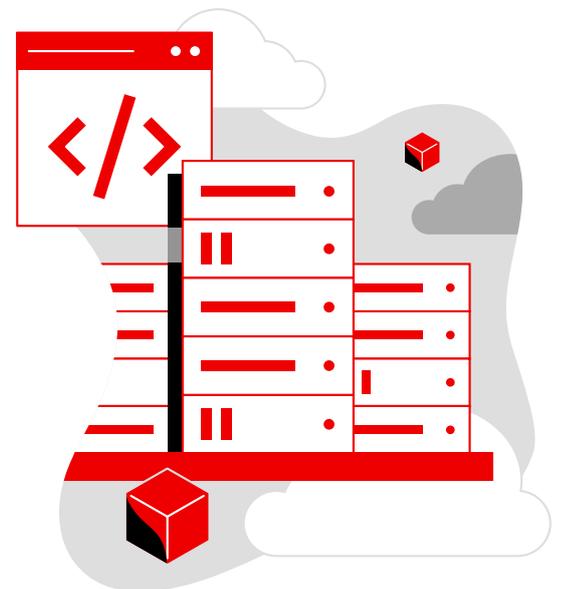
En los años 80, con el incremento en las ventas y la adopción de las computadoras personales, los sistemas operativos se dieron a conocer al público en general. Luego, la invención de las interfaces gráficas de usuario (GUI) revolucionó la forma en la que se interactuaba con las computadoras y las volvió accesibles a un público más amplio.

Con el crecimiento en la demanda de la informática basada en servidores, surgió **Linux®**, un sistema operativo potente y flexible para los centros de datos empresariales de todo el mundo. En 1991, cuando se lanzó el kernel de Linux por primera vez, representaba una alternativa a UNIX gratuita y open source que cualquiera podía ejecutar, estudiar, compartir y modificar. En la actualidad, Linux es uno de los sistemas operativos más utilizados del mundo y constituye una plataforma ideal para la TI moderna e innovadora.

La primera década del siglo XXI vino acompañada de las **tecnologías de virtualización** y los **contenedores**, que impulsaron un uso más eficiente de los recursos de hardware y la migración hacia el **cloud computing**. Así, los sistemas operativos asumieron nuevas funciones de gestión que permitieran implementar las aplicaciones con flexibilidad y optimizar los recursos.

Hoy en día, la influencia de los sistemas operativos trasciende los centros de datos principales e incluye tecnologías nuevas como los **dispositivos del extremo de la red** y el **Internet de las cosas (IoT)**. Los SO permiten procesar con eficiencia los datos en el extremo de la red para reducir la latencia y aumentar el rendimiento en casos prácticos tan variados como las ciudades inteligentes y los vehículos autónomos.

En este ebook, le ofrecemos un resumen con los motivos por los cuales los sistemas operativos, y especialmente Linux, siguen siendo importantes y permiten satisfacer las exigencias de las empresas y la TI moderna.



Ocho razones por las que su sistema operativo sigue siendo importante

A medida que las empresas adoptan entornos de TI cada vez más distribuidos y basados en la nube, la importancia del sistema operativo sigue creciendo.

En la actualidad, el 87 % de las empresas cuenta con una estrategia multicloud y el 50 % de las cargas de trabajo empresariales se ejecuta en una nube pública¹. Su sistema operativo puede servir como base para unificar la infraestructura en las instalaciones y en la nube, la diversidad de hardware y software y las aplicaciones tradicionales y pensadas para la nube. La seguridad, la gestión, la portabilidad y la planificación del ciclo de vida comienzan por el sistema operativo. Una base operativa única y estandarizada que abarque el centro de datos y los entornos de nube le permitirá simplificar las operaciones de TI, aumentar la flexibilidad, mejorar la seguridad y respaldar la innovación.

Como Linux es uno de los sistemas operativos más utilizados del mundo, muchas empresas lo eligen como base de su infraestructura de TI. De hecho, en 2022, la participación de Linux en el mercado mundial de sistemas operativos para servidores era del 65,6 % para las implementaciones físicas totalmente nuevas y del 82,8 % para las implementaciones virtualizadas totalmente nuevas².

Las empresas utilizan sistemas operativos Linux para ejecutar una amplia gama de cargas de trabajo de producción y desarrollo, incluida la infraestructura de TI y web, la gestión de las relaciones con los clientes y la gestión de recursos empresariales³. En este capítulo, se analizan las formas en que este sistema operativo respalda las aplicaciones, los procesos y el entorno de TI en beneficio de toda la empresa.

En este capítulo encontrará:

- 2.1** Conectividad en toda la stack de TI
- 2.2** Compatibilidad en hardware y software
- 2.3** Confiabilidad y estabilidad de las plataformas
- 2.4** Eficiencia operativa de la TI
- 2.5** Seguridad y controles de acceso
- 2.6** Rendimiento de las aplicaciones
- 2.7** Gestión de los recursos virtuales
- 2.8** Implementación de aplicaciones modernas

¹ Flexera. "Flexera 2023 State of the Cloud Report". Marzo de 2023.

² IDC Market Share. "Worldwide Server Operating System Environments Market Shares, 2022: Steady Growth Persists". Documento n.º US51038623. Julio de 2023.

³ Whitepaper de IDC patrocinado por Red Hat. "Red Hat Enterprise Linux: \$1.7 Trillion a Year Boost for Customers". Documento n.º US48931522. Marzo de 2022.

1 El sistema operativo conecta al hardware con las aplicaciones y los usuarios

En su calidad de capa fundamental de la stack de software, posibilita las interacciones entre el hardware y las aplicaciones y se ocupa de los servicios y los recursos esenciales.

Abstrae los elementos fundamentales del hardware para que las aplicaciones puedan ejecutarse en infraestructuras distintas sin que deban modificarse para los sistemas específicos. También gestiona los recursos, como las unidades centrales de procesamiento (CPU), la memoria, el almacenamiento y las redes, para optimizar el rendimiento del sistema y prevenir posibles conflictos entre las aplicaciones en ejecución. La interfaz gráfica y la de línea de comandos de su SO le permiten interactuar con la computadora y las aplicaciones de una manera más intuitiva. Las funciones de seguridad, como las de autenticación de los usuarios, las de controles de acceso y las de cifrado, evitan que se acceda a los recursos y los datos sin autorización. Por último, las funciones para el control de errores y excepciones previenen las fallas del sistema, hacen que el sistema sea más confiable y mejoran la experiencia del usuario en general.

Los sistemas operativos modernos como Linux suelen implementarse en dos modos: en modo de kernel o en modo de usuario. Esto determina los privilegios disponibles para las aplicaciones, los elementos y los usuarios. En modo de kernel, los elementos principales y confiables del software, como el **kernel del sistema operativo** y algunos controladores de dispositivos, pueden llevar adelante operaciones para las que se requieren privilegios, utilizar los recursos de hardware de forma directa y acceder a las partes restringidas de la memoria del sistema.

El resto del software (como las aplicaciones, las bibliotecas y las herramientas de los usuarios) se ejecuta en modo de usuario y posee un acceso limitado a los recursos del sistema. Estas aplicaciones solo pueden acceder al espacio destinado a los usuarios, es decir, a las regiones aisladas de la memoria creadas para evitar que las aplicaciones interfieran con el funcionamiento de los elementos centrales del sistema operativo.

Base su TI en el conocimiento de los especialistas en los que puede confiar

Aunque Linux puede servir como base operativa estable para todas sus cargas de trabajo de TI, existen muchas distribuciones diferentes, cada una con herramientas, servicios y políticas de soporte distintas. Dado que su empresa se sustenta en la base de TI, resulta importante y estratégico elegir al proveedor de Linux que mejor se adapte a sus necesidades.

Debe elegir aquel que le ofrezca la confianza, el conocimiento y la experiencia que su empresa necesita. Algunos aspectos importantes:

- ▶ La distribución de Linux debe poder utilizarse en la producción y estar centrada en las necesidades de los clientes.
- ▶ Las contribuciones periódicas al kernel de Linux y el liderazgo dentro de la comunidad son importantes.
- ▶ Es bueno contar con una comunidad colaborativa de clientes, partners y especialistas.
- ▶ El proveedor debe disponer de un historial demostrado de soporte empresarial con ciclos de vida largos y mantenimiento de la seguridad.

2 Los sistemas operativos garantizan la compatibilidad entre el hardware y el software

Se encargan de gestionar los recursos de hardware como el almacenamiento, las redes y los dispositivos periféricos para aumentar la estabilidad del sistema y la compatibilidad entre el hardware y el software.

Las aplicaciones y los recursos de hardware se comunican a través de los controladores de los dispositivos. Los SO los gestionan y se aseguran de que se instalen y se carguen de manera apropiada y funcionen correctamente. Esto permite que el sistema sea más estable y la compatibilidad entre las aplicaciones y los elementos de hardware fundamentales sea mayor. Por ejemplo, al iniciar el sistema, el SO Linux detecta los recursos que se conectaron o integraron, identifica los dispositivos que conoce y encuentra y carga los controladores correspondientes. Los sistemas operativos también permiten que las aplicaciones interactúen con los dispositivos de hardware sin acceder a su información específica a través de capas de abstracción. Estas interfaces estandarizadas simplifican el desarrollo de aplicaciones y mejoran la portabilidad entre las diversas configuraciones de hardware.

Los controladores de los dispositivos y los sistemas operativos son particularmente importantes para los chipsets, el almacenamiento y las redes. Las cargas de trabajo que consumen muchos recursos informáticos, como las de inteligencia artificial/machine learning, se benefician de la aceleración del hardware en los chipsets. Los sistemas operativos pueden poner a disposición de estas cargas de trabajo las funciones y la aceleración de las unidades de procesamiento gráfico (GPU), los sistemas en chips (SoC) y las matrices de puertas programables en campo (FPGA).

También permiten que se acceda a los **datos almacenados** en discos duros de manera estable y confiable. Gestionan la organización y el almacenamiento de los archivos con métodos optimizados para reducir al máximo la fragmentación de los datos, prevenir los conflictos con los nombres y garantizar la uniformidad entre las aplicaciones.

Por último, organizan las funciones relacionadas con las redes para que la conectividad sea confiable y el intercambio de datos entre los sistemas de la red sea eficiente. Utilizan una stack de redes para gestionar la integración de los distintos protocolos de red y posibilitar la comunicación integral entre las diversas redes. También configuran y gestionan los dispositivos de red, como las tarjetas de interfaz de red (NIC) y los adaptadores inalámbricos, para admitir y acelerar la transmisión de datos entre las aplicaciones. Además, implementan medidas de seguridad en la red, como los firewalls y los protocolos de cifrado, para protegerla de accesos no autorizados y filtraciones de datos.

Obtenga más opciones con un ecosistema de partners certificados

Las pruebas y las certificaciones le brindan la seguridad de que los productos de terceros funcionarán de manera confiable con su SO. Obtenga su distribución de Linux de una empresa que se asocie con los proveedores de nube, hardware y software líderes del sector para ofrecerle más opciones, innovación y estabilidad. Asegúrese de que el ecosistema de partners del proveedor que elija incluya productos y servicios que utiliza actualmente y que tiene previsto utilizar en el futuro.

3 Los sistemas operativos mejoran la confiabilidad y la estabilidad de las plataformas

Al detectar los errores en el hardware y el software y encargarse de ellos, brindan una plataforma estable y confiable para las aplicaciones y los usuarios.

Las aplicaciones ocupan un lugar central en la mayoría de las empresas digitales, y suele ser inaceptable que se produzca tiempo de inactividad. Muchos sistemas operativos incluyen mecanismos avanzados para la detección de errores que encuentran los errores de tiempo de ejecución durante la ejecución de las aplicaciones y se encargan de ellos. Estos mecanismos ayudan a prevenir que todo el sistema colapse, que se produzcan interrupciones y que se dañen los datos. Los sistemas operativos, además, supervisan las aplicaciones y los archivos del sistema esenciales mediante comprobaciones de integridad, sumas de comprobación y firmas digitales para asegurarse de que solo se ejecute el código autorizado y sin adulterar.

También deben ocuparse de los errores en el hardware. Al detectar errores en el hardware tales como las fallas de la memoria, los errores en el disco y el mal funcionamiento del procesador y encargarse de ellos, los sistemas operativos logran que el sistema sea más estable y previenen las fallas generalizadas. Al integrar en las memorias y los dispositivos de almacenamiento la protección que ofrece el código de corrección de errores (ECC) y la verificación por redundancia cíclica (CRC), los SO identifican el hardware defectuoso y se encargan de él para aumentar la confiabilidad de los datos que almacenan y utilizan las aplicaciones. Los mecanismos de detección y corrección de errores, como la creación de registros diarios y sumas de comprobación, les permiten obtener datos para los usuarios y las aplicaciones con rapidez y precisión.

También es importante comprender los problemas del sistema y solucionarlos. Los SO ofrecen herramientas de registro y diagnóstico que recaban información sobre los errores y los eventos del sistema que puede ser de utilidad en la resolución de problemas y las operaciones de mantenimiento predictivo. Los administradores de sistemas pueden utilizarlas para analizar los patrones de los errores, identificar posibles puntos vulnerables y tomar medidas para mantener la estabilidad y la confiabilidad general del sistema.

Aumente la estabilidad del sistema con herramientas de análisis predictivo y resolución preventiva de errores

La gestión de los entornos complejos de TI puede ser complicada y tomar mucho tiempo. La distribución de Linux que elija debe incluir herramientas avanzadas de gestión y automatización que le permitan gestionar preventivamente todo su entorno de TI. Con las herramientas unificadas que funcionan en todos los entornos de la infraestructura y supervisan todos sus sistemas, puede encontrar los problemas antes de que afecten las operaciones de la empresa, y las herramientas centradas en las operaciones, la seguridad y los resultados empresariales le permiten conocer las consecuencias de los cambios y los problemas en su empresa para establecer las acciones de resolución que tienen prioridad.

4 Los sistemas operativos impulsan la eficiencia de las operaciones de TI

Cuando utiliza un sistema operativo uniforme como base unificada de todos sus entornos de TI, puede estandarizar y optimizar las operaciones, aumentar la eficiencia y mejorar la seguridad.

Los entornos de TI modernos suelen consistir en múltiples infraestructuras y arquitecturas. De hecho, el 85 % de las empresas opera en múltiples entornos de implementación, y el 31 % implementa aplicaciones en cinco entornos o más⁴. Por ejemplo, puede que se utilicen tanto centros de datos locales como proveedores de nube pública, y que se implementen cargas de trabajo en servidores, estaciones de trabajo y dispositivos del extremo de la red basados en una variedad de arquitecturas de hardware como x86, ARM e IBM Power.

En este tipo de entornos diversos, la uniformidad es de vital importancia. Los entornos operativos estandarizados le permiten desarrollar procedimientos, políticas y configuraciones comunes para simplificar las operaciones cotidianas y las tareas de gestión, lo cual ofrece muchos beneficios para su empresa de TI:

- ▶ **Interoperabilidad:** al utilizar un mismo sistema operativo, se fomenta la interoperabilidad y la integración en las diversas infraestructuras. Puede implementar y gestionar aplicaciones distribuidas en entornos de enormes proporciones con menos complejidad y solucionar los problemas en ellas.
- ▶ **Capacidad de ajuste:** cuando implementa un sistema operativo uniforme, se simplifica el ajuste de la capacidad de los servicios de TI y los entornos, ya que se pueden replicar las configuraciones actuales y validadas en la infraestructura nueva.
- ▶ **Seguridad:** los entornos operativos estandarizados facilitan la aplicación uniforme de las políticas de seguridad, como la aplicación regular de parches, las actualizaciones y las auditorías de cumplimiento normativo en todos los entornos, lo que reduce el riesgo de aparición de los puntos vulnerables para la seguridad.
- ▶ **Disponibilidad:** al utilizar el mismo sistema operativo en todos los entornos de nube híbrida, se optimiza la resolución de problemas para disminuir el tiempo de inactividad en el sistema.

Estandarice el sistema para obtener más eficiencia

Su SO puede servir de base uniforme y estandarizada en todas las infraestructuras y arquitecturas. Elija un proveedor de Linux que ofrezca múltiples variantes del sistema operativo optimizadas para diferentes entornos de implementación y mantenga la uniformidad general. Asegúrese de que las herramientas de gestión y automatización incluidas y asociadas funcionen de la misma manera en todas las variantes. La adopción de una de estas distribuciones para todas sus infraestructuras puede permitirle crear entornos operativos homogéneos y unificados que optimicen la gestión de la infraestructura, aumenten la eficiencia y la productividad de TI y mejoren la seguridad.

5 Los sistemas operativos protegen su infraestructura, aplicaciones y datos

Los defienden contra las amenazas que comprometen su integridad, confidencialidad y disponibilidad

El kernel de Linux incluye muchas funciones de seguridad para proteger la infraestructura, las aplicaciones y los datos. Contienen, por ejemplo, las herramientas de autenticación y autorización necesarias para implementar **arquitecturas de confianza cero**. La autenticación mediante nombres de usuario, contraseñas, datos biométricos o tokens de seguridad identifica a las personas y las aplicaciones que desean acceder a los sistemas y los recursos informáticos. Los mecanismos de autorización y control de acceso como **Security-Enhanced Linux (SELinux)** definen los permisos y privilegios concedidos a estos usuarios, grupos o aplicaciones. En conjunto, estas herramientas permiten evitar el acceso no autorizado a los recursos y las configuraciones confidenciales del sistema.

Más funciones de seguridad del sistema operativo relevantes:

- ▶ **Cifrado:** las tecnologías integradas de cifrado protegen los archivos y los datos confidenciales, tanto en tránsito como en reposo y en todas las redes. Red Hat® Enterprise Linux, por ejemplo, utiliza políticas de cifrado en todo el sistema para configurar y aplicar automáticamente controles de cifrado predefinidos en los sistemas y las aplicaciones. También admite el cifrado asistido por CPU de las cargas de trabajo de las máquinas virtuales para garantizar la confidencialidad de la informática.
- ▶ **Creación de listas de aplicaciones permitidas:** con esta función, se establece un índice de archivos ejecutables y aplicaciones aprobadas que ciertos usuarios específicos pueden ejecutar en determinado sistema.
- ▶ **Base de hardware de confianza:** Las bases de hardware de confianza, la certificación remota y las tecnologías de arranque medido comprueban la integridad de los sistemas y garantizan que no se hayan modificado ni manipulado.
- ▶ **Análisis de seguridad:** las herramientas de análisis de cumplimiento y puntos vulnerables, como Open Security Content Automation Protocol (OpenSCAP), simplifican las auditorías, encuentran fallas en la configuración de los sistemas y las solucionan, y le permiten mantener el cumplimiento normativo.
- ▶ **Registros del sistema:** las funciones de auditoría y registro recopilan información sobre los eventos y las actividades en el sistema. Luego, los administradores pueden revisarla, identificar el origen de los fallos de seguridad y tomar medidas al respecto.

Cree una base para la confianza cero

Las arquitecturas de confianza cero permiten aplicar la seguridad a cada recurso, en vez de hacerlo únicamente en el perímetro de la red. Si bien Linux incluye las funciones básicas necesarias para diseñar arquitecturas de confianza cero, algunas distribuciones incorporan funciones y herramientas que simplifican su adopción. La distribución de Linux que elija debe provenir de una cadena de suministro de software de confianza e incluir opciones de cifrado para todo el sistema, funciones de base de hardware de confianza, análisis integrado del cumplimiento normativo y herramientas de gestión de identidades basadas en políticas.

Para obtener más información, lea el **resumen**.

6 Los sistemas operativos gestionan el rendimiento de las aplicaciones y las cargas de trabajo

Gestionan el uso de la CPU y la memoria para aumentar al máximo el rendimiento del hardware y ofrecer experiencias de primer nivel para el usuario, con las aplicaciones y las cargas de trabajo.

Para optimizar el uso de la CPU y la memoria, equilibrar las cargas de trabajo entre los recursos y mantener la capacidad de respuesta del sistema, se valen de tecnologías de programación de procesos. Los algoritmos de esta tecnología y los mecanismos de equilibrio de carga aseguran que se haga un uso eficiente del tiempo de la CPU y que se distribuya de manera equitativa. Estos algoritmos también permiten que se avance con múltiples procesos de manera simultánea alternando las CPU con rapidez entre ellos.

Al priorizar los procesos interactivos, los sistemas operativos aumentan la capacidad de respuesta en las experiencias de los usuarios para que estos perciban demoras mínimas o nulas. Además, gracias a las funciones que permiten programar procesos de forma inmediata, aquellos con requisitos estrictos en cuanto a tiempo (como los de los sistemas integrados o de control industrial) pueden completarse en plazos concretos y responder con prontitud a eventos externos.

Linux también incluye funciones de gestión de la memoria para garantizar que las aplicaciones dispongan de memoria suficiente, evitar posibles conflictos y optimizar el rendimiento del sistema. La asignación y la quita dinámica de memoria proporciona a los procesos la memoria necesaria para obtener el máximo rendimiento. Cuando un proceso termina de utilizar la memoria, el SO la pone a disposición de otros procesos.

Los sistemas operativos también mejoran el rendimiento de la memoria mediante mecanismos de caché y almacenamiento en búfer, con los cuales se almacenan los datos de acceso frecuente en cachés más rápidas y costosas y el resto de los datos en memorias de acceso aleatorio (RAM) y dispositivos de almacenamiento más grandes y lentos. Además, al intercambiar los datos entre la memoria y los discos duros, la memoria virtual permite que los sistemas operativos otorguen a los procesos un espacio de direcciones mayor que el disponible físicamente. La memoria virtual aumenta la eficacia para realizar varias tareas a la vez y permite ejecutar aplicaciones más grandes en entornos con menos memoria.

Optimice el rendimiento de las cargas de trabajo

Busque una distribución de Linux que incluya herramientas e interfaces para ajustar, supervisar y gestionar las características de rendimiento del sistema por aplicación, carga de trabajo o caso práctico. Por ejemplo, algunos proveedores ofrecen herramientas y servicios que permiten identificar problemas de rendimiento, perfilar el rendimiento de las aplicaciones y analizar los datos para ayudar a resolver los problemas rápidamente o incluso evitarlos por completo.

7 Los sistemas operativos mejoran el uso de los recursos con máquinas virtuales

Como parte fundamental de las tecnologías de las máquinas virtuales, los sistemas operativos optimizan el uso de los recursos, aíslan las cargas de trabajo y aumentan la capacidad de ajuste en los distintos entornos.

Las **máquinas virtuales** son entornos aislados que ejecutan sus propios sistemas operativos guest que los usuarios y las aplicaciones experimentan como recursos de hardware independientes, aunque puedan compartir los recursos físicos reales con otras máquinas virtuales. Los **hipervisores** son programas especializados que crean y gestionan máquinas virtuales en un único servidor físico. Los sistemas operativos y los hipervisores se parecen en muchas de sus funciones. Por eso, pueden compartir muchos elementos, como los programadores de procesos, los gestores de memoria, los controladores de los dispositivos, las funciones de seguridad y las stacks de red.

Expanda la virtualización

La máquina virtual basada en el **kernel (KVM)** de Linux le permite utilizar Linux como hipervisor. Elija una distribución comercial de Linux que amplíe las capacidades de KVM para lograr una gestión más eficaz.

Los hipervisores desempeñan muchas funciones para respaldar las operaciones de TI:

- ▶ **Asignación de recursos:** Los hipervisores asignan recursos, como el tiempo de CPU y la memoria, a las máquinas virtuales, lo que permite que varias de ellas funcionen en el mismo hardware físico con una calidad de servicio garantizada. También proporcionan a los sistemas operativos guest hardware físico, como adaptadores de red, controladores de almacenamiento y tarjetas gráficas, en forma de dispositivos virtuales para que varias máquinas virtuales puedan utilizar los mismos recursos sin conflictos.
- ▶ **Instantáneas y clones:** muchos hipervisores incluyen funciones para realizar instantáneas y clonar máquinas virtuales con el fin de mejorar la flexibilidad, la capacidad de ajuste y la eficacia. Las instantáneas capturan el estado y los datos de la máquina virtual en momentos concretos. Se pueden utilizar para recuperar el estado anterior de la máquina virtual o volver a configuraciones conocidas. Las funciones de clonación duplican las máquinas virtuales para acelerar la implementación de nuevas instancias.
- ▶ **Migración activa y recuperación:** las funciones de migración activa y alta disponibilidad ayudan a equilibrar las cargas de trabajo, optimizar el uso de los recursos y mejorar el tiempo de actividad de las máquinas virtuales. La migración activa traslada las máquinas virtuales en ejecución entre los hosts físicos sin interrumpir el servicio. Las máquinas virtuales permanecen encendidas, las conexiones de red siguen activas y las aplicaciones continúan ejecutándose. Si las máquinas virtuales se interrumpen debido a un fallo del host, el hipervisor las reinicia automáticamente, en cuestión de segundos y sin intervención humana.
- ▶ **Seguridad y aislamiento:** los hipervisores imponen límites estrictos que impiden que unas máquinas virtuales accedan a la memoria o a los recursos asignados a otras. Con ellos, se refuerza la seguridad y se contienen los efectos de posibles puntos vulnerables y ciberataques.



Los sistemas operativos respaldan las aplicaciones modernas desarrolladas en la nube.

Los sistemas operativos Linux admiten tecnologías de contenedores para implementar y gestionar las aplicaciones modernas y desarrolladas en la nube con mayor agilidad, capacidad de ajuste y uniformidad.

El 52 % de las empresas considera que "organizar las cargas de trabajo en contenedores" es una parte fundamental de las iniciativas de modernización de las aplicaciones⁵. Los **contenedores** son tecnologías que empaquetan elementos de TI como aplicaciones, tiempos de ejecución, bibliotecas y dependencias en entornos ligeros, portátiles y aislados. Las tecnologías de contenedores virtualizan eficazmente el sistema operativo, lo que permite que varios contenedores compartan un único kernel de sistema operativo que gestiona los recursos de hardware y las interacciones con el sistema host físico.

Los sistemas operativos Linux realizan particiones de los recursos del kernel relacionados con los espacios de proceso, los sistemas de archivos y el acceso a la red para dotar a cada contenedor de su propio conjunto de recursos. Al igual que con la virtualización tradicional, de este modo se aísla cada contenedor para evitar conflictos e interferencias entre contenedores y se permite que varios de ellos (cada uno con espacios de usuario y entornos de ejecución únicos) se ejecuten en el mismo host. Para asignar los recursos de forma justa y adecuada, los sistemas operativos gestionan y limitan el uso de los recursos, como la CPU, la memoria y la entrada y la salida (E/S) del disco, en función de cada contenedor.

Al gestionar las interfaces y las configuraciones de red en los entornos de contenedores, los sistemas operativos garantizan que los contenedores puedan comunicarse entre sí y con los sistemas externos cuando sea necesario, sin dejar de mantener el aislamiento de la red. También proporcionan a los contenedores sistemas de archivos aislados que pueden acceder a datos compartidos y almacenamiento permanente a través de controladores de almacenamiento de contenedores.

Por último, los sistemas operativos ofrecen controles de acceso obligatorios (MAC) para aplicar políticas estrictas y predefinidas de acceso a los recursos. Los contenedores solo pueden interactuar con los recursos del sistema especificados para aumentar el aislamiento y protegerse de las amenazas y los puntos vulnerables de seguridad generalizados.

Amplíe su entorno y sus habilidades de TI con los contenedores

Puede empezar a utilizar contenedores con solo disponer de un sistema operativo Linux. Busque una distribución de Linux que incluya herramientas de contenedores como **Podman**, **Skopeo** y **Buildah** que le permitan desarrollar, diseñar, ejecutar y gestionar contenedores en sus sistemas. Si elige un proveedor de Linux que también ofrezca una plataforma de gestión de contenedores, tendrá la opción de ampliar y ajustar el uso de contenedores con el tiempo.

⁵ Ebook de Red Hat. "El enfoque de las empresas sobre la modernización de las aplicaciones heredadas", 6 de febrero de 2023.

Aproveche el software open source

Las comunidades open source crean y mantienen muchos sistemas operativos populares, entre ellos Linux, así como herramientas y software relacionados.

En estas comunidades, los desarrolladores proponen, aportan y prueban nuevas funciones y prestaciones del sistema operativo. Las versiones están disponibles a través de distribuciones comunitarias gratuitas y distribuciones empresariales de pago.

Las distribuciones empresariales o comerciales suelen ofrecerse mediante suscripciones y proporcionan funciones, servicios y soporte adicionales adaptados a las necesidades e inquietudes de la empresa. Por ejemplo, las suscripciones a sistemas operativos empresariales suelen ofrecer soporte técnico permanente para acelerar la resolución de problemas y reducir el tiempo de inactividad. También pueden incluir capacitación y tutoriales que ayuden a los usuarios a administrar, optimizar y solucionar los problemas del sistema operativo con eficacia.

Los ciclos de vida con mantenimiento prolongado aumentan la estabilidad en todos los entornos de TI. Los proveedores comerciales suelen seguir ciclos de lanzamiento predecibles, lo que permite a las empresas planificar y prepararse para las actualizaciones, las mejoras y las nuevas funciones. Las herramientas de actualización integrada y los servicios profesionales pueden hacer que el paso a las nuevas versiones sea sencillo y eficaz.

Los proveedores empresariales suelen contar con equipos de seguridad que evalúan las amenazas cuando surgen, las controlan y responden ante ellas para aumentar la seguridad del sistema operativo. Algunas distribuciones comerciales incluyen servicios que supervisan los sistemas operativos y ofrecen orientación para solucionar los problemas de seguridad, las configuraciones que no cumplen las normas, los sistemas sin parches y los desajustes en la configuración. Los proveedores también pueden certificar sus sistemas operativos según las normas de seguridad del sector para ayudar a mantener el cumplimiento y la protección.

Por último, muchos proveedores comerciales fomentan la existencia de ecosistemas de partners certificados para sus sistemas operativos con el fin de promover operaciones estables y confiables. Estos ecosistemas pueden incluir proveedores de hardware, de software, de nubes públicas y empresas de servicios.

Los beneficios de los sistemas operativos comerciales open source

En comparación con las empresas que utilizan alternativas gratuitas, los usuarios de sistemas operativos comerciales experimentan:

23 %
de reducción en el costo de la infraestructura en las instalaciones durante tres años⁶.

72 %
menos de tiempo de inactividad imprevisto⁶.

USD 17,3 millones
más de ingresos netos al año por empresa en promedio⁶.

⁶ Whitepaper de IDC patrocinado por Red Hat. "El valor empresarial de las soluciones Red Hat en contraste con las alternativas gratuitas". Documento n.º US50423523. Marzo de 2023.

Simplifique la gestión del sistema

Las herramientas para la gestión de los sistemas operativos le permiten configurar, supervisar y optimizar sus entornos de TI con mayor eficacia.



Gestión del rendimiento

Obtenga información sobre el rendimiento del sistema para supervisar el uso que se hace de él, identificar los obstáculos y solucionar los problemas de rendimiento.



Automatización de la TI

Automatice las tareas rutinarias para disminuir la intervención manual, reducir al mínimo los errores y garantizar la uniformidad de las configuraciones del sistema.



Gestión de la seguridad y los accesos

Evalúe, gestione y corrija los puntos vulnerables de la seguridad para proteger las aplicaciones y los datos fundamentales. Aplique controles de acceso, gestione los permisos y asegúrese de que los usuarios dispongan de los privilegios adecuados según sus funciones.



Gestión de la configuración

Aplique actualizaciones y mejoras para garantizar que los sistemas operativos se mantengan al día con los últimos parches de seguridad y mejoras de funciones. Mantenga la uniformidad de las configuraciones en varios sistemas para reducir el desajuste de las configuraciones en los distintos entornos de TI.



Auditoría y supervisión

Registre y audite los eventos del sistema para simplificar la resolución de problemas, el cumplimiento y los análisis de seguridad. Optimice las actividades de auditoría para garantizar el cumplimiento de los estándares operativos y de seguridad. Supervise y optimice los recursos virtuales para garantizar un uso eficiente y rentable del sistema.



Backup y recuperación

Cree y gestione los backups, y aplique procesos de recuperación para resguardar los datos en caso de fallo o pérdidas en el sistema.

Red Hat Enterprise Linux: un punto de partida para la TI moderna

El sistema operativo desempeña un papel fundamental en su infraestructura de TI. Red Hat Enterprise Linux ofrece más beneficios para su empresa.

Independientemente de sus objetivos en cuanto a la TI, Red Hat Enterprise Linux le permitirá diseñar una base eficiente y centrada en la seguridad para generar innovaciones en entornos híbridos y multicloud. Este sistema operativo preparado para la nube ofrece una experiencia uniforme y personalizada en todos los entornos: físicos, virtuales, multicloud, híbridos y en el extremo de la red. Su adopción tanto en el centro de datos de las instalaciones como en los entornos de nube le permite mejorar la productividad, la seguridad y las operaciones a medida que se traslada la nube y se adapta a un mundo cada vez más digital.



Uniformidad entre los entornos



Herramientas de análisis predictivo y resolución de problemas



Funciones avanzadas de seguridad



Cadena de suministro de software confiable



Automatización y gestión incorporadas



Herramientas de optimización del rendimiento



Gran ecosistema de partners certificados



Opciones en las distintas arquitecturas



Herramientas integradas de contenedores



Obtenga más información sobre Red Hat Enterprise Linux