



Red Hat Enterprise Linux 6

Notas de lanzamiento 6.4

Notas de lanzamiento para Red Hat Enterprise Linux 6.4

Edición 4

Red Hat Enterprise Linux 6 Notas de lanzamiento 6.4

Notas de lanzamiento para Red Hat Enterprise Linux 6.4

Edición 4

Landmann

rlandmann@redhat.com

Legal Notice

Copyright © 2012 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 proporcionan un alto nivel de cubrimiento de las mejoras y adiciones que han sido implementadas en Red Hat Enterprise Linux 6.4. Para obtener una documentación detallada sobre todos los cambios a Red Hat Enterprise Linux para la actualización 6.4 consulte Notas técnicas.

Table of Contents

PREFACIO	4
CAPÍTULO 1. INSTALACIÓN	5
Soporte FCoE en el archivo Kickstart	5
Instalación mediante VLAN	5
Cómo configurar la vinculación	5
CAPÍTULO 2. KERNEL	6
Protocolo de canal de fibra: Revisión de consistencia de extremo a extremo	6
Soporte Flash Express para sistema Z de IBM	6
Módulo de kernel Open vSwitch	6
Comparación de sistema de arranque y sistema de vaciado	6
Herramienta Perf actualizada	6
Soporte Uncore PMU	6
Se reduce el consumo de memoria memcg	7
Recuperación de memoria y compactación	7
Soporte de funcionalidad de ejecución transaccional y funcionalidad de instrumentación de tiempo de ejecución	7
Modo de falla abierta	7
kdump y el mecanismo de volcado de kernel kexec para System z de IBM totalmente soportado	7
Plazo TSC para soporte KVM	7
Nombre de dispositivos persistentes	7
Nuevo paquete linuxptp	8
Documentación de Hugepages transparentes	8
Estado de soporte para destinos de volcado	8
CAPÍTULO 3. CONTROLADORES DE DISPOSITIVO	9
Controladores de almacenamiento	9
Controladores de red	10
Controladores varios	11
CAPÍTULO 4. RED	13
HAProxy	13
CAPÍTULO 5. AUTENTICACIÓN E INTEROPERABILIDAD	14
Funcionalidades SSSD totalmente soportadas	14
Nuevo tipo de almacenamiento cache SSSD	14
Adición de dominios AD a grupos externos	14
Certificados de subsistema de manejo de auto-renovación de identidad	14
Configuración automática de herramientas de cliente OpenLDAP en clientes matriculados en Administración de identidad	14
Soporte PKCS#12 para python-nss	14
Búsqueda total persistente para DNS	15
Nueva operación CLEANALLRUV	15
Bibliotecas actualizadas de samba4	15
Cruce de funcionalidad de confianza de dominio de kerberos en manejo de identidad	16
Soporte de esquema Posix para servidor de directorio 389	16
CAPÍTULO 6. SEGURIDAD	18
Cómo tratar las coincidencias de modo autoritario en las búsquedas y entradas de sudo	18
Revisiones adicionales de contraseña para pam_cracklib	18
Opción de tamaño para polinstanciación de tmpfs	18
Bloqueo de cuentas inactivas	18

Nuevos modos de funcionar para libica	18
Optimización y soporte para la biblioteca de compresión zlib de System z	19
Configuración de cortafuegos de reserva	19
CAPÍTULO 7. DERECHOS	20
Actualizaciones de cadenas	20
Prueba de conexión de Proxy	20
Suscribir o cancelar los derechos múltiples	20
Soporte para llaves de activación en GUI	20
Registro con otros servidores externos	20
Cambios de uso en la Interfaz Gráfica de usuario (GUI)	20
CAPÍTULO 8. VIRTUALIZACIÓN	21
8.1. KVM	21
virtio-SCSI	21
Soporte para el procesador Intel core de siguiente generación	21
Soporte para CPU series 4xxx AMD Opteron	21
Migración de huéspedes en vivo mediante reenvío de USB vía SPICE	21
Migración de huéspedes en vivo mediante dispositivos USB	21
Agente de huéspedes QEMU actualizado	22
Indicación de fin de interrupción paravirtualizada (PV-EOI)	22
Paso de sonido configurable	22
8.2. HYPER-V	22
Inclusión y soporte de instalación de huésped para controladores Hyper-V-D de Microsoft	22
8.3. VMWARE ESX	23
Controladores PV VMware	23
CAPÍTULO 9. AGRUPAMIENTO	24
Soporte para el dispositivo de vallas IPDU de IBM	24
Soporte para Dispositivo de valla de controlador de energía de red Eaton	24
Nuevo paquete keepalived	24
Recuperación de Watchdog	24
Soporte para almacenaje basado en VMDK	24
CAPÍTULO 10. ALMACENAJE	25
Paralelo NFS totalmente soportado	25
Soporte de descarte en línea XFS	25
Soporte LVM para Micron PCIe SSD	25
Soporte LVM para Espejo RAID10 de dos vías	25
Configurar y administrar las reservas SCSI persistentes a través de mecanismos mapeadores de dispositivos	25
CAPÍTULO 11. COMPILADOR Y HERRAMIENTAS	26
SystemTap actualizado a la versión 1.8	26
Herramientas lscpu y hcpcu	26
CAPÍTULO 12. ACTUALIZACIONES GENERALES	27
Han sido actualizados los paquetes de samba	27
Nuevo paquete SciPy	27
Soporte TLS v1.1 en NSS	27
Valgrind incorporado de gdbserver	28
Nuevos paquetes libjpeg-turbo	28
Nuevo paquete redhat-lsb-core	28
Ha sido actualizada la herramienta createrepo	28

APÉNDICE A. REVISION HISTORY **29**

PREFACIO

Los lanzamientos menores de Red Hat Enterprise Linux son una adición a las mejoras individuales, seguridad y corrección de erratas. Las *Notas de lanzamiento de Red Hat Enterprise Linux 6.4* documentan los cambios principales del sistema operativo de Red Hat Enterprise Linux 6 y las aplicaciones que lo acompañan para este lanzamiento menor. Notas detalladas sobre cambios (es decir, corrección de errores, mejoras agregadas, y problemas conocidos hallados) en este lanzamiento menor están disponibles en las [Notas técnicas](#). El documento de las Notas técnicas también contiene una lista completa de todas las Muestras de tecnología disponibles actualmente con los paquetes que las proveen.



IMPORTANTE

Las *Notas de lanzamiento Red Hat Enterprise Linux 6.4* localizadas en [aquí](#), deben considerarse como la versión actualizada definitiva. Se recomienda que los usuarios que tengan preguntas sobre el lanzamiento, consulten en línea el *Lanzamiento* y las *Notas técnicas* para su versión de Red Hat Enterprise Linux.

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

CAPÍTULO 1. INSTALACIÓN

Soporte FCoE en el archivo Kickstart

Al usar un archivo kickstart para instalar Red Hat Enterprise Linux 6.4 con la nueva opción *fcoe* de Kickstart, usted puede especificar qué dispositivos de Canal de fibra por Ethernet (FCoE) deben activarse de forma automática además de los que hayan sido descubiertos por los servicios de Unidad de disco mejorado (EDD). Para obtener mayor información, consulte la sección *Opciones Kickstart* en la *Guía de instalación* de Red Hat Enterprise 6.

Instalación mediante VLAN

En Red Hat Enterprise Linux 6.4, la opción de arranque `vlanid=` y la opción Kickstart `--vlanid=` le permiten establecer un ID LAN virtual (etiqueta 802.1q) para un dispositivo de red específico. Al especificar alguna de estas opciones, la instalación del sistema puede realizarse a través de una VLAN.

Cómo configurar la vinculación

La opción de arranque `bond` y las opciones Kickstart `--bondslaves` y `--bondopts` ahora pueden configurar la vinculación como parte del proceso de instalación. Para obtener mayor información sobre cómo configurar la vinculación, consulte las siguientes partes de la *Guía de instalación* de Red Hat Enterprise Linux 6: sección *Opciones Kickstart* y capítulo *Opciones de arranque*

CAPÍTULO 2. KERNEL

Protocolo de canal de fibra: Revisión de consistencia de extremo a extremo

La integridad de datos entre un adaptador de host y el servidor de almacenaje ha sido mejorada en Red Hat Enterprise Linux 6.4 con la implementación de la parte específica zFCP del estándar mejorado T10 DIF SCSI para consistencia de revisión de datos de extremo a extremo (E2E).

Soporte Flash Express para sistema Z de IBM

La Memoria de almacenamiento de clase (SCM) para System z de IBM es una clase de dispositivos de almacenaje de datos que combinan propiedades tanto de almacenamiento como de memoria. La SCM para System z ahora soporta memoria Flash Express. El incremento de la SCM se puede acceder a través de los subcanales del motor de datos asíncronos extendidos (EADM). Cada incremento está representado por un dispositivo de bloque. Esta funcionalidad mejora la tasa de rastreo y el rendimiento de acceso para un almacenamiento temporal, por ejemplo, para depósito de datos.

Módulo de kernel Open vSwitch

Red Hat Enterprise Linux 6.4 incluye el módulo de kernel Open vSwitch como un habilitador para las ofertas de productos en capa de Red Hat. Open vSwitch está soportado únicamente junto con esos productos que contienen las herramientas de espacio de usuario acompañantes. Por favor observe que sin las herramientas de espacio de usuario requeridas, Open vSwitch no funcionará y no podrá habilitarse para su uso. Para obtener mayor información, por favor consulte el siguiente artículo de la Base del conocimientos: <https://access.redhat.com/knowledge/articles/270223>.

Comparación de sistema de arranque y sistema de vaciado

Esta funcionalidad le permite comparar un sistema iniciado con un sistema abandonado para analizar de modo eficiente los cambios que puedan presentarse en la migración de imágenes. Para identificar un huésped, se utilizan los datos `stsi stfle`. La nueva función, `lgr_info_log()` compara los datos actuales (`lgr_info_cur`) con los últimos registrados (`lgr_info_last`).

Herramienta Perf actualizada

La herramienta `perf` ha sido actualizada a la versión 3.6-rc7 de la línea principal de desarrollo, la cual proporciona una gran número de correcciones de errores y mejoras. Las siguientes son las mejoras más importantes:

- Fue añadido soporte de eventos Kprobe
- Se ha incluido un nuevo motor de eventos de sintaxis de la línea de comandos `perf`, el cual permite usar los paréntesis curvos (`{` y `}`) para definir grupos de eventos, por ejemplo: `{cycles, cache-misses}`.
- El navegador `perf` ha sido mejorado para permitir la navegación mediante llamadas y saltos ASM.
- La herramienta `perf` ha sido actualizada para proporcionar una vista por usuario con la nueva opción de línea de comandos `--uid`. Cuando se utiliza, `perf` aparecen las tareas para el usuario especificado únicamente.
- La herramienta `perf` ahora proporciona una amplia variedad de pruebas automatizadas.

Soporte Uncore PMU

El kernel distribuido con Red Hat Enterprise Linux 6.4 añade el soporte "uncore" de la Unidad de monitorización de rendimiento (PMU) al subsistema de eventos Perf para la familia de procesadores Intel Xeon X55xx e Intel Xeon X56xx. El soporte "uncore" se refiere a subsistemas en paquetes de

procesadores físicos que se comparten mediante múltiples núcleos de procesadores, por ejemplo, la memoria cache L3. Con el soporte Uncore PMU, se pueden recolectar fácilmente datos de rendimiento en el nivel de paquetes.

La lectura de eventos PMU ha sido habilitada para permitir la depuración vía perf.

Se reduce el consumo de memoria memcg

Los grupos de control de memoria mantienen su propia Lista Menos usada recientemente (LRU), por ejemplo, recuperar memoria. Esta lista estaba en lo alto de la lista global LRU por zonas. En Red Hat Enterprise Linux 6.4, el consumo de memoria para memcg se redujo al inhabilitar la lista global LRU por zonas y convertir sus usuarios para que operen en las listas cgroup por memoria.

Recuperación de memoria y compactación

El kernel distribuido con Red Hat Enterprise Linux 6.4 emplea solicitudes de recuperación y compactación para asignación de alto orden o presión de memoria.

Soporte de funcionalidad de ejecución transaccional y funcionalidad de instrumentación de tiempo de ejecución

El soporte de la funcionalidad de ejecución transaccional (disponible en zEnterprise EC12 de IBM) en el kernel de Linux ayuda a eliminar la sobrecarga de software que puede impactar el rendimiento y ofrecer un aumento de escalabilidad y paralelismo para obtener un rendimiento de transacción superior. El soporte de la funcionalidad de instrumentación del tiempo de ejecución (disponible en zEnterprise EC12 de IBM) proporciona un mecanismo avanzado para perfilar el código de programación a fin de obtener un análisis mejorado y optimización del código generado por JVM de IBM.

Modo de falla abierta

Red Hat Enterprise Linux 6.4 añade soporte al nuevo modo de falla abierta al usar el destino NFQUEUE de Netfilter. Este modo le permite al usuario inhabilitar temporalmente la inspección del paquete y mantener la conectividad en un alto tráfico de red.

kdump y el mecanismo de volcado de kernel kexec para System z de IBM totalmente soportado

En Red Hat Enterprise Linux 6.4, el mecanismo de volcado de kernel kdump/kexec está habilitado para sistemas System z de IBM como una funcionalidad totalmente soportada, además de System z autónomo de IBM y del mecanismo de volcado del hipervisor. El umbral de autoreserva se establece a 4 GB; por lo tanto, ningún sistema z system de IBM con más de 4 GB de memoria tiene activado el mecanismo kdump/kexec.

Debe haber disponible suficiente memoria porque kdump reserva de forma predeterminada aproximadamente 128 MB. Esto es en especial importante al realizar una actualización a Red Hat Enterprise Linux 6.4. Se debe tener suficiente espacio disponible para almacenar el vaciado en caso de algún daño.

Puede configurar o desactivar kdump a través de `/etc/kdump.conf`, `system-config-kdump`, o `firstboot`.

Plazo TSC para soporte KVM

El temporizador de plazo TSC es un nuevo modo en el temporizador local APIC (LAPIC), el cual genera un temporizador de interrupciones de una toma basadas en el plazo TSC, en lugar del conteo de intervalos de reloj APIC. Proporciona interrupciones de temporizador más precisas (menos de 1 tic) para beneficiar al programador de SO. Ahora KVM expone esta funcionalidad a huéspedes.

Nombre de dispositivos persistentes

Esta funcionalidad almacena el mapeo de nombres de dispositivos (por ejemplo, `sda`, `sdb`, y otros) y los

nombres de dispositivos persistentes (provistos por `udev` en `/dev/disk/by-*/`) para mensajes de kernel. El registro de kernel `/dev/kmsg`, el cual puede desplegarse con el comando `dmesg`, ahora muestra los mensajes para enlaces simbólicos que `udev` ha creado para dispositivos de kernel. Estos mensajes se despliegan en el siguiente formato:

```
udev-alias: <nombre_dispositivo> (<symbolic_link> <symbolic link> ...)
```

Cualquier analizador de registro puede desplegar estos mensajes, que están almacenados en `/var/log/messages` vía `syslog`.

Nuevo paquete `linuxptp`

El paquete `linuxptp` incluido en Red Hat Enterprise Linux 6.4 como una Muestra de tecnología, es una implementación del Protocolo de tiempo de precisión (PTP) según el estándar IEEE 1588 para Linux. Las metas de diseño duales se proporcionan como una implementación sólida del estándar y para usar las interfaces de programación de aplicaciones más importantes (API) ofrecidas por el kernel de Linux. El soporte de las API de legado y otras plataformas no es la meta.

Documentación de Hugepages transparentes

La documentación para Hugepages transparentes ha sido añadida al siguiente archivo:

```
/usr/share/doc/kernel-doc-<versión>/Documentation/vm/transhuge.txt
```

Estado de soporte para destinos de volcado

En Red Hat Enterprise Linux 6.4, el archivo `/usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt` proporciona una lista completa de los destinos de volcado con y sin soporte y desconocidos en la sección “Estatus de soporte para destino de volcado”.

CAPÍTULO 3. CONTROLADORES DE DISPOSITIVO

Controladores de almacenamiento

- El controlador de dispositivos de Dispositivos de almacenamiento de acceso directo (**DASD**) ha sido actualizado para detectar errores de configuración de ruta que no han sido detectados por hardware o microcódigo. Tras la detección, el controlador de dispositivos, no emplea dichas rutas. Con esta funcionalidad, por ejemplo, el controlador de dispositivos DASD detecta rutas que han sido asignadas a un subcanal específico pero que conducen a servidores diferentes de almacenaje.
 - El controlador de dispositivos **zfc** ha sido actualizado con el fin de añadir manejo de estructura de datos y de errores para soportar el modo mejorado de la tarjeta de adaptador de Protocolo de Canal de fibra (FCP) System z. En este modo, el adaptador pasa datos directamente de la memoria a la SAN (datos de enrutamiento) cuando la memoria en la tarjeta adaptadora se bloquea por solicitudes grandes y lentas de E/S.
 - El controlador **mtip32xx** ha sido actualizado para añadir soporte a las unidades más recientes de PCIe SSD.
 - El controlador **lpfc** para Emulex Fibre Channel Host Bus Adapters ha sido actualizado a la versión 8.3.5.82.1p.
 - El controlador **qla2xxx** para Canal de fibra QLogic HBA ha sido actualizado a la versión 8.04.00.04.06.4-k, lo cual añade soporte para el adaptador de red convergido (CNA) 83XX de QLogic, soporte de 16 GBps FC para adaptadores QLogic, y el nuevo Form Factor CNA para servidores HP ProLiant.
 - El controlador **qla4xxx** ha sido actualizado a la versión v5.03.00.00.06.04-k0, la cual añade soporte API de *change_queue_depth*, corrige una cantidad de errores e introduce varias mejoras.
 - El firmware **ql2400-firmware** para HBA de canal de fibra QLogic de 4Gbps, ha sido actualizado a la versión 5.08.00.
 - El firmware **ql2500-firmware** para HBA canal de fibra de 4Gbps de QLogic ha sido actualizado a la versión 5.08.00.
 - El controlador **ipr** para HBA SCSI RAID Power Linux de IBM ha sido actualizado a la versión 2.5.4, la cual añade soporte para los adaptadores SAS Power7 6Gb y habilita la capacidad VRAID de SAS.
 - El controlador **hpsa** ha sido actualizado a la versión 2.0.2-4-RH1 para añadir PCI-ID para la familia de controladores generación 8 Smart Array de HP.
 - El controlador **bnx2i** para Broadcom NetXtreme II iSCSI ha sido actualizado a la versión 2.7.2.2 con habilitaciones de soporte de hardware generales.
- El soporte de arranque iSCSI y FCoE en dispositivos Broadcom ahora tiene total soporte en Red Hat Enterprise Linux 6.4. Estas dos funcionalidades son provistas por los controladores Broadcom **bnx2i** y **bnx2fc**.
- El controlador **bnx2fc** para el chip Broadcom Netxtreme II 57712 ha sido actualizado a la versión 1.0.12.

El soporte de arranque iSCSI y FCoE en dispositivos Broadcom ahora está totalmente soportada en Red Hat Enterprise Linux 6.4. Estos dos factores son proporcionados por los controladores `bnx2i` y `bnx2fc` de Broadcom.

- El controlador `mpt2sas` ha sido actualizado a la versión 13.101.00.00, la cual añade soporte de modo multi segmentos para el controlador BSG de Linux.
- El controlador de canal de fibra de brocado `bfa` y el controlador FCoE han sido actualizados a la versión 3.0.23.0 que incluye soporte de adaptador de Canal de fibra de brocado 1860 16Gbps, nuevo soporte de hardware en servidores de generación 12 en Dell PowerEdge y soporte `issue_lip`. El firmware `bfa` fue actualizado a la versión 3.0.3.1.
- El controlador `be2iscsi` para dispositivos ServerEngines BladeEngine 2 Open iSCSI ha sido actualizado a la versión 4.4.58. 0 para añadir soporte de VLAN netlink iSCSI.
- El controlador `qib` para TrueScale HCA ha sido actualizado a la versión más reciente don las siguientes mejoras:
 - Reconocimiento de NUMA mejorado
 - El agente de control de congestión (CCA) para tejidos de mensajería de escala de rendimiento (PSM)
 - Riel PSMDual para tejidos PSM
 - Mejoras de rendimiento y corrección de errores
- Los controladores a continuación han sido actualizados para incluir las últimas funcionalidades de la línea de desarrollo principal y correcciones de errores: `ahci`, `md/bitmap`, `raid0`, `raid1`, `raid10`, and `raid456`.

Controladores de red

- El controlador `netxen_nic` para la red del multi puerto NetXen (1/10) Gigabit ha sido actualizado a la versión 4.0.80, la cual añade soporte miniDIMM. El firmware `netxen_nic` ha sido actualizado a la versión 4.0.588.
- El controlador `bnx2x` ha sido actualizado a la versión 1.72.51-0 para incluir soporte para chips Broadcom 57800/57810/57811/57840, igualmente, se han corregido errores y se ha actualizado el firmware para chips Broadcom 57710/57711/57712. Esta actualización también incluye las siguientes mejoras:
 - Soporte para descarga iSCSI y puente de centro de datos/Canal de fibra sobre Ethernet (DCB/FCOE) en chips Broadcom 57712/578xx. El chip 57840 de Broadcom está soportado en una configuración de 4x10G únicamente y no soporta descarga iSCSI ni los lanzamientos FCoE. Los lanzamientos futuros soportarán configuraciones adicionales y de descarga iSCSI y FCoE.
 - Soporte de capa adicional física, incluida la Ethernet de energía eficiente (EEE).
 - Mejoras de descarga iSCSI
 - Funcionalidades específicas OEM
- El controlador `be2net` para dispositivos de red ServerEngines BladeEngine2 de 10Gbps ha sido actualizado a la versión 4.4.31. 0 para añadir RDMA sobre soporte de Ethernet convergido (RoCE).

Además, la funcionalidad de SR-IOV del controlador **be2net** de marca Emulex, ahora tiene total soporte en Red Hat Enterprise Linux 6.4. SR-IOV se ejecuta en todas las variantes de Emulex-branded y OEM de hardware basado en BE3, el cual requiere el controlador **be2net** de software.

- El controlador **ixgbev** ha sido actualizado a la versión 2.6.0-k para incluir el soporte de hardware más reciente, mejoras y corrección de errores.
- El controlador **cxgb4** para controladores de red cableados unificados Chelsio Terminator4 de 10G ha sido actualizado para añadir soporte a adaptadores T480-CR y T440-LP-CR de Chelsio.
- El controlador **cxgb3** para la familia Chelsio T3 de dispositivos de red ha sido actualizado a la versión 1.1.5-ko.
- El controlador **ixgbe** para dispositivos de red Intel de 10 Gigabit PCI Express, ha sido actualizado a la versión 3.9.15-k para incluir soporte para SR-IOV con puente de centro de datos (DCB) o Escalamiento de recepción lateral (RSS), soporte PTP como una Muestra de tecnología y soporte para el hardware más reciente, mejoras y corrección de errores.
- El controlador **iw_cxgb3** ha sido actualizado.
- El controlador **iw_cxgb4** ha sido actualizado
- El controlador **e1000e** para dispositivos de red Intel PRO/1000 ha sido actualizado para añadir el soporte más reciente de hardware, funcionalidades y proporcionar un número de correcciones de errores.
- El controlador **enic** para dispositivos Ethernet Cisco de 10G ha sido actualizado a la versión 2.1.1.39.
- El controlador **igbvf** (Controlador de red de función virtual en Gigabit de Intel) has been updated to the latest upstream version.
- El controlador **igb** para Adaptadores Ethernet Gigabit de Intel, ha sido actualizado a la versión 4.0.1 para añadir soporte al hardware más reciente. También, se ha añadido soporte PTP al controlador **igb** como una Muestra de tecnología.
- El controlador **tg3** para dispositivos Broadcom Tigon3 Ethernet ha sido actualizado a la versión 3.124 para añadir soporte al nuevo hardware. También, se ha añadido soporte PTP para el controlador **tg3** como una Muestra de tecnología.
- El controlador **qlcn** para los adaptadores de servidor de 10 Gigabits QLogic Series NC de HP ha sido actualizado a la versión 5.0.29.
- El controlador de brocado **bna** para controladores Ethernet de Brocado de 10Gb PCIe ha sido actualizado a la versión 3.0.23.0 para añadir nuevo soporte de hardware para servidores de generaciónn 12 Dell PowerEdge y para habilitar el uso de cables de cobre Twinax de no brocado. El firmware **bna** firmware fue actualizado a la versión 3.0.3.1.
- El controlador NetXtreme II Broadcom **cn** ha sido actualizado a la versión 2.5.13 para incluir nuevas funcionalidades, corrección de errores, y soporte para nuevas plataformas OEM.

Controladores varios

- El controlador Cpuidle **intel_idle** para procesadores Intel ha sido actualizado para añadir soporte a las series de procesadores E5, X86 V2 Xeon de Intel

soporte a las series de procesadores E5-xxx v2 xeon de intel.

- El controlador wacom ha sido actualizado para añadir soporte para el lápiz Wacom Bamboo CTL-460, la tableta Wacom Intuos5, y la pantalla de lápiz Wacom Cintiq 22HD .
- El controlador de audio ALSA HDA ha sido actualizado para habilitar o mejorar el soporte para un nuevo hardware y corregir un número de errores.
- El controlador `m1x4_en` driver ha sido actualizado a la versión más reciente de la línea de desarrollo principal.
- El controlador `m1x4_ib` ha sido actualizado a la versión más reciente de la línea de desarrollo principal.
- El controlador `m1x4_core` ha sido actualizado a la versión más reciente de la línea de desarrollo principal.
- El controlador de dispositivos `z90crypt` ha sido actualizado para soportar la nueva tarjeta adaptadora Crypto Express 4 (CEX4).

CAPÍTULO 4. RED

HAProxy

HAProxy es un equilibrador de carga de alto rendimiento, autónomo, capa 7, para aplicaciones basadas en TCP y HTTP, las cuales realizan varios tipos de programación basados en el contenido de las solicitudes HTTP. Red Hat Enterprise Linux 6.4 introduce el paquete haproxy como una Muestra de tecnología.

CAPÍTULO 5. AUTENTICACIÓN E INTEROPERABILIDAD

Funcionalidades SSSD totalmente soportadas

Una cantidad de funcionalidades introducidas en Red Hat Enterprise Linux 6.3 ahora están soportadas totalmente en Red Hat Enterprise Linux 6.4

- soporte para manejo central de llaves SSH,
- Asignación de usuario SELinux
- y soporte para guardar en cache mapa de automount.

Nuevo tipo de almacenamiento cache SSSD

La versión 1.10 de Kerberos adicionó un nuevo tipo de almacenamiento cache, **DIR:**, el cual le permite mantener tiquetes que otorgan de forma simultánea un tiquete (TGT) a centros de distribución de llaves multiples (KDC) y autoseleccionan entre ellos cuando negocian con recursos kerberizados. En Red Hat Enterprise Linux 6.4, SSSD ha sido mejorado para permitirle seleccionar la cache **DIR:** para usuarios que se conectan mediante SSSD. Esta funcionalidad se introduce como una Muestra de tecnología.

Adición de dominios AD a grupos externos

En Red Hat Enterprise Linux 6.4, el comando `ipa group-add-member` le permite añadir miembros de dominios de confianza basados en directorios activos a grupos marcados como **externos** en manejo de identidad. Dichos miembros pueden ser especificados por su nombre mediante una sintaxis de dominio o de UPN, por ejemplo `AD\NombredeUsuario` o `AD\NombredeGrupo`, o `Usuario@AD.Dominio`. Cuando se especifica de esta forma, los miembros se resuelven con Catálogo global de dominio confiable basado en Directorios activos para obtener su valor identificador de seguridad (SID).

Alternativamente, un valor SID podría especificarse directamente. En este caso, el comando `ipa group-add-member` solo verificará que la parte del dominio del valor de SID sea uno de los dominios confiables de Active Directory. No se hará ningún intento para verificar la validez del SID dentro del dominio.

Es recomendable usar la sintaxis de nombre de usuario o grupo para especificar los miembros externos en lugar de proveer sus valores SID de forma directa.

Certificados de subsistema de manejo de auto-renovación de identidad

El periodo de validez predeterminado para una Autoridad certificadora (CA) es de 10 años. La CA expide certificados para sus subsistemas (OCSP, registro de auditoría y otros). Los certificados de subsistemas son normalmente válidos por 2 años. Si los certificados expiran, la CA no inicia o no funciona adecuadamente. Por lo tanto, en Red Hat Enterprise Linux 6.4, los servidores de administración de identidad pueden renovar de forma automática sus certificados de subsistemas. Los certificados de subsistemas son rastreados por `certmonger`, el cual intenta automáticamente renovar los certificados antes de que expiren.

Configuración automática de herramientas de cliente OpenLDAP en clientes matriculados en Administración de identidad

En Red Hat Enterprise Linux 6.4, OpenLDAP se configura automáticamente con la URI de LDAP predeterminada, un Nombre distinguido de base y un certificado TLS durante la instalación de Administración de identidad de cliente. Esto mejora la experiencia de usuario al realizar búsquedas LDAP para el servidor de directorio de Administración de identidad.

Soporte PKCS#12 para python-nss

El paquete `python-nss` que proporciona los vínculos para Servicios de seguridad de red (NSS) y el Tiempo de ejecución portátil de Netscape (NSPR), han sido actualizados para añadir soporte PKCS #12.

Búsqueda total persistente para DNS

LDAP en Red Hat Enterprise Linux 6.4 incluye soporte de búsqueda persistente para ambas zonas y sus registros de recursos. La búsqueda persistente le permite al conector `bind-dyndb-ldap` informarse inmediatamente de todos los cambios en una base de datos LDAP. También disminuye el uso de red de banda ancha requerido para sondeos repetidos.

Nueva operación CLEANALLRUV

Los elementos obsoletos en Base de datos del Vector de actualización de réplica (RUV) pueden retirarse con la operación `CLEANRUV`, la cual los retira en un único proveedor o maestro. Red Hat Enterprise Linux 6.4 añade la nueva operación `CLEANALLRUV`, la cual retira datos RUV obsoletos de todas las réplicas y necesita ejecutarse en un solo proveedor/maestro únicamente.

Bibliotecas actualizadas de samba4

Las bibliotecas de `samba4` (provistas por el paquete `samba4-libs`) han sido actualizadas a la última versión de la línea de desarrollo para mejorar la interoperabilidad con dominios de Active Directory (AD). Ahora SSSD usa la biblioteca `libndr-krb5pac` para leer el Certificado de atributos de privilegios (PAC) expedido por un Centro de distribución de llaves AD (KDC). Además, se han realizado varias mejoras a la Autoridad de seguridad local (LSA) y los servicios de inicio de sesión de red para permitir la verificación de confianza desde un sistema de Windows. Para obtener información sobre la introducción de kerberos de cruce de dominios que depende de paquetes `samba4`, consulte [“Cruce de funcionalidad de confianza de dominio de kerberos en manejo de identidad”](#).



AVISO

Si usted hace la actualización de Red Hat Enterprise Linux 6.3 a Red Hat Enterprise Linux 6.4 y está usando Samba, asegúrese de desinstalar el paquete `samba4` para evitar conflictos durante la actualización.

Puesto que la funcionalidad de confianza de cruce de dominios de kerberos es considerada una Muestra de tecnología, los componentes seleccionados de `samba4` se consideran una Muestra de tecnología. Para obtener mayor información sobre qué paquetes de Samba son considerados una Muestra de tecnología, consulte [Tabla 5.1, “Soporte de paquete Samba4”](#).

Tabla 5.1. Soporte de paquete Samba4

Nombre de paquete	¿Nuevo paquete en 6.4?	Estatus de soporte
<code>samba4-libs</code>	No	Muestra de tecnología, a excepción de la funcionalidad requerida por OpenChange
<code>samba4-pidl</code>	No	Muestra de tecnología, a excepción de la funcionalidad requerida por OpenChange

Nombre de paquete	¿Nuevo paquete en 6.4?	Estatus de soporte
samba4	No	Muestra de tecnología
samba4-client	Yes	Muestra de tecnología
samba4-common	Yes	Muestra de tecnología
samba4-python	Yes	Muestra de tecnología
samba4-winbind	Yes	Muestra de tecnología
samba4-dc	Yes	Muestra de tecnología
samba4-dc-libs	Yes	Muestra de tecnología
samba4-swat	Yes	Muestra de tecnología
samba4-test	Yes	Muestra de tecnología
samba4-winbind-clients	Yes	Muestra de tecnología
samba4-winbind-krb5-locator	Yes	Muestra de tecnología

Cruce de funcionalidad de confianza de dominio de kerberos en manejo de identidad

El cruce de funcionalidad de confianzas de dominio de kerberos provisto por el manejo de identidad se incluye como Muestra de tecnología. Esta funcionalidad le permite crear una relación de confianza entre una administración de identidad y un dominio de directorio activo. Es decir que los usuarios del dominio AD pueden acceder a recursos y servicios desde el dominio de administración de identidad con sus credenciales AD. No se necesita sincronizar datos entre el manejo de identidad y los controladores de dominio AD; el usuario AD siempre se autentica con el controlador de dominio AD y la información sobre usuarios puede buscarse sin necesidad de sincronización.

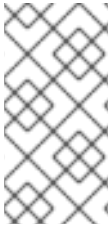
Esta funcionalidad es proporcionada por el paquete opcional `ipa-server-trust-ad`. Dicho paquete depende de funcionalidades que solo están disponibles en **samba4**. Puesto que los paquetes de `samba4-*` están en conflicto con los paquetes correspondientes de `samba-*`, todos los paquetes de `samba-*` se deben retirar antes de que `ipa-server-trust-ad` pueda ser instalado.

Cuando se instale el paquete `ipa-server-trust-ad`, el comando `ipa-adtrust-install` debe ejecutarse en todos los servidores de Administración de identidad y réplicas para que la Administración de identidad maneje confianzas. Al hacer esto, se puede establecer una confianza en la línea de comandos mediante `ipa trust-add` o la WebUI. Para obtener mayor información, consulte la sección *Integración de directorio activo a través de confianzas de kerberos de dominios cruzados* en la *Guía de administración de identidad* en https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/.

Soporte de esquema Posix para servidor de directorio 389

El Active Directory (AD) de Windows soporta el esquema POSIX (RFC 2307 y 2307bis) para entradas

de usuarios y grupos. En muchos casos, AD sirve como fuente autoritativa de datos de usuarios y grupos, incluidos los atributos de POSIX. Con Red Hat Enterprise Linux 6.4, la sincronización del servidor de directorio de Windows ya no ignora dichos atributos. Los usuarios ahora pueden sincronizar los atributos de POSIX con Windows Sync entre AD y el servidor de directorio 389.



NOTA

Al añadir entradas de un nuevos usuarios y grupos al servidor de directorio, los atributos de POSIX no se sincronizan con AD. La adición de entradas de nuevos usuarios y grupos al AD sincronizará al Servidor de directorio y atributos modificadores los sincronizarán de ambos modos.

CAPÍTULO 6. SEGURIDAD

Cómo tratar las coincidencias de modo autoritario en las búsquedas y entradas de sudo

La herramienta `sudo` se puede consultar en el archivo `/etc/nsswitch.conf` para entradas de los usuarios de `sudo` y búsquedas en archivos o mediante LDAP. Anteriormente, cuando se encontraba una coincidencia de entradas de `sudo` en la base de datos, la búsqueda aún continuaba en otras bases de datos (incluidos archivos). En Red Hat Enterprise Linux 6.4, se ha añadido una opción al archivo `/etc/nsswitch.conf` que permite a los usuarios especificar una base de datos después del cual una coincidencia de una entrada de `sudo` es suficiente. Esto elimina la necesidad de consultar otras bases de datos; mejorando así el rendimiento de las entradas de `sudo` en grandes entornos. Esta conducta no está predeterminada y debe ser configurada al añadir la cadena `[SUCCESS=return]` después de la base de datos seleccionada. Cuando se encuentre una coincidencia que preceda directamente esta cadena, no se consultará a otras bases de datos.

Revisiones adicionales de contraseña para pam_cracklib

El módulo `pam_cracklib` ha sido actualizado para añadir múltiples revisiones de fortaleza de contraseñas:

- Algunas políticas de autenticación no aceptan contraseñas que contengan secuencias largas tales como "abcd" or "98765". Esta actualización introduce la posibilidad de limitar la longitud máxima de dichas secuencias mediante la nueva opción `maxsequence`.
- El módulo `pam_cracklib` ahora permite revisar si una nueva contraseña contiene palabras del campo GECOS desde entradas en el archivo `/etc/passwd`. El campo GECOS sirve para almacenar información adicional sobre el usuario, tal como el nombre completod del usuario o un número telefónico, que podría ser utilizado por el atacante para para intentar adivinadr su contraseña.
- El módulo `pam_cracklib` ahora permite especificar el número máximo permitido de caracteres consecutivos de la misma clase (minúsculas, mayúsculas, números y caracteres especiales) en una contraseña mediante la opción `maxrepeatclass option`.
- El módulo `pam_cracklib` ahora soporta la opción `enforce_for_root`, la cual aplica las restricciones de complejidad en las contraseñas para la cuenta de root.

Opción de tamaño para polinstanciación de tmpfs

En un sistema con múltiples montajes `tmpfs`, es necesario limitar su tamaño para evitar que ocupen toda la memoria del sistema. PAM ha sido actualizada para permitir que los usuarios especifiquen el tamaño máximo del montaje del sistema de archivos `tmpfs` al usar polinstanciación instancias mediante la opción `mntopts=tamaño=<tamaño>` en el archivo de configuración `/etc/namespace.conf`.

Bloqueo de cuentas inactivas

Algunas políticas de autenticación requieren soporte para bloqueo de una cuenta que no sea utilizada por un cierto periodo de tiempo. Red Hat Enterprise Linux 6.4 introduce una función adicional para el módulo `pam_lastlog`, el cual le permite a los usuarios bloquear sus cuentas después de un número de días configurable.

Nuevos modos de funcionar para libica

La biblioteca `libica`, la cual contiene un grupo de funciones y herramientas para acceder al hardware de Acelerador criptográfico (ICA) eServer System z de IBM, ha sido modificada para permitir el uso de los nuevos algoritmos que soportan instrucciones de Asistente de seguridad de mensajes Extensión 4

en el Asistente de procesador central para la función criptográfica(CPACF). Para las cifras de bloques DES y 3DES, los siguientes modos de operación ahora tienen soporte:

- Encadenamiento de bloques de cifras con Robo de Ciphertext (CBC-CS)
- Código de autenticación de mensajes basados en cifras (CMAC)

Los siguientes modos de operación para la cifra de bloques AES, ahora tienen soporte:

- Encadenamiento de bloques de cifras con Robo de Ciphertext (CBC-CS)
- Contador con Código de encadenamiento de cifra de bloque (CCM)
- Galois/Contador (GCM)

Esta aceleración de algoritmos complejos mejora de forma significativa el rendimiento de máquinas System z de IBM.

Optimización y soporte para la biblioteca de compresión zlib de System z

La biblioteca zlib, una biblioteca de compresión de datos sin pérdidas, ha sido actualizada para mejorar el rendimiento de compresión en System z de IBM.

Configuración de cortafuegos de reserva

Los servicios `iptables` y `ip6tables` ahora proporcionan la capacidad de asignar una configuración de cortafuegos de reserva si las configuraciones no se pueden aplicar. Si falla la aplicación de reglas de cortafuegos desde `/etc/sysconfig/iptables`, el archivo de reserva se llama `/etc/sysconfig/iptables.fallback` y usa el formato de archivo `iptables-save` (igual a `/etc/sysconfig/iptables`). Si la aplicación del archivo de reserva también falla, no habrá ninguna otra reserva. Para crear un archivo de reserva, use las herramientas estándar de configuración de cortafuegos y cambie el nombre o copie el archivo de reserva. Use el mismo proceso para el servicio `ip6tables` service, only replace all occurrences of “iptables” con “ip6tables”.

CAPÍTULO 7. DERECHOS

Actualizaciones de cadenas

En Red Hat Enterprise Linux 6.4, se ha cambiado el nombre de varias cadenas en el Gestor de suscripción:

- *suscribir* se cambió a *anexar*
- *auto-suscribir* se cambió a *auto-anexar*
- *cancelar suscripción* se cambió a *retirar*
- *usuario* se cambió a *sistema* o *unidad*

Prueba de conexión de Proxy

El diálogo de configuración Proxy ahora permite a los usuarios probar una conexión en un proxy después de ingresar un valor.

Suscribir o cancelar los derechos múltiples

El Gestor de suscripción ahora puede suscribir (anexar) o cancelar suscripción (retirar) de multiples derechos mediante sus números de serie de una sola vez.

Soporte para llaves de activación en GUI

La interfaz gráfica de usuario del Gestor de suscripción ahora le permite registrar un sistema mediante una *llave de activación*. Las llaves de activación le permiten a los usuarios preconfigurar suscripciones para una sistema antes de que sea registrado.

Registro con otros servidores externos

Ahora el Gestor de suscripción soporta la selección de un servidor remoto durante el registro de un sistema. La interfaz de usuario del Gestor de suscripción proporciona la opción de elegir una URL de un servidor con el que se va a registrar, junto con el puerto y un prefijo, durante el proceso de registro. Además, durante el registro en la línea de comandos, se puede usar la opción `--serverurl` para especificar el servidor con el que se va a registrar. Para obtener mayor información sobre esta funcionalidad, consulte la sección *Registro, cancelación de registro, y volver a registrar un sistema* en la *Guía de administración de suscripciones*

Cambios de uso en la Interfaz Gráfica de usuario (GUI)

La GUI del Gestor de suscripción ha sido mejorada con varios cambios basados en los comentarios de los clientes.

CAPÍTULO 8. VIRTUALIZACIÓN

8.1. KVM

virtio-SCSI

La pila de almacenamiento de virtualización de KVM ha sido mejorada con la adición de funcionalidades virtio-SCSI (una arquitectura de almacenamiento para KVM basada en SCSI). Virtio-SCSI proporciona la capacidad de conectar directamente para LUN de SCSI y mejora la escalabilidad de forma significativa comparada con virtio-blk. La ventaja de virtio-SCSI es que puede manejar cientos de dispositivos en comparación con virtio-blk que solamente maneja 25 dispositivos y amortigua ranuras PCI.

Virtio-SCSI puede ahora heredar el conjunto de funcionalidades establecidas como el dispositivo de destino con la capacidad de:

- colocar un disco duro virtual o CD mediante el controlador virtio-scsi,
- pasa a través de un dispositivo SCSI físico del host al invitado a través del dispositivo de bloque scsi QEMU,
- y permite el uso de cientos de dispositivos por huéspedes; una mejora del límite de dispositivo ~25 de virtio-blk.

virtio-scsi se introdujo en Red Hat Enterprise Linux 6.3 como Muestra de tecnología y ahora cuenta con soporte total en Red Hat Enterprise Linux 6.4. Los huéspedes de Windows (a excepción de Windows XP) también tienen soporte con los controladores virtio-win más recientes.

Soporte para el procesador Intel core de siguiente generación

Red Hat Enterprise Linux 6.4 añade soporte para el procesador de siguiente generación de Intel core para `qemu-kvm` a fin de que los huéspedes KVM puedan utilizar las nuevas funcionalidades que dicho procesador ofrece, las más importantes son: Extensiones vectoriales avanzadas 2 (AVX2), Instrucciones de manipulación de bits 1 (BMI1), Instrucciones de manipulación de bits 2 (BMI2), Omisión de bloqueo de hardware (HLE), Memoria transaccional restringida (RTM), Identificador Proceso-Contexto (PCID), Invalidar identificador proceso-contexto (INVPCID), Fusión de multiplicación y suma (FMA), Big-Endian Move Instruction (MOVBE), Instrucción de base de segmento F y segmento G (FSGSBASE), Prevención de ejecución de modo supervisor (SMEP), Enhanced REP MOVSB/STOSB (ERMS).

Soporte para CPU series 4xxx AMD Opteron

El procesador AMD Opteron series 4xxx ahora está soportado por `qemu-kvm`. Esto le permite a las nuevas funcionalidades de estas series de procesador ser expuestas a los huéspedes de KVM, como por ejemplo: el conjunto de instrucciones F16C, Manipulación de arrastre de bits, funciones para diezmar Instrucciones de manipulación de bits 1 (BMI1), y el conjunto de instrucciones para Fusión de multiplicación y suma (FMA).

Migración de huéspedes en vivo mediante reenvío de USB vía SPICE

En Red Hat Enterprise Linux 6.4, KVM soporta migración de huéspedes en vivo mediante reenvío de USB vía SPICE, mientras mantiene la redirección del dispositivo USB para todos los dispositivos configurados.

Migración de huéspedes en vivo mediante dispositivos USB

En Red Hat Enterprise Linux 6.4, KVM soporta migración de huéspedes en vivo con dispositivos USB. Los siguientes dispositivos están soportados: Interfaz de controlador de host mejorada (EHCI) y el paso local de la Interfaz de controlador de host universal (UHCI) y los dispositivos emulados tales como, ratones, teclados, hubs, y otros.

Agente de huéspedes QEMU actualizado

El agente de huéspedes QEMU (provisto por el paquete `qemu-guest-agent`) ahora está soportado totalmente en Red Hat Enterprise Linux 6.4. Ha sido actualizado a la versión de la línea de desarrollo principal versión 1.1, e incluye las siguientes mejoras y correcciones de errores importantes:

- Los comandos `guest -suspend -disk` y `guest -suspend -ram` ahora pueden utilizarse para suspender a RAM o a disco en un sistema Windows.
- El comando `guest -network -get -interfaces` puede utilizarse para adquirir información de interfaz de red en Linux.
- Esta actualización proporciona mejoras de soporte de congelamiento de sistema de archivos y corrección de errores.
- Esta actualización incluye varias correcciones de errores y pequeñas mejoras.

Indicación de fin de interrupción paravirtualizada (PV-EOI)

Los hosts y huéspedes que ejecutan Red Hat Enterprise Linux 6.3 y anteriores requieren dos VM (interruptores de contexto de VM a hipervisor) para cada interrupción: una para inyectar la interrupción, y otra para señalar el fin de la interrupción. Con ambos sistemas de host actualizados para Red Hat Enterprise Linux 6.4 o más reciente, puede negociar una funcionalidad paravirtualizada de fin de interrupción y solo requiere un interruptor para detenerlo. Por consiguiente, a través de Red Hat Enterprise Linux 6.4 o más reciente para host y huésped, el número de salidas se reduce a la mitad para cargas de interrupción intensiva, tales como un tráfico con un dispositivo de red virtio. Esto conduce a una reducción significativa en la utilización de CPU de host para dichas cargas. Observe que solo las interrupciones de margen son mejoradas: Por ejemplo la red `e1000` usa niveles de interrupciones y no fue mejorada.

Paso de sonido configurable

Ahora se puede detectar un dispositivo de sonido como un **micrófono** o un **altavoz** en el sistema de huésped (además se detecta como **línea de entrada** y **línea de salida**). Los dispositivos de sonido ahora pueden funcionar correctamente en aplicaciones de huéspedes que aceptan únicamente ciertos tipos de salida para voz, grabación y audio.

8.2. HYPER-V

Inclusión y soporte de instalación de huésped para controladores Hyper-V-D de Microsoft

La instalación de huésped integrado de Red Hat Enterprise Linux y el soporte del dispositivo paravirtualizado Hyper-V en Red Hat Enterprise Linux 6.4 - Microsoft Hyper-V permite a los usuarios ejecutar Red Hat Enterprise Linux 6.4 como un huésped por encima de hipervisores Hyper-V de Microsoft. Los siguientes controladores Hyper-V y una fuente de reloj han sido agregadas al kernel que se distribuye con Red Hat Enterprise Linux 6.4:

- Un controlador de red (`hv_netvsc`)
- Un controlador de almacenaje `hv_storvsc`)
- Un controlador de ratón compatible con HID (`hid_hyperv`)
- Un controlador VMBus (`hv_vmbus`)
- Un controlador 'util' (`hv_util`)
- Un controlador de disco IDE (`ata_piix`)

- Una fuente de reloj (i386, AMD64/Intel 64: `hyperv_clocksource`)

Red Hat Enterprise Linux 6.4 también incluye soporte para Hyper-V como una fuente de reloj y un demonio Par clave-valor (KVP) Hyper-V de huésped (`hypervkvpd`) que pasa información básica, tal como el IP de huésped, el FQDN, el nombre de SO, y el número de lanzamiento del SO al host a través de VMbus.

8.3. VMWARE ESX

Controladores PV VMware

Los controladores VMware paravirtualizados han sido actualizados para proporcionar una perfecta experiencia fuera de la caja cuando se ejecuta Red Hat Enterprise Linux 6.4 en VMware ESX. El instalador Anaconda también ha sido actualizado para listar los controladores durante el proceso de instalación. Los siguientes controladores han sido actualizados:

- Un controlador de red (`vmxnet3`)
- Un controlador de almacenaje (`vmw_pvscsi`)
- Un controlador de englobamiento de memoria (`vmware_balloon`)
- Un controlador de ratón (`vmmouse_drv`)
- Un controlador de vídeo (`vmware_drv`)

CAPÍTULO 9. AGRUPAMIENTO

Soporte para el dispositivo de vallas IPDU de IBM

Red Hat Enterprise Linux 6.4 añade soporte para dispositivo de valla iPDU de IBM. Para obtener mayor información sobre los parámetros de este dispositivo de valla, consulte el apéndice *Parámetros de dispositivo de valla* en la Guía de *Administración de clúster* de Red Hat Enterprise Linux 6.

Soporte para Dispositivo de valla de controlador de energía de red Eaton

Red Hat Enterprise Linux 6.4 añade soporte para `fence_eaton_snmp`, el agente de valla para el interruptor de energía de red SNMP sobre Eaton. Para obtener mayor información sobre parámetros de este agente de vallas, consulte el apéndice *Parámetros de dispositivos de vallas* en la Guía de *Administración de clúster* de Red Hat Enterprise Linux.

Nuevo paquete keepalived

Red Hat Enterprise Linux 6.4 incluye el paquete `keepalived` como una Muestra de tecnología. El paquete `keepalived` proporciona herramientas simples y robustas para equilibrio de cargas y alta disponibilidad. El marco de equilibrio de carga depende del módulo de kernel de servidor virtual de Linux ampliamente conocido y utilizado, el cual proporciona balanceo de red de carga de capa 4. El demonio `keepalived` implementa un conjunto de revisores de salud para grupos de servidores según su estado. El demonio `keepalived` también implementa el Protocolo de redundancia de enrutador virtual (VRRP), el cual permite a la conmutación de enrutador o de director alcanzar alta disponibilidad

Recuperación de Watchdog

Los nuevos agentes de valla `fence_sanlock` y `checkquorum.wdmd`, incluidos en Red Hat Enterprise Linux 6.4 como una Muestra de tecnología, proporcionan nuevos mecanismos para provocar la recuperación de un nodo a través un dispositivo de Watchdog. Los tutoriales sobre cómo habilitar esta Muestra de tecnología estarán disponibles en <https://fedorahosted.org/cluster/wiki/HomePage>.

Soporte para almacenaje basado en VMDK

Red Hat Enterprise Linux 6.4 añade soporte para clústeres mediante tecnología de imágenes de disco VMDK (Disco de máquina virtual) de VMware con la opción de multi escritura. Esto le permite, por ejemplo, usar almacenaje basado en VMDK con la opción de multi escritor para sistemas de archivos en clúster tales como GFS2.

CAPÍTULO 10. ALMACENAJE

Paralelo NFS totalmente soportado

El NFS paralelo (pNFS) hace parte del estándar NFS v4.1 que permite acceder a dispositivos de almacenaje de forma directa y en paralelo. La arquitectura pNFS puede mejorar la escalabilidad y rendimiento de servidores para varias cargas comunes. En Red Hat Enterprise Linux 6.4, pNFS está totalmente soportado.

pNFS soporta 3 protocolos o distribuciones de almacenaje diferentes: archivos, objetos y bloques. El cliente NFS de Red Hat Enterprise Linux 6.4 soporta el protocolo de distribución de archivos.

Para habilitar el uso de esta nueva funcionalidad, use alguna de las siguientes opciones en montajes desde un servidor habilitado pNFS: `-o minorversion=1` o `-o v4.1`.

Cuando el servidor pNFS esté habilitado, el módulo de kernel `nfs_layout_nfsv41_files` se cargará automáticamente en el primer montaje. Use el siguiente comando para verificar que este módulo ha sido cargado:

```
~]$ lsmod | grep nfs_layout_nfsv41_files
```

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

Soporte de descarte en línea XFS

Una operación en línea de descarte realizada en un sistema de archivos montado, descarta bloques que el sistema de archivos no está utilizando. Las operaciones de descarte ahora tienen soporte en sistemas de archivos XFS. Para obtener mayor información, consulte la sección *Descartar bloque no usados* en la *Guía de administración de almacenaje* de Red Hat Enterprise Linux 6.

Soporte LVM para Micron PCIe SSD

En Red Hat Enterprise Linux 6.4, LVM añade soporte para Unidades de estado sólido (SSD) Micron PCIe como dispositivos que pueden formar una parte del Grupo de volumen.

Soporte LVM para Espejo RAID10 de dos vías

LVM ahora puede crear, retirar y redimensionar volúmenes lógicos RAID10. Para crear un volumen lógico RAID10, como otros tipos de RAID, especifique el tipo de segmento de la siguiente manera:

```
~]# lvcreate --type raid10 -m 1 -i 2 -L 1G -n lv vg
```

Observe que los argumentos `-m` e `-i` se comportan en la misma forma que ellos desearían para los otros tipos de segmentos. Es decir, `-i` es el número total de bandas mientras que `-m` es el número de copias (adicionales) (o sea, `-m 1 -i 2` otorga 2 bandas en la parte superior de los espejos de dos vías).

Configurar y administrar las reservas SCSI persistentes a través de mecanismos mapeadores de dispositivos

Anteriormente, para configurar reservas persistentes en dispositivos multirutas, se requería configurar todo en los dispositivos de ruta. Si un dispositivo de ruta era añadido posteriormente, se necesitaba añadir de forma manual, reservaciones a esa ruta. Red Hat Enterprise Linux 6.4 adiciona la capacidad de configurar y administrar reservaciones persistentes SCSI a través de dispositivos mapeadores con el comando `mpathpersist`. Cuando se añaden los dispositivos de ruta, también se establecen reservaciones de dichos dispositivos.

CAPÍTULO 11. COMPILADOR Y HERRAMIENTAS

SystemTap actualizado a la versión 1.8

SystemTap es una herramienta de trazado y sondeo que permite a los usuarios estudiar y monitorizar las actividades del sistema operativo (en particular, el kernel) en fino detalle. Proporciona información similar a herramientas como `netstat`, `ps`, `top` y `iostat`; sin embargo, SystemTap está diseñada para proporcionar más opciones de filtración y análisis para la información recolectada.

El paquete `systemtap` en Red Hat Enterprise Linux 6.4 ha sido actualizado a la versión 1.8 de la línea de desarrollo, la cual proporciona una cantidad de corrección de errores y mejoras.

- La sintaxis `@var` es ahora una sintaxis de lenguaje alternativa para variables DWARF en manejadores `uprobe` y `kprobe` (proceso, kernel, módulo).
- Ahora SystemTap maneja las variables locales para evitar choques en los encabezados de C incluidos por pulsaciones.
- El servidor de compilación SystemTap y el cliente ahora soportan redes IPv6.
- Ahora, el tiempo de ejecución de SystemTap (`staprun`) acepta la opción de tiempo de espera `-T` que permite menos despertadores frecuentes para sondear scripts de rendimiento bajo.
- El controlador traductor de script de SystemTap (`stap`) proporciona ahora las siguientes opciones de límite de recursos:

```
--rlimit-as=NUM
--rlimit-cpu=NUM
--rlimit-nproc=NUM
--rlimit-stack=NUM
--rlimit-fsize=NUM
```

- Los módulos SystemTap son ahora más pequeños y se compilan más rápido. La información de depuración de módulos ahora se suprime de forma predeterminada.
- Error [CVE-2012-0875](#) (Pánico de kernel al procesar datos malformados DWARF) ha sido corregido

Herramientas `lscpu` y `chcpu`

La herramienta `lscpu`, la cual despliega información detallada sobre las CPU disponibles ha sido actualizada para incluir nuevas funcionalidades. También ha sido añadida la nueva herramienta, `chcpu`, la cual le permite cambiar el estado de CPU (en línea o no, en espera o activa, y en otros estados), inhabilitar o habilitar las CPU y configurar CPU especificadas.

Para obtener mayor información sobre estas herramientas, consulte las páginas de manual `lscpu(1)` y `chcpu(8)`.

CAPÍTULO 12. ACTUALIZACIONES GENERALES

Han sido actualizados los paquetes de samba

Red Hat Enterprise Linux 6.4 incluye paquetes de samba rebasados que introducen varias correcciones de errores y mejoras, lo más importante es que se agregó soporte para el protocolo SMB2. El soporte de SMB2 puede habilitarse con el siguiente parámetro en la sección `[global]` del archivo `/etc/samba/smb.conf`:

```
máx protocolo = SMB2
```

Además, ahora Samba tiene soporte para cifrado AES de Kerberos. Ha estado disponible el soporte AES en el sistema operativo de Microsoft Windows desde Windows Vista y el servidor de Windows 2008. Se ha reportado como predeterminado el nuevo tipo de cifrado de Kerberos desde Windows 7. Ahora Samba añade llaves de Kerberos AES para que la tabla de claves la controle. Esto significa que otros servicios kerberizados que usan tabla de claves Samba y ejecutan la misma máquina pueden beneficiarse del cifrado AES. Con el fin de usar llaves de sesión AES (y no solo usar tiquete que otorga tiquetes AES), la cuenta de máquina Samba en el servidor LDAP del directorio activo debe ser modificada de forma manual. Para obtener mayor información, consulte el [Blog del Equipo de soporte de Open Specifications de Microsoft](#).



AVISO

Los paquetes actualizados de samba también cambian la forma en que la asignación de ID es configurada. Se recomienda a los usuarios modificar sus archivos de configuración de Samba.

Observe que varios archivos de la base de datos Trivial (TDB) han sido actualizados y se ha vuelto a escribir el soporte de impresión para usar la implementación del registro real. Esto significa que todos los archivos TDB se actualizan tan pronto como inicie la nueva versión de `smbd`. No puede cambiar a una versión de Samba anterior a 3.x a menos que tenga copias de seguridad de los archivos TDB.

Para obtener mayor información sobre estos cambios, consulte las [Notas de lanzamiento para Samba 3.6.0](#).

Nuevo paquete SciPy

Red Hat Enterprise Linux 6.4 incluye un nuevo paquete `scipy`. El paquete SciPy proporciona software para matemáticas, ciencia e ingeniería. El paquete NumPy, el cual está diseñado para manipular grandes matrices multidimensionales de registros arbitrarios, es la biblioteca central para SciPy. La biblioteca SciPy se crea para funcionar con matrices NumPy y proporciona varias rutinas numéricas eficientes, por ejemplo, rutinas para integración numérica y optimización.

Soporte TLS v1.1 en NSS

Los paquetes `nss` y `nss-util` han sido actualizados a la versión 3.14 de la línea de desarrollo principal, entre sus funcionalidades está el soporte para la versión TLS 1.1. También, el paquete `nspr` ha sido rebasado a la versión 4.9.2. Para obtener mayor información, consulte las [Notas de lanzamiento NSS 3.14](#).

Valgrind incorporado de gdbserver

El paquete `valgrind` ha sido actualizado a la versión 3.8.1 de la línea de desarrollo principal. Esta versión contiene entre otras, mejoras y correcciones de errores y un `gdbserver` incorporado. Para obtener mayor información, consulte el capítulo *Valgrind* y el apéndice *Cambios en Valgrind 3.8.1* en la *Guía del usuario de caja de herramientas del desarrollador de Red Hat 1.1*.

Nuevos paquetes libjpeg-turbo

Red Hat Enterprise Linux 6.4 incluye el nuevo grupo de paquetes: `libjpeg-turbo`. Estos paquetes reemplazan los paquetes tradicionales `libjpeg` y proporcionan la misma funcionalidad y API como `libjpeg`, pero con un mejor rendimiento.

Nuevo paquete redhat-lsb-core

Al instalar el paquete `redhat-lsb`, se introducen en el sistema un gran número de dependencias para cumplir con los estándares LSB. Red Hat Enterprise Linux 6.4 proporciona un nuevo subpaquete `redhat-lsb-core` que le permite buscar fácilmente el número mínimo de paquetes requeridos para instalar el paquete `redhat-lsb-core`.

Ha sido actualizada la herramienta createrepo

La herramienta `createrepo` ha sido actualizada a la versión más reciente de la línea principal de desarrollo, la cual reduce de forma significativa el uso de memoria y añade soporte de multitareas a través de la opción `--workers`.

APÉNDICE A. REVISION HISTORY

Revisión 1.1-12.1.400 Rebuild with publican 4.0.0	2013-10-31	Rüdiger Landmann
Revisión 1.1-12.1 Translation files synchronised with XML sources 1.1-12	Mon Jan 21 2013	Gladys Guerrero-Lozano
Revisión 1.1-12 Release of the Red Hat Enterprise Linux 6.4 Beta Release Notes.	Wed Dec 4 2012	Martin Prpič