Red Hat Enterprise Linux 8

8.3 Notas de la versión

Notas de la versión de Red Hat Enterprise Linux 8.3

Last Updated: 2021-02-22

Red Hat Enterprise Linux 8 8.3 Notas de la versión

Notas de la versión de Red Hat Enterprise Linux 8.3

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Legal Notice

Resumen

Las Notas de la versión proporcionan una cobertura de alto nivel de las mejoras y adiciones que se han implementado en Red Hat Enterprise Linux 8.3 y documentan los problemas conocidos en esta versión, así como las correcciones de errores notables, las previsiones tecnológicas, la funcionalidad obsoleta y otros detalles.

Table of Contents

2021-02-22Red Hat

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para realizar comentarios sencillos sobre pasajes concretos, asegúrese de que está viendo la documentación en el formato HTML multipágina. Resalte la parte del texto que desea comentar. A continuación, haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado y siga las instrucciones que aparecen.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
    1. Vaya al sitio web de Bugzilla.
    2. Como componente, utilice **Documentation**.
    3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
    4. Haga clic en **Submit Bug**.

CAPÍTULO 1. RESUMEN

Creación del instalador y de la imagen

En RHEL 8.3, puede configurar una contraseña de root y crear una cuenta de usuario antes de comenzar la instalación. Anteriormente, se configuraba una contraseña de root y se creaba una cuenta de usuario después de comenzar el proceso de instalación. También puede crear imágenes personalizadas basadas en un backend mucho más fiable y también enviar imágenes a las nubes a través de la consola web de RHEL.

RHEL para Edge

RHEL 8.3 introduce **RHEL for Edge** para la instalación remota de RHEL en servidores Edge. RHEL for Edge es una imagen rpm-ostree que se puede componer con Image Builder. Puede instalar la imagen utilizando un archivo Kickstart y luego administrar la imagen para incluir actualizaciones de la imagen y para revertir una imagen a un estado funcional anterior.

A continuación se presentan los aspectos más destacados de RHEL for Edge:

- Actualizaciones atómicas, en las que se conoce el estado de cada actualización y no se ven los cambios hasta que se reinicia el dispositivo.
- Comprobaciones de estado personalizadas y reversiones inteligentes para garantizar la resistencia.
- Flujos de trabajo centrados en los contenedores, en los que puede separar las actualizaciones del sistema operativo principal de las de las aplicaciones, y probar e implantar diferentes versiones de las aplicaciones.
- Cargas útiles OTA optimizadas para entornos con poco ancho de banda.

Para más información, consulte Sección 6.1.2, “RHEL para Edge” .

Servicios de infraestructura

La herramienta de ajuste del sistema **Tuned** se ha actualizado a la versión 2.13, que añade soporte para el ajuste dependiente de la arquitectura y múltiples directivas de inclusión.

Seguridad

RHEL 8.3 proporciona roles de Ansible para la implementación automatizada de soluciones de descifrado basadas en políticas (PBD) utilizando **Clevis** y **Tang**, y esta versión del paquete **rhel-system-roles** también contiene un rol de Ansible para el registro de RHEL a través de **Rsyslog**.

Los paquetes **scap-security-guide** han sido rebasados a la versión 0.1.50, y **OpenSCAP** ha sido rebasado a la versión 1.3.3. Estas actualizaciones proporcionan mejoras sustanciales, incluyendo un perfil alineado con el CIS RHEL 7 Benchmark v2.2.0 y un perfil alineado con el Health Insurance Portability and Accountability Act (HIPAA) que es requerido por las organizaciones sanitarias norteamericanas.

Con esta actualización, ahora puede generar funciones de corrección basadas en resultados a partir de perfiles adaptados mediante la herramienta **SCAP Workbench**.

El marco **USBGuard** ahora proporciona su propia política SELinux, notifica a los usuarios del escritorio en la GUI, y la versión 0.7.8 contiene muchas otras mejoras y correcciones de errores.

Lenguajes de programación dinámicos, servidores web y de bases de datos

Las versiones posteriores de los siguientes componentes ya están disponibles como nuevos flujos de módulos:

- **nginx 1.18**

- **Node.js 14**
- **Perl 5.30**
- **PHP 7.4**
- **Ruby 2.7**

Los siguientes componentes han sido actualizados en RHEL 8.3:

- **Git** a la versión 2.27
- **Squid** a la versión 4.11

Para más información, consulte Sección 6.1.11, "Lenguajes de programación dinámicos, servidores web y de bases de datos".

Conjuntos de herramientas de compilación

Los siguientes conjuntos de herramientas de compilación se han actualizado en RHEL 8.3:

- **GCC Toolset 10**
- **LLVM Toolset 10.0.1**
- **Rust Toolset 1.45.2**
- **Go Toolset 1.14.7**

Para más información, consulte Sección 6.1.12, "Compiladores y herramientas de desarrollo" .

Gestión de la identidad

El conjunto de cifrado Rivest Cipher 4 (RC4), el tipo de cifrado por defecto para usuarios, servicios y fideicomisos entre dominios de Active Directory (AD) en un bosque de AD, ha sido obsoleto en RHEL 8. Por razones de compatibilidad, esta actualización introduce una nueva subpolítica criptográfica **AD-SUPPORT** para permitir el soporte del tipo de cifrado RC4 obsoleto. La nueva subpolítica permite utilizar RC4 con las soluciones de integración de RHEL Identity Management (IdM) y SSSD Active Directory.

Para más información, consulte Sección 6.1.13, "Gestión de la identidad" .

La consola web

La consola web proporciona una opción para cambiar entre el acceso administrativo y el acceso limitado desde dentro de una sesión de usuario.

Virtualización

Las máquinas virtuales (VM) alojadas en el hardware IBM Z ahora pueden utilizar la función IBM Secure Execution. Esto hace que las VMs sean resistentes a los ataques si el host está comprometido, y también evita que los hosts no confiables obtengan información de la VM. Además, ahora se pueden asignar dispositivos DASD a las VM en IBM Z.

Escritorio y gráficos

Ahora puede utilizar el escritorio GNOME en los sistemas IBM Z.

El subsistema gráfico del kernel **Direct Rendering Manager** (DRM) ha sido reajustado a la versión 5.6 del kernel de Linux. Esta versión proporciona una serie de mejoras con respecto a la versión anterior, como la compatibilidad con las nuevas GPU y APU, y varias actualizaciones de los controladores.

Consulte Sección 6.1.14, “Escritorio” y Sección 6.1.15, “Infraestructuras gráficas” para más detalles.

Actualización in situ y conversión del sistema operativo

In-place upgrade from RHEL 7 to RHEL 8

Las vías de actualización in situ admitidas actualmente son:

- De RHEL 7.8 a RHEL 8.2 en las arquitecturas Intel de 64 bits, IBM POWER 8 (little endian) e IBM Z
- De RHEL 7.6 a RHEL 8.2 en arquitecturas que requieren la versión 4.14 del kernel: IBM POWER 9 (little endian) e IBM Z (Structure A)
- De RHEL 7.7 a RHEL 8.2 en sistemas con SAP HANA.

Para garantizar que su sistema siga siendo compatible después de actualizar a RHEL 8.2, actualice a la última versión de RHEL 8.3 o habilite los repositorios de RHEL 8.2 Extended Update Support (EUS). En los sistemas con SAP HANA, active los repositorios de RHEL 8.2 Update Services for SAP Solutions (E4S).

Para más información, consulte Rutas de actualización in situ soportadas para Red Hat Enterprise Linux . Para obtener instrucciones sobre cómo realizar una actualización in situ, consulte Actualización de RHEL 7 a RHEL 8.

Las mejoras más destacadas son:

- **Leapp** ahora soporta la entrada del usuario generando preguntas de verdadero/falso para determinar cómo proceder con la actualización.
- Ahora puede actualizar varios hosts simultáneamente mediante la interfaz web de Satellite.
- La actualización in situ es ahora compatible con instancias bajo demanda en AWS y Microsoft Azure, utilizando Red Hat Update Infrastructure (RHUI).
- Con la publicación del aviso RHBA-2021:0569, puede crear scripts personalizados para el informe de preactualización de **Leapp**. Consulte Automatizar el flujo de trabajo del informe de preactualización de Red Hat Enterprise Linux para obtener más detalles.

In-place upgrade from RHEL 6 to RHEL 8

Para actualizar de RHEL 6.10 a RHEL 8.2, siga las instrucciones de Actualización de RHEL 6 a RHEL 8 .

Conversion from a different Linux distribution to RHEL

Si está utilizando CentOS 8 u Oracle Linux 8, puede convertir su sistema operativo a RHEL 8 utilizando la utilidad **Convert2RHEL**. Para obtener más información, consulte https://red.ht/migrate.

Si está utilizando una versión anterior de CentOS u Oracle Linux, concretamente las versiones 6 o 7, puede convertir su sistema operativo a RHEL y luego realizar una actualización in situ a RHEL 8.

.NET 5 ya está disponible en RHEL 8 como Technology Preview

.NET 5 ya está disponible como Technology Preview en Red Hat Enterprise Linux 8 y OpenShift Container Platform. .NET 5 incluye nuevas versiones de lenguaje: C# 9 y F# 5.0. Se han realizado importantes mejoras de rendimiento en las bibliotecas base, GC y JIT. .NET 5 cuenta con **aplicaciones de archivo único**, lo que permite distribuir aplicaciones .NET como un único ejecutable, con todas las dependencias incluidas. Las imágenes UBI8 para .NET 5 están disponibles en el registro de contenedores de Red Hat y pueden utilizarse con OpenShift.

Para utilizar .NET 5, instale el paquete **dotnet-sdk-5.0**:

```
$ sudo dnf install -y dotnet-sdk-5.0
```

Para más información, consulte la documentación de .NET 5.

OpenJDK 11 ya está disponible

Ya está disponible la nueva versión de Open Java Development Kit (OpenJDK). Para obtener más información sobre las características introducidas en esta versión y los cambios en la funcionalidad existente, consulte las características de OpenJDK .

Recursos adicionales

- **Capabilities and limits** de Red Hat Enterprise Linux 8 en comparación con otras versiones del sistema están disponibles en el artículo de la base de conocimientos Capacidades y límites de la tecnología Red Hat Enterprise Linux.
- La información relativa a Red Hat Enterprise Linux **life cycle** se proporciona en el documento Ciclo de vida de Red Hat Enterprise Linux .
- El documento del manifiesto del paquete proporciona un **package listing** para RHEL 8.
- Los principales **differences between RHEL 7 and RHEL 8** están documentados en Consideraciones para la adopción de RHEL 8 .
- En el documento Actualización a RHEL 8 se dan instrucciones sobre cómo realizar un **in-place upgrade from RHEL 7 to RHEL 8**.
- El servicio **Red Hat Insights**, que le permite identificar, examinar y resolver proactivamente los problemas técnicos conocidos, está ahora disponible con todas las suscripciones de RHEL. Para obtener instrucciones sobre cómo instalar el cliente Red Hat Insights y registrar su sistema en el servicio, consulte la página Red Hat Insights Get Started .

Portal de clientes de Red Hat Labs

Red Hat Customer Portal Labs es un conjunto de herramientas en una sección del Portal del Cliente disponible en https://access.redhat.com/labs/. Las aplicaciones del Portal del Cliente de Red Hat Labs pueden ayudarle a mejorar el rendimiento, a solucionar rápidamente los problemas, a identificar los problemas de seguridad y a desplegar y configurar rápidamente las aplicaciones complejas. Algunas de las aplicaciones más populares son:

- Asistente de registro
- Comprobador del ciclo de vida del producto
- Generador Kickstart
- Convertidor Kickstart
- Ayudante de actualización de Red Hat Enterprise Linux
- Ayudante de actualización de Red Hat Satellite
- Navegador de código de Red Hat
- Herramienta de configuración de opciones JVM
- Red Hat CVE Checker

- Certificados de productos Red Hat
- Herramienta de configuración del equilibrador de carga
- Ayudante de configuración del repositorio Yum

CAPÍTULO 2. ARQUITECTURAS

Red Hat Enterprise Linux 8.3 se distribuye con la versión 4.18.0-240 del kernel, que proporciona soporte para las siguientes arquitecturas:

- Arquitecturas de 64 bits de AMD e Intel
- La arquitectura ARM de 64 bits
- IBM Power Systems, Little Endian
- IBM Z

Asegúrese de adquirir la suscripción apropiada para cada arquitectura. Para más información, consulte Introducción a Red Hat Enterprise Linux - arquitecturas adicionales . Para una lista de suscripciones disponibles, vea Utilización de suscripciones en el Portal del cliente.

CAPÍTULO 3. DISTRIBUCIÓN DE CONTENIDOS EN RHEL 8

3.1. INSTALACIÓN

Red Hat Enterprise Linux 8 se instala mediante imágenes ISO. Hay dos tipos de imágenes ISO disponibles para las arquitecturas AMD64, Intel 64 bits, ARM 64 bits, IBM Power Systems e IBM Z:

- DVD ISO binario: Una imagen de instalación completa que contiene los repositorios de BaseOS y AppStream y permite completar la instalación sin repositorios adicionales.

NOTA

La imagen ISO de DVD binario es mayor de 4,7 GB, por lo que es posible que no quepa en un DVD de una sola capa. Se recomienda un DVD de doble capa o una llave USB cuando se utilice la imagen ISO de DVD binario para crear medios de instalación de arranque. También puede utilizar la herramienta Image Builder para crear imágenes RHEL personalizadas. Para obtener más información sobre Image Builder, consulte el *Composing a customized RHEL system image* documento.

- Boot ISO: Una imagen ISO de arranque mínima que se utiliza para arrancar en el programa de instalación. Esta opción requiere acceso a los repositorios de BaseOS y AppStream para instalar los paquetes de software. Los repositorios forman parte de la imagen ISO del DVD binario.

Consulte el documento Realización de una instalación estándar de RHEL para obtener instrucciones sobre la descarga de imágenes ISO, la creación de medios de instalación y la finalización de una instalación de RHEL. Para las instalaciones automatizadas de Kickstart y otros temas avanzados, consulte el documento Realización de una instalación avanzada de RHEL.

3.2. REPOSITORIOS

Red Hat Enterprise Linux 8 se distribuye a través de dos repositorios principales:

- BaseOS
- AppStream

Ambos repositorios son necesarios para una instalación básica de RHEL, y están disponibles con todas las suscripciones de RHEL.

El contenido del repositorio de BaseOS está destinado a proporcionar el conjunto básico de la funcionalidad del sistema operativo subyacente que proporciona la base para todas las instalaciones. Este contenido está disponible en el formato RPM y está sujeto a términos de soporte similares a los de las versiones anteriores de RHEL. Para obtener una lista de los paquetes distribuidos a través de BaseOS, consulte el manifiesto de paquetes.

El contenido del repositorio de flujos de aplicaciones incluye aplicaciones adicionales de espacio de usuario, lenguajes de tiempo de ejecución y bases de datos para apoyar las variadas cargas de trabajo y casos de uso. Los flujos de aplicaciones están disponibles en el conocido formato RPM, como una extensión del formato RPM llamada *modules*, o como Colecciones de Software. Para obtener una lista de paquetes disponibles en AppStream, consulte el manifiesto de paquetes.

Además, el repositorio CodeReady Linux Builder está disponible con todas las suscripciones a RHEL. Proporciona paquetes adicionales para el uso de los desarrolladores. Los paquetes incluidos en el repositorio CodeReady Linux Builder no son compatibles.

Para obtener más información sobre los repositorios de RHEL 8, consulte el manifiesto de paquetes.

3.3. FLUJOS DE APLICACIONES

Red Hat Enterprise Linux 8 introduce el concepto de Application Streams. Ahora se entregan y actualizan múltiples versiones de componentes del espacio de usuario con mayor frecuencia que los paquetes del sistema operativo principal. Esto proporciona una mayor flexibilidad para personalizar Red Hat Enterprise Linux sin afectar a la estabilidad subyacente de la plataforma o a implementaciones específicas.

Los componentes disponibles como Application Streams pueden empaquetarse como módulos o paquetes RPM y se entregan a través del repositorio AppStream en RHEL 8. Cada componente de Application Stream tiene un ciclo de vida determinado, ya sea el mismo que el de RHEL 8 o más corto. Para más detalles, consulte Ciclo de vida de Red Hat Enterprise Linux .

Los módulos son colecciones de paquetes que representan una unidad lógica: una aplicación, una pila de lenguajes, una base de datos o un conjunto de herramientas. Estos paquetes se construyen, se prueban y se publican juntos.

Los flujos de módulos representan versiones de los componentes del flujo de aplicaciones. Por ejemplo, hay dos flujos (versiones) del servidor de base de datos PostgreSQL disponibles en el módulo postgresql: PostgreSQL 10 (el flujo por defecto) y PostgreSQL 9.6. Sólo se puede instalar un flujo del módulo en el sistema. Diferentes versiones pueden ser utilizadas en contenedores separados.

Los comandos detallados de los módulos se describen en el documento Instalación, gestión y eliminación de componentes del espacio de usuario. Para obtener una lista de los módulos disponibles en AppStream, consulte el manifiesto de paquetes.

CAPÍTULO 4. LANZAMIENTO DE RHEL 8.3.1

Red Hat hace que el contenido de Red Hat Enterprise Linux 8 esté disponible trimestralmente, entre las versiones menores (8.Y). Las versiones trimestrales se numeran utilizando el tercer dígito (8.Y.1). A continuación se describen las nuevas características de la versión RHEL 8.3.1.

4.1. NUEVAS CARACTERÍSTICAS

Paquetes Flatpak para varias aplicaciones de escritorio

Flatpak es un sistema para ejecutar aplicaciones gráficas como contenedores. Con Flatpak se puede instalar y actualizar una aplicación independientemente del sistema operativo anfitrión.

Esta actualización proporciona imágenes de contenedores Flatpak de las siguientes aplicaciones en el Catálogo de Contenedores de Red Hat:

Nombre de la aplicación	ID del contenedor Flatpak
Firefox	org.mozilla.firefox
GIMP	org.gimp.GIMP
Inkscape	org.inkscape.Inkscape
Thunderbird	org.mozilla.Thunderbird

Para instalar los contenedores Flatpak disponibles en el Catálogo de Contenedores de Red Hat, utilice el siguiente procedimiento:

1. Asegúrese de que la última versión del cliente Flatpak está instalada en su sistema:

```
# yum update flatpak
```

2. Habilitar el repositorio RHEL Flatpak:

```
# flatpak remote-add rhel https://flatpaks.redhat.io/rhel.flatpakrepo
```

3. Proporcione las credenciales de su cuenta RHEL:

```
# podman login registry.redhat.io
```

   Por defecto, Podman guarda las credenciales sólo hasta que el usuario cierra la sesión.

4. Opcional: Guarde sus credenciales de forma permanente:

```
$ cp $XDG_RUNTIME_DIR/containers/auth.json \
    $HOME/.config/flatpak/oci-auth.json
```

5. Instale la imagen del contenedor Flatpak:

```
$ flatpak install rhel container-id
```

(JIRA:RHELPLAN-30958)

Conjunto de herramientas de Rust rebasado a la versión 1.47.0

Rust Toolset ha sido actualizado a la versión 1.47.0. Los cambios más destacados son:

- Las funciones evaluadas en tiempo de compilación **const fn** han sido mejoradas y ahora pueden utilizar funciones de flujo de control, por ejemplo **if**, **while** y **match**.
- La nueva anotación **#[track_caller]** se puede poner ahora en las funciones. Los pánicos de las funciones anotadas informan del llamador como fuente.
- La Biblioteca Estándar de Rust ahora implementa genéricamente traits para arrays de cualquier longitud. Anteriormente, muchas de las implementaciones de traits para arrays sólo se llenaban para longitudes entre 0 y 32.

Para obtener instrucciones detalladas sobre su uso, consulte Uso del conjunto de herramientas de Rust .

(BZ#1883839)

El rol de sistema de registro ahora soporta el filtro basado en propiedades en sus salidas

Con esta actualización, se han añadido filtros basados en propiedades a la salida de archivos, a la salida de forwards y a la salida de remote_files del rol de sistema de registro. La función se proporciona mediante la subfunción **rsyslog**, y es configurable a través de la función de sistema RHEL de registro. Como resultado, los usuarios pueden beneficiarse de la capacidad de filtrar los mensajes de registro por las propiedades, como el nombre de host, la etiqueta, y el propio mensaje es útil para gestionar los registros.

(BZ#1889492)

El rol de sistema RHEL de registro ahora soporta el comportamiento de rsyslog

Con esta mejora, **rsyslog** recibe el mensaje de Red Hat Virtualization y lo reenvía a **elasticsearch**.

(BZ#1889893)

Ya está disponible la imagen del contenedor ubi8/pause

Podman ahora utiliza la imagen del contenedor **ubi8/pause** en lugar de **k8s.gcr.io/pause** para mantener la información del espacio de nombres de red del pod.

(BZ#1690785)

CAPÍTULO 5. CAMBIOS IMPORTANTES EN LOS PARÁMETROS EXTERNOS DEL NÚCLEO

Este capítulo proporciona a los administradores de sistemas un resumen de los cambios significativos en el kernel enviado con Red Hat Enterprise Linux 8.3. Estos cambios pueden incluir, por ejemplo, entradas **proc** añadidas o actualizadas, valores por defecto de **sysctl** y **sysfs**, parámetros de arranque, opciones de configuración del kernel o cualquier cambio de comportamiento notable.

Nuevos parámetros del núcleo

acpi_no_watchdog = [HW,ACPI,WDT]

Este parámetro permite ignorar la interfaz de vigilancia basada en ACPI (Advanced Configuration and Power Interface) y dejar que el controlador nativo controle el dispositivo de vigilancia.

dfltcc = [HW,S390]

Este parámetro configura el soporte de hardware **zlib** para las arquitecturas IBM Z.
Formato: { on | off | def_only | inf_only | always }

Las opciones son:

- **on** (por defecto) - Soporte de hardware IBM Z **zlib** para la compresión en el nivel 1 y la descompresión
- **off** - No hay soporte de hardware IBM Z **zlib**
- **def_only** - Soporte de hardware IBM Z **zlib** sólo para el algoritmo **deflate** (compresión en el nivel 1)
- **inf_only** - Soporte de hardware IBM Z **zlib** sólo para el algoritmo de **inflado** (descompresión)
- **always** - Similar a **on**, pero ignora el nivel de compresión seleccionado y siempre utiliza el soporte de hardware (utilizado para la depuración)

irqchip.gicv3_pseudo_nmi = [ARM64]

Este parámetro permite el soporte de pseudo interrupciones no enmascarables (NMIs) en el kernel. Para utilizar este parámetro es necesario construir el kernel con el elemento de configuración **CONFIG_ARM64_PSEUDO_NMI**.

panic_on_taint =

Máscara de bits para llamar condicionalmente a **panic()** en **add_taint()**
Formato

Una máscara de bits hexadecimal que representa un conjunto de banderas **TAINT** que hará que el kernel entre en pánico cuando se invoque la llamada al sistema **add_taint()** con cualquiera de las banderas de este conjunto. El modificador opcional **nousertaint** evita los bloqueos forzados por el usuario escribiendo en el archivo **/proc/sys/kernel/tainted** cualquier conjunto de banderas que coincida con la máscara de bits de **panic_on_taint**.

Para más información, consulte la documentación de la versión anterior .

prot_virt = [S390]

Formato

Este parámetro permite alojar máquinas virtuales protegidas que están aisladas del hipervisor si el soporte de hardware está presente.

rcutree.use_softirq = [KNL]

Este parámetro permite eliminar el procesamiento **softirq** de Tree-RCU.
Si establece este parámetro a cero, mueve todo el procesamiento de **RCU_SOFTIRQ** a los kthreads rcuc por CPU. Si establece rcutree **.** use_softirq a un valor distinto de cero (por defecto), se utiliza **RCU_SOFTIRQ** por defecto. Especifique rcutree **.use_softirq=0** para utilizar rcuc kthreads.

split_lock_detect = [X86]

Este parámetro habilita la detección de bloqueo dividido. Cuando está habilitado, y si el soporte de hardware está presente, las instrucciones atómicas que acceden a los datos a través de los límites de la línea de caché resultarán en una excepción de comprobación de alineación.
Las opciones son:

- **off** - no habilitado
- **warn** - el kernel emitirá advertencias de tasa limitada sobre las aplicaciones que activen la Excepción de Comprobación de Alineación (#AC). Este modo es el predeterminado en las CPUs que soportan la detección de bloqueos divididos.
- **fatal** - el kernel enviará la señal de error de Buss (SIGBUS) a las aplicaciones que activen la excepción #AC.
  Si la excepción #AC es golpeada mientras no se ejecuta en el modo de usuario, el kernel emitirá un error oops en el modo **warn** o **fatal**.

srbds = [X86,INTEL]

Este parámetro controla la mitigación del muestreo de datos del búfer de registro especial (SRBDS). Ciertas CPUs son vulnerables a un exploit similar al MDS (Microarchitectural Data Sampling) que puede filtrar bits del generador de números aleatorios.

Por defecto, el microcódigo mitiga este problema. Sin embargo, la corrección del microcódigo puede hacer que las instrucciones **RDRAND** y **RDSEED** sean mucho más lentas. Entre otros efectos, esto resultará en una reducción del rendimiento del dispositivo fuente de números aleatorios del kernel **urandom**.

Para desactivar la mitigación del microcódigo, configure la siguiente opción:

- **off** - Desactivar la mitigación y eliminar el impacto en el rendimiento de **RDRAND** y **RDSEED**

svm = [PPC]

Formato: { on | off | y | n | 1 | 0 }
Este parámetro controla el uso de la Facilidad de Ejecución Protegida en los sistemas pSeries.

nopv = [X86,XEN,KVM,HYPER_V,VMWARE]

Este parámetro deshabilita las optimizaciones PV, lo que obliga al huésped a ejecutarse como huésped genérico sin controladores PV.
Actualmente se soportan los huéspedes XEN HVM, KVM, HYPER_V y VMWARE.

Parámetros del núcleo actualizados

hugepagesz = [HW]

Este parámetro especifica un tamaño de página enorme. Utilice este parámetro junto con el parámetro **hugepages** para preasignar un número de páginas enormes del tamaño especificado. Especifique los parámetros **hugepagesz** y **hugepages** en pares como:

```
hugepagesz=2M hugepages=512
```

El parámetro **hugepagesz** sólo puede especificarse una vez en la línea de comandos para un tamaño de página enorme específico. Los tamaños de página enormes válidos dependen de la arquitectura.

hugepages = [HW]

Este parámetro especifica el número de páginas enormes a preasignar. Este parámetro suele seguir al parámetro válido **hugepagesz** o **default_hugepagesz**.
Sin embargo, si **hugepages** es el primer o el único parámetro de la línea de comandos de HugeTLB, especifica implícitamente el número de páginas enormes del tamaño por defecto a asignar. Si el número de páginas enormes del tamaño por defecto se especifica implícitamente, no puede ser sobrescrito por el parámetro **hugepagesz hugepages** para el tamaño por defecto.

Por ejemplo, en una arquitectura con 2M de tamaño de página enorme por defecto:

```
hugepages=256 hugepagesz=2M hugepages=512
```

La configuración del ejemplo anterior da como resultado la asignación de 256 páginas enormes de 2M y un mensaje de advertencia de que el parámetro **hugepages=512** fue ignorado. Si **hugepages** está precedido por **hugepagesz** no válido, **hugepages** será ignorado.

default_hugepagesz = [HW]

Este parámetro especifica el tamaño de la página enorme por defecto. Puede especificar **default_hugepagesz** sólo una vez en la línea de comandos. Opcionalmente, puedes seguir **default_hugepagesz** con el parámetro **hugepages** para preasignar un número específico de páginas enormes del tamaño por defecto. Además, puede especificar implícitamente el número de páginas enormes de tamaño predeterminado que se preasignarán.
Por ejemplo, en una arquitectura con 2M de tamaño de página enorme por defecto:

```
hugepages=256
default_hugepagesz=2M hugepages=256
hugepages=256 default_hugepagesz=2M
```

Las configuraciones del ejemplo anterior dan como resultado la asignación de 256 páginas enormes de 2M. El tamaño válido de la página enorme por defecto depende de la arquitectura.

efi = [EFI]

Formato: {"mapa_antiguo", "nochunk", "noruntime", "debug", "nosoftreserve" }
Las opciones son:

- **old_map** [X86-64] - Cambia a la antigua asignación de servicios de ejecución EFI basada en ioremap. Los 32 bits todavía utilizan éste por defecto
- **nochunk** - Desactivar la lectura de archivos en "chunks" en el stub de arranque EFI, ya que el chunking puede causar problemas con algunas implementaciones de firmware
- **noruntime** - Desactivar el soporte de los servicios de ejecución EFI
- **debug** - Habilitar la salida de depuración miscelánea

- **nosoftreserve** - El atributo **EFI_MEMORY_SP** (Specific Purpose) a veces hace que el kernel reserve el rango de memoria para que un controlador de mapeo de memoria lo reclame. Especifique **efi=nosoftreserve** para deshabilitar esta reserva y tratar la memoria por su tipo base (por ejemplo **EFI_CONVENTIONAL_MEMORY** / \ "System RAM").

intel_iommu = [DMAR]

Controlador Intel IOMMU Reasignación de acceso directo a la memoria (DMAR).
Las opciones añadidas son:

- **nobounce** (por defecto desactivado) - Desactivar el búfer de rebote para los dispositivos que no son de confianza, como los dispositivos Thunderbolt. Esto tratará los dispositivos no confiables como los confiables. Por lo tanto, esta configuración podría exponer los riesgos de seguridad de los ataques de acceso directo a la memoria (DMA).

mem = nn[KMG] [KNL,BOOT]

Este parámetro fuerza el uso de una cantidad específica de memoria.
La cantidad de memoria que se utilizará en los casos siguientes:

1. Para la prueba.
2. Cuando el kernel no es capaz de ver toda la memoria del sistema.
3. La memoria que se encuentra después del límite de **la memoria** se excluye del hipervisor y se asigna a los huéspedes KVM.
   X86] Funciona como la limitación de la dirección máxima. Se utiliza junto con el parámetro **memmap** para evitar colisiones en el espacio de direcciones físicas. Sin **memmap**, los dispositivos de Interconexión de Componentes Periféricos (PCI) podrían colocarse en direcciones pertenecientes a la RAM no utilizada.

   Tenga en cuenta que esta configuración sólo tiene efecto durante el tiempo de arranque, ya que en el caso 3 anterior, la memoria puede necesitar ser añadida en caliente después del arranque si la memoria del sistema del hipervisor no es suficiente.

pci = [PCI]

Varias opciones del subsistema de interconexión de componentes periféricos (PCI).
Algunas de las opciones aquí presentes operan en un dispositivo específico o en un conjunto de dispositivos (**<pci_dev>**). Se especifican en uno de los siguientes formatos:

```
[<domain>:]<bus>:<dev>.<func>[/<dev>.<func>]*
pci:<vendor>:<device>[:<subvendor>:<subdevice>]
```

Tenga en cuenta que el primer formato especifica una dirección de bus/dispositivo/función PCI que puede cambiar si se inserta nuevo hardware, si el firmware de la placa base cambia, o debido a cambios causados por otros parámetros del kernel. Si el dominio se deja sin especificar, se toma como cero. Opcionalmente, se puede especificar una ruta a un dispositivo a través de múltiples direcciones de dispositivo/función después de la dirección base (esto es más robusto contra problemas de renumeración). El segundo formato selecciona los dispositivos usando IDs del espacio de configuración que pueden coincidir con múltiples dispositivos en el sistema.

Las opciones son:

- **hpmmiosize** - La cantidad fija de espacio de bus que se reserva para la ventana de E/S mapeada en memoria (MMIO) del puente hotplug. El tamaño por defecto es de 2 megabytes.

- **hpmmioprefsize** - La cantidad fija de espacio en el bus que se reserva para la ventana MMIO_PREF del puente hotplug. El tamaño por defecto es de 2 megabytes.

pcie_ports = [PCIE]

Manejo de servicios de puertos de interconexión de componentes periféricos (PCIe).
Las opciones son:

- **nativo** - Utiliza los servicios PCIe nativos (PME, AER, DPC, PCIe hotplug) incluso si la plataforma no da permiso al SO para utilizarlos. Esta configuración puede causar conflictos si la plataforma también intenta utilizar estos servicios.
- **dpc-native** - Utiliza el servicio PCIe nativo sólo para DPC. Esta configuración puede causar conflictos si el firmware utiliza AER o DPC.
- **compat** - Desactivar los servicios PCIe nativos (PME, AER, DPC, PCIe hotplug).

rcu_nocbs = [KNL]

El argumento es una lista de CPUs. Se puede utilizar la cadena "all" para especificar cada CPU del sistema.

usbcore.authorized_default = [USB]

La autorización del dispositivo USB por defecto.
Las opciones son:

- -**1** (por defecto) - Autorizado excepto para el USB inalámbrico
- **0** - No autorizado
- **1** - Autorizado
- **2** - Autorizado si el dispositivo está conectado al puerto interno

usbcore.old_scheme_first = [USB]

Este parámetro permite iniciar con el antiguo esquema de inicialización del dispositivo. Este ajuste sólo se aplica a los dispositivos de baja y máxima velocidad (por defecto 0 = desactivado).

usbcore.quirks = [USB]

Una lista de entradas de quirk para aumentar la lista de quirk del núcleo USB incorporada. Las entradas de la lista están separadas por comas. Cada entrada tiene la forma **VendorID:ProductID:Flags**, por ejemplo **quirks=0781:5580:bk,0a5c:5834:gij**. Los **IDs** son números hexadecimales de 4 dígitos y **Flags** es un conjunto de letras. Cada letra cambiará el quirk incorporado; fijándolo si está claro y borrándolo si está fijado.
Las banderas añadidas:

- **o** - **USB_QUIRK_HUB_SLOW_RESET**, el hub necesita un retardo extra después de reiniciar su puerto

Nuevos parámetros de /proc/sys/fs

protected_fifos

Este parámetro se basa en las restricciones del software Openwall y proporciona protección al permitir evitar escrituras involuntarias en un FIFO controlado por el atacante donde un programa pretendía crear un archivo regular.
Las opciones son:

- **0** - La escritura en los FIFOs no tiene restricciones.
- **1** - No permite la apertura de la bandera **O_CREAT** en FIFOs que no poseemos en directorios pegajosos de escritura mundial a menos que sean propiedad del dueño del directorio.
- **2** - Se aplica a los directorios pegajosos con escritura de grupo.

protegido_regular

Este parámetro es similar al parámetro **protected_fifos**, sin embargo, evita que se escriba en un archivo regular controlado por un atacante donde un programa pretendía crear uno.
Las opciones son:

- **0** - La escritura en archivos regulares no tiene restricciones.
- **1** - No permite la apertura de la bandera **O_CREAT** en archivos regulares que no poseemos en directorios pegajosos de escritura mundial a menos que sean propiedad del dueño del directorio.
- **2** - Se aplica a los directorios pegajosos con escritura de grupo.

CAPÍTULO 6. LANZAMIENTO DE RHEL 8.3.0

6.1. NUEVAS CARACTERÍSTICAS

Esta parte describe las nuevas características y las principales mejoras introducidas en Red Hat Enterprise Linux 8.3.

6.1.1. Creación del instalador y de la imagen

Anaconda rebasado a la versión 33.16

Con esta versión, Anaconda se ha reajustado a la versión 33.16. Esta versión proporciona las siguientes mejoras notables con respecto a la versión anterior.

- El programa de instalación muestra ahora las direcciones IPv6 estáticas en varias líneas y ya no cambia el tamaño de las ventanas.
- El programa de instalación muestra ahora los tamaños de sector de los dispositivos NVDIMM compatibles.
- El nombre de host se configura ahora correctamente en un sistema instalado con configuración estática IPv6.
- Ahora puede utilizar caracteres no ASCII en la frase de contraseña de cifrado de disco.
- El programa de instalación muestra una recomendación adecuada para crear un nuevo sistema de archivos en /boot, /tmp, y todos los puntos de montaje /var y /usr excepto /usr/local y /var/www.
- El programa de instalación ahora comprueba correctamente la disposición del teclado y no cambia el estado de la pantalla de disposición del teclado cuando se utilizan las teclas del teclado (ALT SHIFT) para cambiar entre diferentes disposiciones e idiomas.
- El modo de rescate ya no falla en sistemas con particiones RAID1 existentes.
- El cambio de la versión LUKS del contenedor está ahora disponible en la pantalla de **Particionamiento Manual**.
- El programa de instalación finaliza con éxito la instalación sin el paquete **btrfs-progs**.
- El programa de instalación utiliza ahora la versión LUKS2 por defecto para un contenedor encriptado.
- El programa de instalación ya no se bloquea cuando un archivo Kickstart coloca volúmenes físicos (PV) de un grupo de volúmenes lógicos (VG) en una lista de **ignorados**.
- Introduce una nueva ruta de montaje **/mnt/sysroot** para la raíz del sistema. Esta ruta se utiliza para montar / del sistema de destino. Normalmente, la raíz física y la raíz del sistema son la misma, por lo que **/mnt/sysroot** se adjunta al mismo sistema de archivos que **/mnt/sysimage**. Las únicas excepciones son los sistemas rpm-ostree, donde la raíz del sistema cambia en función de la implementación. Entonces, **/mnt/sysroot** se adjunta a un subdirectorio de **/mnt/sysimage**. Se recomienda utilizar **/mnt/sysroot** para el chroot.

(BZ#1691319, BZ#1679893, BZ#1684045, BZ#1688478, BZ#1700450, BZ#1720145, BZ#1723888, BZ#1754977, BZ#1755996, BZ#1784360, BZ#1796310, BZ#1871680)

Cambios en la interfaz gráfica del programa de instalación de RHEL

El programa de instalación de RHEL incluye ahora la siguiente configuración de usuario en la ventana de resumen de la instalación:

- Contraseña de la raíz
- Creación de usuarios

Con este cambio, ahora puede configurar una contraseña de root y crear una cuenta de usuario antes de comenzar la instalación. Anteriormente, se configuraba una contraseña de root y se creaba una cuenta de usuario después de iniciar el proceso de instalación.

La contraseña de root se utiliza para acceder a la cuenta de administrador (también conocida como superusuario o root) que se utiliza para las tareas de administración del sistema. El nombre de usuario se utiliza para iniciar la sesión desde una línea de comandos; si se instala un entorno gráfico, el gestor de inicio de sesión gráfico utiliza el nombre completo. Para más detalles, consulte el *Performing a standard RHEL installation* documento.

(JIRA:RHELPLAN-40469)

El backend de Image Builder **osbuild-composer** sustituye a **lorax-composer**

El backend **osbuild-composer** sustituye a **lorax-composer**. El nuevo servicio proporciona APIs REST para la construcción de imágenes. Como resultado, los usuarios pueden beneficiarse de un backend más fiable y de imágenes de salida más predecibles.

(BZ#1836211)

Image Builder **osbuild-composer** soporta un conjunto de tipos de imágenes

Con el reemplazo del backend de **osbuild-composer**, el siguiente conjunto de tipos de imagen soportados en **osbuild-composer** esta vez:

- Archivo TAR (.tar)
- QEMU QCOW2 (.qcow2)
- Disco de máquina virtual VMware (.vmdk)
- Imagen de la máquina de Amazon (.ami)
- Imagen de disco Azure (.vhd)
- Imagen OpenStack (.qcow2)

Las siguientes salidas no son compatibles esta vez:

- sistema de archivos ext4
- disco particionado
- Nube de Alibaba
- Google GCE

(JIRA:RHELPLAN-42617)

Image Builder ahora soporta el empuje a las nubes a través de la GUI

Con esta mejora, al crear imágenes, los usuarios pueden elegir la opción de empujar a las nubes de servicio **Azure** y **AWS** a través de la GUI **Image Builder**. Como resultado, los usuarios pueden beneficiarse de cargas e instancias más fáciles.

(JIRA:RHELPLAN-30878)

6.1.2. RHEL para Edge

Presentación de las imágenes de RHEL for Edge

Con esta versión, ahora puede crear imágenes RHEL personalizadas para servidores Edge.

Puede utilizar Image Builder para crear imágenes de RHEL for Edge y luego utilizar el instalador de RHEL para desplegarlas en sistemas AMD e Intel de 64 bits. Image Builder genera una imagen de RHEL for Edge como **rhel-edge-commit** en un archivo **.tar**.

Una imagen de RHEL for Edge es una imagen **rpm-ostree** que incluye paquetes del sistema para instalar remotamente RHEL en servidores Edge.

Los paquetes del sistema incluyen:

- Paquete del sistema operativo base
- Podman como motor de contenedores

Puede personalizar la imagen para configurar el contenido del sistema operativo según sus necesidades, y puede desplegarlas en máquinas físicas y virtuales.

Con una imagen de RHEL for Edge, puede lograr lo siguiente:

- Actualizaciones atómicas, en las que se conoce el estado de cada actualización y no se ven los cambios hasta que se reinicia el dispositivo.
- Comprobaciones de estado personalizadas mediante Greenboot y retrocesos inteligentes para la resiliencia en caso de actualizaciones fallidas.
- Flujos de trabajo centrados en los contenedores, en los que puede separar las actualizaciones del sistema operativo principal de las de las aplicaciones, y probar e implantar diferentes versiones de las aplicaciones.
- Cargas útiles OTA optimizadas para entornos con poco ancho de banda.
- Comprobaciones de salud personalizadas mediante Greenboot para garantizar la resistencia.

Para obtener más información sobre la composición, instalación y gestión de imágenes de RHEL for Edge, consulte Composición, instalación y gestión de imágenes de RHEL for Edge .

(JIRA:RHELPLAN-56676)

6.1.3. Gestión del software

El valor por defecto de la opción de configuración best dnf ha sido cambiado de True a False

Con esta actualización, el valor de la **mejor** opción de configuración de dnf se ha establecido en **True** en el archivo de configuración por defecto para mantener el comportamiento original de dnf. Como

resultado, para los usuarios que utilizan el archivo de configuración por defecto el comportamiento permanece sin cambios.

Si proporciona sus propios archivos de configuración, asegúrese de que la opción **best=True** esté presente para conservar el comportamiento original.

(BZ#1832869)

Ahora está disponible la nueva opción --norepopath para el comando dnf reposync

Anteriormente, el comando **reposync** creaba por defecto un subdirectorio bajo el directorio **--download-path** para cada repositorio descargado. Con esta actualización, se ha introducido la opción **--norepopath**, y **reposync** no crea el subdirectorio. Como resultado, el repositorio se descarga directamente en el directorio especificado por **--download-path**. Esta opción también está presente en la página web **YUM v3**.

(BZ#1842285)

Posibilidad de activar y desactivar los plugins de libdnf

Anteriormente, la comprobación de la suscripción estaba codificada en la versión RHEL de los complementos **libdnf**. Con esta actualización, la utilidad **microdnf** puede habilitar y deshabilitar los complementos de **libdnf**, y la comprobación de las suscripciones puede ahora deshabilitarse del mismo modo que en DNF. Para desactivar la comprobación de suscripciones, utilice el comando **--disableplugin=subscription-manager**. Para desactivar todos los complementos, utilice el comando **--noplugins**.

(BZ#1781126)

6.1.4. Shell y herramientas de línea de comandos

Actualizaciones de ReaR

RHEL 8.3 introduce una serie de actualizaciones en la utilidad Relax-and-Recover **(ReaR**). Los cambios más destacados son:

- Se ha añadido la compatibilidad con Rubrik Cloud Data Management (CDM) de terceros como software de copia de seguridad externa. Para utilizarlo, establezca la opción **BACKUP** en el archivo de configuración como **CDM**.
- Se ha habilitado la creación de una imagen de rescate con un archivo mayor de 4 GB en el IBM POWER, arquitectura little endian.
- La distribución de discos creada por **ReaR** ya no incluye entradas para los dispositivos iSCSI y sistemas de archivos de Rancher 2 Longhorn.

(BZ#1743303)

smartmontools rebasado a la versión 7.1

El paquete **smartmontools** ha sido actualizado a la versión 7.1, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Incorporaciones de HDD, SSD y USB a la base de datos de unidades.
- Nuevas opciones **-j** y **--json** para activar el modo de salida JSON.
- Solución a la respuesta incompleta de las subpáginas de **registro** de algunas unidades SSD SAS.

- Mejora del manejo del comando **READ CAPACITY**.
- Varias mejoras para la decodificación de las páginas de registro.

(BZ#1671154)

opencryptoki rebasado a la versión 3.14.0

Los paquetes **opencryptoki** han sido actualizados a la versión 3.14.0, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Mejoras del servicio criptográfico EP11:
  - Apoyo al dilitio
  - Compatibilidad con el algoritmo de firma digital de la curva de Edwards (EdDSA)
  - Compatibilidad con el relleno de cifrado asimétrico óptimo de Rivest-Shamir-Adleman (RSA-OAEP) con una función de generación de máscaras y hash que no sea SHA1
- Bloqueo de procesos e hilos mejorado
- Mejora del **btree** y del bloqueo de objetos
- Soporte para el nuevo hardware IBM Z z15
- Compatibilidad con múltiples instancias de token para el módulo de plataforma de confianza (TPM), la arquitectura criptográfica de IBM (ICA) y la instalación de servicios criptográficos integrados (ICSF)
- Se ha añadido una nueva herramienta **p11sak**, que enumera las claves de los tokens en un repositorio de tokens de **openCryptoki**
- Se ha añadido una utilidad para migrar un repositorio de tokens a un cifrado compatible con FIPS
- Corregida la herramienta **pkcsep11_migrate**
- Correcciones menores del software ICSF

(BZ#1780293)

gpgme rebasado a la versión 1.13.1.

Los paquetes **gpgme** han sido actualizados a la versión 1.13.1. Los cambios notables incluyen:

- Se han introducido los nuevos indicadores de contexto **no-symkey-cache** (tiene efecto cuando se utiliza con GnuPG 2.2.7 o posterior), **request-origin** (tiene efecto cuando se utiliza con GnuPG 2.2.6 o posterior), **auto-key-locate** y **trust-model**.
- Se ha añadido la nueva herramienta **gpgme-json** como servidor de mensajería nativo para navegadores web. A partir de ahora, se soporta el cifrado y descifrado de clave pública.
- Se ha introducido una nueva API de encriptación para soportar la especificación directa de claves, incluyendo la opción de destinatarios ocultos y la toma de claves desde un archivo. Esto también permite el uso de una subclave.

(BZ#1829822)

6.1.5. Servicios de infraestructura

powertop rebasado a la versión 2.12

Los paquetes de **powertop** han sido actualizados a la versión 2.12. Entre los cambios más destacados respecto a la versión 2.11 disponible anteriormente se encuentran:

- Uso de la gestión de energía de la interfaz del dispositivo (DIPM) para el enlace SATA PM.
- Compatibilidad con los sistemas móviles y de sobremesa Intel Comet Lake, el servidor Skylake y la arquitectura Tremont basada en Atom (Jasper Lake).

(BZ#1783110)

reajustado a la versión 2.14.0

Los paquetes **ajustados** han sido actualizados a la versión 2.14.0. Las mejoras más destacadas son:

- Se ha introducido el perfil **optimizar-serial-consola**.
- Se ha añadido la posibilidad de un perfil cargado por correo.
- Se ha añadido el plugin **irqbalance** para manejar los ajustes de **irqbalance**.
- Se ha añadido un ajuste específico de la arquitectura para las plataformas basadas en Marvell ThunderX y AMD.
- El plugin del programador ha sido ampliado para soportar **cgroups-v1** para la configuración de la afinidad de la CPU.

(BZ#1792264)

tcpdump rebasado a la versión 4.9.3

La utilidad **tcpdump** ha sido actualizada a la versión 4.9.3 para corregir las vulnerabilidades y exposiciones comunes (CVE).

(BZ#1804063)

libpcap rebasado a la versión 1.9.1

Los paquetes **libpcap** han sido actualizados a la versión 1.9.1 para corregir las vulnerabilidades y exposiciones comunes (CVE).

(BZ#1806422)

iperf3 ahora soporta la opción sctp en el lado del cliente

Con esta mejora, el usuario puede utilizar el Protocolo de Transmisión de Control de Flujo (SCTP) en lugar del Protocolo de Control de Transmisión (TCP) en el lado del cliente para probar el rendimiento de la red.

Las siguientes opciones para **iperf3** están ahora disponibles en el lado cliente de las pruebas:

- **--sctp**
- **--xbind**
- **--nstreams**

Para obtener más información, consulte **Opciones específicas del cliente** en la página man de **iperf3**.

(BZ#1665142)

iperf3 ahora soporta SSL

Con esta mejora, el usuario puede utilizar la autenticación RSA entre el cliente y el servidor para restringir las conexiones al servidor sólo a los clientes legítimos.

Las siguientes opciones para **iperf3** están ahora disponibles en el lado del servidor:

- **--rsa-private-key-path**
- **--ruta de usuarios autorizados**

Las siguientes opciones para **iperf3** están ahora disponibles en el lado cliente de la comunicación:

- **--nombre de usuario**
- **--rsa-public-key-path**

(BZ#1700497)

bind rebasado a 9.11.20

El paquete **bind** ha sido actualizado a la versión 9.11.20, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Aumento de la fiabilidad en los sistemas con muchos núcleos de CPU mediante la corrección de varias condiciones de carrera.
- Informe detallado de errores: **dig** y otras herramientas pueden ahora imprimir la opción de error de DNS extendido (EDE), si está presente.
- Los ID de los mensajes en las transferencias entrantes del Protocolo de Transferencia de Zona DNS (AXFR) se comprueban y registran cuando son incoherentes.

(BZ#1818785)

Un nuevo perfil TuneD de optimización de consolas serie para reducir la E/S en las consolas serie reduciendo el valor de printk

Con esta actualización, está disponible un nuevo perfil TuneD **de optimización de la consola serie**. En algunos escenarios, los controladores del kernel pueden enviar grandes cantidades de operaciones de E/S a la consola serie. Este comportamiento puede causar una falta de respuesta temporal mientras la E/S se escribe en la consola serie. El perfil **optimize-serial-console** reduce esta E/S bajando el valor de **printk** del valor por defecto de **7 4 1 7** a **4 4 1 7**. Los usuarios con una consola serial que deseen hacer este cambio en su sistema pueden instrumentar su sistema de la siguiente manera:

```
# tuned-adm profile throughput-performance optimize-serial-console
```

Como resultado, los usuarios tendrán un valor de **printk** más bajo que persiste a través de un reinicio, lo que reduce la probabilidad de cuelgues del sistema.

Este perfil de TuneD reduce la cantidad de E/S que se escribe en la consola serie al eliminar la información de depuración. Si necesitas recoger esta información de depuración, debes asegurarte de que este perfil no está habilitado y de que el valor de **printk** está establecido en **7 4 1 7**. Para comprobar el valor de **printk** ejecute:

```
# cat /proc/sys/kernel/printk
```

(BZ#1840689)

Se han añadido nuevos perfiles TuneD para las plataformas basadas en AMD

En RHEL 8.3, el perfil TuneD **de rendimiento** se ha actualizado para incluir el ajuste para las plataformas basadas en AMD. No es necesario cambiar ningún parámetro manualmente y el ajuste se aplica automáticamente en el sistema **AMD**. Los sistemas AMD **Epyc Naples** y **Rome** alteran los siguientes parámetros en el perfil de rendimiento **por** defecto:

sched_migration_cost_ns=5000000 y **kernel.numa_balancing=0**

Con esta mejora, el rendimiento del sistema aumenta en un ~5%.

(BZ#1746957)

memcached rebasado a la versión 1.5.22

Los paquetes de **memcached** han sido actualizados a la versión 1.5.22. Los cambios notables sobre la versión anterior incluyen:

- Se ha activado TLS.
- Se ha eliminado la opción **-o inline_ascii_response**.
- Se ha añadido la opción **-Y [authfile]** junto con el modo de autenticación para el protocolo ASCII.
- **memcached** puede ahora recuperar su caché entre reinicios.
- Se han añadido nuevos meta comandos experimentales.
- Varias mejoras de rendimiento.

(BZ#1809536)

6.1.6. Seguridad

Cyrus SASL admite ahora la vinculación de canales con los complementos SASL/GSSAPI y SASL/GSS-SPNEGO

Esta actualización añade soporte para los enlaces de canal con los complementos **SASL/GSSAPI** y **SASL/GSS-SPNEGO**. Como resultado, cuando se utiliza en las bibliotecas **openldap**, esta característica permite a **Cyrus SASL** mantener la compatibilidad y el acceso a los sistemas de Microsoft Active Directory y Microsoft Windows que están introduciendo la vinculación de canal obligatoria para las conexiones LDAP.

(BZ#1817054)

Libreswan rebasado a 3.32

Con esta actualización, Libreswan ha sido rebasado a la versión 3.32, que incluye varias características nuevas y correcciones de errores. Las características más destacadas son:

- Libreswan ya no requiere una certificación FIPS 140-2 por separado.

- Libreswan ahora implementa las recomendaciones criptográficas del RFC 8247, y cambia la preferencia de SHA-1 y RSA-PKCS v1.5 a SHA-2 y RSA-PSS.
- Libreswan admite interfaces ipsecXX virtuales XFRMi que simplifican la escritura de reglas de cortafuegos.
- Se ha mejorado la recuperación de los nodos accidentados y reiniciados en una red de encriptación de malla completa.

(BZ#1820206)

La librería libssh ha sido rebasada a la versión 0.9.4

La biblioteca **libssh**, que implementa el protocolo SSH, ha sido actualizada a la versión 0.9.4.

Esta actualización incluye correcciones de errores y mejoras, incluyendo:

- Se ha añadido soporte para claves **Ed25519** en archivos PEM.
- Se ha añadido soporte para el algoritmo de intercambio de claves **diffie-hellman-group14-sha256**.
- Se ha añadido soporte para **localuser** en la palabra clave **Match** en el archivo de configuración del cliente **libssh**.
- Los argumentos de las palabras clave de los criterios de**coincidencia** ahora distinguen entre mayúsculas y minúsculas (tenga en cuenta que las palabras clave no distinguen entre mayúsculas y minúsculas, pero los argumentos de las palabras clave sí)
- Se ha corregido CVE-2019-14889 y CVE-2020-1730.
- Se ha añadido soporte para la creación recursiva de los directorios que faltan y que se encuentran en la cadena de ruta proporcionada para el archivo de hosts conocidos.
- Se ha añadido soporte para claves **OpenSSH** en archivos PEM con comentarios y espacios en blanco al principio.
- Se ha eliminado la inclusión de la configuración del servidor **OpenSSH** en la configuración del servidor **libssh**.

(BZ#1804797)

gnutls rebasado a 3.6.14

Los paquetes de **gnutls** han sido reajustados a la versión 3.6.14. Esta versión proporciona muchas correcciones de errores y mejoras, sobre todo:

- **gnutls** ahora rechaza los certificados con campos de **Hora** que contienen caracteres o formato no válidos.
- **gnutls** ahora comprueba los certificados de CA de confianza para los tamaños de clave mínimos.
- Al mostrar una clave privada cifrada, la utilidad **certtool** ya no incluye su descripción en texto plano.
- Los servidores que utilizan **gnutls** ahora anuncian el soporte de OCSP-stapling.
- Los clientes que utilizan **gnutls** ahora envían grapas OCSP sólo a petición.

(BZ#1789392)

las comprobaciones FIPS DH de gnutls ahora son conformes a la norma NIST SP 800-56A rev. 3

Esta actualización de los paquetes **gnutls** proporciona las comprobaciones requeridas por la Publicación Especial 800-56A Revisión 3 del NIST, secciones 5.7.1.1 y 5.7.1.2, paso 2. El cambio es necesario para las futuras certificaciones FIPS 140-2. Como resultado, **gnutls** ahora sólo acepta parámetros de 2048 bits o más de RFC 7919 y RFC 3526 durante el intercambio de claves Diffie-Hellman cuando funciona en modo FIPS.

(BZ#1849079)

gnutls ahora realiza validaciones según NIST SP 800-56A rev 3

Esta actualización de los paquetes **gnutls** añade las comprobaciones requeridas por la Publicación Especial 800-56A Revisión 3 del NIST, secciones 5.6.2.2.2 y 5.6.2.1.3, paso 2. Esta adición prepara a **gnutls** para futuras certificaciones FIPS 140-2. Como resultado, **gnutls** realiza pasos de validación adicionales para las claves públicas generadas y recibidas durante el intercambio de claves Diffie-Hellman cuando funciona en modo FIPS.

(BZ#1855803)

update-crypto-policies y fips-mode-setup movidos a crypto-policies-scripts

Los scripts **update-crypto-policies** y **fips-mode-setup**, que antes se incluían en el paquete **crypto-policies**, se han trasladado a un subpaquete RPM independiente **crypto-policies-scripts**. El paquete se instala automáticamente a través de la dependencia Recommends en las instalaciones regulares. Esto permite que la imagen **ubi8/ubi-minimal** evite la inclusión del intérprete del lenguaje Python y, por lo tanto, reduce el tamaño de la imagen.

(BZ#1832743)

OpenSC se ha actualizado a la versión 0.20.0

El paquete **opensc** ha sido reajustado a la versión 0.20.0 que soluciona múltiples errores y problemas de seguridad. Los cambios más importantes son:

- Con esta actualización, se solucionan los problemas de seguridad de **CVE-2019-6502**, **CVE-2019-15946**, **CVE-2019-15945**, **CVE-2019-19480**, **CVE-2019-19481** y **CVE-2019-19479**.
- El módulo OpenSC soporta ahora las funciones **C_WrapKey** y **C_UnwrapKey**.
- Ahora puede utilizar la instalación para detectar la inserción y extracción de los lectores de tarjetas como se esperaba.
- La utilidad **pkcs11-tool** ahora soporta el atributo **CKA_ALLOWED_MECHANISMS**.
- Esta actualización permite la detección por defecto de las tarjetas **OsEID**.
- La tarjeta OpenPGP v3 ahora soporta **Elliptic Curve Cryptography** (ECC).
- El URI PKCS#11 ahora trunca el nombre del lector con elipsis.

(BZ#1810660)

stunnel rebasado a la versión 5.56

Con esta actualización, la envoltura de encriptación **de stunnel** ha sido rebasada a la versión 5.56, que incluye varias características nuevas y correcciones de errores. Las características más destacadas son:

- Nuevas opciones **ticketKeySecret** y **ticketMacSecret** que controlan la confidencialidad y la protección de la integridad de los tickets de sesión emitidos. Estas opciones permiten reanudar las sesiones en otros nodos de un clúster.
- Nueva opción de **curvas** para controlar la lista de curvas elípticas en OpenSSL 1.1.0 y posteriores.
- Nueva opción de **ciphersuites** para controlar la lista de ciphersuites TLS 1.3 permitidos.
- Se ha añadido **sslVersion**, **sslVersionMin** y **sslVersionMax** para OpenSSL 1.1.0 y posteriores.

(BZ#1808365)

libkcapi rebasado a la versión 1.2.0

El paquete **libkcapi** ha sido rebasado a la versión 1.2.0, que incluye cambios menores.

(BZ#1683123)

setools rebasado a 4.3.0

El paquete **setools**, que es una colección de herramientas diseñadas para facilitar el análisis de políticas de SELinux, ha sido actualizado a la versión 4.3.0.

Esta actualización incluye correcciones de errores y mejoras, incluyendo:

- Método de **sediff** revisado para las reglas de Type Enforcement (TE), que reduce significativamente los problemas de memoria y tiempo de ejecución.
- Se ha añadido soporte de contexto **infiniband** a **seinfo**, **sediff** y **apol**.
- Se ha añadido la configuración de **apol** para la ubicación de la herramienta asistente de Qt utilizada para mostrar la documentación en línea.
- Se han solucionado problemas de **sediff** con:
  - Visualización de la cabecera de las propiedades cuando no se solicita.
  - Comparación de nombres de archivos **type_transition**.
- Corregido el permiso de la dirección del flujo de información de map socket **sendto**.
- Se han añadido métodos a la clase **TypeAttribute** para convertirla en una colección completa de Python.
- **Genfscon** ahora busca las clases, en lugar de utilizar los valores fijos que se eliminaron de **libsepol**.

El paquete **setools** requiere los siguientes paquetes:

- **setools-console**
- **setools-console-analyses**
- **setools-gui**

(BZ#1820079)

Los archivos y directorios individuales de CephFS ahora pueden tener etiquetas SELinux

El sistema de archivos Ceph (CephFS) ha habilitado recientemente el almacenamiento de etiquetas SELinux en los atributos extendidos de los archivos. Anteriormente, todos los archivos de un volumen CephFS estaban etiquetados con una única etiqueta común **system_u:object_r:cephfs_t:s0**. Con esta mejora, se pueden cambiar las etiquetas de los archivos individuales, y SELinux define las etiquetas de los archivos recién creados basándose en reglas de transición. Tenga en cuenta que los archivos no etiquetados previamente siguen teniendo la etiqueta system_u:object_r: **cephfs_t**:s0 hasta que se cambie explícitamente.

(BZ#1823764)

OpenSCAP rebasado a la versión 1.3.3

Los paquetes de **openscap** se han actualizado a la versión 1.3.3, que proporciona muchas correcciones de errores y mejoras con respecto a la versión anterior, sobre todo:

- Se ha añadido el script **autotailor** que permite generar archivos de adaptación mediante una interfaz de línea de comandos (CLI).
- Se ha añadido la parte de la zona horaria al formato de descripción de la lista de control de configuración extensible (XCCDF)
- Se ha añadido la sonda independiente **yamlfilecontent** como borrador de implementación.
- Introducido el tipo **urn:xccdf:fix:script:kubernetes** fix en XCCDF.
- Se ha añadido la posibilidad de generar la configuración de **la máquina**.
- La herramienta **oscap-podman** ahora puede detectar objetivos de exploración ambiguos.
- La sonda **rpmverifyfile** ahora puede verificar archivos del directorio **/bin**.
- Se han corregido los fallos cuando se ejecutan regexes complicadas en la sonda **textfilecontent58**.
- Las características de evaluación del informe XCCDF son ahora consistentes con las entidades OVAL de la sonda **system_info**.
- Se ha corregido la coincidencia de patrones de rutas de archivos en el modo sin conexión en la sonda **textfilecontent58**.
- Corregida la recursión infinita en la sonda **systemdunitdependency**.

(BZ#1829761)

La guía de seguridad de SCAP ofrece ahora un perfil alineado con el benchmark de CIS RHEL 8 v1.0.0

Con esta actualización, los paquetes **scap-security-guide** proporcionan un perfil alineado con el CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0. El perfil le permite endurecer la configuración del sistema utilizando las directrices del Center for Internet Security (CIS). Como resultado, puede configurar y automatizar el cumplimiento de sus sistemas RHEL 8 con CIS utilizando el Ansible Playbook de CIS y el perfil SCAP de CIS.

Tenga en cuenta que la regla **rpm_verify_permissions** del perfil CIS no funciona correctamente.

(BZ#1760734)

scap-security-guide proporciona ahora un perfil que implementa la HIPAA

Esta actualización de los paquetes **scap-security-guide** añade el perfil de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) al contenido de cumplimiento de seguridad de RHEL 8. Este perfil implementa las recomendaciones que se indican en el sitio web The HIPAA Privacy Rule.

La regla de seguridad de la HIPAA establece normas nacionales para proteger la información médica personal electrónica de los individuos que es creada, recibida, utilizada o mantenida por una entidad cubierta. La Regla de Seguridad exige que se adopten las salvaguardias administrativas, físicas y técnicas adecuadas para garantizar la confidencialidad, integridad y seguridad de la información sanitaria protegida electrónicamente.

(BZ#1832760)

scap-security-guide rebasado a 0.1.50

Los paquetes **scap-security-guide**, que contienen el último conjunto de políticas de seguridad para sistemas Linux, han sido actualizados a la versión 0.1.50.

Esta actualización incluye correcciones de errores y mejoras, sobre todo:

- El contenido de Ansible ha sido mejorado: numerosas reglas contienen remedios de Ansible por primera vez y otras reglas han sido actualizadas para abordar correcciones de errores.
- Correcciones y mejoras en el contenido de **scap-security-guide** para el escaneo de sistemas RHEL7, incluyendo:
  - Los paquetes **scap-security-guide** ahora proporcionan un perfil alineado con el CIS RHEL 7 Benchmark v2.2.0. Note que la regla **rpm_verify_permissions** en el perfil CIS no funciona correctamente; vea el problema conocido **rpm_verify_permissions** fails in the CIS profile.
  - Los perfiles de la Guía de Seguridad SCAP ahora desactivan y enmascaran correctamente los servicios que no deben iniciarse.
  - La regla **audit_rules_privileged_commands** de los paquetes **scap-security-guide** ahora funciona correctamente para los comandos privilegiados.
  - La corrección de la regla **dconf_gnome_login_banner_text** en los paquetes **scap-security-guide** ya no falla incorrectamente.

(BZ#1815007)

SCAP Workbench puede ahora generar remedios basados en resultados a partir de perfiles adaptados

Con esta actualización, ahora puede generar funciones de corrección basadas en resultados a partir de perfiles adaptados mediante la herramienta **SCAP Workbench**.

(BZ#1640715)

El nuevo rol de Ansible proporciona despliegues automatizados de los clientes de Clevis

Esta actualización del paquete **rhel-system-roles** introduce el rol de sistema **nbde_client** RHEL. Este rol de Ansible permite desplegar múltiples clientes Clevis de forma automatizada.

(BZ#1716040)

El nuevo rol de Ansible ahora puede configurar un servidor Tang

Con esta mejora, puede desplegar y gestionar un servidor Tang como parte de una solución automatizada de cifrado de discos con el nuevo rol de sistema **nbde_server**. El rol de Ansible **nbde_server**, que se incluye en el paquete **rhel-system-roles**, admite las siguientes funciones:

- Llaves Tang giratorias
- Despliegue y copia de seguridad de las llaves Tang

Para más información, véase Rotación de las llaves del servidor Tang .

(BZ#1716039)

lahorquilla se ha reajustado a la versión 13

Los paquetes de **la clevis** han sido reajustados a la versión 13, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- el**desbloqueo de la horquilla** se puede utilizar en el dispositivo con un archivo de claves en el modo no interactivo.
- **clevis encrypt tpm2** analiza el campo **pcr_ids** si la entrada se da como una matriz JSON.
- La página man de **clevis-luks-unbind(1)** ya no se refiere sólo a LUKS v1.
- **clevis luks bind** ya no escribe en una ranura inactiva, si la contraseña dada es incorrecta.
- **clevis luks bind** ahora funciona mientras el sistema utiliza la configuración regional no inglesa.
- Se ha añadido soporte para **tpm2-tools** 4.x.

(BZ#1818780)

laedición de las horquillas le permite editar una configuración específica de las clavijas

Esta actualización de los paquetes **clevis** introduce el nuevo subcomando **clevis luks edit** que permite editar una configuración de pines específica. Por ejemplo, ahora puede cambiar la dirección URL de un servidor Tang y el parámetro **pcr_ids** en una configuración TPM2. También puede añadir y eliminar nuevos pines **sss** y cambiar el umbral de un pin **sss**.

(BZ#1436735)

clevis luks bind -y ahora permite la vinculación automática

Con esta mejora, Clevis admite la vinculación automática con el parámetro **-y**. Ahora puede utilizar la opción **-y** con el comando clevis **luks bind**, que responde automáticamente a las indicaciones posteriores con *yes*. Por ejemplo, cuando se utiliza un pin Tang, ya no es necesario confiar manualmente en las claves Tang.

(BZ#1819767)

fapolicyd rebasado a la versión 1.0

Los paquetes **fapolicyd** han sido reajustados a la versión 1.0, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Se ha resuelto el problema de la sincronización de múltiples hilos.

- Mejora del rendimiento con una reducción del tamaño de la base de datos y del tiempo de carga.
- Se ha añadido una nueva opción de confianza para el paquete **fapolicyd** en el archivo **fapolicyd.conf** para personalizar el back end de confianza. Puedes añadir todos los archivos, binarios y scripts de confianza al nuevo archivo **/etc/fapolicyd/fapolicyd.trust**.
- Puede gestionar el archivo **fapolicyd.** trust mediante la CLI.
- Puede limpiar o volcar la base de datos utilizando la CLI.
- El paquete **fapolicyd** anula la base de datos mágica para una mejor decodificación de los scripts. La CLI imprime el tipo MIME del archivo similar al comando file según la anulación.
- El archivo **/etc/fapolicyd/fapolicyd.** rules admite un grupo de valores como valores de atributos.
- El demonio **fapolicyd** tiene una opción **syslog_format** para establecer el formato de los eventos de **auditoría/sylog**.

(BZ#1817413)

fapolicyd proporciona ahora su propia política SELinux en fapolicyd-selinux

Con esta mejora, el marco **fapolicyd** ahora proporciona su propia política de seguridad SELinux. El demonio está confinado bajo el dominio **fapolicyd_t** y la política se instala a través del subpaquete **fapolicyd-selinux**.

(BZ#1714529)

USBGuard rebasado a la versión 0.7.8

Los paquetes **usbguard** han sido reajustados a la versión 0.7.8 que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- El parámetro **HidePII=true|false** en el archivo **/etc/usbguard/usbguard-daemon.** conf ahora puede ocultar la información de identificación personal de las entradas de auditoría.
- El parámetro **AuthorizedDefault=keep|none|all|internal** en el archivo **/etc/usbguard/usbguard-daemon.** conf puede predefinir el estado de autorización de los dispositivos del controlador.
- Con el nuevo atributo de regla **with-connect-type**, los usuarios pueden ahora distinguir el tipo de conexión del dispositivo.
- Ahora los usuarios pueden añadir reglas temporales con la opción **-t**. Las reglas temporales permanecen en la memoria sólo hasta que el demonio se reinicia.
- ahora**usbguard list-rules** puede filtrar las reglas según ciertas propiedades.
- **usbguard generate-policy** ahora puede generar una política para dispositivos específicos.
- El comando **usbguard allow|block|reject** ahora puede manejar cadenas de reglas, y se aplica un objetivo en cada dispositivo que coincida con la cadena de reglas especificada.
- Se incluyen los nuevos subpaquetes **usbguard-notifier** y **usbguard-selinux**.

(BZ#1738590)

USBGuard proporciona muchas mejoras para los usuarios de escritorios corporativos

Esta adición al proyecto USBGuard contiene mejoras y correcciones de errores para mejorar la usabilidad para los usuarios de escritorios corporativos. Los cambios importantes incluyen:

- Para mantener limpio el archivo de reglas **/etc/usbguard/rules.conf**, los usuarios pueden definir varios archivos de configuración dentro del directorio **RuleFolder=/etc/usbguard/rules.d/**. Por defecto, el *RuleFolder* se especifica en el archivo **/etc/usbguard-daemon.** conf.
- La herramienta **usbguard-notifier** ahora proporciona notificaciones en la interfaz gráfica de usuario. La herramienta notifica al usuario cada vez que un dispositivo se conecta o desconecta y si el dispositivo está permitido, bloqueado o rechazado por cualquier usuario.
- Ahora puede incluir comentarios en los archivos de configuración, porque el **demonio usbguard** ya no analiza las líneas que comienzan con **#**.

(BZ#1667395)

USBGuard proporciona ahora su propia política SELinux en usbguard-selinux

Con esta mejora, el marco **USBGuard** ahora proporciona su propia política de seguridad SELinux. El demonio está confinado bajo el dominio **usbguard_t** y la política se instala a través del subpaquete **usbguard-selinux**.

(BZ#1683567)

libcap ahora es compatible con las capacidades ambientales

Con esta actualización, los usuarios pueden conceder capacidades de ambiente en el inicio de sesión y evitar la necesidad de tener acceso de root para los procesos debidamente configurados.

(BZ#1487388)

La librería libseccomp ha sido rebasada a la versión 2.4.3

La biblioteca **libseccomp**, que proporciona una interfaz para el mecanismo de filtrado de llamadas del sistema **seccomp**, se ha actualizado a la versión 2.4.3.

Esta actualización proporciona numerosas correcciones de errores y mejoras. Los cambios más destacados son:

- Actualizada la tabla de **syscall** para Linux v5.4-rc4.
- Ya no se definen los valores de **__NR_x** para las llamadas al sistema que no existen.
- **__SNR_x** se utiliza ahora internamente.
- Se ha añadido **una definición** para **__SNR_ppoll**.
- Se ha corregido un problema de multiplexación con las llamadas al sistema s390/s390x shm*.
- Se ha eliminado la bandera **estática** de la compilación de las herramientas **libseccomp**.
- Se ha añadido soporte para las llamadas al sistema relacionadas con **io-uring**.
- Se ha corregido el problema de nomenclatura del módulo de Python introducido en la versión v2.4.0; el módulo se llama **seccomp** como antes.

- Se ha corregido una posible fuga de memoria identificada por **clang** en la herramienta **scmp_bpf_sim**.

(BZ#1770693)

el móduloomamqp1 ya es compatible

Con esta actualización, el protocolo **AMQP 1.** 0 soporta el envío de mensajes a un destino en el bus. Anteriormente, Openstack utilizaba el protocolo **AMQP1** como estándar de comunicación, y este protocolo ahora puede registrar mensajes en mensajes AMQP. Esta actualización introduce el subpaquete **rsyslog-omamqp1** para ofrecer el modo de salida **omamqp1**, que registra los mensajes y los envía al destino en el bus.

(BZ#1713427)

OpenSCAP comprime el contenido remoto

Con esta actualización, OpenSCAP utiliza la compresión **gzip** para transferir el contenido remoto. El tipo más común de contenido remoto son los feeds de CVE basados en texto, que aumentan de tamaño con el tiempo y normalmente tienen que descargarse para cada exploración. La compresión **gzip** reduce el ancho de banda al 10% del necesario para el contenido sin comprimir. Como resultado, se reducen los requisitos de ancho de banda en toda la cadena entre el sistema escaneado y el servidor que aloja el contenido remoto.

(BZ#1855708)

La guía de seguridad de SCAP proporciona ahora un perfil alineado con NIST-800-171

Con esta actualización, los paquetes **scap-security-guide** proporcionan un perfil alineado con la norma NIST-800-171. El perfil le permite endurecer la configuración del sistema de acuerdo con los requisitos de seguridad para la protección de la información no clasificada controlada (CUI) en los sistemas de información no federales. Como resultado, puede configurar más fácilmente los sistemas para que estén alineados con la norma NIST-800-171.

(BZ#1762962)

6.1.7. Red

Los módulos de seguimiento de conexiones IPv4 e IPv6 se han fusionado en el módulo nf_conntrack

Esta mejora fusiona los módulos de seguimiento de conexiones **nf_conntrack_ipv4** y **nf_conntrack_ipv6** de Netfilter en el módulo del núcleo **nf_conntrack**. Debido a este cambio, la inclusión en la lista negra de los módulos específicos de la familia de direcciones ya no funciona en RHEL 8.3, y se puede incluir en la lista negra sólo el módulo **nf_conntrack** para desactivar el soporte de seguimiento de conexiones para los protocolos IPv4 e IPv6.

(BZ#1822085)

firewalld rebasado a la versión 0.8.2

Los paquetes **firewalld** han sido actualizados a la versión 0.8.2, que proporciona una serie de correcciones de errores respecto a la versión anterior. Para más detalles, consulte las notas de la versión 0.8.2 de firewalld.

(BZ#1809636)

NetworkManager se ha actualizado a la versión 1.26.0

Los paquetes de **NetworkManager** han sido actualizados a la versión 1.26.0, que proporciona una serie de mejoras y correcciones de errores con respecto a la versión anterior:

- NetworkManager restablece la configuración de autonegociación, velocidad y dúplex a su valor original al desactivar un dispositivo.
- Los perfiles Wi-Fi se conectan ahora automáticamente si fallan todos los intentos de activación anteriores. Esto significa que un fallo inicial en la conexión automática a la red ya no bloquea el automatismo. Un efecto secundario es que los perfiles Wi-Fi existentes que antes estaban bloqueados ahora se conectan automáticamente.
- Se han añadido las páginas de manual **nm-settings-nmcli (5**) y **nm-settings-dbus(5)**.
- Se ha añadido soporte para una serie de parámetros de puente.
- Se ha añadido soporte para interfaces de enrutamiento y reenvío virtual (VRF). Para más detalles, consulte Reutilización permanente de la misma dirección IP en diferentes interfaces .
- Se ha añadido la compatibilidad con el modo de cifrado inalámbrico oportunista (OWE) para redes Wi-Fi.
- NetworkManager admite ahora prefijos de 31 bits en los enlaces punto a punto de IPv4 según el RFC 3021.
- La utilidad **nmcli** ahora soporta la eliminación de configuraciones usando la **conexión nmcli modificar**
- NetworkManager ya no crea ni activa dispositivos esclavos si falta un dispositivo maestro.

Para más información sobre los cambios notables, lea las notas de la versión anterior:

- NetworkManager 1.26.0
- NetworkManager 1.24.0

(BZ#1814746)

El XDP es compatible de forma condicional

Red Hat admite la función eXpress Data Path (XDP) sólo si se dan todas las condiciones siguientes:

- Usted carga el programa XDP en una arquitectura AMD o Intel de 64 bits
- Se utiliza la biblioteca **libxdp** para cargar el programa en el kernel
- El programa XDP utiliza uno de los siguientes códigos de retorno: **XDP_ABORTED**, **XDP_DROP**, o **XDP_PASS**
- El programa XDP no utiliza la descarga de hardware XDP

Para más detalles sobre las funciones XDP no soportadas, consulte Resumen de las funciones XDP que están disponibles como Muestra de Tecnología

(BZ#1889736)

xdp-tools es totalmente compatible

El paquete **xdp-tools**, que contiene utilidades de apoyo al espacio de usuario para la función eXpress

Data Path (XDP) del kernel, es ahora compatible con las arquitecturas de 64 bits de AMD e Intel. Incluye la biblioteca **libxdp**, la utilidad **xdp-loader** para cargar programas XDP, el programa de ejemplo **xdp-filter** para filtrar paquetes y la utilidad **xdpdump** para capturar paquetes de una interfaz de red con XDP activado.

(BZ#1820670)

La utilidad dracut por defecto ahora utiliza NetworkManager en el disco RAM inicial

Anteriormente, la utilidad **dracut** utilizaba un script de shell para gestionar la red en el disco RAM inicial, **initrd**. En ciertos casos, esto podía causar problemas. Por ejemplo, el NetworkManager envía otra solicitud de DHCP, incluso si el script en el disco RAM ya ha solicitado una dirección IP, lo que podría resultar en un tiempo de espera.

Con esta actualización, el **dracut** por defecto ahora utiliza el NetworkManager en el disco RAM inicial y evita que el sistema tenga problemas. En caso de que quieras volver a la implementación anterior, y recrear las imágenes del disco RAM, utiliza los siguientes comandos:

```
# echo 'add_dracutmodules+=" network-legacy "' > /etc/dracut.conf.d/enable-network-legacy.conf

# dracut -vf --regenerate-all
```

(BZ#1626348)

La configuración de la red en la línea de comandos del kernel se ha consolidado bajo el parámetro ip

Los parámetros **ipv6**, **máscara de red**, **puerta de enlace** y **nombre de host** para establecer la configuración de red en la línea de comandos del kernel se han consolidado bajo el parámetro **ip**. El parámetro **ip** acepta diferentes formatos, como el siguiente:

```
ip=__IP_address__:__peer__:__gateway_IP_address__:__net_mask__:__host_name__:__interface_name__:__configuration_method__
```

Para más detalles sobre los campos individuales y otros formatos que acepta este parámetro, consulte la descripción del parámetro **ip** en la página man de **dracut.cmdline(7)**.

Los parámetros **ipv6**, **máscara de red**, **puerta de enlace** y **nombre de host** ya no están disponibles en RHEL 8.

(BZ#1905138)

6.1.8. Núcleo

Versión del núcleo en RHEL 8.3

Red Hat Enterprise Linux 8.3 se distribuye con la versión 4.18.0-240 del kernel.

(BZ#1839151)

Filtro de paquetes Berkeley ampliado para RHEL 8.3

La **Extended Berkeley Packet Filter (eBPF)**es una máquina virtual dentro del núcleo que permite la ejecución de código en el espacio del núcleo, en el entorno restringido de la caja de arena con acceso a un conjunto limitado de funciones. La máquina virtual ejecuta un código especial de tipo ensamblador.

El bytecode de **eBPF** se carga primero en el kernel, seguido de su verificación, la traducción del código al código máquina nativo con compilación just-in-time, y luego la máquina virtual ejecuta el código.

Red Hat suministra numerosos componentes que utilizan la máquina virtual **eBPF**. Cada componente se encuentra en una fase de desarrollo diferente y, por lo tanto, no todos los componentes están actualmente soportados. En RHEL 8.3, los siguientes componentes de **eBPF** están soportados:

- El paquete de herramientas **BPF Compiler Collection (BCC)**, que proporciona herramientas para el análisis de E/S, la creación de redes y la supervisión de sistemas operativos Linux mediante **eBPF**
- La biblioteca **BCC** que permite el desarrollo de herramientas similares a las proporcionadas en el paquete de herramientas **BCC**.
- La función **eBPF for Traffic Control (tc)** que permite el procesamiento programable de paquetes dentro de la ruta de datos de la red del núcleo.
- La función **eXpress Data Path (XDP)**, que proporciona acceso a los paquetes recibidos antes de que la pila de red del kernel los procese, está soportada bajo condiciones específicas. Para más detalles, consulte la sección de redes de las Notas de Relase.
- El paquete **libbpf**, que es crucial para las aplicaciones relacionadas con bpf como **bpftrace** y el desarrollo de **bpf/xdp**. Para más detalles, consulte la nota de la versión dedicada libbpf fully supported.
- El paquete **xdp-tools**, que contiene utilidades de apoyo al espacio de usuario para la función **XDP**, es ahora compatible con las arquitecturas de 64 bits de AMD e Intel. Para más detalles, consulte la sección de redes de las Notas de la versión.

Tenga en cuenta que todos los demás componentes de **eBPF** están disponibles como Technology Preview, a menos que se indique que un componente específico es compatible.

Los siguientes componentes notables de **eBPF** están actualmente disponibles como Technology Preview:

- El lenguaje de rastreo **bpftrace**
- La toma **AF_XDP** para conectar la ruta **eXpress Data Path (XDP)** al espacio de usuario

Para más información sobre los componentes de la Previsión Tecnológica, véase Previsiones Tecnológicas.

(BZ#1780124)

Software de host de la arquitectura Omni-Path (OPA) de Cornelis Networks

El software de host Omni-Path Architecture (OPA) es totalmente compatible con Red Hat Enterprise Linux 8.3. OPA proporciona hardware Host Fabric Interface (HFI) con inicialización y configuración para transferencias de datos de alto rendimiento (alto ancho de banda, alta tasa de mensajes, baja latencia) entre nodos de computación y E/S en un entorno de clúster.

Para obtener instrucciones sobre la instalación de la arquitectura Omni-Path, consulte el archivo Intel® Omni-Path Fabric Software Release Notes.

(BZ#1893174)

TSX está ahora desactivado por defecto

A partir de RHEL 8.3, el kernel tiene ahora la tecnología **Intel® Transactional Synchronization Extensions (TSX)** deshabilitada por defecto para mejorar la seguridad del sistema operativo. El cambio se aplica a las CPU que admiten la desactivación de **TSX**, incluidos los procesadores escalables Intel® Xeon® de segunda generación (antes conocidos como Cascade Lake con los chipsets de la serie Intel® C620).

Para los usuarios cuyas aplicaciones no utilizan **TSX**, el cambio elimina la penalización de rendimiento por defecto de las mitigaciones de **TSX Asynchronous Abort (TAA)** en los procesadores escalables Intel® Xeon® de segunda generación.

El cambio también alinea el comportamiento del kernel de RHEL con el de upstream, donde **TSX** está desactivado por defecto desde Linux 5.4.

Para activar **TSX**, añada el parámetro **tsx=on** a la línea de comandos del kernel.

(BZ#1828642)

RHEL 8.3 ahora soporta la función de seguimiento del propietario de la página

Con esta actualización, puede utilizar la función de seguimiento del propietario de la página para observar la utilización de la memoria del kernel a nivel de asignación de la página.

Para activar el rastreador de páginas, ejecute los siguientes pasos:

```
# grubby --args="page_owner=on" --update-kernel=0
# reboot
```

Como resultado, el rastreador de propietarios de páginas rastreará el consumo de memoria del kernel, lo que ayuda a depurar las fugas de memoria del kernel y a detectar los controladores que utilizan mucha memoria.

(BZ#1825414)

Ahora se admite EDAC para los procesadores AMD EPYC™ serie 7003

Esta mejora proporciona compatibilidad con el dispositivo de detección y corrección de errores (EDAC) para los procesadores AMD EPYC™ serie 7003. Anteriormente, los errores de memoria corregidos (CE) y no corregidos (UE) no se informaban en los sistemas basados en los procesadores AMD EPYC™ serie 7003. Con esta actualización, estos errores ahora se informarán mediante EDAC.

(BZ#1735611)

Flamegraph es ahora compatible con la herramienta perf

Con esta actualización, la herramienta de línea de comandos **perf** soporta flamegraphs para crear una representación gráfica del rendimiento del sistema. Los datos **de** perf se agrupan en muestras con backtraces de pila similares. Como resultado, estos datos se convierten en una representación visual para permitir una identificación más fácil de las áreas de código que hacen un uso intensivo de los cálculos. Para generar un flamegraph utilizando la herramienta **perf**, ejecute los siguientes comandos:

```
$ perf script record flamegraph -F 99 -g -- stress --cpu 1 --vm-bytes 128M --timeout 10s
stress: info: [4461] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
stress: info: [4461] successful run completed in 10s
[ perf record: Woken up 1 times to write data ]
[ perf record: Captured and wrote 0.060 MB perf.data (970 samples) ]
$ perf script report flamegraph
dumping data to flamegraph.html
```

Nota : Para generar flamegraphs, instale el rpm **js-d3-flame-graph**.

(BZ#1281843)

/dev/random y /dev/urandom son ahora alimentados condicionalmente por el Kernel Crypto API DRBG

En el modo FIPS, los generadores de números pseudoaleatorios **/dev/random** y **/dev/urandom** se alimentan del generador de bits aleatorios determinista (DRBG) de la Kernel Crypto API. Las aplicaciones en modo FIPS utilizan los dispositivos mencionados como fuente de ruido conforme a FIPS, por lo que los dispositivos deben emplear algoritmos aprobados por FIPS. Para lograr este objetivo, se han añadido los ganchos necesarios al controlador **/dev/random**. Como resultado, los ganchos están habilitados en el modo FIPS y hacen que **/dev/random** y **/dev/urandom** se conecten al DRBG de la API Crypto del núcleo.

(BZ#1785660)

libbpf es totalmente compatible

El paquete **libbpf**, crucial para las aplicaciones relacionadas con bpf como **bpftrace** y el desarrollo de **bpf/xdp**, es ahora totalmente compatible.

Es una réplica del árbol de linux **bpf-next** directorio **bpf-next/tools/lib/bpf** más sus archivos de cabecera de apoyo. La versión del paquete refleja la versión de la interfaz binaria de aplicación (ABI).

(BZ#1759154)

la utilidadlshw proporciona ahora información adicional sobre la CPU

Con esta mejora, la utilidad List Hardware (*lshw*) muestra más información sobre la CPU. El campo de la **versión de** la CPU proporciona ahora los detalles de la familia, el modelo y el paso de los procesadores del sistema en formato numérico como **versión**

(BZ#1794049)

el árbol de fuentes dekernel-rt ha sido actualizado al árbol de RHEL 8.3

Las fuentes de **kernel-rt** han sido actualizadas para utilizar el último árbol de fuentes del kernel de Red Hat Enterprise Linux. El conjunto de parches en tiempo real también se ha actualizado a la última versión de la corriente principal, v5.6.14-rt7. Ambas actualizaciones proporcionan una serie de correcciones de errores y mejoras.

(BZ#1818138, BZ#18142)

tpm2-tools rebasado a la versión 4.1.1

El paquete **tpm2-tools** se ha actualizado a la versión 4.1.1, que proporciona una serie de adiciones, actualizaciones y eliminaciones de comandos. Para obtener más detalles, consulte las actualizaciones del paquete tpm2-tools en la solución RHEL8.3.

(BZ#1789682)

El adaptador de red Mellanox ConnectX-6 Dx es ahora totalmente compatible

Esta mejora añade los IDs PCI del adaptador de red Mellanox ConnectX-6 Dx al controlador **mlx5_core**. En los hosts que utilizan este adaptador, RHEL carga el controlador **mlx5_core** automáticamente. Esta función, que anteriormente estaba disponible como vista previa de la tecnología, es ahora totalmente compatible con RHEL 8.3.

(BZ#1782831)

controladormlxsw rebasado a la versión 5.7

El **controlador mlxsw** se ha actualizado a la versión 5.7 e incluye las siguientes novedades:

- La función de ocupación del búfer compartido, que proporciona datos de ocupación del búfer.
- La función de caída de paquetes, que permite supervisar las caídas de **capa 2**, **capa 3**, **túneles** y **listas de control de** acceso.
- Apoyo a las trampas de paquetes.
- Soporte para la configuración de la prioridad de los puertos por defecto mediante el agente del Protocolo de Descubrimiento de la Capa de Enlace (LLDP).
- Selección de transmisión mejorada (ETS) y compatibilidad con la disciplina de descarga de colas del filtro de cubos de fichas (TBF).
- El modo de **nodrop de** la disciplina de colas RED está activado para evitar la caída temprana de paquetes.
- La acción de edición de la clase de tráfico SKB **skbedit** priority permite cambiar los metadatos de los paquetes y se complementa con **pedit** Traffic Class Offloading (TOS).

(BZ#1821646)

6.1.9. Sistemas de archivos y almacenamiento

LVM ahora puede gestionar volúmenes VDO

LVM ahora soporta el tipo de segmento Virtual Data Optimizer (VDO). Como resultado, ahora puede utilizar las utilidades de LVM para crear y gestionar volúmenes VDO como volúmenes lógicos nativos de LVM.

VDO ofrece funciones de deduplicación en línea a nivel de bloque, compresión y aprovisionamiento ligero.

Para más información, consulte Deduplicar y comprimir volúmenes lógicos en RHEL .

(BZ#1598199)

La pila SCSI ahora funciona mejor con los adaptadores de alto rendimiento

Se ha mejorado el rendimiento de la pila SCSI. Como resultado, los adaptadores de bus de host (HBA) de última generación y alto rendimiento son ahora capaces de alcanzar mayores IOPS (E/S por segundo) en RHEL.

(BZ#1761928)

El controlador megaraid_sas ha sido actualizado a la última versión

El controlador **megaraid_sas** ha sido actualizado a la versión 07.713.01.00-rc1. Esta actualización proporciona varias correcciones de errores y mejoras relacionadas con la mejora del rendimiento, una mayor estabilidad de los adaptadores MegaRAID compatibles y un conjunto de funciones más completo.

(BZ#1791041)

Stratis ahora muestra el nombre de la piscina en caso de error

Cuando se intenta crear un pool de Stratis en un dispositivo de bloque que ya está en uso por un pool de Stratis existente, la utilidad **stratis** ahora reporta el nombre del pool existente. Anteriormente, la utilidad sólo indicaba la etiqueta UUID del pool.

(BZ#1734496)

FPIN Soporte de notificación de tramas ELS

El controlador **lpfc** Fibre Channel (FC) admite ahora las notificaciones de impacto en el rendimiento del tejido (FPIN) relativas a la integridad del enlace, que ayudan a identificar los problemas a nivel de enlace y permiten al conmutador elegir una ruta más fiable.

(BZ#1796565)

Nuevos comandos para depurar los metadatos en disco de LVM

La utilidad **pvck**, que está disponible en el paquete **lvm2**, ahora proporciona comandos de bajo nivel para depurar o rescatar los metadatos en disco de LVM en volúmenes físicos:

- Para extraer los metadatos, utilice el comando **pvck --dump**.
- Para reparar los metadatos, utilice el comando **pvck --repair**.

Para más información, consulte la página man de **pvck(8)**.

(BZ#1541165)

LVM RAID admite la integridad de DM para evitar la pérdida de datos debido a los datos corruptos en un dispositivo

Ahora es posible añadir la integridad de Device Mapper (DM) a una configuración RAID LVM para evitar la pérdida de datos. La capa de integridad detecta la corrupción de datos en un dispositivo y alerta a la capa RAID para que corrija los datos corruptos en todo el RAID LVM.

Mientras que el RAID previene la pérdida de datos debido a un fallo del dispositivo, la adición de integridad a una matriz RAID LVM previene la pérdida de datos debido a datos corruptos en un dispositivo. Puede añadir la capa de integridad cuando cree un nuevo RAID LVM, o puede añadirla a un RAID LVM que ya exista.

(JIRA:RHELPLAN-39320)

Almacenamiento resistente (GFS2) compatible con las nubes públicas de AWS, Azure y Aliyun

Resilient Storage (GFS2) es ahora compatible con las tres principales nubes públicas, Amazon (AWS), Microsoft (Azure) y Alibaba (Aliyun), con la introducción de la compatibilidad con dispositivos de bloques compartidos en esas plataformas. Como resultado, GFS2 es ahora un verdadero sistema de archivos de clúster en la nube híbrida con opciones para usar tanto en las instalaciones como en la nube pública. Para obtener información sobre la configuración del almacenamiento en bloque compartido en Microsoft Azure y en AWS, consulte Implementación de Red Hat Enterprise Linux 8 en plataformas de nube pública. Para obtener información sobre la configuración del almacenamiento en bloque compartido en Alibaba Cloud, consulte Configuración del almacenamiento en bloque compartido para un clúster de alta disponibilidad de Red Hat en Alibaba Cloud.

(BZ#1900019)

El espacio de usuario ahora soporta el último demonio nfsdcld

El espacio de usuario ahora soporta el último demonio **nfsdcld**, que es el único método de seguimiento de clientes consciente del espacio de nombres. Esta mejora garantiza la recuperación de la apertura o el bloqueo del cliente desde el demonio **knfsd** en el contenedor sin ninguna corrupción de datos.

(BZ#1817756)

nconnect admite ahora múltiples conexiones simultáneas

Con esta mejora, puede utilizar la funcionalidad **nconnect** para crear múltiples conexiones concurrentes a un servidor NFS, permitiendo una capacidad de equilibrio de carga diferente. Habilite la funcionalidad **nconnect** con la opción de montaje NFS **nconnect=X**, donde *X* es el número de conexiones concurrentes a utilizar. El límite actual es 16.

(BZ#1683394, BZ#1761352)

ahora se admite el demonio nfsdcld para el seguimiento de la información del cliente

Con esta mejora, el demonio **nfsdcld** es ahora el método por defecto en el seguimiento de la información por cliente en un almacenamiento estable. Como resultado, el NFS v4 que se ejecuta en contenedores permite a los clientes reclamar las aperturas o bloqueos después de un reinicio del servidor.

(BZ#1817752)

6.1.10. Alta disponibilidad y clusters

marcapasos rebasado a la versión 2.0.4

El gestor de recursos de clústeres Pacemaker se ha actualizado a la versión 2.0.4, que proporciona una serie de correcciones de errores.

(BZ#1828488)

Nueva propiedad de clúster de prioridad-cerrado-retraso

Pacemaker soporta ahora la nueva propiedad de cluster **priority-fencing-delay**, que permite configurar un cluster de dos nodos para que en una situación de split-brain el nodo con menos recursos en ejecución sea el que se cerque.

La propiedad **"priority-fencing-delay** " puede establecerse con una duración de tiempo. El valor por defecto de esta propiedad es 0 (desactivado). Si esta propiedad se establece con un valor distinto de cero, y el meta-atributo de **prioridad** está configurado para al menos un recurso, entonces en una situación de división del cerebro el nodo con la mayor prioridad combinada de todos los recursos que se ejecutan en él tendrá más probabilidades de sobrevivir.

Por ejemplo, si se establece pcs **resource defaults priority=1** y **pcs property set priority-fencing-delay=15s** y no se establece ninguna otra prioridad, el nodo que ejecute más recursos tendrá más probabilidades de sobrevivir porque el otro nodo esperará 15 segundos antes de iniciar el fencing. Si un recurso en particular es más importante que el resto, puedes darle una prioridad más alta.

El nodo que ejecuta el rol de maestro de un clon promocionable obtendrá 1 punto extra si se ha configurado una prioridad para ese clon.

Cualquier retraso establecido con **priority-fencing-delay** se añadirá a cualquier retraso de las propiedades del dispositivo **pcmk_delay_base** y **pcmk_delay_max** fence. Este comportamiento permite un cierto retraso cuando ambos nodos tienen la misma prioridad, o ambos nodos necesitan ser cercados por alguna razón que no sea la pérdida del nodo (por ejemplo, **on-fail=fencing** se establece para una operación de monitorización de recursos). Si se utiliza en combinación, se recomienda

establecer la propiedad **priority-fencing-delay** a un valor que sea significativamente mayor que el retardo máximo de **pcmk_delay_base** y **pcmk_delay_max**, para estar seguro de que el nodo priorizado es el preferido (el doble del valor sería completamente seguro).

(BZ#1784601)

Nuevos comandos para gestionar múltiples conjuntos de recursos y operaciones por defecto

Ahora es posible crear, listar, modificar y eliminar múltiples conjuntos de valores por defecto de recursos y operaciones. Cuando se crea un conjunto de valores por defecto, se puede especificar una regla que contenga expresiones de **recursos** y **operaciones**. Esto le permite, por ejemplo, configurar un valor de recurso por defecto para todos los recursos de un tipo determinado. Los comandos que enumeran los valores por defecto existentes ahora incluyen múltiples conjuntos de valores por defecto en su salida.

- El comando **pcs resource [op] defaults set create** crea un nuevo conjunto de valores por defecto. Al especificar reglas con este comando, sólo se permiten las expresiones **resource** y **op**, incluyendo **y**, **o** y paréntesis.
- El comando **pcs resource [op] defaults set delete | remove** elimina conjuntos de valores por defecto.
- El comando **pcs resource [op] defaults set update** cambia los valores por defecto de un conjunto.

(BZ#1817547)

Soporte para etiquetar los recursos del clúster

Ahora es posible etiquetar recursos de cluster en un cluster Pacemaker con el comando **pcs tag**. Esta función le permite administrar un conjunto específico de recursos con un solo comando. También puede utilizar el comando pcs **tag** para eliminar o modificar la etiqueta de un recurso y para mostrar la configuración de la etiqueta.

Los comandos pcs resource **enable**, **pcs resource disable**, **pcs resource manage** y **pcs resource unmanage** aceptan IDs de etiquetas como argumentos.

(BZ#1684676)

Pacemaker ahora soporta la recuperación al degradar un recurso promovido en lugar de detenerlo completamente

Ahora es posible configurar un recurso promocionable en un cluster Pacemaker para que cuando una acción de promoción o monitorización falle para ese recurso, o la partición en la que el recurso se está ejecutando pierda el quórum, el recurso se degradará pero no se detendrá completamente.

Esta característica puede ser útil cuando se prefiere que el recurso siga estando disponible en el modo no promovido. Por ejemplo, si la partición de un maestro de base de datos pierde el quórum, puede preferir que el recurso de base de datos pierda el rol de **maestro**, pero que permanezca vivo en modo de sólo lectura para que las aplicaciones que sólo necesitan leer puedan seguir trabajando a pesar del quórum perdido. Esta función también puede ser útil cuando un descenso exitoso es suficiente para la recuperación y mucho más rápido que un reinicio completo.

Para apoyar esta función:

- El meta-atributo de la operación **"on-fail** " ahora acepta un valor de **degradación** cuando se utiliza con acciones de **promoción**, como en el siguiente ejemplo:

```
pcs resource op add my-rsc promote on-fail="demote"
```

- El meta-atributo de la operación **"on-fail** " ahora acepta un valor de **degradación** cuando se utiliza con acciones de **monitorización** con un **intervalo** establecido a un valor distinto de cero y un **rol** establecido a **Maestro**, como en el siguiente ejemplo:

```
pcs resource op add my-rsc monitor interval="10s" on-fail="demote" role="Master"
```

- La propiedad de clúster **no-quorum-policy** ahora acepta un valor **demote**. Cuando se establece, si una partición de clúster pierde el quórum, cualquier recurso promovido será degradado pero se dejará en funcionamiento y todos los demás recursos se detendrán.

La especificación de un meta-atributo de **degradación** para una operación no afecta a cómo se determina la promoción de un recurso. Si el nodo afectado sigue teniendo la mayor puntuación de promoción, será seleccionado para ser promovido de nuevo.

(BZ#1837747, BZ#1843079)

Nuevo parámetro de configuración SBD_SYNC_RESOURCE_STARTUP SBD para mejorar la sincronización con Pacemaker

Para controlar mejor la sincronización entre SBD y Pacemaker, el archivo **/etc/sysconfig/sbd** admite ahora el parámetro **SBD_SYNC_RESOURCE_STARTUP**. Cuando se instalan los paquetes Pacemaker y SBD de RHEL 8.3 o posterior y SBD se configura con **SBD_SYNC_RESOURCE_STARTUP=true**, SBD se pone en contacto con el demonio Pacemaker para obtener información sobre el estado del demonio.

En esta configuración, el demonio Pacemaker esperará hasta que haya sido contactado por SBD, tanto antes de iniciar sus subdemons como antes de la salida final. Como resultado, Pacemaker no ejecutará recursos si SBD no puede comunicarse activamente con él, y Pacemaker no saldrá hasta que haya informado a SBD de un apagado graceful. De este modo se evita la improbable situación que podría darse durante un apagado graceful cuando SBD no detecta el breve momento en el que no se ejecutan recursos antes de que Pacemaker se desconecte finalmente, lo que provocaría un reinicio innecesario. La detección de un apagado de gracia mediante un apretón de manos definido también funciona en el modo de mantenimiento. El método anterior de detección de un apagado correcto sobre la base de que no queden recursos en ejecución tuvo que ser desactivado en el modo de mantenimiento, ya que los recursos en ejecución no se verían afectados por el apagado.

Además, habilitar esta función evita el riesgo de una situación de cerebro dividido en un clúster cuando SBD y Pacemaker se inician con éxito pero SBD no puede contactar con Pacemaker. Esto podría ocurrir, por ejemplo, debido a las políticas de SELinux. En esta situación, Pacemaker asumiría que SBD está funcionando cuando no es así. Con esta nueva función activada, Pacemaker no completará el arranque hasta que SBD se haya puesto en contacto con él. Otra ventaja de esta nueva característica es que cuando está habilitada SBD contactará con Pacemaker repetidamente, utilizando un latido, y es capaz de hacer entrar en pánico al nodo si Pacemaker deja de responder en cualquier momento.

NOTA

Si usted ha editado su archivo /etc/sysconfig/sbd o ha configurado SBD a través de PCS, entonces una actualización de RPM no incorporará el nuevo parámetro **SBD_SYNC_RESOURCE_STARTUP**. En estos casos, para implementar esta característica debe agregarla manualmente desde el archivo **/etc/sysconfig/sbd.rpmnew** o seguir el procedimiento descrito en la sección **Configuración vía ambiente** de la página man de **sbd**(8).

(BZ#1718324, BZ#1743726)

6.1.11. Lenguajes de programación dinámicos, servidores web y de bases de datos

Una nueva corriente de módulos: ruby:2.7

RHEL 8.3 introduce Ruby 2.7.1 en un nuevo flujo de módulos **ruby:2.7**. Esta versión proporciona una serie de mejoras de rendimiento, correcciones de errores y seguridad, y nuevas características sobre Ruby 2.6 distribuido con RHEL 8.1.

Las mejoras más destacadas son:

- Se ha introducido un nuevo recolector de basura (GC) de compactación. Este GC puede desfragmentar un espacio de memoria fragmentado.
- Ruby yet Another Compiler-Compiler (Racc) proporciona ahora una interfaz de línea de comandos para el generador de análisis sintáctico Look-Ahead Left-to-Right - LALR(1).
- Interactive Ruby Shell(**irb**), el entorno de bucle de lectura-evaluación-impresión (REPL), soporta ahora la edición multilínea.
- La concordancia de patrones, utilizada con frecuencia en los lenguajes de programación funcionales, se ha introducido como característica experimental.
- El parámetro numerado como parámetro de bloque por defecto se ha introducido como característica experimental.

Se han implementado las siguientes mejoras de rendimiento:

- Se ha cambiado la estrategia de caché de fibra para acelerar la creación de fibra.
- Se ha mejorado el rendimiento del método **CGI.escapeHTML**.
- Se ha mejorado el rendimiento de la clase **Monitor** y del módulo **MonitorMixin**.

Además, la conversión automática de los argumentos de palabra clave y de los argumentos posicionales ha quedado obsoleta. En Ruby 3.0, los argumentos posicionales y los argumentos de palabra clave estarán separados. Para más información, consulta la documentación de la versión anterior .

Para suprimir las advertencias sobre características experimentales, utilice la opción de línea de comandos -W: **no-experimental**. Para desactivar una advertencia de desaprobación, utilice la opción de línea de comandos -W: **no-deprecated** o añada **Warning[:deprecated] = false** a su código.

Para instalar el flujo del módulo **ruby:2.7**, utilice:

```
# yum module install ruby:2.7
```

Si desea actualizar desde el flujo **ruby:2.6**, consulte Cambiar a un flujo posterior .

(BZ#1817135)

Una nueva corriente de módulos: nodejs:14

Ya está disponible un nuevo módulo, **nodejs:14**. **Node.js 14**, incluido en RHEL 8.3, aporta numerosas novedades y correcciones de errores y seguridad respecto a **Node.js 12** distribuido en RHEL 8.1.

Los cambios más destacados son:

- El motor V8 ha sido actualizado a la versión 8.3.
- Se ha implementado una nueva interfaz experimental del sistema WebAssembly (WASI).
- Se ha introducido una nueva API experimental de almacenamiento local asíncrono.
- La función de informe de diagnóstico ya es estable.
- Las API de los flujos se han endurecido.
- Se han eliminado los avisos de los módulos experimentales.

Con la publicación del aviso RHEA-2020:5101, RHEL 8 proporciona **Node.js 14.15.0**, que es la versión más reciente de soporte a largo plazo (LTS) con estabilidad mejorada.

Para instalar el flujo del módulo **nodejs:14**, utilice:

```
# yum module install nodejs:14
```

Si desea actualizar desde el flujo **nodejs:12**, consulte Cambiar a un flujo posterior .

(BZ#1815402, BZ#1891809)

git rebasado a la versión 2.27

Los paquetes **git** han sido actualizados a la versión 2.27. Los cambios notables sobre la versión 2.18 disponible anteriormente incluyen:

- El comando **git checkout** se ha dividido en dos comandos distintos:
  - **interruptor git** para la gestión de ramas
  - **git restore** para gestionar los cambios dentro del árbol de directorios
- El comportamiento del comando **git reb** ase se basa ahora en el flujo de trabajo de **fusión** por defecto en lugar del flujo de trabajo anterior **de aplicación de parches**. Para conservar el comportamiento anterior, establece la variable de configuración **rebase.backend** en **apply**.
- El comando **git difftool** ahora puede ser utilizado también fuera de un repositorio.
- Se han introducido cuatro nuevas variables de configuración, **{autor,committer}. {nombre,email}**, para anular **user.{nombre,email}** en casos más específicos.
- Se han añadido varias opciones nuevas que permiten a los usuarios configurar SSL para la comunicación con los proxies.
- Se ha mejorado la gestión de confirmaciones con mensajes de registro en codificación de caracteres no UTF-8 en las utilidades git **fast-export** y **git fast-import**.
- La extensión **lfs** ha sido añadida como un nuevo paquete **git-lfs**. Git Large File Storage (LFS) sustituye los archivos grandes por punteros de texto dentro de **Git** y almacena el contenido de los archivos en un servidor remoto.

(BZ#1825114, BZ#1783391)

Cambios en Python

RHEL 8.3 introduce los siguientes cambios en el flujo del módulo **python38:3.8**:

- El intérprete de **Python** ha sido actualizado a la versión 3.8.3, que proporciona varias correcciones de errores.
- El paquete **python38-pip** ha sido actualizado a la versión 19.3.1, y **pip** ahora soporta la instalación de ruedas **manylinux2014**.

El rendimiento del intérprete de **Python 3.6**, proporcionado por los paquetes **python3**, se ha mejorado considerablemente.

Las imágenes de contenedor **ubi8/python-27**, **ubi8/python-36**, y **ubi8/python-38** ahora soportan la instalación de la utilidad **pipenv** desde un índice de paquetes personalizado o un espejo de PyPI si es proporcionado por el cliente. Anteriormente, **pipenv** sólo podía descargarse desde el repositorio upstream de PyPI, y si el repositorio upstream no estaba disponible, la instalación fallaba.

(BZ#1847416, BZ#1724996, BZ#1827623, BZ#1841001)

Una nueva corriente de módulos: php:7.4

RHEL 8.3 introduce **PHP 7.4**, que proporciona una serie de correcciones de errores y mejoras sobre la versión 7.3.

Esta versión introduce una nueva extensión experimental, Foreign Function Interface (FFI), que permite llamar a funciones nativas, acceder a variables nativas y crear y acceder a estructuras de datos definidas en bibliotecas C. La extensión FFI está disponible en el paquete **php-ffi**.

Se han eliminado las siguientes extensiones:

- La extensión **wddx**, eliminada del paquete **php-xml**
- La extensión **recode**, eliminada del paquete **php-recode**.

Para instalar el flujo del módulo **php:7.4**, utilice:

```
# yum module install php:7.4
```

Si desea actualizar desde el flujo **php:7.3**, consulte Cambiar a un flujo posterior .

Para más detalles sobre el uso de PHP en RHEL 8, consulte Uso del lenguaje de scripting PHP .

(BZ#1797661)

Un nuevo flujo de módulos: nginx:1.18

Ya está disponible el servidor web y proxy **nginx 1.18**, que proporciona una serie de correcciones de errores, correcciones de seguridad, nuevas características y mejoras respecto a la versión 1.16. Los cambios más destacados son:

- Se han implementado mejoras en la tasa de peticiones HTTP y en la limitación de conexiones. Por ejemplo, las directivas **limit_rate** y **limit_rate_after** ahora soportan variables, incluyendo las nuevas variables **$limit_req_status** y **$limit_conn_status**. Además, se ha añadido el modo dry-run para las directivas **limit_conn_dry_run** y **limit_req_dry_run**.
- Se ha añadido una nueva directiva **auth_delay**, que permite retrasar el procesamiento de las solicitudes no autorizadas.
- Las siguientes directivas ahora soportan variables: **grpc_pass**, **proxy_upload_rate** y **proxy_download_rate**.

- Se han añadido variables de protocolo PROXY adicionales, concretamente **$proxy_protocol_server_addr** y **$proxy_protocol_server_port**.

Para instalar el flujo **nginx:1.18**, utilice:

```
# yum module install nginx:1.18
```

Si desea actualizar desde el flujo **nginx:1.16**, consulte Cambiar a un flujo posterior .

(BZ#1826632)

Un nuevo módulo: perl:5.30

RHEL 8.3 introduce **Perl 5.30**, que proporciona una serie de correcciones de errores y mejoras con respecto a la versión anterior **Perl 5.26**. La nueva versión también deja de lado o elimina ciertas características del lenguaje. Los cambios más significativos son los siguientes

- Se han eliminado los módulos **Math::BigInt::CalcEmu**, **arybase** y **B::Debug**
- Los descriptores de archivos se abren ahora con una bandera de **cierre en ejecución**
- Ya no se permite abrir el mismo símbolo como archivo y como manejador de directorio
- Los atributos de las subrutinas ahora deben preceder a las firmas de las subrutinas
- Se han eliminado los atributos **:locked** y **:uniq**
- Ya no se permiten las listas de variables sin comas en los formatos
- Ya no se permite el operador **<<** aquí-documento
- Ya no se permite el uso de un carácter de llave izquierda**({)** en los patrones de expresiones regulares
- La subrutina **AUTOLOAD()** ya no se puede heredar a funciones que no sean métodos
- El pragma de **ordenación** ya no permite especificar un algoritmo de **ordenación**
- La subrutina **B ::OP::terse()** ha sido sustituida por la subrutina **B::Concise::b_terse()**
- La función **File**::Glob **::glob()** ha sido sustituida por la función **File::Glob::bsd_glob()**
- La función **dump(**) ahora debe ser invocada completamente calificada como **CORE::dump()**
- El operador yada-yada (**...**) es una declaración ahora, no se puede utilizar como una expresión
- Asignar un valor distinto de cero a la variable **$[** ahora devuelve un error fatal
- Las variables **$*** y **$#** ya no están permitidas
- Ya no se permite declarar variables utilizando la función **my()** en una rama de condición falsa
- El uso de las funciones **sysread()** y **syswrite()** en los manejadores **:utf8** ahora devuelve un error fatal
- La función **pack(**) ya no devuelve el formato UTF-8 malformado
- Los puntos de código Unicode con un valor superior a **IV_MAX** ya no están permitidos

- Ahora es compatible con Unicode 12.1

Para actualizar desde un flujo de módulos **perl** anterior, consulte Cambiar a un flujo posterior .

Perl 5.30 también está disponible como imagen contenedora s2i-enabled **ubi8/perl-530**.

(BZ#1713592, BZ#1732828)

Un nuevo módulo: perl-libwww-perl:6.34

RHEL 8.3 introduce un nuevo flujo de módulos **perl-libwww-perl:6.34**, que proporciona el paquete **perl-libwww-perl** para todas las versiones de **Perl** disponibles en RHEL 8. El paquete **perl-libwww-perl** no modular, disponible desde RHEL 8.0, que no puede utilizarse con otros flujos de **Perl** que no sean 5.26, ha quedado obsoleto por el nuevo flujo **perl-libwww-perl:6.34** por defecto.

(BZ#1781177)

Un nuevo módulo: perl-IO-Socket-SSL:2.066

Ya está disponible un nuevo flujo del módulo **perl-IO-Socket-SSL:2.066**. Este módulo proporciona los paquetes **perl-IO-Socket-SSL** y **perl-Net-SSLeay** y es compatible con todos los flujos de **Perl** disponibles en RHEL 8.

(BZ#1824222)

El flujo del módulo squid:4 se ha reajustado a la versión 4.11

El servidor proxy **Squid**, proporcionado por el flujo del módulo **squid:4**, ha sido actualizado de la versión 4.4 a la versión 4.11. Esta versión proporciona múltiples correcciones de errores y seguridad, y varias mejoras, como nuevas opciones de configuración.

(BZ#1829467)

Cambios en el flujo del módulo httpd:2.4

RHEL 8.3 introduce los siguientes cambios notables en el servidor HTTP Apache, disponibles a través del flujo de módulos **httpd:2.4**:

- El módulo **mod_http2** se ha actualizado a la versión 1.15.7
- Cambios de configuración en las directivas **H2Upgrade** y **H2Push**
- Una nueva directiva de configuración **H2Padding** para controlar el relleno de las tramas de carga útil de HTTP/2
- Numerosas correcciones de errores.

(BZ#1814236)

Soporte para el registro en journald desde la directiva CustomLog en httpd

Ahora es posible enviar registros de acceso (transferencia) a **journald** desde el servidor HTTP Apache utilizando una nueva opción para la directiva **CustomLog**.

La sintaxis admitida es la siguiente:

```
CustomLog journald:priority format|nickname
```

donde *priority* es cualquier cadena de prioridad hasta la de **depuración**, como se utiliza en la directiva**LogLevel**.

Por ejemplo, para registrar en **journald** utilizando el formato de registro **combinado**, utilice:

```
CustomLog journald:info combinado
```

Tenga en cuenta que cuando se utiliza esta opción, el rendimiento del servidor puede ser menor que cuando se registra directamente en archivos planos.

(BZ#1209162)

6.1.12. Compiladores y herramientas de desarrollo

Nuevo conjunto de herramientas GCC 10

GCC Toolset 10 es un conjunto de herramientas de compilación que proporciona versiones recientes de herramientas de desarrollo. Está disponible como un flujo de aplicaciones en forma de colección de software en el repositorio **AppStream**.

El compilador GCC ha sido actualizado a la versión 10.2.1, que proporciona muchas correcciones de errores y mejoras que están disponibles en GCC upstream.

Las siguientes herramientas y versiones son proporcionadas por GCC Toolset 10:

Herramienta	Versión
GCC	10.2.1
GDB	9.2
Valgrind	3.16.0
SystemTap	4.3
Dyninst	10.1.0
binutils	2.35
elfutils	0.180
dwz	0.12
hacer	4.2.1
strace	5.7
ltrace	0.7.91
annobin	9.29

Para instalar GCC Toolset 10, ejecute el siguiente comando como root:

```
# yum install gcc-toolset-10
```

Para ejecutar una herramienta de GCC Toolset 10:

```
$ scl enable gcc-toolset-10 tool
```

Para ejecutar una sesión de shell en la que las versiones de las herramientas de GCC Toolset 10 anulan las versiones del sistema de estas herramientas:

```
$ scl enable gcc-toolset-10 bash
```

Para obtener más información, consulte Uso del conjunto de herramientas GCC .

Los componentes de GCC Toolset 10 están disponibles en las dos imágenes de contenedores:

- **rhel8/gcc-toolset-10-toolchain**, que incluye el compilador GCC, el depurador GDB y la herramienta de automatización **make**.
- **rhel8/gcc-toolset-10-perftools**, que incluye las herramientas de supervisión del rendimiento, como SystemTap y Valgrind.
  Para extraer una imagen de contenedor, ejecute el siguiente comando como root:

  ```
  # podman pull registry.redhat.io/
  ```

  Tenga en cuenta que ahora sólo se soportan las imágenes contenedoras de GCC Toolset 10. Las imágenes contenedoras de versiones anteriores de GCC Toolset están obsoletas.

Para más detalles sobre las imágenes de contenedor, consulte Uso de las imágenes de contenedor del conjunto de herramientas GCC.

(BZ#1842656)

El conjunto de herramientas de Rust se ha actualizado a la versión 1.45.2

Rust Toolset ha sido actualizado a la versión 1.45.2. Los cambios más destacados son:

- El subcomando de **árbol de carga** para ver las dependencias está ahora incluido en **cargo**.
- La conversión de valores de coma flotante a enteros produce ahora una conversión ajustada. Anteriormente, cuando un valor de coma flotante truncado estaba fuera del rango del tipo entero de destino, el resultado era un comportamiento indefinido del compilador. Los valores de coma flotante no finitos también provocaban un comportamiento indefinido. Con esta mejora, los valores finitos se sujetan al rango mínimo o máximo del entero. Los valores infinitos positivos y negativos se ajustan por defecto al máximo y al mínimo del entero, respectivamente, y los valores no numéricos (NaN) se ajustan a cero.
- Las macros procedimentales tipo función en expresiones, patrones y sentencias están ahora ampliadas y estabilizadas.

Para obtener instrucciones detalladas sobre su uso, consulte Uso del conjunto de herramientas de Rust .

(BZ#1820593)

El conjunto de herramientas LLVM se ha actualizado a la versión 10.0.1

El conjunto de herramientas LLVM ha sido actualizado a la versión 10.0.1. Con esta actualización, los paquetes **clang-libs** ya no incluyen bibliotecas de componentes individuales. Como resultado, ya no es posible enlazar aplicaciones con ellas. Para enlazar aplicaciones con las bibliotecas **clang**, utilice el paquete **libclang-cpp.so**.

Para más información, consulte Uso del conjunto de herramientas LLVM .

(BZ#1820587)

Go Toolset rebasado a la versión 1.14.7

Go Toolset se ha actualizado a la versión 1.14.7 Los cambios más importantes son

- El sistema de módulos Go es ahora totalmente compatible.
- La versión 3.0 de SSL (SSLv3) ya no es compatible. Las mejoras notables del depurador Delve incluyen:
- El nuevo comando **examinemem** (o **x**) para examinar la memoria bruta
- La nueva **pantalla de** comandos para imprimir los valores de una expresión durante cada parada del programa
- La nueva bandera **--tty** para suministrar un teletipo (TTY) para el programa depurado
- El nuevo soporte de coredump para Arm64
- La nueva capacidad de imprimir etiquetas de goroutine
- La liberación del servidor del protocolo de depuración (DAP)
- La salida mejorada de los comandos **dlv trace** y **trace** REPL (read-eval-print-loop)

Para obtener más información sobre Go Toolset, consulte Uso de Go Toolset.

Para más información sobre Delve, consulte la documentación de Delve.

(BZ#1820596)

SystemTap rebasado a la versión 4.3

La herramienta de instrumentación SystemTap ha sido actualizada a la versión 4.3, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Las sondas de espacio de usuario pueden ser dirigidas por el **buildid** hexadecimal de **readelf -n**. Esta alternativa al nombre de la ruta de acceso permite sondear los binarios que coincidan con cualquier nombre y, por lo tanto, permite que un solo script se dirija a un rango de versiones diferentes. Esta característica funciona bien junto con el servidor de **depuración** elfutils.
- Las funciones de los scripts pueden utilizar las variables **$contexto** de la sonda para acceder a las variables de la ubicación sondeada, lo que permite a los scripts de SystemTap utilizar una lógica común para trabajar con una variedad de sondas.
- Las mejoras en el programa **stapbpf**, incluyendo las sentencias try-catch, y las sondas de error, se han realizado para permitir una adecuada tolerancia a los errores en los scripts que se ejecutan en el backend BPF.

Para más información sobre los cambios notables, lea las notas de la versión anterior antes de actualizar.

(BZ#1804319)

Valgrind rebasado a la versión 3.16.0

La herramienta de análisis de código ejecutable Valgrind ha sido actualizada a la versión 3.16.0, que proporciona una serie de correcciones de errores y mejoras respecto a la versión anterior:

- Ahora es posible cambiar dinámicamente el valor de muchas opciones de la línea de comandos mientras su programa se está ejecutando bajo Valgrind: a través de **vgdb**, a través de un **gdb** conectado al gdbserver de Valgrind, o a través de las peticiones del cliente del programa. Para obtener una lista de opciones modificables dinámicamente, ejecute el comando **valgrind --help-dyn-options**.

- Para las herramientas Cachegrind**(cg_annotate**) y Callgrind**(callgrind_annotate**), las opciones **--auto** y **--show-percs** ahora están predeterminadas en **sí**.

- La herramienta Memcheck produce menos errores falsos positivos en el código optimizado. En particular, Memcheck ahora maneja mejor el caso en que el compilador transformó un código **A**

- Se ha eliminado la herramienta experimental de comprobación de pila y matriz global**(exp-sgcheck**). Una alternativa para detectar los desbordamientos de pila y de matriz global es utilizar la facilidad AddressSanitizer (ASAN) de GCC, que requiere reconstruir el código con la opción **-fsanitize=address**.

(BZ#1804324)

elfutils rebasado a la versión 0.180

El paquete **elfutils** ha sido actualizado a la versión 0.180, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Mejor soporte para la información de depuración para el código construido con GCC LTO (optimización en tiempo de enlace). Las utilidades **eu-readelf** y **libdw** ahora pueden leer y manejar las secciones **.gnu.debuglto_**, y resolver correctamente los nombres de archivo para las funciones que se definen a través de CUs (unidades de compilación).

- La utilidad **eu-nm** ahora identifica explícitamente los objetos débiles como **V** y los símbolos comunes como **C**.

- El servidor **de debuginfod** puede ahora indexar archivos **.deb** y tiene una extensión genérica para añadir otros formatos de archivos de paquetes usando la opción -Z **EXT[=CMD]**. Por ejemplo **-Z '.tar.zst=zstdcat'** indica que los archivos que terminan con la extensión **.tar.zst** deben ser desempaquetados usando la utilidad **zstdcat**.

- La herramienta **debuginfo-client** tiene varias funciones de ayuda nuevas, como **debuginfod_set_user_data**, **debuginfod_get_user_data**, **debuginfod_get_url** y **debuginfod_add_http_header**. Ahora también soporta URLs **file:**//.

(BZ#1804321)

GDB ahora soporta la grabación y reproducción de procesos en IBM z15

Con esta mejora, el depurador de GNU (GDB) soporta ahora el registro y la reproducción de procesos con la mayoría de las nuevas instrucciones del procesador IBM z15 (anteriormente conocido como arch13). Tenga en cuenta que las siguientes instrucciones no están actualmente soportadas: SORTL

(listas de ordenación), DFLTCC (llamada a la conversión de deflación), KDSA (computación de autenticación de firma digital).

(BZ#1659535)

Los eventos de monitorización del rendimiento de Marvell ThunderX2 han sido actualizados en papi

Con esta mejora, se han actualizado una serie de eventos de rendimiento específicos de ThunderX2, incluidos los eventos uncore. Como resultado, los desarrolladores pueden investigar mejor el rendimiento del sistema en los sistemas Marvell ThunderX2.

(BZ#1726070)

La biblioteca matemática glibc está ahora optimizada para IBM Z

Con esta mejora, las funciones matemáticas de **libm** se han optimizado para mejorar el rendimiento en las máquinas IBM Z. Los cambios notables incluyen:

- mejora de la gestión del modo de redondeo para evitar conjuntos de registros de control de coma flotante y extractos superfluos
- explotación de la conversión entre el entero z196 y el flotante

(BZ#1780204)

Ya está disponible un directorio temporal adicional específico de libffi

Anteriormente, en los sistemas reforzados, los directorios temporales de todo el sistema podían no tener permisos adecuados para su uso con la biblioteca **libffi**.

Con esta mejora, los administradores del sistema pueden ahora establecer la variable de entorno **LIBFFI_TMPDIR** para que apunte a un directorio temporal específico de libffi con permisos de **escritura** y **ejecución** de montaje o selinux.

(BZ#1723951)

Mejora del rendimiento de strstr() y strcasestr()

Con esta actualización, se ha mejorado el rendimiento de las funciones **strstr()** y **strcasestr()** en varias arquitecturas soportadas. Como resultado, los usuarios se benefician ahora de un rendimiento significativamente mejor de todas las aplicaciones que utilizan rutinas de manipulación de cadenas y memoria.

(BZ#1821531)

glibc ahora maneja correctamente la carga de un archivo local truncado

Si el archivo de locales del sistema se ha truncado previamente, ya sea debido a un corte de energía durante la actualización o a un fallo de disco, un proceso podría terminar inesperadamente al cargar el archivo. Esta mejora añade comprobaciones de consistencia adicionales a la carga del archivo de configuraciones regionales. Como resultado, los procesos son ahora capaces de detectar el truncamiento del archivo y volver a las configuraciones regionales no instaladas en el archivo o a la configuración regional POSIX por defecto.

(BZ#1784525)

GDB ahora soporta debuginfod

Con esta mejora, el depurador de GNU (GDB) puede ahora descargar paquetes de información de depuración desde servidores centralizados bajo demanda utilizando la biblioteca cliente elfutils **debuginfod**.

(BZ#1838777)

pcp rebasado a la versión 5.1.1-3

El paquete **pcp** ha sido actualizado a la versión 5.1.1-3. Los cambios notables incluyen:

- Actualización de las unidades de servicio y mejora de la integración y fiabilidad de **systemd** para todos los servicios de PCP. Mejorada la rotación del registro de archivos y una compresión más oportuna. Corrección de errores de descubrimiento de archivos en el protocolo **pmproxy**.
- Se han mejorado las herramientas de monitorización **pcp-atop**, **pcp-dstat**, **pmrep** y otras relacionadas, así como los informes de etiquetas métricas en las herramientas **pmrep** y de exportación.
- Mejora de **bpftrace**, **OpenMetrics**, MMV, el agente del kernel de Linux y otros agentes de recolección. Nuevos recolectores de métricas para los servidores Open **vSwitch** y **RabbitMQ**.
- Nuevo servicio de descubrimiento de hosts **pmfind systemd**, que sustituye al demonio independiente **pmmgr**.

(BZ#1792971)

grafana rebasado a la versión 6.7.3

El paquete **grafana** ha sido actualizado a la versión 6.7.3. Los cambios más destacados son:

- Soporte de mapeo de roles genéricos **de OAuth**
- Un nuevo panel de registros
- Visualización de texto de varias líneas en el panel de la tabla
- Una nueva moneda y unidades de energía

(BZ#1807323)

grafana-pcp rebasado a la versión 2.0.2

El paquete **grafana-pcp** ha sido actualizado a la versión 2.0.2. Los cambios notables incluyen:

- Soporta los mapas multidimensionales **de eBPF** para ser graficados en el flamegráfico.
- Elimina la caché de autocompletado en el editor de consultas, para que las métricas de PCP puedan aparecer de forma dinámica.

(BZ#1807099)

Una nueva imagen de contenedor rhel8/pcp

La imagen del contenedor **rhel8/pcp** ya está disponible en el Red Hat Container Registry. La imagen contiene el kit de herramientas Performance Co-Pilot (PCP), que incluye el paquete **pcp-zeroconf** preinstalado y el PMDA de **OpenMetrics**.

(BZ#1497296)

Una nueva imagen de contenedor rhel8/grafana

La imagen de contenedor **rhel8/grafana** ya está disponible en el Red Hat Container Registry. Grafana es una utilidad de código abierto con panel de métricas, y editor de gráficos para la herramienta de monitorización **Graphite**, **Elasticsearch**, **OpenTSDB**, **Prometheus**, **InfluxDB** y **PCP**.

(BZ#1823834)

6.1.13. Gestión de la identidad

La utilidad de copia de seguridad de IdM ahora comprueba los roles de réplica requeridos

La utilidad **ipa-backup** ahora comprueba si todos los servicios utilizados en el clúster de IdM, como una Autoridad de Certificados (CA), un Sistema de Nombres de Dominio (DNS) y un Agente de Recuperación de Claves (KRA) están instalados en la réplica donde se está ejecutando la copia de seguridad. Si la réplica no tiene todos estos servicios instalados, la utilidad **ipa-backup** sale con una advertencia, porque las copias de seguridad tomadas en ese host no serían suficientes para una restauración completa del clúster.

Por ejemplo, si su implementación de IdM utiliza una Autoridad de Certificación (CA) integrada, una copia de seguridad ejecutada en una réplica no CA no capturará los datos de la CA. Red Hat recomienda verificar que la réplica en la que se realiza una **copia de seguridad ipa** tenga instalados todos los servicios IdM utilizados en el cluster.

Para obtener más información, consulte Preparación para la pérdida de datos con las copias de seguridad de IdM.

(BZ#1810154)

Nueva herramienta de notificación de caducidad de contraseñas

Expiring Password Notification (EPN), proporcionada por el paquete **ipa-client-epn**, es una herramienta independiente que puede utilizar para crear una lista de usuarios de Gestión de Identidades (IdM) cuyas contraseñas van a caducar pronto.

Los administradores de IdM pueden utilizar EPN para:

- Mostrar una lista de usuarios afectados en formato JSON, que se calcula en tiempo de ejecución
- Calcule cuántos correos electrónicos se enviarán para un día o rango de fechas determinado
- Enviar notificaciones de caducidad de la contraseña por correo electrónico a los usuarios

Red Hat recomienda lanzar EPN una vez al día desde un cliente IdM o una réplica con el temporizador **ipa-epn.timer systemd** incluido.

(BZ#913799)

JSS proporciona ahora un SSLContext compatible con FIPS

Anteriormente, Tomcat utilizaba la directiva SSLEngine de la clase SSLContext de la Arquitectura de Criptografía de Java (JCA). La implementación por defecto de SunJSSE no es compatible con el Estándar Federal de Procesamiento de Información (FIPS), por lo que PKI proporciona ahora una implementación compatible con FIPS a través de JSS.

(BZ#1821851)

Ya está disponible la comprobación de la salud general de su infraestructura de clave pública

Con esta actualización, la herramienta de comprobación de la infraestructura de clave pública (PKI) informa del estado del subsistema PKI a la herramienta de comprobación de la gestión de identidades (IdM), que se introdujo en RHEL 8.1. La ejecución de IdM Healthcheck invoca PKI Healthcheck, que recoge y devuelve el informe de estado del subsistema PKI.

La herramienta **pki-healthcheck** está disponible en cualquier servidor RHEL IdM desplegado o réplica. Todas las comprobaciones proporcionadas por **pki-healthcheck** también están integradas en la herramienta **ipa-healthcheck**. **ipa-healthcheck** puede instalarse por separado del flujo del módulo **idm:DL1**.

Tenga en cuenta que **pki-healthcheck** también puede funcionar en una infraestructura autónoma de Red Hat Certificate System (RHCS).

(BZ#1770322)

Soporte para RSA PSS

Con esta mejora, la PKI admite ahora el algoritmo de firma RSA PSS (Probabilistic Signature Scheme).

Para habilitar esta función, establezca la siguiente línea en el archivo de script **pkispawn** para un subsistema determinado: **pki_use_pss_rsa_signing_algorithm=True**

Como resultado, todos los algoritmos de firma existentes por defecto para este subsistema (especificados en su archivo de configuración **CS.cfg**) utilizarán la versión PSS correspondiente. Por ejemplo, **SHA256withRSA** se convierte en **SHA256withRSA/PSS**

(BZ#1824948)

Directory Server exporta la clave privada y el certificado a un espacio de nombres privado cuando el servicio se inicia

Directory Server utiliza las bibliotecas OpenLDAP para las conexiones salientes, como los acuerdos de replicación. Dado que estas bibliotecas no pueden acceder directamente a la base de datos de los servicios de seguridad de la red (NSS), Directory Server extrae la clave privada y los certificados de la base de datos NSS en las instancias con soporte de cifrado TLS para permitir que las bibliotecas OpenLDAP establezcan conexiones cifradas. Anteriormente, Directory Server extraía la clave privada y los certificados en el directorio establecido en el parámetro **nsslapd-certdir** de la entrada **cn=config** (por defecto: **/etc/dirsrv/slapd-**

(BZ#1638875)

El servidor de directorios ahora puede convertir una instancia en modo de sólo lectura si se alcanza el umbral de monitorización del disco

Esta actualización añade el parámetro **nsslapd-disk-monitoring-readonly-on-threshold** a la entrada **cn=config**. Si habilita este parámetro, Directory Server cambia todas las bases de datos a sólo lectura si la supervisión del disco está habilitada y el espacio libre en el disco es inferior al valor que configuró en **nsslapd-disk-monitoring-threshold**. Con **nsslapd-disk-monitoring-readonly-on-threshold activado**, las bases de datos no pueden modificarse hasta que Directory Server apague correctamente la instancia. Esto puede evitar la corrupción de datos.

(BZ#1728943)

samba rebasado a la versión 4.12.3

Los paquetes *samba* han sido actualizados a la versión 4.12.3, que proporciona una serie de correcciones de errores y mejoras respecto a la versión anterior:

- Las funciones de criptografía incorporadas han sido sustituidas por funciones GnuTLS. Esto mejora el rendimiento del bloque de mensajes del servidor versión 3 (SMB3) y la velocidad de copia de forma significativa.
- El soporte mínimo de tiempo de ejecución es ahora Python 3.5.
- Se ha eliminado el parámetro **del tamaño de la cach** é de escritura porque el concepto anterior de caché de escritura podía reducir el rendimiento en sistemas con limitaciones de memoria.
- Se ha eliminado la compatibilidad con la autenticación de conexiones mediante tickets Kerberos con tipos de cifrado DES.
- Se ha eliminado el módulo del sistema de archivos virtual (VFS) **vfs_netatalk**.
- El parámetro **ldap s** sl ads está marcado como obsoleto y será eliminado en una futura versión de Samba. Para obtener información sobre cómo cifrar alternativamente el tráfico LDAP y más detalles, consulte la solución samba: eliminación de la opción smb.conf "ldap ssl ads" .
- Por defecto, Samba en RHEL 8.3 ya no soporta el conjunto de cifrado RC4 obsoleto. Si ejecuta Samba como miembro de un dominio en un AD que todavía requiere RC4 para la autenticación Kerberos, utilice el comando **update-crypto-policies --set DEFAULT:AD-SUPPORT** para habilitar el soporte para el tipo de cifrado RC4.

Samba actualiza automáticamente sus archivos de base de datos **tdb** cuando se inicia el servicio **smbd**, **nmbd** o **winbind**. Haga una copia de seguridad de los archivos de la base de datos antes de iniciar Samba. Tenga en cuenta que Red Hat no admite la actualización de los archivos de la base de datos **tdb**.

Para más información sobre los cambios notables, lea las notas de la versión anterior antes de actualizar.

(BZ#1817557)

cockpit-session-recording rebasado a la versión 4

El módulo **de grabación de sesiones de cabina** se ha actualizado a la versión 4. Esta versión ofrece los siguientes cambios notables con respecto a la versión anterior:

- Se ha actualizado el identificador de los padres en el archivo **metainfo**.
- Manifiesto del paquete actualizado.
- Corregido **rpmmacro** para resolver la ruta correcta en CentOS7.
- Maneja los datos del diario codificados en matrices de bytes.
- Se ha eliminado el código de las funciones obsoletas del ciclo de vida de React.

(BZ#1826516)

krb5 rebasado a la versión 1.18.2

Los paquetes **krb5** han sido actualizados a la versión 1.18.2. Las correcciones y mejoras más importantes son:

- Se han eliminado los tipos de encriptación simple y triple-DES.

- El borrador 9 PKINIT ha sido eliminado ya que no es necesario para ninguna de las versiones soportadas de Active Directory.
- Ahora se admiten los complementos del mecanismo NegoEx.
- Ahora se admite la canonización de nombres de host**(dns_canonicalize_hostname = fallback**).

(BZ#1802334)

IdM ahora es compatible con los nuevos módulos de gestión de Ansible

Esta actualización introduce varios módulos **ansible-freeipa** para la automatización de tareas comunes de gestión de identidades (IdM) mediante los playbooks de Ansible:

- El módulo **config** permite establecer parámetros de configuración global dentro de IdM.
- El módulo **dnsconfig** permite modificar la configuración global del DNS.
- El módulo **dnsforwardzone** permite añadir y eliminar reenviadores DNS de IdM.
- El **dnsrecord** permite la gestión de registros DNS. A diferencia del **ipa_dnsrecord** anterior, permite la gestión de múltiples registros en una sola ejecución, y soporta más tipos de registros.
- El módulo **dnszone** permite configurar zonas en el servidor DNS.
- El módulo de **servicios** permite asegurar la presencia y ausencia de servicios.
- El módulo de **bóvedas** permite asegurar la presencia y ausencia de bóvedas y de los miembros de las mismas.

Tenga en cuenta que los módulos **ipagroup** e **ipahostgroup** se han ampliado para incluir gestores de pertenencia a grupos de usuarios y de hosts, respectivamente. Un gestor de pertenencia a grupos es un usuario o un grupo que puede añadir miembros a un grupo o eliminar miembros de un grupo. Para más información, consulte las secciones de **variables** de los respectivos archivos **/usr/share/doc/ansible-freeipa/README-***.

(JIRA:RHELPLAN-49954)

IdM ahora soporta un nuevo rol de sistema Ansible para la gestión de certificados

Identity Management (IdM) admite un nuevo rol de sistema Ansible para automatizar las tareas de gestión de certificados. El nuevo rol incluye las siguientes ventajas:

- Esta función ayuda a automatizar la emisión y renovación de certificados.
- El rol puede ser configurado para que la autoridad certificadora **ipa** emita sus certificados. De este modo, puede utilizar su infraestructura de IdM existente para gestionar la cadena de confianza de los certificados.
- El rol permite especificar los comandos que se ejecutarán antes y después de la emisión de un certificado, por ejemplo, la detención e inicio de los servicios.

(JIRA:RHELPLAN-50002)

La gestión de identidades ahora es compatible con FIPS

Con esta mejora, ahora puede utilizar tipos de cifrado aprobados por la Norma Federal de Procesamiento de la Información (FIPS) con los mecanismos de autenticación en Identity Management

(IdM). Tenga en cuenta que una confianza cruzada entre IdM y Active Directory no es compatible con FIPS.

Los clientes que requieran FIPS pero no requieran un fideicomiso AD pueden ahora instalar IdM en modo FIPS.

(JIRA:RHELPLAN-43531)

OpenDNSSEC en idm:DL1 rebasado a la versión 2.1

El componente OpenDNSSEC del flujo del módulo **idm:DL1** se ha actualizado a la serie de versiones 2.1, que es la versión actual de soporte a largo plazo. OpenDNSSEC es un proyecto de código abierto que impulsa la adopción de las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) para mejorar la seguridad de Internet. OpenDNSSEC 2.1 ofrece una serie de correcciones de errores y mejoras con respecto a la versión anterior. Para más información, lea las notas de la versión anterior: https://www.opendnssec.org/archive/releases/

(JIRA:RHELPLAN-48838)

IdM admite ahora la suite de cifrado RC4 obsoleta con una nueva subpolítica criptográfica para todo el sistema

Esta actualización introduce la nueva subpolítica criptográfica **AD-SUPPORT** que habilita el conjunto de cifrado Rivest Cipher 4 (RC4) en la gestión de identidades (IdM).

Como administrador en el contexto de los fideicomisos de bosques cruzados IdM-Active Directory (AD), puede activar la nueva subpolítica **AD-SUPPORT** cuando AD no está configurado para utilizar el Estándar de cifrado avanzado (AES). Más específicamente, Red Hat recomienda activar la nueva subpolítica si se aplica una de las siguientes condiciones:

- Las cuentas de usuario o servicio en AD tienen claves de cifrado RC4 y carecen de claves de cifrado AES.
- Los enlaces de confianza entre dominios individuales de Active Directory tienen claves de cifrado RC4 y carecen de claves de cifrado AES.

Para activar la subpolítica **AD-SUPPORT** además de la política criptográfica **DEFAULT**, introduzca:

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

Como alternativa, para actualizar los fideicomisos entre los dominios de AD en un bosque de AD para que admitan tipos de cifrado AES fuertes, consulte el siguiente artículo de Microsoft: AD DS: Seguridad: Kerberos \ "Unsupported etype" error al acceder a un recurso en un dominio de confianza.

(BZ#1851139)

Adaptación a los nuevos requisitos de enlace del canal LDAP de Microsoft y de firma LDAP

Con las recientes actualizaciones de Microsoft, Active Directory (AD) marca los clientes que no utilizan la configuración predeterminada de Windows para la vinculación del canal LDAP y la firma LDAP. Como consecuencia, los sistemas RHEL que utilizan el demonio de servicios de seguridad del sistema (SSSD) para la integración directa o indirecta con AD podrían desencadenar IDs de eventos de error en AD tras operaciones exitosas de la capa de seguridad y autenticación simple (SASL) que utilizan la interfaz de programa de aplicación de servicios de seguridad genéricos (GSSAPI).

Para evitar estas notificaciones, configure las aplicaciones cliente para que utilicen el mecanismo SASL Simple and Protected GSSAPI Negotiation Mechanism (GSS-SPNEGO) en lugar de GSSAPI. Para configurar SSSD, establezca la opción **ldap_sasl_mech** en **GSS-SPNEGO**.

Además, si se impone la vinculación de canales en el lado de AD, configure cualquier sistema que utilice SASL con SSL/TLS de la siguiente manera:

1. Instale las últimas versiones de los paquetes **cyrus-sasl**, **openldap** y **krb5-libs** que se suministran con RHEL 8.3 y posteriores.

2. En el archivo **/etc/openldap/ldap.conf**, especifique el tipo de enlace de canal correcto estableciendo la opción **SASL_CBINDING** como **tls-endpoint**.

Para obtener más información, consulte Impacto del aviso de seguridad de Microsoft ADV190023 | LDAP Channel Binding and LDAP Signing on RHEL and AD integration.

(BZ#1873567)

SSSD, adcli y realmd ahora soportan el conjunto de cifrado RC4 obsoleto con una nueva subpolítica criptográfica para todo el sistema

Esta actualización introduce la nueva subpolítica criptográfica **AD-SUPPORT** que habilita el conjunto de cifrado Rivest Cipher 4 (RC4) para las siguientes utilidades:

- el demonio de servicios de seguridad del sistema (SSSD)
- **adcli**
- **realmd**

Como administrador, puede activar la nueva subpolítica **AD-SUPPORT** cuando Active Directory (AD) no está configurado para utilizar el estándar de cifrado avanzado (AES) en los siguientes escenarios:

- SSSD se utiliza en un sistema RHEL conectado directamente a AD.
- **adcli** se utiliza para unirse a un dominio AD o para actualizar los atributos del host, por ejemplo, la clave del host.
- **realmd** se utiliza para unirse a un dominio AD.

Red Hat recomienda habilitar la nueva subpolítica si se da una de las siguientes condiciones:

- Las cuentas de usuario o servicio en AD tienen claves de cifrado RC4 y carecen de claves de cifrado AES.
- Los enlaces de confianza entre dominios individuales de Active Directory tienen claves de cifrado RC4 y carecen de claves de cifrado AES.

Para activar la subpolítica **AD-SUPPORT** además de la política criptográfica **DEFAULT**, introduzca:

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

(BZ#1866695)

authselect tiene un nuevo perfil mínimo

La utilidad **authselect** tiene un nuevo perfil **mínimo**. Puede utilizar este perfil para servir sólo a los usuarios y grupos locales directamente desde los archivos del sistema en lugar de utilizar otros

proveedores de autenticación. Por lo tanto, puede eliminar con seguridad los paquetes **SSSD**, **winbind** y **fprintd** y puede utilizar este perfil en sistemas que requieren una instalación mínima para ahorrar espacio en disco y memoria.

(BZ#1654018)

SSSD ahora actualiza el archivo secrets.tdb de Samba al rotar una contraseña

Una nueva opción **ad_update_samba_machine_account_password** en el archivo **sssd.** conf está ahora disponible en RHEL. Puede utilizarla para configurar SSSD para que actualice automáticamente el archivo **secrets.tdb** de Samba cuando rote la contraseña de dominio de una máquina mientras utiliza Samba.

Sin embargo, si SELinux está en modo de aplicación, SSSD no actualiza el archivo **secrets.tdb**. En consecuencia, Samba no tiene acceso a la nueva contraseña. Para solucionar este problema, ponga SELinux en modo permisivo.

(BZ#1793727)

SSSD ahora aplica los GPO de AD por defecto

La configuración por defecto de la opción de SSSD **ad_gpo_access_control** es ahora **enforcing**. En RHEL 8, SSSD aplica por defecto las reglas de control de acceso basadas en los objetos de política de grupo (GPO) de Active Directory.

Red Hat recomienda asegurarse de que los GPOs están configurados correctamente en Active Directory antes de actualizar de RHEL 7 a RHEL 8. Si no desea aplicar los GPOs, cambie el valor de la opción **ad_gpo_access_control** en el archivo **/etc/sssd/sssd.conf** a **permisivo**.

(JIRA:RHELPLAN-51289)

El Servidor de Directorio ahora soporta el atributo de operación pwdReset

Esta mejora añade soporte para el atributo de operación **pwdReset** a Directory Server. Cuando un administrador cambia la contraseña de un usuario, Directory Server establece **pwdReset** en la entrada del usuario a **true**. Como resultado, las aplicaciones pueden utilizar este atributo para identificar si la contraseña de un usuario ha sido restablecida por un administrador.

Tenga en cuenta que **pwdReset** es un atributo operativo y, por lo tanto, los usuarios no pueden editarlo.

(BZ#1775285)

El Servidor de Directorios ahora registra el trabajo y el tiempo de operación en las entradas de RESULTADO

Con esta actualización, el servidor de directorios registra ahora dos valores de tiempo adicionales en las **entradas de RESULTADO en el archivo `/var/log/dirsrv/slapd-**

- El valor **wtime** indica el tiempo que tarda una operación en pasar de la cola de trabajo a un hilo de trabajo.
- El valor de **optime** muestra el tiempo que tardó la operación real en completarse una vez que un hilo trabajador inició la operación.

Los nuevos valores proporcionan información adicional sobre cómo el Servidor de Directorio maneja la carga y procesa las operaciones.

Para más detalles, consulte la sección Referencia de registro de acceso en la Referencia de configuración, comandos y archivos del servidor de directorio de Red Hat.

(BZ#1850275)

6.1.14. Escritorio

Ya está disponible la sesión de solicitud única

Ahora puede iniciar GNOME en una sesión de una sola aplicación, también conocida como modo quiosco. En esta sesión, GNOME muestra sólo una ventana de pantalla completa de una aplicación que haya configurado.

Para activar la sesión de aplicación única:

1. Instale el paquete **gnome-session-kiosk-session**:

```
# yum install gnome-session-kiosk-session
```

2. Cree y edite el archivo **$HOME/.local/bin/redhat-kiosk** del usuario que abrirá la sesión de aplicación única.
   En el archivo, introduzca el nombre del ejecutable de la aplicación que desea lanzar.

   Por ejemplo, para lanzar la aplicación **Text Editor**:

```
#!/bin/sh

gedit &
```

3. Haz que el archivo sea ejecutable:

```
$ chmod x $HOME/.local/bin/redhat-kiosk
```

4. En la pantalla de inicio de sesión de GNOME, seleccione la sesión **Kiosk** en el menú del botón de la rueda dentada e inicie la sesión como usuario de una sola aplicación.

(BZ#1739556)

tigervnc ha sido rebasado a la versión 1.10.1

La suite **tigervnc** ha sido reajustada a la versión 1.10.1. La actualización contiene varias correcciones y mejoras. Las más notables:

- tigervnc ahora sólo soporta el inicio del servidor de computación de red virtual (VNC) utilizando el administrador de servicios **systemd**.
- El portapapeles ahora soporta Unicode completo en el visor nativo, **WinVNC** y Xvnc/libvnc.so.
- El cliente nativo ahora respetará el almacén de confianza del sistema cuando verifique los certificados del servidor.
- Se ha eliminado el servidor web Java.
- **x0vncserver** ahora puede ser configurado para permitir sólo conexiones locales.
- **x0vncserver** ha recibido correcciones para cuando sólo se comparte una parte de la pantalla.

- El sondeo es ahora por defecto en **WinVNC**.
- Se ha mejorado la compatibilidad con el servidor VNC de VMware.
- Se ha mejorado la compatibilidad con algunos métodos de entrada en macOS.
- Se ha mejorado la "reparación" automática de los artefactos JPEG.

(BZ#1806992)

6.1.15. Infraestructuras gráficas

Compatibilidad con las nuevas tarjetas gráficas

Las siguientes tarjetas gráficas son ahora totalmente compatibles:

- La familia AMD Navi 14, que incluye los siguientes modelos:
  - Radeon RX 5300
  - Radeon RX 5300 XT
  - Radeon RX 5500
  - Radeon RX 5500 XT
- La familia de APUs AMD Renoir, que incluye los siguientes modelos:
  - Ryzen 3 4300U
  - Ryzen 5 4500U, 4600U y 4600H
  - Ryzen 7 4700U, 4800U y 4800H
- La familia de APU AMD Dali, que incluye los siguientes modelos:
  - Athlon Silver 3050U
  - Athlon Gold 3150U
  - Ryzen 3 3250U

Además, se han actualizado los siguientes controladores gráficos:

- El controlador Matrox **mgag200**

(JIRA:RHELPLAN-55009)

Aceleración por hardware con Nvidia Volta y Turing

El controlador de gráficos **de nouveau** soporta ahora la aceleración por hardware con las familias de GPUs Nvidia Volta y Turing. Como resultado, el escritorio y las aplicaciones que utilizan gráficos 3D ahora se renderizan de forma eficiente en la GPU. Además, esto libera la CPU para otras tareas y mejora la capacidad de respuesta general del sistema.

(JIRA:RHELPLAN-57564)

Reducción del tearing de la pantalla en XWayland

El backend de visualización de XWayland permite ahora la extensión XPresent. Con XPresent, las aplicaciones pueden actualizar eficazmente el contenido de sus ventanas, lo que reduce el tearing de la pantalla.

Esta función mejora notablemente el renderizado de la interfaz de usuario de las aplicaciones OpenGL a pantalla completa, como los editores 3D.

(JIRA:RHELPLAN-57567)

6.1.16. La consola web

Establecer privilegios desde la sesión de la consola web

Con esta actualización, la consola web proporciona una opción para cambiar entre el acceso administrativo y el acceso limitado desde dentro de una sesión de usuario. Puede cambiar entre los modos haciendo clic en el indicador **Administrative access** o **Limited access** en su sesión de la consola web.

(JIRA:RHELPLAN-42395)

Mejoras en la búsqueda de registros

Con esta actualización, la consola web introduce un cuadro de búsqueda que admite varias formas nuevas de que los usuarios puedan buscar entre los registros. El cuadro de búsqueda admite la búsqueda de expresiones regulares en los mensajes de registro, especificando el servicio o buscando entradas con campos de registro específicos.

(BZ#1710731)

La página de resumen muestra informes más detallados de Insights

Con esta actualización, cuando una máquina está conectada a Red Hat Insights, la tarjeta **Health** en la página **Overview** de la consola web muestra información más detallada sobre el número de accesos y su prioridad.

(JIRA:RHELPLAN-42396)

6.1.17. Roles del sistema Red Hat Enterprise Linux

Terminal log rol añadido a RHEL System Roles

Con esta mejora, se ha añadido un nuevo rol *Terminal log* (TLOG) a los roles de sistema de RHEL que se envían con el paquete **rhel-system-roles**. Ahora los usuarios pueden utilizar el rol **tlog** para establecer y configurar la grabación de sesiones mediante Ansible.

Actualmente, el rol **tlog** soporta las siguientes tareas:

- Configurar **tlog** para que registre los datos de la grabación en el diario de **systemd**
- Habilitar la grabación de sesiones para usuarios y grupos explícitos, a través de SSSD

(BZ#1822158)

La función de sistema de registro de RHEL ya está disponible para Ansible

Con el rol de sistema de registro, puede desplegar varias configuraciones de registro de forma consistente en hosts locales y remotos. Puede configurar un host RHEL como servidor para recopilar registros de muchos sistemas cliente.

(BZ#1677739)

rhel-system-roles-sap totalmente compatible

El paquete **rhel-system-roles-sap**, que anteriormente estaba disponible como una Muestra de Tecnología, es ahora totalmente compatible. Proporciona funciones del sistema Red Hat Enterprise Linux (RHEL) para SAP, que pueden utilizarse para automatizar la configuración de un sistema RHEL para ejecutar cargas de trabajo SAP. Estos roles reducen en gran medida el tiempo de configuración de un sistema para ejecutar cargas de trabajo de SAP, aplicando automáticamente los ajustes óptimos que se basan en las mejores prácticas descritas en las notas pertinentes de SAP. El acceso está limitado a las ofertas de RHEL for SAP Solutions. Póngase en contacto con el Servicio de Atención al Cliente de Red Hat si necesita ayuda con su suscripción.

Los siguientes nuevos roles del paquete **rhel-system-roles-sap** son totalmente compatibles:

- **sap-preconfigure**
- **sap-netweaver-preconfigure**
- **sap-hana-preconfigure**

Para más información, véase Red Hat Enterprise Linux System Roles for SAP .

(BZ#1660832)

El rol de sistema RHEL de métricas ya está disponible para Ansible.

Con la **métrica** RHEL System Role, puede configurar, para los hosts locales y remotos:

- servicios de análisis de rendimiento a través de la aplicación **pcp**
- visualización de estos datos mediante un servidor **grafana**
- consulta de estos datos utilizando la fuente de datos **redis** sin tener que configurar manualmente estos servicios por separado.

(BZ#1890499)

rhel-system-roles-sap actualizado

Los paquetes ***rhel-system-roles-sap*** han sido actualizados a la versión 2.0.0, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Mejora de la configuración y comprobación del nombre de host
- Mejora de la detección y el tratamiento del estado de **la uuidd**
- Añadir soporte para la opción **--check (-c)**
- Aumentar los límites de **no-fichero** de 32800 a 65536
- Añadir el archivo **nfs-utils** a **sap_preconfigure_packages***
- Desactivar **firewalld**. Con este cambio deshabilitamos **firewalld** sólo cuando está instalado.
- Añadir las versiones mínimas requeridas del paquete de **instalación** para RHEL 8.0 y RHEL 8.1.
- Mejorar el manejo del archivo **tmpfiles.d/sap.conf**

- Apoyar la ejecución de un solo paso o la comprobación de las notas de SAP
- Añadir los paquetes **compat-sap-c** necesarios
- Mejorar la gestión de la instalación de paquetes mínimos
- Detectar si se requiere un reinicio después de aplicar los Roles del Sistema RHEL
- Soporta la configuración de cualquier estado de SElinux. El estado por defecto es **"deshabilitado"**
- Ya no falla si hay más de una línea con direcciones IP idénticas
- Ya no se modifica **/etc/hosts** si hay más de una línea que contiene **sap_ip**
- Soporte para HANA en RHEL 7.7
- Soporte para añadir un repositorio para las herramientas de servicio y productividad de IBM para Power, necesarias para SAP HANA en la plataforma **ppc64le**

(BZ#1844190)

6.1.18. Virtualización

La migración de una máquina virtual a un host con una configuración TSC incompatible ahora falla más rápido

Anteriormente, la migración de una máquina virtual a un host con una configuración de contador de tiempo (TSC) incompatible fallaba al final del proceso. Con esta actualización, al intentar dicha migración se genera un error antes de que se inicie el proceso de migración.

(JIRA:RHELPLAN-45950)

Soporte de virtualización para los procesadores AMD EPYC de segunda generación

Con esta actualización, la virtualización en RHEL 8 añade soporte para los procesadores AMD EPYC de segunda generación, también conocidos como EPYC Rome. Como resultado, las máquinas virtuales alojadas en RHEL 8 ahora pueden utilizar el modelo de CPU **EPYC-Rome** y utilizar las nuevas características que los procesadores proporcionan.

(JIRA:RHELPLAN-45959)

Nuevo comando: virsh iothreadset

Esta actualización introduce el comando **virsh iothreadset**, que puede utilizarse para configurar el sondeo dinámico de IOThread. Esto hace posible configurar máquinas virtuales con latencias más bajas para cargas de trabajo de E/S intensivas a expensas de un mayor consumo de CPU para el IOThread. Para las opciones específicas, consulte la página man de virsh.

(JIRA:RHELPLAN-45958)

KVM admite ahora UMIP en los procesadores Intel Core de 10ª generación

Con esta actualización, la función de prevención de instrucciones en modo usuario (UMIP) es ahora compatible con KVM para los hosts que se ejecutan en procesadores Intel Core de 10ª generación, también conocidos como servidores Ice Lake. La función UMIP emite una excepción de protección general si ciertas instrucciones, como **sgdt**, **sidt**, **sldt**, **smsw** y **str**, se ejecutan cuando el nivel de

privilegio actual (CPL) es mayor que 0. Como resultado, UMIP garantiza la seguridad del sistema al impedir que las aplicaciones no autorizadas accedan a ciertas configuraciones de todo el sistema que pueden utilizarse para iniciar ataques de escalada de privilegios.

(JIRA:RHELPLAN-45957)

La biblioteca **libvirt** ahora soporta la asignación de ancho de banda de memoria

libvirt ahora soporta la Asignación de Ancho de Banda de Memoria (MBA). Con MBA, puede asignar partes del ancho de banda de la memoria del host en hilos de vCPU utilizando el elemento **<memorytune>** en la sección **<cputune>**.

MBA es una extensión de la función Cache QoS Enforcement (CQE) existente en los procesadores Intel Xeon v4, también conocidos como servidor Broadwell. Para las tareas que están asociadas a la afinidad de la CPU, el mecanismo utilizado por MBA es el mismo que en CQE.

(JIRA:RHELPLAN-45956)

Las máquinas virtuales de RHEL 6 ahora soportan el tipo de máquina Q35

Las máquinas virtuales (VM) alojadas en RHEL 8 que utilizan RHEL 6 como sistema operativo invitado ahora pueden utilizar Q35, un tipo de máquina más moderno basado en PCI Express. Esto proporciona una variedad de mejoras en las características y el rendimiento de los dispositivos virtuales, y garantiza que una gama más amplia de dispositivos modernos sean compatibles con las VM de RHEL 6.

(JIRA:RHELPLAN-45952)

Todos los eventos registrados de QEMU tienen ahora una marca de tiempo. Como resultado, los usuarios pueden solucionar más fácilmente sus máquinas virtuales utilizando los registros guardados en el directorio **/var/log/libvirt/qemu/.**

Los registros de QEMU ahora incluyen marcas de tiempo para los eventos del servidor de especias

Esta actualización añade marcas de tiempo a los registros de eventos de `spice-server`. Por lo tanto, todos los eventos QEMU registrados tienen ahora una marca de tiempo. Como resultado, los usuarios pueden solucionar más fácilmente sus máquinas virtuales utilizando los registros guardados en el directorio **/var/log/libvirt/qemu/**.

(JIRA:RHELPLAN-45945)

El dispositivo **bochs-display** es ahora compatible

RHEL 8.3 y posteriores introducen el dispositivo de visualización Bochs, que es más seguro que el dispositivo **stdvga** utilizado actualmente. Tenga en cuenta que todas las máquinas virtuales (VM) compatibles con **bochs-display** lo utilizarán por defecto. Esto incluye principalmente las VMs que utilizan la interfaz UEFI.

(JIRA:RHELPLAN-45939)

Protección MDS optimizada para máquinas virtuales

Con esta actualización, un host RHEL 8 puede informar a sus máquinas virtuales (VM) si son vulnerables al muestreo de datos microarquitectónicos (MDS). Las máquinas virtuales que no son vulnerables no utilizan medidas contra el MDS, lo que mejora su rendimiento.

(JIRA:RHELPLAN-45937)

Ahora es posible crear imágenes de disco QCOW2 en RBD

Con esta actualización, es posible crear imágenes de disco QCOW2 en el almacenamiento RADOS Block Device (RBD). Como resultado, las máquinas virtuales pueden utilizar servidores RBD para sus back ends de almacenamiento con imágenes QCOW2.

Sin embargo, hay que tener en cuenta que el rendimiento de escritura de las imágenes de disco QCOW2 en el almacenamiento RBD es actualmente inferior al previsto.

(JIRA:RHELPLAN-45936)

El número máximo de dispositivos VFIO soportados ha aumentado a 64

Con esta actualización, puede adjuntar hasta 64 dispositivos PCI que utilizan VFIO a una sola máquina virtual en un host RHEL 8. Esta cifra es superior a la de 32 de RHEL 8.2 y anteriores.

(JIRA:RHELPLAN-45930)

los comandos**discard y write-zeroes** están ahora soportados en QEMU/KVM

Con esta actualización, los comandos de **descarte** y **escritura de ceros** para **virtio-blk** son ahora compatibles con QEMU/KVM. Como resultado, las máquinas **virtuales** pueden utilizar el dispositivo virtio-blk para descartar los sectores no utilizados de un SSD, llenar los sectores con ceros cuando se vacían, o ambos. Esto puede utilizarse para aumentar el rendimiento del SSD o para garantizar que una unidad se borre de forma segura.

(JIRA:RHELPLAN-45926)

RHEL 8 ahora es compatible con IBM POWER 9 XIVE

Esta actualización introduce en RHEL 8 la compatibilidad con la función External Interrupt Virtualization Engine (XIVE) de IBM POWER9. Como resultado, las máquinas virtuales (VM) que se ejecutan en un hipervisor RHEL 8 en un sistema IBM POWER 9 pueden utilizar XIVE, lo que mejora el rendimiento de las VM de E/S intensiva.

(JIRA:RHELPLAN-45922)

Compatibilidad del Grupo de Control v2 con las máquinas virtuales

Con esta actualización, la suite libvirt soporta grupos de control v2. Como resultado, las máquinas virtuales alojadas en RHEL 8 pueden aprovechar las capacidades de control de recursos del grupo de control v2.

(JIRA:RHELPLAN-45920)

Las IPI paravirtualizadas son ahora compatibles con las máquinas virtuales de Windows

Con esta actualización, se ha añadido el indicador **hv_ipi** a las iluminaciones de hipervisor compatibles con las máquinas virtuales (VM) de Windows. Esto permite que las interrupciones entre procesadores (IPI) se envíen a través de una hiperllamada. Como resultado, las IPIs pueden realizarse más rápidamente en las VMs que ejecutan un SO Windows.

(JIRA:RHELPLAN-45918)

Ahora es posible migrar máquinas virtuales con la caché de disco activada

Esta actualización hace que el hipervisor KVM de RHEL 8 sea compatible con la migración en vivo de la caché de disco. Como resultado, ahora es posible migrar en vivo máquinas virtuales con la caché de disco habilitada.

(JIRA:RHELPLAN-45916)

las interfaces macvtap ahora pueden ser utilizadas por las máquinas virtuales en sesiones no privilegiadas

Ahora es posible que las máquinas virtuales (VM) utilicen una interfaz macvtap previamente creada por un proceso con privilegios. En particular, esto permite que las máquinas virtuales iniciadas por la sesión de **usuario** sin privilegios de **libvirtd** utilicen una interfaz macvtap.

Para ello, primero cree una interfaz macvtap en un entorno privilegiado y configúrela para que sea propiedad del usuario que va a ejecutar **libvirtd** en una sesión sin privilegios. Puede hacer esto usando una aplicación de gestión como la consola web, o usando utilidades de línea de comandos como root, por ejemplo:

```
# ip link add link en2 name mymacvtap0 address 52:54:00:11:11:11 type macvtap mode bridge
# chown myuser /dev/tap$(cat /sys/class/net/mymacvtap0/ifindex)
# ip link set mymacvtap0 up
```

A continuación, modifique el subelemento **<target>** de la configuración de la VM **<interface>** para que haga referencia a la interfaz macvtap recién creada:

```
<interface type='ethernet'>
  <model type='virtio'/>
  <mac address='52:54:00:11:11:11'/>
  <target dev='mymacvtap0' managed='no'/>
</interface>
```

Con esta configuración, si **libvirtd** se ejecuta como el usuario **myuser**, la VM utilizará la interfaz macvtap existente cuando se inicie.

(JIRA:RHELPLAN-45915)

Las máquinas virtuales ya pueden utilizar las características de los procesadores Intel Core de 10ª generación

Los nombres de los modelos de CPU **Icelake-Server** e **Icelake-Client** están ahora disponibles para las máquinas virtuales (VMs). En los hosts con procesadores Intel Core de 10ª generación, el uso de **Icelake-Server** o **Icelake-Client** como tipo de CPU en la configuración XML de una VM hace que las nuevas características de estas CPU estén expuestas a la VM.

(JIRA:RHELPLAN-45911)

QEMU ahora soporta el cifrado LUKS

Con esta actualización, es posible crear discos virtuales utilizando el cifrado de Linux Unified Key Setup (LUKS). Puede cifrar los discos al crear el volumen de almacenamiento incluyendo el campo **<encryption>** en la configuración XML de la máquina virtual (VM). También puede hacer que el disco virtual cifrado **LUKS** sea completamente transparente para la VM incluyendo el campo **<encryption>** en la definición del dominio del disco en el archivo de configuración XML.

(JIRA:RHELPLAN-45910)

Registros mejorados para nbdkit

El registro del servicio **nbdkit** ha sido modificado para ser menos verboso. Como resultado, **nbdkit** registra sólo los mensajes potencialmente importantes, y los registros creados durante las conversiones **virt-v2v** son más cortos y fáciles de analizar.

(JIRA:RHELPLAN-45909)

Mejora de la coherencia de las etiquetas de seguridad y los permisos de SELinux de las máquinas virtuales

Con esta actualización, el servicio **libvirt** puede registrar las etiquetas de seguridad SELinux y los permisos asociados a los archivos, y restaurar las etiquetas después de modificar los archivos. Como resultado, por ejemplo, el uso de utilidades **libguestfs** para modificar una imagen de disco de máquina virtual (VM) propiedad de un usuario específico ya no cambia el propietario de la imagen a root.

Tenga en cuenta que esta función no funciona en sistemas de archivos que no admiten atributos de archivo extendidos, como NFS.

(JIRA:RHELPLAN-45908)

QEMU utiliza ahora la biblioteca gcrypt para los cifrados XTS

Con esta actualización, el emulador QEMU ha sido cambiado para utilizar la implementación del modo de cifrado XTS proporcionada por la biblioteca **gcrypt**. Esto mejora el rendimiento de E/S de las máquinas virtuales cuyo almacenamiento anfitrión utiliza el controlador de cifrado **luks** nativo de QEMU.

(JIRA:RHELPLAN-45904)

Los controladores de Windows Virtio ahora se pueden actualizar mediante Windows Updates

Con esta actualización, se inicia por defecto una nueva cadena **SMBIOS** estándar cuando se inicia QEMU. Los parámetros proporcionados en los campos de **SMBIOS** permiten generar IDs para el hardware virtual que se ejecuta en la máquina virtual(VM). Como resultado, Windows Update puede identificar el hardware virtual y el tipo de máquina del hipervisor RHEL, y actualizar los controladores de Virtio en las VM que ejecutan Windows 10 , Windows Server 2016 y Windows Server 2019 .

(JIRA:RHELPLAN-45901)

Nuevo comando: virsh guestinfo

El comando **virsh guestinfo** ha sido introducido en RHEL 8.3. Esto hace posible reportar los siguientes tipos de información sobre una máquina virtual (VM):

- Información sobre el sistema operativo y el sistema de archivos del huésped
- Usuarios activos
- La zona horaria utilizada

Antes de ejecutar **virsh guestinfo**, asegúrese de que el paquete *qemu-guest-agent* está instalado. Además, el canal **guest_agent** debe estar habilitado en la configuración XML de la VM, por ejemplo de la siguiente manera:

```
<channel type='unix'>
  <target type='virtio' name='org.qemu.guest_agent.0'/>
</channel>
```

(JIRA:RHELPLAN-45900)

Las entradas VNNI para BFLOAT16 son ahora compatibles con KVM

Con esta actualización, las instrucciones de red neuronal vectorial (VNNI) que admiten entradas **BFLOAT16**, también conocidas como instrucciones **AVX512_BF16**, son ahora compatibles con KVM

para los hosts que se ejecutan en los procesadores escalables Intel Xeon de tercera generación, también conocidos como Cooper Lake. Como resultado, el software invitado puede ahora utilizar las instrucciones **AVX512_BF16** dentro de las máquinas virtuales, habilitándolas en la configuración de la CPU virtual.

(JIRA:RHELPLAN-45899)

Nuevo comando: virsh pool-capabilities

RHEL 8.3 introduce la opción del comando **virsh pool-capabilities**. Este comando muestra información que puede ser utilizada para crear pools de almacenamiento, así como volúmenes de almacenamiento dentro de cada pool, en su host. Esto incluye:

- Tipos de pool de almacenamiento
- Formatos de origen del pool de almacenamiento
- Tipos de formato de volumen de almacenamiento de destino

(JIRA:RHELPLAN-45884)

Compatibilidad con CPUID.1F en máquinas virtuales con procesadores Intel Xeon Platinum serie 9200

Con esta actualización, las máquinas virtuales alojadas en RHEL 8 pueden configurarse con una topología de CPU virtual de múltiples troqueles, utilizando la función de hoja de Enumeración de Topología Extendida (CPUID.1F). Esta característica es soportada por los procesadores Intel Xeon Platinum de la serie 9200, anteriormente conocidos como Cascade Lake. Como resultado, ahora es posible en los hosts que utilizan procesadores Intel Xeon Platinum serie 9200 crear una topología vCPU que refleje la topología de la CPU física del host.

(JIRA:RHELPLAN-37573, JIRA:RHELPLAN-45934)

Las máquinas virtuales ya pueden utilizar las funciones de los procesadores escalables Intel Xeon de tercera generación

El nombre del modelo de CPU **Cooperlake** está ahora disponible para las máquinas virtuales (VM). El uso de **Cooperlake** como tipo de CPU en la configuración XML de una VM hace que las nuevas características de los procesadores escalables Intel Xeon de tercera generación estén expuestas a la VM, si el host utiliza esta CPU.

(JIRA:RHELPLAN-37570)

La memoria persistente Intel Optane ahora es compatible con KVM

Con esta actualización, las máquinas virtuales alojadas en RHEL 8 pueden beneficiarse de la tecnología de memoria persistente Intel Optane, anteriormente conocida como Intel Crystal Ridge. Los dispositivos de almacenamiento de memoria persistente Intel Optane proporcionan una tecnología de memoria persistente de clase de centro de datos, que puede aumentar significativamente el rendimiento de las transacciones.

(JIRA:RHELPLAN-14068)

Las máquinas virtuales ahora pueden utilizar Intel Processor Trace

Con esta actualización, las máquinas virtuales (VM) alojadas en RHEL 8 pueden utilizar la función Intel Processor Trace (PT). Cuando su anfitrión utiliza una CPU que soporta Intel PT, puede utilizar un software especializado de Intel para recoger una variedad de métricas sobre el rendimiento de la CPU

de su VM. Tenga en cuenta que esto también requiere habilitar la función **intel-pt** en la configuración XML de la VM.

(JIRA:RHELPLAN-7788)

Ahora se pueden asignar dispositivos DASD a máquinas virtuales en IBM Z

Los dispositivos de almacenamiento de acceso directo (DASD) proporcionan una serie de características de almacenamiento específicas. Utilizando la función **vfio-ccw**, puede asignar DASDs como dispositivos mediados a sus máquinas virtuales (VMs) en hosts IBM Z. Esto, por ejemplo, hace posible que la VM acceda a un conjunto de datos de z/OS, o que comparta los DASDs asignados con una máquina z/OS.

(JIRA:RHELPLAN-40234)

Soporte de IBM Secure Execution para IBM Z

Cuando utilice hardware IBM Z para ejecutar su host RHEL 8, puede mejorar la seguridad de sus máquinas virtuales (VM) configurando IBM Secure Execution para las VM. IBM Secure Execution, también conocido como Virtualización Protegida, impide que el sistema anfitrión acceda al estado y al contenido de la memoria de una VM.

Como resultado, incluso si el host está comprometido, no puede ser utilizado como un vector para atacar el sistema operativo invitado. Además, la ejecución segura puede utilizarse para evitar que los hosts no confiables obtengan información sensible de la máquina virtual.

(JIRA:RHELPLAN-14754)

6.1.19. RHEL en entornos de nube

cloud-utils-growpart rebasado a 0.31

El paquete **cloud-utils-growpart** ha sido actualizado a la versión 0.31, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Se ha corregido un error que impedía que los discos GPT crecieran más allá de los 2TB.
- La operación **growpart** ya no falla cuando el sector de inicio y el tamaño son iguales.
- El redimensionamiento de una partición mediante la utilidad **sgdisk** fallaba anteriormente en algunos casos. Este problema ya se ha solucionado.

(BZ#1846246)

6.1.20. Contenedores

la imagendel contenedorskopeo ya está disponible

La imagen de contenedor **registry.redhat.io/rhel8/skopeo** es una implementación en contenedor del paquete **skopeo**. La herramienta **skopeo** es una utilidad de línea de comandos que realiza varias operaciones en imágenes de contenedores y repositorios de imágenes. Esta imagen de contenedor le permite inspeccionar imágenes de contenedor en un registro, eliminar una imagen de contenedor de un registro y copiar imágenes de contenedor de un registro de contenedor no autenticado a otro. Para extraer la imagen de contenedor **registry.redhat.io/rhel8/skopeo**, necesita una suscripción activa a Red Hat Enterprise Linux.

(BZ#1627900)

la imagen del contenedor**buildah** ya está disponible

La imagen de contenedor **registry.redhat.io/rhel8/buildah** es una implementación en contenedor del paquete **buildah**. La herramienta **buildah** facilita la construcción de imágenes de contenedores OCI. Esta imagen de contenedor le permite construir imágenes de contenedor sin necesidad de instalar el paquete **buildah** en su sistema. El caso de uso no cubre la ejecución de esta imagen en modo sin raíz como usuario no root. Para obtener la imagen de contenedor **registry.redhat.io/rhel8/buildah**, necesita una suscripción activa a Red Hat Enterprise Linux.

(BZ#1627898)

Ya está disponible la API RESTful de Podman v2.0

La nueva API de Podman 2.0 basada en REST sustituye a la antigua API remota basada en la biblioteca varlink. La nueva API funciona tanto en un entorno rootful como en uno sin root y proporciona una capa de compatibilidad con Docker.

(JIRA:RHELPLAN-37517)

La instalación de Podman no requiere **container-selinux**

Con esta mejora, la instalación del paquete **container-selinux** es ahora opcional durante la construcción del contenedor. Como resultado, Podman tiene menos dependencias de otros paquetes.

(BZ#1806044)

6.1.21. Nuevos conductores

Controladores de red

- Controlador CAN para dispositivos Kvaser CAN/USB (kvaser_usb.ko.xz)
- Controlador para dispositivos UCAN de Theobroma Systems (ucan.ko.xz)
- Pensando Ethernet NIC Driver (ionic.ko.xz)

Controladores de gráficos y controladores varios

- Marco genérico del procesador remoto (remoteproc.ko.xz)
- Inyección de estado C en el paquete para CPUs Intel® (intel_powerclamp.ko.xz)
- Controlador térmico X86 PKG TEMP (x86_pkg_temp_thermal.ko.xz)
- Controlador térmico INT3402 (int3402_thermal.ko.xz)
- Controlador térmico ACPI INT3403 (int3403_thermal.ko.xz)
- Intel® acpi thermal rel misc dev driver (acpi_thermal_rel.ko.xz)
- INT3400 Thermal driver (int3400_thermal.ko.xz)
- Manejador de zona térmica común Intel® INT340x (int340x_thermal_zone.ko.xz)
- Controlador del dispositivo de información térmica del procesador (processor_thermal_device.ko.xz)
- Controlador térmico Intel® PCH (intel_pch_thermal.ko.xz)

- Gema DRM ttm helpers (drm_ttm_helper.ko.xz)
- Registro del nodo del dispositivo para los controladores cec (cec.ko.xz)
- Fairchild FUSB302 Type-C Chip Driver (fusb302.ko.xz)
- VHOST IOTLB (vhost_iotlb.ko.xz)
- backend de vhost basado en vDPA para virtio (vhost_vdpa.ko.xz)
- Controlador del reloj PTP virtual de VMware (ptp_vmw.ko.xz)
- Controlador Intel® LPSS PCI (intel-lpss-pci.ko.xz)
- Controlador del núcleo Intel® LPSS (intel-lpss.ko.xz)
- Controlador Intel® LPSS ACPI (intel-lpss-acpi.ko.xz)
- Controlador Mellanox watchdog (mlx_wdt.ko.xz)
- Controlador FAN de Mellanox (mlxreg-fan.ko.xz)
- Controlador de acceso de E/S Mellanox regmap (mlxreg-io.ko.xz)
- Controlador del buzón Intel® speed select interface pci (isst_if_mbox_pci.ko.xz)
- Controlador del buzón de la interfaz Intel® de selección de velocidad (isst_if_mbox_msr.ko.xz)
- Controlador Intel® speed select interface mmio (isst_if_mmio.ko.xz)
- Controlador Mellanox LED regmap (leds-mlxreg.ko.xz)
- simulador de dispositivos vDPA (vdpa_sim.ko.xz)
- Controlador Intel® Tiger Lake PCH pinctrl/GPIO (pinctrl-tigerlake.ko.xz)
- Controlador SSP SPI PXA2xx (spi-pxa2xx-platform.ko.xz)
- Código PCI-SPI CE4100/LPSS para el controlador PXA (spi-pxa2xx-pci.ko.xz)
- Interfaz PCI de Hyper-V (pci-hyperv-intf.ko.xz)
- controlador de bus vDPA para dispositivos virtio (virtio_vdpa.ko.xz)

6.1.22. Controladores actualizados

Actualización de los controladores de red

- El controlador NIC virtual de VMware vmxnet3 (vmxnet3.ko.xz) ha sido actualizado a la versión 1.5.0.0-k.
- Realtek RTL8152/RTL8153 Based USB Ethernet Adapters (r8152.ko.xz) ha sido actualizado a la versión 1.09.10.
- El controlador de red Broadcom BCM573xx (bnxt_en.ko.xz) ha sido actualizado a la versión 1.10.1.

- El controlador del procesador de flujo Netronome (NFP) (nfp.ko.xz) ha sido actualizado a la versión 4.18.0-240.el8.x86_64.
- El controlador de la interfaz de host del conmutador Intel® Ethernet (fm10k.ko.xz) ha sido actualizado a la versión 0.27.1-k.
- El controlador Intel® Ethernet Connection E800 Series Linux (ice.ko.xz) ha sido actualizado a la versión 0.8.2-k.

Actualizaciones de los controladores de almacenamiento

- El controlador Emulex LightPulse Fibre Channel SCSI (lpfc.ko.xz) ha sido actualizado a la versión 0:12.8.0.1.
- El controlador QLogic FCoE (bnx2fc.ko.xz) ha sido actualizado a la versión 2.12.13.
- El controlador del dispositivo LSI MPT Fusion SAS 3.0 (mpt3sas.ko.xz) ha sido actualizado a la versión 34.100.00.00.
- La versión del controlador HP Smart Array (hpsa.ko.xz) ha sido actualizada a la versión 3.4.20-170-RH5.
- El controlador HBA de canal de fibra de QLogic (qla2xxx.ko.xz) ha sido actualizado a la versión 10.01.00.25.08.3-k.
- El controlador Broadcom MegaRAID SAS (megaraid_sas.ko.xz) ha sido actualizado a la versión 07.714.04.00-rh1.

Actualizaciones de gráficos y controladores varios

- El controlador drm independiente para el dispositivo VMware SVGA (vmwgfx.ko.xz) ha sido actualizado a la versión 2.17.0.0.
- Coprocesador Crypto para las tarjetas Chelsio Terminator. (chcr.ko.xz) ha sido actualizado a la versión 1.0.0.0-ko.

6.2. CORRECCIÓN DE ERRORES

Esta parte describe los errores corregidos en Red Hat Enterprise Linux 8.3 que tienen un impacto significativo en los usuarios.

6.2.1. Creación del instalador y de la imagen

La configuración inicial de RHEL 8 ahora funciona correctamente a través de SSH

Anteriormente, la interfaz de configuración inicial de RHEL 8 no se mostraba cuando se iniciaba la sesión en el sistema mediante SSH. Como consecuencia, era imposible realizar la configuración inicial en una máquina RHEL 8 gestionada mediante SSH. Este problema se ha solucionado, y la configuración inicial de RHEL 8 ahora funciona correctamente cuando se realiza a través de SSH.

(BZ#1676439)

La instalación falló al utilizar el comando **reboot --kexec**

Anteriormente, la instalación de RHEL 8 fallaba cuando se utilizaba un archivo Kickstart que contenía el comando **reboot --kexec**.

Con esta actualización, la instalación con **reboot --kexec** ahora funciona como se esperaba.

(BZ#1672405)

America/New York zona horaria ahora se puede establecer correctamente

Anteriormente, el proceso de instalación interactiva de Anaconda no permitía a los usuarios establecer la zona horaria *America/New York* cuando se utilizaba un archivo kickstart. Con esta actualización, los usuarios pueden ahora establecer *America/New York* como zona horaria preferida en el instalador interactivo si no se especifica una zona horaria en el archivo kickstart.

(BZ#1665428)

Los contextos de SELinux ahora se establecen correctamente

Anteriormente, cuando SELinux estaba en modo de aplicación, los contextos incorrectos de SELinux en algunas carpetas y archivos daban lugar a denegaciones inesperadas del CVA al intentar acceder a estos archivos después de la instalación.

Con esta actualización, Anaconda establece los contextos SELinux correctos. Como resultado, ahora puede acceder a las carpetas y archivos sin tener que reetiquetar manualmente el sistema de archivos.

(BZ#1775975)

El particionamiento automático crea ahora una partición /**boot** válida

Anteriormente, cuando se instalaba RHEL en un sistema que utilizaba el particionamiento automático o un archivo kickstart con particiones preconfiguradas, el instalador creaba un esquema de particionamiento que podía contener una partición /**boot** no válida. En consecuencia, el proceso de instalación automática terminaba prematuramente porque fallaba la verificación del esquema de particionamiento. Con esta actualización, Anaconda crea un esquema de particionamiento que contiene una partición /**boot** válida. Como resultado, la instalación automática se completa como se esperaba.

(BZ#1630299)

La instalación de la interfaz gráfica de usuario utilizando la imagen ISO del DVD binario ahora se completa con éxito sin el registro de la CDN

Anteriormente, cuando se realizaba una instalación GUI utilizando el archivo de imagen ISO de DVD binario, una condición de carrera en el instalador impedía que la instalación procediera hasta que se registrara el sistema utilizando la función Conectar con Red Hat.

Con esta actualización, ahora se puede proceder a la instalación sin registrar el sistema mediante la función Conectar con Red Hat.

(BZ#1823578)

los dispositivos iSCSI o FCoE creados en Kickstart y utilizados en el comando **ignoredisk --only-use** ya no detienen el proceso de instalación

Anteriormente, cuando los dispositivos iSCSI o FCoE creados en Kickstart se utilizaban en el comando **ignoredisk --only-use**, el programa de instalación fallaba con un error similar a **Disk \ "disk/by-id/scsi-360a9800042566643352b476d674a774a" dado en el comando ignoredisk no existe**. Esto detuvo el proceso de instalación.

Con esta actualización, el problema se ha solucionado. El programa de instalación sigue funcionando.

(BZ#1644662)

El registro del sistema usando CDN falló con el mensaje de error Name or service not known

Al intentar registrar un sistema mediante la red de entrega de contenidos (CDN), el proceso de registro falló con el mensaje de error **Name or service not known**

Este problema se produjo porque los valores vacíos de **Custom server URL** y **Custom Base URL** sobreescribieron los valores por defecto para el registro del sistema.

Con esta actualización, los valores vacíos ahora no sobrescriben los valores por defecto, y el registro del sistema se completa con éxito.

(BZ#1862116)

6.2.2. Gestión del software

dnf-automatic ahora actualiza sólo los paquetes con firmas GPG correctas

Anteriormente, el archivo de configuración de **dnf-automatic** no comprobaba las firmas GPG de los paquetes descargados antes de realizar una actualización. Como consecuencia, las actualizaciones no firmadas o firmadas por una clave que no se importaba podían ser instaladas por **dnf-automatic** aunque la configuración del repositorio requiriera la comprobación de la firma GPG(**gpgcheck=1**). Con esta actualización, el problema se ha solucionado, y **dnf-automatic** comprueba las firmas GPG de los paquetes descargados antes de realizar la actualización. Como resultado, sólo se instalan las actualizaciones con firmas GPG correctas desde los repositorios que requieren la comprobación de firmas GPG.

(BZ#1793298)

La coma final ya no provoca la eliminación de entradas en una opción de tipo apéndice

Anteriormente, añadir una coma final (una entrada vacía al final de la lista) a una opción de tipo **append** (por ejemplo, **exclude**, **excludepkgs**, **includepkgs**) hacía que se eliminaran todas las entradas de la opción. Además, añadir dos comas (una entrada vacía) hacía que sólo se utilizaran las entradas que iban después de las comas.

Con esta actualización, se ignoran las entradas vacías que no sean comas iniciales (una entrada vacía al principio de la lista). Como resultado, ahora sólo la coma inicial elimina las entradas existentes de la opción de tipo **apéndice**, y el usuario puede utilizarla para sobrescribir estas entradas.

(BZ#1788154)

6.2.3. Shell y herramientas de línea de comandos

La disposición del disco ReaR ya no incluye entradas para los dispositivos iSCSI y sistemas de archivos de Rancher 2 Longhorn

Esta actualización elimina las entradas para los dispositivos iSCSI de Rancher 2 Longhorn y los sistemas de archivos de la disposición de discos creada por **ReaR**.

(BZ#1843809)

La creación de imágenes de rescate con un archivo de más de 4 GB está ahora habilitada en IBM POWER, little endian

Anteriormente, la utilidad **ReaR** no podía crear imágenes de rescate que contuvieran archivos de más de 4 GB en IBM POWER, arquitectura little endian. Con esta actualización, el problema se ha

solucionado y ahora es posible crear una imagen de rescate con un archivo de más de 4 GB en IBM POWER, little endian.

(BZ#1729502)

6.2.4. Seguridad

SELinux ya no impide que **systemd-journal-gatewayd** llame a **newfstat()** en los archivos **/dev/shm/** utilizados por **corosync**

Anteriormente, la política de SELinux no contenía una regla que permitiera al demonio **systemd-journal-gatewayd** acceder a los archivos creados por el servicio **corosync**. Como consecuencia, SELinux denegaba a **systemd-journal-gatewayd** la llamada a la función **newfstat()** en los archivos de memoria compartida creados por **corosync**. Con esta actualización, SELinux ya no impide que **systemd-journal-gatewayd** llame a **newfstat** () en los archivos de memoria compartida creados por **corosync**.

(BZ#1746398)

Libreswan ahora funciona con **seccomp=enabled** en todas las configuraciones

Antes de esta actualización, el conjunto de llamadas al sistema permitidas en la implementación de soporte de **Libreswan** SECCOMP no coincidía con el nuevo uso de las bibliotecas RHEL. En consecuencia, cuando SECCOMP estaba habilitado en el archivo **ipsec.conf**, el filtrado de llamadas al sistema rechazaba incluso las llamadas al sistema necesarias para el correcto funcionamiento del demonio **pluto**; el demonio era eliminado y el servicio **ipsec** se reiniciaba. Con esta actualización, todas las nuevas llamadas al sistema requeridas han sido permitidas, y **Libreswan** ahora funciona con la opción **seccomp=enabled** correctamente.

(BZ#1544463)

SELinux ya no impide que **auditd** detenga o apague el sistema

Anteriormente, la política de SELinux no contenía una regla que permitiera al demonio de auditoría iniciar una unidad **systemd power_unit_file_t**. En consecuencia, **auditd** no podía detener o apagar el sistema incluso cuando estaba configurado para hacerlo en casos como la falta de espacio en una partición de disco de registro.

Esta actualización de los paquetes **selinux-policy** añade la regla que faltaba, y **auditd** puede ahora detener y apagar correctamente el sistema sólo con SELinux en modo de aplicación.

(BZ#1826788)

IPTABLES_SAVE_ON_STOP ahora funciona correctamente

Anteriormente, la función **IPTABLES_SAVE_ON_STOP** del servicio **iptables** no funcionaba porque los archivos con contenido de tablas IP guardadas recibían un contexto SELinux incorrecto. Esto impedía que el script de **iptables** cambiara los permisos, y posteriormente el script no podía guardar los cambios. Esta actualización define un contexto adecuado para los archivos **iptables.save** e **ip6tables.save**, y crea una regla de transición de nombre de archivo. Como consecuencia, la función **IPTABLES_SAVE_ON_STOP** del servicio **iptables** funciona correctamente.

(BZ#1776873)

Las bases de datos NSCD pueden ahora utilizar diferentes modos

Los dominios en el atributo **nsswitch_domain** tienen acceso a los servicios de Name Service Cache Daemon (NSCD). Cada base de datos NSCD se configura en el archivo **nscd.conf**, y la propiedad

shared determina si la base de datos utiliza el modo de memoria compartida o de socket. Anteriormente, todas las bases de datos NSCD tenían que utilizar el mismo modo de acceso, dependiendo del valor booleano **nscd_use_shm**. Ahora, el uso del socket de flujo Unix está siempre permitido, y por lo tanto diferentes bases de datos NSCD pueden utilizar diferentes modos.

(BZ#1772852)

La utilidad oscap-ssh ahora funciona correctamente al escanear un sistema remoto con --sudo

Cuando se realiza un análisis del Protocolo de Automatización de Contenidos de Seguridad (SCAP) de un sistema remoto utilizando la herramienta **oscap-ssh** con la opción **--sudo**, la herramienta **oscap** del sistema remoto guarda los archivos de resultados del análisis y los archivos de informe en un directorio temporal como usuario **root**. Anteriormente, si se cambiaba la configuración de **umask** en la máquina remota, **oscap-ssh** podía no tener acceso a estos archivos. Esta actualización soluciona el problema, y como resultado, **oscap** guarda los archivos como el usuario de destino, y **oscap-ssh** accede a los archivos normalmente.

(BZ#1803116)

OpenSCAP ahora maneja correctamente los sistemas de archivos remotos

Anteriormente, OpenSCAP no detectaba de forma fiable los sistemas de archivos remotos si su especificación de montaje no empezaba con dos barras. Como consecuencia, OpenSCAP manejaba algunos sistemas de archivos basados en la red como locales. Con esta actualización, OpenSCAP identifica los sistemas de archivos utilizando el tipo de sistema de archivos en lugar de la especificación de montaje. Como resultado, OpenSCAP ahora maneja correctamente los sistemas de archivos remotos.

(BZ#1870087)

OpenSCAP ya no elimina las líneas en blanco de las cadenas multilíneas YAML

Anteriormente, OpenSCAP eliminaba las líneas en blanco de las cadenas multilínea YAML dentro de las correcciones de Ansible generadas a partir de un flujo de datos. Esto afectaba a las correcciones de Ansible y hacía que la utilidad **openscap** fallara en las comprobaciones correspondientes de Open Vulnerability and Assessment Language (OVAL), produciendo resultados falsos positivos. El problema se ha solucionado y, como resultado, **openscap** ya no elimina las líneas en blanco de las cadenas multilínea YAML.

(BZ#1795563)

OpenSCAP ahora puede escanear sistemas con un gran número de archivos sin quedarse sin memoria

Anteriormente, al escanear sistemas con poca memoria RAM y un gran número de archivos, el escáner OpenSCAP a veces hacía que el sistema se quedara sin memoria. Con esta actualización, se ha mejorado la gestión de la memoria del escáner OpenSCAP. Como resultado, el escáner ya no se queda sin memoria en sistemas con poca RAM cuando se escanea un gran número de archivos, por ejemplo, grupos de paquetes **Servidor con GUI** y **Estación de Trabajo**.

(BZ#1824152)

config.enabled ahora controla las declaraciones correctamente

Anteriormente, el **rsyslog** evaluaba incorrectamente la directiva **config.enabled** durante el procesamiento de la configuración de una sentencia. Como consecuencia, los errores de **parámetro no** conocido se mostraban para cada sentencia excepto para la de **include()**. Con esta actualización, la

configuración se procesa para todas las sentencias por igual. Como resultado, **config**.enabled ahora desactiva o activa correctamente las sentencias sin mostrar ningún error.

(BZ#1659383)

fapolicyd ya no impide las actualizaciones de RHEL

Cuando una actualización sustituye el binario de una aplicación en ejecución, el kernel modifica la ruta del binario de la aplicación en la memoria añadiendo el sufijo " (eliminado)". Anteriormente, el demonio de la política de acceso a archivos **fapolicyd** trataba dichas aplicaciones como no confiables, y les impedía abrir y ejecutar cualquier otro archivo. Como consecuencia, el sistema a veces no podía arrancar después de aplicar las actualizaciones.

Con la publicación del aviso RHBA-2020:5242, **fapolicyd** ignora el sufijo en la ruta del binario para que éste pueda coincidir con la base de datos de confianza. Como resultado, **fapolicyd** aplica las reglas correctamente y el proceso de actualización puede finalizar.

(BZ#1897090)

El perfil e8 se puede utilizar ahora para remediar los sistemas RHEL 8 con Server con GUI

El uso del complemento OpenSCAP Anaconda para endurecer el sistema en el grupo de paquetes **Server With GUI** con perfiles que seleccionan reglas del grupo **Verify Integrity with RPM** ya no requiere una cantidad extrema de RAM en el sistema. La causa de este problema era el escáner OpenSCAP. Para obtener más detalles, consulte El análisis de un gran número de archivos con OpenSCAP hace que los sistemas se queden sin memoria. Como consecuencia, el endurecimiento del sistema mediante el perfil RHEL 8 Essential Eight (e8) ahora también funciona con **Server With GUI**.

(BZ#1816199)

6.2.5. Red

La carga automática de los módulos de extensión de iptables por el módulo nft_compat ya no se cuelga

Anteriormente, cuando el módulo **nft_compat** cargaba un módulo de extensión mientras ocurría una operación en espacios de nombres de red(**netns**) en paralelo, podía producirse una colisión de bloqueos si esa extensión registraba un subsistema **pernet** durante la inicialización. Como consecuencia, el comando **modprobe** llamado por el kernel se colgaba. Esto también podía ser causado por otros servicios, como **libvirtd**, que también ejecutan comandos **iptables**. Este problema se ha solucionado. Como resultado, la carga de módulos de extensión de **iptables** mediante el módulo **nft_compat** ya no se cuelga.

(BZ#1757933)

El servicio firewalld ahora elimina los ipsets cuando el servicio se detiene

Anteriormente, al detener el servicio **firewalld** no se eliminaban los **ipsets**. Esta actualización soluciona el problema. Como resultado, los ipsets ya no quedan en el sistema después de que **firewalld** se detenga.

(BZ#1790948)

firewalld ya no retiene las entradas de ipset tras el apagado

Anteriormente, el cierre de **firewalld** no eliminaba las entradas ipset. En consecuencia, las entradas ipset permanecían activas en el kernel incluso después de detener el servicio **firewalld**. Con esta corrección, el cierre de **firewalld** elimina las entradas de ipset como se esperaba.

(BZ#1682913)

firewalld ahora restaura las entradas ipset después de la recarga

Anteriormente, **firewalld** no conservaba las entradas de **ipset** en tiempo de ejecución después de la recarga. En consecuencia, los usuarios tenían que volver a añadir manualmente las entradas que faltaban. Con esta actualización, **firewalld** ha sido modificado para restaurar las entradas ipset después de la recarga.

(BZ#1809225)

los serviciosnftables y firewalld son ahora mutuamente excluyentes

Anteriormente, era posible habilitar los servicios **nftables** y **firewalld** al mismo tiempo. Como consecuencia, **nftables** anulaba las reglas de **firewalld**. Con esta actualización, los servicios **nftables** y **firewalld** son ahora mutuamente excluyentes, por lo que no se pueden habilitar al mismo tiempo.

(BZ#1817205)

6.2.6. Núcleo

El script huge_page_setup_helper.py ahora funciona correctamente

Se ha eliminado accidentalmente un parche que actualizaba el script huge_page_setup_helper **.** py para Python 3. En consecuencia, tras ejecutar **huge_page_setup_helper**.py, aparecía el siguiente mensaje de error:

> SyntaxError: Faltan paréntesis en la llamada a 'print'

Con esta actualización, el problema se ha solucionado actualizando el archivo **libhugetlbfs.spec**. Como resultado, **huge_page_setup_helper.py** no muestra ningún error en el escenario descrito.

(BZ#1823398)

Los scripts bcc ahora compilan con éxito un módulo BPF

Durante la compilación del código de script para crear un módulo Berkeley Packet Filter (BPF), el kit de herramientas **bcc** utilizaba las cabeceras del kernel para la definición del tipo de datos. Algunas cabeceras del kernel necesitaban que se definiera la macro **KBUILD_MODNAME**. En consecuencia, los scripts de **bcc** que no añadían **KBUILD_MODNAME**, podían fallar al compilar un módulo BPF en varias arquitecturas de CPU. Los siguientes scripts **bcc** se veían afectados:

- **bindsnoop**
- **sofdsnoop**
- **escuchar**
- **tcpaccept**
- **tcpconnect**
- **tcpconnlat**
- **tcpdrop**
- **tcpretrans**

- **tcpsubnet**
- **tcptop**
- **tcptracer**

Con esta actualización, el problema se ha solucionado añadiendo **KBUILD_MODNAME** al parámetro **cflags** por defecto para **bcc**. Como resultado, este problema ya no aparece en el escenario descrito. Además, los scripts de los clientes tampoco necesitan definir **KBUILD_MODNAME** por sí mismos.

(BZ#1837906)

bcc-tools y bpftrace funcionan correctamente en IBM Z

Anteriormente, un backport de características introdujo la opción del kernel **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE**. Sin embargo, el paquete **bcc-tools** y el paquete de lenguaje de rastreo **bpftrace** para arquitecturas IBM Z no tenían el soporte adecuado para esta opción. En consecuencia, la llamada al sistema **bpf()** fallaba con la excepción de **argumento inválido** y **bpftrace** fallaba con un error que indicaba **Error loading program** al intentar cargar el programa BPF. Con esta actualización, la opción **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE** se ha eliminado. Como resultado, el problema ya no aparece en el escenario descrito.

(BZ#1847837, BZ#1853964)

El proceso de arranque ya no falla por falta de entropía

Anteriormente, el proceso de arranque fallaba por falta de entropía. Ahora se utiliza un mecanismo mejor para permitir que el kernel reúna entropía al principio del proceso de arranque, que no depende de ninguna interrupción específica del hardware. Esta actualización soluciona el problema asegurando la disponibilidad de suficiente entropía para asegurar la generación aleatoria en el arranque temprano. Como resultado, la corrección evita el tiempo de espera del kickstart o los arranques lentos y el proceso de arranque funciona como se espera.

(BZ#1778762)

Los reinicios repetidos usando kexec ahora funcionan como se espera

Anteriormente, durante el reinicio del kernel en la plataforma Amazon EC2 Nitro, no se llamaba al módulo remove**(rmmod**) durante la llamada **shutdown()** de la ruta de ejecución del kernel. En consecuencia, los reinicios repetidos del kernel utilizando la llamada al sistema **kexec** provocaban un fallo. Con esta actualización, el problema se ha solucionado añadiendo el manejador PCI **shutdown** () que permite la ejecución segura del kernel. Como resultado, los reinicios repetidos utilizando **kexec** en las plataformas Amazon EC2 Nitro ya no fallan.

(BZ#1758323)

Los reinicios repetidos utilizando la memoria vPMEM como objetivo de volcado ahora funcionan como se espera

Anteriormente, el uso de espacios de nombres de memoria virtual persistente (vPMEM) como destino de volcado para **kdump** o **fadump** hacía que el módulo **papr_scm** desmapeara y reasignara la memoria respaldada por vPMEM y volviera a añadir la memoria a su mapa lineal.

En consecuencia, este comportamiento desencadenó llamadas del hipervisor (HCalls) al hipervisor POWER. Como resultado, esto ralentiza considerablemente el arranque del kernel de captura y tarda mucho tiempo en guardar el archivo de volcado. Esta actualización soluciona el problema y el proceso de arranque ahora funciona como se espera en el escenario descrito

(BZ#1792125)

Ya no falla el intento de añadir el puerto NIC del controlador ICE a una interfaz maestra de enlace en modo 5

Anteriormente, al intentar añadir el puerto NIC del controlador **ICE** a una interfaz maestra de enlace en modo 5**(balance-tlb**) se producía un fallo con un error **Maestro 'bond0', Esclavo 'ens1f0': Error:** Enslave **failed**. En consecuencia, se producía un fallo intermitente al añadir el puerto NIC a la interfaz maestra de enlace. Esta actualización soluciona el problema y la adición de la interfaz ya no falla.

(BZ#1791664)

6.2.7. Alta disponibilidad y clusters

Cuando se utiliza un sistema de archivos GFS2 con el agente del sistema de archivos, la opción fast_stop ahora es por defecto no

Anteriormente, cuando se utilizaba un sistema de archivos GFS2 con el agente del sistema de archivos, la opción **fast_stop** tenía el valor predeterminado de **sí**. Este valor podía dar lugar a eventos de valla innecesarios debido al tiempo que puede tardar un sistema de archivos GFS2 en desmontarse. Con esta actualización, esta opción pasa a ser **no** por defecto. Para todos los demás sistemas de archivos, sigue siendo por defecto **"sí"**.

(BZ#1814896)

los agentesfence_compute y fence_evacuate ahora interpretan la opción insegura de una manera más estándar

Anteriormente, los agentes **fence_compute** y **fence_evacuate** funcionaban como si se especificara **--insecure** por defecto. Con esta actualización, los clientes que no utilicen certificados válidos para sus servicios de computación o evacuación deben establecer **insecure=true** y utilizar la opción **--insecure** cuando se ejecuten manualmente desde la CLI. Esto es coherente con el comportamiento de todos los demás agentes.

(BZ#1830776)

6.2.8. Lenguajes de programación dinámicos, servidores web y de bases de datos

Consumo de CPU optimizado por libdb

Una actualización anterior de la base de datos **libdb** provocaba un consumo excesivo de la CPU en el hilo de goteo. Con esta actualización, se ha optimizado el uso de la CPU.

(BZ#1670768)

La gema did_you_mean de Ruby ya no contiene un archivo con licencia no comercial

Anteriormente, la gema **did_you_mean** disponible en el flujo del módulo **ruby:2.** 5 contenía un archivo con una licencia no comercial. Esta actualización elimina el archivo afectado.

(BZ#1846113)

nginx ahora puede cargar certificados de servidor desde tokens de seguridad de hardware a través del URI PKCS#11

La directiva **ssl_certificate** del servidor web **nginx** soporta la carga de certificados de servidor TLS desde tokens de seguridad de hardware directamente desde módulos PKCS#11. Anteriormente, era

imposible cargar certificados de servidor desde tokens de seguridad de hardware a través del URI PKCS#11.

(BZ#1668717)

6.2.9. Compiladores y herramientas de desarrollo

El cargador dinámico de glibc ya no falla al cargar una biblioteca compartida que utiliza DT_FILTER y tiene un constructor

Antes de esta actualización, un defecto en la implementación del cargador dinámico de objetos compartidos como filtros hacía que el cargador dinámico fallara al cargar una biblioteca compartida que utilizara un filtro y tuviera un constructor. Con esta versión, la implementación del cargador dinámico de filtros(**DT_FILTER**) ha sido corregida para manejar correctamente tales bibliotecas compartidas. Como resultado, el cargador dinámico ahora funciona como se espera en el escenario mencionado.

(BZ#1812756)

glibc ahora puede eliminar los pseudo-montajes de la lista getmntent()

El kernel incluye pseudo-entradas de **automontaje** en las tablas expuestas al espacio de usuario. En consecuencia, los programas que utilizan la API **getmntent(**) ven tanto los montajes regulares como estos pseudo-montajes en la lista. Los pseudo-montajes no se corresponden con los montajes reales, ni incluyen información válida.

Con esta actualización, si la entrada de montaje tiene la opción de **ignorar el** montaje presente en la configuración de **automount(8**) la biblioteca **glibc** ahora elimina estos pseudo-montajes de la lista de **getmntent()**. Los programas que esperan el comportamiento anterior tienen que utilizar una API diferente.

(BZ#1743445)

El patrón movv1qi ya no provoca errores de compilación en el código autovectorizado en IBM Z

Antes de esta actualización, se emitían instrucciones de carga erróneas para el patrón **movv1qi**. Como consecuencia, cuando la auto-vectorización estaba en efecto, podía ocurrir una mala compilación en los sistemas IBM Z. Esta actualización corrige el patrón **movv1qi**, y como resultado, el código se compila y ejecuta correctamente ahora.

(BZ#1784758)

PAPI_event_name_to_code() ahora funciona correctamente en múltiples hilos

Antes de esta actualización, el código interno de PAPI no manejaba correctamente la coordinación de hilos. Como consecuencia, cuando varios hilos utilizaban la operación **PAPI_event_name_to_code()**, se producía una condición de carrera y la operación fallaba. Esta actualización mejora el manejo de múltiples hilos en el código interno de PAPI. Como resultado, el código multihilo que utiliza la operación **PAPI_event_name_to_code** () ahora funciona correctamente.

(BZ#1807346)

Mejora del rendimiento de las funciones matemáticas de glibc en IBM Power Systems

Anteriormente, las funciones matemáticas de **glibc** realizaban actualizaciones de estado de punto flotante y llamadas al sistema innecesarias en IBM Power Systems, lo que afectaba negativamente al rendimiento. Esta actualización elimina la actualización innecesaria del estado de punto flotante, y

mejora las implementaciones de: **ceil()**, **ceilf()**, **fegetmode()**, **fesetmode()**, **fesetenv()**, **fegetexcept()**, **feenableexcept()**, **fedisablexcept()**, **fegetround()** y **fesetround()**. Como resultado, se ha mejorado el rendimiento de la biblioteca matemática en IBM Power Systems.

(BZ#1783303)

Las llaves de protección de la memoria son ahora compatibles con IBM Power

En IBM Power Systems, las interfaces de la llave de protección de memoria **pkey_set** y **pkey_get** eran anteriormente funciones stub, y en consecuencia siempre fallaban. Esta actualización implementa las interfaces, y como resultado, la biblioteca GNU C**(glibc**) ahora soporta claves de protección de memoria en IBM Power Systems.

Tenga en cuenta que las claves de protección de memoria requieren actualmente la unidad de gestión de memoria (MMU) basada en hash, por lo que podría tener que arrancar ciertos sistemas con el parámetro del kernel **disable_radix**.

(BZ#1642150)

papi-testsuite y papi-devel instalan ahora el paquete papi-libs necesario

Anteriormente, los paquetes RPM **papi-testsuite** y **papi-devel** no declaraban una dependencia del paquete **papi-libs** correspondiente. En consecuencia, las pruebas no se ejecutaban y los desarrolladores no disponían de la versión necesaria de la biblioteca compartida **papi** para sus aplicaciones.

Con esta actualización, cuando el usuario instala los paquetes **papi-testsuite** o **papi-devel**, también se instala el paquete **papi-libs**. Como resultado, el **papi-testsuite** tiene ahora la biblioteca correcta que permite la ejecución de las pruebas, y los desarrolladores que utilizan **papi-devel** tienen sus ejecutables enlazados con la versión adecuada de la biblioteca compartida **papi**.

(BZ#1664056)

La instalación de los paquetes lldb para múltiples arquitecturas ya no provoca conflictos de archivos

Anteriormente, los paquetes **lldb** instalaban archivos dependientes de la arquitectura en ubicaciones independientes de la misma. Como consecuencia, la instalación de las versiones de 32 y 64 bits de los paquetes provocaba conflictos con los archivos. Esta actualización empaqueta los archivos en ubicaciones correctas dependientes de la arquitectura. Como resultado, la instalación de **lldb** en el escenario descrito se completa con éxito.

(BZ#1841073)

getaddrinfo ahora maneja correctamente un fallo de asignación de memoria

Anteriormente, después de un fallo de asignación de memoria, la función **getaddrinfo** de la biblioteca GNU C **glibc** no liberaba el contexto de resolución interno. Como consecuencia, **getaddrinfo** no era capaz de recargar el archivo /**etc**/**resolv.** conf durante el resto del tiempo de vida del hilo de llamada, lo que provocaba una posible fuga de memoria.

Esta actualización modifica la ruta de manejo de errores con una operación de liberación adicional para el contexto de resolución. Como resultado, **getaddrinfo** recarga /**etc**/**resolv.** conf con nuevos valores de configuración incluso después de un fallo intermitente de asignación de memoria.

(BZ#1810146)

glibc evita ciertos fallos causados por el ordenamiento del resolver IFUNC

Anteriormente, la implementación de las bibliotecas **librt** y **libpthread** de la biblioteca GNU C **glibc** contenía los resolvedores de funciones indirectas (IFUNC) para las siguientes funciones: **clock_gettime**, **clock_getcpuclockid**, **clock_nanosleep**, **clock_settime**, **vfork**. En algunos casos, los resolvedores IFUNC podían ejecutarse antes de que las bibliotecas **librt** y **libpthread** fueran reubicadas. En consecuencia, las aplicaciones fallaban en el cargador dinámico de **glibc** durante el inicio temprano del programa.

Con esta versión, las implementaciones de estas funciones se han trasladado al componente **libc** de **glibc**, lo que evita que se produzca el problema descrito.

(BZ#1748197)

Ya no se producen fallos de aserción durante pthread_create

Anteriormente, el cargador dinámico **de glibc** no retrocedía los cambios en el contador interno de ID del módulo de almacenamiento local de hilos (TLS). Como consecuencia, podía producirse un fallo de aserción en la función **pthread_create** después de que la función **dlopen** hubiera fallado en ciertos aspectos. Con esta corrección, el cargador dinámico **de glibc** actualiza el contador de ID del módulo TLS en un momento posterior, después de que ciertos fallos ya no puedan ocurrir. Como resultado, los fallos de aserción ya no ocurren.

(BZ#1774115)

glibc instala ahora las dependencias correctas para las aplicaciones de 32 bits que utilizan nss_db

Anteriormente, el paquete nss_db **.x86_64** no declaraba dependencias del paquete **nss_db**.i686. Por lo tanto, la instalación automatizada no instalaba **nss_db.i686** en el sistema, a pesar de tener un entorno de 32 bits **glibc.i686** instalado. Como consecuencia, las aplicaciones de 32 bits que utilizaban **nss_db** no realizaban búsquedas precisas en la base de datos de usuarios, mientras que las aplicaciones de 64 bits en la misma configuración funcionaban correctamente.

Con esta actualización, los paquetes **glibc** tienen ahora dependencias débiles que activan la instalación del paquete **nss_db**.i686 cuando tanto **glibc.i686** como **nss_db** están instalados en el sistema. Como resultado, las aplicaciones de 32 bits que utilizan **nss_db** ahora funcionan correctamente, incluso si el administrador del sistema no ha instalado explícitamente el paquete **nss_db**.i686.

(BZ#1807824)

información de localización deglibc actualizada con el idioma Odia

El nombre del estado indio anteriormente conocido como Orissa ha cambiado a Odisha, y el nombre de su idioma oficial ha cambiado de Oriya a Odia. Con esta actualización, la información de localización de **glibc** refleja el nuevo nombre del idioma.

(BZ#1757354)

Los subpaquetes de LLVM ahora instalan los archivos dependientes de arch en ubicaciones dependientes de arch

Anteriormente, los subpaquetes de LLVM instalaban archivos dependientes del arco en ubicaciones independientes del mismo. Esto provocaba conflictos al instalar versiones de 32 y 64 bits de LLVM. Con esta actualización, los archivos del paquete se instalan ahora correctamente en ubicaciones dependientes del arco, evitando conflictos de versión.

(BZ#1820319)

Las búsquedas de contraseñas y grupos ya no fallan en glibc

Anteriormente, el módulo **nss_compat** de la biblioteca **glibc** sobrescribía el estado **errno** con códigos de error incorrectos durante el procesamiento de las entradas de contraseñas y grupos. En consecuencia, las aplicaciones no redimensionaban los búferes como se esperaba, haciendo que las búsquedas de contraseñas y grupos fallaran. Esta actualización corrige el problema, y las búsquedas ahora se completan como se esperaba.

(BZ#1836867)

6.2.10. Gestión de la identidad

SSSD ya no descarga por defecto todas las reglas con carácter comodín

Anteriormente, la opción **ldap_sudo_include_regexp** se establecía incorrectamente como **verdadera** por defecto. Como consecuencia, cuando SSSD comenzaba a ejecutarse o después de actualizar las reglas de SSSD, SSSD descargaba todas las reglas que contenían un carácter comodín**(*)** en el atributo **sudoHost**. Esta actualización corrige el error, y la opción **ldap_sudo_include_regexp** está ahora correctamente establecida en **false** por defecto. Como resultado, el problema descrito ya no se produce.

(BZ#1827615)

krb5 ahora sólo solicita los tipos de encriptación permitidos

Anteriormente, los tipos de cifrado permitidos especificados en la variable **permitted_enctypes** del archivo **/etc/krb5.conf** no se aplicaban a los tipos de cifrado por defecto si los atributos **default_tgs_enctypes** o **default_tkt_enctypes** no estaban establecidos. En consecuencia, los clientes de Kerberos podían solicitar suites de cifrado obsoletas como RC4, lo que podía hacer que otros procesos fallaran. Con esta actualización, los tipos de cifrado especificados en la variable **permitted_enctypes** se aplican también a los tipos de cifrado por defecto, y sólo se solicitan los tipos de cifrado permitidos.

El conjunto de cifrado RC4, que ha quedado obsoleto en RHEL 8, es el tipo de cifrado por defecto para los usuarios, servicios y fideicomisos entre los dominios de Active Directory (AD) en un bosque de AD.

- Para garantizar la compatibilidad con los tipos de cifrado AES fuertes entre los dominios de AD en un bosque de AD, consulte el artículo AD DS: Seguridad: Kerberos \ "Unsupported etype" error al acceder a un recurso en un dominio de confianza artículo de Microsoft.
- Para habilitar la compatibilidad con el tipo de cifrado RC4 obsoleto en un servidor de IdM para que sea compatible con AD, utilice el comando **update-crypto-policies --set DEFAULT:AD-SUPPORT**.

(BZ#1791062)

Los KDCs ahora aplican correctamente la política de duración de las contraseñas desde los backends LDAP

Anteriormente, los centros de distribución de Kerberos (KDC) que no eran de IPA no garantizaban la duración máxima de las contraseñas porque el backend LDAP de Kerberos aplicaba incorrectamente las políticas de contraseñas. Con esta actualización, el backend LDAP de Kerberos se ha corregido y los tiempos de vida de las contraseñas se comportan como se espera.

(BZ#1784655)

Envío de notificaciones de caducidad de contraseñas a los clientes de AD mediante SSSD

Anteriormente, los clientes de Active Directory (no IdM) que utilizaban SSSD no recibían avisos de caducidad de las contraseñas debido a un cambio reciente en la interfaz de SSSD para adquirir las credenciales de Kerberos.

Se ha actualizado la interfaz de Kerberos y los avisos de caducidad se envían ahora correctamente.

(BZ#1820311)

El servidor de directorios ya no pierde memoria cuando se utilizan definiciones indirectas de COS

Anteriormente, después de procesar una definición de clase de servicio (COS) indirecta, Directory Server perdía memoria para cada operación de búsqueda que utilizaba una definición de COS indirecta. Con esta actualización, Directory Server libera todas las estructuras de COS internas asociadas a la entrada de la base de datos después de haberla procesado. Como resultado, el servidor ya no pierde memoria cuando utiliza definiciones de COS indirectas.

(BZ#1816862)

La adición de anulaciones de ID de usuarios de AD ahora funciona en la interfaz web de IdM

Anteriormente, la adición de anulaciones de ID de usuarios de Active Directory (AD) a grupos de gestión de identidades (IdM) en la vista de confianza predeterminada con el fin de conceder acceso a las funciones de gestión fallaba al utilizar la interfaz web de IdM. Esta actualización corrige el error. Como resultado, ahora puede utilizar tanto la interfaz web como la interfaz de línea de comandos (CLI) de IdM en este caso.

(BZ#1651577)

FreeRADIUS ya no genera certificados durante la instalación del paquete

Anteriormente, FreeRADIUS generaba certificados durante la instalación del paquete, lo que provocaba los siguientes problemas:

- Si FreeRADIUS se instaló mediante Kickstart, los certificados podrían generarse en un momento en que la entropía del sistema fuera insuficiente, lo que daría lugar a una instalación fallida o a un certificado menos seguro.
- El paquete era difícil de construir como parte de una imagen, como un contenedor, porque la instalación del paquete se produce en la máquina constructora en lugar de la máquina de destino. Todas las instancias que se generan a partir de la imagen tienen la misma información de certificado.
- Era difícil para un usuario final generar una simple VM en su entorno, ya que los certificados tendrían que ser eliminados y regenerados manualmente.

Con esta actualización, la instalación de FreeRADIUS ya no genera certificados CA autofirmados por defecto ni certificados CA subordinados. Cuando FreeRADIUS se lanza a través de **systemd**:

- Si faltan todos los certificados necesarios, se genera un conjunto de certificados por defecto.
- Si uno o más de los certificados esperados están presentes, no genera nuevos certificados.

(BZ#1672285)

FreeRADIUS ahora genera parámetros Diffie-Hellman que cumplen con FIPS

Debido a los nuevos requisitos de FIPS que no permiten que **openssl** genere parámetros Diffie-Hellman (dh) a través de **dhparam**, la generación de parámetros dh se ha eliminado de los scripts de arranque de

FreeRADIUS y el archivo, **rfc3526-group-18-8192.dhparam**, se incluye con los paquetes de FreeRADIUS para todos los sistemas, y así permite que FreeRADIUS se inicie en modo FIPS.

Tenga en cuenta que puede personalizar **/etc/raddb/certs/bootstrap** y **/etc/raddb/certs/Makefile** para restaurar la generación de parámetros DH si es necesario.

(BZ#1859527)

La actualización de Healthcheck ahora actualiza correctamente tanto ipa-healthcheck-core como ipa-healthcheck

Anteriormente, al introducir **yum update healthcheck** no se actualizaba el paquete **ipa-healthcheck**, sino que se sustituía por el paquete **ipa-healthcheck-core**. Como consecuencia, el comando **ipa-healthcheck** no funcionaba después de la actualización.

Esta actualización corrige el error, y la actualización de **ipa-healthcheck** ahora actualiza correctamente tanto el paquete **ipa-healthcheck** como el paquete **ipa-healthcheck-core**. Como resultado, la herramienta **Healthcheck** funciona correctamente después de la actualización.

(BZ#1852244)

6.2.11. Infraestructuras gráficas

Los portátiles con GPUs Nvidia híbridas ya pueden reanudar su actividad desde la suspensión

Anteriormente, el controlador de gráficos **nouveau** a veces no podía encender las GPUs Nvidia híbridas en ciertos portátiles desde el modo de ahorro de energía. Como resultado, los portátiles no se reanudaban desde la suspensión.

Con esta actualización, se han solucionado varios problemas en el sistema de gestión de energía en tiempo real**(runpm**). Como resultado, los portátiles con gráficos híbridos ahora pueden reanudar con éxito desde la suspensión.

(JIRA:RHELPLAN-57572)

6.2.12. Virtualización

La migración de máquinas virtuales con el modelo de CPU por defecto funciona ahora de forma más fiable

Anteriormente, si se creaba una máquina virtual (VM) sin un modelo de CPU específico, QEMU utilizaba un modelo por defecto que no era visible para el servicio **libvirt**. Como consecuencia, era posible migrar la VM a un host que no soportaba el modelo de CPU por defecto de la VM, lo que a veces provocaba cuelgues y un comportamiento incorrecto en el SO invitado tras la migración.

Con esta actualización, **libvirt** utiliza explícitamente el modelo **qemu64** por defecto en la configuración XML de la VM. Como resultado, si el usuario intenta migrar una VM con el modelo de CPU por defecto a un host que no soporta ese modelo, **libvirt** genera correctamente un mensaje de error.

Tenga en cuenta, sin embargo, que Red Hat recomienda encarecidamente utilizar un modelo de CPU específico para sus máquinas virtuales.

(JIRA:RHELPLAN-45906)

6.2.13. Contenedores

Notas sobre el soporte FIPS con Podman

El Estándar Federal de Procesamiento de Información (FIPS) requiere que se utilicen módulos certificados. Anteriormente, Podman instalaba correctamente los módulos certificados en los contenedores habilitando las banderas adecuadas en el arranque. Sin embargo, en esta versión, Podman no configura correctamente los ayudantes de aplicación adicionales que normalmente proporciona el sistema en forma de la política criptográfica de todo el sistema FIPS. Aunque la configuración de la política de cifrado de todo el sistema no es necesaria para los módulos certificados, mejora la capacidad de las aplicaciones para utilizar los módulos de cifrado de forma compatible. Para solucionar este problema, cambie su contenedor para ejecutar el comando **update-crypto-policies --set FIPS** antes de ejecutar cualquier otro código de aplicación. El comando **update-crypto-policies** --set FIPS ya no es necesario con esta corrección.

(BZ#1804193)

6.3. AVANCES TECNOLÓGICOS

Esta parte proporciona una lista de todas las Previsiones Tecnológicas disponibles en Red Hat Enterprise Linux 8.3.

Para obtener información sobre el alcance del soporte de Red Hat para las características de Technology Preview, consulte Alcance del soporte de las características de Technology Preview .

6.3.1. Red

Activado el módulo xt_u32 Netfilter

El módulo **xt_u32** Netfilter está ahora disponible en el rpm **kernel-modules-extra**. Este módulo ayuda en el reenvío de paquetes basado en los datos que son inaccesibles para otros filtros de paquetes basados en protocolos y por lo tanto facilita la migración manual a **nftables**. Sin embargo, el módulo **xt_u32** Netfilter no está soportado por Red Hat.

(BZ#1834769)

nmstate está disponible como una muestra de tecnología

Nmstate es una API de red para hosts. Los paquetes **nmstate**, disponibles como Technology Preview, proporcionan una biblioteca y la utilidad de línea de comandos **nmstatectl** para gestionar la configuración de red de los hosts de forma declarativa. El estado de la red se describe mediante un esquema predefinido. Los informes sobre el estado actual y los cambios al estado deseado se ajustan al esquema.

Para más detalles, consulte el archivo **/usr/share/doc/nmstate/README .md** y los ejemplos del directorio **/usr/share/doc/nmstate/examples**.

(BZ#1674456)

AF_XDP está disponible como Muestra de Tecnología

El socket**Address Family eXpress Data Path(AF_XDP**) está diseñado para el procesamiento de paquetes de alto rendimiento. Acompaña a **XDP** y garantiza una redirección eficaz de los paquetes seleccionados mediante programación a las aplicaciones del espacio de usuario para su posterior procesamiento.

(BZ#1633143)

XDP disponible como Muestra de Tecnología

La función eXpress Data Path (XDP), que está disponible como Technology Preview, ofrece un medio para adjuntar programas de Berkeley Packet Filter (eBPF) ampliados para el procesamiento de paquetes de alto rendimiento en un punto temprano de la ruta de datos de entrada del núcleo, lo que permite un análisis, filtrado y manipulación de paquetes programables y eficientes.

(BZ#1503672)

KTLS está disponible como avance tecnológico

En Red Hat Enterprise Linux 8, la Seguridad de la Capa de Transporte del Kernel (KTLS) se proporciona como una Muestra de Tecnología. KTLS maneja los registros TLS utilizando los algoritmos de cifrado o descifrado simétrico en el kernel para el cifrado AES-GCM. KTLS también proporciona la interfaz para descargar el cifrado de registros TLS a los controladores de interfaz de red (NIC) que soportan esta funcionalidad.

(BZ#1570255)

Funciones del XDP disponibles como Technology Preview

Red Hat proporciona el uso de las siguientes características de eXpress Data Path (XDP) como Technology Preview no soportada:

- Carga de programas XDP en arquitecturas distintas de AMD e Intel de 64 bits. Tenga en cuenta que la biblioteca **libxdp** no está disponible para arquitecturas distintas de AMD e Intel de 64 bits.
- Los códigos de retorno **XDP_TX** y **XDP_REDIRECT**.
- La descarga de hardware XDP. Antes de utilizar esta función, consulte Falla la descarga de programas XDP en las tarjetas de red Netronome que utilizan el controlador **nfp**.

(BZ#1889737)

el móduloact_mpls está disponible como Muestra de Tecnología

El módulo **act_mpls** ya está disponible en el rpm **kernel-modules-extra** como Technology Preview. El módulo permite la aplicación de acciones de Conmutación de Etiquetas Multiprotocolo (MPLS) con filtros de Control de Tráfico (TC), por ejemplo, empujar y sacar entradas de la pila de etiquetas MPLS con filtros TC. El módulo también permite configurar de forma independiente los campos Etiqueta, Clase de tráfico, Fondo de pila y Tiempo de vida.

(BZ#1839311)

Multipath TCP ya está disponible como Technology Preview

Multipath TCP (MPTCP), una extensión de TCP, ya está disponible como Technology Preview. MPTCP mejora el uso de los recursos dentro de la red y la resistencia a los fallos de la misma. Por ejemplo, con Multipath TCP en el servidor RHEL, los smartphones con MPTCP v1 activado pueden conectarse a una aplicación que se ejecuta en el servidor y cambiar entre las redes Wi-Fi y celular sin interrumpir la conexión con el servidor.

Tenga en cuenta que, o bien las aplicaciones que se ejecutan en el servidor deben soportar MPTCP de forma nativa, o bien los administradores deben cargar un programa **eBPF** en el kernel para cambiar dinámicamente **IPPROTO_TCP** a **IPPROTO_MPTCP**.

Para más detalles, consulte la sección " Introducción al TCP multirruta ".

(JIRA:RHELPLAN-41549)

El servicio systemd-resolved ya está disponible como Technology Preview

El servicio **systemd-resolved** proporciona resolución de nombres a las aplicaciones locales. El servicio implementa un resolvedor de stub DNS de caché y validación, un resolvedor de nombres Link-Local Multicast (LLMNR), y un resolvedor y respondedor de DNS Multicast.

Tenga en cuenta que, aunque el paquete **systemd** proporcione **systemd-resolved**, este servicio es una Muestra de Tecnología no soportada.

(BZ#1906489)

6.3.2. Núcleo

La función de reinicio rápido de kexec está disponible como Technology Preview

La función de reinicio **rápido** de kexec sigue estando disponible como Technology Preview. El **reinicio rápido de kexec** acelera significativamente el proceso de arranque al permitir que el kernel arranque directamente en el segundo kernel sin pasar primero por el Sistema Básico de Entrada/Salida (BIOS). Para utilizar esta función:

1. Cargue el kernel **kexec** manualmente.
2. Reinicie el sistema operativo.

(BZ#1769727)

eBPF disponible como Muestra de Tecnología

Extended Berkeley Packet Filter (eBPF)es una máquina virtual dentro del núcleo que permite la ejecución de código en el espacio del núcleo, en el entorno restringido de la caja de arena con acceso a un conjunto limitado de funciones.

La máquina virtual incluye una nueva llamada al sistema **bpf()**, que admite la creación de varios tipos de mapas, y también permite cargar programas en un código especial similar al ensamblador. A continuación, el código se carga en el kernel y se traduce al código máquina nativo con la compilación just-in-time. Tenga en cuenta que la llamada al sistema **bpf(**) sólo puede ser utilizada con éxito por un usuario con la capacidad **CAP_SYS_ADMIN**, como el usuario root. Consulte la página man de **bpf**(2) para más información.

Los programas cargados pueden ser conectados en una variedad de puntos (sockets, tracepoints, recepción de paquetes) para recibir y procesar datos.

Hay numerosos componentes suministrados por Red Hat que utilizan la máquina virtual **eBPF**. Cada componente se encuentra en una fase de desarrollo diferente y, por lo tanto, no todos los componentes están actualmente totalmente soportados. Todos los componentes están disponibles como una Muestra de Tecnología, a menos que un componente específico sea indicado como soportado.

Los siguientes componentes notables de **eBPF** están actualmente disponibles como Muestra de Tecnología:

- **bpftrace**, un lenguaje de trazado de alto nivel que utiliza la máquina virtual **eBPF**.
- **AF_XDP**, un socket para conectar la ruta **eXpress Data Path (XDP)**con el espacio de usuario para aplicaciones que priorizan el rendimiento del procesamiento de paquetes.

(BZ#1559616)

El controlador igc está disponible como Technology Preview para RHEL 8

El controlador de LAN cableada Intel 2.5G Ethernet Linux **de** igc ya está disponible en todas las arquitecturas para RHEL 8 como Technology Preview. La utilidad **ethtool** también es compatible con las LAN cableadas **igc**.

(BZ#1495358)

6.3.3. Sistemas de archivos y almacenamiento

NVMe/TCP está disponible como una Muestra de Tecnología

El acceso y la compartición del almacenamiento Nonvolatile Memory Express (NVMe) a través de redes TCP/IP (NVMe/TCP) y sus correspondientes módulos del núcleo **nvme-tcp.ko** y **nvmet-tcp.ko** se han añadido como Technology Preview.

El uso de NVMe/TCP como cliente de almacenamiento o como destino se puede gestionar con las herramientas proporcionadas por los paquetes **nvme-cli** y **nvmetcli**.

El objetivo NVMe/TCP Technology Preview se incluye sólo con fines de prueba y actualmente no está previsto que sea totalmente compatible.

(BZ#1696451)

El sistema de archivos DAX ya está disponible para ext4 y XFS como Technology Preview

En Red Hat Enterprise Linux 8, el sistema de archivos DAX está disponible como una Muestra de Tecnología. DAX proporciona un medio para que una aplicación mapee directamente la memoria persistente en su espacio de direcciones. Para usar DAX, un sistema debe tener alguna forma de memoria persistente disponible, usualmente en la forma de uno o más módulos de memoria dual en línea no volátil (NVDIMMs), y un sistema de archivos que soporte DAX debe ser creado en los NVDIMMs. Además, el sistema de archivos debe ser montado con la opción de montaje **dax**. Entonces, un **mmap** de un archivo en el sistema de archivos montado en dax resulta en un mapeo directo del almacenamiento en el espacio de direcciones de la aplicación.

(BZ#1627455)

OverlayFS

OverlayFS es un tipo de sistema de archivos de unión. Permite superponer un sistema de archivos sobre otro. Los cambios se registran en el sistema de archivos superior, mientras que el sistema de archivos inferior permanece sin modificar. Esto permite que varios usuarios compartan una imagen del sistema de archivos, como un contenedor o un DVD-ROM, donde la imagen base está en un medio de sólo lectura.

OverlayFS sigue siendo una Muestra de Tecnología en la mayoría de las circunstancias. Como tal, el kernel registra advertencias cuando se activa esta tecnología.

La compatibilidad total con OverlayFS está disponible cuando se utiliza con motores de contenedores compatibles**(podman**, **cri-o** o **buildah**) con las siguientes restricciones:

- OverlayFS está soportado para su uso sólo como controlador de gráficos del motor de contenedores. Su uso se admite sólo para el contenido de contenedores COW, no para el almacenamiento persistente. Debe colocar cualquier almacenamiento persistente en volúmenes que no sean OverlayFS. Sólo puede utilizar la configuración predeterminada del motor de contenedores: un nivel de superposición, un directorio inferior, y ambos niveles inferior y superior están en el mismo sistema de archivos.

- Actualmente sólo se admite el uso de XFS como sistema de archivos de capa inferior.

Además, las siguientes reglas y limitaciones se aplican al uso de OverlayFS:

- La ABI del kernel de OverlayFS y el comportamiento del espacio de usuario no se consideran estables, y podrían cambiar en futuras actualizaciones.
- OverlayFS proporciona un conjunto restringido de los estándares POSIX. Pruebe su aplicación a fondo antes de desplegarla con OverlayFS. Los siguientes casos no son compatibles con POSIX:
  - Los archivos inferiores abiertos con **O_RDONLY** no reciben actualizaciones de **st_atime** cuando se leen los archivos.
  - Los archivos inferiores abiertos con **O_RDONLY**, luego mapeados con **MAP_SHARED** son inconsistentes con la modificación posterior.
  - Los valores **st_ino** o **d_ino** no están habilitados por defecto en RHEL 8, pero puede habilitar el cumplimiento total de POSIX para ellos con una opción de módulo o una opción de montaje.
    Para obtener una numeración consistente de los inodos, utilice la opción de montaje **xino=on**.

    También puede utilizar las opciones **redirect_dir=on** e **index=on** para mejorar el cumplimiento de POSIX. Estas dos opciones hacen que el formato de la capa superior sea incompatible con una superposición sin estas opciones. Es decir, puede obtener resultados inesperados o errores si crea una capa superior con **redirect_dir=on** o **index=on**, desmonta la capa superior y luego monta la capa superior sin estas opciones.
- Para determinar si un sistema de archivos XFS existente es elegible para su uso como superposición, utilice el siguiente comando y compruebe si la opción **ftype=1** está activada:

```
# xfs_info /mount-point | grep ftype
```

- Las etiquetas de seguridad SELinux están habilitadas por defecto en todos los motores de contenedores compatibles con OverlayFS.
- Varios problemas conocidos están asociados con OverlayFS en esta versión. Para más detalles, consulte *Non-standard behavior* en la documentación del núcleo de Linux: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

Para más información sobre OverlayFS, consulte la documentación del núcleo de Linux: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

(BZ#1690207)

Stratis ya está disponible como Muestra de Tecnología

Stratis es un nuevo gestor de almacenamiento local. Proporciona sistemas de archivos gestionados sobre pools de almacenamiento con características adicionales para el usuario.

Stratis le permite realizar más fácilmente tareas de almacenamiento como:

- Gestionar las instantáneas y el thin provisioning
- Aumente automáticamente el tamaño del sistema de archivos según sea necesario

- Mantener los sistemas de archivos

Para administrar el almacenamiento de Stratis, utilice la utilidad **stratis**, que se comunica con el servicio de fondo **stratisd**.

Stratis se suministra como un avance tecnológico.

Para más información, consulte la documentación de Stratis: Gestión del almacenamiento local en capas con Stratis.

RHEL 8.3 actualiza Stratis a la versión 2.1.0. Para más información, consulte las notas de la versión Stratis 2.1.0.

(JIRA:RHELPLAN-1212)

IdM soporta ahora la configuración de un servidor Samba en un miembro del dominio IdM como Technology Preview

Con esta actualización, ahora se puede configurar un servidor Samba en un miembro del dominio de Gestión de Identidades (IdM). La nueva utilidad **ipa-client-samba** proporcionada por el paquete del mismo nombre añade un principal de servicio Kerberos específico de Samba a IdM y prepara el cliente IdM. Por ejemplo, la utilidad crea el archivo **/etc/samba/smb.conf** con la configuración de mapeo de ID para el back end de mapeo de ID **sss**. Como resultado, los administradores pueden ahora configurar Samba en un miembro del dominio IdM.

Debido a que los controladores de confianza de IdM no admiten el servicio de catálogo global, los hosts de Windows inscritos en AD no pueden encontrar usuarios y grupos de IdM en Windows. Además, los controladores de confianza de IdM no admiten la resolución de grupos de IdM mediante los protocolos Distributed Computing Environment / Remote Procedure Calls (DCE/RPC). Como consecuencia, los usuarios de AD sólo pueden acceder a los recursos compartidos e impresoras de Samba desde los clientes de IdM.

Para obtener más detalles, consulte Configuración de Samba en un miembro del dominio IdM .

(JIRA:RHELPLAN-13195)

6.3.4. Alta disponibilidad y clusters

La versión en modo local del comando de configuración del clúster de pcs está disponible como vista previa de la tecnología

Por defecto, el comando pcs **cluster** setup sincroniza automáticamente todos los archivos de configuración a los nodos del cluster. En Red Hat Enterprise Linux 8.3, el comando de configuración de cluster **pcs** proporciona la opción **--corosync-conf** como un avance tecnológico. Al especificar esta opción, el comando cambia al modo **local**. En este modo, **pcs** crea un archivo corosync **.conf** y lo guarda en un archivo especificado sólo en el nodo local, sin comunicarse con ningún otro nodo. Esto permite crear un archivo **corosync**.conf en un script y manejar ese archivo por medio del script.

(BZ#1839637)

Paquetes de Podman de Marcapasos disponibles como Muestra de Tecnología

Los paquetes de contenedores de Pacemaker ahora se ejecutan en la plataforma de contenedores **podman**, y la función de paquetes de contenedores está disponible como Technology Preview. Hay una excepción a que esta característica sea Technology Preview: Red Hat soporta completamente el uso de paquetes Pacemaker para Red Hat Openstack.

(BZ#1619620)

Heurística en corosync-qdevice disponible como Technology Preview

La heurística es un conjunto de comandos que se ejecutan localmente en el arranque, en el cambio de pertenencia al clúster, en la conexión exitosa a **corosync-qnetd** y, opcionalmente, de forma periódica. Cuando todos los comandos terminan con éxito a tiempo (su código de error de retorno es cero), la heurística ha pasado; de lo contrario, ha fallado. El resultado de la heurística se envía a **corosync-qnetd**, donde se utiliza en los cálculos para determinar qué partición debe tener quórum.

(BZ#1784200)

Nuevo agente de valla-heurística-ping

Como muestra de tecnología, Pacemaker soporta ahora el agente **fence_heuristics_ping**. Este agente pretende abrir una clase de agentes de vallas experimentales que no hacen vallas reales por sí mismos, sino que explotan el comportamiento de los niveles de vallas de una manera nueva.

Si el agente heurístico está configurado en el mismo nivel de cercado que el agente que realiza el cercado real, pero está configurado antes que ese agente en la secuencia, el cercado emite una acción de **desactivación** en el agente heurístico antes de intentar hacerlo en el agente que realiza el cercado. Si el agente heurístico da un resultado negativo para la acción de **desactivación**, ya está claro que el nivel de esgrima no va a tener éxito, haciendo que el esgrima Pacemaker se salte el paso de emitir la acción de **desactivación** en el agente que hace el esgrima. Un agente heurístico puede explotar este comportamiento para evitar que el agente que hace el cercado real cerque un nodo bajo ciertas condiciones.

Un usuario puede querer utilizar este agente, especialmente en un cluster de dos nodos, cuando no tenga sentido que un nodo valla al peer si puede saber de antemano que no será capaz de tomar los servicios correctamente. Por ejemplo, puede no tener sentido que un nodo se haga cargo de los servicios si tiene problemas para alcanzar el enlace ascendente de red, haciendo que los servicios sean inalcanzables para los clientes, situación que un ping a un router podría detectar en ese caso.

(BZ#1775847)

6.3.5. Gestión de la identidad

La API JSON-RPC de gestión de identidades está disponible como Technology Preview

Hay una API disponible para la gestión de identidades (IdM). Para ver la API, IdM también proporciona un navegador de API como Technology Preview.

En Red Hat Enterprise Linux 7.3, la API de IdM fue mejorada para permitir múltiples versiones de comandos de la API. Anteriormente, las mejoras podían cambiar el comportamiento de un comando de manera incompatible. Ahora, los usuarios pueden seguir utilizando las herramientas y scripts existentes, incluso si la API de IdM cambia. Esto permite:

- Los administradores pueden utilizar versiones anteriores o posteriores de IdM en el servidor que en el cliente gestor.
- Los desarrolladores pueden utilizar una versión específica de una llamada de IdM, incluso si la versión de IdM cambia en el servidor.

En todos los casos, la comunicación con el servidor es posible, independientemente de que una de las partes utilice, por ejemplo, una versión más nueva que introduzca nuevas opciones para una función.

Para obtener más detalles sobre el uso de la API, consulte Uso de la API de gestión de identidades para comunicarse con el servidor de IdM (PREVISIÓN TECNOLÓGICA).

(BZ#1664719)

DNSSEC disponible como Technology Preview en IdM

Los servidores de gestión de identidades (IdM) con DNS integrado son ahora compatibles con las extensiones de seguridad de DNS (DNSSEC), un conjunto de extensiones de DNS que mejoran la seguridad del protocolo DNS. Las zonas DNS alojadas en los servidores IdM pueden firmarse automáticamente utilizando DNSSEC. Las claves criptográficas se generan y rotan automáticamente.

Se recomienda a los usuarios que decidan asegurar sus zonas DNS con DNSSEC que lean y sigan estos documentos:

- Prácticas operativas de DNSSEC, versión 2: http://tools.ietf.org/html/rfc6781#section-2
- Guía de implantación del sistema de nombres de dominio (DNS) seguro: http://dx.doi.org/10.6028/NIST.SP.800-81-2
- Consideraciones sobre el tiempo de renovación de la clave DNSSEC: http://tools.ietf.org/html/rfc7583

Tenga en cuenta que los servidores IdM con DNS integrado utilizan DNSSEC para validar las respuestas DNS obtenidas de otros servidores DNS. Esto podría afectar a la disponibilidad de las zonas DNS que no estén configuradas de acuerdo con las prácticas de nomenclatura recomendadas.

(BZ#1664718)

6.3.6. Escritorio

El Escritorio GNOME en ARM está disponible como Muestra de Tecnología

El Escritorio GNOME está ahora disponible como Muestra de Tecnología en la arquitectura ARM de 64 bits. Los usuarios que necesiten una sesión gráfica para configurar y gestionar sus servidores pueden ahora conectarse a una sesión gráfica remota que ejecute el Escritorio GNOME usando VNC.

(BZ#1724302)

GNOME para la arquitectura ARM de 64 bits disponible como Technology Preview

El entorno de escritorio GNOME ya está disponible para la arquitectura ARM de 64 bits como Technology Preview. Esto permite a los administradores configurar y gestionar servidores desde una interfaz gráfica de usuario (GUI) de forma remota, utilizando la sesión VNC.

Como consecuencia, hay nuevas aplicaciones de administración disponibles en la arquitectura ARM de 64 bits. Por ejemplo: **Disk Usage Analyzer (baobab)**, **Firewall Configuration (firewall-config)**, **Red Hat Subscription Manager (subscription-manager)**, o el navegador web **Firefox**. Utilizando **Firefox**, los administradores pueden conectarse al demonio local de Cockpit de forma remota.

(JIRA:RHELPLAN-27394, BZ#1667225, BZ#1667516)

El escritorio GNOME en IBM Z está disponible como Technology Preview

El escritorio GNOME, incluyendo el navegador web Firefox, está ahora disponible como Technology Preview en la arquitectura IBM Z. Ahora puede conectarse a una sesión gráfica remota que ejecute GNOME utilizando VNC para configurar y gestionar sus servidores IBM Z.

(JIRA:RHELPLAN-27737)

6.3.7. Infraestructuras gráficas

La consola remota VNC está disponible como Technology Preview para la arquitectura ARM de 64 bits

En la arquitectura ARM de 64 bits, la consola remota de Virtual Network Computing (VNC) está disponible como Technology Preview. Tenga en cuenta que el resto de la pila de gráficos no está actualmente verificada para la arquitectura ARM de 64 bits.

(BZ#1698565)

Gráficos Intel Tiger Lake disponibles como Technology Preview

Los gráficos Intel Tiger Lake UP3 y UP4 Xe ya están disponibles como Technology Preview.

Para activar la aceleración por hardware con los gráficos Intel Tiger Lake, añada la siguiente opción en la línea de comandos del kernel:

```
i915.force_probe=pci-id
```

En esta opción, sustituya *pci-id* por una de las siguientes:

- El PCI ID de su GPU Intel
- El carácter ***** para habilitar el controlador **i915** con todo el hardware de calidad alfa

(BZ#1783396)

6.3.8. Roles del sistema Red Hat Enterprise Linux

El rol **postfix** de RHEL System Roles disponible como Technology Preview

Red Hat Enterprise Linux System Roles proporciona una interfaz de configuración para los subsistemas de Red Hat Enterprise Linux, que facilita la configuración del sistema mediante la inclusión de Ansible Roles. Esta interfaz permite gestionar las configuraciones del sistema en varias versiones de Red Hat Enterprise Linux, así como adoptar nuevas versiones principales.

Los paquetes **rhel-system-roles** se distribuyen a través del repositorio AppStream.

El rol de **postfix** está disponible como Technology Preview.

Las siguientes funciones son totalmente compatibles:

- **kdump**
- **red**
- **selinux**
- **almacenamiento**
- **timesync**

Para más información, consulte el artículo de la base de conocimientos sobre RHEL System Roles.

(BZ#1812552)

6.3.9. Virtualización

La virtualización KVM se puede utilizar en las máquinas virtuales Hyper-V de RHEL 8

Como Technology Preview, la virtualización KVM anidada ahora puede utilizarse en el hipervisor Microsoft Hyper-V. Como resultado, puede crear máquinas virtuales en un sistema invitado RHEL 8 que se ejecuta en un host Hyper-V.

Tenga en cuenta que actualmente, esta característica sólo funciona en los sistemas Intel. Además, en algunos casos la virtualización anidada no está habilitada por defecto en Hyper-V. Para habilitarla, consulte la siguiente documentación de Microsoft:

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization

(BZ#1519039)

AMD SEV para máquinas virtuales KVM

Como muestra de tecnología, RHEL 8 introduce la función de virtualización cifrada segura (SEV) para las máquinas host AMD EPYC que utilizan el hipervisor KVM. Si se activa en una máquina virtual (VM), SEV cifra la memoria de la VM para que el host no pueda acceder a los datos de la VM. Esto aumenta la seguridad de la VM si el host es infectado con éxito por el malware.

Tenga en cuenta que el número de máquinas virtuales que pueden utilizar esta función a la vez en un solo host está determinado por el hardware del host. Los procesadores AMD EPYC actuales admiten hasta 509 máquinas virtuales en ejecución utilizando SEV.

También tenga en cuenta que para que las VMs con SEV configuradas puedan arrancar, también debe configurar la VM con un límite de memoria duro. Para ello, añada lo siguiente a la configuración XML de la VM:

```
<memtune>
<hard_limit unit='KiB'>N</hard_limit>
</memtune>
```

El valor recomendado para N es igual o mayor que los 256 MiB de RAM del huésped. Por ejemplo, si el huésped tiene asignados 2 GiB de RAM, N debe ser 2359296 o mayor.

(BZ#1501618, BZ#1501607, JIRA:RHELPLAN-7677)

Intel vGPU

Como Technology Preview, ahora es posible dividir un dispositivo físico de GPU Intel en múltiples dispositivos virtuales denominados **dispositivos** mediados. Estos dispositivos mediados pueden ser asignados a múltiples máquinas virtuales (VM) como GPUs virtuales. Como resultado, estas máquinas virtuales comparten el rendimiento de una sola GPU Intel física.

Tenga en cuenta que sólo algunas GPUs de Intel son compatibles con la función vGPU. Además, la asignación de una GPU física a las máquinas virtuales imposibilita el uso de la GPU por parte del host y puede impedir el funcionamiento de la salida de pantalla gráfica en el host.

(BZ#1528684)

Creación de máquinas virtuales anidadas

La virtualización KVM anidada se ofrece como Technology Preview para las máquinas virtuales (VM) KVM que se ejecutan en hosts de sistemas AMD64 e IBM Z con RHEL 8. Con esta función, una VM de RHEL 7 o RHEL 8 que se ejecuta en un host físico de RHEL 8 puede actuar como hipervisor y alojar sus propias VM.

Tenga en cuenta que en RHEL 8.2 y posteriores, la virtualización anidada es totalmente compatible con las máquinas virtuales que se ejecutan en un host Intel 64.

(JIRA:RHELPLAN-14047, JIRA:RHELPLAN-24437)

Algunos adaptadores de red de Intel ahora son compatibles con SR-IOV en huéspedes RHEL en Hyper-V

Como Muestra de Tecnología, los sistemas operativos huéspedes de Red Hat Enterprise Linux que se ejecutan en un hipervisor Hyper-V pueden ahora utilizar la función de virtualización de E/S de raíz única (SR-IOV) para los adaptadores de red Intel soportados por los controladores **ixgbevf** e **iavf**. Esta función se habilita cuando se cumplen las siguientes condiciones:

- La compatibilidad con SR-IOV está activada para el controlador de interfaz de red (NIC)
- El soporte de SR-IOV está habilitado para la NIC virtual
- La compatibilidad con SR-IOV está activada para el conmutador virtual
- La función virtual (VF) de la NIC se adjunta a la máquina virtual

La función es actualmente compatible con Microsoft Windows Server 2019 y 2016.

(BZ#1348508)

6.3.10. Contenedores

la imagen del contenedor**podman** está disponible como Technology Preview

La imagen de contenedor **registry.redhat.io/rhel8/podman** es una implementación en contenedor del paquete **podman**. La herramienta **podman** se utiliza para gestionar contenedores e imágenes, volúmenes montados en esos contenedores y pods hechos a partir de grupos de contenedores. Podman se basa en la biblioteca **libpod** para la gestión del ciclo de vida de los contenedores. La librería **libpod** proporciona APIs para gestionar contenedores, pods, imágenes de contenedores y volúmenes. Esta imagen de contenedor permite crear, modificar y ejecutar imágenes de contenedor sin necesidad de instalar el paquete **podman** en su sistema. El caso de uso no cubre la ejecución de esta imagen en modo sin raíz como usuario no root. Para obtener la imagen de contenedor **registry.redhat.io/rhel8/podman**, necesita una suscripción activa a Red Hat Enterprise Linux.

(BZ#1627899)

crun está disponible como Technology Preview

El tiempo de ejecución OCI **crun** ha sido añadido al módulo **container-rools:rhl8**. El **crun** proporciona un acceso a la ejecución con cgoupsV2. El **crun** soporta una anotación que permite al contenedor acceder a los grupos adicionales de los usuarios sin raíz. Esto es útil para el montaje de volúmenes en un directorio al que el usuario sólo tiene acceso de grupo, o el directorio es setgid en él.

(BZ#1841438)

6.4. FUNCIONALIDAD OBSOLETA

Esta parte proporciona una visión general de la funcionalidad que ha sido *deprecated* en Red Hat Enterprise Linux 8.

La funcionalidad obsoleta continúa siendo soportada hasta el final de la vida útil de Red Hat Enterprise Linux 8. La funcionalidad obsoleta probablemente no será soportada en futuras versiones principales de este producto y no se recomienda para nuevas implementaciones. Para la lista más reciente de funcionalidad obsoleta dentro de una versión principal particular, consulte la última versión de la documentación de la versión.

Los componentes de hardware obsoletos no se recomiendan para nuevas implantaciones en las versiones actuales o futuras. Las actualizaciones de los controladores de hardware se limitan a correcciones de seguridad y críticas. Red Hat recomienda reemplazar este hardware tan pronto como sea razonablemente factible.

Un paquete puede ser obsoleto y no se recomienda su uso. En determinadas circunstancias, un paquete puede ser eliminado de un producto. La documentación del producto identifica entonces paquetes más recientes que ofrecen una funcionalidad similar, idéntica o más avanzada a la del paquete obsoleto, y proporciona otras recomendaciones.

Para obtener información sobre la funcionalidad que está presente en RHEL 7 pero que ha sido *removed* en RHEL 8, consulte Consideraciones al adoptar RHEL 8 .

6.4.1. Creación del instalador y de la imagen

Varios comandos y opciones de Kickstart han quedado obsoletos

El uso de los siguientes comandos y opciones en los archivos Kickstart de RHEL 8 imprimirá una advertencia en los registros.

- **auth** o **authconfig**
- **dispositivo**
- **deviceprobe**
- **dmraid**
- **instalar**
- **lilo**
- **lilocheck**
- **ratón**
- **multitrayecto**
- **bootloader --upgrade**
- **ignoredisk --interactive**
- **partición --activa**
- **reboot --kexec**

En los casos en que sólo se enumeran opciones específicas, el comando base y sus otras opciones siguen estando disponibles y no están obsoletos.

Para más detalles y cambios relacionados en Kickstart, consulte la sección de cambios en Kickstart del documento *Considerations in adopting RHEL 8* .

(BZ#1642765)

La opción --interactive del comando ignoredisk Kickstart ha quedado obsoleta

El uso de la **opción --interactive** en futuras versiones de Red Hat Enterprise Linux resultará en un error de instalación fatal. Se recomienda que modifique su archivo Kickstart para eliminar la opción.

(BZ#1637872)

el back end de lorax-composer para Image Builder está obsoleto en RHEL 8

El anterior back end **lorax-composer** para Image Builder se considera obsoleto. Sólo recibirá correcciones selectas durante el resto del ciclo de vida de Red Hat Enterprise Linux 8 y será omitido en futuros lanzamientos importantes. Red Hat recomienda que desinstale **lorax-composer** e instale **osbuild-composer** en su lugar.

Para más detalles, consulte Composición de una imagen de sistema RHEL personalizada .

(BZ#1893767)

6.4.2. Gestión del software

rpmbuild --sign está obsoleto

Con esta actualización, el comando **rpmbuild --sign** ha quedado obsoleto. El uso de este comando en futuras versiones de Red Hat Enterprise Linux puede resultar en un error. Se recomienda utilizar el comando **rpmsign** en su lugar.

(BZ#1688849)

6.4.3. Servicios de infraestructura

mailman está obsoleto

Con esta actualización, los paquetes **mailman** han sido marcados como obsoletos y no estarán disponibles en las futuras versiones principales de Red Hat Enterprise Linux.

(BZ#1890976)

6.4.4. Seguridad

Los cifrados NSS SEED están obsoletos

La librería Mozilla Network Security Services **(NSS**) no soportará suites de cifrado TLS que utilicen un cifrado SEED en una futura versión. Para asegurar una transición suave de las implementaciones que dependen de los cifrados SEED cuando NSS elimine el soporte, Red Hat recomienda habilitar el soporte para otros conjuntos de cifrado.

Tenga en cuenta que los cifrados SEED ya están desactivados por defecto en RHEL.

(BZ#1817533)

TLS 1.0 y TLS 1.1 están obsoletos

Los protocolos TLS 1.0 y TLS 1.1 están desactivados en el nivel de política criptográfica de todo el sistema **DEFAULT**. Si su escenario, por ejemplo, una aplicación de videoconferencia en el navegador web Firefox, requiere el uso de los protocolos obsoletos, cambie la política criptográfica de todo el sistema al nivel **LEGACY**:

```
# update-crypto-policies --set LEGACY
```

Para más información, consulte el artículo de la base de conocimientos Strong crypto defaults in RHEL 8 and deprecation of weak crypto algorithms en el Portal del Cliente de Red Hat y la página man **update-crypto-policies(8)**.

(BZ#1660839)

DSA está obsoleto en RHEL 8

El Algoritmo de Firma Digital (DSA) se considera obsoleto en Red Hat Enterprise Linux 8. Los mecanismos de autenticación que dependen de claves DSA no funcionan en la configuración por defecto. Tenga en cuenta que los clientes **OpenSSH** no aceptan claves de host DSA incluso en el nivel de política criptográfica de todo el sistema **LEGACY**.

(BZ#1646541)

SSL2 Client Hello ha quedado obsoleto en NSS

El protocolo Transport Layer Security**(TLS**) versión 1.2 y anteriores permiten iniciar una negociación con un mensaje **Client Hello** formateado de manera compatible con el protocolo Secure Sockets Layer**(SSL**) versión 2. La compatibilidad con esta función en la biblioteca de servicios de seguridad de la red**(NSS**) ha quedado obsoleta y está desactivada por defecto.

Las aplicaciones que requieran soporte para esta función deben utilizar la nueva API **SSL_ENABLE_V2_COMPATIBLE_HELLO** para habilitarla. El soporte para esta función puede ser eliminado completamente en futuras versiones de Red Hat Enterprise Linux 8.

(BZ#1645153)

El TPM 1.2 está obsoleto

La versión estándar del criptoprocesador seguro Trusted Platform Module (TPM) se actualizó a la versión 2.0 en 2016. El TPM 2.0 ofrece muchas mejoras con respecto al TPM 1.2, y no es compatible con la versión anterior. El TPM 1.2 está obsoleto en RHEL 8, y es posible que se elimine en la próxima versión principal.

(BZ#1657927)

6.4.5. Red

Los scripts de red están obsoletos en RHEL 8

Los scripts de red están obsoletos en Red Hat Enterprise Linux 8 y ya no se proporcionan por defecto. La instalación básica proporciona una nueva versión de los scripts **ifup** e **ifdown** que llaman al servicio **NetworkManager** a través de la herramienta **nmcli**. En Red Hat Enterprise Linux 8, para ejecutar los scripts **ifup** e **ifdown**, NetworkManager debe estar ejecutándose.

Tenga en cuenta que los comandos personalizados en los scripts **/sbin/ifup-local**, **ifdown-pre-local** e **ifdown-local** no se ejecutan.

Si se requiere alguno de estos scripts, la instalación de los scripts de red obsoletos en el sistema sigue siendo posible con el siguiente comando:

```
~]# yum install network-scripts
```

Los scripts **ifup** e **ifdown** enlazan con los scripts de red heredados instalados.

Al llamar a los scripts de red heredados se muestra una advertencia sobre su desaprobación.

(BZ#1647725)

6.4.6. Núcleo

La instalación de RHEL for Real Time 8 mediante el arranque sin disco ha quedado obsoleta

El arranque sin disco permite que varios sistemas compartan un sistema de archivos raíz a través de la red. Aunque es conveniente, el arranque sin disco es propenso a introducir latencia de red en cargas de trabajo en tiempo real. Con una futura actualización menor de RHEL for Real Time 8, la función de arranque sin disco dejará de estar soportada.

(BZ#1748980)

El controlador qla3xxx está obsoleto

El controlador **qla3xxx** ha quedado obsoleto en RHEL 8. Es probable que el controlador no sea soportado en futuras versiones importantes de este producto, por lo que no se recomienda para nuevas implantaciones.

(BZ#1658840)

Los controladores dl2k, dnet, ethoc y dlci están obsoletos

Los controladores **dl2k**, **dnet**, **ethoc** y **dlci** han quedado obsoletos en RHEL 8. Es probable que estos controladores no reciban soporte en futuras versiones importantes de este producto, por lo que no se recomiendan para nuevas implantaciones.

(BZ#1660627)

6.4.7. Sistemas de archivos y almacenamiento

El parámetro de la línea de comandos del núcleo del ascensor está obsoleto

El parámetro de línea de comandos del kernel **elevador** se utilizaba en versiones anteriores de RHEL para establecer el programador de discos para todos los dispositivos. En RHEL 8, el parámetro está obsoleto.

El kernel de Linux ha eliminado el soporte para el parámetro **elevador**, pero todavía está disponible en RHEL 8 por razones de compatibilidad.

Tenga en cuenta que el kernel selecciona un programador de disco por defecto basado en el tipo de dispositivo. Esta es típicamente la configuración óptima. Si necesita un planificador diferente, Red Hat recomienda que utilice las reglas **udev** o el servicio Tuned para configurarlo. Coinciden con los dispositivos seleccionados y cambian el planificador sólo para esos dispositivos.

Para más información, consulte Configuración del programador de discos .

(BZ#1665295)

La réplica LVM está obsoleta

El tipo de segmento **espejo** LVM está ahora obsoleto. La compatibilidad con el **espejo** se eliminará en una futura versión importante de RHEL.

Red Hat recomienda que utilice dispositivos RAID 1 de LVM con un tipo de segmento **raid1** en lugar de **espejo**. El tipo de segmento **raid1** es el tipo de configuración RAID por defecto y reemplaza **al** espejo como la solución recomendada.

Para convertir los dispositivos **en** espejo en **raid1**, consulte Convertir un dispositivo LVM en espejo en un dispositivo RAID1.

La **réplica de** LVM tiene varios problemas conocidos. Para más detalles, consulte los problemas conocidos en sistemas de archivos y almacenamiento .

(BZ#1827628)

peripety está obsoleto

El paquete **peripety** está obsoleto desde RHEL 8.3.

El demonio de notificación de eventos de almacenamiento Peripety analiza los registros de almacenamiento del sistema en eventos de almacenamiento estructurados. Le ayuda a investigar los problemas de almacenamiento.

(BZ#1871953)

NFSv3 sobre UDP ha sido desactivado

El servidor NFS ya no abre o escucha en un socket del Protocolo de Datagramas de Usuario (UDP) por defecto. Este cambio sólo afecta a la versión 3 de NFS porque la versión 4 requiere el Protocolo de Control de Transmisión (TCP).

NFS sobre UDP ya no está soportado en RHEL 8.

(BZ#1592011)

6.4.8. Gestión de la identidad

openssh-ldap ha quedado obsoleto

El subpaquete **openssh-ldap** ha sido obsoleto en Red Hat Enterprise Linux 8 y será eliminado en RHEL 9. Como el subpaquete **openssh-ldap** no se mantiene en el upstream, Red Hat recomienda utilizar SSSD y el helper **sss_ssh_authorizedkeys**, que se integran mejor con otras soluciones IdM y son más seguras.

Por defecto, los proveedores SSSD **ldap** e **ipa** leen el atributo LDAP **sshPublicKey** del objeto usuario, si está disponible. Tenga en cuenta que no puede utilizar la configuración predeterminada de SSSD para el proveedor de **anuncios** o los dominios de confianza de IdM para recuperar claves públicas SSH de Active Directory (AD), ya que AD no tiene un atributo LDAP predeterminado para almacenar una clave pública.

Para permitir que el ayudante **sss_ssh_authorizedkeys** obtenga la clave de SSSD, habilite el respondedor **ssh** añadiendo **ssh** a la opción de **servicios** en el archivo **sssd.conf**. Consulte la página man de **sssd.conf(5**) para más detalles.

Para permitir que **sshd** utilice **sss_ssh_authorizedkeys**, añada las opciones **AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys** y **AuthorizedKeysCommandUser**

nobody al archivo **/etc/ssh/sshd_config** como se describe en la página man de **sss_ssh_authorizedkeys(1)**.

(BZ#1871025)

Se han eliminado los tipos de cifrado DES y 3DES

Debido a razones de seguridad, el algoritmo del Estándar de Encriptación de Datos (DES) ha sido obsoleto y deshabilitado por defecto desde RHEL 7. Con la reciente actualización de los paquetes de Kerberos, los tipos de cifrado Single-DES (DES) y Triple-DES (3DES) se han eliminado de RHEL 8.

Si has configurado los servicios o los usuarios para que sólo utilicen el cifrado DES o 3DES, podrías experimentar interrupciones del servicio como:

- Errores de autenticación de Kerberos
- errores de codificación de**tipo de letra desconocido**
- Los centros de distribución de Kerberos (KDC) con claves maestras de bases de datos encriptadas con DES (**K/M**) no se inician

Realice las siguientes acciones para preparar la actualización:

1. Compruebe si su KDC utiliza el cifrado DES o 3DES con los scripts de código abierto Python **krb5check**. Consulte krb5check en GitHub.
2. Si utiliza el cifrado DES o 3DES con alguna entidad de crédito de Kerberos, vuelva a cifrarla con un tipo de cifrado compatible, como el estándar de cifrado avanzado (AES). Para obtener instrucciones sobre el cambio de claves, consulte Retirar DES en la documentación de MIT Kerberos.
3. Pruebe la independencia de DES y 3DES configurando temporalmente las siguientes opciones de Kerberos antes de la actualización:
    a. En **/var/kerberos/krb5kdc/kdc.conf** en el KDC, establezca **supported_enctypes** y no incluya **des** o **des3**.
    b. Para cada host, en **/etc/krb5.conf** y cualquier archivo en **/etc/krb5.conf.d**, establece **allow_weak_crypto** como **falso**. Es falso por defecto.
    c. Para cada host, en **/etc/krb5.conf** y cualquier archivo en **/etc/krb5.conf.d**, establezca **permitted_enctypes**, **default_tgs_enctypes**, y **default_tkt_enctypes** y no incluya **des** o **des3**.
4. Si no experimenta ninguna interrupción del servicio con la configuración de Kerberos de prueba del paso anterior, elimínela y actualice. No necesita esos ajustes después de actualizar a los últimos paquetes de Kerberos.

(BZ#1877991)

6.4.9. Escritorio

La biblioteca libgnome-keyring ha quedado obsoleta

La librería **libgnome-keyring** ha sido obviada en favor de la librería **libsecret**, ya que **libgnome-keyring** no es mantenida por el upstream, y no sigue las políticas criptográficas necesarias para RHEL. La nueva biblioteca **libsecret** es el reemplazo que sigue los estándares de seguridad necesarios.

(BZ#1607766)

6.4.10. Infraestructuras gráficas

Las tarjetas gráficas AGP ya no son compatibles

Las tarjetas gráficas que utilizan el bus Accelerated Graphics Port (AGP) no son compatibles con Red Hat Enterprise Linux 8. Utilice las tarjetas gráficas con bus PCI-Express como reemplazo recomendado.

(BZ#1569610)

6.4.11. La consola web

La consola web ya no admite traducciones incompletas

La consola web de RHEL ya no proporciona traducciones para los idiomas que tienen traducciones disponibles para menos del 50 % de las cadenas traducibles de la consola. Si el navegador solicita la traducción a dicho idioma, la interfaz de usuario estará en inglés.

(BZ#1666722)

6.4.12. Roles del sistema Red Hat Enterprise Linux

El paquete **geoipupdate** ha quedado obsoleto

El paquete **geoipupdate** requiere una suscripción de terceros y también descarga contenido propietario. Por lo tanto, el paquete **geoipupdate** ha quedado obsoleto y se eliminará en la próxima versión principal de RHEL.

(BZ#1874892)

6.4.13. Virtualización

virt-manager ha quedado obsoleto

La aplicación Virtual Machine Manager, también conocida como **virt-manager**, ha quedado obsoleta. La consola web de RHEL 8, también conocida como **Cockpit**, está destinada a convertirse en su reemplazo en una versión posterior. Por lo tanto, se recomienda utilizar la consola web para gestionar la virtualización en una GUI. Tenga en cuenta, sin embargo, que algunas funciones disponibles en **virt-manager** pueden no estar aún disponibles en la consola web de RHEL 8.

(JIRA:RHELPLAN-10304)

Las instantáneas de las máquinas virtuales no se soportan correctamente en RHEL 8

El mecanismo actual de creación de instantáneas de máquinas virtuales (VM) ha quedado obsoleto, ya que no funciona de forma fiable. En consecuencia, se recomienda no utilizar las instantáneas de VM en RHEL 8.

Tenga en cuenta que se está desarrollando un nuevo mecanismo de instantáneas de máquinas virtuales que se implementará completamente en una futura versión menor de RHEL 8.

(BZ#1686057)

El tipo de GPU virtual Cirrus VGA ha quedado obsoleto

Con una futura actualización mayor de Red Hat Enterprise Linux, el dispositivo **Cirrus VGA** GPU ya no será soportado en las máquinas virtuales KVM. Por lo tanto, Red Hat recomienda utilizar los dispositivos **stdvga**, **virtio-vga**, o **qxl** en lugar de Cirrus VGA.

(BZ#1651994)

SPICE ha quedado obsoleto

En RHEL 8.3, el protocolo de visualización remota SPICE ha quedado obsoleto. Tenga en cuenta que SPICE seguirá siendo compatible con RHEL 8, pero Red Hat recomienda utilizar soluciones alternativas para la transmisión de pantalla remota:

- Para el acceso remoto a la consola, utilice el protocolo VNC.
- Para funciones avanzadas de visualización remota, utilice herramientas de terceros como RDP, HP RGS o Mechdyne TGX.

(BZ#1849563)

6.4.14. Contenedores

La API REST de Podman basada en varlink V1 ha quedado obsoleta

La API REST de Podman basada en varlink V1 ha sido obviada en favor de la nueva API REST de Podman V2. Esta funcionalidad será eliminada en una versión posterior de Red Hat Enterprise Linux 8.

(JIRA:RHELPLAN-60226)

6.4.15. Paquetes obsoletos

Los siguientes paquetes han sido obviados y probablemente no serán incluidos en una futura versión mayor de Red Hat Enterprise Linux:

- 389-ds-base-legacy-tools
- authd
- custodia
- nombre de host
- libidn
- lorax-composer
- mercurial
- herramientas de red
- red-scripts
- nss-pam-ldapd
- sendmail
- yp-tools
- ypbind

- ypserv

6.5. PROBLEMAS CONOCIDOS

Esta parte describe los problemas conocidos en Red Hat Enterprise Linux 8.3.

6.5.1. Creación del instalador y de la imagen

Los comandos Kickstart **auth** y **authconfig** requieren el repositorio AppStream

El paquete **authselect-compat** es necesario para los comandos **auth** y **authconfig** Kickstart durante la instalación. Sin este paquete, la instalación falla si se utilizan **auth** o **authconfig**. Sin embargo, por diseño, el paquete **authselect-compat** sólo está disponible en el repositorio de AppStream.

Para solucionar este problema, verifique que los repositorios de BaseOS y AppStream estén disponibles para el instalador o utilice el comando **authselect** Kickstart durante la instalación.

(BZ#1640697)

Los comandos **reboot --kexec** e **inst.kexec** no proporcionan un estado predecible del sistema

Realizar una instalación de RHEL con el comando **reboot --kexec** Kickstart o los parámetros de arranque del kernel **inst.kexec** no proporcionan el mismo estado predecible del sistema que un reinicio completo. Como consecuencia, cambiar al sistema instalado sin reiniciar puede producir resultados impredecibles.

Tenga en cuenta que la función **kexec** está obsoleta y se eliminará en una futura versión de Red Hat Enterprise Linux.

(BZ#1697896)

El acceso a la red no está activado por defecto en el programa de instalación

Varias funciones de instalación requieren acceso a la red, por ejemplo, el registro de un sistema mediante la red de distribución de contenidos (CDN), la compatibilidad con el servidor NTP y las fuentes de instalación de la red. Sin embargo, el acceso a la red no está habilitado por defecto, y como resultado, estas características no pueden ser utilizadas hasta que se habilite el acceso a la red.

Para solucionar este problema, añada **ip=dhcp** a las opciones de arranque para permitir el acceso a la red cuando se inicie la instalación. Opcionalmente, pasar un archivo Kickstart o un repositorio ubicado en la red utilizando las opciones de arranque también resuelve el problema. Como resultado, las características de instalación basadas en la red pueden ser utilizadas.

(BZ#1757877)

El nuevo back-end de **osbuild-composer** no replica el estado del blueprint de **lorax-composer** en las actualizaciones

Los usuarios de Image Builder que están actualizando desde el back end **lorax-composer** al nuevo back end **osbuild-composer**, los blueprints pueden desaparecer. Como resultado, una vez completada la actualización, los blueprints no se muestran automáticamente. Para solucionar este problema, realice los siguientes pasos.

Requisitos previos

- Tiene instalada la utilidad **composer-cli** CLI.

Procedimiento

1. Ejecute el comando para cargar los planos anteriores basados en **lorax-composer** en el nuevo back end **osbuild-composer**:

```
$ for blueprint in $(find /var/lib/lorax/composer/blueprints/git/workspace/master -name
'*.toml'); do composer-cli blueprints push \ "${blueprint}"; done
```

Como resultado, los mismos planos están ahora disponibles en el back end **de osbuild-composer**.

Recursos adicionales

- Para más detalles sobre este problema conocido, vea el artículo Los planos de Image Builder ya no están presentes tras una actualización a Red Hat Enterprise Linux 8.3.

(BZ#1897383)

El servidor HTTPS autofirmado no se puede utilizar en la instalación de Kickstart

Actualmente, el instalador falla al instalar desde un servidor https autofirmado cuando se especifica el origen de la instalación en el archivo kickstart y se utiliza la opción **--noverifyssl**:

```
url --url=https://SERVER/PATH --noverifyssl
```

Para solucionar este problema, añada el parámetro **inst.noverifyssl** a la línea de comandos del kernel al iniciar la instalación kickstart.

Por ejemplo:

```
inst.ks=
```

(BZ#1745064)

La instalación de la interfaz gráfica de usuario podría fallar si se intenta anular el registro mediante la CDN antes de que se complete la actualización del repositorio

Desde RHEL 8.2, cuando se registra el sistema y se adjuntan suscripciones utilizando la Red de Entrega de Contenidos (CDN), el programa de instalación de la GUI inicia una actualización de los metadatos del repositorio. El proceso de actualización no es parte del proceso de registro y suscripción, y como consecuencia, el botón **Unregister** está habilitado en la ventana **Connect to Red Hat** Dependiendo de la conexión de red, el proceso de actualización puede tardar más de un minuto en completarse. Si hace clic en el botón **Unregister** antes de que se complete el proceso de actualización, la instalación de la GUI podría fallar, ya que el proceso de desregistro elimina los archivos del repositorio de la CDN y los certificados necesarios para que el programa de instalación se comunique con la CDN.

Para solucionar este problema, complete los siguientes pasos en la instalación de la GUI después de haber pulsado el botón **Register** en la ventana **Connect to Red Hat**

1. Desde la ventana **Connect to Red Hat**, haga clic en **Done** para volver a la ventana **Installation Summary**.

2. Desde la ventana **Installation Summary**, verifique que los mensajes de estado **Installation Source** y **Software Selection** en cursiva no muestran ninguna información de procesamiento.

3. Cuando las categorías de Fuente de Instalación y Selección de Software estén listas, haga clic en **Connect to Red Hat**

4. Haga clic en el botón **Unregister**.

Después de realizar estos pasos, puede anular con seguridad el registro del sistema durante la instalación de la GUI.

(BZ#1821192)

El registro falla para las cuentas de usuario que pertenecen a varias organizaciones

Actualmente, cuando se intenta registrar un sistema con una cuenta de usuario que pertenece a varias organizaciones, el proceso de registro falla con el mensaje de error **You must specify an organization for new units**.

Para solucionar este problema, puedes

- Utilice una cuenta de usuario diferente que no pertenezca a varias organizaciones.
- Utilice el método de autenticación **Activation Key** disponible en la función Conectar con Red Hat para las instalaciones GUI y Kickstart.
- Omita el paso de registro en Conéctese a Red Hat y utilice el Gestor de suscripciones para registrar su sistema después de la instalación.

(BZ#1822880)

El instalador de RHEL no se inicia cuando se configuran las interfaces de red InfiniBand mediante las opciones de arranque del instalador

Cuando se configuran las interfaces de red InfiniBand en una fase temprana de la instalación de RHEL utilizando las opciones de arranque del instalador (por ejemplo, para descargar la imagen del instalador utilizando el servidor PXE), el instalador no consigue activar las interfaces de red.

Este problema se produce porque RHEL NetworkManager no reconoce las interfaces de red en modo InfiniBand y, en su lugar, configura conexiones Ethernet para las interfaces.

Como resultado, la activación de la conexión falla, y si la conectividad a través de la interfaz InfiniBand es requerida en una etapa temprana, el instalador de RHEL falla al iniciar la instalación.

Para solucionar este problema, cree un nuevo medio de instalación que incluya los paquetes actualizados de Anaconda y NetworkManager, utilizando la herramienta Lorax.

Para más información sobre cómo crear un nuevo medio de instalación que incluya los paquetes actualizados de Anaconda y NetworkManager, utilizando la herramienta Lorax, consulte No se puede instalar Red Hat Enterprise Linux 8.3.0 con interfaces de red InfiniBand

(BZ#1890261)

La instalación de Anaconda falla cuando el espacio de nombres del dispositivo NVDIMM está configurado en modo devdax.

La instalación de Anaconda falla con un trackback después de arrancar con el espacio de nombres del dispositivo NVDIMM configurado en modo **devdax** antes de la instalación de la GUI.

Para solucionar este problema, reconfigure el dispositivo NVDIMM para establecer el espacio de nombres en un modo diferente al modo **devdax** antes de comenzar la instalación. Como resultado, puede continuar con la instalación.

(BZ#1891827)

No se detecta la fuente de instalación de **medios locales** cuando se arranca la instalación desde un USB creado con una herramienta de terceros

Cuando se arranca la instalación de RHEL desde un USB creado con una herramienta de terceros, el instalador no detecta la fuente de instalación de **medios locales** (sólo se detecta 'Red Hat CDN').

Este problema se produce porque la opción de arranque por defecto **int.stage2=** intenta buscar el formato de imagen **iso9660**. Sin embargo, una herramienta de terceros podría crear una imagen ISO con un formato diferente.

Como solución, utilice cualquiera de las siguientes soluciones:

- Al arrancar la instalación, pulse la tecla **Tab** para editar la línea de comandos del kernel, y cambie la opción de arranque **inst.stage2=** por **inst.repo=**.
- Para crear un dispositivo USB de arranque en Windows, utilice Fedora Media Writer.
- Si utiliza una herramienta de terceros como Rufus para crear un dispositivo USB de arranque, primero regenere la imagen ISO de RHEL en un sistema Linux y luego utilice la herramienta de terceros para crear un dispositivo USB de arranque.

Para obtener más información sobre los pasos necesarios para llevar a cabo cualquiera de las soluciones especificadas, consulte, Los medios de instalación no se detectan automáticamente durante la instalación de RHEL 8.3

(BZ#1877697)

Anaconda ahora muestra un diálogo para discos DASD **ldl** o sin formato en modo texto

Anteriormente, durante una instalación en modo texto, Anaconda no mostraba un cuadro de diálogo para los discos de distribución de discos Linux**(ldl**) o los discos de dispositivos de almacenamiento de acceso directo (DASD) no formateados. Como resultado, los usuarios no podían utilizar esos discos para la instalación.

Con esta actualización, en el modo de texto Anaconda reconoce los discos DASD **ldl** y no formateados y muestra un diálogo en el que los usuarios pueden formatearlos adecuadamente para su futura utilización en la instalación.

(BZ#1874394)

6.5.2. Gestión de suscripciones

los complementos syspurpose no tienen efecto en la salida de subscription-manager attach --auto.

En Red Hat Enterprise Linux 8, se han añadido cuatro atributos de la herramienta de línea de comandos **syspurpose**: **role,** usage, **service_level_agreement** y **addons**. Actualmente, sólo **role**, **usage** y **service_level_agreement** afectan la salida de la ejecución del comando **subscription-manager attach --auto**. Los usuarios que intenten establecer valores en el argumento **addons** no observarán ningún efecto en las suscripciones que se adjuntan automáticamente.

(BZ#1687900)

6.5.3. Servicios de infraestructura

libmaxminddb-devel-debuginfo.rpm se elimina al ejecutar dnf update

Al ejecutar el comando **dnf update**, la herramienta binaria **mmdblookup** se mueve del subpaquete **libmaxminddb-devel** al paquete principal **libmaxmindb**. En consecuencia, se elimina el **archivo libmaxminddb-devel-debuginfo.** rpm, lo que puede crear una ruta de actualización rota para este paquete. Para solucionar este problema, elimine **libmaxminddb-devel-debuginfo** antes de ejecutar el comando **dnf update**.

Nota: **libmaxminddb-debuginfo** es el nuevo paquete **debuginfo**.

(BZ#1642001)

6.5.4. Seguridad

Los usuarios pueden ejecutar comandos sudo como usuarios bloqueados

En los sistemas donde los permisos **sudoers** están definidos con la palabra clave **ALL**, los usuarios con permisos **sudo** pueden ejecutar comandos **sudo** como usuarios cuyas cuentas están bloqueadas. En consecuencia, las cuentas bloqueadas y caducadas pueden seguir utilizándose para ejecutar comandos.

Para solucionar este problema, habilite la opción recién implementada **runas_check_shell** junto con la configuración adecuada de shells válidos en **/etc/shells**. Esto evita que los atacantes ejecuten comandos bajo cuentas del sistema como **bin**.

(BZ#1786990)

GnuTLS falla al reanudar la sesión actual con el servidor NSS

Cuando se reanuda una sesión TLS (Transport Layer Security) 1.3, el cliente **GnuTLS** espera 60 milisegundos más un tiempo estimado de ida y vuelta para que el servidor envíe los datos de reanudación de la sesión. Si el servidor no envía los datos de reanudación en este tiempo, el cliente crea una nueva sesión en lugar de reanudar la sesión actual. Esto no tiene efectos adversos graves, salvo un impacto menor en el rendimiento de una negociación de sesión normal.

(BZ#1677754)

libselinux-python sólo está disponible a través de su módulo

El paquete **libselinux-python** sólo contiene bindings de Python 2 para el desarrollo de aplicaciones SELinux y se utiliza por compatibilidad con versiones anteriores. Por esta razón, **libselinux-python** ya no está disponible en los repositorios por defecto de RHEL 8 a través del comando **dnf install libselinux-python**.

Para solucionar este problema, active los módulos **libselinux-python** y **python27**, e instale el paquete **libselinux-python** y sus dependencias con los siguientes comandos:

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

Alternativamente, instale **libselinux-python** utilizando su perfil de instalación con un solo comando:

```
# dnf module install libselinux-python:2.8/common
```

Como resultado, puede instalar **libselinux-python** utilizando el módulo correspondiente.

(BZ#1666328)

udica procesa contenedores UBI 8 sólo cuando se inicia con --env container=podman

Los contenedores Red Hat Universal Base Image 8 (UBI 8) establecen la variable de entorno **del** contenedor con el valor **oci** en lugar del valor **podman**. Esto evita que la herramienta **udica** analice un archivo de notación de objetos JavaScript (JSON) del contenedor.

Para solucionar este problema, inicie un contenedor UBI 8 utilizando un comando **podman** con el parámetro **--env container=podman**. Como resultado, **udica** puede generar una política SELinux para un contenedor UBI 8 sólo cuando se utiliza la solución descrita.

(BZ#1763210)

Efectos negativos de la configuración de registro por defecto en el rendimiento

La configuración del entorno de registro por defecto puede consumir 4 GB de memoria o incluso más y los ajustes de los valores de límite de velocidad son complejos cuando **systemd-journald** se ejecuta con **rsyslog**.

Consulte el artículo de la base de conocimientos Efectos negativos de la configuración de registro por defecto de RHEL en el rendimiento y sus mitigaciones para obtener más información.

(JIRA:RHELPLAN-10431)

Los permisos de archivo de /etc/passwd- no están alineados con el Benchmark 1.0.0 de CIS RHEL 8

Debido a un problema con el CIS Benchmark, la remediación de la regla SCAP que asegura los permisos en el archivo **/etc/passwd-** backup configura los permisos a **0644**. Sin embargo, el CIS **Red Hat Enterprise Linux 8 Benchmark 1.0.0** requiere permisos de archivo **0600** para ese archivo. Como consecuencia, los permisos de archivo de **/etc/passwd-** no están alineados con el benchmark después de la remediación.

(BZ#1858866)

SELINUX=disabled en /etc/selinux/config no funciona correctamente

Desactivar SELinux usando la opción **SELINUX=disabled** en el **archivo /etc/selinux/config** resulta en un proceso en el que el kernel arranca con SELinux activado y cambia a modo desactivado más tarde en el proceso de arranque. Esto podría causar fugas de memoria y condiciones de carrera y, en consecuencia, también pánicos en el kernel.

Para solucionar este problema, desactive SELinux añadiendo el parámetro **selinux=0** a la línea de comandos del kernel, tal y como se describe en la sección Cambio de los modos de SELinux en el arranque del título Uso de SELinux, si su escenario realmente requiere desactivar SELinux por completo.

(JIRA:RHELPLAN-34199)

ssh-keyscan no puede recuperar las claves RSA de los servidores en modo FIPS

El algoritmo **SHA-1** está desactivado para las firmas RSA en el modo FIPS, lo que impide que la utilidad **ssh-keyscan** recupere las claves RSA de los servidores que operan en ese modo.

Para solucionar este problema, utilice claves ECDSA en su lugar, o recupere las claves localmente desde el archivo **/etc/ssh/ssh_host_rsa_key.pub** en el servidor.

(BZ#1744108)

OpenSSL maneja incorrectamente los tokens PKCS #11 que no admiten firmas RSA o RSA-PSS en bruto

La biblioteca **OpenSSL** no detecta las capacidades relacionadas con las claves de los tokens PKCS #11. En consecuencia, el establecimiento de una conexión TLS falla cuando se crea una firma con un token que no admite firmas RSA o RSA-PSS en bruto.

Para solucionar el problema, añada las siguientes líneas después de la línea **.include** al final de la sección **crypto_policy** en el archivo **/etc/pki/tls/openssl.cnf**:

```
SignatureAlgorithms =
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384
MaxProtocol = TLSv1.2
```

Como resultado, se puede establecer una conexión TLS en el escenario descrito.

(BZ#1685470)

OpenSSL en modo FIPS sólo acepta parámetros D-H específicos

En el modo FIPS, los clientes de la capa de seguridad de transporte (TLS) que utilizan OpenSSL devuelven un error de **valor dh incorrecto** y abortan las conexiones TLS con servidores que utilizan parámetros generados manualmente. Esto se debe a que OpenSSL, cuando está configurado para trabajar de acuerdo con FIPS 140-2, sólo funciona con parámetros D-H que cumplen con el Apéndice D de NIST SP 800-56A rev3 (grupos 14, 15, 16, 17 y 18 definidos en RFC 3526 y con grupos definidos en RFC 7919). Además, los servidores que utilizan OpenSSL ignoran todos los demás parámetros y en su lugar seleccionan parámetros conocidos de tamaño similar. Para solucionar este problema, utilice sólo los grupos que cumplen con la normativa.

(BZ#1810911)

La eliminación del paquete rpm-plugin-selinux conlleva la eliminación de todos los paquetes selinux-policy del sistema

Eliminar el paquete **rpm-plugin-selinux** deshabilita SELinux en la máquina. También elimina todos los paquetes **selinux-policy** del sistema. La instalación repetida del paquete **rpm-plugin-selinux** instala entonces la política **SELinux-policy-minimum**, incluso si la política **selinux-policy-targeted** estaba previamente presente en el sistema. Sin embargo, la instalación repetida no actualiza el archivo de configuración de SELinux para tener en cuenta el cambio de política. Como consecuencia, SELinux está deshabilitado incluso al reinstalar el paquete **rpm-plugin-selinux**.

Para solucionar este problema:

1. Introduzca el comando **umount /sys/fs/selinux/**.
2. Instale manualmente el paquete **selinux-policy-targeted** que falta.
3. Edite el archivo **/etc/selinux/config** para que la política sea igual a **SELINUX=enforcing**.
4. Introduzca el comando **load_policy -i**.

Como resultado, SELinux está habilitado y ejecuta la misma política que antes.

(BZ#1641631)

el serviciosystemd no puede ejecutar comandos desde rutas arbitrarias

El servicio **systemd** no puede ejecutar comandos desde rutas arbitrarias **/home/user/bin** porque el paquete de políticas de SELinux no incluye ninguna regla de este tipo. En consecuencia, los servicios personalizados que se ejecutan en rutas que no son del sistema fallan y finalmente registran los

mensajes de auditoría de denegación de Access Vector Cache (AVC) cuando SELinux deniega el acceso. Para solucionar este problema, realice una de las siguientes acciones:

- Ejecute el comando utilizando un script **shell** con la opción **-c**. Por ejemplo,

  ```
  bash -c command
  ```

- Ejecuta el comando desde una ruta común utilizando los directorios comunes **/bin**, **/sbin**, **/usr/sbin**, **/usr/local/bin** y **/usr/local/sbin**.

(BZ#1860443)

rpm_verify_permissions falla en el perfil CIS

La regla **rpm_verify_permissions** compara los permisos de los archivos con los permisos por defecto de los paquetes. Sin embargo, el perfil del Centro de Seguridad de Internet (CIS), que es proporcionado por los paquetes **scap-security-guide**, cambia algunos permisos de archivos para que sean más estrictos que los predeterminados. Como consecuencia, la verificación de ciertos archivos usando **rpm_verify_permissions** falla.

Para solucionar este problema, verifique manualmente que estos archivos tengan los siguientes permisos:

- **/etc/cron.d** (0700)
- **/etc/cron.hourly** (0700)
- **/etc/cron.monthly** (0700)
- **/etc/crontab** (0600)
- **/etc/cron.weekly** (0700)
- **/etc/cron.daily** (0700)

(BZ#1843913)

Kickstart utiliza org_fedora_oscap en lugar de com_redhat_oscap en RHEL 8

El Kickstart hace referencia al complemento Anaconda del Protocolo de Automatización de Contenidos de Seguridad Abierta (OSCAP) como **org_fedora_oscap** en lugar de **com_redhat_oscap**, lo que podría causar confusión. Esto se hace para mantener la compatibilidad con Red Hat Enterprise Linux 7.

(BZ#1665082)

Algunos conjuntos de reglas interdependientes en SSG pueden fallar

La remediación de las reglas de **la Guía de Seguridad SCAP** (SSG) en un benchmark puede fallar debido al orden indefinido de las reglas y sus dependencias. Si dos o más reglas deben ejecutarse en un orden determinado, por ejemplo, cuando una regla instala un componente y otra regla configura el mismo componente, pueden ejecutarse en el orden incorrecto y la corrección informa de un error. Para solucionar este problema, ejecute la corrección dos veces, y la segunda ejecución corrige las reglas dependientes.

(BZ#1750755)

El complemento OSCAP Anaconda no instala todos los paquetes en modo texto

El **complemento OSCAP Anaconda** no puede modificar la lista de paquetes seleccionados para su instalación por el instalador del sistema si la instalación se ejecuta en modo texto. En consecuencia, cuando se especifica un perfil de política de seguridad mediante Kickstart y la instalación se ejecuta en modo texto, cualquier paquete adicional requerido por la política de seguridad no se instala durante la instalación.

Para solucionar este problema, ejecute la instalación en modo gráfico o especifique todos los paquetes que requiere el perfil de la política de seguridad en la sección **%packages** de su archivo Kickstart.

Como resultado, los paquetes requeridos por el perfil de política de seguridad no se instalan durante la instalación de RHEL sin una de las soluciones descritas, y el sistema instalado no cumple con el perfil de política de seguridad dado.

(BZ#1674001)

El complemento OSCAP Anaconda no maneja correctamente los perfiles personalizados

El plugin **OSCAP Anaconda Addon** no maneja adecuadamente los perfiles de seguridad con personalizaciones en archivos separados. En consecuencia, el perfil personalizado no está disponible en la instalación gráfica de RHEL aunque lo especifique correctamente en la sección Kickstart correspondiente.

Para solucionar este problema, siga las instrucciones del artículo de la base de conocimientos Creación de un único flujo de datos SCAP a partir de un DS original y un archivo de adaptación. Como resultado de esta solución, puede utilizar un perfil SCAP personalizado en la instalación gráfica de RHEL.

(BZ#1691305)

Los perfiles basados en OSPP son incompatibles con los grupos de paquetes GUI.

Los paquetes de**GNOME** instalados por el grupo de paquetes *Server with GUI* requieren el paquete **nfs-utils** que no es compatible con el Perfil de Protección del Sistema Operativo (OSPP). Como consecuencia, al seleccionar el grupo de paquetes *Server with GUI* durante la instalación de un sistema con perfiles OSPP o basados en OSPP, por ejemplo, Guía de Implementación Técnica de Seguridad (STIG), OpenSCAP muestra una advertencia de que el grupo de paquetes seleccionado no es compatible con la política de seguridad. Si el perfil basado en OSPP se aplica después de la instalación, el sistema no puede arrancar. Para solucionar este problema, no instale el grupo de paquetes *Server with GUI* ni ningún otro grupo que instale GUI cuando utilice el perfil OSPP y los perfiles basados en OSPP. Si utiliza los grupos de paquetes *Server* o *Minimal Install* en su lugar, el sistema se instala sin problemas y funciona correctamente.

(BZ#1787156)

No es posible la instalación con el Servidor con selecciones de software de GUI o Estación de Trabajo y perfil de seguridad CIS

El perfil de seguridad CIS no es compatible con las selecciones de software Servidor con **GUI** y **Estación de Trabajo**. En consecuencia, no es posible realizar una instalación de RHEL 8 con la selección de software Servidor con **GUI** y el perfil CIS. Un intento de instalación utilizando el perfil CIS y cualquiera de estas selecciones de software generará el mensaje de error:

> el paquete xorg-x11-server-common ha sido añadido a la lista de paquetes excluidos, pero no puede ser eliminado de la selección de software actual sin romper la instalación.

Para solucionar el problema, no utilice el perfil de seguridad CIS con las selecciones de software **Servidor con GUI** o **Estación de trabajo**.

(BZ#1843932)

La corrección de las reglas relacionadas con el servicio durante las instalaciones de kickstart podría fallar

Durante una instalación kickstart, la utilidad OpenSCAP a veces muestra incorrectamente que no es necesaria una remediación del estado de **habilitación** o **deshabilitación de** servicios. En consecuencia, OpenSCAP podría establecer los servicios del sistema instalado en un estado no compatible. Como solución, puede escanear y remediar el sistema después de la instalación kickstart. Esto solucionará los problemas relacionados con los servicios.

(BZ#1834716)

Algunas cadenas de prioridad de rsyslog no funcionan correctamente

La compatibilidad con la cadena de prioridad **GnuTLS** para **imtcp** que permite un control detallado de la codificación no es completa. En consecuencia, las siguientes cadenas de prioridad no funcionan correctamente en **rsyslog**:

```
NINGUNO: VERS-ALL:-VERS-TLS1.3: MAC-ALL: DHE-RSA: AES-256-GCM: SIGN-RSA-SHA384: COMP-ALL: GROUP-ALL
```

Para evitar este problema, utilice sólo cadenas de prioridad que funcionen correctamente:

```
NINGUNO: VERS-ALL:-VERS-TLS1.3: MAC-ALL: ECDHE-RSA: AES-128-CBC: SIGN-RSA-SHA1: COMP-ALL: GROUP-ALL
```

En consecuencia, las configuraciones actuales deben limitarse a las cadenas que funcionan correctamente.

(BZ#1679512)

laspolíticas criptográficas permiten incorrectamente los cifrados de Camellia

Las políticas criptográficas de todo el sistema de RHEL 8 deberían deshabilitar los cifrados de Camellia en todos los niveles de políticas, como se indica en la documentación del producto. Sin embargo, el protocolo Kerberos habilita los cifrados por defecto.

Para solucionar el problema, aplique la subpolítica **NO-CAMELLIA**:

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

En el comando anterior, sustituya **DEFAULT** por el nombre del nivel criptográfico si ha cambiado de **DEFAULT** previamente.

Como resultado, los cifrados de Camellia están correctamente desautorizados en todas las aplicaciones que utilizan políticas de cifrado en todo el sistema sólo cuando los desactiva a través de la solución.(BZ#1919155)

6.5.5. Red

La utilidad iptables ahora solicita la carga del módulo para los comandos que actualizan una cadena independientemente de la bandera NLM_F_CREATE

Anteriormente, al establecer la política de una cadena, la utilidad **iptables-nft** generaba un mensaje **NEWCHAIN** pero no establecía la bandera **NLM_F_CREATE**. Como consecuencia, el kernel de RHEL 8

no cargaba ningún módulo y el comando de cadena de actualización resultante fallaba si los módulos del kernel asociados no se cargaban manualmente. Con esta actualización, la utilidad **iptables-nft** ahora solicita la carga de módulos para todos los comandos que actualizan una cadena y los usuarios pueden establecer la política de una cadena utilizando la utilidad **iptables-nft** sin cargar manualmente los módulos asociados.

(BZ#1812666)

El soporte para la actualización de los contadores de paquetes/bytes en el kernel se modificó incorrectamente entre RHEL 7 y RHEL 8

Cuando se hace referencia a un comando **ipset** con contadores habilitados desde una regla **iptables**, que especifica restricciones adicionales en las entradas **ipset** que coinciden, los contadores **ipset** se actualizan sólo si todas las restricciones adicionales coinciden. Esto también es problemático con las restricciones **--packets-gt** o **--bytes-gt**.

Como resultado, al migrar un conjunto de reglas **iptables** de RHEL 7 a RHEL 8, las reglas que implican búsquedas de **ipset** pueden dejar de funcionar y necesitan ser ajustadas. Para solucionar este problema, evite utilizar las opciones **--packets-gt** o **--bytes-gt** y sustitúyalas por las opciones **--packets-lt** o **--bytes-lt**.

(BZ#1806882)

La descarga de programas XDP falla en las tarjetas de red Netronome que utilizan el controlador nfp

El controlador **nfp** para las tarjetas de red Netronome contiene un error. Por lo tanto, la descarga de programas eXpress Data Path (XDP) falla si se utilizan dichas tarjetas y se carga el programa XDP utilizando la función **IFLA_XDP_EXPECTED_FD** con la bandera **XDP_FLAGS_REPLACE**. Por ejemplo, este fallo afecta a los programas XDP que se cargan utilizando la biblioteca **libxdp**. Actualmente, no hay ninguna solución disponible para este problema.

(BZ#1880268)

Anaconda no tiene acceso a la red cuando utiliza DHCP en la opción de arranque ip

El disco RAM inicial**(initrd**) utiliza NetworkManager para gestionar la red. El módulo **dracut** NetworkManager proporcionado por el archivo ISO de RHEL 8.3 asume incorrectamente que el primer campo de la opción **ip** en las opciones de arranque de Anaconda está siempre establecido. Como consecuencia, si utiliza DHCP y establece **ip=::::**

Tienes las siguientes opciones para solucionar el problema:

1. Establezca el primer campo de la **opción ip` como `.** (punto):

   ```
   ip=.::::
   ```

   Tenga en cuenta que esta solución no funcionará en futuras versiones de RHEL cuando el problema se haya solucionado.

2. Vuelva a crear el archivo **boot.iso** utilizando los últimos paquetes del repositorio de BaseOS que contienen una corrección del error: .

```
# lorax '--product=Red Hat Enterprise Linux' --version=8.3 --release=8.3 \
    --source=<URL_to_BaseOS_repository> \
    --source=<URL_to_AppStream_repository> \
    --nomacboot --buildarch=x86_64 '--volid=RHEL 8.3' <output_directory>
```

. Tenga en cuenta que Red Hat no admite archivos ISO creados por uno mismo.

Como resultado, RHEL recupera una dirección IP del servidor DHCP, y el acceso a la red está disponible en Anaconda.

(BZ#1902791)

6.5.6. Núcleo

Los sistemas con una gran cantidad de memoria persistente experimentan retrasos durante el proceso de arranque

Los sistemas con una gran cantidad de memoria persistente tardan mucho en arrancar porque la inicialización de la memoria se hace en serie. Por lo tanto, si hay sistemas de archivos de memoria persistente listados en el archivo **/etc/fstab**, el sistema puede perder el tiempo mientras espera que los dispositivos estén disponibles. Para solucionar este problema, configure la opción **DefaultTimeoutStartSec** en el archivo **/etc/systemd/system.conf** con un valor suficientemente grande.

(BZ#1666538)

El kernel devuelve falsos positivos en los sistemas IBM Z

En RHEL 8, los sistemas IBM Z carecen de una entrada en la lista blanca de la zona de memoria **ZONE_DMA** para permitir el acceso del usuario. En consecuencia, el kernel devuelve advertencias falsas positivas como:

```
...
Bad or missing usercopy whitelist? Kernel memory exposure attempt detected from SLUB object
'dma-kmalloc-192' (offset 0, size 144)!
WARNING: CPU: 0 PID: 8519 at mm/usercopy.c:83 usercopy_warn+0xac/0xd8
...
```

Las advertencias aparecen cuando se accede a cierta información del sistema a través de la interfaz **sysfs**. Por ejemplo, al ejecutar el script **debuginfo.sh**.

Para solucionar este problema, añada el parámetro **hardened_usercopy=off** a la línea de comandos del kernel.

Como resultado, no se muestra ningún mensaje de advertencia en el escenario descrito.

(BZ#1660290)

La espera ocupada del servicio rngd provoca un consumo total de la CPU en modo FIPS

Se ha añadido una nueva fuente de entropía del kernel para el modo FIPS para los kernels que comienzan con la versión 4.18.0-193.10. En consecuencia, cuando está en modo FIPS, el servicio **rngd** está ocupado esperando la llamada **al** sistema **poll()** para el dispositivo **/dev/random**, lo que provoca un consumo del 100% del tiempo de la CPU. Para solucionar este problema, detenga y desactive **rngd** ejecutando

```
# systemctl stop rngd
# systemctl disable rngd
```

Como resultado, **rngd** ya no ocupa las esperas de **poll()** en el escenario descrito.

(BZ#1884857)

Una captura de vmcore falla después de la operación de conexión o desconexión de la memoria

Después de realizar la operación de conexión o desconexión en caliente de la memoria, el evento se produce después de actualizar el árbol de dispositivos que contiene la información de la disposición de la memoria. De este modo, la utilidad **makedumpfile** intenta acceder a una dirección física inexistente. El problema aparece si se cumplen todas las condiciones siguientes:

- Una variante little-endian de IBM Power System ejecuta RHEL 8.
- El servicio **kdump** o **fadump** está activado en el sistema.

En consecuencia, el kernel de captura no guarda **el vmcore** si se produce un fallo del kernel después de la operación de conexión o desconexión en caliente de la memoria.

Para solucionar este problema, reinicie el servicio **kdump** después de conectar o desconectar en caliente:

```
# systemctl restart kdump.service
```

Como resultado, **vmcore** se guarda con éxito en el escenario descrito.

(BZ#1793389)

El uso de irqpoll provoca un fallo en la generación de vmcore

Debido a un problema existente con el controlador **nvme** en las arquitecturas ARM de 64 bits que se ejecutan en las plataformas en la nube de Amazon Web Services (AWS), la generación de **vmcore** falla cuando se proporciona el parámetro de línea de comandos del kernel **irqpoll** al primer kernel. En consecuencia, no se vuelca ningún archivo **vmcore** en el directorio **/var/crash/** después de un fallo del kernel. Para solucionar este problema:

1. Añade **irqpoll** a la clave **KDUMP_COMMANDLINE_REMOVE** en el archivo **/etc/sysconfig/kdump**.
2. Reinicie el servicio **kdump** ejecutando el comando **systemctl restart kdump**.

Como resultado, el primer kernel arranca correctamente y se espera que el archivo **vmcore** sea capturado al caer el kernel.

Tenga en cuenta que el servicio **kdump** puede utilizar una cantidad significativa de memoria del kernel de captura para volcar el archivo **vmcore**. Asegúrese de que el kernel de captura tiene suficiente memoria disponible para el servicio **kdump**.

(BZ#1654962)

El kernel de depuración no arranca en el entorno de captura de fallos en RHEL 8

Debido a la naturaleza de demanda de memoria del kernel de depuración, se produce un problema cuando el kernel de depuración está en uso y se desencadena un pánico del kernel. Como consecuencia, el kernel de depuración no es capaz de arrancar como el kernel de captura, y en su lugar se genera una traza de pila. Para solucionar este problema, aumente la memoria del kernel de captura en consecuencia. Como resultado, el kernel de depuración arranca con éxito en el entorno de captura de fallos.

(BZ#1659609)

zlib puede ralentizar una captura de vmcore en algunas funciones de compresión

El archivo de configuración de **kdump** utiliza el formato de compresión **lzo(makedumpfile -l**) por defecto. Cuando se modifica el archivo de configuración utilizando el formato de compresión **zlib**, (makedumpfile**-c**) es probable que traiga un mejor factor de compresión a costa de ralentizar el proceso de captura de **vmcore**. Como consecuencia, el **kdump** tarda hasta cuatro veces más en capturar un **vmcore** con **zlib**, en comparación con **lzo**.

Como resultado, Red Hat recomienda utilizar el **lzo** por defecto para los casos en los que la velocidad es el factor principal. Sin embargo, si la máquina de destino tiene poco espacio disponible, **zlib** es una mejor opción.

(BZ#1790635)

El NMI watchdog de HP no siempre genera un volcado de fallos

En ciertos casos, el controlador **hpwdt** para el vigilante NMI de HP no puede reclamar una interrupción no enmascarable (NMI) generada por el temporizador del vigilante HPE porque el NMI fue consumido por el controlador **perfmon**.

La falta de NMI se inicia por una de dos condiciones:

1. El botón **Generate NMI** en el software de gestión del servidor Integrated Lights-Out (iLO). Este botón es activado por un usuario.

2. El **hpwdt** watchdog. La expiración por defecto envía un NMI al servidor.

Ambas secuencias suelen ocurrir cuando el sistema no responde. En circunstancias normales, el manejador de NMI para ambas situaciones llama a la función **kernel panic()** y, si está configurado, el servicio **kdump** genera un archivo **vmcore**.

Sin embargo, debido a la falta de NMI, no se llama a **kernel panic()** y no se recoge **vmcore**.

En el primer caso (1.), si el sistema no responde, lo sigue haciendo. Para solucionar este escenario, utilice el botón virtual **Power** para reiniciar o apagar el servidor.

En el segundo caso (2.), el NMI que falta es seguido 9 segundos más tarde por un reinicio de la recuperación automática del sistema (ASR).

La línea de servidores HPE Gen9 experimenta este problema en porcentajes de un solo dígito. La Gen10 con una frecuencia aún menor.

(BZ#1602962)

El comando tuned-adm profile powersave hace que el sistema deje de responder

La ejecución del comando **tuned-adm profile powersave** conduce a un estado de falta de respuesta de los sistemas Penguin Valkyrie 2000 de 2 sockets con los procesadores Thunderx (CN88xx) más antiguos. En consecuencia, reinicie el sistema para que vuelva a funcionar. Para evitar este problema, evite utilizar el perfil **powersave** si su sistema cumple con las especificaciones mencionadas.

(BZ#1609288)

El valor predeterminado de 7 4 1 7 printk a veces provoca una falta de respuesta temporal del sistema

El valor predeterminado **7 4 1 7printk** permite una mejor depuración de la actividad del kernel. Sin embargo, cuando se combina con una consola en serie, este valor **printk** puede causar intensas ráfagas

de E/S que pueden hacer que un sistema RHEL deje de responder temporalmente. Para solucionar este problema, hemos añadido un nuevo perfil TuneD **optimize-serial-console**, que reduce el valor **printk** por defecto a **4 4 1 7**. Los usuarios pueden instrumentar su sistema de la siguiente manera:

```
# tuned-adm profile throughput-performance optimize-serial-console
```

Tener un valor de **printk** más bajo persistente a través de un reinicio reduce la probabilidad de cuelgues del sistema.

Tenga en cuenta que este cambio de configuración se produce a costa de perder la información de depuración adicional.

Para más información sobre la nueva función, consulte Un nuevo perfil TuneD **de optimización de consolas serie** para reducir la E/S en las consolas serie reduciendo el valor de **printk** .

(JIRA:RHELPLAN-28940)

El controlador ACPI del kernel informa que no tiene acceso a una región de memoria PCIe ECAM

La tabla de la interfaz de configuración avanzada y alimentación (ACPI) proporcionada por el firmware no define una región de memoria en el bus PCI en el método de configuración de recursos actuales (_CRS) para el dispositivo de bus PCI. En consecuencia, se produce el siguiente mensaje de advertencia durante el arranque del sistema:

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not
reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

Sin embargo, el kernel sigue siendo capaz de acceder a la región de memoria **0x30000000-0x31ffff**, y puede asignar esa región de memoria al Mecanismo de Acceso a la Configuración Mejorada (ECAM) de PCI correctamente. Puedes verificar que PCI ECAM funciona correctamente accediendo al espacio de configuración PCIe sobre el offset de 256 bytes con la siguiente salida:

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-
if 02 [NVM Express])
 ...
        Capabilities: [900 v1] L1 PM Substates
                L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
                        PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
                L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
                        T_CommonMode=0us LTR1.2_Threshold=0ns
                L1SubCtl2: T_PwrOn=10us
```

Por lo tanto, puede ignorar el mensaje de advertencia.

Para más información sobre el problema, consulte la solución "Firmware Bug: ECAM area **mem 0x30000000-0x31ffffff** not reserved in ACPI namespace" que aparece durante el arranque del sistema.

(BZ#1868526)

El controlador cxgb4 provoca un fallo en el kernel kdump

El kernel **kdump** se bloquea al intentar guardar información en el archivo **vmcore**. En consecuencia, el controlador **cxgb4** impide que el **kdump** kernel guarde un núcleo para su posterior análisis. Para solucionar este problema, añada el parámetro **novmcoredd** a la línea de comandos de kdump kernel

para permitir guardar archivos de núcleo.

(BZ#1708456)

La biblioteca OPEN MPI puede provocar fallos en tiempo de ejecución con la PML por defecto

En la implementación de OPEN Message Passing Interface (OPEN MPI) de la serie 4.0.x, Unified Communication X (UCX) es el comunicador punto a punto (PML) por defecto. Las versiones posteriores de OPEN MPI de la serie 4.0.x obviaron **openib** Byte Transfer Layer (BTL).

Sin embargo, OPEN MPI, cuando se ejecuta sobre un cluster **homogeneous** (misma configuración de hardware y software), UCX sigue utilizando **openib** BTL para las operaciones MPI unilaterales. Como consecuencia, esto puede provocar errores de ejecución. Para solucionar este problema:

- Ejecute el comando **mpirun** con los siguientes parámetros:

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

donde,

- El parámetro **-mca btl openib** desactiva **openib** BTL
- El parámetro **-mca pml ucx** configura OPEN MPI para utilizar **ucx** PML.
- El parámetro **x UCX_NET_DEVICES=** restringe a UCX el uso de los dispositivos especificados

El OPEN MPI, cuando se ejecuta sobre un cluster **heterogeneous** (diferente configuración de hardware y software), utiliza UCX como PML por defecto. Como consecuencia, esto puede provocar que los trabajos de OPEN MPI se ejecuten con un rendimiento errático, un comportamiento poco receptivo o fallos en la ejecución. Para solucionar este problema, configure la prioridad de UCX como

- Ejecute el comando **mpirun** con los siguientes parámetros:

```
-mca pml_ucx_priority 5
```

Como resultado, la biblioteca OPEN MPI es capaz de elegir una capa de transporte alternativa disponible sobre UCX.

(BZ#1866402)

6.5.7. Sistemas de archivos y almacenamiento

El sistema de archivos /**boot** no puede colocarse en LVM

No se puede colocar el sistema de archivos /**boot** en un volumen lógico LVM. Esta limitación existe por las siguientes razones:

- En los sistemas EFI, el *EFI System Partition* sirve convencionalmente como sistema de archivos /**boot**. El estándar uEFI requiere un tipo de partición GPT específico y un tipo de sistema de archivos específico para esta partición.
- RHEL 8 utiliza *Boot Loader Specification* (BLS) para las entradas de arranque del sistema. Esta especificación requiere que el sistema de archivos /**boot** sea legible por el firmware de la plataforma. En los sistemas EFI, el firmware de la plataforma solo puede leer la configuración de /**boot** definida por el estándar uEFI.

- El soporte para volúmenes lógicos LVM en el gestor de arranque GRUB 2 es incompleto. Red Hat no planea mejorar el soporte porque el número de casos de uso para la función está disminuyendo debido a estándares como uEFI y BLS.

Red Hat no planea soportar /**boot** en LVM. En su lugar, Red Hat proporciona herramientas para gestionar las instantáneas del sistema y la reversión que no necesitan que el sistema de archivos /**boot** se coloque en un volumen lógico LVM.

(BZ#1496229)

LVM ya no permite crear grupos de volúmenes con tamaños de bloque mixtos

Las utilidades de LVM como **vgcreate** o **vgextend** ya no permiten crear grupos de volúmenes (VG) en los que los volúmenes físicos (PV) tienen diferentes tamaños de bloque lógicos. LVM ha adoptado este cambio porque los sistemas de archivos no se pueden montar si se extiende el volumen lógico (LV) subyacente con un PV de un tamaño de bloque diferente.

Para volver a habilitar la creación de VGs con tamaños de bloque mixtos, establezca la opción **allow_mixed_block_sizes=1** en el archivo **lvm.conf**.

(BZ#1768536)

Limitaciones de la caché de escriturade LVM

El método de almacenamiento en caché **de** LVM tiene las siguientes limitaciones, que no están presentes en el método de **caché**:

- No se puede nombrar un volumen lógico **con caché de escritura** cuando se utilizan comandos **pvmove**.
- No se pueden utilizar volúmenes lógicos con **writecache** en combinación con thin pools o VDO.

La siguiente limitación también se aplica al método de **la caché**:

- No se puede redimensionar un volumen lógico mientras **la caché** o la **caché de escritura** están conectadas a él.

(JIRA:RHELPLAN-27987, BZ#1798631, BZ#1808012)

Los dispositivos de espejo LVM que almacenan un volumen LUKS a veces no responden

Los dispositivos LVM en espejo con un tipo de segmento en **espejo** que almacenan un volumen LUKS pueden dejar de responder bajo ciertas condiciones. Los dispositivos que no responden rechazan todas las operaciones de E/S.

Para solucionar el problema, Red Hat recomienda que utilice dispositivos RAID 1 de LVM con un tipo de segmento **raid1** en lugar de **espejo** si necesita apilar volúmenes LUKS sobre el almacenamiento resistente definido por software.

El tipo de segmento **raid1** es el tipo de configuración RAID por defecto y sustituye **al espejo** como solución recomendada.

Para convertir los dispositivos **espejo** en **raid**, consulte Convertir un dispositivo LVM espejo en un dispositivo RAID1.

(BZ#1730502)

Un parche de NFS 4.0 puede reducir el rendimiento con una carga de trabajo abierta

Anteriormente, se corrigió un error que, en algunos casos, podía hacer que una operación de apertura de NFS pasara por alto el hecho de que un archivo había sido eliminado o renombrado en el servidor. Sin embargo, la corrección puede causar un rendimiento más lento con cargas de trabajo que requieren muchas operaciones abiertas. Para solucionar este problema, puede ser útil utilizar la versión 4.1 o superior de NFS, que ha sido mejorada para conceder delegaciones a los clientes en más casos, permitiendo a los clientes realizar operaciones de apertura de forma local, rápida y segura.

(BZ#1748451)

6.5.8. Lenguajes de programación dinámicos, servidores web y de bases de datos

getpwnam() podría fallar cuando es llamado por una aplicación de 32 bits

Cuando un usuario de NIS utiliza una aplicación de 32 bits que llama a la función **getpwnam()**, la llamada falla si falta el paquete **nss_nis.** i686. Para solucionar este problema, instale manualmente el paquete que falta mediante el comando **yum install nss_nis.i686**.

(BZ#1803161)

Los conflictos de símbolos entre las librerías de OpenLDAP podrían provocar fallos en httpd

Cuando las bibliotecas **libldap** y **libldap_r** proporcionadas por OpenLDAP se cargan y utilizan dentro de un mismo proceso, pueden producirse conflictos de símbolos entre estas bibliotecas. En consecuencia, los procesos hijo de Apache **httpd** que utilizan la extensión PHP **ldap** podrían terminar inesperadamente si los módulos **mod_security** o **mod_auth_openidc** también son cargados por la configuración de **httpd**.

Con esta actualización de la biblioteca Apache Portable Runtime (APR), se puede solucionar el problema estableciendo la variable de entorno **APR_DEEPBIND**, que habilita el uso de la opción del enlazador dinámico **RTLD_DEEPBIND** cuando se cargan los módulos **httpd**. Cuando la variable de entorno **APR_DEEPBIND** está activada, ya no se producen fallos en las configuraciones de **httpd** que cargan bibliotecas conflictivas.

(BZ#1819607)

6.5.9. Gestión de la identidad

La instalación de KRA falla si todos los miembros de KRA son réplicas ocultas

La utilidad **ipa-kra-install** falla en un cluster donde la Autoridad de Recuperación de Claves (KRA) ya está presente, si la primera instancia de KRA está instalada en una réplica oculta. En consecuencia, no se pueden añadir más instancias de KRA al clúster.

Para solucionar este problema, desoculte la réplica oculta que tiene el rol de KRA antes de añadir nuevas instancias de KRA. Puede volver a ocultarla cuando **ipa-kra-install** se complete con éxito.

(BZ#1816784)

El uso de la utilidad cert-fix con la opción --agent-uid pkidbuser rompe el sistema de certificados

El uso de la utilidad **cert-fix** con la opción **--agent-uid pkidbuser** corrompe la configuración LDAP de Certificate System. Como consecuencia, el sistema de certificados puede volverse inestable y es necesario tomar medidas manuales para recuperar el sistema.

(BZ#1729215)

Los certificados emitidos por PKI ACME Responder conectados a PKI CA pueden fallar la validación de OCSP

El perfil de certificado ACME por defecto proporcionado por PKI CA contiene una URL OCSP de muestra que no apunta a un servicio OCSP real. Como consecuencia, si PKI ACME Responder está configurado para utilizar un emisor de PKI CA, los certificados emitidos por el respondedor pueden fallar la validación de OCSP.

Para solucionar este problema, debe establecer la propiedad **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0** con un valor en blanco en el archivo de configuración **/usr/share/pki/ca/profiles/ca/acmeServerCert.cfg**:

1. En el archivo de configuración de ACME Responder, cambie la línea policyset. **serverCertSet .5.default.params. authInfoAccessADLocation_0=http://ocsp.example.com** por **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=**.

2. Reinicie el servicio y regenere el certificado.

Como resultado, PKI CA generará certificados ACME con una URL OCSP autogenerada que apunta a un servicio OCSP real.

(BZ#1868233)

FreeRADIUS trunca silenciosamente las contraseñas de túnel de más de 249 caracteres

Si una contraseña de túnel tiene más de 249 caracteres, el servicio FreeRADIUS la trunca silenciosamente. Esto puede dar lugar a incompatibilidades inesperadas de la contraseña con otros sistemas.

Para solucionar el problema, elige una contraseña de 249 caracteres o menos.

(BZ#1723362)

6.5.10. Escritorio

No es posible desactivar los repositorios **flatpak** desde los repositorios de software

Actualmente, no es posible desactivar o eliminar los repositorios **flatpak** en la herramienta de Repositorios de Software en la utilidad de Software de GNOME.

(BZ#1668760)

Arrastrar y soltar no funciona entre el escritorio y las aplicaciones

Debido a un error en el paquete **gnome-shell-extensions**, la funcionalidad de arrastrar y soltar no funciona actualmente entre el escritorio y las aplicaciones. El soporte para esta función se añadirá de nuevo en una futura versión.

(BZ#1717947)

Las máquinas virtuales RHEL 8 de segunda generación a veces no arrancan en hosts Hyper-V Server 2016

Cuando se utiliza RHEL 8 como sistema operativo invitado en una máquina virtual (VM) que se ejecuta en un host Microsoft Hyper-V Server 2016, la VM en algunos casos no arranca y vuelve al menú de arranque GRUB. Además, se registra el siguiente error en el registro de eventos de Hyper-V:

> El sistema operativo invitado informó que falló con el siguiente código de error: 0x1E

-

Este error se produce debido a un error de firmware UEFI en el host de Hyper-V. Para solucionar este problema, utilice Hyper-V Server 2019 como host.

(BZ#1583445)

6.5.11. Infraestructuras gráficas

radeon no reinicia el hardware correctamente

El controlador del kernel **de** radeon actualmente no restablece el hardware en el contexto kexec correctamente. En su lugar, **radeon** se cae, lo que hace que el resto del servicio **kdump** falle.

Para solucionar este problema, desactive **radeon** en **kdump** añadiendo la siguiente línea al archivo **/etc/kdump.conf**:

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

Reinicie la máquina y **kdump**. Después de iniciar **kdump**, la línea **force_rebuild 1** puede ser eliminada del archivo de configuración.

Tenga en cuenta que en este escenario, no habrá gráficos disponibles durante **kdump**, pero **kdump** funcionará con éxito.

(BZ#1694705)

Varias pantallas HDR en una misma topología MST pueden no encenderse

En los sistemas que utilizan GPUs NVIDIA Turing con el controlador **nouveau**, el uso de un concentrador **DisplayPort** (como un dock de portátil) con varios monitores que soportan HDR conectados a él puede provocar un fallo en el encendido. Esto se debe a que el sistema piensa erróneamente que no hay suficiente ancho de banda en el concentrador para soportar todas las pantallas.

(BZ#1812577)

No se pueden ejecutar aplicaciones gráficas con el comando sudo

Al intentar ejecutar aplicaciones gráficas como un usuario con privilegios elevados, la aplicación falla al abrirse con un mensaje de error. El fallo se produce porque **Xwayland** está restringido por el archivo **Xauthority** a utilizar credenciales de usuario normales para la autenticación.

Para solucionar este problema, utilice el comando **sudo -E** para ejecutar las aplicaciones gráficas como usuario **root**.

(BZ#1673073)

VNC Viewer muestra colores incorrectos con la profundidad de color de 16 bits en IBM Z

La aplicación VNC Viewer muestra colores incorrectos cuando se conecta a una sesión VNC en un servidor IBM Z con la profundidad de color de 16 bits.

Para solucionar el problema, configure la profundidad de color de 24 bits en el servidor VNC. Con el servidor **Xvnc**, sustituya la opción **-depth 16** por **-depth 24** en la configuración de **Xvnc**.

Como resultado, los clientes VNC muestran los colores correctos pero utilizan más ancho de banda de la red con el servidor.

(BZ#1886147)

La aceleración por hardware no es compatible con ARM

Los controladores gráficos integrados no son compatibles con la aceleración por hardware ni con la API Vulkan en la arquitectura ARM de 64 bits.

Para activar la aceleración por hardware o Vulkan en ARM, instale el controlador propietario de Nvidia.

(JIRA:RHELPLAN-57914)

6.5.12. La consola web

Los usuarios sin privilegios pueden acceder a la página de suscripciones

Si una persona que no es administrador navega a la página **Subscriptions** de la consola web, la consola web muestra un mensaje de error genérico **Cockpit tuvo un error interno inesperado**.

Para solucionar este problema, inicie sesión en la consola web con un usuario con privilegios y asegúrese de marcar la casilla **Reuse my password for privileged tasks**

(BZ#1674337)

6.5.13. Roles del sistema Red Hat Enterprise Linux

la entrada de**oVirt** y las funcionalidades de salida de **elasticsearch** no son compatibles con el registro de roles del sistema

La entrada de **oVirt** y la salida de **elasticsearch** no están soportadas en System Roles Logging aunque se mencionan en el archivo README. No hay ninguna solución disponible por el momento.

(BZ#1889468)

6.5.14. Virtualización

La visualización de múltiples monitores de máquinas virtuales que utilizan Wayland no es posible con QXL

El uso de la utilidad **remote-viewer** para mostrar más de un monitor de una máquina virtual (VM) que está utilizando el servidor de visualización Wayland hace que la VM no responda y que se muestre indefinidamente el mensaje de estado *Waiting for display*.

Para solucionar este problema, utilice **virtio-gpu** en lugar de **qxl** como dispositivo GPU para las máquinas virtuales que utilizan Wayland.

(BZ#1642887)

los comandos**virsh iface-*** no funcionan consistentemente

Actualmente, los comandos **virsh** iface-*, como **virsh iface-start** y **virsh iface-destroy**, fallan frecuentemente debido a las dependencias de configuración. Por lo tanto, se recomienda no utilizar los comandos virsh **iface-*** para configurar y gestionar las conexiones de red del host. En su lugar, utilice el programa NetworkManager y sus aplicaciones de gestión relacionadas.

(BZ#1664592)

Las máquinas virtuales a veces no se inician cuando se utilizan muchos discos virtio-blk

Añadir un gran número de dispositivos virtio-blk a una máquina virtual (VM) puede agotar el número de vectores de interrupción disponibles en la plataforma. Si esto ocurre, el SO invitado de la VM falla al arrancar, y muestra un **dracut-initqueue[392]: Advertencia:** Error de **no** poder arrancar.

(BZ#1719687)

Adjuntar dispositivos LUN a máquinas virtuales usando virtio-blk no funciona

El tipo de máquina q35 no es compatible con los dispositivos virtio 1.0 de transición, por lo que RHEL 8 carece de soporte para las características que quedaron obsoletas en virtio 1.0. En particular, no es posible en un host RHEL 8 enviar comandos SCSI desde dispositivos virtio-blk. Como consecuencia, adjuntar un disco físico como dispositivo LUN a una máquina virtual falla cuando se utiliza el controlador virtio-blk.

Tenga en cuenta que los discos físicos pueden seguir pasando por el sistema operativo invitado, pero deben ser configurados con la opción **device='disk'** en lugar de **device='lun'**.

(BZ#1777138)

Las máquinas virtuales que utilizan Cooperlake no pueden arrancar cuando TSX está desactivado en el host

Las máquinas virtuales (VM) que utilizan el modelo de CPU **Cooperlake** actualmente no arrancan cuando el indicador de CPU **TSX** está deshabilitado en el host. En su lugar, el host muestra el siguiente mensaje de error:

```
la CPU es incompatible con la CPU del host: La CPU anfitriona no proporciona las características requeridas: hle, rtm
```

Para que las máquinas virtuales con **Cooperlake** se puedan utilizar en dicho host, desactive los indicadores HLE, RTM y TAA_NO en la configuración de la máquina virtual en la configuración XML de la máquina virtual:

```
<feature policy='disable' name='hle'/>
<feature policy='disable' name='rtm'/>
<feature policy='disable' name='taa-no'/>
```

(BZ#1860743)

Las máquinas virtuales a veces no pueden arrancar en los hosts Witherspoon

Las máquinas virtuales (VMs) que utilizan el tipo de máquina **pseries-rhel7.6.0-sxxm** en algunos casos fallan al arrancar en los hosts *Power9 S922LC for HPC* (también conocidos como Witherspoon) que utilizan la CPU DD2.2 o DD2.3.

Al intentar arrancar una máquina virtual de este tipo, se genera el siguiente mensaje de error:

```
qemu-kvm: El nivel de capacidad de bifurcación indirecta solicitada no está soportado por kvm
```

Para solucionar este problema, configure la configuración XML de la máquina virtual de la siguiente manera:

```
<domain type='qemu' xmlns:qemu='http://libvirt.org/schemas/domain/qemu/1.0'>
  <qemu:commandline>
    <qemu:arg value='-machine'/>
```

```
  <qemu:arg value='cap-ibs=workaround'/>
</qemu:commandline>
```

(BZ#1732726)

6.5.15. RHEL en entornos de nube

Problemas con la GPU en las instancias Azure NV6

Cuando se ejecuta RHEL 8 como sistema operativo invitado en una instancia de Microsoft Azure NV6, reanudar la máquina virtual (VM) desde la hibernación a veces hace que la GPU de la VM funcione incorrectamente. Cuando esto ocurre, el kernel registra el siguiente mensaje:

```
hv_irq_unmask() falló: 0x5
```

(BZ#1846838)

kdump a veces no se inicia en Azure y Hyper-V

En los sistemas operativos invitados de RHEL 8 alojados en los hipervisores de Microsoft Azure o Hyper-V, el inicio del kernel **kdump** en algunos casos falla cuando los notificadores post-ejecución están habilitados.

Para solucionar este problema, deshabilite los notificadores de correo de crash kexec:

```
# echo N
```

(BZ#1865745)

La configuración de la IP estática en una máquina virtual RHEL 8 en un host VMWare no funciona

Actualmente, cuando se utiliza RHEL 8 como sistema operativo invitado de una máquina virtual (VM) en un host VMWare, la función DatasourceOVF no funciona correctamente. Como consecuencia, si utiliza la utilidad **cloud-init** para establecer la red de la VM en IP estática y luego reinicia la VM, la red de la VM cambiará a DHCP.

(BZ#1750862)

El volcado del núcleo de las máquinas virtuales RHEL 8 con ciertas NICs a una máquina remota en Azure tarda más de lo esperado

Actualmente, el uso de la utilidad **kdump** para guardar el archivo de volcado del núcleo de una máquina virtual (VM) RHEL 8 en un hipervisor de Microsoft Azure en una máquina remota no funciona correctamente cuando la VM está utilizando una NIC con la red acelerada habilitada. Como consecuencia, el archivo de volcado se guarda después de aproximadamente 200 segundos, en lugar de inmediatamente. Además, el siguiente mensaje de error se registra en la consola antes de que se guarde el archivo de volcado.

```
dispositivo (eth0): linklocal6: DAD falló para una dirección EUI-64
```

(BZ#1854037)

Los contadores de paquetes TX/RX no aumentan después de que las máquinas virtuales se reanuden desde la hibernación

Los contadores de paquetes **TX**/**RX** dejan de aumentar cuando una máquina virtual (VM) RHEL 8, con una NIC CX4 VF, se reanuda desde la hibernación en Microsoft Azure. Para que los contadores sigan funcionando, reinicie la VM. Tenga en cuenta que, al hacerlo, se reiniciarán los contadores.

(BZ#1876527)

Las máquinas virtuales de RHEL 8 no se reanudan desde la hibernación en Azure

El GUID de la función virtual (VF), **dispositivo vmbus**, cambia cuando una máquina virtual (VM) RHEL 8, con **SR-IOV** habilitado, se hiberna y se desasigna en Microsoft Azure . Como resultado, cuando la VM se reinicia, no se reanuda y se bloquea. Como solución, reinicie la VM utilizando la consola de serie de Azure.

(BZ#1876519)

La migración de un huésped POWER9 de un host RHEL 7-ALT a RHEL 8 falla

Actualmente, la migración de una máquina virtual POWER9 desde un sistema anfitrión RHEL 7-ALT a RHEL 8 no responde con un estado "Estado de la migración: activo".

Para solucionar este problema, desactive Transparent Huge Pages (THP) en el host RHEL 7-ALT, lo que permite que la migración se complete con éxito.

(BZ#1741436)

6.5.16. Soporte

redhat-support-tool no funciona con la política criptográfica **FUTURE**

Dado que una clave criptográfica utilizada por un certificado en la API del Portal del Cliente no cumple los requisitos de la política criptográfica de todo el sistema **FUTURE**, la utilidad **redhat-support-tool** no funciona con este nivel de política por el momento.

Para solucionar este problema, utilice la política criptográfica **DEFAULT** al conectarse a la API del Portal del Cliente.

(BZ#1802026)

6.5.17. Contenedores

No se espera que UDICA funcione con la corriente estable 1.0

UDICA, la herramienta para generar políticas SELinux para contenedores, no se espera que funcione con contenedores que se ejecutan a través de podman 1.0.x en el flujo de módulos **container-tools:1.0**.

(JIRA:RHELPLAN-25571)

podman system connection add no establece automáticamente la conexión por defecto

El comando podman system **connection add** no establece automáticamente que la primera conexión sea la conexión por defecto. Para establecer la conexión por defecto, debe ejecutar manualmente el comando **podman system connection default**

(BZ#1881894)

6.6. INTERNACIONALIZACIÓN

6.6.1. Idiomas internacionales de Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 admite la instalación de varios idiomas y el cambio de idiomas en función de sus necesidades.

- Lenguas de Asia oriental: japonés, coreano, chino simplificado y chino tradicional.
- Idiomas europeos: inglés, alemán, español, francés, italiano, portugués y ruso.

La siguiente tabla enumera los tipos de letra y los métodos de entrada proporcionados para varios idiomas principales.

Idioma	Fuente por defecto (paquete de fuentes)	Métodos de entrada
Inglés	dejavu-sans-fonts	
Francés	dejavu-sans-fonts	
Alemán	dejavu-sans-fonts	
Italiano	dejavu-sans-fonts	
Ruso	dejavu-sans-fonts	
Español	dejavu-sans-fonts	
Portugués	dejavu-sans-fonts	
Chino simplificado	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
Chino tradicional	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
Japonés	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
Coreano	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-hangul, libhangul

6.6.2. Cambios notables en la internacionalización en RHEL 8

RHEL 8 introduce los siguientes cambios en la internacionalización en comparación con RHEL 7:

- Se ha añadido la compatibilidad con el estándar informático **Unicode 11**.
- La internacionalización se distribuye en múltiples paquetes, lo que permite realizar instalaciones de menor tamaño. Para más información, consulte Uso de paquetes de idiomas .

- Varias localizaciones de **glibc** se han sincronizado con Unicode Common Locale Data Repository (CLDR).

APÉNDICE A. LISTA DE ENTRADAS POR COMPONENTE

Los IDs de Bugzilla y JIRA aparecen en este documento como referencia. Los errores de Bugzilla que son de acceso público incluyen un enlace al ticket.

Componente	Entradas
389-ds-base	BZ#1816862, BZ#1638875, BZ#1728943
NetworkManager	BZ#1814746, BZ#1626348
anaconda	BZ#1665428, BZ#1775975, BZ#1630299, BZ#1823578, BZ#1672405, BZ#1644662, BZ#1745064, BZ#1821192, BZ#1822880, BZ#1862116, BZ#1890261, BZ#1891827,BZ#1691319
apr	BZ#1819607
authselect	BZ#1654018
bcc	BZ#1837906
bind	BZ#1818785
buildah-container	BZ#1627898
buildah	BZ#1806044
horquilla	BZ#1716040, BZ#1818780, BZ#1436735, BZ#1819767
cloud-init	BZ#1750862
cloud-utils-growpart	BZ#1846246
sesión de cabina-grabación	BZ#1826516
cabina de mando	BZ#1710731, BZ#1666722
corosync-qdevice	BZ#1784200
crun	BZ#1841438
cripto-políticas	BZ#1832743, BZ#1660839
cyrus-sasl	BZ#1817054
distribución	BZ#1815402, BZ#1657927

Componente	Entradas
dnf	BZ#1793298, BZ#1832869, BZ#1842285
elfutils	BZ#1804321
fapolicyd	BZ#1897090, BZ#1817413, BZ#1714529
agentes de vallas	BZ#1830776, BZ#1775847
firewalld	BZ#1790948, BZ#1682913, BZ#1809225, BZ#1817205, BZ#1809636
freeradius	BZ#1672285, BZ#1859527, BZ#1723362
gcc-toolset-10-gdb	BZ#1838777
gcc	BZ#1784758
gdb	BZ#1659535
git	BZ#1825114
glibc	BZ#1812756, BZ#1743445, BZ#1783303, BZ#1642150, BZ#1810146, BZ#1748197, BZ#1774115, BZ#1807824, BZ#1757354, BZ#1836867, BZ#1780204, BZ#1821531, BZ#1784525
gnome-session	BZ#1739556
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1677754, BZ#1789392, BZ#1849079, BZ#1855803
go-toolset	BZ#1820596
gpgme	BZ#1829822
grafana-container	BZ#1823834
grafana-pcp	BZ#1807099

Componente	Entradas
grafana	BZ#1807323
grub2	BZ#1583445
httpd	BZ#1209162
configuración inicial	BZ#1676439
ipa-healthcheck	BZ#1852244
ipa	BZ#1816784, BZ#1810154, BZ#913799, BZ#1651577, BZ#1851139, BZ#1664719, BZ#1664718
iperf3	BZ#1665142, BZ#1700497
jss	BZ#1821851
kernel-rt	BZ#1818138
núcleo	BZ#1758323, BZ#1812666, BZ#1793389, BZ#1694705, BZ#1748451, BZ#1654962, BZ#1792125, BZ#1708456, BZ#1812577, BZ#1757933, BZ#1847837, BZ#1791664, BZ#1666538, BZ#1602962, BZ#1609288, BZ#1730502, BZ#1806882, BZ#1660290, BZ#1846838, BZ#1865745, BZ#1868526, BZ#1884857, BZ#1854037, BZ#1876527, BZ#1876519, BZ#1823764, BZ#1822085, BZ#1735611, BZ#1281843, BZ#1828642, BZ#1825414, BZ#1761928, BZ#1791041, BZ#1796565, BZ#1834769, BZ#1785660, BZ#1683394, BZ#1817752, BZ#1782831, BZ#1821646, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1570255, BZ#1696451, BZ#1348508, BZ#1778762, BZ#1839311, BZ#1783396, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610
krb5	BZ#1791062, BZ#1784655, BZ#1820311, BZ#1802334, BZ#1877991
libbpf	BZ#1759154
libcap	BZ#1487388
libdb	BZ#1670768
libffi	BZ#1723951

Componente	Entradas
libgnome-keyring	BZ#1607766
libkcapi	BZ#1683123
libmaxminddb	BZ#1642001
libpcap	BZ#1806422
libreswan	BZ#1544463, BZ#1820206
libseccomp	BZ#1770693
módulo libselinux-python-2.8	BZ#1666328
libssh	BZ#1804797
libvirt	BZ#1664592, BZ#1528684
lldb	BZ#1841073
llvm-toolset	BZ#1820587
llvm	BZ#1820319
lshw	BZ#1794049
lvm2	BZ#1496229, BZ#1768536, BZ#1598199, BZ#1541165, JIRA:RHELPLAN-39320
memcached	BZ#1809536
mesa	BZ#1886147
microdnf	BZ#1781126
mod_http2	BZ#1814236
nfs-utils	BZ#1817756, BZ#1592011
nginx	BZ#1668717, BZ#1826632
nmstate	BZ#1674456

Componente	Entradas
nss_nis	BZ#1803161
nss	BZ#1817533, BZ#1645153
opencryptoki	BZ#1780293
openmpi	BZ#1866402
opensc	BZ#1810660
openscap	BZ#1803116, BZ#1870087, BZ#1795563, BZ#1824152, BZ#1829761
openssh	BZ#1744108
openssl	BZ#1685470, BZ#1810911
oscap-anaconda-addon	BZ#1816199, BZ#1665082, BZ#1674001, BZ#1691305, BZ#1787156, BZ#1843932, BZ#1834716
marcapasos	BZ#1828488, BZ#1784601, BZ#1837747, BZ#1718324
papi	BZ#1807346, BZ#1664056, BZ#1726070
contenedor pcp	BZ#1497296
pcp	BZ#1792971
pcs	BZ#1817547, BZ#1684676, BZ#1839637, BZ#1619620
módulo perl-5.30	BZ#1713592
perl-IO-Socket-SSL	BZ#1824222
perl-libwww-perl	BZ#1781177
php	BZ#1797661
pki-core	BZ#1729215, BZ#1868233, BZ#1770322, BZ#1824948
podman	BZ#1804193, BZ#1881894, BZ#1627899

Componente	Entradas
powertop	BZ#1783110
pykickstart	BZ#1637872
pitón38	BZ#1847416
qemu-kvm	BZ#1719687, BZ#1860743, JIRA:RHELPLAN-45901, BZ#1651994
trasera	BZ#1843809, BZ#1729502, BZ#1743303
redhat-support-tool	BZ#1802026
recursos-agentes	BZ#1814896
rhel-system-roles-sap	BZ#1844190, BZ#1660832
rhel-system-roles	BZ#1889468, BZ#1822158, BZ#1677739
rpm	BZ#1688849
rsyslog	BZ#1659383, JIRA:RHELPLAN-10431, BZ#1679512, BZ#1713427
módulo ruby-2.7	BZ#1817135
rubí	BZ#1846113
herrumbre-herramienta	BZ#1820593
samba	BZ#1817557, JIRA:RHELPLAN-13195
scap-guía de seguridad	BZ#1843913, BZ#1858866, BZ#1750755, BZ#1760734, BZ#1832760, BZ#1815007
scap-workbench	BZ#1640715
selinux-policy	BZ#1826788, BZ#1746398, BZ#1776873, BZ#1772852, BZ#1641631, BZ#1860443
setools	BZ#1820079
skopeo-contenedor	BZ#1627900
smartmontools	BZ#1671154

Componente	Entradas
especias	BZ#1849563
calamar	BZ#1829467
sssd	BZ#1827615, BZ#1793727
stratis-cli	BZ#1734496
aturdimiento	BZ#1808365
gestor de suscripciones	BZ#1674337
sudo	BZ#1786990
systemtap	BZ#1804319
tang	BZ#1716039
tcpdump	BZ#1804063
tigervnc	BZ#1806992
tpm2-tools	BZ#1789682
afinado	BZ#1792264, BZ#1840689, BZ#1746957
udica	BZ#1763210
usbguard	BZ#1738590, BZ#1667395, BZ#1683567
valgrind	BZ#1804324
wayland	BZ#1673073
xdp-tools	BZ#1880268, BZ#1820670
xorg-x11-drv-qxl	BZ#1642887
servidor xorg-x11	BZ#1698565
yum	BZ#1788154

Componente	Entradas
otros	JIRA:RHELPLAN-45950, JIRA:RHELPLAN-57572, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1790635, BZ#1823398, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1897383, BZ#1900019, BZ#1839151, BZ#1780124, JIRA:RHELPLAN-42395, BZ#1889736, BZ#1842656, JIRA:RHELPLAN-45959, JIRA:RHELPLAN-45958, JIRA:RHELPLAN-45957, JIRA:RHELPLAN-45956, JIRA:RHELPLAN-45952, JIRA:RHELPLAN-45945, JIRA:RHELPLAN-45939, JIRA:RHELPLAN-45937, JIRA:RHELPLAN-45936, JIRA:RHELPLAN-45930, JIRA:RHELPLAN-45926, JIRA:RHELPLAN-45922, JIRA:RHELPLAN-45920, JIRA:RHELPLAN-45918, JIRA:RHELPLAN-45916, JIRA:RHELPLAN-45915, JIRA:RHELPLAN-45911, JIRA:RHELPLAN-45910, JIRA:RHELPLAN-45909, JIRA:RHELPLAN-45908, JIRA:RHELPLAN-45906, JIRA:RHELPLAN-45904, JIRA:RHELPLAN-45900, JIRA:RHELPLAN-45899, JIRA:RHELPLAN-45884, JIRA:RHELPLAN-37573, JIRA:RHELPLAN-37570, JIRA:RHELPLAN-49954, JIRA:RHELPLAN-50002, JIRA:RHELPLAN-43531, JIRA:RHELPLAN-48838, BZ#1873567, BZ#1866695, JIRA:RHELPLAN-14068, JIRA:RHELPLAN-7788, JIRA:RHELPLAN-40469, JIRA:RHELPLAN-42617, JIRA:RHELPLAN-30878, JIRA:RHELPLAN-37517, JIRA:RHELPLAN-55009, JIRA:RHELPLAN-42396, BZ#1836211, JIRA:RHELPLAN-57564, JIRA:RHELPLAN-57567, BZ#1890499, JIRA:RHELPLAN-40234, JIRA:RHELPLAN-56676, JIRA:RHELPLAN-14754, JIRA:RHELPLAN-51289, BZ#1893174, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-41549, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, BZ#1748980, BZ#1827628, BZ#1871025, BZ#1871953, BZ#1874892, BZ#1893767, JIRA:RHELPLAN-60226

APÉNDICE B. HISTORIAL DE REVISIONES

0-1-3

Mar Feb 16 2021, Lenka Špačková(lspackova@redhat.com)

- Publicación de las notas de la versión de Red Hat Enterprise Linux 8.3.1.
- Actualización de la sección de actualización in situ en Overview con la publicación del aviso RHBA-2021:0569.

0-1-2

Vie Feb 12 2021, Lucie Maňásková(lmanasko@redhat.com)

- Se han añadido dos problemas conocidos (Seguridad, Instalador).

0-1-1

Mie Feb 10 2021, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido un problema conocido (Virtualización).

0-1-0

Wed Feb 03 2021, Lenka Špačková(lspackova@redhat.com)

- Se ha añadido una nota sobre la consolidación de la configuración de red en la línea de comandos del kernel bajo el parámetro **ip** (Networking).
- Se ha añadido **mercurial** a los paquetes obsoletos.
- Se ha añadido un problema conocido relacionado con los hosts Witherspoon (Virtualización).

0-0-9

Fri Jan 29 2021, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una nueva descripción de corrección de errores (Seguridad).
- Se ha añadido una nota sobre la desaparición del paquete **mailman** (Gestión de software).
- Se ha actualizado la sección de novedades (seguridad, gestión de identidades).
- Se ha añadido una nota de la Vista Previa de la Tecnología sobre el servicio **systemd-resolved**.
- Otras actualizaciones menores.

0.0-8

Lun 14 Dic 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha actualizado la sección de problemas conocidos y la sección de correcciones de errores.

0.0-7

Fri Nov 27 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una corrección de errores para el problema con **fapolicyd** (Seguridad).

- Más actualizaciones en la sección de corrección de errores.
- Se ha añadido una nota sobre la eliminación de la API REST de Podman basada en varlink V1 (contenedores).
- Se ha actualizado la sección de novedades.
- Se ha añadido un nuevo problema conocido sobre la replicación de planos desde el back-end de **lorax-composer** al nuevo back-end **de osbuild-composer** (Image Builder).

0.0-6

Fri Nov 20 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una descripción de la corrección de errores de OpenSCAP (Seguridad).
- Se ha actualizado la sección de novedades (Gestión del software).

0.0-5

Wed Nov 18 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha añadido información sobre la conversión de Oracle Linux o CentOS a RHEL (Visión general).

0.0-4

Thu Nov 12 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha añadido información sobre **Node.js 14.15.0** publicada con el aviso RHEA-2020:5101.

0.0-3

Wed Nov 11 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una descripción sobre la compatibilidad con el software de host Omni-Path Architecture (OPA) a las nuevas características.

0.0-2

Lun Nov 09 2020, Lenka Špačková(lspackova@redhat.com)

- Se han añadido los gráficos Tiger Lake de Intel como una muestra de tecnología (infraestructuras gráficas).

0.0-1

Wed Nov 04 2020, Lucie Maňásková(lmanasko@redhat.com)

- Publicación de las notas de la versión de Red Hat Enterprise Linux 8.3.

0.0-0

Tue Jul 28 2020, Lucie Maňásková(lmanasko@redhat.com)

- Publicación de las notas de la versión beta de Red Hat Enterprise Linux 8.3.