



Red Hat Enterprise Linux 7 Notas de lanzamiento 7.2

Notas de lanzamiento para Red Hat Enterprise Linux 7.2

Red Hat Servicios de contenidos del
cliente

Red Hat Enterprise Linux 7 Notas de lanzamiento 7.2

Notas de lanzamiento para Red Hat Enterprise Linux 7.2

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 ofrecen cubrimiento de alto nivel de las mejoras y adiciones implementadas en Red Hat Enterprise Linux 7.2 y documenta los problemas conocidos en esta lanzamiento. Para obtener una documentación detallada sobre los cambios a Red Hat Enterprise Linux para la actualización de 7.2, consulte Technical Notes.

Table of Contents

Prefacio	6
Capítulo 1. Arquitecturas	7
Parte I. Nuevas funcionalidades	8
Capítulo 2. Autenticación	9
ca-certificate rebase a versión 2.4	9
Soporte para confianzas unidireccionales	9
openldap rebase a la versión 2.4.40	9
Autenticación caché en SSSD	9
SSSD permite el mapeo de UID y GID sobre clientes individuales	9
SSSD ahora puede negar acceso a SSH a cuentas bloqueadas	9
La herramienta sudo ahora puede verificar el comando checksum	10
Soporte SSSD para tarjeta inteligente	10
Múltiples certificados para soporte de perfiles	10
Contraseña Vault	10
Soporte DNSSEC en Administración de identidades	10
Proxy Kerberos HTTPS en Administración de identidades	11
Recarga del fondo de entradas en memoria caché	11
Almacenamiento en caché para operaciones initgroups	11
Negociar autenticación simplificada con mod_auth_gssapi	11
Funcionalidades de administración de ciclo de vida de usuario	11
Soporte SCEP en certmonger	11
Nuevos paquetes: epsilon	11
NSS aumenta los valores de poder mínimos de llaves	12
rebase ss y nss-util a la versión 3.19.1	12
Módulos Apache para IdM ahora reciben total soporte	12
Capítulo 3. Agrupamiento	13
systemd y pacemaker ahora se coordinan correctamente durante el apagado del sistema	13
Los comandos pcs resource move y pcs resource ban ahora muestran un mensaje de advertencia para aclarar la conducta de los comandos.	13
Nuevo comando para desplazar un recurso Pacemaker a su nodo preferido	13
Soporte para que el comando clufter transforme y analice los formatos de configuración de clúster	13
Capítulo 4. Compilador y herramientas	14
tail --follow ahora funciona correctamente en archivos sobre el Sistema de archivos Veritas Clustered (VXFS)	
El comando dd ahora muestra el progreso de la transferencia	14
Se mejoraron los tiempos de espera en libcurl	14
La biblioteca libcurl ahora implementa un handshake SSL de no bloqueo	14
GDB en IBM Power Systems ya no falla cuando se accede a la tabla de símbolos	14
nscd se actualizó para recargar de forma automática los datos de configuración	14
La función de biblioteca dlopen ya no se cuelga en llamadas recursivas.	14
La herramienta operf ahora reconoce los identificadores de páginas gigantes estáticas	15
El comando rsync -X ahora funciona correctamente	15
Los ejecutables Subversion ahora se integran totalmente con datos RELRO	15
La extensión de hilos en TCL ahora funciona correctamente	15
Capítulo 5. Escritorio	16
GNOME 3.14	16
El paquete ibus-gtk2 ahora actualiza el archivo immodules.cache	16
Capítulo 6. Sistemas de archivos	18

Rebase gfs2-utils a la versión 3.1.8	18
GFS2 ahora evita que los usuarios se excedan en sus cuotas	18
Rebase XFS la versión 4.1	18
Actualización de ext4 y jbd2	18
cifs se rebasa a la versión 3.17	18
Capítulo 7. Actualizaciones generales	19
lftp ahora maneja correctamente redirección 302	19
Más información de diagnóstico y complementos renombrados para sosreport	19
Capítulo 8. Instalación y arranque	20
Configuración de red en initrd se corrige si la configuración de red está provista en Kickstart	20
Anaconda ahora soporta la creación de volúmenes lógicos en memoria caché	20
Se mejoró el ordenamiento del menú de arranque GRUB2	20
Anaconda ahora revierte las acciones de disco cuando la selección de disco cambie	20
Se mejoró la detección de nombres de discos device-mapper	20
Se corrigió el manejo de PReP Boot durante el particionamiento	20
Particiones EFI en dispositivos RAID1	21
La instalación en modo texto ya no falla durante la configuración de red	21
Las pantallas en modo de rescate en IBM System z ya no se cortan	21
Complemento OpenSCAP en Anaconda	21
Anaconda ya no expira cuando espera el archivo kickstart en un CD o DVD	21
Capítulo 9. Kernel	23
Los parámetros de kernel SHMMAX y SHMALL retornaban valores predeterminados	23
Las páginas gigantes transparentes ya no corrompen la memoria	23
Rebase de SCSI LIO	23
makedumpfile ahora soporta el nuevo formato sadump que representa hasta 16 TB de memoria física	23
El retiro o actualización de kernel ya no muestra una advertencia	23
Nuevo paquete: libevdev	23
Tuned ahora puede ejecutarse en modo no-daemon	23
Nuevo paquete: tuned-profiles-realtime	24
Programación E/S de Multiqueue con blk-mq	24
Los mensajes de error SCSI ahora pueden interpretarse sin ningún problema	24
Los subsistemas y los controladores libATA han sido actualizados	24
FCoE y DCB han sido actualizados	25
rebase de perf a la versión 4.1	25
Soporte para TPM 2.0	25
Turbostat ahora proporciona salida correcta	25
Soporte para el procesador Intel Xeon v5	25
La herramienta zswap hace uso de la API zpool	25
La longitud del archivo /proc/pid/cmdline ahora es ilimitada	25
Ahora se proporciona soporte para dma_rmb y dma_wmb	25
Capítulo 10. Red	27
SNMP ahora obedece correctamente la directiva clientaddr en IPv6	27
tcpdump soporta las opciones -J, -j y --time-stamp-precision	27
Actualización de TCP/IP	27
Capítulo 11. Servidores y servicios	28
La directiva ErrorPolicy ahora está validada	28
CUPS ahora inhabilita el cifrado SSLv3 de forma predeterminada	28
Cups ahora permite el caracter de subrayado en los nombres de impresoras	28
Se retiró la dependencia innecesaria del paquete tftp-server	28

Ha sido retirado el archivo depreciado <code>/etc/sysconfig/conman</code>	28
Capítulo 12. Almacenamiento	29
Nuevas opciones <code>delay_watch_checks</code> y <code>delay_wait_checks</code> en el archivo <code>multipath.conf</code>	29
La nueva opción <code>config_dir</code> en el archivo <code>multipath.conf</code> .	29
Actualización DM	29
El nuevo comando <code>dmstats</code> muestra y maneja estadísticas de E/S para las regiones de dispositivos definidas para usuarios, que usan el controlador <code>device-mapper</code> .	29
Soporte para DIX en hardware especificado	29
Caché LVM	30
Nueva política caché LVM/DM	30
LVM <code>systemID</code>	30
Capítulo 13. Sistema y Administración de suscripciones	32
PowerTOP ahora respeta los nombres de archivos de reporte <code>user-defined</code>	32
Se corrigieron los comandos <code>yum-config-manager</code>	32
Nuevo complemento <code>search-disabled</code> para YUM	32
Capítulo 14. Virtualización	33
Los buses root PCI root adicionales ahora reciben soporte mediante los dispositivos de puente PCI expander	33
<code>qemu-kvm</code> soporta eventos de trazado de apagado de máquina virtual	33
Intel MPX expuesto para el huésped	33
La extracción de volcado de memoria del huésped del núcleo <code>qemu-kvm</code>	33
<code>virt-v2v</code> is Fully Supported	33
Virtualización en IBM Power Systems	33
Soporte <code>VirtIO-1</code>	33
Soporte Hyper-V TRIM	33
Capítulo 15. Red Hat Software Collections	35
Parte II. Muestras de tecnología	36
Capítulo 16. Autenticación	37
Uso de los proveedores <code>sudo</code> AD y LDAP	37
Capítulo 17. Sistemas de archivos	38
OverlayFS	38
Soporte para clientes NFSv4 con distribución de archivos flexible	38
NFS en RDMA	38
Sistema de archivos <code>btrfs</code>	38
Capítulo 18. Habilitación de hardware	40
Soporte para tarjetas OSA-Express5s en <code>qethqoat</code>	40
Instrumentación de tiempo Runtime para IBM System z	40
Adaptadores LSI Syncro CS HA-DAS	40
Capítulo 19. Kernel	41
Soporte para CPU múltiple en <code>kdump</code> en sistemas AMD64 e Intel 64	41
La herramienta <code>criu</code>	41
Espacio de nombre de usuario	41
LPAR Watchdog para IBM System z	41
Actualizaciones dinámicas de kernel con <code>kpatch</code>	41
<code>i40evf</code> maneja grandes reinicializaciones	41
Capítulo 20. Redes	43
Actualización de controlador de adaptador de servidor Ethernet Intel X710/XL710	43
Salida <code>ethtool</code> precisa	43

Controlador Cisco usNIC	43
Controlador de kernel Cisco VIC	43
Conexión de red confiable	43
Funcionalidad SR-IOV en el controlador qlcnic	43
Capítulo 21. Almacenamiento	44
Programación de E/S de colas múltiples para SCSI	44
Se mejoró la infraestructura de bloqueo LVM	44
El complemento de destino de libStorageMgmt API	44
DIF/DIX	44
destino dm-era device-mapper	44
Capítulo 22. Virtualización	45
Virtualización anidada	45
La herramienta virt-p2v	45
Soporte USB 3.0 para huéspedes KVM	45
Parte III. Controladores de dispositivos	46
Capítulo 23. Actualización de controlador de almacenamiento	47
Capítulo 24. Actualizaciones de controladores de red	48
Capítulo 25. Controlador gráfico y varias actualizaciones de controladores	49
Parte IV. Problemas conocidos	50
Capítulo 26. Compilador y herramientas	51
Múltiples errores al arrancar de SAN por FCo2	51
Valgrind no puede ejecutar programas contruidos con una versión anterior de Open MPI	51
Capítulo 27. Escritorio	52
Las dependencias del paquete Broken pygobject3 impiden la actualización de Red Hat Enterprise Linux 7.1	52
Capítulo 28. Actualizaciones generales	53
Los nuevos nombres de dispositivos pueden interrumpir la conexión de red	53
Capítulo 29. Instalación y arranque	54
La instalación en modo texto ya no se daña durante la configuración de red	54
Posible mensaje de error NetworkManager durante la instalación	54
La instalación Atomic Host ofrece cryptsetup aunque no está disponible	54
El instalador solamente puede agregar almacenamiento avanzado la primera vez que se entra el spoke de almacenamiento.	54
Capítulo 30. Kernel	55
Algunos sistemas de archivos ext4 no se pueden redimensionar	55
La pérdida de conexión con destinos iSCSI activados iSER	55
Comando de E/S de llamadas mid-layer SCSI hasta forzar el apagado del sistema	55
El certificado de la llave pública Red Hat Beta necesita ser cargado manualmente	55
Capítulo 31. Redes	56
La política de apagado no está habilitada en el kernel de	56
Capítulo 32. Sistema y Administración de suscripciones	57
Registro incompleto en caso de un error	57
El botón Atrás en el complemento del Gestor de suscripción para arranque inicial	57

Capítulo 33. Virtualización	58
Navegación de GRUB 2 problemática con KVM	58
El reajuste de tamaño de los discos de la Tabla de particiones GUID (GPT) en huéspedes Hyper-V, produce errores en la tabla de particiones	58
Apéndice A. Versiones de componentes	59
Apéndice B. Historia de revisiones	60

Prefacio

Los lanzamientos menores de Red Hat Enterprise Linux son una adición a las mejoras individuales, mejoras de seguridad y de corrección de erratas. Las *Notas de lanzamiento de Red Hat Enterprise Linux 7.2* documentan los cambios principales hechos al sistema operativo Red Hat Enterprise Linux 7, las aplicaciones que lo acompañan para este lanzamiento menor, los problemas conocidos y una lista completa de todas las Muestras de tecnología disponibles.

Las funcionalidades y límites de Red Hat Enterprise Linux 7 con respecto a otras versiones del sistema están disponibles en el artículo de la base de conocimientos en <https://access.redhat.com/articles/rhel-limits>.

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

Capítulo 1. Arquitecturas

Red Hat Enterprise Linux 7.2 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] Observe que la instalación de Red Hat Enterprise Linux 7.2 es compatible únicamente en hardware de 64 bits. Red Hat Enterprise Linux 7.2 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 7.2 (little endian) únicamente tiene soporte actualmente como huésped de KVM en hipervisores **Red Hat Enterprise Virtualization for Power** y **PowerVM**

[3] Observe que Red Hat Enterprise Linux 7.2 soporta hardware IBM zEnterprise 196 o posterior; los sistemas para computadora central IBM System z10 ya no reciben soporte y no arrancarán Red Hat Enterprise Linux 7.2.

Parte I. Nuevas funcionalidades

Esta parte describe nuevas funcionalidades y mejoras importantes introducidas en Red Hat Enterprise Linux 7.2.

Capítulo 2. Autenticación

ca-certificate rebase a versión 2.4

El paquete `ca-certificate` ha sido actualizado a la versión 2.4, la cual proporciona una serie de correcciones de errores y mejoras de la versión anterior. En particular, `ca-certificate` ahora contiene las siguientes modificaciones:

Mozilla había retirado la confianza de varias certificaciones CA de legado que contienen llaves RSA de 1024 bits. Esta versión de paquete `ca-certificate` modifica la lista de Mozilla para mantener de forma continua estos certificados CA de legado confiables. Estas modificaciones se han realizado para garantizar la compatibilidad con implementaciones PKI existentes y con software basado en OpenSSL o GnuTLS.

El paquete `ca-certificate` ahora incluye el comando **`ca-legacy`**, el cual puede utilizarse para inhabilitar las modificaciones de compatibilidad mencionadas. Consulte la página de manual `ca-legacy(8)` para obtener más información sobre cómo usar el comando.

Se aconseja a los usuarios que piensen hacer modificaciones de legado que consulten en la base de conocimientos el artículo 1413643, el cual proporciona información sobre estas modificaciones y las consecuencias de inhabilitarlas.

Observe que se requiere el uso de almacén CA unificado para poder usar el comando **`ca-legacy`**. Consulte la página de manual `update-ca-trust(8)` para saber cómo habilitar el almacén CA unificado.

Soporte para confianzas unidireccionales

Administración de identidades ahora permite al usuario configurar una confianza unidireccional con el comando **`ipa trust-add`**.

openldap rebase a la versión 2.4.40

Los paquetes `openldap` han sido actualizados a la versión 2.4.40 de la línea de desarrollo principal, la cual ofrece una serie de correcciones y una mejora de la versión anterior. Principalmente, se han agregado reglas de ORDENAMIENTO correspondientes a las descripciones del tipo de atributo **`ppolicy`**. Entre las correcciones está que el servidor ya no termina de forma inesperada cuando procesa los registros SRV y se ha agregado la información que faltaba de **`objectClass`**, lo cual permite al usuario modificar la configuración front-end a través de medios estándar.

Autenticación caché en SSSD

Ahora está disponible en SSSD la autenticación en caché sin intento de reconexión, incluso en modo desconectado. La autenticación directa del servidor de red de forma repetitiva podía ocasionar excesiva latencia de aplicaciones, lo cual podría hacer que el proceso de inicio fuera demasiado prolongado.

SSSD permite el mapeo de UID y GID sobre clientes individuales

Ahora es posible asociar usuarios a diferentes UID y GID en clientes Red Hat Enterprise Linux específicos, a través de configuración del lado del cliente mediante SSSD. Esta posibilidad de lado del cliente puede resolver problemas ocasionados por duplicación de UID y GID.

SSSD ahora puede negar acceso a SSH a cuentas bloqueadas

Anteriormente, cuando SSSD usaba OpenLDAP como base de datos de autenticación, los usuarios podían autenticarse en el sistema con una llave SSH, incluso si la cuenta de usuario estaba bloqueada. El

parámetro **ldap_access_order** ahora acepta el valor **ppolicy**, el cual puede negar el acceso a SSH para el usuario en la situación descrita. Para obtener más información sobre el uso de **ppolicy**, consulte la descripción **ldap_access_order** en la página de manual `sssd-ldap(5)`.

La herramienta sudo ahora puede verificar el comando checksum

La configuración de la herramienta sudo almacena la suma de verificación del comando o script autorizado. Al volver a ejecutar el comando o el script, la suma de verificación es comparada con la suma de verificación almacenada para chequear si ha habido cambios. Si el comando o binario cambia, la herramienta sudo se rehusará a ejecutar el comando o registrará una advertencia.

Soporte SSSD para tarjeta inteligente

SSSD ahora soporta tarjetas inteligentes para autenticación local. Con esta funcionalidad, el usuario puede usar una tarjeta inteligente para entrar al sistema mediante una consola de texto o una consola gráfica, como también servicios locales tales como el servicio sudo. El usuario coloca la tarjeta inteligente en el lector y proporciona el nombre de usuario y el PIN de tarjeta inteligente en el indicador de inicio. Si el certificado en la tarjeta inteligente es verificado, el usuario se habrá autenticado correctamente.

Observe que SSSD no autoriza al usuario de forma concurrente para adquirir un tique de kerberos mediante una tarjeta inteligente. Para obtener un tique kerberos, el usuario aun debe autenticarse mediante la herramienta kinit.

Múltiples certificados para soporte de perfiles

El Administrador de identidades ahora soporta múltiples perfiles para otorgar certificados en lugar de ofrecer soporte únicamente de un solo perfil de certificado para un servidor. Los perfiles se almacenan en el Sistema de certificados.

Contraseña Vault

Ha sido agregada una nueva funcionalidad para permitir almacenamiento central seguro de la información privada de usuario, tales como contraseñas y llaves públicas. La contraseña Vault se crea por encima del subsistema de Autoridad de recuperación de llaves (PKI) de la infraestructura de llave pública (PKI).

Soporte DNSSEC en Administración de identidades

Los servidores de Administración de identidades con el DNS integrado ahora soportan Extensiones de seguridad DNS (DNSSEC), una conjunto de extensiones para DNS que mejoran la seguridad del protocolo DNS. Las zonas DNS alojadas en servidores de Administración de identidades pueden ser firmadas de forma automática con DNSSEC. Las llaves criptográficas se generan y rotan de forma automática.

Se aconseja a los usuarios que decidan proteger sus zonas DNS con DNSSEC que consulten los siguientes documentos:

DNSSEC Operational Practices, Version 2: <http://tools.ietf.org/html/rfc6781#section-2>

Secure Domain Name System (DNS) Deployment Guide: <http://dx.doi.org/10.6028/NIST.SP.800-81-2>

Observe que los servidores de Administración de identidades con DNS integrado usan DNSSEC para validar preguntas DNS obtenidas desde otros servidores DNS. Esto podría afectar la disponibilidad de zonas DNS que no están configuradas según las prácticas de denominación descritas en Red Hat Enterprise Linux Networking Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices

Proxy Kerberos HTTPS en Administración de identidades

En Administración de identidades ahora está disponible una función proxy del Centro de distribución de llaves (KDC), que interopera con la implementación de Microsoft Kerberos KDC Proxy Protocol (MS-KKDCP) y permite a los clientes acceder mediante HTTPS al KDC y a los servicios **kpasswd**. Los administradores de sistemas ahora pueden exponer, de extremo a extremo, el proxy en su red con una simple reversión del proxy HTTPS sin necesidad de configurar y administrar una aplicación dedicada.

Recarga del fondo de entradas en memoria caché

SSSD ahora permite que las entradas en caché sean actualizadas fuera de banda en segundo plano. Antes de esta actualización, cuando expiraba la validez de las entradas en caché, SSSD las buscaba desde el servidor remoto y las realmacenaba en una base de datos, lo cual consumía mucho tiempo. Gracias a esta actualización, las entradas retornan de forma instantánea porque el segundo plano las mantiene actualizadas en todo momento. Observe que esta acción produce una carga mayor en el servidor porque las descargas SSSD se efectúan periódicamente y no a solicitud.

Almacenamiento en caché para operaciones **initgroups**

La caché de memoria rápida SSSD ahora soporta las operaciones **initgroups**, lo cual mejora la velocidad del procesamiento **initgroups** y mejora el rendimiento de algunas aplicaciones, por ejemplo GlusterFS y **slapi-nis**.

Negociar autenticación simplificada con **mod_auth_gssapi**

Administración de identidades ahora usa el módulo **mod_auth_gssapi**, el cual usa llamadas GSSAPI en lugar de llamadas kerberos directas utilizadas por el módulo **mod_auth_kerb** utilizado anteriormente.

Funcionalidades de administración de ciclo de vida de usuario

La administración de ciclo de vida de usuario le brinda al administrador un mayor grado de control sobre la activación y desactivación de cuentas de usuarios. El administrador ahora puede aprovisionar nuevas cuentas de usuario agregándolas a una zona de tránsito sin activarlas completamente; activar las cuentas de usuario inactivas, o desactivarlas sin necesidad de borrarlas completamente de la base de datos.

Las funcionalidades de administración de ciclo de vida ofrecen importantes beneficios a un gran número de implementaciones IdM. Observe que los usuarios también pueden ser agregados directamente a la zona de tránsito desde un cliente LDAP estándar, mediante operaciones LDAP directas. Anteriormente, IdM solamente administraba usuarios a través de las herramientas de línea de comandos IdM o la interfaz de usuario web IdM.

Soporte SCEP en **certmonger**

El servicio **certmonger** ha sido actualizado para soportar el Protocolo de registro de certificado simple (SCEP). Ahora es posible expedir, renovar o reemplazar un certificado por SCEP.

Nuevos paquetes: **ipsilon**

El paquete *ipsilon* proporciona servicio de proveedor de identidad Ipsilon para autenticación única (SSO) federada. Ipsilon vincula proveedores de autenticación y aplicaciones o herramientas para permitir autenticación única. Incluye un servidor y herramientas para configurar los proveedores de servicios basados en Apache.

La autenticación de usuario SSO provista para Ipsilon se realiza en un sistema de Administración de identidades, tal como el servidor de Administración de identidades. Ipsilon se comunica con varias aplicaciones y herramientas a través de protocolos de federación, tales como SAML u OpenID.

NSS aumenta los valores de poder mínimos de llaves

La biblioteca de Servicios de Seguridad de Red (NSS) en Red Hat Enterprise Linux 7.2 ya no acepta parámetros de intercambio de llave Diffie-Hellman (DH) de menos de 768 bits, ni certificados RSA y DSA de menos de 1023 bits. El aumento de los valores de poder mínimos evita el aprovechamiento de vulnerabilidades conocidas como vulnerabilidades Logjam (CVE-2015-4000) y FREAK (CVE-2015-0204).

Observe que ahora fallan los intentos para conectarse a un servidor con llaves más débiles que los nuevos valores mínimos, aunque dichas conexiones funcionaban en versiones anteriores de Red Hat Enterprise Linux.

rebase ss y nss-util a la versión 3.19.1

Los paquetes *nss* y *nss-util* han sido actualizados a la versión 3.19.1 de la línea de desarrollo principal, la cual proporciona una serie de correcciones de errores de la versión anterior. En particular, la actualización le permite a los usuarios mejorar Mozilla Firefox 38 Extended Support Release y evita que los atacantes aprovechen la vulnerabilidad de seguridad Logjam CVE-2015-4000.

Módulos Apache para IdM ahora reciben total soporte

Ahora, los siguientes módulos Apache para Administración de identidad (IdM), agregados como muestra de tecnología en Red Hat Enterprise Linux 7.1, son totalmente aceptados: **mod_authnz_pam**, **mod_lookup_identity**, and **mod_intercept_form_submit**. Los módulos Apache pueden utilizarse mediante aplicaciones externas para efectuar una interacción más hermética con IdM superior a la autenticación simple.

Capítulo 3. Agrupamiento

systemd y pacemaker ahora se coordinan correctamente durante el apagado del sistema

Anteriormente, systemd y pacemaker no se coordinaban correctamente durante el apagado del sistema, lo cual hacía que los recursos de pacemaker no se finalizaran de forma adecuada. Gracias a esta actualización, se ordena a pacemaker que se detenga antes de dbus y otros servicios de systemd iniciados por pacemaker. Eso permite que tanto pacemaker como los recursos que pacemaker administra se apaguen de forma correcta.

Los comandos `pcs resource move` y `pcs resource ban` ahora muestran un mensaje de advertencia para aclarar la conducta de los comandos.

El comando `pcs resource move` y los comandos `pcs resource ban` crean restricciones de ubicación que evitan que el recurso se ejecute efectivamente en el nodo actual hasta que la restricción sea retirada o hasta que el tiempo de vida de la restricción expire. Esta conducta no se había aclarado a los usuarios. Ahora estos comandos presentan un mensaje de advertencia que explica esta conducta, y las pantalla de ayuda y documentación para que estos comandos han sido clarificados.

Nuevo comando para desplazar un recurso Pacemaker a su nodo preferido

Después de que el recurso Pacemaker haya sido desplazado, ya sea debido a que el recurso se ha desplazado, ya sea debido a conmutación o a que un administrador ha desplazado de forma manual un nodo, no necesariamente se devuelve a su nodo original incluso después de que las circunstancias hayan causado la conmutación hayan sido corregidas. Usted puede usar el comando `pcs resource relocate run` para desplazar un recurso a su nodo preferido, como está determinado por el estatus de clúster actual, las restricciones, la ubicación de recursos y otros parámetros. Usted también puede usar el comando `pcs resource relocate show` para desplegar los recurso migrados. Para obtener más información sobre estos comandos, consulte High Availability Add-On Reference.

Soporte para que el comando `cluftr` transforme y analice los formatos de configuración de clúster

El comando `cluftr` proporciona una herramienta para transformar y analizar formatos de configuración de clúster. El comando `cluftr` puede servir para ayudar a migrar desde la configuración de una pila anterior a una configuración más reciente que apalanque a Pacemaker. Para obtener más información sobre las funcionalidades del comando `cluftr`, consulte la página de manual `cluftr(1)` o entregue la salida del comando `cluftr -h`.

Capítulo 4. Compilador y herramientas

tail --follow ahora funciona correctamente en archivos sobre el Sistema de archivos Veritas Clustered (VXFS)

Sistema de archivos Veritas en clúster (VXFS) es un sistema de archivos remoto, y en sistemas de archivos remotos **tail** no puede usar la funcionalidad 'inotify' para modo '--follow'. El sistema de archivos Veritas en clúster ha sido agregado a la lista de sistemas de archivos remotos, para el cual se utiliza el modo de sondeo en lugar de 'inotify'. **tail --follow** ahora funciona correctamente, incluso en archivos sobre VXFS.

El comando dd ahora muestra el progreso de la transferencia

El comando **dd**, el cual se utiliza para copiar archivos por bytes, ahora proporciona la opción 'status=progress' para mostrar el progreso de la transferencia. Esto sirve para transferencias de grandes archivos debido a que permite al usuario calcular el tiempo restante y detectar los problemas potenciales con la transferencia.

Se mejoraron los tiempos de espera en libcurl

La biblioteca **libcurl** utilizaba una extensa demora que bloqueaba las acciones con descriptores de archivos activos, incluso en operaciones cortas. Esto significaba que algunas acciones, tales como la resolución de un nombre de host mediante **/etc/hosts**, tardaban mucho tiempo en completar. Ahora, el código de bloqueo en **libcurl** ha sido modificado para que la demora inicial sea corta y aumente gradualmente hasta que se presente un evento. Las operaciones **libcurl** rápidas ahora se completan de una forma más rápida.

La biblioteca libcurl ahora implementa un handshake SSL de no bloqueo

Anteriormente, la biblioteca **libcurl** no implementaba un handshake SSL de no bloqueo, el cual afectaba de forma negativa el rendimiento de las aplicaciones basadas en la API multi **libcurl**. Para resolver este problema, el handshake SSL de no bloqueo ha sido implementado en **libcurl**, y la API multi **libcurl** ahora retorna inmediatamente el control para la aplicación cuando no se puedan leer o escribir datos desde o hacia el socket de red subyacente.

GDB en IBM Power Systems ya no falla cuando se accede a la tabla de símbolos

Anteriormente, GDB en 64-bit IBM Power Systems desasignaba de forma incorrecta una variable importante que guardaba la tabla de símbolos para el binario en curso de depuración, lo que ocasionaba una falla de segmentación cuando GDB intentaba acceder a la tabla de acceso. Para resolver este problema, la variable específica se ha establecido a persistente, y GDB ahora puede acceder la información necesaria más adelante, durante la sesión de depuración, sin leer una región inválida de memoria.

nscd se actualizó para recargar de forma automática los datos de configuración

Esta actualización de Demonio de caché para el servicio de nombres (NSCD) agrega un sistema de monitorización basado en inotify y monitorización de copia de seguridad basada en stat para archivos de configuración nscd, por lo tanto, nscd ahora detecta correctamente los cambios hechos a su configuración y recarga los datos. Esto evita que nscd entregue datos desactualizados.

La función de biblioteca dlopen ya no se cuelga en llamadas recursivas.

Anteriormente un defecto en la función **dlopen** de la biblioteca podía ocasionar llamadas recursivas a esta función o dañarse o abortar con una aserción de biblioteca. Las llamadas recursivas se hacen posibles si una implementación **malloc** provista por el usuario llama a **dlopen**.

La implementación ahora es reentrante y las llamadas recursivas ya no se cuelgan o abortan con una confirmación.

La herramienta **operf** ahora reconoce los identificadores de páginas gigantes estáticas

Anteriormente, al perfilar el rendimiento de código compilado de Java 'justo a tiempo' (JIT) con páginas gigantes estáticas habilitadas, el comando **operf** de OProfile registraba una gran cantidad de muestras de eventos en memoria anónima (en `anon_hugepage`) en lugar de en el método Java apropiado. Gracias a esta actualización, **operf** reconoce los identificadores de páginas gigantes estáticas y asigna muestras a los métodos Java cuando se usan páginas gigantes asignadas estáticas.

El comando **rsync -X** ahora funciona correctamente

Anteriormente, la herramienta **rsync** cambiaba el propietario del archivo, sin antes, establecer los atributos de seguridad. Como consecuencia, faltaban los atributos de seguridad en el destino, y la ejecución del comando **rsync -X** no funcionaba correctamente en algunas circunstancias. En esta actualización, se ha cambiado el orden de las operaciones y ahora **rsync** cambia el propietario antes de establecer los atributos de seguridad. Como resultado, los atributos de seguridad están presentes como se esperaba en la situación descrita.

Los ejecutables **Subversion** ahora se integran totalmente con datos **RELRO**

Los ejecutables provistos con el paquete *subversion* ahora están integrados a los datos de reubicación de solo-lectura (RELRO), los cuales protegen de algunos tipos de ataques de corrupción de memoria. Como resultado, será más difícil atacar a Subversión si se descubren futuras vulnerabilidades.

La extensión de hilos en **TCL** ahora funciona correctamente

Anteriormente, el soporte de hilos en lenguaje de comandos de herramientas (TCL) no se implementaba de forma óptima. Si la llamada de bifurcación() no se usaba junto con la extensión del hilo habilitado en el intérprete TCL, el proceso no respondía más. Debido a esto, el intérprete TCL y la aplicación TK anteriormente se distribuían con la extensión de hilo inhabilitada. Como consecuencia, las aplicaciones de terceros que dependían de TCL en hilo o TK no funcionaban correctamente. Se ha implementado un parche para corregir este error y ahora TCL y TK tienen la extensión de hilos habilitada de forma predeterminada.

Capítulo 5. Escritorio

GNOME 3.14

Escritorio GNOME ha sido actualizado a la versión 3.14 de la línea de desarrollo principal, la cual incluye nuevas funcionalidades y mejoras. A saber:

Un número de funcionalidades ha sido agregada al protocolo de ventana **Wayland**, incluidos la configuración de teclado, el soporte a pantalla táctil, el soporte de arrastrar y soltar, los menús de contexto funcional, ayudas emergentes y cuadros combinados, soporte de pantalla de alta resolución y ventana de mover y redimensionar.

Gestos mutitáctiles ahora pueden utilizarse como pantallas táctiles para navegar el sistema, como también en aplicaciones. Los gestos pueden utilizarse para abrir la visión general de Actividades, la vista de Aplicaciones y la Bandeja de mensajes o también para cambiar de aplicación y espacio de trabajo.

GNOME 3.14 proporciona soporte para hotspots WIFI mejorados. Ahora al conectarse a un Portal Wi-Fi que requiere autenticación, GNOME muestra de forma automática la página de inicio como una parte del proceso de conexión.

La compartición personal de **archivos (WebDAV)**, **medios (DLNA)** y **pantalla (VNC)** ahora recuerdan la red que el usuario desea tener activa. También, Parámetros proporcionan la posibilidad de controlar las redes que puede compartir. Esta funcionalidad evita la compartición de contenido y servicios en espacios públicos.

Ahora cuando se utilizan varios monitores, GNOME 3.14 los restaura a su posición original cuando son desconectados y conectados nuevamente.

La aplicación de GNOME para máquinas virtuales y remotas, **Boxes** introduce las instantáneas. También, **Boxes** ahora provee descarga automática, ejecución de varios cuadros en ventanas individuales y mejoras de interfaz de usuario, incluidas la conducta de pantalla completa y miniaturas.

GTK+ 3.14 incluye una serie de correcciones y mejoras, tales como carga automática de menús, soporte de mutiselección en **GtkListBox**, vinculación de propiedades en archivos **GtkBuilder**, soporte para asignación de asistentes de dibujo (`gtk_widget_set_clip()`), nuevos tipos de transición en **GtkStack**, y carga y guardado de archivos con **GtkSourceView**. Además, **GTK+** ahora proporciona soporte para interacción de gestos. Gracias a 3.14, la mayoría de gestos multitáctiles están disponibles para ser utilizados en aplicaciones GTK+, p.ej., para pulsar, arrastrar, deslizar, pellizcar y rotar. Los gestos pueden añadirse a las aplicaciones existentes GTK+ mediante **GtkGesture**.

Glib 3.14 ahora proporciona soporte para la especificación de asociaciones de aplicaciones MIME, soporte SHA-512 en GHmac, soporte para implementaciones en archivos de escritorio y soporte unicode 7.0.

El navegador de documentación de **Ayuda** ha sido rediseñado para que sea consistente con otras aplicaciones GNOME 3. Ayuda ahora usa la barra de cabecera, tiene una función de búsqueda y una interfaz de marcado.

Una extensión shell de GNOME, **Looking Glass Inspector**, ha obtenido una serie de funcionalidades para desarrolladores: muestra todos los métodos, clases, etc. en un espacio de nombre tras la inspección, expansión de historial de la inspección de objetos o copia de los resultados de 'Looking Glass' como cadenas, y pasando eventos en `gnome-shell`.

El paquete ibus-gtk2 ahora actualiza el archivo immodules.cache

Anteriormente, el script **update-gtk-immodules** buscaba un directorio **/etc/gtk-2.0/\$host** que ya no existía. Como consecuencia, el script de posinstalación del paquete *ibus-gtk2* fallaba y salía sin crear o actualizar la memoria caché. Este problema ya no se presenta porque el script de posinstalación ha sido cambiado para remplazar a **update-gtk-immodules** por **gtk-query-immodules-2.0-BITS**.

Capítulo 6. Sistemas de archivos

Rebase gfs2-utils a la versión 3.1.8

El paquete *gfs2-utils* ha sido rebasado a la versión 3.1.8, la cual proporciona correcciones y una serie de mejoras importantes:

- * Ha sido mejorado el rendimiento de las herramientas **fsck.gfs2**, **mkfs.gfs2**, y **gfs2_edit**.
- * La herramienta **fsck.gfs2** ahora realiza mejores revisiones de diarios, el jindex, inodos de sistemas y valores 'goal' de inodo.
- * Las herramientas **gfs2_jadd** y **gfs2_grow** son ahora dos programas independientes en lugar de enlaces simbólicos para **mkfs.gfs2**.
- * Han sido mejorados el grupo de paquetes y la documentación relacionada.
- * El paquete ya no depende de Perl.

GFS2 ahora evita que los usuarios se excedan en sus cuotas

Anteriormente, GFS2 solamente revisaba las violaciones de cuotas después de completar operaciones, lo cual hacía que los usuarios o grupos se excedieran en las cuotas asignadas. Esta conducta ha sido corregida y ahora GFS2 predice el número de bloques que una operación asignaría y revisa si al asignarlas ha ocurrido una violación de cuotas. Las operaciones que resulten como violaciones de cuotas se rechazan, y de esta forma, los usuarios nunca excederán sus cuotas asignadas.

Rebase XFS la versión 4.1

XFS ha sido actualizado a la versión de la corriente principal de desarrollo 4.1 incluidas correcciones de errores menores, refactorizaciones, y el retrabajo de ciertos mecanismos internos tales como registro, contabilidad pcpu y el nuevo bloqueo mmap. Además de los cambios de la corriente de desarrollo principal, esta actualización extiende la función `rename()` para agregar `cross-rename` (una variante simétrica de `rename()`) y el manejo de `whiteout`.

Actualización de ext4 y jbd2

Los dispositivos ext4 y jbd2 han sido actualizados a la versión más reciente de la corriente principal de desarrollo, la cual proporciona correcciones de errores y mejoras con respecto a la versión anterior.

cifs se rebasa a la versión 3.17

El módulo CIFS ha sido actualizado a la versión de la corriente principal de desarrollo 3.17, la cual provee correcciones y funcionalidades para Server Message Block 2 y 3 (SMB2 y SMB3).

Capítulo 7. Actualizaciones generales

Iftp ahora maneja correctamente redirección 302

Iftp ha sido actualizado para manejar correctamente redirección 302 durante la ejecución en modo de espejo. Anteriormente Iftp se detenía con un error.

Más información de diagnóstico y complementos renombrados para sosreport

La herramienta sosreport ha sido mejorada para recolectar la información relacionada con el proceso desde varias aplicaciones, incluidas ptp, lastlog, y ethtool. Como parte de este cambio, el complemento **startup** ha sido renombrado como **services** para comunicar mejor su función.

Capítulo 8. Instalación y arranque

Configuración de red en `initrd` se corrige si la configuración de red está provista en Kickstart

Anteriormente el instalador no podía configurar o reconfigurar las interfaces de red en `initrd`, si estas interfaces se definían en archivos Kickstart. Esto hacía que la instalación fallara y que entrara en modo de emergencia si otros comandos en el archivo Kickstart requerían acceder a la red.

Este problema ha sido resuelto y Anaconda ahora maneja adecuadamente la configuración de redes a partir de archivos Kickstart en `initrd`, desde el comienzo del proceso de arranque.

Anaconda ahora soporta la creación de volúmenes lógicos en memoria caché

El instalador ahora soporta la creación de volúmenes lógicos LVM en caché y la instalación de estos volúmenes en el sistema.

Actualmente, este enfoque solamente es compatible en Kickstart. Para crear un volumen lógico, use las nuevas opciones del comando Kickstart `--cachevps=`, `--cachesize=`, y `--cachemode=` options of the `logvol`.

Consulte la Guía de instalación Red Hat Enterprise Linux 7 para obtener información detallada sobre estas nuevas opciones.

Se mejoró el ordenamiento del menú de arranque GRUB2

Un problema con el mecanismo de ordenamiento utilizado por el comando `grub2-mkconfig` podría hacer que el archivo de configuración `grub.cfg` sea generado con kernel disponibles organizados de forma incorrecta.

GRUB2 ahora usa el paquete `rpmdevtools` para ordenar los kernel disponibles y el archivo de configuración se genera correctamente con la versión más reciente listada en la parte superior.

Anaconda ahora revierte las acciones de disco cuando la selección de disco cambie

Anteriormente, Anaconda y Blivet no revertían acciones programadas en discos cuando se cambiaba la selección del disco. En esta actualización Anaconda ha sido corregida para crear una instantánea de la configuración de almacenamiento original y retornarla cuando la selección de disco cambie, de ese modo se revierten completamente todas las acciones programadas para discos.

Se mejoró la detección de nombres de discos `device-mapper`

En el lanzamiento anterior de Red Hat Enterprise Linux 7, el instalador podía dañarse durante la instalación en discos los cuales contenían volúmenes lógicos LVM y los metadatos para estos volúmenes aún permanecían. El instalador no reconocía los nombres de `device-mapper` y el proceso de creación de volúmenes lógicos LVM fallaba.

El método para obtener nombres de dispositivos `device-mapper` ha sido actualizado y la instalación en discos que contenían metadatos LVM existentes ahora es más confiable.

Se corrigió el manejo de `PRéP Boot` durante el particionamiento

En algunas circunstancias, la partición `PRéP Boot` en sistemas IBM Power Systems se establecía a un tamaño inválido durante la personalización de las particiones. En esa situación, el retiro de cualquier

partición hacía que el instalador fallara.

Las revisiones ahora se implementan en *anaconda* para garantizar que la partición siempre se divida de forma correcta entre **4096 KiB** y **10 MiB**. Además, ya no es necesario cambiar el formato del orden de la partición **PreP Boot** para cambiar su tamaño.

Particiones EFI en dispositivos RAID1

El sistema de particiones EFI ahora puede ser creado en un dispositivo RAID1, esto es para habilitar la recuperación del sistema cuando un disco de arranque falla. Sin embargo, si el comando **Boot####** y **BootOrder**, y el volumen del ESP que es descubierto por el firmware se corrompen, pero aún parece ser un ESP válido, la orden de arranque no se recreará automáticamente. Sin embargo, el sistema debe arrancar de forma manual desde el segundo disco.

La instalación en modo texto ya no falla durante la configuración de red

Anteriormente, en la pantalla de Configuración de red con el instalador en modo de texto interactivo, el uso del espacio durante la especificación de servidores de nombre hacía que el instalador dejara de funcionar.

Anaconda ahora maneja correctamente espacios en definiciones de servidor de nombre y el instalador ya no falla si se utiliza un espacio para separar direcciones de servidores de nombre por separado.

Las pantallas en modo de rescate en IBM System z ya no se cortan

Anteriormente, la segunda y tercera pantalla en modo de rescate en servidores IBM System z se desplegaban de forma inadecuada y las partes de la interfaz se cortaban. El modo de rescate en esta arquitectura ha sido mejorado y todas las pantallas ahora funcionan correctamente.

Complemento OpenSCAP en Anaconda

Ahora es posible aplicar un contenido de Protocolo de automatización de contenido (SCAP) durante el proceso de instalación. Este nuevo complemento de instalador proporciona una forma fácil y confiable para configurar una política de seguridad sin tener que depender de scripts personalizados.

Este complemento proporciona una nueva sección de Kickstart ("%addon org_fedora_oscaps") y una nueva pantalla en la interfaz de usuario gráfica durante una instalación interactiva. Todas estas tres partes se documentan en la Guía de instalación Red Hat Enterprise Linux 7.

La aplicación de una política de seguridad durante la instalación realizará varios cambios durante e inmediatamente después de la instalación, según la política que usted habilite. Si se selecciona un perfil, el paquete *openscap-scanner* (una herramienta de examen de cumplimiento OpenSCAP) se agrega a la selección de su paquete y se realiza un escán de cumplimiento inicial después de que la instalación finalice. Los resultados de este escán se guardan en **/root/openscap_data**.

Se proporcionan varios perfiles en los medios de instalación mediante el paquete *scap-security-guide*. También puede cargar otro contenido como una cadena de datos, archivo o un paquete RPM desde un servidor HTTP, HTTPS o FTP si es necesario.

Observe que la aplicación de la política de seguridad no es necesaria en todos los sistemas. Este complemento solamente puede usarse cuando se ordena en las reglas de la organización o en los lineamientos del gobierno, de lo contrario el complemento puede dejarse en su estado predeterminado, el cual no aplica ninguna política de seguridad.

Anaconda ya no expira cuando espera el archivo kickstart en un CD o DVD

Anteriormente, si Anaconda se configuraba para cargar un archivo Kickstart desde un medio óptico mediante el comando **inst.ks=cdrom:/ks.cfg** y el sistema también se arrancaba desde un CD o DVD, el instalador esperaría un corto tiempo hasta que usted cambiara el disco. Esta ventana de tiempo era demasiado corta, solamente se predeterminaba a 30 segundos. Después de este tiempo de expiración, el sistema entraba en modo de emergencia.

Anaconda ha sido modificado para que el tiempo de espera nunca expire y para que el usuario proporcione un archivo Kickstart en un CD o DVD. Si las opciones de arranque **inst.ks=cdrom** que se utilizan en el archivo Kickstart no se detectan, Anaconda despliega un indicador y espera hasta proporcionar el archivo o volver a arrancar.

Capítulo 9. Kernel

Los parámetros de kernel SHMMAX y SHMALL retornaban valores predeterminados

Anteriormente, los valores de los parámetros `kernel.shmmax` y `kernel.shmall`, los cuales se establecían en el archivo `/usr/lib/sysctl.d/00-system.conf`, eran demasiado bajos. Como consecuencia, algunas aplicaciones, tales como SAP, no podían funcionar adecuadamente. Los valores inapropiados se han retirado y ahora se utilizan los predeterminados del kernel, los cuales son lo suficientemente altos.

Las páginas gigantes transparentes ya no corrompen la memoria

Las páginas gigantes transparentes no se sincronizaban correctamente durante las operaciones de lectura y escritura. En algunas circunstancias, la memoria se dañaba cuando se habilitaban las páginas gigantes transparentes. Se han agregado barreras de memoria al manejo de las páginas gigantes transparentes de memoria para que esta corrupción de memoria ya no se presente.

Rebase de SCSI LIO

El destino de kernel SCSI, LIO, ha sido rebasado desde Linux-4.0.stable. Esto no solamente incluye muchas correcciones de errores, las más importantes para iSER, sino también soporte agregado para comandos XCOPY, WRITE SAME, y ATS; y soporte de integridad de datos, DIF.

makedumpfile ahora soporta el nuevo formato sadump que representa hasta 16 TB de memoria física

El comando `makedumpfile` ahora es compatible con el nuevo formato `sadump` que representa más de 16 TB de espacio de memoria física. Permite que los usuarios de `makedumpfile` leer los archivos de volcado mayores de 16 TB, generados por `sadump` en próximos modelos de servidor.

El retiro o actualización de kernel ya no muestra una advertencia

El script `weak-modules`, el cual es utilizado por `kmod` para administrar enlaces simbólicos de módulo kABI-compatible, retiraba el directorio `/lib/modules/<version>/weak-updates` cuando retiraba los archivos asociados al kernel. Este directorio pertenece al paquete `kernel` y el retiro ocasionaba inconsistencias entre el sistema de archivos y el estado esperado por `rpm`. Esto producía una advertencia cada vez que se actualizaba o retiraba el kernel.

El script ha sido actualizado para retirar el contenido del directorio `weak-updates`, pero abandona al directorio mismo, y ya las advertencias no aparecen.

Nuevo paquete: libevdev

`Libevdev` es una biblioteca de nivel bajo para la interfaz de dispositivo de eventos de entrada del kernel Linux. Esto proporciona interfaces seguras para funcionalidades y eventos de procesos desde dispositivos. Las versiones actuales de `xorg-x11-drv-evdev` y `xorg-x11-drv-synaptics` requieren que esta biblioteca como dependencia.

Tuned ahora puede ejecutarse en modo no-daemon

Anteriormente, Tuned podía ejecutarse como demonio, lo cual podía afectar el rendimiento de sistemas pequeños debido a la huella digital de memoria del demonio Tuned. Gracias a esta actualización, el modo no-daemon (one shot), el cual no requiere ningún residente en memoria, ha sido agregado en Tuned. El modo no-daemon es inhabilitado de forma predeterminada porque en este modo falta mucha funcionalidad de Tuned.

Nuevo paquete: tuned-profiles-realtime

El paquete *tuned-profiles-realtime* ha sido agregado a Red Hat Enterprise Linux Server y Red Hat Enterprise Linux para Real Time. Contiene un perfil realtime utilizado por la herramienta **tuned** para realizar aislamiento de CPU y ajuste IRQ. Cuando el perfil ha sido activado, lee una sección de variables, la cual especifica las CPU que deben ser aisladas y desplaza todos los hilos que puedan retirarse de esos núcleos de CPU.

Programación E/S de Multiqueue con blk-mq

Red Hat Enterprise Linux 7.2 incluye una nueva cola múltiple de mecanismo de programación E/S para dispositivos de bloques conocidos como blk-mq. Puede mejorar el rendimiento al permitir a algunos controladores asignar solicitudes de E/S a múltiples colas de hardware o software. El rendimiento mejorado surge de reducir la contención de bloqueo presente cuando los hilos múltiples de ejecución realizan E/S a un dispositivo individual. Los dispositivos más recientes, tales como Non-Volatile Memory Express (NVMe), se posicionan mejor para aprovechar esta funcionalidad debido a su soporte nativo para enviar múltiples colas de hardware y de colas de completado, y sus características de rendimiento de baja latencia. Las ganancias de rendimiento, como siempre, dependerán del hardware exacto y carga de trabajo.

La funcionalidad blk-mq se implementó actualmente y ahora se habilita de forma predeterminada, en los siguientes controladores: virtio-blk, mtip32xx, nvme, y rbd.

La funcionalidad relacionada, scsi-mq, le permite a los controladores de dispositivos SCSI ('Small Computer System Interface') el uso de la infraestructura blk-mq. La funcionalidad scsi-mq está provista como muestra previa de tecnología en Red Hat Enterprise Linux 7.2. Para habilitar scsi-mq, especifique **scsi_mod.use_blk_mq=y** en la línea de comandos de kernel. El valor predeterminado es **n** (inhabilitado).

El destino multirrutas del mapeador de dispositivos (DM), el cual usa DM request-based, también puede configurarse para usar la infraestructura blk-mq si se especifica la opción de kernel **dm_mod.use_blk_mq=y**. El valor predeterminado es **n** (inhabilitado).

Puede ser benéfico para establecer **dm_mod.use_blk_mq=y** si los dispositivos SCSI subyacentes también usan blk-mq, al hacerlo se reduce la carga de bloqueo en la capa DM.

Para determinar si las multirrutas DM están utilizando blk-mq en un sistema, ejecute el comando 'cat 'al archivo **/sys/block/dm-X/dm/use_blk_mq**, donde **dm-X** se reemplaza por el dispositivo multirrutas DM en cuestión. Este archivo es solamente de lectura y refleja el valor que había en **/sys/module/dm_mod/parameters/use_blk_mq** en el momento que se creó el dispositivo multirrutas DM.

Los mensajes de error SCSI ahora pueden interpretarse sin ningún problema

Anteriormente los cambios de kernel a la función printk() producían mensajes de error en SCSI que se registraban en múltiples líneas. Como consecuencia, si se presentaban múltiples errores en diferentes dispositivos, se dificultaba la interpretación correcta de mensajes de errores. Esta actualización cambia el código de registro de errores SCSI para registrar los mensajes de error mediante la opción dev_printk(), la cual asocia cada mensaje de error con el dispositivo que generaba el error.

Los subsistemas y los controladores libATA han sido actualizados

Esta actualización de mejoras proporciona una gran cantidad de correcciones de errores de los subsistemas y controladores libATA.

FCoE y DCB han sido actualizados

Los componentes de kernel de Canal de fibra por Ethernet (FCoE) y Puente de centro de datos (DCB) han sido actualizados a las versiones más recientes de la corriente principal, lo cual proporciona una gran cantidad de correcciones en comparación con las versiones anteriores.

rebase de perf a la versión 4.1

Los paquetes perf han sido actualizados a la versión 4.1 de la corriente de desarrollo principal, lo cual proporciona un correcciones respecto a rendimiento y estabilidad en comparación con la versión anterior. En particular, este rebase agrega las funcionalidades de Intel Cache QoS Monitoring y AMD IBS Ops y proporciona soporte para Intel Xeon v4, para módulos de kernel comprimidos, para eventos parametrizados y soporte para especificar la longitud del punto de interrupción. Además, se han agregado una cantidad de opciones a la herramienta perf, tales como **--system-wide**, **top -z**, **top -w**, **trace --filter-pids** y **trace --event**.

Soporte para TPM 2.0

Esta actualización agrega soporte a nivel de dispositivos a la versión 2.0 en cumplimiento con los dispositivos de Módulo de Plataforma Confiable (TPM).

Turbostat ahora proporciona salida correcta

Anteriormente, la herramienta turbostat detectaba si el sistema tenía el soporte para dispositivo MSR al leer el archivo `/dev/cpu/0/msr` para **cpu0** en lugar del **cpu**. Como consecuencia, al inhabilitar una CPU hacía que las CPU se borrarán de la salida turbostat. Este error ha sido corregido y la ejecución del comando **turbostat ls** ahora retorna la salida correcta.

Soporte para el procesador Intel Xeon v5

Esta mejora agrega soporte al procesador a la herramienta turbost.

La herramienta zswap hace uso de la API zpool

Anteriormente, la herramienta zswap usaba directamente zbud, un grupo de almacenamiento que guarda páginas comprimidas en una relación de 2:1 (cuando están llenas). Esta actualización introduce la API zpool, la cual provee acceso a grupos zbud o zsmalloc: zsmalloc almacena páginas comprimidas en una densidad en potencia más alta, lo cual requiere más memoria para páginas altamente comprimibles. En esta actualización, zsmalloc ha sido promovida a los controladores para que zpool funcione como se espera.

La longitud del archivo /proc/pid/cmdline ahora es ilimitada

La longitud del archivo `/proc/pid/cmdline` para el comando ps se fijaba a 4096 caracteres. Esta actualización garantiza que la longitud de `/proc/pid/cmdline` sea ilimitada, lo cual es muy útil, especialmente para procesos de listado con largos argumentos de línea de comandos.

Ahora se proporciona soporte para dma_rmb y dma_wmb

Esta actualización introduce actualizaciones a dos nuevos primitivos para sincronizar memoria coherente en caché de escritura y lectura, `dma_wmb()` y `dma_rmb()`. Esta funcionalidad estará disponible para uso

apropiado de controladores.

Capítulo 10. Red

SNMP ahora obedece correctamente la directiva `clientaddr` en IPv6

Anteriormente, la opción `clientaddr` en `snmp.conf` solamente afectaba mensajes salientes enviados por IPv4. Gracias a este lanzamiento, los mensajes de salida IPv6 se envían correctamente desde la interfaz especificada por `clientaddr`.

`tcpdump` soporta las opciones `-J`, `-j` y `--time-stamp-precision`

Ya que `kernel`, `glibc` y `libpcap` ahora proporcionan las API para obtener marcas de tiempo de resoluciones de nanosegundos, `tcpdump` ha sido actualizada para soportar esta funcionalidad. Los usuarios ahora pueden solicitar fuentes de marcas de tiempo que están disponibles (`-J`), establecer una fuente de marca de tiempo específica (`-j`), y solicitar marcas de tiempo con resolución especificada (`--time-stamp-precision`).

Actualización de TCP/IP

Los paquetes `squid` han sido actualizados a la versión 3.1.23 de la corriente principal de desarrollo, la cual proporciona correcciones de errores y mejoras con respecto a la versión anterior. Entre otras, esta actualización añade el soporte para las respuestas HTTP/1.1 POST y PUT sin ningún cuerpo de mensaje para `squid`. (BZ#999305)

Capítulo 11. Servidores y servicios

La directiva `ErrorPolicy` ahora está validada

La directiva de configuración `ErrorPolicy` no se validaba en el inicio, y se podía utilizar una política de error predeterminada imprevista sin una advertencia. Ahora, la directiva se valida en el inicio y restablece el valor predeterminado si el valor configurado es incorrecto. La política destinada se utiliza o de lo contrario, se registra un mensaje de advertencia.

CUPS ahora inhabilita el cifrado SSLv3 de forma predeterminada

Anteriormente, no era posible inhabilitar el cifrado SSLv3 en el programador CUPS, lo cual lo hacía vulnerable a ataques contra SSLv3. Para resolver este problema, la palabra clave `cupsd.conf` **SSLOptions** ha sido extendida para incluir dos nuevas opciones: **AllowRC4** y **AllowSSL3**, cada cual habilita la funcionalidad determinada en `cupsd`. Las nuevas opciones también reciben soporte en el archivo `/etc/cups/client.conf`. Ahora tanto RC4 como SSL3 se predeterminan como inhabilitadas para `cupsd`.

Cups ahora permite el caracter de subrayado en los nombres de impresoras

El servicio `cups` ahora permite incluir el caracter `character` (`_`) en nombres de impresoras locales.

Se retiró la dependencia innecesaria del paquete `tftp-server`

Anteriormente, el paquete adicional era instalado por el predeterminado durante la instalación del paquete `tftp-server`. Con esta actualización, se ha retirado la dependencia superflua de paquetes y el paquete innecesario ya no se instala de forma predeterminada durante la instalación de `tftp-server`.

Ha sido retirado el archivo depreciado `/etc/sysconfig/conman`

Antes de introducir el gestor `systemd`, se pueden configurar varios límites para servicios en el archivo `/etc/sysconfig/conman`. Después de migrar a `systemd`, `/etc/sysconfig/conman` ya no se utiliza y por lo tanto se ha retirado. Para establecer los límites y otros parámetros de demonio, tales como `LimitCPU=`, `LimitDATA=` o `LimitCORE=`, modifique el archivo `conman.service`. Para obtener más información, por favor consulte la página de manual `systemd.exec(5)`. Además se ha agregado una nueva variable `LimitNOFILE=10000` al archivo `systemd.service`. Esta variable está descomentada de forma predeterminada. Observe que después de hacer cambios a la configuración de `systemd`, debe ejecutar el comando `systemctl daemon-reload` para que los cambios se efectúen.

Capítulo 12. Almacenamiento

Nuevas opciones `delay_watch_checks` y `delay_wait_checks` en el archivo `multipath.conf`

Si la ruta no es fiable, como cuando la conexión se corta con frecuencia, `multipathd` aún seguirá intentando usar esa ruta. El tiempo de espera antes de que `multipathd` se de cuenta de que la ruta ya no es accesible es de 300 segundos, lo cual da la impresión de que `multipathd` se ha detenido.

Para corregir este error, se han agregado dos nuevas opciones de configuración: `delay_watch_checks` y `delay_wait_checks`. La opción `delay_watch_checks` establece el número de ciclos que `multipathd` debe vigilar la ruta hasta que se conecte en línea. Si la ruta falla bajo ese valor asignado, `multipathd` no la usará. `multipathd` confiará entonces en la opción `delay_wait_checks` para decirle cuántos ciclos consecutivos deben pasar antes de que la ruta se invalide nuevamente. Esto evita que las rutas que no son confiables sean utilizadas inmediatamente después de la reconexión en línea.

La nueva opción `config_dir` en el archivo `multipath.conf`.

Los usuarios eran capaces de dividir su configuración entre archivos `/etc/multipath.conf` y otros archivos de configuración. Esto evitaba que los usuarios configuraran el archivo de configuración principal para todas las máquinas y mantuviera la información de configuración en archivos independientes para cada máquina.

Para solucionar este problema, se ha agregado la opción `config_dir` en el archivo `multipath.conf`. Los usuarios deben cambiar la opción `config_dir` ya sea a una cadena vacía o a un nombre de ruta de directorio calificado. Cuando se establece algo diferente a una cadena vacía, `multipathd` leerá en orden alfabético todos los archivos `.conf`. Luego aplicará exactamente las configuraciones como si hubieran sido agregadas al archivo `/etc/multipath.conf`. Si no se hace este cambio, `config_dir` se predeterminará a `/etc/multipath/conf.d`.

Actualización DM

El mapeador de dispositivos (DM) ha sido actualizado a la versión 4.0 de la corriente principal de desarrollo, la cual proporciona una cantidad de correcciones de errores y mejoras con respecto a la versión anterior, incluidas una importante actualización de rendimiento DM crypt; actualización de DM core para soportar Multi-Queue Block I/O Queueing Mechanism (blk-mq).

El nuevo comando `dmstats` muestra y maneja estadísticas de E/S para las regiones de dispositivos definidas para usuarios, que usan el controlador device-mapper.

El comando **`dmstats`** proporciona soporte a userspace para estadísticas device-mapper I/O. Esto permite al usuario crear, manejar y reportar contadores de E/S, métrica e histograma de latencia para regiones de dispositivos device-mapper. Los campos de estadística ahora están disponibles en los reportes **`dmsetup`** y el comando **`dmstats`** agrega nuevos modos de reporte diseñados para usar con información de estadísticas. Para obtener más información sobre el comando **`dmstats`**, por favor consulte la página de manual `dmstats(8)`.

Soporte para DIX en hardware especificado

SCSI T10 DIX recibe soporte total en Red Hat Enterprise Linux 7.2, únicamente las siguientes HBAs y matrices de almacenamiento y no en LUN utilizadas para arrancar desde un entorno SAN. Además, T10 DIX recibe soporte en RHEL 7 solamente en hardware nativo, no en huéspedes virtualizados.

* EMULEX LPe16000/LPe16002

- * QLOGIC QLE2670/QLE2672
- * FUJITSU ETERNUS DX100 S3
- * FUJITSU ETERNUS DX200 S3
- * FUJITSU ETERNUS DX500 S3
- * FUJITSU ETERNUS DX600 S3
- * FUJITSU ETERNUS DX8100 S3
- * FUJITSU ETERNUS DX8700 S3
- * FUJITSU ETERNUS DX8900 S3
- * FUJITSU ETERNUS DX200F
- * FUJITSU ETERNUS DX60 S3

Soporte para DIX sigue en Muestra de tecnología para otros HBA y matrices de almacenamiento .

Observe que T10 DIX requiere base de datos o algún otro software que proporcione generación y revisiones de suma de verificación en bloques de discos. Ningún sistema de archivos Linux tiene esta funcionalidad.

Caché LVM

LVM caché ha recibido soporte total desde Red Hat Enterprise Linux 7.1. Esta funcionalidad le permite a los usuarios crear volúmenes lógicos (LVs) con un dispositivo rápido pequeño ejecutándose como una memoria caché para dispositivos grandes más lentos. Consulte la página de manual `lvmcache(7)` para obtener información sobre cómo crear volúmenes lógicos cache.

Observe las siguientes restricciones en el uso de caché LV:

*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.

* La LV sub-LV caché (la LV de origen, LV de metadatos, y el LV de datos) solamente pueden ser del tipo lineal, en bandas o RAID.

* Las propiedades de la memoria caché LV no se pueden cambiar después de crearlas. Para cambiar las propiedades caché, retire la caché como se describe en `lvmcache(7)` y vuélvala a crear con las propiedades deseadas.

Nueva política caché LVM/DM

Se ha escrito una nueva política `dm-cache smq` que reduce el consumo de memoria y mejora el rendimiento en la mayoría de los casos de uso. Ahora, esta nueva política caché es la predeterminada para los volúmenes lógicos LVM cache. Los usuarios que prefieran usar la política caché `mq` de legado aún pueden hacerlo al proveer un argumento `-cachepolicy` durante la creación del volumen lógico caché.

LVM systemID

Los grupos de volúmenes LVM ahora pueden asignarse a un propietario. El propietario de grupo de volúmenes es el ID de sistemas de un host. Únicamente el host con ID de sistema determinado puede usar el Grupo de volúmenes (VG). Esto puede beneficiar los grupos de volúmenes que existen en dispositivos compartidos, visibles a múltiples hosts, que de otra manera no estarían protegidos del uso simultáneo de

hosts múltiples. Los grupos de volúmenes LVM en dispositivos compartidos con un ID de sistema asignado solo pertenecen a un host y están protegidos de otros hosts.

Capítulo 13. Sistema y Administración de suscripciones

PowerTOP ahora respeta los nombres de archivos de reporte user-defined

Anteriormente, los nombres de archivo de reporte PowerTOP se generaban en una forma no muy clara y sin documentar. Con esta actualización, la implementación ha sido mejorada y los nombres de archivo ahora respetan los nombres solicitados por el usuario. Esto aplica tanto a reportes CSV como a reportes HTML.

Se corrigieron los comandos `yum-config-manager`

Anteriormente, la ejecución del comando `yum-config-manager --disable` inhabilitaba todos los repositorios configurados, mientras que el comando `yum-config-manager --enable` no habilitaba ninguno. Esta inconsistencia ha sido corregida. Los comandos `--disable` y `--enable` ahora requieren el uso de `*` en la sintaxis y `yum-config-manager --enable *` habilita los repositorios. Si ejecuta los comandos sin agregar `*` se imprime un mensaje que le pide al usuario ejecutar `yum-config-manager --disable *` o `yum-config-manager --enable *` si desea inhabilitar o habilitar los repositorios.

Nuevo complemento `search-disabled` para YUM

El complemento `search-disabled-repos` para YUM ha sido agregado a los paquetes de `subscription-manager`. Esta complemento permite a los usuarios completar operaciones YUM que fallan debido al repositorio fuente que está dependiendo en el repositorio inhabilitado. Cuando `search-disabled-repos` está instalado en el escenario descrito, YUM presenta instrucciones para habilitar temporalmente los repositorios inhabilitados y buscar las dependencias que faltan. Después de hacer las modificaciones necesarias para el archivo `/etc/yum/pluginconf.d/search-disabled-repos.conf`, la operación YUM puede reanudarse con los repositorios inhabilitados que se utilizan como si estuvieran habilitados.

Capítulo 14. Virtualización

Los buses root PCI root adicionales ahora reciben soporte mediante los dispositivos de puente PCI expander

A diferencia de los puentes PCI-PCI, un bus en un puente PCI expander puede ser asociado con un nodo NUMA, lo cual permite al sistema operativo de huéspedes reconocer la proximidad de un dispositivo a RAM y CPU. Con esta actualización, los dispositivos asignados pueden asociarse con el nodo NUMA correspondiente, lo cual produce un rendimiento óptimo.

qemu-kvm soporta eventos de trazado de apagado de máquina virtual

Se ha agregado soporte para eventos de trazado qemu-kvm durante el proceso de apagado del sistema de máquina virtual, el cual permite a los usuarios obtener diagnósticos detallados sobre solicitudes de apagado del sistema de huésped emitidas por el comando **virsh shutdown** o por la aplicación virt-manager. Esto proporciona a los usuarios capacidades mejoradas para aislar y depurar problemas de huéspedes durante el apagado.

Intel MPX expuesto para el huésped

Gracias a esta actualización, qemu-kvm permite que la funcionalidad de Extensiones de Protección de Memoria (MPX) sea expuesta al huésped. En los sistemas Intel 64 de host que soportan MPX, esto permite el uso de extensiones que proporcionan soporte de hardware para proteger límites en referencias de punteros.

La extracción de volcado de memoria del huésped del núcleo qemu-kvm

El script `dump-guest-memory.py` script ha sido introducido a QEMU, lo cual hace posible analizar un volcado de memoria de huésped del núcleo qemu-kvm en caso de que el kernel de huésped falle. Para obtener más información, ejecute el comando **help dump-guest-memory** para consultar el texto de ayuda.

virt-v2v is Fully Supported

Con Red Hat Enterprise Linux 7.2, la herramienta de línea de comandos virt-v2v ahora tiene soporte total. Esta herramienta convierte máquinas virtuales que se ejecutan en hipervisores foráneos para que se ejecuten en KVM. Actualmente, virt-v2v puede convertir Red Hat Enterprise Linux y huéspedes de Windows que se ejecutan en Red Hat Enterprise Linux 5 Xen and VMware vCenter.

Virtualización en IBM Power Systems

Red Hat Enterprise Linux con KVM recibe soporte en AMD64 y sistemas Intel 64, pero no en IBM Power Systems. Red Hat actualmente proporciona una solución POWER8-based con Red Hat Enterprise Virtualization para IBM Power Systems.

Para obtener más información sobre soporte de versión y procedimientos de instalación, consulte en la base de conocimientos, el artículo: <https://access.redhat.com/articles/1247773>

Soporte VirtIO-1

Los controladores Virtio han sido actualizados a Kernel 4.1 para proveer soporte de dispositivos VirtIO 1.0.

Soporte Hyper-V TRIM

Ahora es posible usar disco duro virtual Thin Provisioned Hyper-V (VHDX). La actualización añade soporte para reducir los archivos destacados VHDX para máquinas virtuales Microsoft Hyper-V al tamaño actual utilizado.

Capítulo 15. Red Hat Software Collections

Red Hat Software Collections es un conjunto de contenido de Red Hat de lenguajes de programación dinámicos, servidores de bases de datos y paquetes relacionados que usted 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 base de datos y otras herramientas distribuidas con Red Hat Software Collections no reemplazan las herramientas de sistema predeterminadas provistas en Red Hat Enterprise Linux, ni se prefieren a estas herramientas. Para proveer un set paralelo de paquetes, Red Hat Software Collections usa un mecanismo de paquetes alternativo basado en la herramienta **sc1**. Este set permite el uso opcional de versiones de paquetes alternativos en Red Hat Enterprise Linux. Al utilizar la herramienta **sc1**, los usuarios eligen la versión del paquete que desean ejecutar en cualquier momento.

Red Hat Developer Toolset hace ahora parte de Red Hat Software Collections. Se incluye 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.



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](#).

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

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

Parte II. Muestras de tecnología

Esta parte presenta una visión general de Muestras de tecnología introducidas o actualizadas en Red Hat Enterprise Linux 7.2.

Para más información sobre Red Hat Technology Previews, consulte <https://access.redhat.com/support/offerings/techpreview/>.

Capítulo 16. Autenticación

Uso de los proveedores sudo AD y LDAP

El proveedor Active Directory (AD) es un servidor de fondo utilizado para conectarse a un servidor AD. En Red Hat Enterprise Linux 7.2, el uso del proveedor sudo AD junto con el proveedor LDAP se acepta como una Muestra de tecnología. Para habilitar el proveedor sudo AD, agregue el parámetro **sudo_provider=ad** en la sección [domain] del archivo **sssd.conf**.

Capítulo 17. Sistemas de archivos

OverlayFS

OverlayFS es un tipo de sistema de archivos de unión. Permite al usuario **cubrir** un sistema de archivos con otro. Los cambios se registran en el sistema de archivos superior, mientras que el sistema de archivos inferior permanece sin modificar. Esto permite que múltiples usuarios compartan una imagen de sistema de archivos, como por ejemplo, un contenedor o un DVD-ROM, donde la imagen está en medios de solo lectura. Consulte el archivo de kernel Documentation/filesystems/overlayfs.txt para obtener más información.

OverlayFS permanece como una Muestra de tecnología en Red Hat Enterprise Linux 7.2 en la mayoría de circunstancias. Como tal, el kernel registrará advertencias cuando esta tecnología sea activada.

Soporte total está disponible para OverlayFS cuando se utilice con Docker con las siguientes restricciones:

- * OverlayFS solamente recibe soporte como un controlador Docker gráfico. Su uso únicamente puede recibir soporte para contenido de contenedor COW y no para almacenamiento persistente. Para que tenga soporte, todo almacenamiento persistente debe colocarse en volúmenes non-OverlayFS. Solamente puede usarse la configuración predeterminada de Docker, es decir, un nivel de cobertura overlay, y lowerdir, y los niveles superiores e inferiores que se encuentran en el mismo sistema de archivos).
- * En la actualidad, solamente XFS recibe soporte para usar como un sistemas de archivos de capa inferior
- * SELinux debe estar habilitado y en modo impositivo en la máquina física, pero debe estar inhabilitado en el contenedor al realizar la separación de contenedores; es decir, /etc/sysconfig/docker no debe contener --selinux-enabled. La corriente de desarrollo principal está desarrollando soporte SELinux para OverlayFS y se espera un lanzamiento futuro.
- * La ABI de kernel OverlayFS y la conducta del espacio de usuario no se consideran estables, y se verán cambios en futuras actualizaciones.

Observe que OverlayFS proporciona una serie de estándares POSIX. Pruebe su aplicación minuciosamente antes de implementarla con OverlayFS.

Existen también varios problemas asociados con OverlayFSA después del lanzamiento Red Hat Enterprise Linux 7.2. Para obtener más información, consulte **Non-standard behavior** en el archivo Documentation/filesystems/overlayfs.txt file.

Soporte para clientes NFSv4 con distribución de archivos flexible

Red Hat Enterprise Linux 7.2 agrega soporte para la distribución de archivos flexible en clientes NFSv4 . Esta tecnología permite funcionalidades avanzadas tales como movilidad de archivos sin interrupción y la copia en espejo del lado del cliente, lo cual proporciona mejoras en el uso en áreas tales como bases de datos , datos masivos y virtualización.

Consulte <https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/> para obtener información detallada sobre la distribución de archivos flexible NFS.

NFS en RDMA

El servicio NFSoRDMA se ofrece como Muestra de tecnología en Red Hat Enterprise Linux 7.2. Esto hace que el módulo svcrdma esté disponible para usuarios que pretenden usar transporte Acceso directo a memoria remota (RDMA) con el servidor NFS de Red Hat Enterprise Linux 7.

Sistema de archivos btrfs

El sistema de archivos Btrfs (B-Tree) recibe soporte como una Muestra de tecnología en Red Hat Enterprise Linux 7.2. Este sistema de archivos ofrece funcionalidades de gestión avanzada, confiabilidad, escalabilidad. Permite a los usuarios crear instantáneas, compresión y administración de dispositivos integrados.

Capítulo 18. Habilitación de hardware

Soporte para tarjetas OSA-Express5s en qethcoat

Se ha agregado soporte para tarjetas OSA-Express5s a la herramienta qethcoat, parte del paquete s390utils. Esta mejora extiende la capacidad de servicio de redes y configuración para tarjetas OSA-Express5s y se incluye como una Muestra de tecnología en Red Hat Enterprise Linux 7.2 sobre IBM System z.

Instrumentación de tiempo Runtime para IBM System z

Soporte para la funcionalidad de instrumentación Runtime está disponible como una Muestra de tecnología en Red Hat Enterprise Linux 7.2 sobre IBM System z. La instrumentación Runtime permite el análisis y ejecución avanzados para un número de aplicaciones disponibles de espacio de usuario con el sistema IBM zEnterprise EC12.

Adaptadores LSI Syncro CS HA-DAS

Red Hat Enterprise Linux 7.1 incluía código en el controlador megaraid_sas para habilitar adaptadores de Almacenamiento Avanzado de Alta Disponibilidad directa LSI Syncro CS (HA-DAS) . Mientras que el controlador megaraid_sas contaba con soporte total para adaptadores anteriormente habilitados, el uso de este controlador para Syncro CS está disponible como una Muestra de tecnología. LSI, su integrador de sistemas o su proveedor de sistema proporciona directamente soporte para este adaptador. Se invita a los usuarios que implementan Syncro CS en Red Hat Enterprise Linux 7.2 a hacer sus comentarios y sugerencias a a Red Hat y LSI. Para obtener más información, por favor consulte <http://www.lsi.com/products/shared-das/pages/default.aspx>.

Capítulo 19. Kernel

Soporte para CPU múltiple en kdump en sistemas AMD64 e Intel 64

En sistemas AMD64 e Intel 64, el mecanismo de volcado de memoria de kernel **kdump** ahora puede arrancar con más de una CPU habilitada. Esto resuelve el problema en sistemas con un tamaño de memoria grande en los que, debido a la gran cantidad de salida y entrada durante la creación de un volcado de kernel, Linux no podía asignar interrupciones a dispositivos cuando solo había una CPU habilitada ("maxcpus=1" o **nr_cpus=1**).

Para habilitar múltiples CPU en el kernel de fallos, proporcione el **nr_cpus=X** (donde **X** es el número de procesadores) y las opciones **disable_cpu_apicid=0** en la línea de comandos de kernel.

La herramienta criu

Red Hat Enterprise Linux 7.2 introduce la herramienta **criu** como una Muestra de tecnología. Esta herramienta implementa **Checkpoint/Restore en User-space** para congelar una aplicación en ejecución y almacenarla como una colección de archivos. Posteriormente, la aplicación puede restaurarse de su estado congelado.

La herramienta **criu** depende de **Protocol Buffers**, un mecanismo de lenguaje neutro, mecanismo extensible de plataforma neutra para serializar datos estructurados. Los paquetes *protobuf* y *protobuf-c*, los cuales proporcionan esta dependencia, también se agregan a Red Hat Enterprise Linux 7.2 como una Muestra de tecnología.

Espacio de nombre de usuario

Esta funcionalidad proporciona protección adicional a servidores que se ejecutan en contenedores Linux al proveer aislamiento entre el host y los contenedores. Los administradores de un contenedor ya no pueden realizar operaciones administrativas en el host, lo cual aumenta la seguridad.

LPAR Watchdog para IBM System z

Ahora está disponible un controlador de vigilancia mejorado para IBM System z como una Muestra de tecnología. Este controlador soporta Particiones lógicas Linux (LPAR) al igual que huéspedes de Linux en el hipervisor z/VM, y proporciona reinicio automático y funcionalidades de volcado automático si el sistema Linux no responde más.

Actualizaciones dinámicas de kernel con kpatch

La herramienta **kpatch** le permite a los usuarios administrar una colección de parches binarios de kernel, que pueden servir para parchear de forma dinámica el kernel sin necesidad de reiniciar. **kpatch** recibe soporte como una Muestra de tecnología y solo para arquitecturas AMD64 e Intel 64.

i40evf maneja grandes reinicializaciones

El tipo más común de reinicializaciones que la Función virtual (VF) encuentra es una reinicialización de la Función física (PF) que cae en cascada dentro de una reinicialización VF para cada VF. No obstante, para reinicializaciones mayores, tales como una reinicialización Core o EMP, cuando el dispositivo se reiniciaba, el VF no obtenía la misma VSI original, por lo tanto no era posible recuperar VF, ya que continuaba solicitando recursos para su VSI original. Como una Muestra de tecnología, esta actualización

agrega un estado adicional a la máquina de estado de cola de administración, para que el controlador pueda volver a solicitar su información de configuración en tiempo de ejecución. Durante la recuperación de reinicialización, esta parte se define en el campo `aq_required`, y la información de configuración se recupera antes de intentar reactivar el controlador.

Capítulo 20. Redes

Actualización de controlador de adaptador de servidor Ethernet Intel X710/XL710

Los controladores de kernel i40e e i40evf han sido actualizados a la versión 1.3.4-k. Estos controladores actualizados se incluyen como una Muestra previa de tecnología en Red Hat Enterprise Linux 7.2.

Salida ethtool precisa

Las funcionalidades de solicitud de redes de la herramienta ethtool han sido mejoradas en la Muestra de tecnología para Red Hat Enterprise Linux 7.2 sobre IBM System z. Por consiguiente, al usar hardware compatible con las solicitudes mejoradas, ethtool ofrece opciones de monitorización mejorada, y despliega parámetros de tarjeta de redes y valores de una forma más precisa.

Controlador Cisco usNIC

Los servidores del Gestor de comunicaciones unificadas Cisco (UCM) tienen una funcionalidad opcional para proporcionar un Controlador de interfaz de redes de espacio de usuario (usNIC), que permite operaciones similares al Acceso directo a memoria remota (RDMA) para aplicaciones de espacio de usuario. El controlador libusnic_verbs, el cual recibe soporte como una Muestra de tecnología, hace posible el uso de dispositivos usNIC vía programación InfiniBand RDMA estándar basada en los Verbs API.

Controlador de kernel Cisco VIC

El controlador de kernel Cisco VIC Infiniband, el cual recibe soporte como una Muestra previa de tecnología, permite usar un directorio de acceso de memoria remota (RDMA)-como semántica en arquitecturas Cisco de propietario.

Conexión de red confiable

Trusted Network Connect, soportada por una Muestra previa de tecnología. NAC se utiliza con soluciones NAC (Control de acceso de red), tales como TLS, 802.1X o IPsec para integrar la postura de evaluación 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). Trusted Network Connect, 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 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. Otra funcionalidad en el controlador qlcnic permanece con soporte total.

Capítulo 21. Almacenamiento

Programación de E/S de colas múltiples para SCSI

Red Hat Enterprise Linux 7.2 incluye un nuevo mecanismo de programación de E/S de colas múltiples para dispositivos de bloque conocidos como blk-mq. Este paquete `scsi-mq` permite que el subsistema de la Interfaz de Sistemas de Computadores Pequeños (SCSI) utilice el nuevo mecanismo de colas. Esta funcionalidad se ofrece como una Muestra de tecnología y no se habilita de forma predeterminada. Para habilitarla, agregue `scsi_mod.use_blk_mq=Y` a la línea de comandos de kernel.

Se mejoró la infraestructura de bloqueo LVM

lvmlockd no es una infraestructura de bloqueo de siguiente generación para LVM. Permite que LVM administre correctamente el almacenamiento compartido desde múltiples hosts, mediante los gestores de bloqueo **dlm** o **sanlock**. **sanlock** permite a **lvmlockd** coordinar hosts a través del bloqueo basado en almacenamiento, sin necesidad de una infraestructura de clúster completa. Para obtener más información, consulte la página de manual ``lvmlockd'(8)`.

El complemento de destino de libStorageMgmt API

A partir de Red Hat Enterprise Linux 7.1, la administración de matrices de almacenamiento con `libStorageMgmt`, una API independiente de matrices de almacenamiento, está totalmente soportada. La API provista es estable, consistente y permite a los desarrolladores administrar de forma programática diferentes matrices de almacenamiento y utilizar las funcionalidades aceleradas de hardware. Los administradores de sistemas también pueden usar `libStorageMgmt` para configurar el almacenamiento de forma manual y automatizar las tareas administrativas de almacenamiento con la interfaz de línea de comandos.

El complemento `Targetd` plug-in no recibe soporte total y permanece como Muestra de tecnología.

DIF/DIX

DIF/DIX es una adición nueva para SCSI Standard. Recibe soporte total en Red Hat Enterprise Linux 7.2 para las HBA y las matrices de almacenamiento especificadas en el capítulo de funcionalidades, pero sigue siendo una Muestra de tecnología para todas las demás HBA y matrices de almacenamiento.

DIF/DIX aumenta el tamaño del bloque de disco de 512 bytes comúnmente usado a 520 bytes, agregando 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 del host (HBA) cuando se produce la escritura. El dispositivo de almacenamiento luego confirma la suma de verificación en la recepción y almacena los datos y la suma de verificación. Por otra parte, cuando se presenta la escritura, la suma de verificación puede verificarse mediante el dispositivo de almacenamiento y la recepción de HBA.

destino dm-era device-mapper

Red Hat Enterprise Linux 7.1 introdujo el destino `dm-era` device-mapper como una Muestra de tecnología. `dm-era` rastrea qué bloques se escribieron dentro de un tiempo definido de usuario denominado **era**. Cada instancia de destino de era mantiene la era actual como un aumento monolítico: contador de 32 bits. Este destino permite que la copia de seguridad del software rastree qué bloques han cambiado desde el último respaldo. También permite invalidar parcialmente el contenido de una memoria caché para restaurar coherencia después de restaurar la instantánea del proveedor. Se espera principalmente que el destino `dm-era` sea emparejado con el destino `dm-cache`.

Capítulo 22. Virtualización

Virtualización anidada

Como una Muestra de tecnología, Red Hat Enterprise Linux 7.2 ofrece la funcionalidad de virtualización anidada. Esto permite el uso de huéspedes KVM-QEMU como hosts, lo cual permite al usuario crear huéspedes dentro de estos huéspedes.

La herramienta virt-p2v

Red Hat Enterprise Linux 7.2 ofrece la herramienta virt-p2v como una Muestra de tecnología. Virt-p2v (física o virtual) es una imagen de CD-ROM, ISO o PXE que el usuario puede arrancar en la máquina física y que convierte la máquina física en la máquina virtual que se ejecuta en KVM.

Soporte USB 3.0 para huéspedes KVM

La emulación del adaptador USB 3.0 de host (xHCI) para huéspedes KVM sigue siendo una Muestra de tecnología en Red Hat Enterprise Linux 7.2.

Parte III. Controladores de dispositivos

Este capítulo proporciona un lista completo de todos los controladores de dispositivos que fueron actualizados en Red Hat Enterprise Linux 7.2.

Capítulo 23. Actualización de controlador de almacenamiento

- ✧ El controlador hpsa ha sido actualizado a la versión 3.4.4-1-RH4.
- ✧ El controlador qla2xxx ha sido actualizado a la versión 8.07.00.18.07.2-k.
- ✧ El controlador lpfc ha sido actualizado a la versión 10.7.0.1.
- ✧ El controlador megaraid_sas ha sido actualizado a la versión 06.807.10.00.
- ✧ El controlador fnic ha sido actualizado a la versión 1.6.0.17
- ✧ El controlador mpt2sas ha sido actualizado a la versión 20.100.00.00.
- ✧ El controlador mpt3sas ha sido actualizado a la versión 9.100.00.00.
- ✧ El controlador Emulex be2iscsi ha sido actualizado a la versión 10.6.0.0r.
- ✧ El controlador aacraid ha sido actualizado a la versión 1.2.
- ✧ El controlador bnx2i ha sido actualizado a la versión 2.7.10.1.
- ✧ El controlador bnx2fc ha sido actualizado a la versión 2.4.2.

Capítulo 24. Actualizaciones de controladores de red

- El controlador tg3 ha sido actualizado a la versión 3.137.
- El controlador e1000 ha sido actualizado a la versión 7.3.21-k8-NAPI, la cual proporciona soporte para retardo de actualización txtd al usar la variable xmit_more Boolean.
- El controlador e1000e ha sido actualizado a la versión 2.3.2-k.
- El controlador igb ha sido actualizado a la versión 5.2.15-k.
- El controlador igbvf ha sido actualizado a la versión 2.0.2-k.
- El controlador ixgbevf ha sido actualizado a la versión 2.12.1-k.
- El controlador ixgbe ha sido actualizado a la versión 4.0.1-k.
- El controlador bna y firmware han sido actualizados a la versión 3.2.23.0r.
- El controlador bnx2 ha sido actualizado a la versión 2.4.2.
- El controlador CNIC ha sido actualizado a la versión 2.5.21.
- El controlador bnx2x ha sido actualizado a la versión 1.710.51-0, la cual agrega también soporte qllogic NPAR para adaptadores qllogic-nx2.
- El controlador be2net ha sido actualizado a la versión 10.6.0.2.
- El controlador bna ha sido actualizado a la versión 3.2.23.0r.
- El controlador qlcn driver ha sido actualizado a la versión 5.3.62.
- El controlador qlge ha sido actualizado a la versión 1.00.00.34, la cual corrige una condición de race entre el registro de New API (NAPI) y la cancelación de registro, lo cual hacía que el sistema se cayera, si ciertos parámetros eran cambiados cuando la tarjeta de interfaz de red (NIC) se establecía a "down".
- El controlador r8169 ha sido actualizado a la versión 2.3LK-NAPI.
- Los controladores i40e and i40evf han sido actualizados a la versión 1.3.4-k.
- El controlador netxen_nic ha sido actualizado a la versión 4.0.82.
- El controlador sfc ha sido actualizado a la versión más reciente de la línea principal de desarrollo.
- Esta actualización agrega el controlador fm10k de la versión 0.15.2-k.
- Esta actualización agrega soporte VTI6 support incluidas las funcionalidades netns.
- El controlador de vinculación ha sido actualizado a la versión 3.7.1.
- El controlador iwlwifi ha sido actualizado a la versión más reciente de la línea principal de desarrollo.
- El controlador vxlan ha sido actualizado a la versión 0.1.

Capítulo 25. Controlador gráfico y varias actualizaciones de controladores

- ✧ El controlador HDA ha sido actualizado a la versión más reciente de la línea principal de desarrollo para usar el nuevo método jack kctls .
- ✧ El controlador HPI ha sido actualizado a la versión 4.14.
- ✧ El controlador Realtek HD-audio codec ha sido actualizado a la versión para incluir los códigos init EAPD.
- ✧ El controlador IPMI ha sido actualizado para reemplazar timespec por timespec64.
- ✧ El controlador i915 ha sido actualizado para incluir el rebase de controlador de Extensiones de vídeo ACPI en Red Hat Enterprise Linux 7.2.
- ✧ El controlador ACPI ha sido actualizado a la versión 0.25.
- ✧ El controlador NVM-Express ha sido actualizado a la versión 3.19.
- ✧ El controlador rtsx ha sido actualizado a la versión 4.0 para soportar chips rtl8402, rts524A y rts525A.
- ✧ El controlador de dispositivos Generic WorkQueue Engine ha sido actualizado a la versión más reciente de la línea principal de desarrollo.
- ✧ El controlador PCI ha sido actualizado a la versión 3.16.
- ✧ El módulo de kernel EDAC kernel ha sido actualizado para proporcionar soporte para procesadores Intel Xeon v4.
- ✧ El controlador pstate ha sido actualizado para soportar el procesador Intel Core de sexta generación.
- ✧ El controlador intel_idle ha sido actualizado para soportar el procesador Intel Core de sexta generación.

Parte IV. Problemas conocidos

Esta parte documenta problemas conocidos en Red Hat Enterprise Linux 7.2.

Capítulo 26. Compilador y herramientas

Múltiples errores al arrancar de SAN por FCo2

Se han presentado múltiples errores al arrancar desde la implementación actual de arranque a partir de la Red de área de almacenamiento (SAN) mediante Canal de fibra por Ethernet (FCoE). Red Hat tiene está en la mira de un nuevo lanzamiento de Red Hat Enterprise Linux 7 para corregir estos errores. Si desea obtener una lista de los errores afectados y las soluciones temporales (si están disponibles), por favor contacte a su representante de soporte Red Hat.

Valgrind no puede ejecutar programas contruidos con una versión anterior de Open MPI

Red Hat Enterprise Linux 7.2 únicamente soporta la Interfaz binaria de aplicaciones, ABI, en la versión 1.10, la cual es incompatible con la versión 1.6 de Open MPI ABI. Como consecuencia, los programas creados con la versión anterior de Open MPI no se pueden ejecutar en Valgrind que se incluye en Red Hat Enterprise Linux 7.2. Para dar una solución al problema, use la versión Red Hat Developer Toolset de Valgrind para programas vinculados con la versión 1.6 de Open MPI.

Capítulo 27. Escritorio

Las dependencias del paquete **Broken pygobject3** impiden la actualización de Red Hat Enterprise Linux 7.1

El paquete *pygobject3-devel.i686* de 32 bits ha sido retirado de Red Hat Enterprise Linux 7.2 y remplazado por una versión multilib. Si usted tiene instalada la versión de 32 bits del paquete en un sistema Red Hat Enterprise Linux 7.1, encontrará el error **yum** cuando intente hacer la actualización a Red Hat Enterprise Linux 7.2.

Para darle una solución a este problema, use el comando **yum remove pygobject3-devel.i686** como **root** para desinstalar la versión de 32 bits del paquete antes de actualizar su sistema.

Capítulo 28. Actualizaciones generales

Los nuevos nombres de dispositivos pueden interrumpir la conexión de red

Anteriormente, la asignación de nombres de interfaz de redes estables, para dispositivos virtio era imposible, ya que el orden de enumeración de estos dispositivos no era predecible. Con esta corrección, solamente hay un dispositivo PCI padre por bus virtio, y los dispositivos de redes virtio ahora tienen nombres de dispositivos persistentes en máquinas virtuales (según

<http://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>).

Por favor observe que después de actualizar systemd y de reiniciar la máquina virtual, la cual anteriormente tenía nombres de interfaces de un espacio de nombre (eth0, eth1,...), fueron asignados nuevos nombres de dispositivos en el siguiente arranque lo cual puede interrumpir la conexión de redes en la máquina virtual.

Capítulo 29. Instalación y arranque

La instalación en modo texto ya no se daña durante la configuración de red

Anteriormente, en la pantalla de Configuración de red en el instalador en modo de texto interactivo, el uso de un espacio al especificar los servidores de nombres hacía que el instalador se dañara.

Anaconda ahora maneja correctamente espacios en definiciones de servidor de nombre y el instalador ya no se daña si se utiliza un espacio para separar direcciones de servidores de nombre por separado.

Posible mensaje de error NetworkManager durante la instalación

Durante la instalación, aparece el siguiente mensaje:

```
ERR NetworkManager: <error> [devices/nm-device.c:2590] activation_source_schedule(): (eth0): activation stage already scheduled
```

En este momento no hay una solución disponible para este error.

La instalación Atomic Host ofrece cryptsetup aunque no está disponible

Durante la instalación de Red Hat Enterprise Linux 7 Atomic Host, el instalador ofrece la opción para cifrar y descifrar particiones mediante **cryptsetup** en la pantalla de particionamiento manual, de la misma forma que ofrece hacerlo durante la instalación de Red Hat Enterprise Linux 7.2.

Sin embargo, las particiones cifradas ya no reciben soporte en Atomic Host. Si usted cifra cualquier partición durante la instalación, no podrá desbloquearla más adelante.

Para darle una solución a este problema, no cifre ninguna partición o volúmenes lógicos durante la instalación de Red Hat Enterprise Linux Atomic Host, incluso si el instalador le presenta esta opción.

El instalador solamente puede agregar almacenamiento avanzado la primera vez que se entra el spoke de almacenamiento.

Durante una instalación interactiva mediante la interfaz gráfica Anaconda, la adición de almacenamiento avanzado (iSCSI, zFCP, FCoE) a su selección de discos no funciona si usted ya ha ingresado y dejado el spoke de almacenamiento. Para solucionar este problema, verifique si la red, si es necesario, esté activa y luego entre el spoke de almacenamiento y agregue los dispositivos de almacenamiento avanzado.

Capítulo 30. Kernel

Algunos sistemas de archivos ext4 no se pueden redimensionar

Debido a un error en el código de ext4, actualmente es imposible redimensionar los sistemas de archivos ext4 que tienen un tamaño de bloque de 1 kilobyte e inferior a 32 megabytes.

La pérdida de conexión con destinos iSCSI activados iSER

Al usar el servidor como un destino iSCSI activado iSER, se presentan pérdidas de conexión repetidamente, el destino puede dejar de responder al igual que el kernel. Para dar una solución a este problema, minimice las pérdidas de conexión iSER o revierta el modo iSCSI sin iSER.

Comando de E/S de llamadas mid-layer SCSI hasta forzar el apagado del sistema

Cuando una matriz retorna un estatus CHECK CONDITION pero los datos sense no son válidos, el código mid-layer de la Interfaz de Sistemas de Computadores Pequeños (SCSI) hace otro intento de realizar una operación de E/S. Si las siguientes operaciones de E/S reciben el mismo resultado, SCSI sigue intentando realizar la operación de E/S de forma indefinida. Actualmente no hay una solución provisional disponible para este error.

El certificado de la llave pública Red Hat Beta necesita ser cargado manualmente

El administrador de sistemas puede usar el mecanismo de llave de propietario de máquina (MOK) para cargar el correspondiente certificado de llave pública Red Hat Beta, el cual es necesario para autenticar el kernel incluido en un lanzamiento Red Hat Enterprise Linux Beta. El registro de la llave pública de Red Hat Certificate Authority (CA) Beta es un procedimiento de una sola vez para un sistema en el cual Red Hat Enterprise Linux 7.2 Beta se ejecutará con UEFI Secure Boot habilitado:

1. Apague UEFI Secure Boot off e instale Red Hat Enterprise Linux 7.2 Beta.
2. Instale el paquete kernel-doc si aún no ha sido instalado. Este paquete proporciona un archivo de certificados que contiene la llave pública de Red Hat CA en el archivo: `/usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer`, donde `<kernel-ver>` es la cadena de versión de kernel sin el sufijo de arquitectura de plataforma, por ejemplo, `3.10.0-314.el7`.
3. Manualmente solicite la inscripción de la llave pública a la lista de llaves de propietario de máquina (MOK) en el sistema mediante la herramienta mokutil. Ejecute el siguiente comando como usuario root:

```
mokutil --import /usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer
```

No se le pedirá una contraseña para la solicitud de registro.

4. En el siguiente arranque del sistema, se le pedirá en la consola del sistema que complete la inscripción de la solicitud MOK. Deberá responder a las preguntas y proveer la contraseña que proporcionó para mokutil en el paso 3.
5. Cuando complete la inscripción MOK, se restablecerá el sistema y se reiniciará. Usted puede reactivar UEFI Secure Boot en el reinicio o en otros reinicios posteriores del sistema.

Capítulo 31. Redes

La política de apagado no está habilitada en el kernel de

El comando **nfct timeout** no tiene soporte en Red Hat Enterprise Linux 7.2. A manera de solución temporal, use los valores disponibles de tiempo de espera en `/proc/sys/net/netfilter/nf_conntrack_*_timeout_*` para establecer el valor de tiempo espera.

Capítulo 32. Sistema y Administración de suscripciones

Registro incompleto en caso de un error

Al registrar un sistema en la GUI del Gestor de suscripción, si el registro falla, la ventana principal de registro no se cierra cuando el usuario hace clic en **OK** sobre el cuadro de diálogo de error. Como consecuencia, la ventana principal quedaba abierta, en un estado en el que no podía completar la tarea correctamente. Este problema se presenta, por ejemplo, cuando el usuario proporciona información de identificación inválida o cuando se utiliza auto-attach para registro. A modo de solución temporal, haga clic en el botón **Cancelar** en la ventana de registro principal si se presenta un error durante el proceso.

El botón Atrás en el complemento del Gestor de suscripción para arranque inicial

El botón **Atrás** en el panel principal del complemento del Gestor de suscripción en la herramienta de configuración inicial no funciona. A modo de solución, haga clic en **Listo** en la parte superior de Configuración inicial para salir del flujo de trabajo de registro.

Capítulo 33. Virtualización

Navegación de GRUB 2 problemática con KVM

Al usar la consola serial a través de KVM y mantener la tecla de flecha por un tiempo prolongado para navegar en los resultados de menú GRUB 2 se producía una conducta errática. A modo de solución evite la salida rápida ocasionada al mantener por un tiempo prolongado la tecla de flecha abajo.

El reajuste de tamaño de los discos de la Tabla de particiones GUID (GPT) en huéspedes Hyper-V, produce errores en la tabla de particiones

El gestor Hyper-V soporta la reducción de un disco particionado con la GPT en un huésped, si queda espacio libre suficiente después de la última partición, permitiendo al usuario entregar la última parte del disco no utilizada. Sin embargo, esta operación borrará silenciosamente el encabezamiento GPT secundario del disco, lo cual puede desencadenar mensajes de error cuando el huésped examina la tabla de particiones (por ejemplo, con `parted(8)`). Esta es una limitación conocida de Hyper-V.

Como solución temporal, puede restaurar manualmente el encabezamiento secundario GPT con el comando `expert gdisk(8) e`, después de reducir el disco de la GPT. Esto también se presenta al usar la opción Expand de Hyper-V, pero también se puede corregir con la herramienta `parted(8)`.

Apéndice A. Versiones de componentes

Este apéndice es una lista de componentes y sus versiones en el lanzamiento Red Hat Enterprise Linux 7.2.

Tabla A.1. Versiones de componentes

Componente	Versión
Kernel	3.10.0-306.0.1
Controlador QLogic qla2xxx	8.07.00.08.07.1-k1
Controlador QLogic qla4xxx	5.04.00.04.07.01-k0
Controlador Emulex lpfc	10.2.8021.1
funcionalidades del iniciador iSCSI	<i>iscsi-initiator-utils-6.2.0.873-32</i>
DM-Multipath	<i>device-mapper-multipath-0.4.9-82</i>
LVM	<i>lvm2-2.02.128-1</i>

Apéndice B. Historia de revisiones

Revisión 0.0-1.16.3	Fri Oct 30 2015	Gladys Guerrero Lozano
traducido		
Revisión 0.0-1.16.2	Fri Oct 30 2015	Gladys Guerrero Lozano
Los archivos de traducción sincronizados con fuentes XML 0.0-1.16		
Revisión 0.0-1.16.1	Mon Oct 26 2015	Gladys Guerrero Lozano
Los archivos de traducción sincronizados con fuentes XML 0.0-1.16		
Revisión 0.0-1.16	Mon Oct 12 2015	Lenka Špačková
Se agregaron nuevas funcionalidades y problemas conocidos		
Revisión 0.0-1.15	Thu Oct 8 2015	Lenka Špačková
Se reestructuraron problemas conocidos y se agregaron varios elementos a este capítulo. Se agregaron arquitecturas y se actualizaron Muestras de tecnología.		
Revisión 0.0-1.14	Thu Oct 1 2015	Lenka Špačková
Se actualizaron los controladores de dispositivos y se agregaron varios problemas conocidos		
Revisión 0.0-1.13	Wed Sep 16 2015	Lenka Špačková
Se agregaron múltiples funcionalidades y problemas conocidos.		
Revisión 0.0-1.10	Wed Sep 09 2015	Laura Bailey
Se agregaron actualizaciones de controlador para 7.2 Beta.		
Revisión 0.0-1.9	Wed Sep 09 2015	Laura Bailey
Se agregaron problemas conocidos relacionados con Muestra de tecnología OverlayFS		
Revisión 0.0-1.8	Mon Sep 07 2015	Laura Bailey
Se reescribieron las notas de lanzamiento para basarse en funcionalidades y documentar beneficios, cambios de parámetros de kernel y muestra de tecnología.		
Revisión 0.0-1.7	Fri Sep 04 2015	Laura Bailey
Se agregaron elementos de muestra de tecnología a las Notas de lanzamiento.		
Revisión 0.0-1.4	Mon Aug 31 2015	Laura Bailey
Publicación de las Notas de lanzamiento Beta de Red Hat Enterprise Linux 7.2.		