Red Hat Enterprise Linux 8

8.2 Notas de la versión

Notas de la versión de Red Hat Enterprise Linux 8.2

Last Updated: 2021-02-23

Red Hat Enterprise Linux 8 8.2 Notas de la versión

Notas de la versión de Red Hat Enterprise Linux 8.2

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 8.2 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 8.2, puede registrar su sistema, adjuntar suscripciones a RHEL e instalar desde Red Hat Content Delivery Network (CDN) antes de la instalación de paquetes. También puede registrar su sistema en Red Hat Insights durante la instalación. Las instalaciones interactivas de la GUI, así como las instalaciones automatizadas de Kickstart, soportan estas nuevas características.

Para más información, consulte Sección 5.1, “Creación del instalador y de la imagen” .

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.

Para más información, consulte Sección 5.4, “Servicios de infraestructura”.

Seguridad

System-wide cryptographic policies soporta ahora **customization**. El administrador puede ahora definir una política completa o modificar sólo ciertos valores.

RHEL 8.2 incluye los paquetes **setools-gui** y **setools-console-analyses** que proporcionan herramientas para el análisis de políticas de SELinux y la inspección de flujos de datos.

La Guía de Seguridad SCAP ofrece ahora un perfil que cumple con el modelo de madurez del Centro Australiano de Ciberseguridad (ACSC) **Essential Eight**

Para más información, consulte Sección 5.5, “Seguridad”.

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:

- **Python 3.8**
- **Maven 3.6**

Consulte Sección 5.10, “Lenguajes de programación dinámicos, servidores web y de bases de datos” para más detalles.

Conjuntos de herramientas de compilación

Los siguientes conjuntos de herramientas de compilación se han actualizado en RHEL 8.2:

- **GCC Toolset 9**
- **Clang and LLVM Toolset 9.0.1**
- **Rust Toolset 1.41**
- **Go Toolset 1.13**

Para más información, consulte Sección 5.11, “Compiladores y herramientas de desarrollo” .

Gestión de la identidad

Identity Management presenta una nueva herramienta de línea de comandos **Healthcheck**. **Healthcheck** ayuda a los usuarios a encontrar problemas que puedan afectar a la idoneidad de sus entornos de IdM.

Identity Management ahora es compatible con los roles y módulos de Ansible para su instalación y gestión. Esta actualización facilita la instalación y configuración de las soluciones basadas en IdM.

Para más información, consulte Sección 5.12, "Gestión de la identidad" .

La consola web

La consola web ha sido rediseñada para utilizar el diseño del sistema de interfaz de usuario de PatternFly 4.

Se ha añadido un tiempo de espera de la sesión en la consola web para mejorar la seguridad.

Para más información, consulte Sección 5.15, "La consola web" .

Escritorio

El conmutador de espacios de trabajo en el entorno de GNOME Classic ha sido modificado. El conmutador se encuentra ahora en la parte derecha de la barra inferior, y está diseñado como una tira horizontal de miniaturas. El cambio entre espacios de trabajo es posible haciendo clic en la miniatura requerida.

El subsistema gráfico del kernel **Direct Rendering Manager** (DRM) ha sido reajustado a la versión 5.3 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.

Actualización en el lugar

In-place upgrade from RHEL 7 to RHEL 8

La ruta de actualización in situ admitida es:

- De RHEL 7.9 a RHEL 8.2 en las arquitecturas Intel de 64 bits, IBM POWER 8 (little endian) e IBM Z
- Desde RHEL 7.6 hasta RHEL 8.2 en arquitecturas que requieren la versión 4.14 del kernel: ARM de 64 bits, IBM POWER 9 (little endian) e IBM Z (Structure A). Tenga en cuenta que estas arquitecturas siguen siendo totalmente compatibles con RHEL 7, pero ya no reciben actualizaciones menores desde RHEL 7.7.

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:

- Ahora puede utilizar repositorios personalizados adicionales para una actualización in situ de RHEL 7 a RHEL 8. También es posible actualizar sin Red Hat Subscription Manager.
- Puede crear sus propios actores para migrar sus aplicaciones personalizadas o de terceros utilizando la utilidad Leapp.

Para más detalles, consulte Personalización de la actualización in situ de Red Hat Enterprise Linux .

Si está utilizando CentOS 7 u Oracle Linux 7, puede convertir su sistema operativo a RHEL 7 utilizando la utilidad **convert2rhel** antes de actualizar a RHEL 8. Para obtener instrucciones, consulte Cómo convertir de CentOS u Oracle Linux a RHEL.

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 .

Si está utilizando CentOS 6 u Oracle Linux 6, puede convertir su sistema operativo a RHEL 6 utilizando la utilidad **convert2rhel** antes de actualizar a RHEL 8. Para obtener instrucciones, consulte Cómo convertir de CentOS u Oracle Linux a RHEL.

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 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 8.2 se distribuye con la versión 4.18.0-193 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 8.2.1

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 8.2.1.

4.1. NUEVAS CARACTERÍSTICAS

JDK Mission Control se ha actualizado a la versión 7.1.1

El perfilador JDK Mission Control (JMC) para JVMs HotSpot, proporcionado por el flujo de módulos **jmc:rhel8**, se ha actualizado a la versión 7.1.1 con la versión RHEL 8.2.1.

Esta actualización incluye numerosas correcciones de errores y mejoras, entre ellas:

- Múltiples optimizaciones de las reglas
- Una nueva vista de JOverflow basada en Standard Widget Toolkit (SWT)
- Una nueva vista del gráfico de la llama
- Una nueva forma de visualizar la latencia mediante el histograma de alto rango dinámico (HDR)

El flujo del módulo **jmc:rhel8** tiene dos perfiles:

- El perfil **común**, que instala toda la aplicación JMC
- El perfil **del núcleo**, que instala sólo las bibliotecas Java del núcleo **(jmc-core**)

Para instalar el perfil **común** del flujo del módulo **jmc:rhel8**, utilice

```
# yum module install jmc:rhel8/common
```

Cambie el nombre del perfil a **core** para instalar sólo el paquete **jmc-core**.

(BZ#1792519)

Conjunto de herramientas de Rust rebasado a la versión 1.43

Rust Toolset ha sido actualizado a la versión 1.43. Los cambios más destacados son:

- Los números de línea útiles se incluyen ahora en los mensajes de pánico de **las opciones** y los **resultados** cuando se invocan.
- Se ha ampliado la compatibilidad con los patrones de subcortes.
- La macro **matches!** proporciona una coincidencia de patrones que devuelve un valor booleano.
- los fragmentos de**elementos** pueden interpolarse en traits, impls y bloques externos.
- Mejora de la inferencia de tipos en torno a las primitivas.
- Constantes asociadas para flotadores y enteros.

Para instalar el módulo Rust Toolset, ejecute el siguiente comando como **root**:

```
# yum module install rust-toolset
```

Para obtener información sobre su uso, consulte la documentación sobre el uso del conjunto de herramientas de Rust.

(BZ#1811997)

Los registros de contenedores ahora soportan el comando de sincronización de skopeo

Con esta mejora, los usuarios pueden utilizar **el** comando skopeo sync para sincronizar los registros de contenedores y los registros locales. El comando skopeo **sync** es útil para sincronizar una réplica del registro de contenedores local y para rellenar los registros que se ejecutan dentro de los entornos de air-gapped.

El comando **skopeo sync** requiere que los transportes de origen **(--src**) y de destino **(--dst**) se especifiquen por separado. Los transportes de origen y destino disponibles son **docker** (repositorio alojado en un registro de contenedores) y **dir** (directorio en una ruta de directorio local). Los transportes de origen también incluyen **yaml** (ruta del archivo YAML local). Para información sobre el uso de **skopeo sync**, vea la página man de **skopeo-sync**.

(BZ#1811779)

El archivo de configuración container.conf ya está disponible

Con esta mejora, los usuarios y administradores pueden especificar opciones de configuración por defecto y banderas de línea de comandos para los motores de contenedores. Los motores de contenedores leen los archivos **/usr/share/containers/containers.conf** y **/etc/containers/containers.conf** si existen. En el modo sin raíz, los motores de contenedores leen los archivos **$HOME/.config/containers/containers**.conf.

Los campos especificados en el archivo **containers**.conf anulan las opciones por defecto, así como las opciones de los archivos **containers.** conf leídos previamente. El archivo **container**.conf se comparte entre Podman y Buildah y sustituye al archivo **libpod.conf**.

(BZ#11826486)

Ahora puede entrar y salir de un servidor de registro

Con esta mejora, puedes entrar y salir de un servidor de registro específico usando los comandos skopeo **login** y **skopeo logout**. El comando **skopeo** login lee el nombre de usuario y la contraseña desde la entrada estándar. El nombre de usuario y la contraseña también se pueden establecer usando las opciones **--username** (o **-u**) y **--password** (o **-p**).

Puede especificar la ruta del archivo de autenticación estableciendo el indicador **--authfile**. La ruta por defecto es **${XDG_RUNTIME_DIR}/contenedores/auth.json**. Para información sobre el uso de skopeo **login** y **skopeo logout**, vea las páginas man de **skopeo-login** y **skopeo-logout**, respectivamente.

(JIRA:RHELPLAN-47311)

Ahora puede restablecer el almacenamiento de podman

Con esta mejora, los usuarios pueden utilizar el comando **podman** system reset para restablecer el almacenamiento de **podman** al estado inicial. El comando **podman** system reset elimina todos los pods, contenedores, imágenes y volúmenes. Para más información, consulte la página man de **podman-system-reset**.

(JIRA:RHELPLAN-48941)

CAPÍTULO 5. NUEVAS CARACTERÍSTICAS

Esta parte describe las nuevas características y las principales mejoras introducidas en Red Hat Enterprise Linux 8.2.

5.1. CREACIÓN DEL INSTALADOR Y DE LA IMAGEN

Posibilidad de registrar su sistema, adjuntar suscripciones a RHEL e instalar desde el CDN de Red Hat

En RHEL 8.2, puede registrar su sistema, adjuntar suscripciones a RHEL e instalar desde la Red Hat Content Delivery Network (CDN) antes de la instalación de paquetes. Las instalaciones interactivas de la GUI, así como las instalaciones automatizadas de Kickstart, soportan esta característica. Los beneficios incluyen:

- El uso del archivo de imagen ISO de arranque más pequeño elimina la necesidad de descargar el archivo de imagen ISO de DVD binario más grande.
- La CDN utiliza los últimos paquetes que dan como resultado un sistema totalmente suscrito y actualizado inmediatamente después de la instalación. No es necesario instalar las actualizaciones de los paquetes después de la instalación.
- El registro se realiza antes de la instalación de los paquetes, lo que hace que el proceso de instalación sea más corto y ágil.
- Está disponible el soporte integrado para Red Hat Insights.

(BZ#1748281)

Posibilidad de registrar el sistema en Red Hat Insights durante la instalación

En RHEL 8.2, puede registrar su sistema en Red Hat Insights durante la instalación. Las instalaciones interactivas de la GUI, así como las instalaciones automatizadas de Kickstart, soportan esta característica.

Los beneficios incluyen:

- Es más fácil identificar, priorizar y resolver los problemas antes de que las operaciones comerciales se vean afectadas.
- Identifique y corrija proactivamente las amenazas a la seguridad, el rendimiento, la disponibilidad y la estabilidad con análisis predictivos.
- Evite problemas y tiempos de inactividad imprevistos en su entorno.

(BZ#1746391)

Image Builder ofrece ahora compatibilidad con cloud-init para crear imágenes de Azure

Con esta mejora, la compatibilidad con cloud-init está disponible para las imágenes de Azure creadas por Image Builder. Como resultado, la creación de imágenes locales con aprovisionamiento rápido y la capacidad de añadir datos personalizados está disponible para los clientes.

(BZ#1754711)

5.2. GESTIÓN DEL SOFTWARE

La cadena de encabezado User-Agent ahora incluye información leída del archivo /etc/os-release

Con esta mejora, la cadena de cabecera **User-Agent**, que normalmente se incluye con las peticiones HTTP realizadas por DNF, se ha ampliado con información leída del archivo **/etc/os-release**.

Para obtener más información, consulte **user_agent** en la página man de **dnf.conf(5)**.

(BZ#1676891)

Todas las unidades de temporización dnf-automatic.timer utilizan ahora el reloj en tiempo real por defecto

Anteriormente, las unidades de temporización **dnf-automatic.timer** utilizaban el reloj monotónico, lo que daba lugar a un tiempo de activación imprevisible tras el arranque del sistema. Con esta actualización, las unidades de temporización se ejecutan entre las 6 y las 7 de la mañana. Si el sistema está apagado durante ese tiempo, las unidades de temporización se activan una hora después del arranque del sistema.

(BZ#1754609)

La utilidad createrepo_c ahora omite los paquetes cuyos metadatos contienen los caracteres de control no permitidos

Para garantizar un XML válido, los metadatos del paquete no deben contener ningún carácter de control, a excepción de:

- la pestaña horizontal
- el carácter de nueva línea
- el carácter de retorno de carro

Con esta actualización, la utilidad **createrepo_c** no incluye paquetes con metadatos que contengan caracteres de control no permitidos en un repositorio recién creado, y devuelve el siguiente mensaje de error:

```
C_CREATEREPOLIB: Crítico: No se puede volcar el XML para PACKAGE_NAME
(PACKAGE_SUM): Se han encontrado caracteres de control prohibidos (valores ASCII
```

(BZ#1743186)

5.3. SHELL Y HERRAMIENTAS DE LÍNEA DE COMANDOS

opencv rebasado a la versión 3.4.6

Los paquetes **opencv** han sido actualizados a la versión 3.4.6. Los cambios notables incluyen:

- Soporte para nuevos parámetros de Open CL, como **OPENCV_OPENCL_BUILD_EXTRA_OPTIONS** y **OPENCV_OPENCL_DEVICE_MAX_WORK_GROUP_SIZE**.
- El módulo **objdetect** ahora soporta el algoritmo de detección de códigos QR.
- Varios métodos nuevos, como **MatSize::dims** o **VideoCapture::getBackendName**.
- Múltiples funciones nuevas, como **drawFrameAxes** o **getVersionMajor**.

- Varias mejoras de rendimiento, incluyendo mejoras de la función GaussianBlur, **v_load_deinterleave** y **v_store_interleave** intrínsecas cuando se utilizan instrucciones SSSE3.

(BZ#1694647)

5.4. SERVICIOS DE INFRAESTRUCTURA

graphviz-python3 se distribuye ahora en el repositorio CRB

Esta actualización añade el paquete **graphviz-python3** a RHEL 8. El paquete proporciona los enlaces necesarios para el uso del software de visualización de gráficos Graphviz desde Python.

Tenga en cuenta que el paquete **graphviz-python3** se distribuye en el repositorio CodeReady Linux Builder (CRB) sin soporte.

(BZ#1704875)

reajustado a la versión 2.13.0

Los paquetes **ajustados** han sido actualizados a la versión 2.13.0. Las mejoras más destacadas son:

- Se ha añadido un marco de ajuste dependiente de la arquitectura.
- Se ha añadido soporte para múltiples directivas de inclusión.
- Se ha actualizado el ajuste en los perfiles de **sap-hana**, **latencia-rendimiento** y **tiempo real**.

(BZ#1738250)

powertop rebasado a la versión 2.11

El paquete **powertop** se ha actualizado a la versión 2.11, que aporta el siguiente cambio notable:

- Soporte para las plataformas EHL, TGL, ICL/ICX

(BZ#1716721)

BIND soporta ahora .GeoIP2 en lugar de GeoLite Legacy GeoIP

La biblioteca GeoLite Legacy GeoIP ya no está soportada en BIND. Con esta actualización, GeoLite Legacy GeoP ha sido sustituida por GeoIP2, que se proporciona en el formato de datos **libmaxminddb**.

Tenga en cuenta que el nuevo formato puede requerir algunos cambios de configuración, y que el formato tampoco es compatible con la configuración de la lista de control de acceso (ACL) de GeoIP:

- geoip netspeed
- geoip org
- Códigos de país ISO 3166 Alpha-3

(BZ#1564443)

stale-answer ahora proporciona registros antiguos en caché en caso de ataque DDoS

Anteriormente, el ataque de denegación de servicio distribuido (DDoS) hacía que los servidores autoritativos fallaran con el error SERVFAIL. Con esta actualización, la funcionalidad **stale-answer** proporciona los registros caducados hasta que se obtiene una nueva respuesta.

Para habilitar o deshabilitar la función **de servir a la gente**, utilice cualquiera de estas opciones:

- Archivo de configuración
- Canal de control remoto (rndc)

(BZ#1664863)

BIND rebasado a la versión 9.11.13

Los paquetes **bind** han sido actualizados a la versión 9.11.13. Los cambios notables incluyen:

- Se ha añadido la variable estadística **tcp-highwater**. Esta variable muestra el máximo de clientes TCP concurrentes registrados durante una ejecución.
- Se ha añadido el algoritmo **SipHash-2-4-based** DNS Cookies (RFC 7873).
- Las direcciones de cola para las consultas de enraizamiento se devuelven independientemente de cómo se establezca la opción de configuración **de respuestas mínimas**.
- El comando **named-checkconf** asegura ahora la validez de los prefijos de red **DNS64**.
- La renovación automática según RFC 5011 ya no falla cuando las declaraciones **trusted-keys** y **managed-keys** están configuradas para el mismo nombre. En su lugar, se registra un mensaje de advertencia.
- El procesamiento de nombres de dominio internacionalizados (IDN) en las utilidades **dig** y **nslookup** está ahora desactivado por defecto cuando no se ejecutan en el terminal (por ejemplo, en un script). El procesamiento de IDN en **dig** puede activarse mediante las opciones **idnin** e **idnout**.

(BZ#1704328)

5.5. SEGURIDAD

RHEL 8 contiene ahora el perfil DISA STIG

Las Guías Técnicas de Implementación de Seguridad (STIG) son un conjunto de recomendaciones básicas publicadas por la Agencia de Sistemas de Información de Defensa (DISA) para reforzar la seguridad de los sistemas de información y el software que de otro modo podrían ser vulnerables. Esta versión incluye el perfil y el archivo Kickstart para esta política de seguridad. Con esta mejora, los usuarios pueden comprobar la conformidad de los sistemas, remediar los sistemas para que sean conformes e instalar sistemas conformes con DISA STIG para Red Hat Enterprise Linux 8.

(BZ#1755447)

ahora se pueden personalizarlas criptopolíticas

Con esta actualización, puede ajustar ciertos algoritmos o protocolos de cualquier nivel de política o establecer un nuevo archivo de política completo como la política criptográfica actual de todo el sistema. Esto permite a los administradores personalizar la política criptográfica de todo el sistema según lo requieran los diferentes escenarios.

Los paquetes RPM deben almacenar las políticas proporcionadas por ellos en el directorio **/usr/share/crypto-policies/policies**. El directorio **/etc/crypto-policies/policies** contiene las políticas locales personalizadas.

Para obtener más información, consulte la sección **Políticas personalizadas** en la página de manual **update-crypto-policies (8)** y la sección **Formato de definición de políticas Crypto** en la página de manual **update-crypto-policies(8)**.

(BZ#1690565)

La Guía de Seguridad de SCAP ahora es compatible con ACSC Essential Eight

Los paquetes **scap-security-guide** proporcionan ahora el perfil de cumplimiento del Australian Cyber Security Centre (ACSC) Essential Eight y un archivo Kickstart correspondiente. Con esta mejora, los usuarios pueden instalar un sistema que se ajuste a esta línea de base de seguridad. Además, pueden utilizar el paquete **OpenSCAP** para comprobar el cumplimiento de la seguridad y su corrección utilizando esta especificación de controles mínimos de seguridad definidos por el ACSC.

(BZ#1755194)

ya está disponible**oscap-podman** para la exploración de la seguridad y el cumplimiento de los contenedores

Esta actualización de los paquetes **openscap** introduce una nueva utilidad para el escaneo de seguridad y cumplimiento de los contenedores. La herramienta **oscap-podman** proporciona un equivalente de la utilidad **oscap-docker** que sirve para escanear contenedores e imágenes de contenedores en RHEL 7.

(BZ#1642373)

setroubleshoot ahora puede analizar y reaccionar a las denegaciones de acceso **a execmem**

Esta actualización introduce un nuevo plugin **setroubleshoot**. El plugin puede analizar las denegaciones de acceso **a execmem** (AVCs) y proporcionar los consejos pertinentes. Como resultado, **setroubleshoot** ahora puede sugerir la posibilidad de cambiar un booleano si permite el acceso, o informar del problema cuando ningún booleano puede permitir el acceso.

(BZ#1649842)

Nuevos paquetes: **setools-gui** y **setools-console-analyses**

El paquete **setools-gui**, que ha formado parte de RHEL 7, se introduce ahora en RHEL 8. Las herramientas gráficas ayudan a inspeccionar las relaciones y los flujos de datos, especialmente en sistemas de varios niveles con políticas SELinux muy especializadas. Con la herramienta gráfica **apol** del paquete **setools-gui**, se pueden inspeccionar y analizar aspectos de una política SELinux. Las herramientas del paquete **setools-console-analyses** permiten analizar las transiciones de dominio y los flujos de información de las políticas SELinux.

(BZ#1731519)

Los usuarios confinados en SELinux ahora pueden gestionar los servicios de sesión de los usuarios

Anteriormente, los usuarios confinados no podían gestionar los servicios de sesión de usuario. Como resultado, no podían ejecutar los comandos **systemctl --user** o **busctl --user** ni trabajar en la consola web de RHEL. Con esta actualización, los usuarios confinados pueden gestionar las sesiones de usuario.

(BZ#1727887)

El servicio **lvmdbusd** está ahora confinado por SELinux

El servicio **lvmdbusd** proporciona una API D-Bus al gestor de volúmenes lógicos (LVM). Anteriormente, el demonio **lvmdbusd** no podía pasar al contexto **lvm_t** aunque la política SELinux para **lvm_t** estuviera definida. Como consecuencia, el demonio **lvmdbusd** se ejecutaba en el dominio **unconfined_service_t**

y SELinux etiquetaba a **lvmdbusd** como no confinado. Con esta actualización, el archivo ejecutable de **lvmdbusd** tiene el contexto **lvm_exec_t** definido y **lvmdbusd** puede utilizarse ahora correctamente con SELinux en modo de refuerzo.

(BZ#1726166)

semanage ahora soporta el listado y la modificación de puertos SCTP y DCCP.

Anteriormente, **semanage** port sólo permitía listar y modificar los puertos TCP y UDP. Esta actualización añade el soporte de los protocolos SCTP y DCCP a **semanage** port. Como resultado, los administradores pueden ahora comprobar si dos máquinas pueden comunicarse a través de SCTP y habilitar completamente las características de SCTP para desplegar con éxito las aplicaciones basadas en SCTP.

(BZ#1563742)

laexportación de semanage ahora muestra las personalizaciones relacionadas con los dominios permisivos

Con esta actualización, la utilidad **semanage**, que forma parte del paquete **policycoreutils** para SELinux, es capaz de mostrar las personalizaciones relacionadas con los dominios permisivos. Los administradores del sistema ahora pueden transferir las modificaciones locales permisivas entre máquinas utilizando el comando semanage **export**.

(BZ#1417455)

udica puede añadir nuevas reglas de permiso generadas a partir de denegaciones de SELinux a la política de contenedores existente

Cuando un contenedor que se ejecuta bajo una política generada por la utilidad **udica** desencadena una denegación de SELinux, **udica** es ahora capaz de actualizar la política. El nuevo parámetro **-a** o **--append-rules** puede utilizarse para añadir reglas desde un archivo AVC.

(BZ#1732704)

Los nuevos tipos de SELinux permiten que los servicios se ejecuten confinados

Esta actualización introduce nuevos tipos de SELinux que permiten que los siguientes servicios se ejecuten como servicios confinados en el modo de aplicación de SELinux en lugar de ejecutarse en el dominio **unconfined_service_t**:

- **lldpd** ahora se ejecuta como **lldpad_t**
- **rrdcached** ahora se ejecuta como **rrdcached_t**
- **stratisd** ahora se ejecuta como **stratisd_t**
- **timedatex** ahora se ejecuta como **timedatex_t**

(BZ#1726246, BZ#1726255, BZ#1726259, BZ#1730204)

Clevis es capaz de enumerar las políticas vigentes para un determinado dispositivo LUKS

Con esta actualización, el comando clevis **luks list** enumera las políticas PBD vigentes para un determinado dispositivo LUKS. Esto facilita la búsqueda de información sobre los pines de la horquilla en uso y la configuración de los pines, por ejemplo, las direcciones del servidor Tang, los detalles de las políticas **tpm2** y los umbrales SSS.

(BZ#1766526)

Clevis proporciona nuevos comandos para informar del estado de las llaves y volver a enlazar las llaves caducadas

El comando **clevis luks report** proporciona ahora una forma sencilla de informar si las claves de un determinado enlace requieren rotación. Las rotaciones regulares de las claves en un servidor Tang mejoran la seguridad de los despliegues de Network-Bound Disk Encryption (NBDE), y por lo tanto el cliente debe proporcionar la detección de las claves caducadas. Si la clave está caducada, Clevis sugiere utilizar el comando **clevis luks regen** que vuelve a enlazar la ranura de la clave caducada con una clave actual. Esto simplifica significativamente el proceso de rotación de claves.

(BZ#1564559, BZ#1564566)

Ahora Clevis puede extraer la frase de contraseña utilizada para vincular una ranura concreta en un dispositivo LUKS

Con esta actualización del marco de descifrado basado en políticas de Clevis, ahora se puede extraer la frase de contraseña utilizada para vincular una ranura concreta en un dispositivo LUKS. Anteriormente, si se borraba la frase de contraseña de instalación de LUKS, Clevis no podía realizar tareas administrativas de LUKS, como volver a cifrar, habilitar una nueva ranura de clave con una frase de contraseña de usuario y volver a vincular Clevis cuando el administrador necesita cambiar el umbral **sss**. Esta actualización introduce el comando **clevis luks pass** que muestra la frase de contraseña utilizada para vincular una ranura concreta.

(BZ#1436780)

Clevis proporciona ahora un soporte mejorado para descifrar múltiples dispositivos LUKS en el arranque

Los paquetes **clevis** han sido actualizados para proporcionar un mejor soporte para descifrar múltiples dispositivos cifrados por LUKS en el arranque. Antes de esta mejora, el administrador tenía que realizar complicados cambios en la configuración del sistema para permitir el descifrado adecuado de múltiples dispositivos por parte de Clevis en el arranque. Con esta versión, puede configurar el descifrado utilizando el comando clevis **luks bind** y actualizando el initramfs mediante el comando **dracut -fv --regenerate-all**.

Para más detalles, consulte la sección Configuración del desbloqueo automático de volúmenes encriptados mediante el descifrado basado en políticas.

(BZ#1784524)

openssl-pkcs11 rebasado a 0.4.10

El paquete **openssl-pkcs11** ha sido actualizado a la versión 0.4.10, que proporciona muchas correcciones de errores y mejoras respecto a la versión anterior. El paquete **openssl-pkcs11** proporciona acceso a los módulos PKCS #11 a través de la interfaz del motor. Los principales cambios introducidos por la nueva versión son:

- Si un objeto de clave pública correspondiente a la clave privada no está disponible al cargar una clave privada ECDSA, el motor carga la clave pública de un certificado coincidente, si está presente.
- Puede utilizar un URI PKCS #11 genérico (por ejemplo **pkcs11:type=public**) porque el motor **openssl-pkcs11** busca todos los tokens que coincidan con un URI PKCS #11 determinado.
- El sistema intenta iniciar la sesión con un PIN sólo si un único dispositivo coincide con la búsqueda URI. Esto evita los fallos de autenticación debidos a que se proporciona el PIN a todos los tokens que coinciden.

- Al acceder a un dispositivo, el motor **openssl-pkcs11** marca ahora la estructura de métodos RSA con la bandera **RSA_FLAG_FIPS_METHOD**. En el modo FIPS, OpenSSL requiere que la bandera se establezca en la estructura de métodos RSA. Tenga en cuenta que el motor no puede detectar si un dispositivo está certificado por FIPS.

(BZ#1745082)

rsyslog rebasado a 8.1911.0

La utilidad **rsyslog** se ha actualizado a la versión 8.1911.0, que proporciona una serie de correcciones de errores y mejoras con respecto a la versión anterior. La siguiente lista incluye mejoras notables:

- El nuevo módulo **omhttp** permite enviar mensajes a través de la interfaz HTTP REST.
- El módulo de entrada de archivos se ha mejorado para aumentar la estabilidad, la notificación de errores y la detección de truncamientos.
- El nuevo parámetro **action.resumeIntervalMax**, que puede utilizarse con cualquier acción, permite limitar el crecimiento del intervalo de reintentos a un valor determinado.
- La nueva opción **StreamDriver.PermitExpiredCerts** para TLS permite las conexiones incluso si un certificado ha expirado.
- Ahora puede suspender y reanudar la salida basándose en el contenido del archivo externo configurado. Esto es útil en los casos en los que el otro extremo siempre acepta los mensajes y los abandona silenciosamente cuando no es capaz de procesarlos todos.
- Se ha mejorado el informe de errores del módulo de salida de archivos y ahora contiene nombres de archivos reales y más información sobre las causas de los errores.
- Las colas de disco ahora se ejecutan con varios hilos, lo que mejora el rendimiento.
- Puede establecer modos de funcionamiento TLS más estrictos: comprobación del campo de certificado **extendedKeyUsage** y comprobación más estricta de los campos de certificado **CN**/**SAN**.

(BZ#1740683)

rsyslog ahora proporciona el plugin omhttp para la comunicación a través de una interfaz HTTP REST

Con esta actualización de los paquetes **rsyslog**, puede utilizar el nuevo plugin **omhttp** para producir una salida compatible con los servicios que utilizan una API de transferencia de estado representativa (REST), como la plataforma de almacenamiento Ceph, Amazon Simple Storage Service (Amazon S3) y Grafana Loki. Este nuevo módulo de salida HTTP proporciona una ruta REST configurable y un formato de mensaje, soporte para varios formatos de lotes, compresión y encriptación TLS.

Para más detalles, consulte el archivo **/usr/share/doc/rsyslog/html/configuration/modules/omhttp.html** instalado en su sistema con el paquete **rsyslog-doc**.

(BZ#1676559)

omelasticsearch en rsyslog ahora soporta rebindinterval

Esta actualización de los paquetes **rsyslog** introduce el soporte para configurar el tiempo de reconexión periódica en el módulo **omelasticsearch**. Puede mejorar el rendimiento al enviar registros a un clúster de nodos de Elasticsearch configurando este parámetro de acuerdo con su escenario. El valor del

parámetro **rebindinterval** indica el número de operaciones enviadas a un nodo después del cual **rsyslog** cierra la conexión y establece una nueva. El valor por defecto **-1** significa que **rsyslog** no restablece la conexión.

(BZ#1692073)

rsyslog mmkubernetes ahora proporciona la expiración de la caché de metadatos

Con esta actualización de los paquetes **rsyslog**, puede utilizar dos nuevos parámetros para el módulo **mmkubernetes** para establecer la caducidad de la caché de metadatos. Esto garantiza que los objetos de Kubernetes eliminados se eliminen de la caché estática **de mmkubernetes**. El valor del parámetro **cacheentryttl** indica la edad máxima de las entradas de la caché en segundos. El parámetro **cacheexpireinterval** tiene los siguientes valores:

- -**1** para desactivar la comprobación de la caducidad de la caché
- **0** para activar la comprobación de la caducidad de la caché
- mayor que 0 para las comprobaciones periódicas de la caducidad de la caché en segundos

(BZ#1692072)

auditoría basada en la versión 3.0-0.14

Los paquetes de **auditoría** se han actualizado a la versión 3.0-0.14, que proporciona muchas correcciones de errores y mejoras con respecto a la versión anterior, sobre todo:

- Se ha añadido una opción para interpretar los campos en el plugin de syslog
- Dividido el archivo **30-ospp-v42.rules** en archivos más granulares
- Mover las reglas de ejemplo al directorio **/usr/share/audit/sample-rules/**
- Corregido el modo de transporte de la Auditoría KRB5 para el registro remoto

(BZ#1757986)

La auditoría contiene ahora muchas mejoras del kernel v5.5-rc1

Esta adición al kernel de Linux contiene la mayoría de las mejoras, correcciones de errores y limpiezas relacionadas con el subsistema de auditoría e introducidas entre la versión 4.18 y la 5.5-rc1. La siguiente lista destaca los cambios importantes:

- Uso más amplio del campo **exe** para el filtrado
- Compatibilidad con las capacidades namespaced de la v3
- Mejoras en el filtrado de sistemas de archivos remotos
- Fijación de la regla del filtro **gid**
- Correcciones de una corrupción de memoria de uso después de libre y de fugas de memoria
- Mejoras en la asociación de registros de eventos
- Limpieza de la interfaz **fanoticy**, de las opciones de configuración de la auditoría y de la interfaz syscall
- Fijación del valor de retorno del módulo de verificación ampliado (EVM)

- Correcciones y limpiezas de varios formatos de registro
- Simplificaciones y correcciones de la auditoría del sistema de archivos virtuales (VFS)

(BZ#1716002)

fapolicyd rebasado a 0.9.1-2

Los paquetes **fapolicyd** que proporcionan la lista blanca de aplicaciones de RHEL han sido actualizados a la versión 0.9.1-2. Entre las mejoras y correcciones de errores más destacadas se encuentran:

- La identificación del proceso es fija.
- La parte del sujeto y la parte del objeto se colocan ahora estrictamente en la regla. Ambas partes están separadas por dos puntos, y contienen el permiso requerido (ejecutar, abrir, cualquiera).
- Se consolidan los atributos de sujeto y objeto.
- El nuevo formato de las reglas es el siguiente:

  ```
  PERMISO DE DECISIÓN SUJETO : OBJETO
  ```

  Por ejemplo:

  ```
  allow perm=open exe=/usr/bin/rpm : all
  ```

(BZ#1759895)

sudo rebasado a 1.8.29-3.el8

los paquetes**sudo** han sido actualizados a la versión 1.8.29-3, que proporciona una serie de correcciones de errores y mejoras respecto a la versión anterior. Los principales cambios introducidos por la nueva versión son:

- **sudo** ahora escribe los mensajes del Pluggable Authentication Module (PAM) en la terminal del usuario, si está disponible, en lugar de la salida estándar o la salida de error estándar. Esto evita la posible confusión de la salida PAM y la salida de comandos enviada a archivos y tuberías.
- Las opciones **notBefore** y **notAfter** de LDAP y SSSD ahora funcionan y se muestran correctamente con el comando **sudo -l**.
- El comando **cvtsudoers** ahora rechaza las entradas que no sean del formato de intercambio de datos LDAP (LDIF) al convertir de LDIF a los formatos **sudoers** y JSON.
- Con las nuevas configuraciones **log_allowed** y **log_denied** para **los sudoers**, puedes desactivar el registro y la auditoría de los comandos permitidos y denegados.
- Ahora puede utilizar **sudo** con la opción **-g** para especificar un grupo que coincida con cualquiera de los grupos del usuario de destino, incluso si no hay grupos presentes en la especificación **de runas_spec**. Anteriormente, sólo se podía hacer si el grupo coincidía con el grupo principal del usuario de destino.
- Se ha corregido un error que impedía a **sudo** hacer coincidir el nombre del host con el valor de **ipa_hostname** de **sssd.**conf, si se especificaba.

- Se ha corregido una vulnerabilidad que permitía a un usuario **sudo** ejecutar un comando como root cuando la especificación **Runas** no permitía el acceso de **root** con la palabra clave **ALL** (CVE-2019-14287).

- El uso de IDs de usuarios y grupos desconocidos para las entradas de **sudoers** permisivos, por ejemplo usando la palabra clave ALL, está ahora deshabilitado. Puede habilitarlo con el ajuste **runas_allow_unknown_id** (CVE-2019-19232).

(BZ#1733961)

El módulo pam_namespace ahora permite especificar opciones de montaje adicionales para tmpfs

Las opciones de montaje **nosuid**, **noexec** y **nodev** pueden utilizarse ahora en el archivo de configuración **/etc/security/namespace.conf** para desactivar, respectivamente, el efecto del bit setuid, desactivar la ejecución de ejecutables y evitar que los archivos se interpreten como dispositivos de carácter o de bloque en el sistema de archivos **tmpfs** montado.

Las opciones de montaje adicionales se especifican en la página man de **tmpfs(5)**.

(BZ#1252859)

pam_faillock ahora puede leer los ajustes del archivo de configuración faillock.conf

El módulo **pam_faillock**, que forma parte de los módulos de autenticación enchufables (PAM), ahora puede leer los ajustes del archivo de configuración ubicado en **/etc/security/faillock.conf**. Esto facilita la configuración de un bloqueo de cuenta en caso de fallos de autenticación, proporcionar perfiles de usuario para esta funcionalidad y manejar diferentes configuraciones de PAM simplemente editando el archivo **faillock**.conf.

(BZ#1537242)

5.6. RED

Las aplicaciones de espacio de usuario pueden ahora recuperar el id de red seleccionado por el kernel

Las aplicaciones del espacio de usuario pueden solicitar al núcleo que seleccione un nuevo ID de **netns** y lo asigne a un espacio de nombres de red. Con esta mejora, los usuarios pueden especificar la bandera **NLM_F_ECHO** al enviar un mensaje de enlace de **red RTM_NETNSID** al núcleo. El núcleo envía entonces el mensaje de enlace de **red** de vuelta al usuario. Este mensaje incluye el ID de **netns** establecido al valor que el kernel seleccionó. Como resultado, las aplicaciones del espacio de usuario tienen ahora una opción fiable para identificar el ID de enlace de **red** que el núcleo ha seleccionado.

(BZ#1763661)

firewalld rebasado a la versión 0.8

Los paquetes **firewalld** han sido actualizados a la versión 0.8. Los cambios notables incluyen:

- Esta versión de **firewalld** incluye todas las correcciones de errores desde la versión 0.7.0.

- **firewalld** ahora utiliza la interfaz **libnftables** JSON para el subsistema **nftables**. Esto mejora el rendimiento y la fiabilidad de la aplicación de reglas.

- En las definiciones de servicio, el nuevo elemento **helper** sustituye **al módulo**.

- Esta versión permite que los ayudantes personalizados utilicen los módulos de ayuda estándar.

(BZ#1740670)

ndptool ahora puede especificar una dirección de destino en la cabecera IPv6

Con esta actualización, la utilidad **ndptool** puede enviar un mensaje Neighbor Solicitation (NS) o Neighbor Advertisement (NA) a un destino específico especificando la dirección en la cabecera IPv6. Como resultado, se puede enviar un mensaje a otras direcciones además de la dirección de enlace local.

(BZ#1697595)

nftables ahora soporta tipos de conjuntos IP multidimensionales

Con esta mejora, el marco de filtrado de paquetes **de nftables** admite tipos de conjuntos con concatenaciones e intervalos. Como resultado, los administradores ya no necesitan soluciones para crear tipos de conjuntos IP multidimensionales.

(BZ#1593711)

nftables rebasado a la versión 0.9.3

Los paquetes *nftables* han sido actualizados a la versión 0.9.3, que proporciona una serie de correcciones de errores y mejoras respecto a la versión anterior:

- Se ha añadido una API JSON a la biblioteca **libnftables**. Esta biblioteca proporciona una interfaz de alto nivel para gestionar los conjuntos de reglas de *nftables* desde aplicaciones de terceros. Para utilizar la nueva API en Python, instale el paquete **python3-nftables**.
- Las declaraciones admiten prefijos y rangos de IP, como **192.0.2.0/24** y **192.0.2.0-192.0.2.30**.
- Se ha añadido soporte para las huellas del sistema operativo para marcar los paquetes en función del sistema operativo adivinado. Para más detalles, consulte la sección de **expresiones osf** en la página man de **nft(8)**.
- Se ha añadido soporte de proxy transparente para redirigir paquetes a un socket local sin cambiar la cabecera del paquete de ninguna manera. Para más detalles, consulte la sección de la **sentencia tproxy** en la página man de **nft(8)**.
- Por defecto, **nft** muestra los nombres textuales del conjunto de prioridades al crear las cadenas nft. Para ver los valores numéricos de prioridad estándar, utilice la opción **-y**. Para más detalles, consulte la sección Valores de prioridad estándar y nombres textuales.
- Se ha añadido el soporte de la marca de seguridad.
- Se ha mejorado la compatibilidad con las actualizaciones de conjuntos dinámicos para fijar las actualizaciones de la ruta de los paquetes.
- Se ha añadido la compatibilidad con la coincidencia de puertos de cabecera de transporte.

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

- https://lore.kernel.org/netfilter-devel/20190624164910.defehs5giqziqnir@salvia/
- https://lore.kernel.org/netfilter-devel/20190819115807.myv6owxzblj2bthd@salvia/
- https://lore.kernel.org/netfilter-devel/20191202211737.xvmd6e6xxj4xvvjl@salvia/

(BZ#1643192)

Las reglas para el servicio firewalld ahora pueden utilizar ayudantes de seguimiento de conexiones para los servicios que se ejecutan en un puerto no estándar

Los ayudantes definidos por el usuario en el servicio **firewalld** ahora pueden utilizar módulos de ayuda estándar del kernel. Esto permite a los administradores crear reglas de **firewalld** para utilizar ayudantes de seguimiento de conexiones para servicios que se ejecutan en un puerto no estándar.

(BZ#1733066)

El paquete whois ya está disponible

Con esta mejora, el paquete **whois** está ahora disponible en RHEL 8.2.0. Como resultado, ahora es posible recuperar información sobre un nombre de dominio o una dirección IP específicos.

(BZ#1734183)

eBPF para tc ya es totalmente compatible

El subsistema del kernel Traffic Control (tc) y la herramienta **tc** pueden adjuntar programas de Berkeley Packet Filtering (eBPF) ampliados como clasificadores de paquetes y acciones para las disciplinas de colas de entrada y salida. Esto permite el procesamiento programable de paquetes dentro de la ruta de datos de la red del kernel. eBPF para **tc**, que anteriormente estaba disponible como vista previa de la tecnología, es ahora totalmente compatible con RHEL 8.2.

(BZ#1755347)

5.7. NÚCLEO

Versión del núcleo en RHEL 8.2

Red Hat Enterprise Linux 8.2 se distribuye con la versión 4.18.0-193 del kernel.

Véase también Cambios importantes en los parámetros externos del kernel y en los controladores de dispositivos.

(BZ#1797671)

Filtro de paquetes Berkeley ampliado para RHEL 8.2

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 8.2, los siguientes componentes de **eBPF** están soportados:

- El paquete de herramientas **BPF Compiler Collection (BCC)**, que es una colección de espacio de usuario de utilidades de rastreo dinámico del kernel que utilizan la máquina virtual **eBPF** para crear programas eficientes de rastreo y manipulación del kernel. El paquete **BCC** proporciona herramientas para el análisis de E/S, la creación de redes y la supervisión de sistemas operativos Linux que utilizan **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.

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 función **eXpress Data Path (XDP)**

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

(BZ#1780124)

Software de host Intel ® Omni-Path Architecture (OPA)

El software de host Intel Omni-Path Architecture (OPA) es totalmente compatible con Red Hat Enterprise Linux 8.2. Intel 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 documentación de la Arquitectura Intel Omni-Path, consulte: https://cdrdv2.intel.com/v1/dl/getContent/616368

(BZ#1833541)

Control Group v2 es ahora totalmente compatible con RHEL 8

el mecanismo**Control Group v2** es un grupo de control jerárquico unificado. **Control Group v2** organiza los procesos jerárquicamente y distribuye los recursos del sistema a lo largo de la jerarquía de forma controlada y configurable.

A diferencia de la versión anterior, **Control Group v2** tiene una sola jerarquía. Esta única jerarquía permite al kernel de Linux:

- Clasificar los procesos en función de la función de su propietario.
- Elimina los problemas de políticas conflictivas de múltiples jerarquías.

Control Group v2 es compatible con numerosos controladores. Algunos de los ejemplos son:

- El controlador de la CPU regula la distribución de los ciclos de la CPU. Este controlador implementa:
  - Modelos de peso y límite de ancho de banda absoluto para la política de programación normal.
  - Modelo de asignación de ancho de banda absoluto para la política de programación en tiempo real.

- El controlador cpuset limita la colocación del procesador y/o la memoria de los procesos sólo a los recursos mencionados que se especifican en los archivos de la interfaz **cpuset**.
- El controlador de memoria regula la distribución de la memoria. En la actualidad, se controlan los siguientes tipos de usos de la memoria:
  - Memoria de usuario: caché de página y memoria anónima.
  - Estructuras de datos del kernel como las dentrías y los inodos.
  - Búferes de socket TCP.
- El controlador de E/S regula la distribución de los recursos de E/S.
- El controlador de escritura interactúa con los controladores de memoria y de E/S y es específico de **Control Group v2**.

La información anterior se ha basado en la documentación de Control Group v2 upstream. Puede consultar el mismo enlace para obtener más información sobre controladores concretos de **Control Group v2**.

Tenga en cuenta que no todas las características mencionadas en el documento de la corriente ascendente están implementadas todavía en RHEL 8.

(BZ#1401552)

Aleatorización de las listas libres: Mejora del rendimiento y la utilización de la memoria lateral-cache de mapeo directo

Con esta mejora, se puede habilitar el asignador de páginas para aleatorizar las listas libres y mejorar la utilización media de una caché lateral de memoria de mapeo directo. La opción de línea de comandos del kernel **page_alloc.shuffle**, permite al asignador de páginas aleatorizar las listas libres y establece la bandera booleana a **True**. El archivo **sysfs**, que se encuentra en **/sys/module/page_alloc/parameters/shuffle** lee el estado de la bandera, baraja las listas libres, de manera que la memoria dinámica de acceso aleatorio (DRAM) se almacena en caché, y la banda de latencia entre la DRAM y la memoria persistente se reduce. Como resultado, se dispone de una memoria persistente de mayor capacidad y menor ancho de banda en las plataformas de servidor de propósito general.

(BZ#1620349)

La herramienta de espacio de usuario TPM se ha actualizado a la última versión

La herramienta de espacio de usuario **tpm2-tools** ha sido actualizada a la versión 3.2.1. Esta actualización proporciona varias correcciones de errores, en particular en relación con el código de registro de configuración de la plataforma y la limpieza de la página manual.

(BZ#1725714)

El chipset PCH de la serie C620 ahora es compatible con la función Intel Trace Hub

Esta actualización añade soporte de hardware para Intel Trace Hub (TH) en el Platform Controller Hub (PCH) de la serie C620, también conocido como Lewisburg PCH. Los usuarios con PCH de la serie C620 ahora pueden utilizar Intel TH.

(BZ#1714486)

La herramienta de **perfeccionamiento** ahora soporta la agregación de eventos por matriz para los procesadores CLX-AP y CPX

Con esta actualización, la herramienta **perf** ofrece ahora soporte para la agregación de recuentos de eventos por troquel para algunas CPU de Intel con múltiples troqueles. Para habilitar este modo, añada la opción **--per-die** además de la opción **-a** para los procesadores de sistema Xeon Cascade Lake-AP (CLX-AP) y Cooper Lake (CPX). Como resultado, esta actualización detecta cualquier desequilibrio entre los dies. El comando **perf stat** captura los recuentos de eventos y muestra la salida como:

```
# perf stat -e cycles --per-die -a -- sleep 1
 Performance counter stats for 'system wide':
S0-D0        8      21,029,877      cycles
S0-D1        8      19,192,372      cycles
```

(BZ#1660368)

El umbral de **crashkernel=auto** se reduce en IBM Z

El umbral inferior del parámetro de línea de comandos del kernel **crashkernel=auto** se reduce ahora de 4G a 1G en los sistemas IBM Z. Esta implementación permite que el IBM Z se alinee con el umbral de los sistemas AMD64 e Intel 64 para compartir la misma política de reserva en el umbral inferior de **crashkernel=auto**. Como resultado, el crashkernel es capaz de reservar automáticamente la memoria para **kdump** en sistemas con menos de 4GB de RAM.

(BZ#1780432)

La entrada del manual **numactl** aclara la salida del uso de la memoria

Con esta versión de RHEL 8, la página del manual de **numactl** menciona explícitamente que la información sobre el uso de la memoria refleja sólo las páginas residentes del sistema. El motivo de esta adición es eliminar la posible confusión de los usuarios sobre si la información de uso de la memoria se refiere a las páginas residentes o a la memoria virtual.

(BZ#1730738)

El documento **de kexec-tools** se ha actualizado para incluir la compatibilidad con el objetivo Kdump FCoE

En esta versión, se ha actualizado el archivo **/usr/share/doc/kexec-tools/supported-kdump-targets.txt** para incluir el soporte de Kdump Fibre Channel over Ethernet (FCoE). Como resultado, los usuarios ahora pueden tener una mejor comprensión del estado y los detalles del mecanismo de volcado de fallos de **kdump** en un soporte de objetivos FCoE.

(BZ#1690729)

El volcado asistido por el firmware ahora es compatible con PowerNV

El mecanismo de volcado asistido por el firmware**(fadump**) es ahora compatible con la plataforma PowerNV. La función es compatible con la versión de firmware IBM POWER9 FW941 y posteriores. En el momento del fallo del sistema, **fadump**, junto con el archivo **vmcore**, también exporta el archivo **opalcore**. El archivo **opalcore** contiene información sobre el estado de la memoria de OpenPOWER Abstraction Layer (OPAL) en el momento de la avería. El archivo **opalcore** es útil para depurar los fallos de los sistemas basados en OPAL.

(BZ#1524687)

el árbol de fuentes de**kernel-rt** ahora coincide con el último árbol de RHEL 8

Las fuentes de **kernel-rt** han sido actualizadas para utilizar el último árbol de fuentes del kernel RHEL. El conjunto de parches en tiempo real también se ha actualizado a la última versión v5.2.21-rt13. Ambas actualizaciones proporcionan una serie de correcciones de errores y mejoras.

(BZ#1680161)

rngd ahora puede ejecutarse con privilegios de no-root

El demonio generador de números aleatorios**(rngd**) comprueba si los datos suministrados por la fuente de aleatoriedad son suficientemente aleatorios y, a continuación, almacena los datos en la reserva de entropía de números aleatorios del kernel. Con esta actualización, **rngd** puede ejecutarse con privilegios de usuario no root para mejorar la seguridad del sistema.

(BZ#1692435)

La memoria virtual persistente es ahora compatible con RHEL 8.2 y posteriores en POWER 9

Cuando se ejecuta un host RHEL 8.2 o posterior con un hipervisor PowerVM en hardware IBM POWER9, el host puede ahora utilizar la función de memoria virtual persistente (vPMEM). Con vPMEM, los datos persisten a través de los reinicios de aplicaciones y particiones hasta que el servidor físico se apaga. Como resultado, el reinicio de las cargas de trabajo que utilizan vPMEM es significativamente más rápido.

Los siguientes requisitos deben cumplirse para que su sistema pueda utilizar vPMEM:

- Consola de gestión de hardware (HMC) V9R1 M940 o posterior
- Nivel de firmware FW940 o posterior
- Firmware del sistema E980 FW940 o posterior
- Firmware del sistema L922 FW940 o posterior
- Nivel de PowerVM V3.1.1

Tenga en cuenta que actualmente se producen varios problemas conocidos en RHEL 8 con vPMEM. Para más detalles, consulte los siguientes artículos de la base de conocimientos:

- La conexión/desconexión en caliente de la memoria pmem puede provocar el pánico del kernel en POWER9
- El arranque del kernel de captura tarda mucho tiempo utilizando los espacios de nombres vPMEM como objetivo de volcado para kdump/fadump

(BZ#1859262)

5.8. SISTEMAS DE ARCHIVOS Y ALMACENAMIENTO

LVM ahora soporta el método de caché dm-writecache

Los volúmenes de caché LVM ahora proporcionan el método de caché **dm-writecache** además del método existente **dm-cache**.

dm-cache

Este método acelera el acceso a los datos de uso frecuente al almacenarlos en caché en el volumen más rápido. El método almacena en caché tanto las operaciones de lectura como las de escritura.

dm-writecache

Este método sólo almacena en caché las operaciones de escritura. El volumen más rápido, normalmente un SSD o un disco de memoria persistente (PMEM), almacena primero las operaciones de escritura y luego las migra al disco más lento en segundo plano.

Para configurar el método de almacenamiento en caché, utilice la opción **--type cache** o **--type writecache** con la utilidad **lvconvert**.

Para obtener más información, consulte Activación del almacenamiento en caché para mejorar el rendimiento del volumen lógico.

(BZ#1600174)

La política asíncrona de VDO es ahora compatible con ACID

Con esta versión, el modo de escritura **asíncrono** de VDO es ahora compatible con Atomicidad, Consistencia, Aislamiento y Durabilidad (ACID). Si el sistema se detiene inesperadamente mientras VDO está escribiendo datos en modo **asíncrono**, los datos recuperados son ahora siempre consistentes.

Debido al cumplimiento de ACID, el rendimiento de **async** es ahora menor en comparación con la versión anterior. Para restablecer el rendimiento original, puede cambiar el modo de escritura de su volumen VDO al modo **async-unsafe**, que no es compatible con ACID.

Para más información, consulte Seleccionar un modo de escritura VDO .

(BZ#1657301)

Ahora puede importar volúmenes VDO

La utilidad **vdo** ahora le permite importar volúmenes VDO existentes que actualmente no están registrados en su sistema. Para importar un volumen VDO, utilice el comando **vdo import**.

Además, puede modificar el Identificador Único Universal (UUID) de un volumen VDO utilizando el comando **vdo import**.

(BZ#1713749)

El nuevo contador de errores por operación está ahora disponible en la salida de mountstats y nfsiostat

Una característica menor de soporte está disponible para los sistemas cliente NFS: la salida de los comandos **mountstats** y **nfsiostat** en **nfs-utils** tienen un conteo de errores **por** operación. Esta mejora permite que estas herramientas muestren los recuentos y porcentajes de errores **por** operación que pueden ayudar a reducir los problemas en puntos de montaje NFS específicos en una máquina cliente NFS. Tenga en cuenta que estas nuevas estadísticas dependen de los cambios del kernel que están dentro del kernel de Red Hat Enterprise Linux 8.2.

(BZ#1719983)

Las IOs de escritura con conocimiento de cgroup están ahora disponibles en XFS

Con esta versión, XFS soporta IOs de escritura con conciencia de **cgroup**. En general, el writeback de **cgroups** requiere soporte explícito del sistema de archivos subyacente. Hasta ahora, las IOs de writeback en XFS eran el atributo para el **cgroup** raíz solamente.

(BZ#1274406)

Los sistemas de archivos FUSE ahora implementan copy_file_range()

La llamada al sistema **copy_file_range()** proporciona una forma de que los sistemas de archivos implementen un mecanismo eficiente de copia de datos. Con esta actualización, GlusterFS, que utiliza el marco de trabajo Filesystem in Userspace (FUSE) aprovecha este mecanismo. Dado que la funcionalidad de lectura/escritura de los sistemas de archivos FUSE implica múltiples copias de datos, el uso de **copy_file_range** () puede mejorar significativamente el rendimiento.

(BZ#1650518)

Los comandos mountstats y nfsiostat ya soportan las estadísticas por operación

Una característica de soporte está ahora disponible para los sistemas cliente NFS: el archivo **/proc/self/mountstats** tiene el contador de errores **por** operación. Con esta actualización, en cada fila de estadísticas por **operación**, el noveno número indica el número de operaciones que se han completado con un valor de estado inferior a cero. Este valor de estado indica un error. Para obtener más información, consulte las actualizaciones de los programas **mountstats** y **nfsiostat** en **nfs-utils** que muestran estos nuevos recuentos de errores.

(BZ#1636572)

Las nuevas estadísticas de montaje lease_time y lease_expired están disponibles en el archivo /proc/self/mountstats

Existe una función de soporte para los sistemas cliente NFSv4.x. El archivo **/proc/self/mountstats** tiene los campos **lease_time** y **lease_expired** al final de la línea que comienza con **nfsv4:**. El campo **lease_time** indica el número de segundos del tiempo de arrendamiento NFSv4. El campo **lease_expired** indica el número de segundos desde que el arrendamiento ha expirado, o 0 si el arrendamiento no ha expirado.

(BZ#1727369)

5.9. ALTA DISPONIBILIDAD Y CLUSTERS

Nuevas opciones de comando para desactivar un recurso sólo si esto no afectaría a otros recursos

A veces es necesario desactivar recursos sólo si esto no tiene efecto sobre otros recursos. Asegurarse de que este sea el caso puede ser imposible de hacer a mano cuando se establecen relaciones complejas de recursos. Para responder a esta necesidad, el comando **pcs resource disable** ahora soporta las siguientes opciones:

- **pcs resource disable --simulate**: muestra los efectos de desactivar los recursos especificados sin cambiar la configuración del cluster
- **pcs resource disable --safe**: desactiva los recursos especificados sólo si ningún otro recurso se vería afectado de alguna manera, como por ejemplo si se migra de un nodo a otro
- **pcs resource disable --safe --no-strict**: desactiva los recursos especificados sólo si no se detienen o degradan otros recursos

Además, se ha introducido el comando pcs **resource safe-disable** como alias de **pcs resource disable --safe**.

(BZ#1631519)

Nuevo comando para mostrar las relaciones entre los recursos

El nuevo comando **pcs resource relations** permite visualizar las relaciones entre los recursos del cluster en una estructura de árbol.

(BZ#1631514)

Nuevo comando para mostrar el estado de un clúster de sitio primario y de sitio de recuperación

Si ha configurado un clúster para utilizarlo como sitio de recuperación, ahora puede configurar ese clúster como un clúster de sitio de recuperación con el comando **pcs** dr. A continuación, puede utilizar el comando **pcs** dr para mostrar el estado del clúster del sitio primario y del clúster del sitio de recuperación desde un único nodo.

(BZ#1676431)

Las restricciones de recursos caducadas se ocultan ahora por defecto al enumerar las restricciones

El listado de restricciones de recursos ya no muestra por defecto las restricciones caducadas. Para incluir las restricciones caducadas, utilice la opción **--all** del comando **pcs constraint**. De este modo, se listarán las restricciones caducadas, anotando las restricciones y sus reglas asociadas como **(caducadas)** en la pantalla.

(BZ#1442116)

Compatibilidad con Pacemaker para configurar los recursos para que permanezcan detenidos en caso de apagado limpio del nodo

Cuando un nodo del clúster se apaga, la respuesta por defecto de Pacemaker es detener todos los recursos que se ejecutan en ese nodo y recuperarlos en otro lugar. Algunos usuarios prefieren tener una alta disponibilidad sólo para los fallos, y tratar los apagados limpios como interrupciones programadas. Para solucionar esto, Pacemaker ahora admite las propiedades de cluster **shutdown-lock** y **shutdown-lock-limit** para especificar que los recursos activos en un nodo cuando se apaga deben permanecer detenidos hasta que el nodo se vuelva a unir. Los usuarios pueden ahora utilizar los apagados limpios como interrupciones programadas sin ninguna intervención manual. Para obtener información sobre cómo configurar los recursos para que permanezcan detenidos en un cierre limpio de nodo, consulte el enlace: Configurar los recursos para que permanezcan detenidos en un apagado de nodo limpio.

(BZ#1712584)

Soporte para ejecutar el entorno de cluster en un solo nodo

Un clúster con un solo miembro configurado ahora puede iniciar y ejecutar recursos en un entorno de clúster. Esto permite a un usuario configurar un sitio de recuperación de desastres separado para un clúster de varios nodos que utiliza un solo nodo para la copia de seguridad. Tenga en cuenta que un clúster con un solo nodo no es en sí mismo tolerante a fallos.

(BZ#1700104)

5.10. LENGUAJES DE PROGRAMACIÓN DINÁMICOS, SERVIDORES WEB Y DE BASES DE DATOS

Un nuevo módulo: python38

RHEL 8.2 introduce Python 3.8, proporcionado por el nuevo módulo **python38** y la imagen del contenedor **ubi8/python-38**.

Entre las mejoras notables en comparación con Python 3.6 se incluyen:

- Nuevos módulos de Python, por ejemplo, **contextvars**, **dataclasses** o **importlib.resources**
- Nuevas características del lenguaje, como las expresiones de asignación (el llamado operador morsa, **:=**) o los parámetros sólo posicionales
- Mejora de la experiencia del desarrollador con la función incorporada **breakpoint()**, la especificación de la cadena de formato **=** y la compatibilidad entre las compilaciones de depuración y no depuración de Python y los módulos de extensión
- Mejoras en el rendimiento
- Mejora de la compatibilidad con las sugerencias de tipo estático opcionales
- Adición del especificador **=** a los literales de cadena formateados (cadenas f) para facilitar la depuración
- Versiones actualizadas de paquetes, como **pip**, **requests** o **Cython**

Python 3.8 y los paquetes creados para él pueden instalarse en paralelo con Python 3.6 en el mismo sistema.

Tenga en cuenta que el módulo **python38** no incluye los mismos enlaces binarios a las herramientas del sistema (RPM, DNF, SELinux y otras) que se proporcionan para el módulo **python36**.

Para instalar paquetes del módulo **python38**, utilice, por ejemplo

```
# yum install python38
# yum install python38-Cython
```

El flujo del módulo **python38:3.8** se habilitará automáticamente.

Para ejecutar el intérprete, utilice, por ejemplo:

```
$ python3.8
$ python3.8 -m cython --help
```

Para más información, consulte Uso de Python.

Tenga en cuenta que Red Hat seguirá proporcionando soporte para Python 3.6 hasta el final de la vida de RHEL 8. Python 3.8 tendrá un ciclo de vida más corto, véase el ciclo de vida de RHEL 8 Application Streams.

(BZ#1747329)

Cambios en la instalación de mod_wsgi

Anteriormente, cuando el usuario intentaba instalar el módulo **mod_wsgi** mediante el comando **yum install mod_wsgi**, siempre se instalaba el paquete **python3-mod_wsgi**. RHEL 8.2 introduce Python 3.8 como complemento de Python 3.6. Con esta actualización, es necesario especificar qué versión de **mod_wsgi** se quiere instalar, de lo contrario se devuelve un mensaje de error.

Para instalar la versión Python 3.6 de **mod_wsgi**:

```
# yum install python3-mod_wsgi
```

Para instalar la versión de Python 3.8 de **mod_wsgi**:

```
# yum install python38-mod_wsgi
```

Tenga en cuenta que los paquetes **python3-mod_wsgi** y **python38-mod_wsgi** entran en conflicto entre sí, y que sólo se puede instalar un módulo **mod_wsgi** en un sistema debido a una limitación del servidor HTTP Apache.

Este cambio introdujo un problema conocido de dependencia descrito en BZ#1829692.

(BZ#1779705)

Soporte para deflate acelerado por hardware en zlib en IBM Z

Esta actualización añade soporte para un algoritmo de deflación acelerado por hardware a la biblioteca **zlib** en los mainframes IBM Z. Como resultado, se ha mejorado el rendimiento de la compresión y la descompresión en las máquinas vectoriales IBM Z.

(BZ#1659433)

Mejora del rendimiento al descomprimir gzip en IBM Power Systems, little endian

Esta actualización añade una optimización para la comprobación de redundancia cíclica de 32 bits (CRC32) a la biblioteca **zlib** en IBM Power Systems, little endian. Como resultado, se ha mejorado el rendimiento de la descompresión de archivos **gzip**.

(BZ#1666798)

Un nuevo flujo de módulos: maven:3.6

RHEL 8.2 introduce un nuevo flujo de módulos, **maven**:3.6. Esta versión de la herramienta de gestión y comprensión de proyectos de software Maven proporciona numerosas correcciones de errores y varias mejoras respecto a la corriente maven:3 **.5** distribuida con RHEL 8.0.

Para instalar el flujo **maven:3.6**, utilice:

```
# yum module install maven:3.6
```

Si desea actualizar desde el flujo **maven:3.5**, consulte Cambiar a un flujo posterior .

(BZ#1783926)

mod_md ahora soporta el protocolo ACMEv2

El módulo **mod_md** ha sido actualizado a la versión 2.0.8. Esta actualización añade una serie de características, en particular la compatibilidad con la versión 2 del protocolo de emisión y gestión de certificados del Entorno de Gestión Automática de Certificados (ACME), que es el estándar del Grupo de Trabajo de Ingeniería de Internet (IETF) (RFC 8555). El protocolo original ACMEv1 sigue siendo compatible, pero está obsoleto para los proveedores de servicios más populares.

(BZ#1747923)

Nuevas extensiones para PHP 7.3

El flujo de módulos de **php:7.3** ha sido actualizado para proporcionar dos nuevas extensiones de PHP: **rrd** y **Xdebug**.

La extensión **rrd** proporciona enlaces a la biblioteca **RRDtool** C. **RRDtool** es un sistema de registro de datos y gráficos de alto rendimiento para datos de series temporales.

La extensión **Xdebug** se incluye para ayudarle con la depuración y el desarrollo. Tenga en cuenta que la extensión se proporciona únicamente con fines de desarrollo y no debe utilizarse en entornos de producción.

Para obtener información sobre la instalación y el uso de PHP en RHEL 8, consulte Uso del lenguaje de scripting PHP.

(BZ#1769857, BZ#1764738)

Nuevos paquetes: perl-LDAP y perl-Convert-ASN1

Esta actualización añade los paquetes **perl-LDAP** y **Perl-Convert-ASN1** a RHEL 8. El paquete **perl-LDAP** proporciona un cliente LDAP para el lenguaje Perl. **perl-LDAP** requiere el paquete **perl-Convert-ASN1**, que codifica y descodifica las estructuras de datos de la Notación de Sintaxis Abstracta Uno (ASN.1) utilizando Reglas de Codificación Básica (BER) y Reglas de Codificación Distinguida (DER).

(BZ#1663063, BZ#1746898)

sscg ahora soporta la generación de archivos de claves privadas protegidas por una contraseña

La utilidad **sscg** es ahora capaz de generar archivos de claves privadas protegidas por una contraseña. Esto añade otro nivel de protección para las claves privadas, y es requerido por algunos servicios, como FreeRADIUS.

(BZ#1717880)

5.11. COMPILADORES Y HERRAMIENTAS DE DESARROLLO

grafana rebasado a la versión 6.3.6

El paquete **grafana** ha sido actualizado a la versión 6.3.6, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Base de datos: Reescribe la consulta de las estadísticas del sistema para mejorar el rendimiento.
- Explora:
  - Se corrige el diseño de los campos de consulta en la vista dividida para los navegadores Safari.
  - Añade la opción Live para las fuentes de datos soportadas, añade el **orgId** a la URL para compartirla.
  - Añade soporte para los nuevos parámetros de **inicio** y **fin** de **loki** para el punto final de las etiquetas.
  - Añade soporte para alternar el modo de consulta sin procesar en el Explore, lo que permite cambiar entre las métricas y los registros.
  - Muestra el contexto de las líneas de registro, no analiza los niveles de registro si se proporcionan por campo o etiqueta.
  - Soporta la nueva sintaxis de filtrado **LogQL**.

    - Utiliza el nuevo **TimePicker** de Grafana/UI.
    - Maneja las nuevas líneas en el Resaltador de **Filas**.
    - Arregla la navegación de vuelta al panel del tablero.
    - Se corrige el filtro por nivel de serie en el gráfico de registros.
    - Corregir problemas cuando se carga y el gráfico/tabla está colapsado.
    - Corrige la selección/copia de líneas de registro.

- Cuadro de mando: Corrige el error de carga **del init de** los cuadros de mando con enlaces a paneles a los que les faltaban propiedades, y corrige la configuración de la zona horaria del cuadro de mando al exportar a los valores separados por comas (CSV) Enlaces de datos.
- Editor: Se ha corregido un problema por el que sólo se copiaban líneas enteras.
- LDAP: Integración de los componentes de autenticación **multi ldap** y **ldap**.
- Perfil/UserAdmin: Corrige el parser del agente de usuario que bloquea el **servidor de grafana** en las versiones de 32 bits.
- Prometeo:
    - Evita que el editor de paneles se cuelgue al cambiar a la fuente de datos **de Prometheus**, cambia el comportamiento de **inserción de corchetes** para que sea menos molesto.
    - Corrige las consultas con el **label_replace** y elimina la coincidencia de $1 al cargar el editor de consultas.
    - Permite de forma consistente las consultas de varias líneas en el editor, teniendo en cuenta la zona horaria para la alineación de los pasos.
    - Utiliza el rango del panel anulado para **$__range** en lugar del rango del tablero.
    - Añade un filtro de rango de tiempo a la consulta de las etiquetas de las series, escapa a los literales **|** en las variables interpoladas **de PromQL**.
    - Correcciones al añadir etiquetas para las métricas que contienen dos puntos en el Explore.
- Automatización: Permite la caducidad de las claves de la API, devuelve el dispositivo, el sistema operativo y el navegador al enumerar los tokens de autenticación del usuario en la API HTTP, admite la lista y la revocación de los tokens de autenticación del usuario en la interfaz de usuario.
- Enlaces de datos: Aplica correctamente las variables de ámbito a los enlaces de datos, sigue la zona horaria al mostrar la marca de tiempo del punto de datos en el menú contextual del gráfico, utiliza correctamente la marca de tiempo del punto de datos al interpolar las variables, corrige la interpolación incorrecta del **${__nombre_de_serie}**.
- Gráfico: Corrige el problema de la leyenda al hacer clic en el icono de la línea de la serie y el problema de la barra de desplazamiento horizontal que es visible en las ventanas, añade una nueva opción de relleno del gradiente.
- Grafito: Evita el glob de las variables de matriz de un solo valor, corrige problemas con la función de alias que se mueve en último lugar, corrige el problema con la **serieByTag**

- Series de tiempo: Asume que los valores son todos números.
- Gauge/BarGauge: Se corrige un problema de pérdida de umbrales y un problema de carga de Gauge con la estadística **avg**.
- Enlaces del panel: Se ha corregido el problema de bloqueo del indicador
- OAuth: Corrige el fallo de inicio de sesión de OAuth **en estado guardado** debido a la política de cookies de SameSite, corrige el token de usuario erróneo actualizado en la actualización de **OAuth** en el proxy DS.
- Auth Proxy: Incluye cabeceras adicionales como parte de la clave de la caché.
- **cli**: Arreglo para reconocer cuando está en modo dev, arregla el problema de **encriptar-fuente-de-datos-contraseñas** fallando con el error sql.
- Permisos: Mostrar los plugins en la navegación para los usuarios que no son administradores, pero oculta la configuración de los plugins.
- TimePicker: Aumenta la altura máxima del desplegable de rango rápido y corrige un problema de estilo para el popover de rango personalizado.
- Loki: Muestra los registros de cola en vivo en el orden correcto en el Explore.
- Rango de tiempo: Se corrige un error por el que los rangos de tiempo personalizados no seguían la Hora Universal Coordinada (UTC).
- **remote_cache**: Arregla el parsing de **connstr de redis**.
- Alertas: Añadir etiquetas a las reglas de alerta, intentos de enviar notificaciones por correo electrónico a todas las direcciones de correo electrónico dadas, mejora de las pruebas de las reglas de alerta, soporte para configurar el campo de contenido para el notificador de alerta **de Discord**.
- Gestor de alertas: Sustituye los caracteres ilegales por guiones bajos en los nombres de las etiquetas.
- AzureMonitor: Cambia las variables integradas en Grafana que chocan o los nombres de las macros para los Azure Logs.
- CloudWatch: Hecha la región visible para Amazon Web Services (AWS) Cloudwatch Expressions, añade las métricas de AWS **DocDB**.
- GraphPanel: No ordenar las series cuando la tabla de leyenda y la columna de ordenación no son visibles.
- InfluxDB: Permite visualizar los registros en el Explore.
- MySQL/Postgres/MSSQL: Añade el análisis de intervalos de días, semanas y años en las macros, añade soporte para recargar periódicamente los certificados de los clientes.
- Plugins: Reemplaza la lista de **dataFormats** con la bandera **skipDataQuery** en el archivo **plugin.json**.
- Refrescar el selector: Maneja los intervalos vacíos.
- Singlestat: Añade la configuración **y** min/max a los sparklines singlestat.

- Plantillas: Muestra correctamente el **__texto** en la variable multivalor después de recargar la página, soporta la selección de todos los valores filtrados de una variable multivalor.
- Frontend: Corrige el problema del componente de árbol Json que no funciona.
- InfluxDB: Corrige los problemas de las comillas simples no escapadas en los filtros de valores de las etiquetas.
- Config: Corrige la opción **connectionstring** para el **remote_cache** en el archivo **defaults.ini**.
- Elasticsearch: Corrige la consulta vacía (a través de la variable de plantilla) debe ser enviada como comodín, corrige el máximo de solicitudes concurrentes de shard por defecto, soporta la visualización de los registros en el Explore.
- TablePanel: Arregla la visualización de las anotaciones.
- Grafana-CLI: Corrige la recepción de banderas a través de la línea de comandos, el wrapper para el **grafana-cli** dentro de los paquetes **RPM**/**DEB** y **config**/**homepath** son ahora banderas globales.
- HTTPServer: Corrige el formato de la cabecera **X-XSS-Protection**, las opciones para devolver las nuevas cabeceras **X-Content-Type-Options**, **X-XSS-Protection** y **Strict-Transport-Security**, corrige la cabecera **Strict-Transport-Security**, sirve a Grafana con un prefijo de ruta URL personalizado.

(BZ#1725278)

pcp rebasado a la versión 5.0.2

El paquete **pcp** ha sido actualizado a la versión 5.0.2, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- Los paquetes **pcp-webapp-*** son ahora reemplazados por el paquete **grafana-pcp** y **pmproxy**.
- La herramienta **pcp-collectl** se sustituye ahora por las configuraciones **pmrep**.
- Nuevos y mejorados agentes del dominio de la métrica del rendimiento (PMDA):
  - **pmdamssql**: Nueva implementación de PMDA para Microsoft SQL Server.
  - **pmdanetcheck**: Nuevo PMDA para realizar comprobaciones de red.
  - **pmdaopenmetrics**: Cambia el nombre del agente **prometheus** por el de **openmetrics**.
  - **pmdanfsclient**: Añade las métricas de error **rpc por operación** y **por montaje**.
  - **pmdalmsensors**: Mejoras en el parsing de nombres y en el manejo de errores.
  - **pmdaperfevent**: Soporta eventos de nido **hv_24x7** en el sistema multinodal.
  - **pmdalinux**:
    - Maneja correctamente los nodos numa dispersos o discontinuos.
    - Utiliza **el nombre de** la cpu y no el **instid** para las estadísticas numa **por cpu**.
    - Añade una losa activa y total al análisis sintáctico de **slabinfo** v2

        - Corrige varios socket unix, **icmp6** métricas, hugepage valor de la métrica. cálculos, **segfault** en el código de interrupciones con grandes cuentas de la CPU
        - Obtiene más métricas de red en el espacio de nombres **--container**.
    - **pmdabcc**: Corrige el módulo tracepoints para las versiones **bcc** 0.10.0 y superiores
    - **pmdabpftrace**: Nuevo PMDA para las métricas de los scripts **bpftrace**
    - **pmdaproc**:
        - Corrige la pérdida de memoria en el refresco de **la lista de pedidos**.
        - Evita el exceso de llamadas a las estadísticas en **cgroups_scan**.
        - Conserva las rutas de **los cgroups** y sólo desescape los nombres de las instancias.
    - **pmdaroot**: Mejora el manejo del comportamiento del **cgroup** en caché o inactivo y refresca el **indom** del contenedor en el cambio de fs **del cgroup** también.
- Correcciones en las herramientas del colector (servidor):
    - **pmproxy**: Soporte de Openmetrics a través del endpoint **/metrics**, consolida la API REST **de pmseries/grafana**, y añade una nueva implementación de la API REST asíncrona **PMWEBAPI(3)**.
    - **selinux**: Numerosas actualizaciones de la política de pcp.
    - python **pmdas**: Habilita el soporte de autenticación, nuevo método **set_comm_flags** para establecer las banderas de comunicación.
    - **api de python**: Exporta el **pmdaGetContext()** y añade una envoltura de depuración.
    - **perl api**: Asegura la configuración del contexto para el almacén PMDA como con el wrapper de python.
    - **systemd**: Añade un tiempo de espera de 120s en todos los servicios y corrige el fallo al iniciar el servicio **pmlogger**.
- Correcciones en las herramientas de análisis (cliente):
    - **pmchart**: Corrige el autoescalado del gráfico en condiciones de error de obtención.
    - **pmrep**: Corrige la **fórmula wait.** para **collectl-dm-sD** y **collectl-sD**.
    - **pmseries**: Proporciona soporte para la palabra clave delta y mejores marcas de tiempo.
    - **pcp-atop**: Corrige el modo de escritura **(-w**) para manejar las métricas **proc** vs **hotproc**.
    - **pcp-atopsar**: Corrige el mal manejo de algunos argumentos de la línea de comandos.
    - **pcp-dstat**: Corrige las cabeceras desalineadas en la salida CSV y el manejo de la opción de línea de comandos **--bits**.
    - **libpcp**: Corrige el **segv** de **cockpit-pcp** con el contexto local y el manejo de errores de repetición de archivos múltiples para los archivos corruptos.

(BZ#1723598)

grafana-pcp ya está disponible en RHEL 8.2

El paquete **grafana-pcp** proporciona nuevas fuentes de datos de **grafana** y plugins de aplicación que conectan **PCP** con **grafana**. Con el paquete **grafana-pcp**, puede analizar las métricas históricas de **PCP** y las métricas de **PCP** en tiempo real utilizando el lenguaje de consulta **pmseries** y los servicios en vivo **pmwebapi** respectivamente. Para obtener más información, consulte Performance Co-Pilot Grafana Plugin.

(BZ#1685315)

Actualización del conjunto de herramientas GCC 9

GCC Toolset 9 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**.

Entre los cambios notables introducidos con RHEL 8.2 se incluyen:

- El compilador GCC ha sido actualizado a la versión 9.2.1, que proporciona muchas correcciones de errores y mejoras que están disponibles en GCC upstream.
- Los componentes de GCC Toolset 9 ya están disponibles en las dos imágenes de contenedores:
  - **rhel8/gcc-toolset-9-toolchain**, que incluye el compilador GCC, el depurador GDB y la herramienta de automatización **make**.
  - **rhel8/gcc-toolset-9-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/<image_name>
    ```

Las siguientes herramientas y versiones son proporcionadas por GCC Toolset 9:

Herramienta	Versión
GCC	9.2.1
GDB	8.3
Valgrind	3.15.0
SystemTap	4.1
Dyninst	10.1.0
binutils	2.32
elfutils	0.176
dwz	0.12

Herramienta	Versión
hacer	4.2.1
strace	5.1
ltrace	0.7.91
annobin	9.08

Para instalar GCC Toolset 9, ejecute el siguiente comando como root:

```
# yum install gcc-toolset-9
```

Para ejecutar una herramienta de GCC Toolset 9:

```
$ scl enable gcc-toolset-9 tool
```

Para ejecutar una sesión de shell en la que las versiones de las herramientas de GCC Toolset 9 tienen prioridad sobre las versiones del sistema de estas herramientas:

```
$ scl enable gcc-toolset-9 bash
```

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

(BZ#1789401)

GCC Toolset 9 ahora soporta la descarga de objetivos NVIDIA PTX

El compilador GCC en GCC Toolset 9 ahora soporta la descarga de objetivos OpenMP para NVIDIA PTX.

(BZ#1698607)

El compilador GCC actualizado ya está disponible para RHEL 8.2

El compilador GCC del sistema, versión 8.3.1, se ha actualizado para incluir numerosas correcciones de errores y mejoras disponibles en el GCC upstream.

La colección de compiladores de GNU (GCC) proporciona herramientas para desarrollar aplicaciones con los lenguajes de programación C, C , y Fortran.

Para obtener información de uso, consulte Desarrollo de aplicaciones C y C en RHEL 8 .

(BZ#1747157)

Un nuevo sintonizador para cambiar el tamaño máximo de fastbin en glibc

La función **malloc** utiliza una serie de fastbins que contienen trozos de memoria reutilizables hasta un tamaño determinado. El tamaño máximo de los trozos por defecto es de 80 bytes en sistemas de 32 bits y de 160 bytes en sistemas de 64 bits. Esta mejora introduce un nuevo ajuste **glibc.malloc.mxfast** en **glibc** que permite cambiar el tamaño máximo de los fastbins.

(BZ#1764218)

La biblioteca matemática vectorial está ahora habilitada para GNU Fortran en GCC Toolset 9

Con esta mejora, GNU Fortran de GCC Toolset puede ahora utilizar rutinas de la biblioteca matemática vectorizada **libmvec**. Anteriormente, el compilador de Fortran en GCC Toolset necesitaba un archivo de cabecera de Fortran antes de poder utilizar las rutinas de **libmvec** proporcionadas por la biblioteca de C de GNU **glibc**.

(BZ#1764238)

Se ha mejorado el ajuste de glibc.malloc.tcache

La variable de ajuste glibc.malloc. **tcache_count** permite establecer el número máximo de trozos de memoria de cada tamaño que se pueden almacenar en la caché por hilo (tcache). Con esta actualización, el límite superior de la sintonizable glibc.malloc **.tcache_count** se ha incrementado de 127 a 65535.

(BZ#1746933)

El cargador dinámico de glibc se ha mejorado para proporcionar un mecanismo de precarga de bibliotecas no heredado

Con esta mejora, ahora se puede invocar el cargador para cargar un programa de usuario con una opción **--preload** seguida de una lista de bibliotecas a precargar separada por dos puntos. Esta característica permite a los usuarios invocar sus programas directamente a través del cargador con una lista de precarga de bibliotecas no heredada.

Anteriormente, los usuarios tenían que utilizar la variable de entorno LD_PRELOAD que era heredada por todos los procesos hijos a través de su entorno.

(BZ#1747453)

GDB ahora soporta la extensión ARCH(13) en la arquitectura IBM Z

Con esta mejora, el depurador de GNU (GDB) soporta ahora las nuevas instrucciones implementadas por la extensión ARCH(13) en la arquitectura IBM Z.

(BZ#1768593)

elfutils rebasado a la versión 0.178

El paquete **elfutils** ha sido actualizado a la versión 0.178, que proporciona múltiples correcciones de errores y mejoras. Los cambios más destacados son:

- **elfclassify**: una nueva herramienta para analizar objetos ELF.
- **debuginfod**: un nuevo servidor, herramienta cliente y biblioteca para indexar y obtener automáticamente ELF, DWARF y fuentes de archivos y archivos RPM a través de HTTP.
- **libebl** se compila ahora directamente en **libdw.so**.
- **eu-readelf** tiene múltiples banderas nuevas para las notas, la numeración de secciones y las tablas de símbolos.
- **libdw** ha mejorado el soporte multihilo.
- **libdw** soporta extensiones GNU DWARF adicionales.

(BZ#1744992)

SystemTap rebasado a la versión 4.2

La herramienta de instrumentación SystemTap ha sido actualizada a la versión 4.2. Las mejoras más destacadas son:

- Ahora, el seguimiento puede incluir los nombres de los archivos de origen y los números de línea.
- Ya están disponibles numerosas extensiones del back-end del Berkeley Packet Filter (BPF), por ejemplo, para los procesos de bucle, temporización y otros.
- Está disponible un nuevo servicio para gestionar los scripts de SystemTap. Este servicio envía métricas a un sistema de supervisión compatible con Prometheus.
- SystemTap ha heredado la funcionalidad de un nuevo servidor de archivos HTTP para **elfutils** llamado **debuginfod**. Este servidor envía automáticamente recursos de depuración a SystemTap.

(BZ#1744989)

Mejoras en los contadores de rendimiento de la serie Z de IBM

Las máquinas IBM serie Z tipo 0x8561, 0x8562 y 0x3907 (z14 ZR1) son ahora reconocidas por **libpfm**. Ahora están disponibles los eventos de rendimiento para supervisar las operaciones de criptografía de curva elíptica (ECC) en la serie Z de IBM. Esto permite la monitorización de subsistemas adicionales en máquinas de la serie Z de IBM.

(BZ#1731019)

Conjunto de herramientas de Rust rebasado a la versión 1.41

Rust Toolset ha sido actualizado a la versión 1.41. Los cambios más destacados son:

- La implementación de nuevos rasgos es ahora más fácil porque la regla de orfandad es menos estricta.
- Ahora puede adjuntar el atributo **#[non_exhaustive]** a una **estructura**, un **enum** o variantes de **enum**.
- El uso de **Box<T>** en el Foreign Function Interface (FFI) tiene ahora más garantías. **Box<T>** tendrá el mismo Application Binary Interface (ABI) que un puntero **T*** en el FFI.
- Se supone que Rust detecta errores de seguridad de memoria en tiempo de compilación, pero el anterior verificador de préstamos tenía limitaciones y permitía comportamientos indefinidos y falta de seguridad de memoria. El nuevo verificador de préstamos de vidas no léxicas (NLL) puede reportar problemas de inseguridad de memoria como errores duros. Ahora se aplica a las ediciones de Rust 2015 y Rust 2018. Anteriormente, en Rust 2015 el verificador de préstamos NLL sólo lanzaba advertencias sobre estos problemas.

Para instalar el módulo **rust-toolset**, ejecute el siguiente comando como root:

```
# yum module install rust-toolset
```

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

(BZ#1776847)

El conjunto de herramientas LLVM se ha actualizado a la versión 9.0.1

El conjunto de herramientas LLVM ha sido actualizado a la versión 9.0.1. Con esta actualización, ahora se soportan las sentencias **asm goto**. Este cambio permite compilar el kernel de Linux en las arquitecturas AMD64 e Intel 64.

Para instalar el módulo **llvm-toolset**, ejecute el siguiente comando como root:

```
# yum module install llvm-toolset
```

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

(BZ#1747139)

Go Toolset rebasado a la versión 1.13

Go Toolset ha sido actualizado a la versión 1.13. Las mejoras más destacadas son:

- Ahora Go puede utilizar un módulo criptográfico certificado por FIPS cuando el sistema RHEL se inicia en el modo FIPS. Los usuarios pueden habilitar este modo manualmente utilizando la variable de entorno **GOLANG_FIPS=1**.
- El depurador Delve, versión 1.3.2, ya está disponible para Go. Es un depurador a nivel de código fuente para el lenguaje de programación Go**(golang**).

Para instalar el módulo **go-toolset**, ejecute el siguiente comando como root:

```
# yum module install go-toolset
```

Para instalar el depurador Delve, ejecute el siguiente comando como root:

```
# yum install delve
```

Para depurar un programa **helloworld.** go utilizando Delve, ejecute el siguiente comando:

```
$ dlv debug helloworld.go
```

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

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

(BZ#1747150)

OpenJDK ahora también soporta secp256k1

Anteriormente, Open Java Development Kit (OpenJDK) sólo podía utilizar curvas de la biblioteca NSS. En consecuencia, OpenJDK sólo proporcionaba las curvas secp256r1, secp384r1 y secp521r1 para la criptografía de curva elíptica (ECC). Con esta actualización, OpenJDK utiliza la implementación interna de ECC y soporta también la curva secp256k1.

(BZ#1746875, BZ#1746879)

5.12. GESTIÓN DE LA IDENTIDAD

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 **ipauser** automatiza la adición y eliminación de usuarios.
- El módulo **ipagroup** automatiza la adición y eliminación de usuarios y grupos de usuarios a y desde grupos de usuarios.
- El módulo **ipahost** automatiza la adición y eliminación de hosts.
- El módulo **ipahostgroup** automatiza la adición y eliminación de hosts y grupos de hosts a y desde grupos de hosts.
- El módulo **ipasudorule** automatiza la gestión del comando **sudo** y la regla **sudo**.
- El módulo **ipapwpolicy** automatiza la configuración de las políticas de contraseñas en IdM.
- El módulo **ipahbacrule** automatiza la gestión del control de acceso basado en host en IdM.

Tenga en cuenta que puede combinar dos o más llamadas a **ipauser** en una sola con la variable **users** o, alternativamente, utilizar un archivo JSON que contenga los usuarios. Del mismo modo, puede combinar dos o más llamadas a **ipahost** en una sola con la variable **hosts** o, alternativamente, utilizar un archivo JSON que contenga los hosts. El módulo **ipahost** también puede asegurar la presencia o ausencia de varias direcciones IPv4 e IPv6 para un host.

(JIRA:RHELPLAN-37713)

IdM Healthcheck ahora soporta el cribado de registros DNS

Esta actualización introduce una prueba manual independiente de los registros DNS en un servidor de gestión de identidades (IdM).

La prueba utiliza la herramienta **Healthcheck** y realiza una consulta DNS utilizando el resolver local en el archivo **etc/resolv.conf**. La prueba asegura que los registros DNS esperados requeridos para el autodescubrimiento son resolubles.

(JIRA:RHELPLAN-37777)

La integración directa de RHEL en AD mediante SSSD ahora es compatible con FIPS

Con esta mejora, el demonio de seguridad de servicios del sistema (SSSD) se integra ahora con las implantaciones de Active Directory (AD) cuyos mecanismos de autenticación utilizan tipos de cifrado aprobados por la norma federal de procesamiento de información (FIPS). La mejora permite integrar directamente los sistemas RHEL en AD en entornos que deben cumplir los criterios FIPS.

(BZ#1841170)

El protocolo SMB1 ha sido desactivado en las utilidades del servidor y del cliente Samba por defecto

En Samba 4.11, los valores por defecto de los parámetros de **protocolo mínimo del servidor** y **protocolo mínimo del cliente** se han cambiado de **NT1** a **SMB2_02** porque el protocolo de bloque de mensajes del servidor versión 1 (SMB1) está obsoleto. Si no ha establecido estos parámetros en el archivo **/etc/samba/smb.conf**:

- Los clientes que sólo soportan SMB1 ya no pueden conectarse al servidor Samba.

- Las utilidades del cliente Samba, como **smbclient**, y la biblioteca **libsmbclient** fallan al conectarse a servidores que sólo soportan SMB1.

Red Hat recomienda no utilizar el protocolo SMB1. Sin embargo, si su entorno requiere SMB1, puede volver a habilitar manualmente el protocolo.

Para volver a habilitar SMB1 en un servidor Samba:

- Añada la siguiente configuración al archivo /**etc**/**samba**/**smb.conf**:

```
protocolo mínimo del servidor = NT1
```

- Reinicie el servicio **smb**:

```
# systemctl restart smb
```

Para volver a habilitar SMB1 para las utilidades del cliente Samba y la biblioteca **libsmbclient**:

- Añada la siguiente configuración al archivo /**etc**/**samba**/**smb.conf**:

```
protocolo mínimo del cliente = NT1
```

- Reinicie el servicio **smb**:

```
# systemctl restart smb
```

Tenga en cuenta que el protocolo SMB1 se eliminará en una futura versión de Samba.

(BZ#1785248)

samba rebasado a la versión 4.11.2

Los paquetes *samba* han sido actualizados a la versión 4.11.2, que proporciona una serie de correcciones de errores y mejoras con respecto a la versión anterior. Los cambios más importantes son:

- Por defecto, el protocolo de bloque de mensajes del servidor versión 1 (SMB1) está ahora deshabilitado en el servidor Samba, las utilidades del cliente y la biblioteca **libsmbclient**. Sin embargo, puede establecer manualmente los parámetros de **protocolo mínimo del servidor** y **protocolo mínimo del cliente** a **NT1** para volver a habilitar SMB1. Red Hat no recomienda volver a habilitar el protocolo SMB1.

- Los parámetros **lanman auth** y **encrypt passwords** están obsoletos. Estos parámetros permiten la autenticación insegura y sólo están disponibles en el protocolo obsoleto SMB1.

- Se ha eliminado el parámetro **-o** de la utilidad de base de datos trivial agrupada (CTDB) **de un nodo**.

- Samba utiliza ahora la biblioteca GnuTLS para el cifrado. Como resultado, si el modo FIPS en RHEL está activado, Samba es compatible con el estándar FIPS.

- El servicio **ctdbd** ahora registra cuando utiliza más del 90% de un hilo de CPU.

- Se ha eliminado el soporte de Python 2, que estaba obsoleto.

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: https://www.samba.org/samba/history/samba-4.11.0.html

(BZ#1754409)

El servidor de directorios se ha actualizado a la versión 1.4.2.4

Los paquetes *389-ds-base* han sido actualizados a la versión 1.4.2.4, que proporciona una serie de correcciones de errores y mejoras con respecto a la versión anterior. Para obtener una lista completa de los cambios notables, lea las notas de la versión upstream antes de actualizar:

- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-1.html

(BZ#1748994)

Algunas secuencias de comandos heredadas han sido sustituidas en el servidor de directorio

Esta mejora proporciona reemplazos para los scripts heredados **dbverify**, **validate-syntax.pl**, **cl-dump.pl**, **fixup-memberuid.pl** y **repl-monitor.pl** no soportados en Directory Server. Estos scripts han sido sustituidos por los siguientes comandos:

- **dbverify**: **dsctl *instance_name* dbverify**
- **validar-sintaxis.pl**: **dsconf esquema validar-sintaxis**
- **cl-dump.pl**: **dsconf replication dump-changelog**
- **fixup-memberuid.pl**: **dsconf plugin posix-winsync fixup**
- **repl-monitor.pl**: **monitor de replicación dsconf**

Para una lista de todos los scripts heredados y sus reemplazos, vea Utilidades de línea de comandos reemplazadas en Red Hat Directory Server 11.

(BZ#1739718)

La configuración de IdM como réplica oculta es ahora totalmente compatible

La gestión de identidades (IdM) en RHEL 8.2 soporta completamente la configuración de servidores IdM como réplicas ocultas. Una réplica oculta es un servidor IdM que tiene todos los servicios en ejecución y disponibles. Sin embargo, no se anuncia a otros clientes o maestros porque no existen registros **SRV** para los servicios en DNS, y los roles del servidor LDAP no están habilitados. Por lo tanto, los clientes no pueden utilizar el descubrimiento de servicios para detectar las réplicas ocultas.

Las réplicas ocultas están diseñadas principalmente para servicios dedicados que, de otro modo, pueden interrumpir a los clientes. Por ejemplo, una copia de seguridad completa de IdM requiere apagar todos los servicios de IdM en el maestro o la réplica. Dado que ningún cliente utiliza una réplica oculta, los

administradores pueden apagar temporalmente los servicios en este host sin afectar a ningún cliente. Otros casos de uso incluyen operaciones de alta carga en la API de IdM o el servidor LDAP, como una importación masiva o consultas extensas.

Para instalar una nueva réplica oculta, utilice el comando **ipa-replica-install --hidden-replica**. Para cambiar el estado de una réplica existente, utilice el comando ipa **server-state**.

Para más detalles, consulte Instalación de una réplica oculta de IdM .

(BZ#1719767)

La política de tickets de Kerberos ahora admite indicadores de autenticación

Los indicadores de autenticación se adjuntan a los tickets de Kerberos en función del mecanismo de preautenticación que se haya utilizado para adquirir el ticket:

- **otp** para la autenticación de dos factores (contraseña OTP)
- **radius** para la autenticación RADIUS
- **pkinit** para la autenticación de PKINIT, tarjetas inteligentes o certificados
- **endurecido** para contraseñas endurecidas (SPAKE o FAST)

El Centro de Distribución de Kerberos (KDC) puede aplicar políticas como el control de acceso a los servicios, la duración máxima del ticket y la edad máxima renovable, en las solicitudes de tickets de servicio que se basan en los indicadores de autenticación.

Con esta mejora, los administradores pueden lograr un control más fino sobre la emisión de tickets de servicio al requerir indicadores de autenticación específicos de los tickets de un usuario.

(BZ#1777564)

El paquete krb5 es ahora compatible con FIPS

Con esta mejora, se prohíbe la criptografía no conforme. Como resultado, los administradores pueden utilizar Kerberos en entornos regulados por FIPS.

(BZ#1754690)

Directory Server establece el parámetro sslVersionMin basándose en la política crypto de todo el sistema

Por defecto, Directory Server ahora establece el valor del parámetro **sslVersionMin** basado en la política crypto de todo el sistema. Si establece el perfil de la política crypto en el archivo **/etc/crypto-policies/config** a:

- **DEFAULT**, **FUTURE** o **FIPS**, el servidor de directorio establece **sslVersionMin** en **TLS1.2**
- **LEGACY**, Directory Server establece **sslVersionMin** a **TLS1.0**

Alternativamente, puede establecer manualmente **sslVersionMin** a un valor más alto que el definido en la política criptográfica:

```
# dsconf -D \ "cn=Directory Manager" __ldap://server.example.com__ security set --tls-protocol-min TLS1.3
```

(BZ#1828727)

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)

5.13. ESCRITORIO

Wayland está ahora habilitado en sistemas de doble GPU

Anteriormente, el entorno de GNOME utilizaba por defecto la sesión **X11** en ordenadores portátiles y otros sistemas que tienen dos unidades de procesamiento gráfico (GPU). Con esta versión, GNOME ahora utiliza por defecto la sesión **Wayland** en sistemas de doble GPU, que es el mismo comportamiento que en sistemas de una sola GPU.

(BZ#1749960)

5.14. INFRAESTRUCTURAS GRÁFICAS

Compatibilidad con las nuevas tarjetas gráficas

Las siguientes tarjetas gráficas son ahora compatibles:

- Gráficos Intel HD 610, 620 y 630, que se encuentran en los procesadores Intel Comet Lake H y U
- Gráficos Intel Ice Lake UHD 910 y gráficos Iris Plus 930, 940 y 950.
  Ya no es necesario configurar la opción del kernel **alpha_support** para habilitar la compatibilidad con los gráficos Intel Ice Lake.
- La familia AMD Navi 10, que incluye los siguientes modelos:
  - Radeon RX 5600
  - Radeon RX 5600 XT
  - Radeon RX 5700
  - Radeon RX 5700 XT
  - Radeon Pro W5700
- La familia Nvidia Turing TU116, que incluye los siguientes modelos.
  Tenga en cuenta que el controlador gráfico de **nouveau** todavía no soporta la aceleración 3D con la familia Nvidia Turing TU116.
  - GeForce GTX 1650 Super
  - GeForce GTX 1660
  - GeForce GTX 1660 Super

- GeForce GTX 1660 Ti
- GeForce GTX 1660 Ti Max-Q

Además, se han actualizado los siguientes controladores gráficos:

- El controlador Matrox **mgag2000**
- El conductor de Aspeed **ast**
- El controlador Intel **i915**

(JIRA:RHELPLAN-41384)

5.15. LA CONSOLA WEB

Los administradores pueden ahora utilizar certificados de cliente para autenticarse en la consola web de RHEL 8

Con esta mejora de la consola web, un administrador de sistemas puede utilizar certificados de cliente para acceder a un sistema RHEL 8 de forma local o remota mediante un navegador con autenticación de certificados incorporada. No se requiere ningún software de cliente adicional. Estos certificados son comúnmente proporcionados por una tarjeta inteligente o Yubikey, o pueden ser importados en el navegador.

Al iniciar la sesión con un certificado, el usuario no puede actualmente realizar acciones administrativas en la consola web. Pero el usuario puede realizarlas en la página de Terminal con el comando **sudo** después de autenticarse con una contraseña.

(JIRA:RHELPLAN-2507)

Opción de iniciar sesión en la consola web con un certificado de cliente TLS

Con esta actualización, es posible configurar la consola web para iniciar sesión con un certificado de cliente TLS proporcionado por un navegador o un dispositivo como una tarjeta inteligente o una YubiKey.

(BZ#1678465)

Cambios en el acceso a la consola web

La consola web de RHEL ha sido actualizada con los siguientes cambios:

- La consola web cerrará automáticamente la sesión actual tras 15 minutos de inactividad. Puedes configurar el tiempo de espera en minutos en el archivo **/etc/cockpit/cockpit.conf**.
- Al igual que en el caso de SSH, la consola web ahora puede mostrar opcionalmente el contenido de los archivos de banner en la pantalla de inicio de sesión. Los usuarios deben configurar la funcionalidad en el archivo **/etc/cockpit/cockpit.conf**.

Consulte la página del manual de **cockpit.conf(5**) para obtener más información.

(BZ#1754163)

La consola web de RHEL ha sido rediseñada para utilizar el sistema de diseño de interfaz de usuario PatternFly 4

El nuevo diseño proporciona una mejor accesibilidad y se ajusta al diseño de OpenShift 4. Las actualizaciones incluyen:

- La página de información general ha sido completamente rediseñada. Por ejemplo, la información se ha agrupado en paneles más fáciles de entender, la información sobre salud ocupa un lugar más destacado, los gráficos de recursos se han trasladado a su propia página y la página de información sobre hardware es ahora más fácil de encontrar.
- Los usuarios pueden utilizar el nuevo campo de búsqueda en el menú de navegación para encontrar fácilmente páginas específicas basadas en palabras clave.

Para más información sobre PatternFly, consulte la página del proyecto PatternFly.

(BZ#1784455)

Actualizaciones de la página de máquinas virtuales

La página de **máquinas virtuales** de la consola web ha recibido varias mejoras de almacenamiento:

- La creación de volúmenes de almacenamiento ahora funciona para todos los tipos soportados por libvirt.
- Los pools de almacenamiento se pueden crear en LVM o iSCSI.

Además, la página de **Máquinas Virtuales** ahora soporta la creación y eliminación de interfaces de red virtuales.

(BZ#1676506, BZ#1672753)

Consola web Actualizaciones de la página de almacenamiento

Las pruebas de usabilidad mostraron que el concepto de *default mount point* en la página de **almacenamiento** de la consola web de RHEL era difícil de entender y generaba mucha confusión. Con esta actualización, la consola web ya no ofrece la opción *Default* al montar un sistema de archivos. La creación de un nuevo sistema de archivos ahora siempre requiere un punto de montaje especificado.

Además, la consola web ahora oculta la distinción entre la configuración(**/etc/fstab**) y el estado de ejecución(**/proc/mounts**). Los cambios realizados en la consola web siempre se aplican tanto a la configuración como al estado de ejecución. Cuando la configuración y el estado en tiempo de ejecución difieren entre sí, la consola web muestra una advertencia, y permite a los usuarios volver a sincronizarlos fácilmente.

(BZ#1784456)

5.16. VIRTUALIZACIÓN

Al intentar crear una máquina virtual RHEL a partir de un árbol de instalación, ahora se devuelve un mensaje de error más útil.

Las máquinas virtuales de RHEL 7 y RHEL 8 creadas con la utilidad **virt-install** con la opción **--location** en algunos casos no arrancan. Esta actualización añade un mensaje de error de virt-install que proporciona instrucciones sobre cómo solucionar este problema.

(BZ#1677019)

Procesadores de la serie Intel Xeon Platinum 9200 compatibles con invitados KVM

La compatibilidad con los procesadores de la serie Intel Xeon Platinum 9200 (anteriormente conocidos

como **Cascade Lake**) se ha añadido al hipervisor KVM y al código del kernel, así como a la API libvirt. Esto permite que las máquinas virtuales KVM utilicen los procesadores Intel Xeon Platinum de la serie 9200.

(JIRA:RHELPLAN-13995)

EDK2 rebasado a la versión estable201908

El paquete *EDK2* ha sido actualizado a la versión **stable201908**, que aporta múltiples mejoras. En particular:

- *EDK2* ahora incluye soporte para OpenSSL-1.1.1.
- Para cumplir con los requisitos de licencia del proyecto upstream, la licencia del paquete *EDK2* se ha cambiado de **BSD y OpenSSL y MIT** a **BSD-2-Clause-Patent y OpenSSL y MIT**.

(BZ#1748180)

Creación de máquinas virtuales anidadas

Con esta actualización, la virtualización anidada es totalmente compatible con las máquinas virtuales (VM) KVM que se ejecutan en un host Intel 64 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 los sistemas AMD64, la virtualización KVM anidada sigue siendo una Muestra de Tecnología.

(JIRA:RHELPLAN-14047, JIRA:RHELPLAN-24437)

5.17. CONTENEDORES

Se ha actualizado la lista de búsqueda de registros por defecto en **/etc/containers/registries.conf**

La lista por defecto de **registries.search** en **/etc/containers/registries.conf** ha sido actualizada para incluir sólo los registros de confianza que proporcionan imágenes de contenedores curadas, parcheadas y mantenidas por Red Hat y sus socios.

Red Hat recomienda utilizar siempre nombres de imagen totalmente cualificados, incluyendo:

- El servidor de registro (nombre DNS completo)
- Espacio de nombres
- Nombre de la imagen
- Etiqueta (por ejemplo, **registry.redhat.io/ubi8/ubu:latest**)

Cuando se utilizan nombres cortos, siempre hay un riesgo inherente de suplantación de identidad. Por ejemplo, un usuario quiere sacar una imagen llamada **foobar** de un registro y espera que proceda de myregistry **.**com. Si myregistry. **com** no es el primero en la lista de búsqueda, un atacante podría colocar una imagen **foobar** diferente en un registro anterior en la lista de búsqueda. El usuario accidentalmente sacaría y ejecutaría la imagen y el código del atacante en lugar del contenido previsto. Red Hat recomienda sólo añadir registros que sean de confianza, es decir, registros que no permitan a usuarios desconocidos o anónimos crear cuentas con nombres arbitrarios. Esto evita que una imagen sea suplantada, ocupada o convertida en insegura.

(BZ#1810053)

Podman ya no depende de **oci-systemd-hook**

Podman no necesita ni depende del paquete **oci-systemd-hook**, que ha sido eliminado de los módulos **container-tools:rhel8** y **container-tools:2.0**.

(BZ#1645280)

CAPÍTULO 6. 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 distribuido con Red Hat Enterprise Linux 8.2. Estos cambios incluyen 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.

6.1. NUEVOS PARÁMETROS DEL NÚCLEO

cpuidle.governor = [CPU_IDLE]

Nombre del gobernador **cpuidle** a utilizar.

deferred_probe_timeout = [KNL]

Este es un parámetro de depuración para establecer un tiempo de espera en segundos para que la sonda diferida deje de esperar a las dependencias para sondear.
Sólo se ignorarán las dependencias específicas (subsistemas o controladores) que hayan optado por la entrada. Un tiempo de espera de 0 se agotará al final de las **llamadas de entrada**. Este parámetro también descargará los dispositivos que sigan en la lista de sondas diferidas después de reintentar.

kvm.nx_huge_pages = [KVM]

Este parámetro controla la solución de software para el error **X86_BUG_ITLB_MULTIHIT**.
Las opciones son:

- **force** - Siempre despliegue la solución.
- **off** - No desplegar nunca la solución.
- **auto** (por defecto) - Implementa una solución basada en la presencia de **X86_BUG_ITLB_MULTIHIT**.

Si la solución de software está activada para el host, los huéspedes no necesitan activarla para los huéspedes anidados.

kvm.nx_huge_pages_recovery_ratio = [KVM]

Este parámetro controla la cantidad de páginas de 4KiB que se recuperan periódicamente a páginas enormes. El valor 0 desactiva la recuperación, de lo contrario, si el valor es N, la máquina virtual basada en el kernel (KVM) zappeará 1/ésimo de las páginas de 4KiB cada minuto. El valor por defecto es 60.

page_alloc.shuffle = [KNL]

Bandera booleana para controlar si el asignador de páginas debe aleatorizar sus listas libres.
La aleatorización puede ser activada automáticamente si el kernel detecta que se está ejecutando en una plataforma con una caché del lado de la memoria con mapeo directo. Este parámetro puede utilizarse para anular/desactivar ese comportamiento.

El estado de la bandera se puede leer del pseudo sistema de archivos **sysfs** desde el archivo **/sys/module/page_alloc/parameters/shuffle**.

panic_print =

Máscara de bits para imprimir información del sistema cuando se produce un pánico.
El usuario puede elegir la combinación de los siguientes bits:

- bit 0: imprimir la información de todas las tareas
- bit 1: imprimir información de la memoria del sistema
- bit 2: imprimir información del temporizador
- bit 3: imprimir información sobre los bloqueos si la configuración del kernel **CONFIG_LOCKDEP** está activada
- bit 4: imprimir el buffer **ftrace**
- bit 5: imprimir todos los mensajes **printk** en el buffer

rcutree.sysrq_rcu = [KNL]

Comandeer una clave **sysrq** para volcar el árbol **rcu_node** de Tree RCU con el fin de determinar por qué un nuevo período de gracia aún no ha comenzado.

rcutorture.fwd_progress = [KNL]

Habilitar la prueba de avance del periodo de gracia de la actualización de la copia de lectura (RCU) para los tipos de RCU que soportan esta noción.

rcutorture.fwd_progress_div = [KNL]

Especifique la fracción de un período de advertencia de parada de la CPU para realizar pruebas de avance en bucle cerrado.

rcutorture.fwd_progress_holdoff = [KNL]

Número de segundos de espera entre pruebas sucesivas de avance.

rcutorture.fwd_progress_need_resched = [KNL]

Incluya las llamadas a **cond_resched(**) dentro de las comprobaciones de **need_resched()** durante las pruebas de avance de bucle cerrado.

tsx = [X86]

Este parámetro controla la función de Extensiones de Sincronización Transaccional (TSX) en los procesadores Intel que soportan el control TSX.
Las opciones son:

- **on** - Habilitar TSX en el sistema. Aunque existen mitigaciones para todas las vulnerabilidades de seguridad conocidas, TSX aceleró varios CVEs anteriores relacionados con la especulación. Como resultado, puede haber riesgos de seguridad desconocidos asociados a dejarla activada.
- **off** - Desactivar TSX en el sistema. Esta opción sólo tiene efecto en las CPUs más nuevas que no son vulnerables al muestreo de datos de microarquitectura (MDS). En otras palabras, tienen **MSR_IA32_ARCH_CAPABILITIES.MDS_NO=1** y obtienen el nuevo registro específico del modelo **IA32_TSX_CTRL** (MSR) a través de una actualización del microcódigo. Este nuevo MSR permite una desactivación fiable de la funcionalidad TSX.
- **auto** - Desactivar TSX si **X86_BUG_TAA** está presente, en caso contrario activar TSX en el sistema.

No especificar este parámetro equivale a **tsx=off**.

Para más detalles, consulte la documentación del kernel.

tsx_async_abort = [X86,INTEL]

Este parámetro controla la mitigación de la vulnerabilidad TSX Async Abort (TAA).
Al igual que el muestreo de datos de la microarquitectura (MDS), ciertas CPU que soportan las extensiones de sincronización transaccional (TSX) son vulnerables a un exploit contra los búferes internos de la CPU. El exploit es capaz de enviar información a un gadget de divulgación bajo ciertas condiciones.

En los procesadores vulnerables, los datos reenviados especulativamente pueden utilizarse en un ataque de canal lateral de caché, para acceder a datos a los que el atacante no tiene acceso directo.

Las opciones son:

- **completo** - Activar la mitigación de TAA en las CPUs vulnerables si TSX está activado.
- **full,nosmt** - Activa la mitigación de TAA y desactiva el Multi Threading Simultáneo (SMT) en las CPUs vulnerables. Si TSX está desactivado, SMT no se desactiva porque la CPU no es vulnerable a los ataques TAA de hilos cruzados.
- **off** - Desactivar incondicionalmente la mitigación TAA.
  En las máquinas afectadas por MDS, el parámetro **tsx_async_abort=off** puede evitarse mediante una mitigación MDS activa, ya que ambas vulnerabilidades se mitigan con el mismo mecanismo. Por lo tanto, para desactivar esta mitigación, es necesario especificar también el parámetro **mds=off**.

  No especificar esta opción es equivalente a **tsx_async_abort=full**. En las CPUs que están afectadas por MDS y despliegan la mitigación de MDS, la mitigación de TAA no es necesaria y no proporciona ninguna mitigación adicional.

Para más detalles, consulte la documentación del kernel.

6.2. PARÁMETROS DEL NÚCLEO ACTUALIZADOS

intel_iommu = [DMAR]

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

- **sm_on** [Predeterminado Off] - Por defecto, el modo escalable estará deshabilitado incluso si el hardware anuncia que tiene soporte para la traducción del modo escalable. Con esta opción establecida, el modo escalable se utilizará en el hardware que afirme soportarlo.

isolcpus = [KNL,SMP,ISOL]

Este parámetro aísla un conjunto determinado de CPUs de las perturbaciones.

- **managed_irq** - Un subparámetro que evita que las CPUs aisladas sean objetivo de las interrupciones gestionadas, que tienen una máscara de interrupción que contiene las CPUs aisladas. La afinidad de las interrupciones administradas es manejada por el kernel y no puede ser cambiada a través de las interfaces /**proc**/**irq**/*.
  Este aislamiento es el mejor esfuerzo y sólo es efectivo si la máscara de interrupción asignada automáticamente de una cola de dispositivos contiene CPUs aisladas y de mantenimiento. Si las CPUs de mantenimiento están en línea, dichas interrupciones se dirigen a la CPU de mantenimiento para que las E/S enviadas a la CPU de mantenimiento no puedan perturbar a la CPU aislada.

  Si la máscara de afinidad de la cola contiene sólo CPUs aisladas, este parámetro no tiene efecto en la decisión de enrutamiento de las interrupciones. Sin embargo, las interrupciones

sólo se entregan cuando las tareas que se ejecutan en esas CPUs aisladas envían E/S. La E/S enviada en las CPUs de mantenimiento no tiene influencia en esas colas.

mds = [X86,INTEL]

Los cambios en las opciones:

- **off** - En las máquinas afectadas por TSX Async Abort (TAA), **mds=off** puede ser impedido por una mitigación activa de TAA ya que ambas vulnerabilidades se mitigan con el mismo mecanismo. Por lo tanto, para desactivar esta mitigación, es necesario especificar también el parámetro del kernel **tsx_async_abort=off**.

No especificar este parámetro equivale a **mds=full**.

Para más detalles, consulte la documentación del kernel.

mem_encrypt = [X86-64]

Control de encriptación de memoria segura (SME) de AMD
...

Para más detalles sobre cuándo se puede activar la encriptación de la memoria, consulte la documentación del kernel upstream.

mitigación =

Los cambios en las opciones:

- **off** - Desactivar todas las mitigaciones opcionales de la CPU. Esto mejora el rendimiento del sistema, pero también puede exponer a los usuarios a varias vulnerabilidades de la CPU. Equivalente a:
  - **nopti [X86,PPC]**
  - **kpti=0 [ARM64]**
  - **nospectre_v1 [X86,PPC]**
  - **nobp=0 [S390]**
  - **nospectre_v2 [X86,PPC,S390,ARM64]**
  - **spectre_v2_user=off [X86]**
  - **spec_store_bypass_disable=off [X86,PPC]**
  - **ssbd=force-off [ARM64]**
  - **l1tf=off [X86]**
  - **mds=off [X86]**
  - **tsx_async_abort=off [X86]**
  - **kvm.nx_huge_pages=off [X86]**
    Excepciones:

Esto no tiene ningún efecto sobre kvm **. nx_huge_pages** cuando **kvm.nx_huge_pages=force**.

- **auto,nosmt** - Mitiga todas las vulnerabilidades de la CPU, deshabilitando el Multihilo Simultáneo (SMT) si es necesario. Esta opción es para los usuarios que siempre quieren estar completamente mitigados, incluso si significa perder SMT.
  Equivalente a:
  - **l1tf=flush,nosmt [X86]**
  - **mds=full,nosmt [X86]**
  - **tsx_async_abort=full,nosmt [X86]**

rcutree.jiffies_till_sched_qs = [KNL]

Este parámetro establece la edad requerida en jiffies para un periodo de gracia dado antes de que Read-copy update (RCU) comience a solicitar ayuda de estado de reposo desde las funciones **rcu_note_context_switch()** y **cond_resched()**. Si no se especifica, el núcleo calculará un valor basado en la configuración más reciente de los parámetros del núcleo **rcutree .jiffies_till_first_fqs** y **rcutree.jiffies_till_next_fqs**.
Este valor calculado puede verse en el parámetro del núcleo **rcutree**.jiffies_to_sched_qs. Cualquier intento de establecer **rcutree**.jiffies_to_sched_qs se sobrescribirá.

tsc =

Este parámetro desactiva las comprobaciones de estabilidad de la fuente de reloj para el contador de tiempo (TSC).
Formato: <string>

Las opciones son:

- **reliable** [x86] - Marca la fuente de reloj del TSC como fiable. Esta opción desactiva la verificación de la fuente de reloj en tiempo de ejecución, así como las comprobaciones de estabilidad realizadas en el arranque. La opción también habilita el modo de temporizador de alta resolución en hardware antiguo y en entornos virtualizados.
- **noirqtime** [x86] - No utilizar el TSC para realizar la contabilidad de las peticiones de interrupción (IRQ). Se utiliza para deshabilitar en tiempo de ejecución **IRQ_TIME_ACCOUNTING** en cualquier plataforma en la que el contador de tiempo de lectura (RDTSC) sea lento y esta contabilidad pueda añadir sobrecarga.
- **inestable** [x86] - Marca la fuente de reloj del TSC como inestable. Esta opción marca el TSC como incondicionalmente inestable en el arranque y evita cualquier otro tambaleo una vez que el perro guardián del TSC se da cuenta.
- **nowatchdog** [x86] - Desactiva el perro guardián de la fuente de reloj. Esta opción se utiliza en situaciones con requisitos de latencia estrictos en las que no se aceptan las interrupciones del perro guardián de la fuente de reloj.

6.3. NUEVOS PARÁMETROS DE /PROC/SYS/KERNEL

impresión_de_pánico

Máscara de bits para imprimir la información del sistema cuando se produce un pánico.
El usuario puede elegir la combinación de los siguientes bits:

- bit 0: imprimir la información de todas las tareas
- bit 1: imprimir información de la memoria del sistema
- bit 2: imprimir información del temporizador
- bit 3: imprimir información sobre los bloqueos si el elemento de configuración del kernel **CONFIG_LOCKDEP** está activado
- bit 4: imprimir el buffer **ftrace**
  Por ejemplo, para imprimir las tareas y la información de la memoria en caso de pánico, ejecute:

```
# echo 3 > /proc/sys/kernel/panic_print
```

sched_energy_aware

Este parámetro habilita o deshabilita la programación consciente de la energía (EAS).
EAS se inicia automáticamente en las plataformas con topologías de CPU asimétricas que tienen un modelo de energía disponible.

Si su plataforma cumple los requisitos para el EAS pero no quiere utilizarlo, cambie este valor a 0.

6.4. PARÁMETROS ACTUALIZADOS DE /PROC/SYS/KERNEL

hilos-max

Este parámetro controla el número máximo de hilos que la función **fork()** puede crear.
Durante la inicialización, el kernel establece este valor de forma que, aunque se cree el máximo número de hilos, las estructuras de los hilos sólo ocupen una parte (1/8) de las páginas de RAM disponibles.

El valor mínimo que se puede escribir en **threads-max** es 1. El valor máximo viene dado por la constante **FUTEX_TID_MASK (0x3fffffff)**.

Si se escribe un valor fuera de este rango en **threads-max**, se produce un error **EINVAL**.

6.5. PARÁMETROS ACTUALIZADOS DE /PROC/SYS/NET

bpf_jit_enable

Este parámetro activa el compilador **Berkeley Packet Filter Just-in-Time (BPF JIT)**.
BPF es una infraestructura flexible y eficiente que permite ejecutar bytecode en varios puntos de enganche. Se utiliza en varios subsistemas del kernel de Linux, como las redes (por ejemplo, **XDP**, **tc**), el rastreo (por ejemplo, **kprobes**, **uprobes**, **tracepoints**) y la seguridad (por ejemplo, **seccomp**).

LLVM tiene un back-end **BPF** que puede compilar C restringido en una secuencia de instrucciones **BPF**. Después de cargar el programa a través de la llamada al sistema **bpf()** y de pasar un verificador en el núcleo, **JIT** traducirá estos progletos de **BPF** en instrucciones nativas de la CPU.

Hay dos tipos de **JIT**, el más nuevo **eBPF JIT** es actualmente compatible con las siguientes arquitecturas de CPU:

- **x86_64**

- **brazo64**
- **ppc64** (tanto endians pequeños como grandes)
- **s390x**

CAPÍTULO 7. CONTROLADORES DE DISPOSITIVOS

Este capítulo proporciona una lista completa de todos los controladores de dispositivos que son nuevos o han sido actualizados en Red Hat Enterprise Linux 8.2.

7.1. NUEVOS CONDUCTORES

Controladores de red

- controlador gVNIC (gve.ko.xz)
- Controlador de bus Broadcom UniMAC MDIO (mdio-bcm-unimac.ko.xz)
- Software iWARP Driver (siw.ko.xz)

Controladores de gráficos y controladores varios

- Ayudantes de gestión de memoria DRM VRAM (drm_vram_helper.ko.xz)
- controlador cpuidle para el gobernador haltpoll (cpuidle-haltpoll.ko.xz)
- controlador stm_ftrace (stm_ftrace.ko.xz)
- controlador stm_console (stm_console.ko.xz)
- Clase de dispositivo del módulo System Trace (stm_core.ko.xz)
- dispositivo dummy_stm (dummy_stm.ko.xz)
- controlador stm_heartbeat (stm_heartbeat.ko.xz)
- Controlador de Intel® Trace Hub Global Trace Hub (intel_th_gth.ko.xz)
- Controlador de salida Intel® Trace Hub PTI/LPP (intel_th_pti.ko.xz)
- Controlador del concentrador Intel® Trace (intel_th.ko.xz)
- Controlador de la unidad de almacenamiento de memoria Intel® Trace Hub (intel_th_msu.ko.xz)
- Controlador del Intel® Trace Hub Software Trace Hub (intel_th_sth.ko.xz)
- Disipador de software de la unidad de almacenamiento de memoria Intel® Trace Hub (intel_th_msu_sink.ko.xz)
- Controlador del controlador Intel® Trace Hub PCI (intel_th_pci.ko.xz)
- Controlador del concentrador Intel® Trace Hub ACPI (intel_th_acpi.ko.xz)
- Controlador MC para los procesadores Intel de 10nm para servidores (i10nm_edac.ko.xz)
- Dispositivo DAX: dispositivo de mapeo de acceso directo (dax_pmem_core.ko.xz)
- PMEM DAX: acceso directo a la memoria persistente (dax_pmem.ko.xz)
- PMEM DAX: soporte de la interfaz /sys/class/dax obsoleta (dax_pmem_compat.ko.xz)
- Init de la plataforma Intel PMC Core (intel_pmc_core_pltdrv.ko.xz)

- Control Intel RAPL (Running Average Power Limit) a través de la interfaz MSR (intel_rapl_msr.ko.xz)
- Código común del límite de potencia media en tiempo de ejecución de Intel (RAPL) (intel_rapl_common.ko.xz)

Controladores de almacenamiento

- Soporte de clustering para MD (md-cluster.ko.xz)

7.2. CONTROLADORES ACTUALIZADOS

Actualización de los controladores de red

- El controlador NIC virtual de VMware vmxnet3 (vmxnet3.ko.xz) ha sido actualizado a la versión 1.4.17.0-k.
- El controlador de red de función virtual Intel® 10 Gigabit (ixgbevf.ko.xz) ha sido actualizado a la versión 4.1.0-k-rh8.2.0.
- El controlador de red Intel® 10 Gigabit PCI Express (ixgbe.ko.xz) ha sido actualizado a la versión 5.1.0-k-rh8.2.0.
- El controlador Intel® Ethernet Connection E800 Series Linux (ice.ko.xz) ha sido actualizado a la versión 0.8.1-k.
- El controlador del procesador de flujo Netronome (NFP) (nfp.ko.xz) ha sido actualizado a la versión 4.18.0-185.el8.x86_64.
- Elastic Network Adapter (ENA) (ena.ko.xz) ha sido actualizado a la versión 2.1.0K.

Actualizaciones de gráficos y controladores varios

- El controlador HPE watchdog (hpwdt.ko.xz) ha sido actualizado a la versión 2.0.3.
- El controlador Intel I/OAT DMA Linux (ioatdma.ko.xz) ha sido actualizado a la versión 5.00.

Actualizaciones de los controladores de almacenamiento

- El controlador para HPE Smart Array Controller (hpsa.ko.xz) ha sido actualizado a la versión 3.4.20-170-RH4.
- El controlador del dispositivo LSI MPT Fusion SAS 3.0 (mpt3sas.ko.xz) ha sido actualizado a la versión 32.100.00.00.
- El controlador QLogic FCoE (bnx2fc.ko.xz) ha sido actualizado a la versión 2.12.10.
- El controlador Emulex LightPulse Fibre Channel SCSI (lpfc.ko.xz) ha sido actualizado a la versión 0:12.6.0.2.
- QLogic FastLinQ 4xxxx FCoE Module (qedf.ko.xz) ha sido actualizado a la versión 8.42.3.0.
- El controlador HBA de canal de fibra de QLogic (qla2xxx.ko.xz) ha sido actualizado a la versión 10.01.00.21.08.2-k.
- La versión del controlador de la familia Smart de Microsemi (smartpqi.ko.xz) ha sido actualizada a la versión 1.2.10-025.

- QLogic FastLinQ 4xxxx iSCSI Module (qedi.ko.xz) ha sido actualizado a la versión 8.37.0.20.
- El controlador Broadcom MegaRAID SAS (megaraid_sas.ko.xz) ha sido actualizado a la versión 07.710.50.00-rc1.

CAPÍTULO 8. CORRECCIÓN DE ERRORES

Esta parte describe los errores corregidos en Red Hat Enterprise Linux 8.2 que tienen un impacto significativo en los usuarios.

8.1. CREACIÓN DEL INSTALADOR Y DE LA IMAGEN

El uso de los parámetros de arranque del kernel **version** o **inst.version** ya no detiene el programa de instalación

Anteriormente, al arrancar el programa de instalación desde la línea de comandos del kernel utilizando los parámetros de arranque **version** o **inst.version** se imprimía la versión, por ejemplo **anaconda 30.25.6**, y se detenía el programa de instalación.

Con esta actualización, los parámetros **version** y **inst.version** son ignorados cuando el programa de instalación se inicia desde la línea de comandos del kernel, y como resultado, el programa de instalación no se detiene.

(BZ#1637472)

Soporte de arranque seguro para s390x en el instalador

Anteriormente, RHEL 8.1 proporcionaba soporte para la preparación de discos de arranque para su uso en entornos IBM Z que obligaban al uso del arranque seguro. Las capacidades del servidor y del hipervisor utilizados durante la instalación determinaban si el formato en disco resultante contenía soporte para el arranque seguro. No había forma de influir en el formato en disco durante la instalación. En consecuencia, si se instalaba RHEL 8.1 en un entorno que soportaba el arranque seguro, el sistema no podía arrancar cuando se trasladaba a un entorno que no soportaba el arranque seguro, como se hace en algunos escenarios de conmutación por error.

Con esta actualización, ahora puedes configurar la opción de arranque seguro de la herramienta **zipl**. Para ello, puede utilizar cualquiera:

- El comando **zipl** de Kickstart y una de sus opciones, por ejemplo: **--secure-boot**, **--no-secure-boot** y **--force-secure-boot**.
- En la ventana de **resumen de la instalación** en la interfaz gráfica de usuario, puede seleccionar el **enlace Sistema > Destino de la instalación > Resumen del disco completo y cargador de arranque** y establecer el dispositivo de arranque. Como resultado, la instalación ahora puede arrancarse en entornos que carecen de soporte de arranque seguro.

(BZ#1659400)

La función de arranque seguro ya está disponible

Anteriormente, el valor por defecto de la opción de arranque **seguro=** no estaba configurado en **auto**, y como resultado, la función de arranque seguro no estaba disponible. Con esta actualización, a menos que se haya configurado previamente, el valor por defecto se establece en **auto**, y la función de arranque seguro está ahora disponible.

(BZ#1750326)

El archivo **/etc/sysconfig/kernel** ya no hace referencia al script **new-kernel-pkg**

Anteriormente, el archivo **/etc/sysconfig/kernel** hacía referencia al script **new-kernel-pkg**. Sin embargo, el script **new-kernel-pkg** no está incluido en un sistema RHEL 8. Con esta actualización, la referencia al script **new-kernel-pkg** se ha eliminado del archivo **/etc/sysconfig/kernel**.

(BZ#1747382)

La instalación no establece más que el número máximo de dispositivos permitidos en la variable **NVRAM del dispositivo de arranque**

Anteriormente, el programa de instalación de RHEL 8 establecía más del número máximo de dispositivos permitidos en la variable **NVRAM del dispositivo de arranque**. Como resultado, la instalación fallaba en sistemas que tenían más del número máximo de dispositivos. Con esta actualización, el programa de instalación de RHEL 8 comprueba ahora la configuración del dispositivo máximo y sólo añade el número permitido de dispositivos.

(BZ#1748756)

Las instalaciones funcionan para una ubicación de la imagen que utiliza un comando URL en un archivo Kickstart situado en una ubicación fuera de la red

Anteriormente, la instalación fallaba al principio del proceso cuando la activación de la red desencadenada por la ubicación remota de la imagen se especificaba mediante un comando URL en un archivo Kickstart situado en una ubicación que no era de red. Esta actualización soluciona el problema, y las instalaciones que proporcionan la ubicación de la imagen mediante un comando URL en un archivo Kickstart que se encuentra en una ubicación que no es de red, por ejemplo, un CD-ROM o un dispositivo de bloque local, ahora funcionan como se espera.

(BZ#1649359)

El programa de instalación de RHEL 8 sólo comprueba la existencia de dispositivos ECKD DASD no formateados

Anteriormente, al comprobar si había dispositivos sin formatear, el programa de instalación comprobaba todos los dispositivos DASD. Sin embargo, el programa de instalación sólo debería haber comprobado los dispositivos DASD ECKD. Como consecuencia, la instalación fallaba con un rastro cuando se utilizaba un dispositivo DASD FBA con SWAPGEN. Con esta actualización, el programa de instalación no comprueba los dispositivos DASD FBA, y la instalación se completa con éxito.

(BZ#1715303)

8.2. GESTIÓN DEL SOFTWARE

yum repolist ya no termina en el primer repositorio no disponible

Anteriormente, la opción de configuración del repositorio **skip_if_unavailable** se establecía por defecto de la siguiente manera:

```
skip_if_unavailable=false
```

Esta configuración obligaba al comando **yum** repolist a finalizar en el primer repositorio no disponible con un error y un estado de salida 1. En consecuencia, **yum repolist** no continuaba listando los repositorios disponibles.

Con esta actualización, **yum repolist** ha sido corregido para que ya no requiera ninguna descarga. Como resultado, **yum repolist** no proporciona ninguna salida que requiera metadatos, y el comando ahora continúa listando los repositorios disponibles como se esperaba.

Tenga en cuenta que el número de paquetes disponibles sólo es devuelto por **yum repolist --verbose** o **yum repoinfo** que aún requieren metadatos disponibles. Por lo tanto, estos comandos terminarán en el primer repositorio no disponible.

(BZ#1697472)

8.3. SHELL Y HERRAMIENTAS DE LÍNEA DE COMANDOS

Actualizaciones de ReaR

RHEL 8.2 introduce una serie de actualizaciones en la utilidad Relax-and-Recover (**ReaR**).

Se ha cambiado el manejo del directorio de construcción. Anteriormente, el directorio de construcción se mantenía en una ubicación temporal en caso de que **ReaR** encontrara un fallo. Con esta actualización, el directorio de construcción se elimina por defecto en las ejecuciones no interactivas para evitar el consumo de espacio en disco.

La semántica de la variable de configuración **KEEP_BUILD_DIR** se ha mejorado para incluir un nuevo valor de **error**. Puede establecer la variable **KEEP_BUILD_DIR** con los siguientes valores:

- **errores** para conservar el directorio de construcción en los errores para la depuración (el comportamiento anterior)
- **y (true)** para conservar siempre el directorio de construcción
- **n (false)** para no conservar nunca el directorio de construcción

El valor por defecto es una cadena vacía con el significado de **errores** cuando **ReaR** está siendo ejecutado de forma interactiva (en un terminal) y **falso** si **ReaR** está siendo ejecutado de forma no interactiva. Tenga en cuenta que **KEEP_BUILD_DIR** se establece automáticamente a **true** en el modo de depuración (**-d**) y en el modo debugscript (**-D**); este comportamiento no se ha cambiado.

Las correcciones de errores más destacadas son:

- Se ha corregido la compatibilidad con NetBackup 8.0.
- **ReaR** ya no aborta con un error bash similar a **xrealloc: no puede asignar** en sistemas con un gran número de usuarios, grupos y usuarios por grupo.
- El comando **bconsole** muestra ahora su prompt, que permite realizar una operación de restauración cuando se utiliza la integración de Bacula.
- **ReaR** ahora hace una copia de seguridad correcta de los archivos también en situaciones en las que el servicio **Docker** se está ejecutando pero no se ha definido ningún directorio raíz **Docker**, o cuando es imposible determinar el estado del servicio **Docker**.
- La recuperación ya no falla cuando se utilizan grupos pequeños o se recupera un sistema en modo de migración.
- Se ha solucionado la reconstrucción extremadamente lenta de **initramfs** durante el proceso de recuperación con LVM.
- **ReaR** ahora crea una imagen ISO de arranque que funciona en las arquitecturas AMD e Intel de 64 bits cuando se utiliza el cargador de arranque UEFI. El arranque de una imagen de rescate en esta configuración ya no aborta en Grub con el mensaje de error **Unknown command 'configfile' (...) Entering rescue mode....** El soporte para GRUB_RESCUE en esta configuración, que anteriormente podía fallar debido a la falta de soporte del sistema de archivos XFS, también ha sido corregido.

(BZ#1729501)

mlocate-updatedb.timer se activa ahora durante la instalación del paquete mlocate

Anteriormente, la reindexación de la base de datos de archivos no se realizaba automáticamente, porque el temporizador **mlocate-updatedb**.timer estaba desactivado después de la instalación del paquete **mlocate**. Con esta actualización, el temporizador mlocate-updatedb. **timer** forma ahora parte del archivo **90-default.preset** y se activa por defecto tras la instalación del paquete **mlocate**. Como resultado, la base de datos de archivos se actualiza automáticamente.

(BZ#1817591)

8.4. SERVICIOS DE INFRAESTRUCTURA

dnsmasq ahora maneja correctamente las consultas DNS no recursivas

Anteriormente, **dnsmasq** reenviaba todas las consultas no recursivas a un servidor upstream, lo cual llevaba a respuestas diferentes. Con esta actualización, las consultas no recursivas a nombres locales conocidos, como nombres de arrendamiento de hosts DHCP o hosts leídos del archivo **/etc/hosts**, son manejados por **dnsmasq** y no son reenviados a un servidor upstream. Como resultado, se devuelve la misma respuesta que a las consultas recursivas a nombres conocidos.

(BZ#1700916)

dhclient ya no falla al renovar la dirección IP después de los cambios de hora del sistema

Anteriormente, si la hora del sistema cambiaba, el sistema podía perder la dirección IP asignada debido a la eliminación por parte del kernel. Con esta actualización, **dhclient** utiliza un temporizador monotónico para detectar los saltos de tiempo hacia atrás y emite el mensaje **DHCPREQUEST** para la extensión del arrendamiento en caso de salto discontinuo en la hora del sistema. Como resultado, el sistema ya no pierde la dirección IP en el escenario descrito.

(BZ#1729211)

ipcalc ahora devuelve la dirección de difusión correcta para las redes /31

Esta actualización corrige la utilidad **ipcalc** para que siga correctamente el estándar RFC 3021. Como resultado, **ipcalc** devuelve la dirección de difusión correcta cuando se utiliza el prefijo **/31** en una interfaz.

(BZ#1638834)

/etc/services contiene ahora la definición de puerto NRPE adecuada

Esta actualización añade la definición del puerto del servicio Nagios Remote Plug-in Executor (NRPE) al archivo **/etc/services**.

(BZ#1730396)

El código de resolución DNS de Postfix ahora utiliza res_search en lugar de res_query

Tras su anterior actualización en **postfix**, el código del resolver DNS utilizaba la función **res_query** en lugar de la función **res_search**. Como consecuencia, el resolvedor de DNS no buscaba los nombres de host en los dominios actuales y superiores con la siguiente configuración de **postfix**:

```
# postconf -e "smtp_host_lookup = dns"
# postconf -e "smtp_dns_resolver_options = res_defnames, res_dnsrch"
```

Por ejemplo, para:

```
# postconf -e \ "relayhost = [smtp]\N"
```

y el nombre de dominio en el formato *example.com*, el resolvedor DNS no utilizó el servidor SMTP smtp.*example.com* para la retransmisión.

Con esta actualización, el código del resolvedor de DNS se ha cambiado para utilizar **res_search** en lugar de **res_query**, y ahora busca los nombres de host en los dominios actuales y superiores correctamente.

(BZ#1723950)

PCRE, CDB y SQLite pueden utilizarse ahora con Postfix

En RHEL 8, el paquete **postfix** se ha dividido en múltiples subpaquetes, cada uno de los cuales proporciona un plug-in para una base de datos específica. Anteriormente, los paquetes RPM que contenían los complementos **postfix-pcre**, **postfix-cdb** y **postfix-sqlite** no se distribuían. En consecuencia, las bases de datos con estos plug-ins no podían ser utilizadas con Postfix. Esta actualización añade paquetes RPM que contienen los plug-ins PCRE, CDB y SQLite al repositorio de AppStream. Como resultado, estos plug-ins pueden ser utilizados después de que el paquete RPM apropiado sea instalado.

(BZ#1745321)

8.5. SEGURIDAD

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-2020:5243, **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#1897091)

openssl-pkcs11 ya no bloquea los dispositivos al intentar iniciar sesión en varios dispositivos

Anteriormente, el motor **openssl-pkcs11** intentaba iniciar sesión en el primer resultado de una búsqueda utilizando el URI PKCS #11 proporcionado y utilizaba el PIN proporcionado incluso si el primer resultado no era el dispositivo previsto y el PIN coincidía con otro dispositivo. Estos intentos fallidos de autenticación bloqueaban el dispositivo.

openssl-pkcs11 ahora intenta entrar en un dispositivo sólo si el URI PKCS #11 proporcionado coincide con un único dispositivo. El motor ahora falla intencionalmente en caso de que la búsqueda de PKCS #11 encuentre más de un dispositivo. Por esta razón, debe proporcionar un URI PKCS #11 que coincida con un solo dispositivo cuando utilice **openssl-pkcs11** para iniciar sesión en el dispositivo.

(BZ#1705505)

OpenSCAP los escaneos fuera de línea utilizando rpmverifyfile ahora funcionan correctamente

Antes de esta actualización, el explorador **OpenSCAP** no cambiaba correctamente el directorio de

trabajo actual en modo fuera de línea, y la función **fchdir** no se llamaba con los argumentos correctos en la sonda **rpmverifyfile** de **OpenSCAP**. El escáner **OpenSCAP** ha sido corregido para cambiar correctamente el directorio de trabajo actual en modo offline, y la función **fchdir** ha sido corregida para usar los argumentos correctos en **rpmverifyfile**. Como resultado, el contenido SCAP que contiene OVAL **rpmverifyfile** puede ser usado por OpenSCAP para escanear sistemas de archivos arbitrarios.

(BZ#1636431)

httpd ahora se inicia correctamente si se utiliza una clave privada ECDSA sin que coincida con la clave pública almacenada en un dispositivo PKCS #11

A diferencia de las claves RSA, las claves privadas ECDSA no contienen necesariamente información sobre la clave pública. En este caso, no se puede obtener la clave pública de una clave privada ECDSA. Por esta razón, un dispositivo PKCS #11 almacena la información de la clave pública en un objeto separado, ya sea un objeto de clave pública o un objeto de certificado. OpenSSL espera que la estructura **EVP_PKEY** proporcionada por un motor para una clave privada contenga la información de la clave pública. Al rellenar la estructura **EVP_PKEY** que se proporcionaba a OpenSSL, el motor del paquete **openssl-pkcs11** intentaba obtener la información de la clave pública sólo de los objetos de clave pública que coincidían e ignoraba los objetos de certificado presentes.

Cuando OpenSSL solicitaba una clave privada ECDSA al motor, la estructura **EVP_PKEY** proporcionada no contenía la información de la clave pública si ésta no estaba presente en el dispositivo PKCS #11, incluso cuando se disponía de un certificado coincidente que contenía la clave pública. Como consecuencia, dado que el servidor web Apache **httpd** llamaba a la función **X509_check_private_key()**, que requiere la clave pública, en su proceso de arranque, **httpd** fallaba al iniciarse en este escenario. Este problema se ha resuelto cargando la clave pública de la CE desde el certificado si el objeto de clave pública no está disponible. Como resultado, **httpd** ahora se inicia correctamente cuando las claves ECDSA se almacenan en un dispositivo PKCS #11.

(BZ#1664807)

scap-security-guide Las correcciones PCI-DSS de las reglas de auditoría ahora funcionan correctamente

Anteriormente, el paquete **scap-security-guide** contenía una combinación de remediación y una comprobación que podía dar lugar a uno de los siguientes escenarios:

- corrección incorrecta de las normas de auditoría
- evaluación de escaneo que contiene falsos positivos donde las reglas aprobadas se marcaron como fallidas

En consecuencia, durante el proceso de instalación de RHEL, el escaneo del sistema instalado reportó algunas reglas de Auditoría como fallidas o con errores.

Con esta actualización, se han corregido las correcciones y el escaneo del sistema instalado con la política de seguridad PCI-DSS ya no reporta falsos positivos para las reglas de Auditoría.

(BZ#1754919)

OpenSCAP ahora ofrece escaneo sin conexión de máquinas virtuales y contenedores

Anteriormente, la refactorización de la base de código **OpenSCAP** provocaba que ciertas sondas RPM no pudieran escanear los sistemas de archivos de las máquinas virtuales y los contenedores en modo offline. En consecuencia, las siguientes herramientas no podían incluirse en el paquete **openscap-utils**: **oscap-vm** y **oscap-chroot**. Además, el paquete **openscap-containers** fue eliminado por completo de RHEL 8. Con esta actualización se han solucionado los problemas de las sondas.

Como resultado, RHEL 8 contiene ahora las herramientas **oscap-podman**, **oscap-vm** y **oscap-chroot** en el paquete **openscap-utils**.

(BZ#1618489)

OpenSCAP rpmverifypackage ahora funciona correctamente

Anteriormente, las llamadas al sistema **chdir** y **chroot** eran llamadas dos veces por la sonda **rpmverifypackage**. En consecuencia, se producía un error cuando la sonda se utilizaba durante un análisis de **OpenSCAP** con contenido personalizado de Open Vulnerability and Assessment Language (OVAL). La sonda **rpmverifypackage** ha sido corregida para utilizar correctamente las llamadas al sistema **chdir** y **chroot**. Como resultado, **rpmverifypackage** ahora funciona correctamente.

(BZ#1646197)

8.6. RED

El bloqueo en la función qdisc_run ahora no provoca el bloqueo del kernel

Anteriormente, una condición de carrera cuando la disciplina de la cola **pfifo_fast** se restablece mientras el tráfico dequeuing estaba llevando a la transmisión de paquetes después de que fueron liberados. Como consecuencia, a veces el kernel se terminaba inesperadamente. Con esta actualización, se ha mejorado el bloqueo en la función **qdisc_run**. Como resultado, el kernel ya no se bloquea en el escenario descrito.

(BZ#1744397)

Las APIs de DBus en org.fedoraproject.FirewallD1.config.service funcionan como se espera

Anteriormente, las funciones **getIncludes**, **setIncludes** y **queryIncludes** de la API de DBus en org. **fedoraproject . FirewallD1** devolvían un mensaje de error: **org.fedoraproject.FirewallD1.Exception: list index out of range** due to bad indexing. Con esta actualización, las funciones **getIncludes**, **setIncludes** y **queryIncludes** de la API de DBus funcionan como se esperaba.

(BZ#1737045)

RHEL ya no registra una advertencia del kernel al descargar el módulo ipvs

Anteriormente, el módulo del servidor virtual IP**(ipvs**) utilizaba un recuento de referencias incorrecto, lo que provocaba una condición de carrera al descargar el módulo. En consecuencia, RHEL registraba una advertencia del kernel. Esta actualización corrige la condición de carrera. Como resultado, el kernel ya no registra la advertencia cuando se descarga el módulo **ipvs**.

(BZ#1687094)

La utilidad nft ya no interpreta los argumentos como opciones de la línea de comandos después del primer argumento no opcional

Anteriormente, la utilidad **nft** aceptaba opciones en cualquier parte de un comando **nft**. Por ejemplo, los administradores podían usar opciones entre o después de argumentos que no eran opciones. Como consecuencia, debido al guión inicial, **nft** interpretaba los valores de prioridad negativos como opciones, y el comando fallaba. El analizador de la línea de comandos de la utilidad **nft** se ha actualizado para que no interprete los argumentos que comienzan con un guión después de que se haya leído el primer argumento que no es una opción. Como resultado, los administradores ya no necesitan soluciones para pasar valores de prioridad negativa a **nft**.

Tenga en cuenta que, debido a este cambio, ahora debe pasar todas las opciones de comandos a **nft**

antes del primer argumento que no sea una opción. Antes de actualizar, verifique sus scripts de nftables para que se ajusten a este nuevo criterio para asegurarse de que el script funciona como se espera después de instalar esta actualización.

(BZ#1778883)

Los archivos /etc/hosts.allow y /etc/hosts.deny ya no contienen referencias obsoletas a los tcp_wrapperseliminados

Anteriormente, los archivos **/etc/hosts.allow** y **/etc/hosts.deny** contenían información obsoleta sobre el paquete **tcp_wrappers**. Los archivos se han eliminado en RHEL 8 porque ya no son necesarios para **tcp_wrappers**, que se ha eliminado.

(BZ#1663556)

Se ha añadido un parámetro de configuración a firewalld para desactivar la deriva de zonas

Anteriormente, el servicio **firewalld** contenía un comportamiento no documentado conocido como "zone drifting". RHEL 8.0 eliminó este comportamiento porque podía tener un impacto negativo en la seguridad. Como consecuencia, en los hosts que utilizaban este comportamiento para configurar una zona de captura o de reserva, **firewalld** denegaba conexiones que antes estaban permitidas. Esta actualización vuelve a añadir el comportamiento de deriva de zona, pero como una característica configurable. Como resultado, los usuarios pueden ahora decidir usar el desvío de zona o deshabilitar el comportamiento para una configuración más segura del cortafuegos.

Por defecto, en RHEL 8.2, el nuevo parámetro **AllowZoneDrifting** en el archivo **/etc/firewalld/firewalld.conf** está establecido en **yes**. Tenga en cuenta que, si el parámetro está activado, **firewalld** registra:

> ADVERTENCIA: AllowZoneDrifting está activado. Se considera una opción de configuración insegura. Se eliminará en una futura versión. Por favor, considere desactivarla ahora.

(BZ#1772208)

8.7. NÚCLEO

Ahora la memoria de subsección hotplug es totalmente compatible

Anteriormente, algunas plataformas alineaban las regiones de memoria física, como los Módulos Duales en Línea (DIMM) y los conjuntos de intercalación a los límites de memoria de 64MiB. Sin embargo, como el subsistema de conexión en caliente de Linux utiliza un tamaño de memoria de 128MiB, la conexión en caliente de nuevos dispositivos hacía que se superpusieran varias regiones de memoria en una única ventana de memoria de conexión en caliente. Consecuentemente, esto causó un fallo en el listado de los espacios de nombres de memoria persistente disponibles con el siguiente o similar trazado de llamada:

```
WARNING: CPU: 38 PID: 928 at arch/x86/mm/init_64.c:850
add_pages+0x5c/0x60
   [..]
   RIP: 0010:add_pages+0x5c/0x60
   [..]
   Call Trace:
    devm_memremap_pages+0x460/0x6e0
    pmem_attach_disk+0x29e/0x680 [nd_pmem]
    ? nd_dax_probe+0xfc/0x120 [libnvdimm]
    nvdimm_bus_probe+0x66/0x160 [libnvdimm]
```

Esta actualización corrige el problema y admite el subsistema de hotplug de Linux para permitir que varias regiones de memoria compartan una única ventana de memoria de hotplug.

(BZ#1724969)

La corrupción de datos ahora desencadena un BUG en lugar de un mensaje WARN

Con esta mejora, las corrupciones de la lista en **lib/list_debug.** c ahora desencadenan un BUG, que genera un informe con un **vmcore**. Anteriormente, cuando se encontraba una corrupción de datos, se generaba un simple WARN, que probablemente pasaba desapercibido. Con el **set CONFIG_BUG_ON_DATA_CORRUPTION**, el kernel ahora crea un crash y dispara un BUG en respuesta a la corrupción de datos. Esto evita daños mayores y reduce el riesgo de seguridad. El **kdump** ahora genera un **vmcore**, lo que mejora la notificación de errores de corrupción de datos.

(BZ#1714330)

La compatibilidad con la tarjeta Intel Carlsville está disponible pero no se ha verificado en RHEL 8.2

El soporte de la tarjeta **Intel Carlsville** está disponible pero no ha sido probado en Red Hat Enterprise Linux 8.2.

(BZ#1720227)

RPS y XPS ya no colocan trabajos en CPUs aisladas

Anteriormente, el mecanismo de cola de software Receive Packet Steering (RPS) y el mecanismo de selección de cola de transmisión Transmit Packet Steering (XPS) asignaban trabajos en todos los conjuntos de CPU, incluidas las CPU aisladas. En consecuencia, esto podía provocar un pico de latencia inesperado en un entorno de tiempo real cuando una carga de trabajo sensible a la latencia utilizaba la misma CPU en la que se ejecutaban los trabajos RPS o XPS. Con esta actualización, la función **store_rps_map()** no incluye ninguna CPU aislada a efectos de configuración de RPS. Del mismo modo, los controladores del kernel utilizados para la configuración de XPS respetan el aislamiento de la CPU. Como resultado, RPS y XPS ya no colocan trabajos en CPUs aisladas en el escenario descrito. Si se configura una CPU aislada en el archivo **/sys/devices/pci*/net/dev/queues/rx-*/rps_cpus**, aparece el siguiente error:

```
Error: "-bash: echo:write error: Argumento inválido"
```

Sin embargo, la configuración manual de una CPU aislada en el archivo **/sys/devices/pci*/net/dev/queues/tx-*/xps_cpus** asigna con éxito los trabajos XPS en la CPU aislada.

Tenga en cuenta que una carga de trabajo de red en un entorno con CPUs aisladas es probable que experimente alguna variación de rendimiento.

(BZ#1867174)

8.8. SISTEMAS DE ARCHIVOS Y ALMACENAMIENTO

Los controladores SCSI ya no utilizan una cantidad excesiva de memoria

Anteriormente, algunos controladores SCSI utilizaban una mayor cantidad de memoria que en RHEL 7. En algunos casos, como la creación de vPort en un adaptador de bus de host (HBA) de canal de fibra, el uso de memoria era excesivo, dependiendo de la configuración del sistema.

El aumento del uso de la memoria se debe a la preasignación de memoria en la capa de bloques. Tanto la programación de dispositivos de bloques de cola múltiple (BLK-MQ) como la pila SCSI de cola

múltiple (SCSI-MQ) preasignaban memoria para cada solicitud de E/S, lo que provocaba un mayor uso de la memoria.

Con esta actualización, la capa de bloques limita la cantidad de preasignación de memoria y, como resultado, los controladores SCSI ya no utilizan una cantidad excesiva de memoria.

(BZ#1698297)

VDO ahora puede suspender antes de que UDS haya terminado de reconstruir

Anteriormente, el comando **dmsetup suspender** no respondía si se intentaba suspender un volumen VDO mientras se reconstruía el índice UDS. El comando terminaba sólo después de la reconstrucción.

Con esta actualización, el problema se ha solucionado. El comando **dmsetup suspender** puede terminar antes de la reconstrucción UDS se hace sin llegar a ser insensible.

(BZ#1737639)

8.9. LENGUAJES DE PROGRAMACIÓN DINÁMICOS, SERVIDORES WEB Y DE BASES DE DATOS

Se han solucionado los problemas de registro de mod_cgid

Antes de esta actualización, si el módulo **httpd** de Apache **mod_cgid** se utilizaba bajo un módulo de multiprocesamiento roscado (MPM), se producían los siguientes problemas de registro:

- La salida **stderr** del script CGI no tenía el prefijo de la información estándar de la marca de tiempo.
- La salida **stderr** del script CGI no era redirigida correctamente a un archivo de registro específico del **VirtualHost**, si estaba configurado.

Esta actualización corrige los problemas, y el registro de **mod_cgid** ahora funciona como se esperaba.

(BZ#1633224)

8.10. COMPILADORES Y HERRAMIENTAS DE DESARROLLO

Los objetos compartidos no reubicados y no inicializados ya no provocan fallos si dlopen falla

Anteriormente, si la llamada **dlopen** fallaba, el enlazador dinámico **de glibc** no eliminaba los objetos compartidos con la marca **NODELETE** antes de informar del error. En consecuencia, los objetos compartidos no reubicados y no inicializados permanecían en la imagen del proceso, resultando eventualmente en fallos de aserción o caídas. Con esta actualización, el cargador dinámico utiliza un estado **NODELETE** pendiente para eliminar los objetos compartidos ante un fallo de **dlopen**, antes de marcarlos como **NODELETE** de forma permanente. Como resultado, el proceso no deja ningún objeto sin ubicar. Además, los fallos de enlace perezoso mientras se ejecutan los constructores y destructores ELF ahora terminan el proceso.

(BZ#1410154)

Las funciones SIMD avanzadas en la arquitectura ARM de 64 bits ya no se compilan mal cuando se resuelven de forma perezosa

Anteriormente, el nuevo estándar de llamadas a procedimientos vectoriales (PCS) para la SIMD

avanzada no guardaba y restauraba correctamente ciertos registros guardados en la calle al resolver perezosamente funciones de la SIMD avanzada. Como consecuencia, los binarios podían comportarse mal en tiempo de ejecución. Con esta actualización, las funciones vectoriales de SIMD avanzada y SVE en la tabla de símbolos se marcan con **.variant_pcs** y, como resultado, el enlazador dinámico enlazará dichas funciones antes.

(BZ#1726641)

El script envolvente de sudo ahora analiza las opciones

Anteriormente, el script envolvente **/opt/redhat/devtoolset*/root/usr/bin/sudo** no analizaba correctamente las opciones de **sudo**. Como consecuencia, algunas opciones de **sudo** (por ejemplo, **sudo -i**) no podían ser ejecutadas. Con esta actualización, más opciones de **sudo** se analizan correctamente y, como resultado, el script envolvente de **sudo** funciona más como **/usr/bin/sudo**.

(BZ#1774118)

Se ha corregido la alineación de las variables TLS en glibc

Anteriormente, los datos alineados del almacenamiento local de hilos (TLS) podían, bajo ciertas condiciones, instanciarse sin la alineación esperada. Con esta actualización, la biblioteca de hilos POSIX **libpthread** ha sido mejorada para asegurar la correcta alineación bajo cualquier condición. Como resultado, los datos TLS alineados son ahora instanciados correctamente para todos los hilos con la alineación correcta.

(BZ#1764214)

Las llamadas repetidas a pututxline tras un error EINTR o EAGAIN ya no corrompen el archivo utmp

Cuando la función **pututxline** intenta adquirir un bloqueo y no lo consigue a tiempo, la función devuelve con el código de error **EINTR** o **EAGAIN**. Anteriormente, en esta situación, si se volvía a llamar inmediatamente a **pututxline** y se lograba obtener el bloqueo, no se utilizaba un espacio coincidente ya asignado en el archivo **utmp**, sino que se añadía otra entrada en su lugar. Como consecuencia, estas entradas no utilizadas aumentaban sustancialmente el tamaño del archivo **utmp**. Esta actualización corrige el problema, y ahora las entradas se añaden al archivo **utmp** correctamente.

(BZ#1749439)

mtrace ya no se cuelga cuando se producen fallos internos

Anteriormente, un defecto en la implementación de la herramienta **mtrace** podía hacer que el rastreo de memoria se colgara. Para solucionar este problema, la implementación del rastreo de memoria de **mtrace** se ha hecho más robusta para evitar el cuelgue incluso ante fallos internos. Como resultado, los usuarios pueden ahora llamar a **mtrace** y ya no se cuelga, completándose en un tiempo limitado.

(BZ#1764235)

La función de bifurcación evita ciertos bloqueos relacionados con el uso de pthread_atfork

Anteriormente, si un programa registraba un manejador de **atfork** e invocaba a **fork** desde un manejador de señales asíncronas, un defecto en el bloqueo interno dependiente de la implementación podía hacer que el programa se congelara. Con esta actualización, la implementación de **fork** y sus manejadores **atfork** se ajusta para evitar el bloqueo en programas de un solo hilo.

(BZ#1746928)

strstr ya no devuelve coincidencias incorrectas para un patrón truncado

En algunas plataformas IBM Z (z15, antes conocida como arch13), la función **strstr** no actualizaba correctamente un registro de la CPU al manejar patrones de búsqueda que cruzaban un límite de página. Como consecuencia, **strstr** devolvía coincidencias incorrectas. Esta actualización corrige el problema, y como resultado, **strstr** funciona como se espera en el escenario mencionado.

(BZ#1777241)

Se han corregido las expresiones de elipsis de fuente de C.UTF-8 en glibc

Anteriormente, un defecto en la configuración regional de origen C.UTF-8 hacía que todos los puntos de código Unicode por encima de U 10000 carecieran de pesos de cotejo. Como consecuencia, todos los puntos de código por encima de U 10000 no se cotejaban como se esperaba. Se ha corregido la configuración regional de origen C.UTF-8 y la configuración regional binaria recién compilada tiene ahora pesos de cotejo para todos los puntos de código Unicode. La configuración regional C.UTF-8 compilada es 5,3MiB mayor como resultado de esta corrección.

(BZ#1361965)

glibc ya no falla cuando se llama a getpwent( ) sin llamar a setpwent()

Si su archivo **/etc/nsswitch.conf** apuntaba al proveedor de contraseñas Berkeley DB **(db**), podía solicitar datos usando la función **getpwent** () sin llamar primero a setpwent( ) sólo una vez. Cuando se llamaba a la función **endpwent** (), las siguientes llamadas a **getpwent()** sin llamar primero a **setpwent** () hacían que **glibc** fallara porque **endpwent()** no podía restablecer los internos para permitir una nueva consulta. Esta actualización soluciona el problema. Como resultado, después de terminar una consulta con **endpwent()**, las siguientes llamadas a **getpwent** () iniciarán una nueva consulta incluso si no se llama a **setpwent()**.

(BZ#1747502)

ltrace ahora puede rastrear las llamadas al sistema en los binarios reforzados

Anteriormente, **ltrace** no producía ningún resultado en ciertos binarios reforzados, como los binarios del sistema, en las arquitecturas de 64 bits de AMD e Intel. Con esta actualización, **ltrace** ahora puede rastrear las llamadas al sistema en los binarios reforzados.

(BZ#1655368)

El fallo JCC de Intel ya no provoca una pérdida de rendimiento significativa en el compilador GCC

Ciertas CPUs de Intel están afectadas por el error de código condicional de salto (JCC) que provoca la ejecución incorrecta de instrucciones de máquina. En consecuencia, las CPUs afectadas podrían no ejecutar los programas correctamente. La solución completa implica la actualización del microcódigo de las CPUs vulnerables, lo que puede causar una degradación del rendimiento. Esta actualización habilita una solución en el ensamblador que ayuda a reducir la pérdida de rendimiento. La solución está activada por defecto en **not**.

Para aplicar la solución, recompile un programa utilizando GCC con la opción de línea de comandos **-Wa,-mbranches-within-32B-boundaries**. Un programa recompilado con esta opción de línea de comandos no se verá afectado por el fallo de JCC, pero la actualización del microcódigo sigue siendo necesaria para proteger completamente un sistema.

Tenga en cuenta que la aplicación de la solución aumentará el tamaño del programa y puede causar una ligera disminución del rendimiento, aunque debería ser menor de lo que habría sido sin la recompilación.

(BZ#1777002)

make ya no se ralentiza al utilizar construcciones paralelas

Anteriormente, mientras se ejecutaban compilaciones paralelas, los subprocesos **de make** podían dejar de responder temporalmente cuando esperaban su turno para ejecutarse. Como consecuencia, las construcciones con valores **-j** altos se ralentizaban o se ejecutaban con valores **-j** efectivos más bajos. Con esta actualización, la lógica de control de trabajos de **make** es ahora no bloqueante. Como resultado, las compilaciones con valores **-j** altos se ejecutan a la máxima velocidad **-j**.

(BZ#1774790)

La herramienta ltrace ahora informa correctamente de las llamadas a funciones

Debido a las mejoras en el endurecimiento de los binarios aplicadas a todos los componentes de RHEL, la herramienta **ltrace** no podía detectar anteriormente las llamadas a funciones en los archivos binarios procedentes de los componentes de RHEL. Como consecuencia, la salida de **ltrace** estaba vacía porque no informaba de ninguna llamada detectada cuando se utilizaba en dichos archivos binarios. Esta actualización corrige la forma en que **ltrace** maneja las llamadas a funciones, lo que evita que se produzca el problema descrito.

(BZ#1618748)

8.11. GESTIÓN DE LA IDENTIDAD

La utilidad dsctl ya no falla al gestionar instancias con un guión en su nombre

Anteriormente, la utilidad **dsctl** no analizaba correctamente los guiones en los nombres de las instancias de Directory Server. Como consecuencia, los administradores no podían utilizar **dsctl** para gestionar instancias con un guión en su nombre. Esta actualización corrige el problema, y **dsctl** ahora funciona como se espera en el escenario mencionado.

(BZ#1715406)

Los nombres de las instancias del Servidor de Directorio ahora pueden tener hasta 103 caracteres

Cuando un cliente LDAP establece una conexión con Directory Server, el servidor almacena la información relacionada con la dirección del cliente en un buffer local. Anteriormente, el tamaño de este búfer era demasiado pequeño para almacenar un nombre de ruta LDAPI de más de 46 caracteres. Este es el caso, por ejemplo, si el nombre de la instancia del Servidor de Directorio es demasiado largo. Como consecuencia, el servidor terminaba inesperadamente debido a un desbordamiento del búfer. Esta actualización aumenta el tamaño del búfer hasta el tamaño máximo que admite la biblioteca Netscape Portable Runtime (NSPR) para el nombre de la ruta. Como resultado, Directory Server ya no se bloquea en el escenario mencionado.

Tenga en cuenta que, debido a la limitación de la biblioteca NSPR, un nombre de instancia puede tener un máximo de 103 caracteres.

(BZ#1748016)

La utilidad pkidestroy ahora escoge la instancia correcta

Anteriormente, el comando **pkidestroy --force** ejecutado en una instancia medio eliminada elegía la instancia **pki-tomcat** por defecto, independientemente del nombre de la instancia especificado con la opción **-i *instance***.

Como consecuencia, esto eliminó la instancia **pki-tomcat** en lugar de la instancia prevista, y la opción **--remove-logs** no eliminó los registros de la instancia prevista. **pkidestroy** ahora aplica el nombre de la instancia correcta, eliminando sólo los restos de la instancia prevista.

(BZ#1698084)

Se ha actualizado la descripción de ldap_user_authorized_service en la página man de sssd-ldap

La pila de módulos de autenticación enchufables (PAM) ha cambiado en RHEL 8. Por ejemplo, la sesión de usuario **systemd** ahora inicia una conversación PAM utilizando el servicio PAM **systemd-user**. Este servicio ahora incluye recursivamente el servicio PAM **system-auth**, que puede incluir la interfaz **pam_sss.so**. Esto significa que el control de acceso SSSD siempre es llamado.

Debe tener en cuenta este cambio cuando diseñe reglas de control de acceso para los sistemas RHEL 8. Por ejemplo, puede añadir el servicio **systemd-user** a la lista de servicios permitidos.

Tenga en cuenta que para algunos mecanismos de control de acceso, como IPA HBAC o AD GPOs, el servicio **systemd-user** se ha añadido a la lista de servicios permitidos por defecto y no es necesario realizar ninguna acción.

La página man de **sssd-ldap** ha sido actualizada para incluir esta información.

(BZ#1669407)

Ahora se muestra la información sobre los registros DNS necesarios al activar la compatibilidad con la confianza de AD en IdM

Anteriormente, cuando se habilitaba el soporte para la confianza de Active Directory (AD) en la instalación de Red Hat Enterprise Linux Identity Management (IdM) con gestión externa de DNS, no se mostraba información sobre los registros DNS requeridos. Era necesario introducir manualmente el comando **ipa dns-update-system-records --dry-run** para obtener una lista de todos los registros DNS requeridos por IdM.

Con esta actualización, el comando **ipa-adtrust-install** enumera correctamente los registros del servicio DNS para añadirlos manualmente a la zona DNS.

(BZ#1665051)

8.12. ESCRITORIO

GNOME Shell en Wayland ya no funciona lentamente cuando se utiliza un renderizador de software

Anteriormente, el back-end de Wayland de GNOME Shell no utilizaba un framebuffer cacheable cuando se utilizaba un renderizador por software. Como consecuencia, el GNOME Shell renderizado por software en Wayland era lento comparado con el GNOME Shell renderizado por software en el back end de X.org.

Con esta actualización, se ha añadido un framebuffer de sombra intermedio en GNOME Shell en Wayland. Como resultado, GNOME Shell en Wayland, renderizado por software, funciona tan bien como GNOME Shell en X.org.

(BZ#1737553)

8.13. VIRTUALIZACIÓN

El inicio de una máquina virtual en un procesador Intel Core de 10ª generación ya no falla

Anteriormente, el inicio de una máquina virtual (VM) fallaba en un modelo de host que utilizaba un procesador Intel Core de 10ª generación, también conocido como Icelake-Server. Con esta actualización, **libvirt** ya no intenta desactivar la función **pconfig** CPU, que no es compatible con QEMU. Como resultado, el inicio de una máquina virtual en un modelo de host que ejecuta un procesador Intel de 10ª generación ya no falla.

(BZ#1749672)

El uso de cloud-init para aprovisionar máquinas virtuales en Microsoft Azure ahora funciona correctamente

Anteriormente, no era posible utilizar la utilidad **cloud-init** para aprovisionar una máquina virtual (VM) RHEL 8 en la plataforma Microsoft Azure. Esta actualización corrige el manejo de **cloud-init** de los puntos finales de Azure, y el aprovisionamiento de máquinas virtuales RHEL 8 en Azure ahora se realiza como se espera.

(BZ#1641190)

Las máquinas virtuales de RHEL 8 en los hosts de RHEL 7 pueden verse de forma fiable con una resolución superior a 1920x1200

Anteriormente, cuando se utilizaba una máquina virtual (VM) RHEL 8 que se ejecutaba en un sistema anfitrión RHEL 7, ciertos métodos de visualización de la salida gráfica de la VM, como la ejecución de la aplicación en modo quiosco, no podían utilizar una resolución superior a 1920x1200. Como consecuencia, la visualización de VMs utilizando esos métodos sólo funcionaba en resoluciones de hasta 1920x1200 aunque el hardware del host soportara resoluciones mayores. Esta actualización ajusta los controladores DRM y QXL de forma que se evite el problema descrito.

(BZ#1635295)

La personalización de una VM ESXi utilizando cloud-init y el reinicio de la VM ahora funciona correctamente

Anteriormente, si el servicio **cloud-init** se utilizaba para modificar una máquina virtual (VM) que se ejecutaba en el hipervisor VMware ESXi para utilizar IP estática y la VM se clonaba a continuación, la nueva VM clonada tardaba en algunos casos mucho tiempo en reiniciarse. Esta actualización modifica **cloud-init** para que no reescriba la IP estática de la VM a DHCP, lo que evita que se produzca el problema descrito.

(BZ#1666961, BZ#1706482)

8.14. CONTENEDORES

La extracción de imágenes del registro de quay.io ya no conduce a imágenes no deseadas

Anteriormente, tener el registro de imágenes de contenedores quay.io en la lista de búsqueda de registros por defecto proporcionada en **/etc/containers/registries**.conf podía permitir a un usuario obtener una imagen falsa cuando se utilizaba un nombre corto. Para solucionar este problema, se ha eliminado el registro de imágenes de contenedores de quay.io de la lista de búsqueda de registros por defecto en **/etc/containers/registries**.conf. Como resultado, la extracción de imágenes del registro **quay**.io ahora requiere que los usuarios especifiquen el nombre completo del repositorio, como **quay.io/myorg/myimage**. El registro quay.io puede añadirse de nuevo a la lista de búsqueda de registros por defecto en **/etc/containers/registries.** conf para volver a activar la extracción de imágenes de contenedores utilizando nombres cortos, sin embargo, esto no se recomienda ya que podría crear un riesgo de seguridad.

(BZ#1784267)

CAPÍTULO 9. AVANCES TECNOLÓGICOS

Esta parte proporciona una lista de todas las Previsiones Tecnológicas disponibles en Red Hat Enterprise Linux 8.2.

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 .

9.1. RED

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)

La utilidad dracut ahora soporta la creación de imágenes initrd con soporte de NetworkManager como una tecnología previa

Por defecto, la utilidad **dracut** utiliza un script de shell para gestionar la red en el disco RAM inicial**(initrd**). En ciertos casos, esto podría causar problemas cuando el sistema cambia del disco RAM al sistema operativo que utiliza NetworkManager para configurar la red. Por ejemplo, NetworkManager

podría enviar otra solicitud de DHCP, incluso si el script en el disco RAM ya solicitó una dirección IP. Esta solicitud desde el disco RAM podría resultar en un tiempo de espera.

Para resolver este tipo de problemas, **dracut** en RHEL 8.2 puede ahora utilizar NetworkManager en el disco RAM. Utilice los siguientes comandos para habilitar la función y recrear las imágenes del disco RAM:

```
echo 'add_dracutmodules+=" network-manager "' > /etc/dracut.conf.d/enable-nm.conf
dracut -vf --regenerate-all
```

Tenga en cuenta que Red Hat no admite las funciones de vista previa de la tecnología. Sin embargo, para dar su opinión sobre esta función, póngase en contacto con el soporte de Red Hat.

(BZ#1626348)

El controlador mlx5_core es compatible con el adaptador de red Mellanox ConnectX-6 Dx como Technology Preview

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. Tenga en cuenta que Red Hat proporciona esta función como una Muestra de Tecnología no soportada.

(BZ#1687434)

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)

9.2. NÚCLEO

kexec fast reboot como Technology Preview

La función de reinicio rápido de **kexec**, sigue estando disponible como Muestra de Tecnología. El reinicio es ahora significativamente más rápido gracias al **reinicio** rápido de kexec. Para utilizar esta función, cargue el kernel de kexec manualmente y, a continuación, 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**.
- La función eXpress Data Path (XDP), una tecnología de red que permite el procesamiento rápido de paquetes en el kernel utilizando la máquina virtual **eBPF**.

(BZ#1559616)

libbpf está disponible como Technology Preview

El paquete **libbpf** está actualmente disponible como Technology Preview. El paquete **libbpf** es crucial para las aplicaciones relacionadas con bpf como **bpftrace** y el desarrollo de **bpf/xdp**.

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)

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)

9.3. 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 8.2, 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. Consulte la documentación del núcleo de Linux para obtener información adicional: https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

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 se puede utilizar la configuración predeterminada del motor de contenedores; es decir, un nivel de superposición, un directorio inferior, y ambos niveles inferiores y superiores 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 ver cambios 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.

- Comandos utilizados con XFS:
  - Los sistemas de archivos XFS deben crearse con la opción **-n ftype=1** activada para su uso como superposición.
  - Con el rootfs y cualquier sistema de archivos creado durante la instalación del sistema, establezca los parámetros **--mkfsoptions=-n ftype=1** en el kickstart de Anaconda.
  - Al crear un nuevo sistema de archivos después de la instalación, ejecute el comando **# mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE**.
  - Para determinar si un sistema de archivos existente es elegible para su uso como superposición, ejecute el comando **# xfs_info /PATH/TO/DEVICE | grep ftype** para ver si la opción **ftype=1** está habilitada.
- Las etiquetas de seguridad SELinux están habilitadas por defecto en todos los motores de contenedores compatibles con OverlayFS.
- Hay varios problemas conocidos 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.

(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 8.2 actualiza Stratis a la versión 2.0.0. Esta versión mejora la fiabilidad y la API DBus de Stratis. Para más información sobre la versión 2.0.0, vea Stratis 2.0.0 Release Notes.

(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)

9.4. ALTA DISPONIBILIDAD Y CLUSTERS

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)

9.5. 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)

La comprobación de la salud general de su infraestructura de clave pública ya está disponible como Muestra de Tecnología

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#1303254)

9.6. 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#1667516, BZ#1667225)

9.7. 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)

9.8. 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)

rhel-system-roles-sap disponible como Technology Preview

El paquete **rhel-system-roles-sap** proporciona roles de sistema de 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 SAP, aplicando automáticamente los ajustes óptimos que se basan en las mejores prácticas descritas en las Notas SAP pertinentes. 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** están disponibles como Technology Preview:

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

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

Nota: Está previsto que RHEL 8.2 for SAP Solutions se valide para su uso con SAP HANA en arquitectura Intel 64 e IBM POWER9. La compatibilidad con otras aplicaciones y productos de bases de datos de SAP, por ejemplo, SAP NetWeaver y SAP ASE, está vinculada a las versiones GA, y los clientes pueden utilizar las funciones de RHEL 8.2 tras la versión GA. Consulte las notas de SAP 2369910 y 2235581 para obtener la información más reciente sobre las versiones validadas y el soporte de SAP.

(BZ#1660832)

9.9. VIRTUALIZACIÓN

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 **i40evf**. 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)

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)

9.10. CONTENEDORES

la imagen del contenedor **skopeo** está disponible como Technology Preview

La imagen de contenedor **registry.redhat.io/rhel8/skopeo** es una implementación en contenedor del paquete **skopeo**. El **skopeo** es una herramienta de línea de comandos que realiza varias operaciones en imágenes de contenedores y repositorios de imágenes. Esta imagen de contenedor permite inspeccionar y copiar imágenes de contenedor de un registro de contenedores no autenticado a otro.

(BZ#1627900)

la imagen del contenedor **buildah** está disponible como Technology Preview

La imagen de contenedor **registry.redhat.io/rhel8/buildah** es una implementación en contenedor del paquete **buildah**. El **buildah** es una herramienta que 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.

(BZ#1627898)

CAPÍTULO 10. FUNCIONALIDAD OBSOLETA

Esta parte proporciona una visión general de la funcionalidad que ha sido *deprecated* en Red Hat Enterprise Linux 8.2.

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 .

10.1. 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)

10.2. 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)

10.3. SEGURIDAD

Los cifradosNSS SEED están obsoletos

La librería Mozilla Network Security Services**(NSS**) no soportará suites de cifrado TLS que usen un cifrado SEED en una futura versión. Para las implementaciones que dependen de los cifrados SEED, Red Hat recomienda habilitar el soporte para otros conjuntos de cifrado. De esta forma, se asegura una transición suave cuando NSS elimine el soporte para ellos.

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)

10.4. 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)

10.5. 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)

10.6. 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)

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)

10.7. 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)

10.8. 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)

10.9. 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)

10.10. 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)

El modelo de CPU cpu64-rhel6 ha sido obsoleto y eliminado

El modelo de CPU virtual de QEMU **cpu64-rhel6** ha quedado obsoleto en RHEL 8.1, y ha sido eliminado en RHEL 8.2. Se recomienda utilizar los otros modelos de CPU proporcionados por QEMU y libvirt, según la CPU presente en la máquina anfitriona.

(BZ#1741346)

10.11. 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
- herramientas de red
- red-scripts
- nss-pam-ldapd
- sendmail
- yp-tools
- ypbind
- ypserv

CAPÍTULO 11. PROBLEMAS CONOCIDOS

Esta parte describe los problemas conocidos en Red Hat Enterprise Linux 8.2.

11.1. 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)

La instalación de Anaconda incluye límites bajos de requisitos de configuración de recursos mínimos

Anaconda inicia la instalación en sistemas con una configuración mínima de recursos disponibles y no proporciona un mensaje previo de advertencia sobre los recursos necesarios para realizar la instalación con éxito. Como resultado, la instalación puede fallar y los errores de salida no proporcionan mensajes claros para una posible depuración y recuperación. Para solucionar este problema, asegúrese de que el sistema dispone de los recursos mínimos necesarios para la instalación: 2GB de memoria en PPC64(LE) y 1GB en x86_64. Como resultado, debería ser posible realizar una instalación exitosa.

(BZ#1696609)

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

La instalación de RHEL 8 falla cuando se utiliza un archivo Kickstart que contiene el comando reboot **--kexec**. Para evitar el problema, utilice el comando **reboot** en lugar de reboot **--kexec** en su archivo Kickstart.

(BZ#1672405)

La configuración inicial de RHEL 8 no puede realizarse a través de SSH

Actualmente, la interfaz de configuración inicial de RHEL 8 no se muestra cuando se inicia la sesión en el sistema mediante SSH. Como consecuencia, es imposible realizar la configuración inicial en una máquina RHEL 8 gestionada mediante SSH. Para solucionar este problema, realice la configuración inicial en la consola principal del sistema (ttyS0) y, posteriormente, inicie sesión mediante SSH.

(BZ#1676439)

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 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)

En ocasiones, la instalación de la interfaz gráfica de usuario mediante la imagen ISO del DVD binario no puede llevarse a cabo sin el registro de la CDN

Cuando se realiza una instalación GUI utilizando el archivo de imagen ISO de DVD binario, una condición de carrera en el instalador puede a veces impedir que la instalación continúe hasta que se registre el sistema utilizando la función Conectar con Red Hat. Para solucionar este problema, realice los siguientes pasos:

1. Seleccione **Installation Source** en la ventana **Installation Summary** de la instalación de la GUI.
2. Compruebe que está seleccionado **Auto-detected installation media**
3. Haga clic en **Done** para confirmar la selección y volver a la ventana **Installation Summary**.
4. Compruebe que **Local Media** aparece como el estado **Installation Source** en la ventana **Installation Summary**.

Como resultado, puede proceder a la instalación sin registrar el sistema utilizando la función Conectar con Red Hat.

(BZ#1823578)

Al copiar el contenido del archivo DVD.iso binario en una partición se omiten los archivos .treeinfo y .discinfo

Durante la instalación local, mientras se copia el contenido del archivo de imagen RHEL 8 Binary

DVD.iso a una partición, el * en el comando **cp <path>/* <mounted partition>/dir** falla al copiar los archivos **.treeinfo** y **.discinfo**. Estos archivos son necesarios para una instalación correcta. Como resultado, los repositorios BaseOS y AppStream no se cargan, y un mensaje de registro relacionado con la depuración en el archivo **anaconda.log** es el único registro del problema.

Para solucionar el problema, copie los archivos **.treeinfo** y **.discinfo** que faltan en la partición.

(BZ#1687747)

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=<URL> inst.noverifyssl
```

(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

En 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)

11.2. 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)

Los datos de los dispositivos de almacenamiento de rutas múltiples se pierden al instalar RHEL utilizando un archivo Kickstart

Los datos de los dispositivos de almacenamiento multirruta que están conectados a un host se pierden al instalar RHEL utilizando un archivo Kickstart. Este problema se produce porque el instalador no ignora los dispositivos de almacenamiento de rutas múltiples que se especifican mediante el comando **ignoredisk --drives**. Como resultado, se pierden los datos de los dispositivos.

Para solucionar este problema, separe los dispositivos antes de la instalación o utilice el comando **ignoredisk --only-use** para especificar los dispositivos para la instalación.

(BZ#1862131)

11.3. SHELL Y HERRAMIENTAS DE LÍNEA DE COMANDOS

Las aplicaciones que utilizan el protocolo Wayland no pueden ser reenviadas a servidores de visualización remotos

En Red Hat Enterprise Linux 8, la mayoría de las aplicaciones utilizan el protocolo Wayland por defecto en lugar del protocolo X11. Como consecuencia, el servidor ssh no puede reenviar las aplicaciones que usan el protocolo Wayland pero es capaz de reenviar las aplicaciones que usan el protocolo X11 a un servidor de visualización remoto.

Para solucionar este problema, establezca la variable de entorno **GDK_BACKEND=x11** antes de iniciar las aplicaciones. Como resultado, la aplicación puede ser reenviada a servidores de visualización remotos.

(BZ#1686892)

systemd-resolved.service no se inicia en el arranque

El servicio **systemd-resolved** ocasionalmente no se inicia en el arranque. Si esto ocurre, reinicie el servicio manualmente después de que termine el arranque utilizando el siguiente comando:

```
# systemctl start systemd-resolved
```

Sin embargo, el fallo de **systemd-resolved** on boot no afecta a ningún otro servicio.

(BZ#1640802)

11.4. SEGURIDAD

La vigilancia de los ejecutables de auditoría en los enlaces simbólicos no funciona

La monitorización de archivos proporcionada por la opción **-w** no puede rastrear directamente una ruta. Tiene que resolver la ruta a un dispositivo y un inodo para hacer una comparación con el programa ejecutado. Un reloj que monitoriza un enlace simbólico ejecutable monitoriza el dispositivo y un inodo del propio enlace simbólico en lugar del programa ejecutado en memoria, que se encuentra a partir de la resolución del enlace simbólico. Incluso si la vigilancia resuelve el enlace simbólico para obtener el programa ejecutable resultante, la regla se dispara en cualquier binario de llamada múltiple llamado desde un enlace simbólico diferente. Esto hace que se inunden los registros con falsos positivos. En consecuencia, las vigilancias de auditoría de ejecutables en enlaces simbólicos no funcionan.

Para solucionar el problema, configure una vigilancia para la ruta resuelta del ejecutable del programa, y filtre los mensajes de registro resultantes utilizando el último componente listado en los campos **comm=** o **proctitle=**.

(BZ#1846345)

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)

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)

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)

SELinux impide que systemd-journal-gatewayd llame a newfstat() en archivos de memoria compartida creados por corosync

La política de SELinux no contiene una regla que permita al demonio **systemd-journal-gatewayd** acceder a los archivos creados por el servicio **corosync**. Como consecuencia, SELinux niega a **systemd-journal-gatewayd** la posibilidad de llamar a la función **newfstat()** en los archivos de memoria compartida creados por **corosync**.

Para solucionar este problema, cree un módulo de política local con una regla de permiso que permita el escenario descrito. Consulte la página man de **audit2allow(1)** para obtener más información sobre la generación de la política de SELinux *allow* y las reglas de *dontaudit*. Como resultado de la solución anterior, **systemd-journal-gatewayd** puede llamar a la función en archivos de memoria compartida creados por **corosync** con SELinux en modo de aplicación.

(BZ#1746398)

SELinux impide que auditd detenga o apague el sistema

La política de SELinux no contiene una regla que permita al demonio de Auditoría iniciar una unidad **systemd power_unit_file_t**. En consecuencia, **auditd** no puede detener o apagar el sistema incluso cuando está configurado para hacerlo en casos como la falta de espacio en una partición de disco de registro.

Para solucionar este problema, cree un módulo de política SELinux personalizado. Como resultado, **auditd** puede detener o apagar el sistema correctamente sólo si aplica la solución.

(BZ#1826788)

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)

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)

Errores de parámetros no conocidos en la salida de rsyslog con config.enabled

En la salida de **rsyslog**, se produce un error inesperado en los errores de procesamiento de la configuración utilizando la directiva **config**.enabled. Como consecuencia, se muestran errores de **parámetros no** conocidos mientras se utiliza la directiva config **.** enabled excepto en las sentencias **include()**.

Para solucionar este problema, establezca **config.enabled=on** o utilice las sentencias **include()**.

(BZ#1659383)

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)

Las conexiones a servidores con firmas SHA-1 no funcionan con GnuTLS

Las firmas SHA-1 en los certificados son rechazadas por la biblioteca de comunicaciones seguras GnuTLS como inseguras. En consecuencia, las aplicaciones que utilizan GnuTLS como backend TLS no pueden establecer una conexión TLS con pares que ofrezcan tales certificados. Este comportamiento

es inconsistente con otras bibliotecas criptográficas del sistema. Para solucionar este problema, actualice el servidor para utilizar certificados firmados con SHA-256 o un hash más fuerte, o cambie a la política LEGACY.

(BZ#1628553)

TLS 1.3 no funciona en NSS en modo FIPS

TLS 1.3 no es compatible con los sistemas que funcionan en modo FIPS. Como resultado, las conexiones que requieren TLS 1.3 para la interoperabilidad no funcionan en un sistema que funciona en modo FIPS.

Para habilitar las conexiones, desactive el modo FIPS del sistema o habilite el soporte para TLS 1.2 en el peer.

(BZ#1724250)

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 genera una extensión **status_request** malformada en el mensaje **CertificateRequest** en TLS 1.3

Los servidores OpenSSL envían una extensión **status_request** malformada en el mensaje **CertificateRequest** si el soporte para la extensión **status_request** y la autenticación basada en el certificado del cliente están activados. En este caso, OpenSSL no interopera con las implementaciones que cumplen con el protocolo **RFC 8446**. Como resultado, los clientes que verifican correctamente las extensiones en el mensaje **CertificateRequest** abortan las conexiones con el servidor OpenSSL. Para solucionar este problema, desactive la compatibilidad con el protocolo TLS 1.3 en ambos lados de la conexión o desactive la compatibilidad con **status_request** en el servidor OpenSSL. Esto evitará que el servidor envíe mensajes malformados.

(BZ#1749068)

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)

Libreswan no funciona correctamente con seccomp=enabled en todas las configuraciones

El conjunto de llamadas al sistema permitidas en la implementación del soporte SECCOMP **de Libreswan** no está actualmente completo. En consecuencia, cuando SECCOMP está habilitado en el archivo **ipsec.conf**, el filtrado de llamadas al sistema rechaza incluso las llamadas al sistema necesarias para el correcto funcionamiento del demonio **pluto**; el demonio es eliminado, y el servicio **ipsec** es reiniciado.

Para solucionar este problema, vuelva a poner la opción **seccomp=** en estado **desactivado**. El soporte de SECCOMP debe permanecer deshabilitado para ejecutar **ipsec** correctamente.

(BZ#1777474)

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)

SCAP Workbench no genera correcciones basadas en resultados a partir de perfiles adaptados

El siguiente error se produce al intentar generar roles de corrección basados en resultados a partir de un perfil personalizado utilizando la herramienta **SCAP Workbench**:

> Error al generar el rol de remediación .../remediación.sh: El código de salida de oscap era 1: [salida truncada]

Para solucionar este problema, utilice el comando **oscap** con la opción **--tailoring-file**.

(BZ#1640715)

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)

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)

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)

La utilidad oscap-ssh falla 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**. Si la configuración de **umask** en la máquina remota ha sido cambiada, **oscap-ssh** podría no tener acceso a estos archivos. Para solucionar este problema, modifique la herramienta **oscap-ssh** como se describe en esta solución "oscap-ssh --sudo" no recupera los archivos de resultados con el error "scp: ...: Permiso denegado". Como resultado, **oscap** guarda los archivos como el usuario de destino, y **oscap-ssh** accede a los archivos normalmente.

(BZ#1803116)

OpenSCAP produce falsos positivos causados por la eliminación de las líneas en blanco de las cadenas multilínea YAML

Cuando OpenSCAP genera remedios de Ansible a partir de un flujo de datos, elimina las líneas en blanco de las cadenas multilíneas de YAML. Dado que algunas reparaciones de Ansible contienen contenido literal de archivos de configuración, la eliminación de líneas en blanco afecta a las reparaciones correspondientes. Esto hace que la utilidad **openscap** falle las comprobaciones correspondientes de Open Vulnerability and Assessment Language (OVAL), aunque las líneas en blanco no tengan ningún efecto. Para solucionar este problema, compruebe las descripciones de las reglas y omita los resultados del análisis que fallaron debido a la falta de líneas en blanco. Como alternativa, utilice remedios de Bash en lugar de remedios de Ansible, porque los remedios de Bash no producen estos resultados falsos positivos.

(BZ#1795563)

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, si se selecciona el grupo de paquetes *Server with GUI* durante la instalación de un sistema con perfiles OSPP o basados en OSPP, por ejemplo, la Guía de Implementación Técnica de Seguridad (STIG), se aborta la instalación. 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)

El sistema RHEL8 con el grupo de paquetes *Server with GUI* no puede ser remediado usando el perfil e8

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* requiere una cantidad extrema de RAM en el sistema. Este problema es causado por el escáner de OpenSCAP; para más detalles vea El escaneo de un gran número de archivos con OpenSCAP hace que los sistemas se queden sin memoria. Como consecuencia, el endurecimiento del sistema utilizando el perfil RHEL8 Essential Eight (e8) no tiene éxito. Para solucionar este problema, elija un grupo de paquetes más pequeño, por ejemplo, Server, e instale los paquetes adicionales que necesite después de la instalación. Como resultado, el sistema tendrá un número menor de paquetes, el escaneo requerirá menos memoria y, por lo tanto, el sistema puede ser endurecido automáticamente.

(BZ#1816199)

El escaneo de un gran número de archivos con OpenSCAP hace que los sistemas se queden sin memoria

El escáner OpenSCAP almacena todos los resultados recogidos en la memoria hasta que finaliza el escaneo. Como consecuencia, el sistema podría quedarse sin memoria en sistemas con poca RAM al escanear un gran número de archivos, por ejemplo de los grandes grupos de paquetes *Server with GUI* y *Workstation*. Para solucionar este problema, utilice grupos de paquetes más pequeños, por ejemplo, *Server* y *Minimal Install* en sistemas con poca memoria RAM. Si necesita utilizar grupos de paquetes grandes, puede probar si su sistema tiene suficiente memoria en un entorno virtual o de ensayo. Como alternativa, puede adaptar el perfil de exploración para deseleccionar las reglas que implican la recursión en todo el sistema de archivos /:

- **rpm_verify_hashes**
- **rpm_verify_permissions**
- **rpm_verify_ownership**
- **archivo_permisos_no_autorizados_mundo_de_escritura**
- **no_files_unowned_by_user**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_unroupowned**
- **dir_perms_world_writable_sticky_bits**

Esto evitará que el escaneo de OpenSCAP haga que el sistema se quede sin memoria.

(BZ#1824152)

11.5. RED

El tráfico de red IPsec falla durante la descarga de IPsec cuando GRO está desactivado

No se espera que la descarga de IPsec funcione cuando la descarga de recepción genérica (GRO) está desactivada en el dispositivo. Si la descarga de IPsec está configurada en una interfaz de red y GRO está desactivado en ese dispositivo, el tráfico de red IPsec falla.

Para solucionar este problema, mantenga activado el sistema GRO en el dispositivo.

(BZ#1649647)

iptables no solicita la carga de módulos para los comandos que actualizan una cadena si no se conoce el tipo de cadena especificado

Nota: Este problema provoca errores espurios sin implicación funcional al detener el servicio **iptables systemd** si se utiliza la configuración por defecto de los servicios.

Cuando se establece la política de una cadena con **iptables-nft**, el comando de actualización de la cadena resultante enviado al kernel fallará si el módulo del kernel asociado no está ya cargado. Para solucionar el problema, utilice los siguientes comandos para hacer que se carguen los módulos:

```
# iptables -t nat -n -L
# iptables -t mangle -n -L
```

(BZ#1812666)

La carga automática de los módulos back-end **LOG** específicos de la familia de direcciones por parte del módulo **nft_compat** puede colgar

Cuando el módulo **nft_compat** carga extremos posteriores de destino **LOG** específicos de la familia de direcciones mientras se realiza una operación en espacios de nombres de red**(netns**) en paralelo, puede producirse una colisión de bloqueos. Como consecuencia, la carga de los extremos posteriores de los objetivos **LOG** específicos de la familia de direcciones puede colgarse. Para solucionar el problema, cargue manualmente los extremos posteriores del objetivo **LOG** relevantes, como **nf_log_ipv4.ko** y **nf_log_ipv6.ko**, antes de ejecutar la utilidad **iptables-restore**. Como resultado, la carga de los extremos posteriores del objetivo **LOG** no se cuelga. Sin embargo, si el problema aparece durante el arranque del sistema, no hay ninguna solución disponible.

Tenga en cuenta que otros servicios, como **libvirtd**, también ejecutan comandos **de iptables**, lo que puede provocar el problema.

(BZ#1757933)

11.6. NÚCLEO

La eliminación accidental del parche hace que **huge_page_setup_helper.py** muestre un error

Un parche que actualiza el script **huge_page_setup_helper.** py, fue eliminado accidentalmente. En consecuencia, tras ejecutar el script **huge_page_setup_helper**.py, aparece el siguiente mensaje de error:

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

Para solucionar este problema, copie el script **huge_page_setup_helper.py** de RHEL 8.1 e instálelo en el directorio /**usr**/**bin**/:

1. Descargue el paquete **libhugetlbfs-utils-2.21-3.el8.x86_64.** rpm desde el medio de instalación de RHEL-8.1.0 o desde el Portal del Cliente de Red Hat.

2. Ejecute el comando **rpm2cpio**:

   ```
   # rpm2cpio libhugetlbfs-utils-2.21-3.el8.x86_64.rpm | cpio -D / -iduv
   '*/huge_page_setup_helper.py'
   ```

   El comando extrae el script **huge_page_setup_helper.py** del RPM de RHEL 8.1 y lo guarda en el directorio /**usr**/**bin**/.

Como resultado, el script **huge_page_setup_helper.py** funciona correctamente.

(BZ#1823398)

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)

KSM a veces ignora las políticas de memoria NUMA

Cuando la función de memoria compartida del kernel (KSM) está activada con el parámetro **merge_across_nodes=1**, KSM ignora las políticas de memoria establecidas por la función mbind(), y puede fusionar páginas de algunas áreas de memoria a nodos de acceso a memoria no uniforme (NUMA) que no coinciden con las políticas.

Para solucionar este problema, desactive KSM o establezca el parámetro **merge_across_nodes** a **0** si utiliza la unión de memoria NUMA con QEMU. Como resultado, las políticas de memoria NUMA configuradas para la VM KVM funcionarán como se espera.

(BZ#1153521)

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)

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 mecanismo de volcado fadump cambia el nombre de la interfaz de red a kdump-<interface-name>

Cuando se utiliza el volcado asistido por firmware (**fadump**) para capturar un **vmcore** y almacenarlo en una máquina remota utilizando el protocolo SSH o NFS, se renombra la interfaz de red a **kdump-<interface-name>**. El renombramiento ocurre cuando el **<interface-name>** es genérico, por ejemplo, *eth#, o net# y así sucesivamente. Este problema ocurre porque los scripts de captura de **vmcore** en el disco RAM inicial (**initrd**) añaden el prefijo kdump- al nombre de la interfaz de red para asegurar la persistencia del nombre. Como el mismo **initrd** se utiliza también para un arranque normal, el nombre de la interfaz se cambia también para el kernel de producción.

(BZ#1745507)

El sistema entra en el modo de emergencia en el momento del arranque cuando fadump está activado

El sistema entra en el modo de emergencia cuando se habilita el módulo de squash **fadump** (**kdump**) o **dracut** en el esquema **initramfs** porque el gestor **systemd** no consigue obtener la información de montaje y configurar la partición LV para montarla. Para solucionar este problema, añada el siguiente parámetro de línea de comandos del kernel **rd.lvm.lv=<VG>/<LV>** para descubrir y montar la partición LV fallida adecuadamente. Como resultado, el sistema arrancará con éxito en el escenario descrito.

(BZ#1750278)

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 uso de la memoria vPMEM como objetivo de volcado retrasa el proceso de captura de fallos del kernel

Cuando se utilizan espacios de nombres de memoria persistente virtual (vPEM) como objetivo de **kdump** o **fadump**, el módulo **papr_scm** se ve obligado a desmapear y remapear la memoria respaldada por vPMEM y a volver a añadir la memoria a su mapa lineal. En consecuencia, este comportamiento desencadena llamadas del hipervisor (HCalls) al hipervisor POWER, y el tiempo total empleado, ralentiza considerablemente el arranque del kernel de captura. Por lo tanto, se recomienda no utilizar espacios de nombres vPMEM como objetivo de volcado para kdump o fadump.

Si debe utilizar vPMEM, para solucionar este problema ejecute los siguientes comandos:

1. Cree el archivo **/etc/dracut.conf.d/99-pmem-workaround.conf** y añada:

```
add_drivers ="nd_pmem nd_btt libnvdimm papr_scm"
```

2. Reconstruir el sistema de archivos del disco RAM inicial (initrd):

```
# touch /etc/kdump.conf
# systemctl restart kdump.service
```

(BZ#1792125)

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 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)

El intento de añadir el puerto NIC del controlador ICE a una interfaz maestra de enlace en modo 5(balance-tlb) puede provocar un fallo

Al intentar añadir el puerto NIC del controlador **ICE** a una interfaz maestra de enlace en modo 5 (balance-tlb) puede producirse un fallo con un error **Maestro 'bond0', Esclavo 'ens1f0': Error:** Enslave **failed**. En consecuencia, se produce un fallo intermitente al añadir el puerto NIC a la interfaz maestra de enlace. Para solucionar este problema, intente volver a añadir la interfaz.

(BZ#1791664)

Adjuntar la función virtual a la máquina virtual con el tipo de interfaz='hostdev' puede fallar a veces

Adjuntar una Función Virtual (VF) a una máquina virtual utilizando un archivo .XML, siguiendo el método **Assignment with <interface type='hostdev'>**, puede fallar en ocasiones. Esto ocurre porque el uso del método **Assignment with <interface type='hostdev'>** impide que la VM se conecte a la NIC de la VF presentada a esta máquina virtual. Para solucionar este problema, adjunte el VF a la VM utilizando el archivo .XML con el método **Assignment with <hostdev>**. Como resultado, el comando **virsh attach-device** tiene éxito sin error. Para obtener más detalles sobre la diferencia entre **Assignment with <hostdev>** y **Assignment with <interface type='hostdev'>** (sólo dispositivos SRIOV), consulte PCI Passthrough de dispositivos de red de host.

(BZ#1792691)

11.7. 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)

DM Multipath podría no iniciarse cuando se conectan demasiados LUNs

El servicio **multipathd** puede agotarse y no iniciarse si hay demasiadas unidades lógicas (LUNs) conectadas al sistema. El número exacto de LUNs que causa el problema depende de varios factores, incluyendo el número de dispositivos, el tiempo de respuesta de la matriz de almacenamiento, la configuración de la memoria y la CPU, y la carga del sistema.

Para solucionar el problema, aumente el valor del tiempo de espera en el archivo de la unidad **multipathd**:

1. Abra la unidad **multipathd** en el editor de unidades:

```
# systemctl edit multipathd
```

2. Introduzca la siguiente configuración para anular el valor del tiempo de espera:

```
[Service]
TimeoutSec=300
```

Red Hat recomienda aumentar el valor a 300 desde el valor predeterminado de 90, pero también puede probar otros valores por encima de 90.

3. Guarde el archivo en el editor.

4. Recarga las unidades **systemd** para aplicar el cambio:

```
# systemctl daemon-reload
```

Como resultado, **multipathd** puede ahora arrancar con éxito con un mayor número de LUNs.

(BZ#1797660)

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 tomar una instantánea de un volumen lógico mientras el volumen lógico esté utilizando **la caché de escritura**.
- No se puede adjuntar o quitar **la caché de escritura** mientras un volumen lógico está activo.
- Cuando se adjunta **la caché de escritura** a un volumen lógico inactivo, se debe utilizar un tamaño de bloque **de caché de escritura** que coincida con el tamaño de bloque del sistema de archivos existente.
  Para más detalles, consulte la página man de **lvmcache(7)**.
- No se puede redimensionar un volumen lógico mientras **la caché de escritura** está conectada a él.
- No se pueden utilizar los comandos **pvmove** en dispositivos que se utilizan con **writecache**.
- No se pueden utilizar volúmenes lógicos con **writecache** en combinación con thin pools o VDO.

(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)

11.8. 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)

nginx no puede cargar los certificados del servidor desde los tokens de seguridad del hardware

El servidor web **nginx** soporta la carga de claves privadas TLS desde tokens de seguridad de hardware directamente desde los módulos PKCS#11. Sin embargo, actualmente es imposible cargar certificados de servidor desde tokens de seguridad de hardware a través del URI PKCS#11. Para solucionar este problema, almacene los certificados del servidor en el sistema de archivos

(BZ#1668717)

php-fpm causa denegaciones de SELinux AVC cuando php-opcache es instalado con PHP 7.2

Cuando se instala el paquete **php-opcache**, el gestor de procesos FastCGI **(php-fpm**) provoca denegaciones de SELinux AVC. Para solucionar este problema, cambie la configuración por defecto en el archivo **/etc/php.d/10-opcache.ini** por la siguiente:

```
opcache.huge_code_pages=0
```

Tenga en cuenta que este problema sólo afecta al flujo **php:7.2**, no al **php:7.3**.

(BZ#1670386)

Falta el nombre del paquete mod_wsgi cuando se instala como dependencia

Con un cambio en la instalación de **mod_wsgi**, descrito en BZ#1779705, el paquete **python3-mod_wsgi** ya no proporciona el nombre **mod_wsgi**. Al instalar el módulo **mod_wsgi**, debe especificar el nombre completo del paquete. Este cambio causa problemas con las dependencias de paquetes de terceros.

Si intenta instalar un paquete de terceros que requiere una dependencia llamada **mod_wsgi**, se devuelve un error similar al siguiente:

```
Error:
 Problem: conflicting requests
  - nothing provides mod_wsgi needed by package-requires-mod_wsgi.el8.noarch
```

Para solucionar este problema, elige una de las siguientes opciones:

a. Reconstruya el paquete (o pida al proveedor de terceros una nueva construcción) para requerir el nombre completo del paquete **python3-mod_wsgi**.

b. Crear un meta paquete con el nombre del paquete que falta:

   1. Construye tu propio meta paquete vacío que proporciona el nombre **mod_wsgi**.

   2. Añada la línea **module_hotfixes=True** al archivo de configuración **.repo** del repositorio que incluye el meta paquete.

   3. Instalar manualmente **python3-mod_wsgi**.

(BZ#1829692)

11.9. COMPILADORES Y HERRAMIENTAS DE DESARROLLO

Las funciones sintéticas generadas por GCC confunden a SystemTap

La optimización de GCC puede generar funciones sintéticas para copias parcialmente inline de otras funciones. Herramientas como SystemTap y GDB no pueden distinguir estas funciones sintéticas de las reales. Como consecuencia, SystemTap coloca sondas tanto en los puntos de entrada de las funciones sintéticas como en los reales y, por lo tanto, registra múltiples impactos de sonda para una sola llamada a una función real.

Para solucionar este problema, modifique los scripts de SystemTap para detectar la recursividad y evitar la colocación de sondas relacionadas con funciones parciales inline.

Este script de ejemplo

```
sonda kernel.function(\ "can_nice").call { }
```

se puede modificar de esta manera:

```
global in_can_nice%

probe kernel.function("can_nice").call {
  in_can_nice[tid()] ++;
  if (in_can_nice[tid()] > 1) { next }
  /* code for real probe handler */
}

probe kernel.function("can_nice").return {
  in_can_nice[tid()] --;
}
```

Tenga en cuenta que este script de ejemplo no considera todos los escenarios posibles, tales como kprobes o kretprobes perdidos, o la recursión genuina prevista.

(BZ#1169184)

11.10. GESTIÓN DE LA IDENTIDAD

Cambiar /etc/nsswitch.conf requiere un reinicio manual del sistema

Cualquier cambio en el archivo **/etc/nsswitch .** conf, por ejemplo la ejecución del comando **authselect select profile_id**, requiere un reinicio del sistema para que todos los procesos relevantes utilicen la versión actualizada del archivo **/etc/nsswitch.conf**. Si no es posible reiniciar el sistema, reinicie el servicio que une su sistema a Active Directory, que es el **demonio de servicios de seguridad del sistema** (SSSD) o **winbind**.

(BZ#1657295)

SSSD devuelve la pertenencia a un grupo LDAP incorrecto para los usuarios locales cuando el dominio de archivos está habilitado

Si el demonio de servicios de seguridad del sistema (SSSD) sirve a los usuarios desde los archivos locales y el atributo **ldap_rfc2307_fallback_to_local_users** de la sección [domain/LDAP] del archivo **sssd.** conf se establece como True, el proveedor de archivos no incluye la pertenencia a grupos de otros dominios. Como consecuencia, si un usuario local es miembro de un grupo LDAP, el comando **id local_user** no devuelve la pertenencia al grupo LDAP del usuario. Para solucionar este problema, desactive el dominio de **archivos** implícito añadiendo

```
enable_files_domain=False
```

a la sección **[sssd]** en el archivo **/etc/sssd/sssd.conf**.

Como resultado, **id local_user** devuelve la pertenencia correcta al grupo LDAP para los usuarios locales.

(BZ#1652562)

SSSD no maneja correctamente varias reglas de coincidencia de certificados con la misma prioridad

Si un certificado determinado coincide con varias reglas de coincidencia de certificados con la misma prioridad, el demonio de servicios de seguridad del sistema (SSSD) sólo utiliza una de las reglas. Como solución, utilice una única regla de coincidencia de certificados cuyo filtro LDAP esté formado por los filtros de las reglas individuales concatenados con el operador | (o). Para ver ejemplos de reglas de coincidencia de certificados, consulte la página de manual de sss-certamp(5).

(BZ#1447945)

Los grupos privados no se crean con auto_private_group = hybrid cuando se definen varios dominios

Los grupos privados no se crean con la opción auto_private_group = hybrid cuando se definen varios dominios y la opción hybrid se utiliza en cualquier dominio que no sea el primero. Si se define un dominio de archivos implícito junto con un dominio AD o LDAP en el archivo **sssd.conf** y no se marca como **MPG_HYBRID**, entonces SSSD falla al crear un grupo privado para un usuario que tiene uid=gid y el grupo con este gid no existe en AD o LDAP.

El respondedor sssd_nss comprueba el valor de la opción **auto_private_groups** sólo en el primer dominio. Como consecuencia, en las configuraciones en las que hay varios dominios configurados, lo que incluye la configuración por defecto en RHEL 8, la opción **auto_private_group** no tiene ningún efecto.

Para solucionar este problema, establezca **enable_files_domain = false** en la sección sssd de

sssd.conf. Como resultado, si la opción **enable_files_domain** se establece en false, entonces sssd no añade un dominio con **id_provider=files** al principio de la lista de dominios activos, y por lo tanto no se produce este error.

(BZ#1754871)

python-ply no es compatible con FIPS

El módulo YACC del paquete **python-ply** utiliza el algoritmo hash MD5 para generar la huella digital de una firma YACC. Sin embargo, el modo FIPS bloquea el uso de MD5, que sólo está permitido en contextos no relacionados con la seguridad. Como consecuencia, python-ply no es compatible con FIPS. En un sistema en modo FIPS, todas las llamadas a **ply.yacc.yacc()** fallan con el mensaje de error:

```
UnboundLocalError: variable local 'sig' referenciada antes de la asignación
```

El problema afecta a **python-pycparser** y a algunos casos de uso de **python-cffi**. Para solucionar este problema, modifique la línea 2966 del archivo **/usr/lib/python3.6/site-packages/ply/yacc.py**, sustituyendo **sig = md5()** por **sig = md5(usedforsecurity=False)**. Como resultado, **python-ply** puede utilizarse en modo FIPS.

(BZ#1747490)

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)

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)

Directory Server advierte sobre los atributos que faltan en el esquema si esos atributos se utilizan en un filtro de búsqueda

Si establece el parámetro **nsslapd-verify-filter-schema** como **warn-invalid**, Directory Server procesa las operaciones de búsqueda con atributos que no están definidos en el esquema y registra una advertencia. Con esta configuración, Directory Server devuelve los atributos solicitados en los resultados de la búsqueda, independientemente de si los atributos están definidos en el esquema o no.

Una futura versión de Directory Server cambiará la configuración por defecto de **nsslapd-verify-filter-schema** para aplicar comprobaciones más estrictas. El nuevo valor predeterminado advertirá sobre los atributos que faltan en el esquema, y rechazará las solicitudes o devolverá sólo resultados parciales.

(BZ#1790259)

ipa-healthcheck-0.4 no obvia las versiones anteriores de ipa-healthcheck

La herramienta **Healthcheck** se ha dividido en dos subpaquetes: **ipa-healthcheck** e **ipa-healthcheck-core**. Sin embargo, sólo el subpaquete **ipa-healthcheck-core** está correctamente configurado para obviar las versiones anteriores de **ipa-healthcheck**. Como resultado, al actualizar **Healthcheck** sólo se instala **ipa-healthcheck-core** y el comando **ipa-healthcheck** no funciona después de la actualización.

Para solucionar este problema, instale el subpaquete **ipa-healthcheck-0.** 4 manualmente utilizando **yum install ipa-healthcheck-0.4**.

(BZ#1852244)

11.11. ESCRITORIO

Limitaciones de la sesión Wayland

Con Red Hat Enterprise Linux 8, el entorno GNOME y el Gestor de pantalla de GNOME (GDM) utilizan **Wayland** como tipo de sesión por defecto en lugar de la sesión **X11**, que se utilizaba con la versión principal anterior de RHEL.

Las siguientes funciones no están disponibles actualmente o no funcionan como se esperaba en **Wayland**:

- las utilidades de configuración de**X11**, como **xrandr**, no funcionan bajo **Wayland** debido a su diferente enfoque en el manejo, resoluciones, rotaciones y diseño. Puede configurar las características de la pantalla utilizando los ajustes de GNOME.
- La grabación de pantalla y el escritorio remoto requieren que las aplicaciones sean compatibles con la API del portal en **Wayland**. Algunas aplicaciones heredadas no son compatibles con la API del portal.
- La accesibilidad del puntero no está disponible en **Wayland**.
- No hay gestor de portapapeles disponible.
- GNOME Shell en **Wayland** ignora las capturas de teclado emitidas por la mayoría de las aplicaciones heredadas de **X11**. Puede habilitar una aplicación de **X11** para que emita pulsaciones de teclado utilizando la tecla GSettings de **/org/gnome/mutter/wayland/xwayland-grab-access-rules**. Por defecto, GNOME Shell en **Wayland** permite que las siguientes aplicaciones emitan pulsaciones de teclado:
  - **GNOME Boxes**
  - **Vinagre**
  - **Xephyr**
  - **virt-manager**, **virt-viewer** y **remote-viewer**
  - **vncviewer**
- **Wayland** dentro de máquinas virtuales (VM) invitadas tiene problemas de estabilidad y rendimiento. RHEL vuelve automáticamente a la sesión **X11** cuando se ejecuta en una VM.

Si actualiza a RHEL 8 desde un sistema RHEL 7 en el que utilizaba la sesión de GNOME **X11**, su sistema sigue utilizando **X11**. El sistema también vuelve automáticamente a **X11** cuando los siguientes controladores gráficos están en uso:

- El controlador propietario de NVIDIA

- El conductor de **Cirrus**
- El conductor **mga**
- El conductor de **aspeed**

Puede desactivar el uso de **Wayland** manualmente:

- Para desactivar **Wayland** en GDM, establece la opción **WaylandEnable=false** en el archivo **/etc/gdm/custom.conf**.
- Para desactivar **Wayland** en la sesión de GNOME, seleccione la opción de legado **X11** utilizando el menú de rueda dentada en la pantalla de inicio de sesión después de introducir su nombre de usuario.

Para más detalles sobre **Wayland**, consulte https://wayland.freedesktop.org/.

(BZ#1797409)

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)

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)

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)

La caída del sistema puede provocar la pérdida de la configuración de fadump

Este problema se observa en sistemas en los que el volcado asistido por el firmware (fadump) está habilitado y la partición de arranque se encuentra en un sistema de archivos con registro en el diario, como XFS. Un fallo del sistema puede hacer que el cargador de arranque cargue un **initrd** más antiguo que no tenga habilitado el soporte de captura de volcado. En consecuencia, después de la recuperación, el sistema no captura el archivo **vmcore**, lo que resulta en la pérdida de la configuración de fadump.

Para solucionar este problema:

- Si **/boot** es una partición separada, realice lo siguiente:

  1. Reinicie el servicio kdump

  2. Ejecute los siguientes comandos como usuario root, o utilizando una cuenta de usuario con derechos CAP_SYS_ADMIN:

     ```
     # fsfreeze -f
     # fsfreeze -u
     ```

- Si **/boot** no es una partición separada, reinicie el sistema.

(BZ#1723501)

11.12. INFRAESTRUCTURAS GRÁFICAS

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)

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, ponga en la lista negra **a 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 que no se enciendan todas las pantallas a pesar de haberlo hecho en versiones anteriores de RHEL. Esto se debe a que el sistema piensa erróneamente que no hay suficiente ancho de banda en el hub para soportar todas las pantallas.

(BZ#1812577)

11.13. 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)

11.14. VIRTUALIZACIÓN

Bajo rendimiento de visualización de la GUI en máquinas virtuales RHEL 8 en un host Windows Server 2019

Cuando se utiliza RHEL 8 como sistema operativo invitado en modo gráfico en un host de Windows Server 2019, el rendimiento de visualización de la interfaz gráfica de usuario es bajo, y la conexión a una salida de consola del invitado actualmente tarda bastante más de lo esperado.

Este es un problema conocido en los hosts de Windows 2019 y está pendiente de una solución por parte de Microsoft. Para solucionar este problema, conéctese al invitado mediante SSH o utilice Windows Server 2016 como anfitrión.

(BZ#1706541)

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 RHEL 8 a veces no pueden arrancar en los hosts Witherspoon

Las máquinas virtuales (VMs) de RHEL 8 que utilizan el tipo de máquina **pseries-rhel7.6.0-sxxm** en algunos casos fallan al arrancar en 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 como sigue:

```
<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, BZ#1751054)

Las máquinas virtuales IBM POWER no funcionan correctamente con nodos NUMA vacíos

Actualmente, cuando una máquina virtual (VM) IBM POWER que se ejecuta en un host RHEL 8 está configurada con un nodo NUMA que utiliza cero memoria**(memory='0'**) y cero CPUs, la VM no puede arrancar. Por lo tanto, Red Hat recomienda encarecidamente no utilizar VMs IBM POWER con tales nodos NUMA vacíos en RHEL 8.

(BZ#1651474)

La topología de la CPU SMT no es detectada por las máquinas virtuales cuando se utiliza el modo de paso de host en AMD EPYC

Cuando una máquina virtual (VM) arranca con el modo de paso de host de CPU en un host AMD EPYC, la bandera de la función **TOPOEXT** CPU no está presente. En consecuencia, la VM no puede detectar una topología de CPU virtual con múltiples hilos por núcleo. Para solucionar este problema, inicie la máquina virtual con el modelo de CPU EPYC en lugar de con el modo de paso de host.

(BZ#1740002)

Los identificadores de disco en las máquinas virtuales RHEL 8.2 pueden cambiar al reiniciar la máquina.

Cuando se utiliza una máquina virtual (VM) con RHEL 8.2 como sistema operativo invitado en un hipervisor Hyper-V, los identificadores de dispositivo para los discos virtuales de la VM en algunos casos cambian cuando la VM se reinicia. Por ejemplo, un disco originalmente identificado como **/dev/sda** puede convertirse en **/dev/sdb**. Como consecuencia, la VM podría no arrancar, y los scripts que hacen referencia a los discos de la VM podrían dejar de funcionar.

Para evitar este problema, Red Hat recomienda encarecidamente establecer nombres persistentes para los discos en la VM. Para obtener información detallada, consulte la documentación de Microsoft Azure: https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-device-names-problems.

(BZ#1777283)

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)

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)

11.15. 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)

11.16. 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)

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.

(BZ#1804193)

CAPÍTULO 12. INTERNACIONALIZACIÓN

12.1. 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, libhangu

12.2. 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 .
- Las actualizaciones de los paquetes **glibc** para varias localizaciones están ahora sincronizadas con el repositorio de datos de localización común (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#1715406, BZ#1748016, BZ#1790259, BZ#1748994, BZ#1739718
NetworkManager	BZ#1626348
anaconda	BZ#1747382, BZ#1637472, BZ#1748756, BZ#1649359, BZ#1715303, BZ#1696609, BZ#1672405, BZ#1687747, BZ#1745064, BZ#1659400, BZ#1821192, BZ#1822880, BZ#1823578, BZ#1748281, BZ#1746391
auditoría	BZ#1757986
authselect	BZ#1657295
bind	BZ#1564443, BZ#1664863, BZ#1704328
binutils	BZ#1777002, BZ#1618748
buildah-container	BZ#1627898
horquilla	BZ#1766526, BZ#1564559, BZ#1436780, BZ#1784524
cloud-init	BZ#1641190, BZ#1666961
cockpit-appstream	BZ#1676506
cabina de mando	BZ#1678465, BZ#1754163, BZ#1666722
módulo container-tools-rhel8	BZ#1784267
corosync-qdevice	BZ#1784200
createrepo_c	BZ#1743186
cripto-políticas	BZ#1690565, BZ#1660839
device-mapper-multipath	BZ#1797660
dhcp	BZ#1729211

Componente	Entradas
distribución	BZ#1657927
dnf	BZ#1676891, BZ#1754609
dnsmasq	BZ#1700916
edk2	BZ#1748180
elfutils	BZ#1744992
fapolicyd	BZ#1759895
agentes de vallas	BZ#1775847
firewalld	BZ#1737045, BZ#1740670, BZ#1733066
freeradius	BZ#1723362
gcc-toolset-9	BZ#1774118
gcc	BZ#1726641, BZ#1698607, BZ#1747157
gdb	BZ#1768593
gdm	BZ#1749960
glibc	BZ#1410154, BZ#1764214, BZ#1749439, BZ#1764235, BZ#1746928, BZ#1777241, BZ#1361965, BZ#1747502, BZ#1764218, BZ#1764238, BZ#1746933, BZ#1747453
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1628553, BZ#1677754
go-toolset	BZ#1747150
grafana-pcp	BZ#1685315
grafana	BZ#1725278

Componente	Entradas
graphviz	BZ#1704875
grub2	BZ#1583445, BZ#1723501
módulo httpd-2.4	BZ#1747923
httpd	BZ#1633224
configuración inicial	BZ#1676439
ipa	BZ#1665051, BZ#1816784, BZ#1719767, BZ#1777564, BZ#1664719, BZ#1664718
ipcalc	BZ#1638834
java-11-openjdk	BZ#1746875
kernel-rt	BZ#1680161
núcleo	BZ#1744397, BZ#1698297, BZ#1687094, BZ#1720227, BZ#1846345, BZ#1635295, BZ#1793389, BZ#1706541, BZ#1666538, BZ#1602962, BZ#1649647, BZ#1153521, BZ#1694705, BZ#1348508, BZ#1748451, BZ#1708456, BZ#1654962, BZ#1609288, BZ#1777283, BZ#1791664, BZ#1792125, BZ#1792691, BZ#1812666, BZ#1812577, BZ#1757933, BZ#1763661, BZ#1780432, BZ#1401552, BZ#1716002, BZ#1593711, BZ#1620349, BZ#1724969, BZ#1714330, BZ#1714486, BZ#1660368, BZ#1524687, BZ#1274406, BZ#1650518, BZ#1636572, BZ#1727369, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1570255, BZ#1696451, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610, BZ#1730502
kexec-tools	BZ#1750278, BZ#1690729
kmod-kvdo	BZ#1737639, BZ#1657301
krb5	BZ#1754690
libbpf	BZ#1759154
libdnf	BZ#1697472

Componente	Entradas
libgnome-keyring	BZ#1607766
libndp	BZ#1697595
libpfm	BZ#1731019
libreswan	BZ#1777474
módulo libselinux-python-2.8	BZ#1666328
libvirt	BZ#1749672, BZ#1664592, BZ#1528684
llvm-toolset	BZ#1747139
lorax	BZ#1754711
ltrace	BZ#1655368
lvm2	BZ#1600174, BZ#1496229, BZ#1768536
hacer	BZ#1774790
maven	BZ#1783926
mod_wsgi	BZ#1829692, BZ#1779705
murmurar	BZ#1737553
nfs-utils	BZ#1719983, BZ#1592011
nftables	BZ#1778883, BZ#1643192
nginx	BZ#1668717
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1724250, BZ#1817533, BZ#1645153
numactl	BZ#1730738
opencv	BZ#1694647

Componente	Entradas
openscap	BZ#1636431, BZ#1618489, BZ#1646197, BZ#1803116, BZ#1795563, BZ#1824152, BZ#1642373
openssh	BZ#1744108
openssl-pkcs11	BZ#1705505, BZ#1664807, BZ#1745082
openssl	BZ#1685470, BZ#1749068
oscap-anaconda-addon	BZ#1665082, BZ#1674001, BZ#1691305, BZ#1787156, BZ#1816199
marcapasos	BZ#1712584, BZ#1700104
pam	BZ#1252859, BZ#1537242
pcp	BZ#1723598
pcs	BZ#1631519, BZ#1631514, BZ#1676431, BZ#1442116, BZ#1619620
perl-LDAP	BZ#1663063
módulo php-7.2	BZ#1670386
php-pecl-xdebug	BZ#1769857
pki-core	BZ#1698084, BZ#1303254
podman	BZ#1804193, BZ#1645280
policycoreutils	BZ#1563742, BZ#1417455
postfix	BZ#1723950, BZ#1745321
powertop	BZ#1716721
pykickstart	BZ#1637872
pitón-ply	BZ#1747490
módulo python38-3.8	BZ#1747329

Componente	Entradas
qemu-kvm	BZ#1651474, BZ#1740002, BZ#1719687, BZ#1651994, BZ#1741346
trasera	BZ#1729501
redhat-release	BZ#1817591
redhat-support-tool	BZ#1802026
rhel-system-roles-sap	BZ#1660832
rng-tools	BZ#1692435
rpm	BZ#1688849
rsyslog	JIRA:RHELPLAN-10431, BZ#1659383, BZ#1679512, BZ#1740683, BZ#1676559, BZ#1692073, BZ#1692072
herrumbre-herramienta	BZ#1776847
s390utils	BZ#1750326
samba	BZ#1754409, JIRA:RHELPLAN-13195
scap-guía de seguridad	BZ#1755447, BZ#1754919, BZ#1750755, BZ#1755194
scap-workbench	BZ#1640715
selinux-policy	BZ#1641631, BZ#1746398, BZ#1826788, BZ#1727887, BZ#1726166, BZ#1726246
setools	BZ#1731519
setroubleshoot-plugins	BZ#1649842
configuración	BZ#1730396, BZ#1663556
skopeo-contenedor	BZ#1627900
skopeo	BZ#1810053
sscg	BZ#1717880

Componente	Entradas
sssd	BZ#1669407, BZ#1652562, BZ#1447945, BZ#1754871
gestor de suscripciones	BZ#1674337
sudo	BZ#1786990, BZ#1733961
systemd	BZ#1686892, BZ#1640802
systemtap	BZ#1744989
tpm2-tools	BZ#1725714
afinado	BZ#1738250
udica	BZ#1763210, BZ#1732704
vdo	BZ#1713749
virt-manager	BZ#1677019
wayland	BZ#1673073
whois	BZ#1734183
xorg-x11-drv-qxl	BZ#1642887
servidor xorg-x11	BZ#1698565
zlib	BZ#1659433, BZ#1666798
otros	BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1797409, BZ#1790635, BZ#1823398, BZ#1745507, BZ#1732726, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, BZ#1797671, BZ#1780124, JIRA:RHELPLAN-2507, JIRA:RHELPLAN-37713, JIRA:RHELPLAN-37777, BZ#1841170, JIRA:RHELPLAN-13995, BZ#1785248, BZ#1755347, BZ#1784455, BZ#1784456, BZ#1789401, JIRA:RHELPLAN-41384, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, BZ#1748980, BZ#1827628

APÉNDICE B. HISTORIAL DE REVISIONES

0.1-8

Mie Feb 10 2021, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido un problema conocido (Virtualización).

0.1-7

Thu Jan 28 2021, Lucie Maňásková(lmanasko@redhat.com)

- Se ha actualizado el capítulo de avances tecnológicos.

0.1-6

Thu Dec 10 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha añadido información sobre el manejo de GPOs de AD en SSSD a Nuevas características (Gestión de identidades).

0.1-5

Tue Dec 01 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una corrección de errores para el problema con fapolicyd (Seguridad).
- Se ha añadido un problema conocido (instalador).

0.1-4

Mar Nov 24 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha actualizado la sección de novedades (Redes).

0.1-3

Fri Oct 30 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha actualizado la descripción de Application Streams en la sección de Repositorios.

0.1-2

Lun Oct 05 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una corrección de errores (red).

0.1-1

Tue Sep 29 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha actualizado la ruta de actualización in situ con el lanzamiento de RHEL 7.9.

0.1-0

Thu Aug 27 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una corrección de errores (Kernel).

0.0-9

Lun Ago 10 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido un problema conocido (gestión de identidades).

0.0-8

Tue Jul 21 2020, Lucie Maňásková(lmanasko@redhat.com)

- Publicación de las notas de la versión de Red Hat Enterprise Linux 8.2.1.

0.0-7

Thu Jul 16 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha añadido una vista previa de la tecnología (red).
- Se ha actualizado la sección de novedades.

0.0-6

Thu Jun 25 2020, Jaroslav Klech(jklech@redhat.com)

- Granulado del capítulo de parámetros del núcleo.
- Se han añadido varias mejoras en el capítulo de controladores de dispositivos.

0.0-5

Fri Jun 19 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se han añadido nuevos problemas conocidos.
- Varias actualizaciones de otras notas de la versión.

0.0-4

Thu Jun 04 2020, Lucie Maňásková(lmanasko@redhat.com)

- Se ha actualizado la sección de novedades.
- Se ha añadido un problema conocido (Contenedores).

0.0-3

Wed May 20 2020, Lenka Špačková(lspackova@redhat.com)

- Se ha añadido un problema conocido (lenguajes de programación dinámicos, servidores web y de bases de datos).
- Se ha añadido una corrección de errores (compiladores y herramientas de desarrollo).
- Varias actualizaciones de otras notas de la versión.

0.0-2

Tue Apr 28 2020, Lucie Maňásková(lmanasko@redhat.com)

- Publicación de las notas de la versión de Red Hat Enterprise Linux 8.2.

0.0-1

Lun Mar 09 2020, Jaroslav Klech(jklech@redhat.com)

- Proporcionó cambios importantes en los capítulos de Parámetros del Núcleo Externo y Nuevos Controladores.

0.0-0

Tue Jan 21 2020, Lucie Maňásková(lmanasko@redhat.com)

- Publicación de las notas de la versión beta de Red Hat Enterprise Linux 8.2.