



Red Hat Enterprise Linux 7 Notas de lanzamiento 7.1

Notas de lanzamiento para Red Hat Enterprise Linux 7.17

Red Hat Servicios de contenidos del
cliente

Red Hat Enterprise Linux 7 Notas de lanzamiento 7.1

Notas de lanzamiento para Red Hat Enterprise Linux 7.17

Red Hat Servicios de contenidos del cliente

Legal Notice

Copyright © 2015 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Resumen

Las Notas de lanzamiento documentan funcionalidades y mejoras implementadas en el lanzamiento de Red Hat Enterprise Linux 7.1 y los problemas conocidos en este lanzamiento 7.1. Para obtener más información sobre los cambios entre Red Hat Enterprise Linux6 y 7, consulte la Guía de planificación de migración Reconocimientos Red Hat Global Support Services desea expresar su reconocimiento a Sterling Alexander y Michael Everette por su excepcional contribución en la prueba de Red Hat Enterprise Linux 7.

Table of Contents

Prefacio	4
Parte I. Nuevas funcionalidades	5
Capítulo 1. Arquitecturas	6
1.1. Red Hat Enterprise Linux for POWER, Little Endian	6
Capítulo 2. Hardware Enablement	7
2.1. Intel Broadwell Processor and Graphics Support	7
2.2. Support for TCO Watchdog and I2C (SMBUS) on Intel Communications Chipset 89xx Series	7
2.3. Intel Processor Microcode Update	7
Capítulo 3. Instalación y arranque	8
3.1. Instalador	8
3.2. Gestor de arranque	12
Capítulo 4. Almacenamiento	13
Cache LVM	13
Administración de matriz de almacenamiento con API de libStorageMgmt	13
Soporte para LSI Syncro	13
Interfaz de programación de aplicaciones LVM	14
Soporte para DIF/DIX	14
Mejoramiento de verificación de errores de sintaxis multirrutas del mapeador de dispositivos multirrutas y salida	14
Capítulo 5. Sistemas de archivos	15
Soporte para sistema de archivos Btrfs	15
OverlayFS	15
Soporte de NFS paralelo	15
Capítulo 6. Kernel	16
Soporte para dispositivos de bloque Ceph	16
Actualizaciones de Flash MCL simultáneas	16
Parche de kernel dinámico	16
Crashkernel con más de una CPU	16
Destino dm-era	16
Controlador de kernel Cisco VIC	16
Administración de entropía mejorada en hwrng	16
Mejoras de rendimiento del programador de balance de carga	17
Balance newidle mejorado en programador	17
HugeTLB Soporta asignación de Per-Node 1GB Huge Page	17
Nuevo mecanismo de bloqueo basado en MCS	17
El tamaño de pila del proceso aumentó de 8KB a 16KB	17
Las funcionalidades unprobe y uretprobe habilitadas en perf y systemtap	17
Verificación de consistencia de datos de punta a punta	17
DRBG en sistemas de 32 bits	17
Soporte para grandes tamaños de crashkernel	17
Capítulo 7. Virtualización	19
Aumento en el número máximo de vCPU en KVM	19
Soporte para nuevas instrucciones para Intel Core 5a generación en QEMU, KVM y libvirt API	19
Soporte de USB 3.0 para huéspedes KVM	19
Compresión para el comando dump-guest-memory	19
Open Virtual Machine Firmware	19

Mejoras de rendimiento de red en Hyper-V	19
hypervcopyd en hyperv-daemons	19
Nuevas funcionalidades en libguestfs	19
Seguimiento de registro de vuelo	20
RDMA-based Migration of Live Guests	20
Capítulo 8. Agrupamiento	21
Tiempo de espera de Dynamic Token para Corosync	21
Mejoramiento de disyuntor Corosync	21
Mejoras para Red Hat High Availability	21
Capítulo 9. Compilador y herramientas	22
Soporte de corrección en caliente para Linux en binarios System z	22
Mejoramiento en la Interfaz de programación de rendimiento (PAPI)	22
OProfile	22
OpenJDK8	22
sosreport reemplaza a Snap	22
Soporte GDB para Little-Endian 64-bit PowerPC	23
Mejora de Tuna	23
Capítulo 10. Red	24
Conexión de red confiable	24
Funcionalidad SR-IOV en el controlador qlcnic	24
Filtro de paquetes Berkeley	24
Estabilidad de reloj mejorada	24
Paquetes libnetfilter_queue	24
Mejoras en equipo	24
Controlador Intel QuickAssist Technology	24
Soporte LinuxPTP timemaster Support para conmutación entre PTP y NTP	25
initscripts de red	25
TCP Delayed ACK	25
NetworkManager	25
Espacios de nombres de red y VTI	25
Almacenamiento de configuración alternativo para MemberOf Plug-In	25
Capítulo 11. Linux Containers	26
11.1. Components of docker Formatted Containers	26
11.2. Advantages of Using Containers	27
11.3. Comparación con máquinas virtuales	28
11.4. Using Containers on Red Hat Enterprise Linux 7.1	28
11.5. Containers with the LXC Format Have Been Deprecated	28
Capítulo 12. Autenticación e interoperatividad	30
Manual Backup and Restore Functionality	30
Soporte para migración de WinSync a Trust	30
One-Time Password Authentication	30
Integración SSSD para Sistema de archivos comunes de Internet	30
Certificar herramienta de administración de autoridad	30
Aumentó granularidad de control de acceso	30
Acceso de dominio limitado para usuarios no privilegiados	30
Configuración de proveedor de datos automático	31
Uso de proveedores sudo de AD y LDAP	31
32-bit Version of krb5-server and krb5-server-ldap Deprecated	31
Capítulo 13. Seguridad	32

Guía de seguridad SCAP	32
Política SELinux	32
Nuevas funcionalidades en OpenSSH	32
Nuevas funcionalidades en Libreswan	32
Nuevas funcionalidades en TNC	33
Nuevas funcionalidades en GnuTLS	33
Capítulo 14. Escritorio	35
Soporte para visuales estéreo Quad-buffered OpenGL	35
Proveedores de cuenta en línea	35
Capítulo 15. Mantenimiento y Soporte	36
Micro reporte autorizado ABRT	36
Capítulo 16. Colecciones de software de Red Hat	37
Capítulo 17. Red Hat Enterprise Linux for Real Time	38
Parte II. Controladores de dispositivo	39
Capítulo 18. Actualizaciones de controlador de almacenamiento	40
Capítulo 19. Actualizaciones de controladores de red	41
Capítulo 20. Actualización de controladores gráficos	42
Parte III. Known Issues	43
Capítulo 21. Installation and Booting	44
Capítulo 22. Networking	45
Capítulo 23. Authentication and Interoperability	46
Capítulo 24. Desktop	47
Apéndice A. Historia de revisiones	48

Prefacio

Los lanzamientos menores de Red Hat Enterprise Linux son una adición individual de mejoras, seguridad y corrección de erratas. Las *Red Hat Enterprise Linux 7.1 Notas de lanzamiento* contienen los cambios más importantes, funcionalidades y mejoras introducidas en el sistema operativo de Red Hat Enterprise Linux 7 y a las aplicaciones que acompañan a este lanzamiento menor. Además las *Red Hat Enterprise Linux 7.1 Notas de lanzamiento* documentan los problemas conocidos en Red Hat Enterprise Linux 7.1.



Importante

Las *Red Hat Enterprise Linux 7.1 Notas de lanzamiento* en línea, que se localizan [aquí](#), se deben considerar como la versión actualizada definitiva. A los clientes que tengan preguntas acerca del lanzamiento se les recomienda consultar las *Notas de lanzamiento* en línea para su versión de Red Hat Enterprise Linux.



Nota

Para descripciones de problemas, consulte [English version of the Red Hat Enterprise Linux 7.1 Release Notes](#).

Si requiere información sobre el ciclo de vida de Red Hat Enterprise Linux consulte <https://access.redhat.com/support/policy/updates/errata/>.

Parte I. Nuevas funcionalidades

Esta parte describe las nuevas funcionalidades y mejoras introducidas en Red Hat Enterprise Linux 7.1.

Capítulo 1. Arquitecturas

Red Hat Enterprise Linux 7.1 está disponible como un kit individual en las siguientes arquitecturas: [1].

- 64-bit AMD
- 64-bit Intel
- IBM POWER7 y POWER8 (big endian)
- IBM POWER8 (little endian) [2].
- IBM System z [3]

En este lanzamiento, Red Hat agrupa todas las mejoras de servidores y sistemas y toda la experiencia de código abierto de Red Hat.

1.1. Red Hat Enterprise Linux for POWER, Little Endian

Red Hat Enterprise Linux 7.1 introduce soporte little endian en servidores IBM Power Systems mediante procesadores IBM POWER8. Anteriormente en Red Hat Enterprise Linux 7, solo una variante de big endian se ofrecía para IBM Power Systems. El soporte para little endian en servidores basados en POWER8 tiene como fin mejorar la portabilidad de aplicaciones entre sistemas compatibles 64-bit Intel (**x86_64**) e IBM Power Systems.

- Instalación independiente de los medios se ofrece para instalar Red Hat Enterprise Linux en servidores IBM Power Systems en modo little endian. Estos medios están disponibles desde la sección de Descargas de Red Hat Customer Portal.
- Solo los servidores basados en procesadores IBM POWER8 reciben soporte con Red Hat Enterprise Linux for POWER, little endian.
- Actualmente, Red Hat Enterprise Linux para POWER, little endian únicamente recibe soporte como huésped KVM en **Red Hat Enterprise Virtualization para Power**. La instalación en hardware vacío tiene soporte en la actualidad.
- El gestor de arranque **GRUB2** se utiliza en los medios de instalación y para arranque de red. La [Guía de instalación](#) ha sido actualizada con instrucciones para configurar un servidor de arranque de red para clientes IBM Power Systems mediante **GRUB2**.
- Todos los paquetes de software para IBM Power Systems están disponibles tanto para little endian y la variante big endian de Red Hat Enterprise Linux para POWER.
- Los paquetes compilados para Red Hat Enterprise Linux para POWER, little endian usan el código de arquitectura **ppc64le** - por ejemplo, *gcc-4.8.3-9.ael7b.ppc64le.rpm*.

[1] Observe que la instalación de Red Hat Enterprise Linux 7.1 solo tiene soporte en hardware de 64 bits. Red Hat Enterprise Linux 7.1 puede ejecutarse en sistemas operativos de 32 bits, incluidas las versiones anteriores de Red Hat Enterprise Linux, como máquinas virtuales.

[2] Red Hat Enterprise Linux 7.1 (little endian) solo tiene soporte actualmente como huésped de KVM en hipervisores **Red Hat Enterprise Virtualization for Power y PowerVM**

[3] Observe que Red Hat Enterprise Linux 7.1 soporta hardware IBM zEnterprise 196 o posterior; los sistemas para computador principal IBM System z10 ya no reciben soporte y no arrancarán Red Hat Enterprise Linux 7.1.

Capítulo 2. Hardware Enablement

2.1. Intel Broadwell Processor and Graphics Support

Red Hat Enterprise Linux 7.1 adds support for all current 5th generation Intel processors (code name Broadwell). Support includes the CPUs themselves, integrated graphics in both 2D and 3D mode, and audio support (Broadwell High Definition Legacy Audio, HDMI Audio and DisplayPort Audio).

The **turbostat** tool (part of the *kernel-tools* package) has also been updated with support for the new processors.

2.2. Support for TCO Watchdog and I2C (SMBUS) on Intel Communications Chipset 89xx Series

Red Hat Enterprise Linux 7.1 adds support for TCO Watchdog and I2C (SMBUS) on the 89xx series Intel Communications Chipset (formerly Coletto Creek).

2.3. Intel Processor Microcode Update

CPU microcode for Intel processors in the *microcode_ctl* package has been updated from version **0x17** to version **0x1c** in Red Hat Enterprise Linux 7.1.

Capítulo 3. Instalación y arranque

3.1. Instalador

El instalador de Red Hat Enterprise Linux, **Anaconda**, ha sido mejorado para mejorar el proceso de instalación de Red Hat Enterprise Linux 7.1.

Interfaz

- ❖ La interfaz del instalador gráfico ahora contiene una pantalla adicional que permite configurar el mecanismo de volcado de daños de kernel **Kdump** durante la instalación. Anteriormente, se configuraba después de la instalación mediante la herramienta **firstboot**, la cual no era accesible sin una interfaz gráfica. Ahora, usted puede configurar **Kdump** como parte del proceso de instalación en sistemas sin un entorno gráfico. La nueva pantalla se accede desde el menú principal de instalador (**Resumen de instalación**).

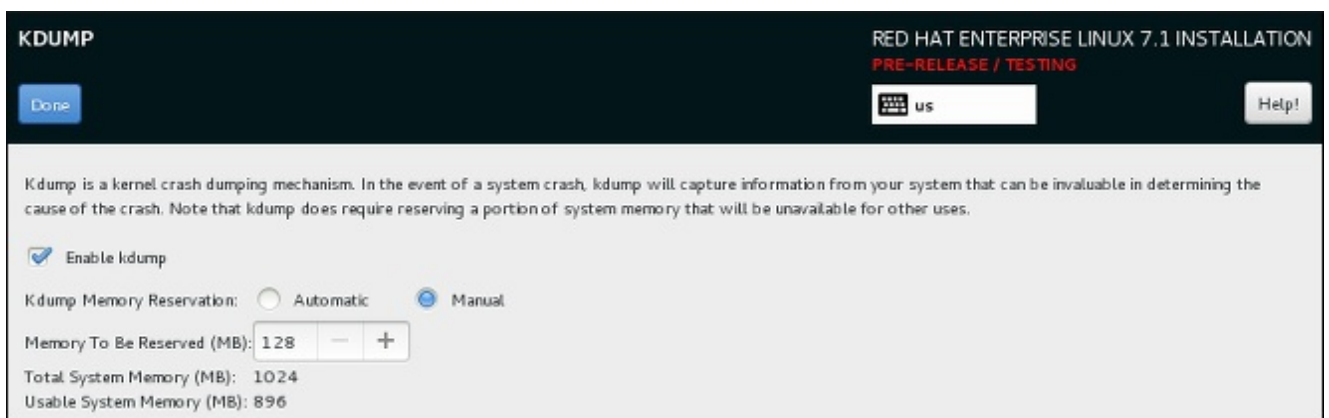


Figura 3.1. Nueva pantalla kdump

- ❖ La pantalla de partición manual ha sido rediseñada para mejorar la experiencia del usuario. Algunos de los controles han sido desplazados a diferentes sitios de la pantalla.

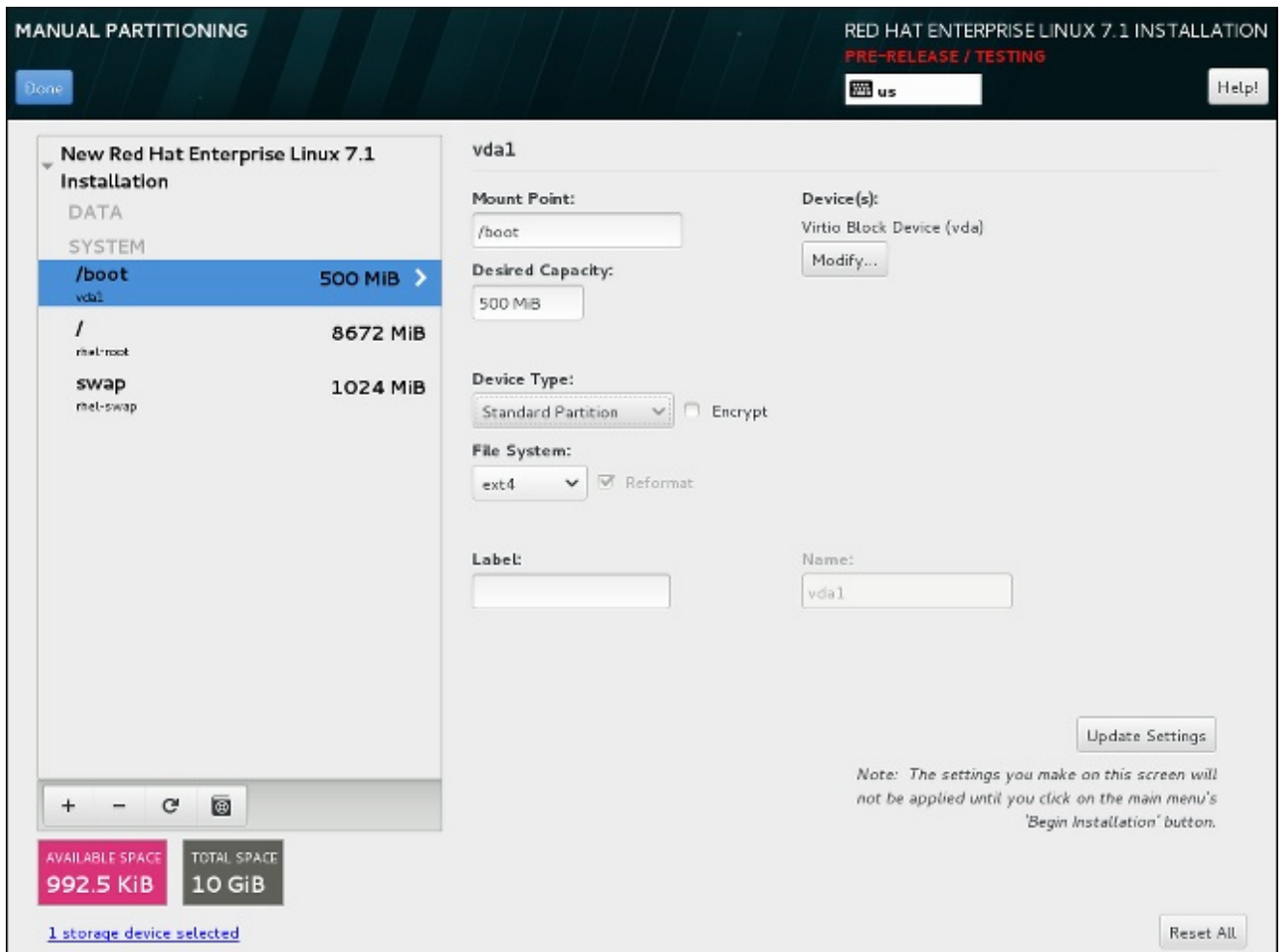


Figura 3.2. Pantalla de partición manual rediseñada

- ✦ Configure un puente de red en la pantalla del instalador **Red & Nombre de host**. Para hacerlo, haga clic en el botón **+** que está en la parte inferior de la lista de interfaces, seleccione **Puente** desde el menú, y configure el puente en el diálogo **Editar conexión de puente**, el cual aparece después. Este diálogo es proporcionado por **NetworkManager** y se documenta totalmente en la Guía de red *Red Hat Enterprise Linux 7.1*.

Se han agregado nuevas opciones Kickstart para configuración de puente. Ver los detalles a continuación.

- ✦ El instalador ya no utiliza consolas para desplegar registros. En su lugar, todos los registros están en paneles **tmux** en la consola virtual 1 (**tty1**). Para acceder a los registros durante la instalación, presione **Ctrl+Alt+F1** para pasar a **tmux**, y luego use **Ctrl+b X** para pasar entre diferentes ventanas (reemplace X por el número de la ventana en particular como se despliega en la parte inferior de la pantalla).

Para volver a la interfaz de instalación gráfica, presione **Ctrl+Alt+F6**.

- ✦ La interfaz de línea de comandos para **Anaconda** ahora incluye ayuda completa. Para verla, use el comando **anaconda -h** en un sistema con el paquete *anaconda* instalado. La interfaz de línea de comandos le permite ejecutar el instalador en un sistema instalado, el cual es útil para instalaciones de imágenes de disco.

Opciones y comandos de Kickstart

- ✦ El comando **logvol** tiene una nueva opción: **--profile=**. Use esta opción para especificar el nombre del perfil de configuración para usar con los volúmenes lógicos. Si se utiliza, el nombre se incluirá en los metadatos para el volumen lógico.

Los perfiles disponibles son **default** y **thin-performance** los cuales se definen en el directorio **/etc/lvm/profile**. Consulte la página de manual **lvm(8)** para obtener información adicional.

- ✦ The behavior of the **--size=** and **--percent=** options of the **logvol** command has changed. Previously, the **--percent=** option was used together with **--grow** and **--size=** to specify how much a logical volume should expand after all statically-sized volumes have been created.

Starting with Red Hat Enterprise Linux 7.1, **--size=** and **--percent=** can not be used on the same **logvol** command.

- ✦ La opción **--autoscreenshot** del comando de kickstart **autostep** ha sido corregido y ahora guarda una instantánea de cada pantalla en el directorio **/tmp/anaconda-screenshots** después de salir de la pantalla mencionada. Después de que la instalación se complete, estas instantáneas se trasladan a **/root/anaconda-screenshots**.
- ✦ El comando **liveimg** ahora soporta instalación desde archivos tar así como también de imágenes de disco. El archivo tar debe contener el medio de instalación del sistema de archivos de root y el nombre del archivo debe finalizar con **.tar**, **.tbz**, **.tgz**, **.txz**, **.tar.bz2**, **.tar.gz**, o **.tar.xz**.
- ✦ Se han agregado nuevas opciones al comando **network** para configurar puentes de redes. Estas opciones son las siguientes:
 - **--bridgeslaves=**: Cuando se utiliza esta opción, se creará el puente de red con el nombre de dispositivo especificado con la opción **--device=**, y se agregarán al puente los dispositivos definidos en la opción **--bridgeslaves=**. Por ejemplo:

```
network --device=bridge0 --bridgeslaves=em1
```

- **--bridgeopts=**: Una lista opcional separada por comas de los parámetros para la interfaz en puente. Los valores disponibles son: **stp**, **priority**, **forward-delay**, **hello-time**, **max-age**, y **ageing-time**. Para más información sobre estos parámetros, consulte la página de manual **nm-settings(5)**.
- ✦ El comando **autopart** tiene una nueva opción, **--fstype**. Esta opción le permite cambiar el tipo de sistema de archivos predeterminado (**xfs**) cuando utilice la partición automática en un archivo Kickstart.
- ✦ Several new features were added to Kickstart for better container support. These features include:
 - **repo --install**: Esta nueva opción guarda la configuración de repositorio provista en el sistema instalado en el directorio **/etc/yum.repos.d/**. Sin usar esta opción, un repositorio configurado en un archivo Kickstart, solo estará disponible durante el proceso de instalación, no en el sistema instalado.
 - **bootloader --disabled**: Esta opción evitará que el gestor de arranque sea instalado.
 - **%packages --nocore**: Una nueva opción para la sección **%packages** de un archivo kickstart que no permita que el sistema instale el grupo de paquetes **@core**. Esto permite la instalación de sistemas extremadamente mínimos para ser utilizados con los contenedores.

Please note that the described options are only useful when combined with containers, and using the options in a general-purpose installation could result in an unusable system.

Entropy Gathering for LUKS Encryption

- If you choose to encrypt one or more partitions or logical volumes during the installation (either during an interactive installation or in a Kickstart file), **Anaconda** will attempt to gather 256 bits of entropy (random data) to ensure the encryption is secure. The installation will continue after 256 bits of entropy are gathered or after 10 minutes. The attempt to gather entropy happens at the beginning of the actual installation phase when encrypted partitions or volumes are being created. A dialog window will open in the graphical interface, showing progress and remaining time.

The entropy gathering process can not be skipped or disabled. However, there are several ways to speed the process up:

- If you can access the system during the installation, you can supply additional entropy by pressing random keys on the keyboard and moving the mouse.
- If the system being installed is a virtual machine, you can attach a *virtio-rng* device (a virtual random number generator) as described in the [Red Hat Enterprise Linux 7.1 Virtualization Deployment and Administration Guide](#).

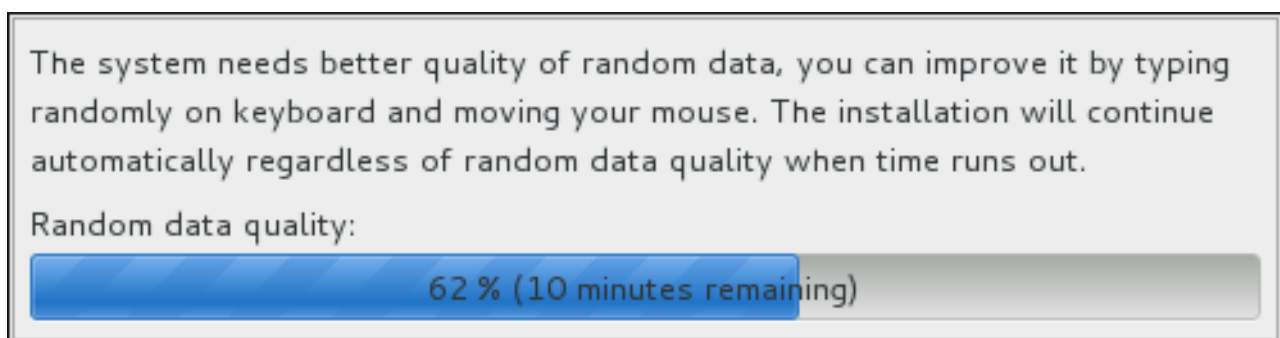


Figura 3.3. Gathering Entropy for Encryption

Ayuda incorporada en instalador gráfico

Cada ventana en la interfaz gráfica de instalador y la herramienta **Initial Setup** ahora tiene un botón de **Ayuda** en la esquina superior derecha. Al hacer clic en este botón se abre la sección de la [Guía de instalación](#) relevante para la pantalla actual mediante el explorador de ayuda **Yelp**.



Figura 3.4. Anaconda built-in help

3.2. Gestor de arranque

Los medios de instalación para IBM Power Systems ahora usan el gestor de arranque **GRUB2** en lugar de **yaboot**. Para la variante big endian de Red Hat Enterprise Linux para POWER, **GRUB2** es el preferido pero **yaboot** también puede utilizarse. La variante little endian recientemente utilizada requiere **GRUB2** para arrancar.

La [Guía de instalación](#) ha sido actualizada con instrucciones para configurar un servidor de arranque de red para clientes de IBM Power Systems mediante **GRUB2**.

Capítulo 4. Almacenamiento

Cache LVM

As of Red Hat Enterprise Linux 7.1, LVM cache is fully supported. This feature allows users to create logical volumes with a small fast device performing as a cache to larger slower devices. Please refer to the **lvm(7)** manual page for information on creating cache logical volumes.

Observe las siguientes restricciones en el uso de los volúmenes lógicos (LV) de cache :

- LV cache debe ser un dispositivo de alto nivel. No puede utilizarse como un LV de grupo fino, una imagen de un LV RAID u otros subtipos de LV.
- The cache LV sub-LVs (the origin LV, metadata LV, and data LV) can only be of linear, stripe, or RAID type.
- Las propiedades del LV cache no se pueden cambiar después de la creación. Para cambiar propiedades cache, retire la memoria cache y vuélvala a crear con las propiedades deseadas.

Administración de matriz de almacenamiento con API de libStorageMgmt

En Red Hat Enterprise Linux 7.1, la administración de matrices de almacenamiento con **libStorageMgmt**, una matriz independiente de API, recibe soporte total. La API es estable, consistente, y permite a los desarrolladores manejar programáticamente las diferentes matrices de almacenamiento y utilizar las funcionalidades aceleradas de hardware. Los administradores de sistemas también pueden usar **libStorageMgmt** para configurar manualmente el almacenamiento y automatizar las tareas de administración de almacenamiento con la interfaz de línea de comandos. Observe que el complemento **Targetd** no recibe soporte total y permanece como Muestra previa de tecnología.

- NetApp Filer (ontap 7-Mode)
- Nexenta (nstor 3.1.x only)
- SMI-S, para los siguientes proveedores:
 - HP 3PAR
 - Lanzamiento del SO 3.2.1 o posterior
 - EMC VMAX y VNX
 - Habilitador de soluciones V7.6.2.48 o posterior
 - Proveedor SMI-S V4.6.2.18 hotfix kit o posterior
 - Proveedor no incorporado de matriz HDS VSP
 - Hitachi Command Suite v8.0 o posterior

Para obtener más información sobre **libStorageMgmt**, consulte el [capítulo relevante en la Guía de administración de almacenamiento](#).

Soporte para LSI Syncro

Red Hat Enterprise Linux 7.1 incluye código en el controlador **megaraid_sas** para habilitar adaptadores HA-SAS LSI Syncro CS. Aunque el controlador **megaraid_sas** recibe soporte total para adaptadores anteriores, el uso de este controlador para Syncro CS está disponible como Muestra previa de tecnología. El soporte para este adaptador se puede obtener directamente de LSI, el integrador de sistemas o el distribuidor del sistema. Se recomienda a los usuarios que implementen Syncro CS en Red Hat Enterprise Linux 7.1 provean sus comentarios a Red Hat y LSI. Para obtener más información sobre soluciones LSI Syncro CS, consulte <http://www.lsi.com/products/shared-das/pages/default.aspx>.

Interfaz de programación de aplicaciones LVM

Red Hat Enterprise Linux 7.1 introduce la interfaz de programación de aplicaciones (API) como una muestra previa de tecnología. Esta API se utiliza para solicitar y controlar algunos aspectos de LVM.

Para obtener más información, vaya al archivo del encabezado **lvm2app.h**.

Soporte para DIF/DIX

DIF/DIX es una nueva adición al estándar de SCSI y una muestra previa de tecnología en Red Hat Enterprise Linux 7.1. DIF/DIX aumenta el tamaño de 512 bytes de bloque de disco utilizado comúnmente a 512 a 520 bytes, y adiciona el Campo de integridad de datos (DIF). El DIF almacena un valor de suma de verificación para el bloque de datos que es calculado por el Adaptador de bus de host (HBA) cuando se presenta una escritura. El dispositivo de almacenamiento confirma entonces la suma de verificación en recepción y guarda los datos y la suma de verificación. Igualmente, cuando se presenta una lectura, la suma de verificación puede ser revisada por el dispositivo de almacenamiento y por el HBA que recibe.

For more information, refer to the section Block Devices with DIF/DIX Enabled in the [Storage Administration Guide](#).

Mejoramiento de verificación de errores de sintaxis multirrutas del mapeador de dispositivos multirrutas y salida

Se mejoró la herramienta **device-mapper-multipath** para verificar de una forma más fiable, el archivo **multipath.conf**. Como resultado, si **multipath.conf** contiene líneas que no pueden leerse, **device-mapper-multipath** reporta un error e ignora estas líneas para evitar una lectura incorrecta.

Además, se han agregado las siguientes expresiones de comodines para el comando **multipathd show paths format**:

- ✦ %N y %n para el host y los Nombres de nodos universales de Canal de fibra de destino, respectivamente.
- ✦ %R y %r para el host y los Nombres de puerto universal de canal de fibra, respectivamente.

Ahora es más fácil asociar multirrutas con hosts de Canal de fibra, destinos y sus puertos, lo cual permite a los usuarios manejar su configuración de almacenamiento de una forma más efectiva.

Capítulo 5. Sistemas de archivos

Soporte para sistema de archivos Btrfs

Se ofrece soporte al sistema de archivos **Btrfs** (B-Tree) como Muestra previa de tecnología en Red Hat Enterprise Linux 7.1. Este sistema de archivos ofrece funcionalidades de administración avanzada, fiabilidad y escalabilidad. permite a los usuarios crear instantáneas, permite compresión y administración de dispositivos integrados.

OverlayFS

The **OverlayFS** file system service allows the user to "overlay" one file system on top of another. Changes are recorded in the upper file system, while the lower file system becomes read-only. This can be useful because it allows multiple users to share a file system image, for example containers, or when the base image is on read-only media, for example a DVD-ROM.

On Red Hat Enterprise Linux 7.1, OverlayFS is supported as a Technology Preview. There are currently two restrictions:

- ✦ It is recommended to use **ext4** as the lower file system; the use of **xfs** and **gfs2** file systems is not supported.
- ✦ SELinux is not supported, and to use OverlayFS, it is required to disable enforcing mode.

Soporte de NFS paralelo

El soporte de NFS paralelo (pNFS) es una parte del estándar NFS v4.1 que permite a los clientes acceder directamente a dispositivos de almacenamiento en paralelo. La arquitectura pNFS puede mejorar la escalabilidad y rendimiento de servidores NFS para varias cargas de trabajo comunes.

pNFS defines three different storage protocols or layouts: files, objects, and blocks. The client supports the files layout, and with Red Hat Enterprise Linux 7.1, the blocks and object layouts are fully supported.

Red Hat continúa funcionando con socios y proyectos de código abierto para calificar nuevos tipos de distribución pNFS y ofrecer soporte total a más tipos de distribuciones en el futuro.

Para obtener más información sobre pNFS, consulte <http://www.pnfs.com/>.

Capítulo 6. Kernel

Soporte para dispositivos de bloque Ceph

Los módulos **libceph.ko** y **rbd.ko** han sido agregados al kernel de Red Hat Enterprise Linux 7.1. Estos módulos RBD de kernel permiten que un host Linux vea un dispositivo de bloque Ceph como una entrada de disco regular que puede ser montada a un directorio y formateada con un sistema de archivos estándar, tales como **XFS** o **ext4**.

Observe que el módulo CephFS , **ceph.ko**, en la actualidad no tiene soporte en Red Hat Enterprise Linux 7.1.

Actualizaciones de Flash MCL simultáneas

Las actualizaciones de nivel microcódigo (MCL) están activadas en Red Hat Enterprise Linux 7.1 en la arquitectura IBM System z . Estas actualizaciones pueden aplicarse sin impactar las operaciones de E/S para los medios de almacenamiento flash y notificar usuarios del nivel de servicio de hardware.

Parche de kernel dinámico

Red Hat Enterprise Linux 7.1 introduce **kpatch**, una herramienta dinámica de parches de kernel, como una muestra previa de tecnología. La herramienta **kpatch** permite a los usuarios manejar una colección de parches de kernel binarios que se pueden usar de forma dinámica para parchear el kernel sin necesidad de reiniciar. Observe que **kpatch** tiene soporte para ejecutarse en arquitecturas AMD64 e Intel 64, únicamente.

Crashkernel con más de una CPU

Red Hat Enterprise Linux 7.1 permite el arranque de crashkernel con más de una CPU. Esta función recibe soporte como muestra previa de tecnología.

Destino dm-era

Red Hat Enterprise Linux 7.1 introduce el mapeador de dispositivo dm-era como una muestra previa de tecnología. dm-era mantiene el rastro de los bloques que fueron escritos dentro de un determinado tiempo de usuario denominado "era". Cada instancia de destino de era mantiene la era actual como un contador de 32 bits que aumenta de forma monótona. Este destino permite que software de respaldo pueda rastrear bloques que hayan cambiado desde la última copia de seguridad. También permite la invalidación parcial del contenido de la memoria cache para restaurar coherencia tras volver a la instantánea de distribuidor. Se espera principalmente que el destino dm-era sea emparejado con el destino dm-cache.

Controlador de kernel Cisco VIC

El controlador de kernel Cisco VIC Infiniband ha sido agregado a Red Hat Enterprise Linux 7.1 como una muestra previa de tecnología. Este controlador permite usar un directorio de acceso de memoria remota (RDMA)-como semántica en arquitecturas Cisco de propietario .

Administración de entropía mejorada en hwrng

El soporte de hardware paravirtualizado RNG (hwrng) para huéspedes de Linux vía virtio-rng ha sido mejorado en Red Hat Enterprise Linux 7.1. Anteriormente, el demonio **rngd** debía iniciarse en el huésped y dirigirse al grupo de entropía de kernel de huéspedes. Al iniciar con Red Hat Enterprise Linux 7.1, el paso manual ha sido retirado, El nuevo hilo **khwrngd** busca entropía desde el dispositivo **virtio-rng** si la entropía de huéspedes cae por debajo del nivel específico. Al hacer este proceso transparente, ayuda a que

todos los huéspedes de Red Hat Enterprise Linux utilicen los beneficios de seguridad mejorada del hardware RNG paravirtualizado provisto por hosts KVM.

Mejoras de rendimiento del programador de balance de carga

Anteriormente, el código de balance de carga de programador equilibraba todas las CPU inactivas. En Red Hat Enterprise Linux 7.1, el balance de carga inactivo en una CPU inactiva solo se realiza cuando la CPU está pendiente de un balance de carga. Esta nueva conducta reduce la tasa de balanceo de carga en CPU no inactivas y por lo tanto, la cantidad de trabajo innecesaria del programador, lo cual mejora el rendimiento.

Balance newidle mejorado en programador

La conducta del programador ha sido modificada para detener la búsqueda de tareas en el código de balance **newidle** si hay tareas ejecutables, lo cual conlleva a un mejor rendimiento.

HugeTLB Soporta asignación de Per-Node 1GB Huge Page

Red Hat Enterprise Linux 7.1 ha sido agregado para soportar asignación de páginas gigantes en tiempo de ejecución, lo cual permite que el usuario de **hugetlbfs** de 1 GB especifique el Nodo de 1 GB que debe ser asignado durante el tiempo de ejecución.

Nuevo mecanismo de bloqueo basado en MCS

Red Hat Enterprise Linux 7.1 introduce un nuevo mecanismo de bloqueo, cerrojos MCS. Este nuevo mecanismo de bloqueo reduce de forma significativa la sobrecarga **spinlock** en grandes sistemas, lo cual hace que los **spinlocks** sean por lo general, más eficientes en Red Hat Enterprise Linux 7.1.

El tamaño de pila del proceso aumentó de 8KB a 16KB

Al iniciar con Red Hat Enterprise Linux 7.1, el tamaño de pila del proceso de kernel ha aumentado de 8KB a 16KB para ayudar a grandes procesos que usan espacio de pila.

Las funcionalidades uprobe y uretprobe habilitadas en perf y systemtap

En Red Hat Enterprise Linux 7.1, las funcionalidades **uprobe** y **uretprobe** operan correctamente con el comando **perf** y el script **systemtap**.

Verificación de consistencia de datos de punta a punta

La verificación de consistencia de datos de punta a punta en IBM System z recibe soporte total en Red Hat Enterprise Linux 7.1. Así, se mejora la integridad de datos y se evita la corrupción y la pérdida de datos de una forma más efectiva.

DRBG en sistemas de 32 bits

Con Red Hat Enterprise Linux 7.1, el generador de bits aleatorio determinista, DRBG, ha sido actualizado para operar en sistemas de 32 bits.

Soporte para grandes tamaños de crashkernel

The **Kdump** kernel crash dumping mechanism on systems with large memory, that is up to the Red Hat Enterprise Linux 7.1 maximum memory supported limit of 6TB, has become fully supported in Red Hat Enterprise Linux 7.1.

Capítulo 7. Virtualización

Aumento en el número máximo de vCPU en KVM

El número máximo de CPU virtuales en (vCPU) en un huésped KVM se aumentó a 240. De este modo, aumenta la cantidad de unidades de procesamiento virtual que el usuario puede asignar al huésped y por lo tanto, mejora su rendimiento potencial.

Soporte para nuevas instrucciones para Intel Core 5a generación en QEMU, KVM y libvirt API

En Red Hat Enterprise Linux 7.1, soporte para 5a generación de procesadores Intel Core ha sido agregado para el hipervisor QEMU, el código de kernel KVM y la API **libvirt**. De esta manera, los huéspedes KVM pueden usar las siguientes instrucciones y funcionalidades: ADCX, ADOX, RDSFEED, PREFETCHW, y Prevención de acceso en modo de supervisor (SMAP).

Soporte de USB 3.0 para huéspedes KVM

Red Hat Enterprise Linux 7.1 Soporte mejorado de funcionalidades USB al agregar la emulación del adaptador host USB 3.0 (xHCI) como Muestra previa de tecnología.

Compresión para el comando dump-guest-memory

En Red Hat Enterprise Linux 7.1, el comando **dump-guest-memory** ofrece soporte para compresión de volcado de daños. Esto hace que los usuarios que no puedan usar el comando **virsh dump** para requieran menos espacio de disco duro para volcados de daños de huéspedes. Además, guardar un volcado de daños de huésped con frecuencia, toma menos tiempo que guardar uno que no esté comprimido.

Open Virtual Machine Firmware

El Firmware abierto para máquina virtual Machine Firmware (OVMF) está disponible en Red Hat Enterprise Linux 7.1 como una Muestra previa de tecnología. OVMF es un entorno UEFI de arranque seguro para huéspedes Intel AMD64 e Intel 64.

Mejoras de rendimiento de red en Hyper-V

Varias funcionalidades del controlador de red Hyper-V reciben soporte para mejorar el rendimiento de red. Por ejemplo, escalamiento de recepción lateral, Carga de envío grande, Distribución y Recolección de E/S ahora tiene soporte, y rendimiento de red mejorado.

hypervcopyd en hyperv-daemons

El demonio **hypervcopyd** ha sido agregado a los paquetes *hyperv-daemons*. **hypervcopyd** es una implementación de la funcionalidad del servicio de copia de archivos para Linux Guest que se ejecutan en host Hyper-V 2012 R2 . Permite al host copiar un archivo (por VMBUS) en Linux Guest.

Nuevas funcionalidades en libguestfs

Red Hat Enterprise Linux 7.1 introduce un número de nuevas funcionalidades en **libguestfs**, un conjunto de herramientas para acceder y modificar imágenes de disco de máquinas virtuales.

Nuevas herramientas

- ✦ **virt-builder** — una nueva herramienta para construir imágenes de máquinas virtuales. Utilice virt-builder para crear huéspedes de una forma segura y rápida y personalizarlos.
- ✦ **virt-customize** — una nueva herramienta para personalizar imágenes de disco de máquinas virtuales. Utilice virt-customize para editar archivos de configuración, ejecutar scripts y establecer contraseñas.
- ✦ **virt-diff** — una nueva herramienta para mostrar las diferencias entre los sistemas de archivos de dos máquinas virtuales. Use virt-diff para descubrir fácilmente qué archivos han sido cambiados entre instantáneas.
- ✦ **virt-log** — una nueva herramienta para listar archivos de registro desde huéspedes. La herramienta virt-log soporta una variedad de huéspedes incluidos el Linux tradicional, el Linux que usa diarios y el registro de eventos de Windows.
- ✦ **virt-v2v** — una nueva herramienta para convertir huéspedes desde un hipervisor externo para ejecutarse en KVM, administrado por libvirt, OpenStack, oVirt, Red Hat Enterprise Virtualization (RHEV), y otros destinos. Actualmente, virt-v2v puede convertir huéspedes Red Hat Enterprise Linux y Windows que se ejecutan en Xen y VMware ESX.

Seguimiento de registro de vuelo

Support for flight recorder tracing has been introduced in Red Hat Enterprise Linux 7.1. Flight recorder tracing uses **SystemTap** to automatically capture qemu-kvm data as long as the guest machine is running. This provides an additional avenue for investigating qemu-kvm problems, more flexible than qemu-kvm core dumps.

Para obtener más información sobre instrucciones para configurar y usar el seguimiento de registro de vuelo, consulte la [Guía de implementación y administración de virtualización](#).

RDMA-based Migration of Live Guests

The support for Remote Direct Memory Access (RDMA)-based migration has been added to **libvirt**. As a result, it is now possible to use the new **rdma://** migration URI to request migration over RDMA, which allows for significantly shorter live migration of large guests. Note that prior to using RDMA-based migration, RDMA has to be configured and **libvirt** has to be set up to use it.

Capítulo 8. Agrupamiento

Tiempo de espera de Dynamic Token para Corosync

La opción **token_coefficient** ha sido agregada a **Corosync Cluster Engine**. El valor de **token_coefficient** se utiliza únicamente cuando la sección **nodelist** se especifica y contiene al menos tres nodos. En tal situación, el tiempo de espera se computa de la siguiente manera:

$$[\text{token} + (\text{amount of nodes} - 2)] * \text{token_coefficient}$$

Esto permite al clúster escalar sin cambiar manualmente el tiempo de espera del token cada vez que se agrega un nuevo nodo. El valor predeterminado es de 650 milisegundos, pero puede establecerse a 0, resultando en una remoción efectiva de esta funcionalidad.

Esta funcionalidad permite a **Corosync** manejar la adición y remoción dinámicas de nodos.

Mejoramiento de disyuntor Corosync

La funcionalidad del cuórum **auto_tie_breaker** de **Corosync** ha sido mejorada para proporcionar opciones para configuración y modificación de nodos disyuntores más flexibles. Los usuarios ahora pueden seleccionar una lista de nodos que retendrán un cuórum en caso de una división igual de clúster, o elegir que el cuórum será retenido por el nodo con el ID de nodo más bajo o el ID de nodo más alto.

Mejoras para Red Hat High Availability

Para el lanzamiento de Red Hat Enterprise Linux 7.1, **Red Hat High Availability Add-On** soporta las siguientes funcionalidades. Para obtener información sobre funcionalidades, consulte el manual *High Availability Add-On Reference*.

- Ahora, el comando **pcs resource cleanup** puede restablecer el estatus de recursos y **failcount** para todos los recursos.
- Puede especificar un parámetro **lifetime** para el comando **pcs resource move** para indicar el tiempo en el que la restricción del recursos que crea este comando permanecerá en vigor.
- Utilice el comando **pcs acl** para establecer permisos para usuarios locales para otorgar permisos de solo lectura o de lectura y escritura para configuración de clúster mediante el uso de listas de control de acceso (ACL).
- Ahora, el comando **pcs constraints** soporta la configuración de opciones de restricción específicas además de las opciones de recursos generales.
- El comando **pcs resource create** soporta el parámetro **disabled** para indicar que el recurso está siendo creado automáticamente.
- El comando **pcs cluster quorum unblock** evita que el clúster espere por todos los nodos cuando establece un cuórum.
- Configure el orden de grupo de recursos con los parámetros **before** y **after** del comando **pcs resource create**.
- Realice una copia de seguridad la configuración de clúster en un tarball y restaure los archivos de configuración de clúster en todos los nodos desde el respaldo con las opciones **backup** y **restore** del comando **pcs config**.

Capítulo 9. Compilador y herramientas

Soporte de corrección en caliente para Linux en binarios System z

La colección del compilador GNU (GCC) implementa soporte para correcciones en línea de código multihilos para Linux en binarios System z. La selección de funciones específicas para correcciones en caliente se habilita al usar un "atributo de función" y puede habilitarse para todas las funciones con la opción de línea de comandos **-mhotpatch**.

La activación de correcciones en caliente tienen un impacto negativo en el tamaño y rendimiento del software. Es por lo tanto, recomendable usar correcciones en caliente para funciones específicas en lugar de habilitar soporte de correcciones en caliente para todas las funciones.

El soporte para correcciones en caliente para Linux en binarios System z era una Muestra previa de tecnología para Red Hat Enterprise Linux 7.0. Con el lanzamiento de Red Hat Enterprise Linux 7.1, ahora tiene soporte total.

Mejoramiento en la Interfaz de programación de rendimiento (PAPI)

Red Hat Enterprise Linux 7 incluye la **Interfaz de programación de aplicaciones y rendimiento (PAPI)**. PAPI es una especificación de interfaces entre plataformas a contadores de rendimiento de hardware en microprocesadores. Estos contadores existen como un conjunto pequeño de registros que cuentan eventos, los cuales son incidentes de señales específicas para la función del procesador. La monitorización de estos eventos tiene una variedad de usos en análisis de rendimiento de aplicaciones y ajustes.

In Red Hat Enterprise Linux 7.1 PAPI and the related **libpfm** libraries have been enhanced to provide support for IBM Power8, Applied Micro X-Gene, ARM Cortex A57, and ARM Cortex A53 processors. In addition, the events sets have been updated for Intel Haswell, Ivy Bridge, and Sandy Bridge processors.

OProfile

OProfile es un perfilador amplio de sistema para sistemas Linux. El perfilador se ejecuta de forma transparente en el segundo plano y los datos de perfil se recolectan en cualquier momento. En Red Hat Enterprise Linux 7.1, **OProfile** ha sido mejorada para proporcionar soporte para las siguientes familias de procesadores: Intel Atom Processor C2XXX, 5th Generation Intel Core Processors, IBM Power8, AppliedMicro X-Gene, y ARM Cortex A57.

OpenJDK8

Como una muestra de tecnología, Red Hat Enterprise Linux 7.1 presenta los paquetes *java-1.8.0-openjdk*, los cuales contienen la última versión del Open Java Development Kit (OpenJDK), OpenJDK8. Estos paquetes proporcionan una implementación completa de conformidad con Java SE 8 y puede ser utilizada en paralelo con los paquetes existentes *java-1.7.0-openjdk*, los cuales están disponibles en Red Hat Enterprise Linux 7.1.

Java 8 ofrece numerosas mejoras, tales como expresiones Lambda, métodos predeterminados, un nuevo Stream API para colecciones, JDBC 4.2, soporte para hardware AES y mucho más. Además, OpenJDK8 contiene numerosas actualizaciones de rendimiento y correcciones de errores.

sosreport reemplaza a Snap

La herramienta depreciada **snap** ha sido retirada del paquete *powerpc-utils*. Su funcionalidad ha sido integrada dentro de la herramienta **sosreport**.

Soporte GDB para Little-Endian 64-bit PowerPC

Red Hat Enterprise Linux 7.1 implementa soporte para la arquitectura 64-bit PowerPC little-endian en el GNU Debugger (GDB).

Mejora de Tuna

Tuna es una herramienta que ha sido utilizada para ajustar programadores de ajustes, tales como la política del programador, prioridad RT, y afinidad de CPU. Con Red Hat Enterprise Linux 7.1, la Interfaz gráfica de usuario **Tuna** ha sido mejorada para solicitar autorización de root para ser lanzada, a fin de que el usuario no tenga que ejecutar escritorio como root para invocar la GUI de **Tuna**. Para obtener más información sobre **Tuna**, consulte [Tuna User Guide](#).

Capítulo 10. Red

Conexión de red confiable

Red Hat Enterprise Linux 7.1 introduce la NAC (funcionalidad de conexión de red de confianza) como una muestra previa de tecnología. NAC se utiliza con soluciones NAC (Control de acceso de red), tales como TLS, 802.1X o IPsec para evaluar la postura de punto final; es decir, recoger información de sistema de punto final, tal como parámetros de configuración del sistema operativo, paquetes instalados, y otros, denominados como medidas de integridad). La conexión de red de confianza, se utiliza para verificar estas medidas con el acceso de políticas antes de permitir el punto final para acceder a la red.

Funcionalidad SR-IOV en el controlador qlcnic

Se ha añadido soporte para virtualización de E/S de root individual (SR-IOV) al controlador **qlcnic** como una muestra previa de tecnología. El soporte para esta funcionalidad será proporcionado directamente por QLogic, y se anima a los clientes a hacer sus comentarios a QLogic y Red Hat. La otra funcionalidad en el controlador qlcnic sigue recibiendo soporte total.

Filtro de paquetes Berkeley

Se ha agregado soporte para Filtro de paquetes Berkeley (BPF) basado en *clasificador de tráfico* a Red Hat Enterprise Linux 7.1. BPF se utiliza en filtraje de paquetes para conectores de paquetes, entornos de prueba en *modo de computación seguro* (seccomp), y en Netfilter. BPF tiene una implementación justo a tiempo para las arquitecturas más importantes y tiene una sintaxis rica para filtros de construcción.

Estabilidad de reloj mejorada

Anteriormente, los resultados de los tests indicaban que al inhabilitar la capacidad del kernel sin intervalo podría mejorar de forma significativa la estabilidad de reloj del sistema. El modo de kernel sin intervalo, puede inhabilitarse al agregar **nohz=off** a los parámetros de opciones de arranque de kernel en Red Hat Enterprise Linux 7.1 ha mejorado bastante la estabilidad del reloj del sistema y la diferencia en estabilidad del reloj con y sin **nohz=off** debe ser mucho más pequeña ahora para la mayoría de usuarios. Esto es útil para sincronizar aplicaciones mediante **PTP** y **NTP**.

Paquetes libnetfilter_queue

Se ha agregado el paquete *libnetfilter_queue* a Red Hat Enterprise Linux 7.1. **libnetfilter_queue** es una biblioteca de espacio de usuario que ofrece una API para paquetes que han estado en cola por el filtro de paquetes de kernel. Habilita la recepción de paquetes en cola desde el subsistema del kernel **nfnetlink_queue**, al leer los paquetes, describir encabezados de paquetes y reinyectar paquetes alterados.

Mejoras en equipo

El paquete *libteam* ha sido actualizado a la versión **1.14-1** en Red Hat Enterprise Linux 7.1. Proporciona una cantidad de correcciones de errores y mejoras, en particular, **teamd** puede ser regenerado automáticamente por **systemd**, el cual aumenta confiabilidad en general.

Controlador Intel QuickAssist Technology

Se ha agregado el controlador Intel QuickAssist Technology (QAT) a Red Hat Enterprise Linux 7.1. El controlador QAT habilita el hardware QuickAssist, el cual agrega capacidades criptográficas de descarga a un sistema.

Soporte LinuxPTP timemaster Support para conmutación entre PTP y NTP

El paquete *linuxptp* ha sido actualizado a la versión **1.4** en Red Hat Enterprise Linux 7.1. Proporciona una cantidad de correcciones de errores y mejoras, en particular, ofrece soporte para conmutación entre los dominios **PTP** y fuentes **NTP** mediante la aplicación **timemaster**. Cuando hay varios dominios **PTP** disponibles en la red, o se necesita recuperación a **NTP**, se puede utilizar el programa **timemaster** para sincronizar el reloj del sistema con todas las fuentes de tiempo disponibles.

initscripts de red

Se ha agregado soporte para nombres VLAN personalizados en Red Hat Enterprise Linux 7.1. Se ha agregado soporte mejorado para **IPv6** en túneles GRE; la dirección interna ahora persiste entre rearranques.

TCP Delayed ACK

Se ha agregado soporte para TCP Delayed ACK configurable al paquete *iproute* en Red Hat Enterprise Linux 7.1. Puede habilitarse mediante el comando `ip route quickack`.

NetworkManager

Opción de vinculación **lACP_rate** ahora tiene soporte en Red Hat Enterprise Linux 7.1. **NetworkManager** ha sido mejorado para facilitar denominación de dispositivos cuando se renombran las interfaces master con interfaces esclavas.

Además, se ha agregado un parámetro de prioridad a la función de auto-connect de **NetworkManager**. Si hay más de un candidato eligible está disponible ahora para auto-connect, **NetworkManager** selecciona la conexión con la prioridad más alta. Si todas las conexiones tienen valores de prioridad iguales, **NetworkManager** usa la conducta predeterminada y selecciona la última conexión activa.

Espacios de nombres de red y VTI

Se ha agregado soporte para las *interfaces de túnel virtual* (VTI) con espacios de nombres en Red Hat Enterprise Linux 7.1. Esto permite el tráfico desde una VTI para ser pasada entre diferentes espacios de nombres cuando los paquetes están encapsulados o desencapsulados.

Almacenamiento de configuración alternativo para MemberOf Plug-In

La configuración del complemento **MemberOf** para el Servidor de directorio 389 ahora puede almacenarse en un sufijo asignado a una base de datos de segundo plano. Permite la replicación de la configuración del complemento **MemberOf**, lo cual facilita al usuario el mantenimiento constante **MemberOf** en un entorno replicado.

Capítulo 11. Linux Containers

The **Docker** project is an open-source project that automates the deployment of applications inside Linux Containers, and provides the capability to package an application with its runtime dependencies into a container. It provides a command-line tool for the life cycle management of image-based containers. Linux containers enable rapid application deployment, simpler testing, maintenance, and troubleshooting while improving security. Using Red Hat Enterprise Linux 7 with containers allows customers to increase staff efficiency, deploy third-party applications faster, enable a more agile development environment, and manage resources more tightly.

To quickly get up-and-running with docker formatted containers, refer to [Get Started with docker Formatted Containers](#).

Red Hat Enterprise Linux 7.1 ships with docker version 1.4.1, which includes a number of new features, security fixes, patches and changes. Highlights include:

- The ENV instruction in the Dockerfile now supports arguments in the form of ENV name=value name2=value2 ...
- An experimental overlayfs storage driver has been introduced.
- An update is included for CVE-2014-9356: Path traversal during processing of absolute symlinks. Absolute symlinks were not adequately checked for traversal which created a vulnerability via image extraction and/or volume mounts.
- An update is included for CVE-2014-9357: Escalation of privileges during decompression of LZMA (.xz) archives. Docker 1.3.2 added chroot for archive extraction. This created a vulnerability that could allow malicious images or builds to write files to the host system and escape containerization, leading to privilege escalation.
- An update is included for CVE-2014-9358: Path traversal and spoofing opportunities via image identifiers. Image IDs passed either via docker load or registry communications were not sufficiently validated. This created a vulnerability to path traversal attacks wherein malicious images or repository spoofing could lead to graph corruption and manipulation.

Red Hat provides platform container images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7.

Red Hat también proporciona **Kubernetes** para uso en contenedores organizados. Para más información sobre Kubernetes, consulte [Get Started Orchestrating Docker Containers with Kubernetes](#).

Linux containers are supported running on hosts with SELinux enabled. SELinux is not supported when the `/var/lib/docker` directory is located on a volume using the B-tree file system (Btrfs).

11.1. Components of docker Formatted Containers

The docker container format works with the following fundamental components:

- *Contenedor* – un entorno de prueba de aplicaciones. Cada contenedor se basa en una *imagen* que guarda los datos de configuración necesarios. Cuando usted lanza un contenedor desde una imagen, se agrega una capa de escritura en la parte superior de esta imagen. Cada vez que usted envía un contenedor (mediante el comando **docker commit**), se agrega una nueva capa de imagen para guardar sus cambios.

- ❖ *Imagen* – una instantánea estática de la configuración de contenedores. La imagen es una capa de solo lectura que nunca se modifica, todos los cambios se hacen en la parte superior de la capa de escritura y pueden guardarse únicamente al crear una nueva imagen. Cada imagen depende de una o más imágenes padres.
- ❖ *Platform Container Image* – an image that has no parent. Platform container images define the runtime environment, packages, and utilities necessary for a containerized application to run. The platform image is read-only, so any changes are reflected in the copied images stacked on top of it. See an example of such stacking in [Figura 11.1, “Capas de imágenes con el formato Docker”](#).
- ❖ *Registro* – un repositorio de imágenes. Los registros son repositorios públicos o privados que contienen imágenes disponibles para descargar. Algunos registros permiten a los usuarios cargar imágenes para que puedan estar disponibles para otros.
- ❖ *Dockerfile* – un archivo de configuración con instrucciones de construcción para imágenes de Docker. Dockerfiles proporcionan una forma de automatizar, reutilizar y compartir procedimientos de construcción.

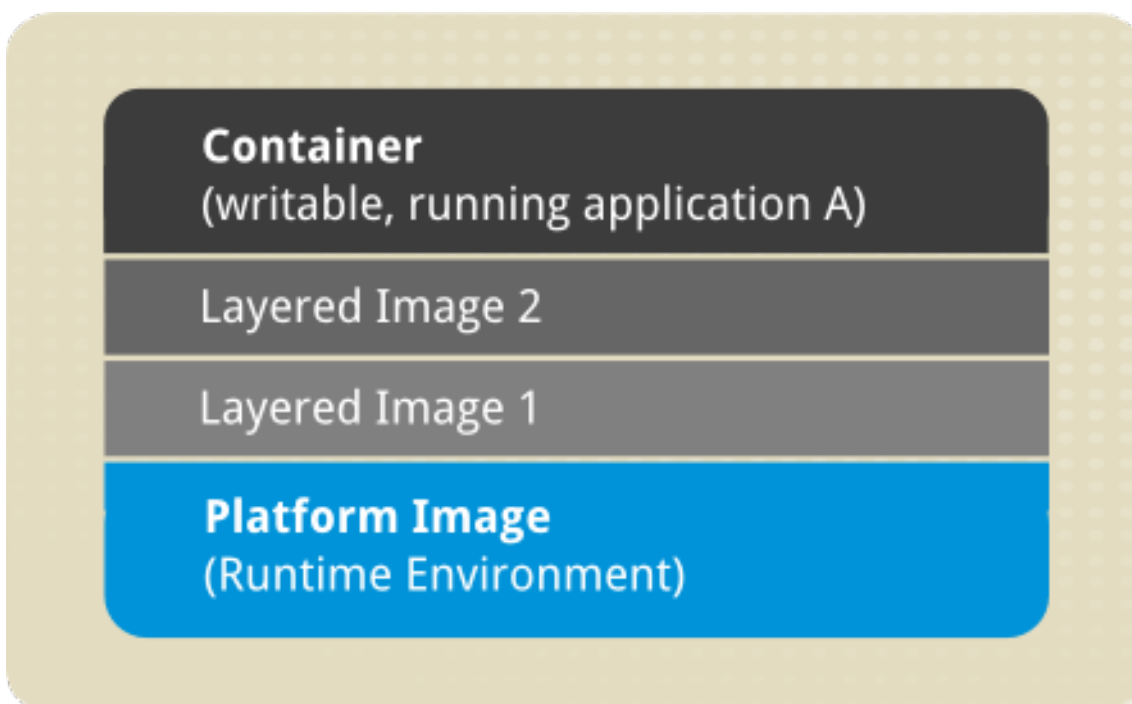


Figura 11.1. Capas de imágenes con el formato Docker

11.2. Advantages of Using Containers

The Docker project provides an API for container management, an image format, and the possibility to use a remote registry for sharing containers. This scheme benefits both developers and system administrators with advantages such as:

- ❖ *Rápida implementación de aplicaciones* – los contenedores incluyen los requerimientos de tiempo de ejecución mínimos de la aplicación, al reducir su tamaño y permitirles ser implementadas rápidamente.
- ❖ *Portabilidad a través de máquinas* – una aplicación y todas las dependencias que pueden vincularse en un contenedor individual, independiente de la versión de host del kernel de Linux, distribución de plataforma o modelo de desarrollo. Este contenedor puede transferirse a otra máquina que ejecute Docker, y ejecutarse allí sin problemas de compatibilidad.

- *Control de versión y reutilización de componentes* – puede rastrear versiones sucesivas de un contenedor, inspeccionar diferencias o recuperar versiones anteriores. Los contenedores reutilizan componentes de las capas precedentes, lo cual las hace notablemente más livianas.
- *Compartir* – puede usar un repositorio remoto para compartir su contenedor. Red Hat proporciona un registro para este propósito y también es posible configurar su propio repositorio privado.
- *Huella liviana y gasto mínimo* – Las imágenes Docker suelen ser muy pequeñas, lo cual facilita la entrega rápida y reduce el tiempo de implementación de los nuevos contenedores de aplicaciones.
- *Mantenimiento simplificado* – Docker reduce esfuerzo y riesgo de problemas con dependencias de aplicaciones.

11.3. Comparación con máquinas virtuales

Virtual machines represent an entire server with all of the associated software and maintenance concerns. Containers provide application isolation and can be configured with minimum run-time environments. In a container, the kernel and parts of the operating system infrastructure are shared. For the virtual machine, a full operating system must be included.

- Puede crear o destruir contenedores de forma rápida y fácil. Las máquinas virtuales requieren instalaciones completas y más recursos de computación para ejecutarse.
- Los contenedores son livianos, por lo tanto, se pueden ejecutar más contenedores que máquinas virtuales en una máquina host.
- Los contenedores comparten recursos de forma eficiente. Las máquinas virtuales están aisladas. Por lo tanto, también pueden ser bastante livianas múltiples variaciones de una aplicación que se ejecuten en contenedores. Por ejemplo, los binarios compartidos no se duplican en el sistema.
- Las máquinas virtuales pueden migrarse cuando aún están en ejecución, sin embargo los contenedores no pueden migrarse cuando se estén ejecutando y deben detenerse antes de pasar de una máquina host a otra máquina host.

Los contenedores no reemplazan las máquinas virtuales para todos los casos de uso. Se requiere una evaluación meticulosa para determinar qué es el mejor para su aplicación.

To quickly get up-and-running with docker formatted containers, refer to [Get Started with docker Formatted Containers](#).

More information about Linux Containers, the Docker project, subscriptions and support can be found in this [FAQ](#).

11.4. Using Containers on Red Hat Enterprise Linux 7.1

Packages containing **docker**, **kubernetes**, and registry software have been released as part of the Extras channel in Red Hat Enterprise Linux. Once the Extras channel has been enabled, the packages can be installed in the usual way. For more information on installing packages or enabling channels, see the [System Administrator's Guide](#).

Red Hat provides a registry of platform container images and Red Hat Atomic Container Images. This registry provides base images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 and pre-built solutions usable on Red Hat Enterprise Linux 7.1 with Docker. For more information about the registry and a list of available packages, see [Container Images](#).

11.5. Containers with the LXC Format Have Been Deprecated

The following LXC packages, which contain Linux resource containers, are deprecated starting with Red Hat Enterprise Linux 7.1:

- ✦ `libvirt-daemon-driver-lxc`
- ✦ `libvirt-daemon-lxc`
- ✦ `libvirt-login-shell`

The Linux container functionality is now focused on the docker management interface (docker command-line interface). Please note: It is possible that the listed LXC packages will not be shipped with future releases of Red Hat Enterprise Linux, as they may be considered for formal removal.

Capítulo 12. Autenticación e interoperatividad

Manual Backup and Restore Functionality

This update introduces the **ipa-backup** and **ipa-restore** commands to Identity Management (IdM), which allow users to manually back up their IdM data and restore them in case of a hardware failure. For further information, see the [ipa-backup\(1\)](#) and [ipa-restore\(1\)](#) manual pages or the documentation in the [Linux Domain Identity, Authentication, and Policy Guide](#).

Soporte para migración de WinSync a Trust

This update implements the new **ID Views** mechanism of user configuration. It enables the migration of Identity Management users from a **WinSync** synchronization-based architecture used by **Active Directory** to an infrastructure based on Cross-Realm Trusts. For the details of **ID Views** and the migration procedure, see the documentation in the [Windows Integration Guide](#).

One-Time Password Authentication

One of the best ways to increase authentication security is to require two factor authentication (2FA). A very popular option is to use one-time passwords (OTP). This technique began in the proprietary space, but over time some open standards emerged (HOTP: RFC 4226, TOTP: RFC 6238). Identity Management in Red Hat Enterprise Linux 7.1 contains the first implementation of the standard OTP mechanism. For further details, see the documentation in the [System-Level Authentication Guide](#).

Integración SSSD para Sistema de archivos comunes de Internet

A plug-in interface provided by **SSSD** has been added to configure the way in which the **cifs-utils** utility conducts the ID-mapping process. As a result, an **SSSD** client can now access a CIFS share with the same functionality as a client running the **Winbind** service. For further information, see the documentation in the [Windows Integration Guide](#).

Certificar herramienta de administración de autoridad

The **ipa-cacert-manage renew** command has been added to the Identity management (IdM) client, which makes it possible to renew the IdM Certification Authority (CA) file. This enables users to smoothly install and set up IdM using a certificate signed by an external CA. For details on this feature, see the [ipa-cacert-manage\(1\)](#) manual page.

Aumentó granularidad de control de acceso

It is now possible to regulate read permissions of specific sections in the Identity Management (IdM) server UI. This allows IdM server administrators to limit the accessibility of privileged content only to chosen users. In addition, authenticated users of the IdM server no longer have read permissions to all of its contents by default. These changes improve the overall security of the IdM server data.

Acceso de dominio limitado para usuarios no privilegiados

The **domains=** option has been added to the **pam_sss** module, which overrides the **domains=** option in the **/etc/sss/sss.conf** file. In addition, this update adds the **pam_trusted_users** option, which allows the user to add a list of numerical UIDs or user names that are trusted by the **SSSD** daemon, and the **pam_public_domains** option and a list of domains accessible even for untrusted users. The mentioned

additions allow the configuration of systems, where regular users are allowed to access the specified applications, but do not have login rights on the system itself. For additional information on this feature, see the documentation in the [Linux Domain Identity, Authentication, and Policy Guide](#).

Configuración de proveedor de datos automático

El comando **ipa-client-install** ahora configura **SSSD** como proveedor de datos para el servicio sudo. Esta conducta puede ser inhabilitada con la opción **--no-sudo**. Además, la opción **--nisdomain** ha sido agregada para especificar el nombre de dominio NIS para la instalación del cliente de administración de identidad, y la opción **--no_nisdomain** ha sido agregada para establecer el nombre de dominio NIS. Si ninguna de estas opciones es utilizada, el dominio IPA se utiliza en su lugar.

Uso de proveedores sudo de AD y LDAP

El proveedor AD es un segundo plano utilizado para conectar a un servidor de directorio activo. En Red Hat Enterprise Linux 7.1, el uso del proveedor sudo AD junto con el proveedor LDAP recibe soporte como una Muestra previa de tecnología. Para habilitar el proveedor sudo AD, agregue el parámetro **sudo_provider=ad** en la sección de dominio del archivo **sssd.conf**.

32-bit Version of krb5-server and krb5-server-ldap Deprecated

The 32-bit version of **Kerberos 5 Server** is no longer distributed, and the following packages are deprecated starting with Red Hat Enterprise Linux 7.1: *krb5-server.i686*, *krb5-server.s390*, *krb5-server.ppc*, *krb5-server-ldap.i686*, *krb5-server-ldap.s390*, and *krb5-server-ldap.ppc*. There is no need to distribute the 32-bit version of *krb5-server* on Red Hat Enterprise Linux 7, which is supported only on the following architectures: AMD64 and Intel 64 systems (**x86_64**), 64-bit IBM Power Systems servers (**ppc64**), and IBM System z (**s390x**).

Capítulo 13. Seguridad

Guía de seguridad SCAP

El paquete *scap-security-guide* se ha incluido en Red Hat Enterprise Linux 7.1 para brindar orientación sobre seguridad, bases y mecanismos de validación asociados con mecanismos de validación. La orientación se especifica en *Security Content Automation Protocol* (SCAP por sus siglas en inglés), el cual constituye un catálogo de consejos prácticos de endurecimiento. **SCAP Security Guide** contiene los datos necesarios para realizar un escaneo del cumplimiento de la seguridad del sistema con relación a los requerimientos de la política de seguridad prescritos; se incluyen una descripción escrita y una prueba automatizada (sondeo). Al automatizar la prueba, **SCAP Security Guide** ofrece una forma conveniente y fiable para verificar con regularidad el cumplimiento del sistema.

The Red Hat Enterprise Linux 7.1 version of the **SCAP Security Guide** includes the *Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)*, which can be used for compliance scans of Red Hat Enterprise Linux Server 7.1 cloud systems.

Also, the Red Hat Enterprise Linux 7.1 *scap-security-guide* package contains SCAP datastream content format files for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7, so that remote compliance scanning of both of these products is possible.

The Red Hat Enterprise Linux 7.1 system administrator can use the **oscap** command line tool from the *openscap-scanner* package to verify that the system conforms to the provided guidelines. See the *scap-security-guide(8)* manual page for further information.

Política SELinux

En Red Hat Enterprise Linux 7.1, la política SELinux ha sido modificada; los servicios sin su propia política SELinux que anteriormente se ejecutaban en el dominio **init_t** ahora se ejecutan en el dominio recién agregado **unconfined_service_t**. Consulte [Procesos no confinados](#) en [Guía del administrador y usuario SELinux](#) para Red Hat Enterprise Linux 7.1.

Nuevas funcionalidades en OpenSSH

El conjunto de herramientas **OpenSSH** ha sido actualizado a la versión 6.6.1p1, la cual agrega varias funcionalidades relacionadas con la criptografía:

- El intercambio de llave mediante curva elíptica **Diffie-Hellman** en **Curve25519** de Daniel Bernstein no recibe soporte. Este método ahora es el predeterminado tanto el servidor como el cliente lo soportan.
- Se agregó soporte para el uso del esquema de firma de curva elíptica **Ed25519** como un tipo de llave pública. **Ed25519**, el cual puede utilizarse para llaves de usuario y de host, ofrece más seguridad y rendimiento que **ECDSA** y **DSA**.
- Se ha agregado un nuevo formato de llave que utiliza la función de derivación de claves **bcrypt** (KDF). Este formato es el predeterminado para llaves **Ed25519**, pero también puede solicitarse para otros tipos de llaves.
- Se agregó una nueva cifra de transporte, **chacha20-poly1305@openssh.com**. Combina la cifra de corriente de Daniel Bernstein **ChaCha20** con el código de autenticación del mensaje **Poly1305** (MAC).

Nuevas funcionalidades en Libreswan

La implementación de **Libreswan** de VPN IPsec, ha sido actualizada a la versión 3.12, la cual añade varias funcionalidades y mejoras:

- ✦ Se agregaron nuevas cifras.
- ✦ **IKEv2** support has been improved.
- ✦ Se agregó soporte de cadena de certificados intermediarios en **IKEv1** e **IKEv2**.
- ✦ Se mejoró el manejo de conexión
- ✦ Se mejoró la interoperabilidad con sistemas OpenBSD, Cisco, y Android.
- ✦ Se mejoró el soporte para **systemd**.
- ✦ Se agregó soporte para **CERTREQ** en hash y estadísticas de tráfico.

Nuevas funcionalidades en TNC

The Trusted Network Connect (TNC) Architecture, provided by the *strongimcv* package, has been updated and is now based on **strongSwan 5.2.0**. The following new features and improvements have been added to the TNC:

- ✦ The **PT-EAP** transport protocol ([RFC 7171](#)) for Trusted Network Connect has been added.
- ✦ The Attestation *Integrity Measurement Collector* (IMC)/*Integrity Measurement Verifier* (IMV) pair now supports the IMA-NG measurement format.
- ✦ Se mejoró el soporte de atestación IMV al implementar un nuevo ítem de trabajo TPMRA.
- ✦ Se agregó soporte para JSON-based REST API con SWID IMV.
- ✦ The SWID IMC can now extract all installed packages from the **dpkg**, **rpm**, or **pacman** package managers using the [swidGenerator](#), which generates SWID tags according to the new ISO/IEC 19770-2:2014 standard.
- ✦ The **libtls TLS 1.2** implementation as used by **EAP-(T)TLS** and other protocols has been extended by AEAD mode support, currently limited to **AES-GCM**.
- ✦ Improved (IMV) support for sharing access requestor ID, device ID, and product information of an access requestor via a common **imv_session** object.
- ✦ Varios errores han sido corregidos en los protocolos existentes: **IF-TNCCS (PB-TNC, IF-M (PA-TNC))** y en el par: **OS IMC/IMV**.

Nuevas funcionalidades en GnuTLS

La implementación **GnuTLS** de los protocolos **SSL**, **TLS**, y **DTLS**, ha sido actualizada a la versión 3.3.8, la cual ofrece una cantidad de funcionalidades y mejoras.

- ✦ Se ha agregado soporte para **DTLS 1.2**.
- ✦ Se ha agregado soporte para *Negociación de protocolo de capas de aplicación* (ALPN).
- ✦ El rendimiento de paquetes de cifras de curva elíptica ha sido mejorado.
- ✦ Se han agregado paquetes de nuevas cifras, **RSA-PSK** y **CAMELLIA-GCM**.
- ✦ Se ha agregado soporte nativo para el estándar de *Módulo de plataforma confiable* (TPM).
- ✦ Se ha mejorado en varias formas el soporte para tarjetas inteligentes **PKCS#11** y *módulos de seguridad de hardware* (HSM).

- ✦ Ha sido mejorado en varias formas el cumplimiento con los estándares de seguridad *FIPS 140* (*Estándares de procesamiento de información federal*).

Capítulo 14. Escritorio

Soporte para visuales estéreo Quad-buffered OpenGL

GNOME Shell y el gestor de composición de ventanas **Mutter** ahora le permite usar visuales estéreo quad-buffered OpenGL en hardware que recibe soporte. Debe tener NVIDIA Display Driver, versión 337 o posterior instalada para poder usar adecuadamente esta funcionalidad.

Proveedores de cuenta en línea

Ha sido agregada una nueva llave **GSettings org.gnome.online-accounts.whitelisted-providers** a **GNOME Online Accounts** (proporcionado por el paquete *gnome-online-accounts*). Dicha llave ofrece una lista de proveedores en línea que tienen permiso explícito para ser cargados en el inicio. Al especificar esta llave, los administradores de sistemas pueden activar proveedores apropiados o desactivar de forma selectiva a otros.

Capítulo 15. Mantenimiento y Soporte

Micro reporte autorizado ABRT

In Red Hat Enterprise Linux 7.1, the **Automatic Bug Reporting Tool (ABRT)** receives tighter integration with the Red Hat Customer Portal and is capable of directly sending micro-reports to the Portal. **ABRT** provides a utility, **abrt-auto-reporting**, to easily configure user's Portal credentials necessary to authorize micro-reports.

The integrated authorization allows **ABRT** to reply to a micro-report with a rich text which may include possible steps to fix the cause of the micro-report. For example, **ABRT** can suggest which packages are supposed to be upgraded or offer Knowledge base articles related to the issue.

Consulte el Portal del cliente [para obtener más información sobre esta funcionalidad](#).

Capítulo 16. Colecciones de software de Red Hat

Red Hat Software Collections es un conjunto de contenido de Red Hat de programación de lenguajes dinámicos, servidores de bases de datos y paquetes relacionados que puede instalar y usar en todos los lanzamientos que tienen soporte de Red Hat Enterprise Linux 6 y Red Hat Enterprise Linux 7 en arquitecturas AMD64 e Intel 64.

Los lenguajes dinámicos, servidores de bases de datos y otras herramientas que se distribuyen con Red Hat Software Collections no reemplazan las herramientas del sistema predeterminado provistas por Red Hat Enterprise Linux, ni se utilizan como preferenciales.

Red Hat Software Collections usa un mecanismo de empaquetamiento alternativo basado en la herramienta **sc1** para proveer un conjunto paralelo de paquetes. Este conjunto habilita el uso de versiones de paquetes alternativos en Red Hat Enterprise Linux. Al usar la herramienta **sc1**, los usuarios pueden elegir la versión del paquete en cualquier momento en el que deseen ejecutarla.



Importante

Red Hat Software Collections tiene un ciclo de vida y un término de soporte más corto que Red Hat Enterprise Linux. Para obtener más información, consulte [Red Hat Software Collections Product Life Cycle](#).

Ahora, Red Hat Developer Toolset hace parte de Red Hat Software Collections, incluidas como un Software Collection individual. Red Hat Developer Toolset está diseñado para que los desarrolladores trabajen en la plataforma de Red Hat Enterprise Linux. Proporciona las versiones actuales de GNU Compiler Collection, GNU Debugger, la plataforma de desarrollo Eclipse, y otras herramientas de desarrollo, depuración y monitorización de rendimiento.

Consulte [Red Hat Software Collections documentation](#) para información sobre componentes incluidos en el conjunto, requerimientos del sistema, problemas conocidos, el uso y las especificaciones de Software Collections individuales.

Consulte [Red Hat Developer Toolset documentation](#) para obtener más información sobre componentes incluidos en este Software Collection, uso de instalación y problemas conocidos.

Capítulo 17. Red Hat Enterprise Linux for Real Time

Red Hat Enterprise Linux for Real Time is a new offering in Red Hat Enterprise Linux 7.1 comprised of a special kernel build and several user space utilities. With this kernel and appropriate system configuration, Red Hat Enterprise Linux for Real Time brings deterministic workloads, which allow users to rely on consistent response times and low and predictable latency. These capabilities are critical in strategic industries such as financial service marketplaces, telecommunications, or medical research.

For instructions on how to install Red Hat Enterprise Linux for Real Time, and how to set up and tune the system so that you can take full advantage of this offering, refer to the [Red Hat Enterprise Linux for Real Time 7 Installation Guide](#).

Parte II. Controladores de dispositivo

Este capítulo proporciona un listado completo de todos los controladores que fueron actualizados en Red Hat Enterprise Linux 7.1.

Capítulo 18. Actualizaciones de controlador de almacenamiento

- El controlador **hpsa** ha sido promovido a la versión 3.4.4-1-RH1.
- El controlador **qla2xxx** ha sido promovido a la versión 8.07.00.08.07.1-k1.
- The **qla4xxx** driver has been upgraded to version 5.04.00.04.07.01-k0.
- El controlador **qlcnic** ha sido promovido a la versión 5.3.61.
- El controlador **netxen_nic** ha sido promovido a la versión 4.0.82.
- El controlador **qlge** ha sido promovido a la versión 1.00.00.34.
- El controlador **bnx2fc** ha sido actualizado a la versión 2.4.2.
- El controlador **bnx2i** ha sido promovido a la versión 2.7.10.1.
- El controlador **cnic** ha sido promovido a la versión 2.5.20.
- El controlador **bnx2x** ha sido promovido a la versión 1.710.51-0.
- El controlador **bnx2** ha sido promovido a la versión 2.2.5.
- El controlador **megaraid_sas** ha sido promovido a la versión 06.805.06.01-rc1.
- El controlador **mpt2sas** ha sido promovido a la versión 18.100.00.00.
- El controlador **ipr** ha sido promovido a la versión 2.6.0.
- Los paquetes *kmod-lpfc* han sido agregados a Red Hat Enterprise Linux 7, el cual garantiza mayor estabilidad al usar el controlador lpfc con Canal de fibra (FC) Y Canal de fibra por adaptadores Ethernet (FCoE). El controlador **lpfc** ha sido promovido a la versión 0:10.2.8021.1.
- El controlador **be2iscsi** ha sido promovido a la versión 10.4.74.0r.
- El controlador **nvme** ha sido promovido a la versión 0.9.

Capítulo 19. Actualizaciones de controladores de red

- El controlador **bn**a ha sido promovido a la versión 3.2.23.0r.
- El controlador **cxgb3** ha sido promovido a la versión 1.1.5-ko.
- El controlador **cxgb3i** ha sido promovido a la versión 2.0.0.
- El controlador **iw_cxgb3** ha sido promovido a la versión 1.1.
- El controlador **cxgb4** ha sido promovido a la versión 2.0.0-ko.
- El controlador **cxgb4vf** ha sido promovido a la versión 2.0.0-ko.
- El controlador **cxgb4i** ha sido promovido a la versión 0.9.4.
- El controlador **iw_cxgb4** ha sido promovido a la versión 0.1.
- El controlador **e1000e** ha sido promovido a la versión 2.3.2-k.
- El controlador **igb** ha sido promovido a la versión 5.2.13-k.
- El controlador **igbvf** ha sido promovido a la versión 2.0.2-k.
- El controlador **ixgbe** ha sido promovido a la versión 3.19.1-k.
- El controlador **ixgbev**f ha sido promovido a la versión 2.12.1-k.
- El controlador **i40e** ha sido promovido a la versión 1.0.11-k.
- El controlador **i40ev**f ha sido promovido a la versión 1.0.1.
- El controlador **e1000** ha sido promovido a la versión 7.3.21-k8-NAPI.
- El controlador **m1x4_en** ha sido promovido a la versión 2.2-1.
- El controlador **m1x4_ib** ha sido promovido a la versión 2.2-1.
- El controlador **m1x5_core** ha sido promovido a la versión 2.2-1.
- El controlador **m1x5_ib** ha sido promovido a la versión 2.2-1.
- El controlador **ocrdma** ha sido promovido a la versión 10.2.287.0u.
- El controlador **ib_ipoib** ha sido promovido a la versión 1.0.0.
- El controlador **ib_qib** ha sido promovido a la versión 1.11.
- El controlador **enic** ha sido promovido a la versión 2.1.1.67.
- El controlador **be2net** ha sido promovido a la versión 10.4r.
- El controlador **tg3** ha sido promovido a la versión 3.137.
- El controlador **r8169** ha sido promovido a la versión 2.3LK-NAPI.

Capítulo 20. Actualización de controladores gráficos

- ✦ El controlador **vmwgfx** ha sido promovido a la versión 2.6.0.0.

Parte III. Known Issues

This part describes known issues in Red Hat Enterprise Linux 7.1.

Capítulo 21. Installation and Booting

anaconda component, BZ#1067868

Under certain circumstances, when installing the system from the boot DVD or ISO image, not all assigned IP addresses are shown in the network spoke once network connectivity is configured and enabled. To work around this problem, leave the network spoke and enter it again. After re-entering, all assigned addresses are shown correctly.

Capítulo 22. Networking

rsync component, [BZ#1082496](#)

The **rsync** utility cannot be run as a socket-activated service because the **rsyncd@.service** file is missing from the *rsync* package. Consequently, the **systemctl start rsyncd.socket** command does not work. However, running **rsync** as a daemon by executing the **systemctl start rsyncd.service** command works as expected.

Capítulo 23. Authentication and Interoperability

bind-dyndb-ldap component, [BZ#1139776](#)

The latest version of the **bind-dyndb-ldap** system plug-in offers significant improvements over the previous versions, but currently has some limitations. One of the limitations is missing support for the LDAP rename (MODRDN) operation. As a consequence, DNS records renamed in LDAP are not served correctly. To work around this problem, restart the **named** daemon to resynchronize data after each MODRDN operation. In an Identity Management (IdM) cluster, restart the **named** daemon on all IdM replicas.

ipa component, [BZ#1186352](#)

When you restore an Identity Management (IdM) server from backup and re-initialize the restored data to other replicas, the Schema Compatibility plug-in can still maintain a cache of the old data from before performing the restore and re-initialization. Consequently, the replicas might behave unexpectedly. For example, if you attempt to add a user that was originally added after performing the backup, and thus removed during the restore and re-initialization steps, the operation might fail with an error, because the Schema Compatibility cache contains a conflicting user entry. To work around this problem, restart the IdM replicas after re-initializing them from the master server. This clears the Schema Compatibility cache and ensures that the replicas behave as expected in the described situation.

ipa component, [BZ#1188195](#)

Both anonymous and authenticated users lose the default permission to read the **facsimiletelephonenumber** user attribute after upgrading to the Red Hat Enterprise Linux 7.1 version of Identity Management (IdM). To manually change the new default setting and make the attribute readable again, run the following command:

```
ipa permission-mod 'System: Read User Addressbook Attributes' --  
includedattrs facsimiletelephonenumber
```

Capítulo 24. Desktop

gobject-introspection component, [BZ#1076414](#)

The **gobject-introspection** library is not available in a 32-bit multilib package. Users who wish to compile 32-bit applications that rely on GObject introspection or libraries that use it, such as **GTK+** or **GLib**, should use the *mock* package to set up a build environment for their applications.

Apéndice A. Historia de revisiones

Revisión 1.0-9.3	Wed Jan 29 2015	Gladys Guerrero Lozano
-------------------------	------------------------	-------------------------------

Archivos de traducción sincronizados con fuentes XML sources 1.0-9

Revisión 1.0-9	Wed Jan 14 2015	Milan Navrátil
-----------------------	------------------------	-----------------------

Publicación de las Notas de lanzamiento de Red Hat Enterprise Linux 7.1.

Revisión 1.0-8	Thu Dec 15 2014	Jiří Herrmann
-----------------------	------------------------	----------------------

Publicación de las Notas de lanzamiento Beta de Red Hat Enterprise Linux 7.1.