Red Hat Enterprise Linux 6

6.10 Technical Notes

Technical Notes for Red Hat Enterprise Linux 6.10

Edition 10

Last Updated: 2018-08-22

Red Hat Enterprise Linux 6 6.10 Technical Notes

Technical Notes for Red Hat Enterprise Linux 6.10
Edition 10

Red Hat Customer Content Services
rhel-notes@redhat.com

Legal Notice

Abstract

The Technical Notes provide information about notable bug fixes, Technology Previews, deprecated functionality, and other details in Red Hat Enterprise Linux 6.10. For high-level coverage of the improvements implemented in Red Hat Enterprise Linux 6.10 and a list of known problems in this release, refer to the Release Notes. TODO: update link for Beta/GA

Table of Contents

PREFACE

Red Hat Enterprise Linux (RHEL) minor releases are an aggregation of individual enhancement, security, and bug fix errata. The *Red Hat Enterprise Linux 6.10 Technical Notes* document provides a list of notable bug fixes, all currently available Technology Previews, deprecated functionality, and other information. The Release Notes document describes the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release, as well as known problems.

Capabilities and limits of Red Hat Enterprise Linux 6 as compared to other versions of the system are available in the Red Hat Knowledgebase article available at https://access.redhat.com/articles/rhel-limits.

Packages distributed with this release are listed in Red Hat Enterprise Linux 6 Package Manifest. Migration to Red Hat Enterprise Linux 7 is documented in the Migration Planning Guide.

For information regarding the Red Hat Enterprise Linux life cycle, refer to https://access.redhat.com/support/policy/updates/errata/.

CHAPTER 1. RED HAT ENTERPRISE LINUX 6.10 INTERNATIONAL LANGUAGES

Red Hat Enterprise Linux 6.10 supports installation of multiple languages and changing of languages based on your requirements.

The following languages are supported in Red Hat Enterprise Linux 6.10:

- East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese
- European Languages - English, German, Spanish, French, Portuguese Brazilian, and Russian,

The table below summarizes the currently supported languages, their locales, default fonts installed and packages required for some of the supported languages

Table 1.1. Red Hat Enterprise Linux 6 International Languages

Territory	Language	Locale	Fonts	Package Names
China	Simplified Chinese	zh_CN.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-pinyin, scim-tables
Japan	Japanese	ja_JP.UTF-8	Sazanami (Gothic and Mincho)	fonts-japanese, scim-anthy
Korea	Hangul	ko_KR.UTF-8	Baekmuk (Batang, Dotum, Gulim, Headline)	fonts-korean, scim-hangul
Taiwan	Traditional Chinese	zh_TW.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-chewing, scim-tables
Brazil	Portuguese	pt_BR.UTF-8	standard latin fonts	
France	French	ft_FR.UTF-8	standard latin fonts	
Germany	German	de_DE.UTF-8	standard latin fonts	
Italy	Italy	it_IT.UTF-8	standard latin fonts	
Russia	Russian	ru_RU.UTF-8	Cyrillic	dejavu-lgc-sans-fonts, dejavu-lgc-sans-mono-fonts, dejavu-lgc-serif-fonts, xorg-x11-fonts-cyrillic
Spain	Spanish	es_ES.UTF-8	standard latin fonts	

PART I. NOTABLE BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 6.10 that have a significant impact on users.

CHAPTER 2. GENERAL UPDATES

Users with any UID are now able to log in after the update to RHEL 7

Since Red Hat Enterprise Linux 7.3, the default value of the **`first_valid_uid`** configuration option of Dovecot changed from **`500`** in Red Hat Enterprise Linux 6 to **`1000`** in Red Hat Enterprise Linux 7. Consequently, if a Red Hat Enterprise Linux 6 installation did not have **`first_valid_uid`** explicitly defined, the Dovecot configuration did not allow users with UID less than **`1000`** to log in after the update to Red Hat Enterprise Linux 7. Note that only installations where **`first_valid_uid`** was not explicitly defined were affected. This problem has been addressed by the post-upgrade script, which now changes the **`first_valid_uid`** value from **`1000`** to the original value on the source system. As a result, users with any UID are able to log in after the update to Red Hat Enterprise Linux 7. (BZ#1388967)

CHAPTER 3. COMPILER AND TOOLS

C exception handling no longer causes unexpected terminations

Previously, an incorrect unwind routine was called on the 32-bit Intel architecture because of an erroneous check in the code handling C exceptions. As a consequence, the **pthread_cond_wait()** function from the **glibc** library could write data out of bounds and applications written in the C programming language using **glibc** sometimes terminated unexpectedly. The erroneous check has been fixed and the unexpected termination no longer occurs. (BZ#1104812)

Executable files created using the `-pie` option now start correctly

Previously, the linker included in the **binutils** package produced incorrect dynamic relocations for position-independent binaries for the 32-bit Intel architecture. As a consequence, building code with the **-pie** compiler option produced binary files that failed to start. The linker has been fixed and now generates position-independent executable files that run correctly. (BZ#1427285)

Thread cancellation support for APIs depending on `/etc/hosts.conf`

A defect in thread-cancellation support for the **setmntent()** function could cause the function to fail and return an error where it was expected to succeed. Consequently, programs that rely on **setmntent()** could fail to start. The **setmntent()** function has been fixed, and now works as expected.

In addition, the **setttyent()** and **setnetgrent()** functions, and all APIs that rely on the **/etc/hosts.conf** file, have been enhanced to provide improved support for thread cancellation. (BZ#1437147)

`ld` no longer produces invalid executable files with code after initialized data

Previously, the binutils **ld** linker placed code at an incorrect location in memory when the code followed after data initialized to zero values. As a consequence, programs in the linked executable files terminated unexpectedly with a segmentation fault. The linker has been fixed to properly allocate space for the data and position the executable code at the correct starting address. As a result, the linked executable files now run correctly. (BZ#1476412)

The `ss` program no longer stops when providing a long list of filters

Previously, providing a long list of filters to the **ss** command caused an integer value overflow. As a consequence, the 'ss' tool could stop the program execution. With this update, faulty bits in the source code are corrected, and the described problem no longer occurs. (BZ#1476664)

SystemTap no longer causes kernel panic on systems under heavy load

Previously, when probes of the **SystemTap** tool were added and removed at the same time by multiple processes, a kernel panic occurred. As a consequence, unloading **SystemTap** modules on systems under heavy load in some cases caused kernel panics. The procedure for removing probes has now been fixed and **SystemTap** no longer causes a kernel panic in the described situation. (BZ#1525651)

CHAPTER 4. DESKTOP

Multiple mount changes no longer cause performance drop for clients of the `GUnixMountMonitor` object

Previously, when the **autofs** program initiated multiple mount changes in a short period of time, services using the **GUnixMountMonitor** object caused a high CPU load. This update makes it possible to skip accumulated file change events of the **/proc/mounts** file that cannot be handled in real-time. As a result, the CPU load for the clients of **GUnixMountMonitor** is lower. (BZ#1154183)

`xfreerdp` client now works correctly on systems with enabled FIPS mode

Previously, when the **xfreerdp** client was used on systems with enabled FIPS mode, it exited unexpectedly due to usage of FIPS non-compliant encryption algorithms. This update ensures that **xfreerdp** does not exit unexpectedly when it is used with FIPS mode enabled and that FIPS security encryption method is negotiated. As a result, **xfreerdp** now works correctly with the RDP and TLS security protocols on systems with enabled FIPS mode.

However, an error now occurs if the Network Level Authentication (NLA) protocol is required, because its implementation requires FIPS non-compliant algorithms. (BZ#1347920)

CHAPTER 5. HARDWARE ENABLEMENT

Hardware utility tools now correctly identify recently released hardware

Prior to this update, obsolete ID files caused that recently released hardware connected to a computer was reported as unknown. To fix this bug, PCI, USB, and vendor device identification files have been updated. As a result, hardware utility tools now correctly identify recently released hardware. (BZ#1489294)

CHAPTER 6. INSTALLATION AND BOOTING

GRE network interfaces now start correctly

A change introduced in the previous release of Red Hat Enterprise Linux 6 introduced a bug which in some cases caused **initscripts** to fail to correctly start Generic Routing Encapsulation (GRE) network interfaces. This update provides a fix to **initscripts** that ensures GRE interfaces start as expected. (BZ#1436061)

KSH no longer fails to process /etc/init.d/functions

The Korn Shell (*KSH*) is unable to process code where the word **local** appears on the same line as an array definition. This previously caused **KSH** to fail to source the **/etc/init.d/functions** file. This update provides a workaround to the **KSH** limitation, and the function file is now being sourced as expected.

Note that **KSH** may still be unable use some of the functions in **/etc/init.d/functions** file. This update only allows KSH to not fail during the sourcing of **/etc/init.d/functions**. (BZ#1518429)

CHAPTER 7. KERNEL

Kernel dumps are now reliably generated under high memory load

Previously, if a kernel panic occurred under high memory load, a deadlock in some cases occurred and a kernel dump was not generated. This update fixes the **vmalloc_sync_all()** function to avoid waiting on a spinlock that may be never released. As a result, the kernel dump is collected correctly. (BZ#1146727)

Runqueues no longer ignore clock updates

Previously, runqueues on systems with overcommitment of CPUs were prone to ignoring clock updates for extended periods of time. As a consequence, the real-time runqueues were limited, which prevented critical tasks and their dependant tasks from running. This update ensures that the runqueues do not ignore clock updates for extended periods of time. As a result, critical tasks and their dependant tasks are able to run in such situations. (BZ#1212959)

dma_pin_iovec_pages() no longer causes the system out of memory

Previously, when the dma_pin_iovec_pages() function requested a large amount of memory but the request failed, it was unable to release the memory that was reserved. As a consequence, the system run out of memory. With this update, dma_pin_iovec_pages() now allocates the full amount of memory correctly and releases the memory when it is not needed. As a result, the described problem no longer occurs. (BZ#1459263)

A **cgroups** deadlock has been fixed

In certain circumstances when using **cgroups**, a system deadlock occurred due to a race condition. This update adds a work queue that fixes the race condition, which prevents the deadlock from happening. (BZ#1463754)

Audit of unsuccessful **execve()** now works properly

Previously, the audit call in the Linux kernel used the arguments of its parent process when logging arguments of an unsuccessful **execve()** system call. As a consequence, audit was able to use pointers to non-mapped addresses, and the process terminated with a segmentation fault. With this update, audit has been fixed to reinstate the check for the failed **execve()**. As a result, processes no longer terminate erroneously after unsuccessful **execve()**. (BZ#1488822)

vmcp now successfuly executes **cp**

Previously, the kernel memory allocation using the **GFP_DMA** flag caused the **vmcp** command to fail to execute the **cp** command. This update removes the need to use **GFP_DMA** and allows the **GFP_KERNEL** flag to allocate the kernel memory instead. As a result, **vmcp** succeeds to execute **cp**. (BZ#1496105)

CHAPTER 8. NETWORKING

Both `iptables` and `ip6tables` services now recognize the security table in the set_policy() function

Previously, when the security table was used, the **`iptables`** or **`ip6tables`** services failed to clear correctly the firewall ruleset during the shutdown. As a consequence, an error message was displayed when stopping these services. With this update, both **`iptables`** and **`ip6tables`** init scripts recognize but ignore the security table when clearing the firewall ruleset. As a result, the error message is no longer displayed in the described scenario. (BZ#1210563)

Unusual `skbs` no longer cause the kernel to crash

Under a rare network condition, the TCP stack created and tried to transmit unusual **`socket buffers (skbs)`**. Previously, certain core kernel functions did not support such unusual **`skbs`**. As a consequence, the **`BUG()`** kernel message was displayed, and the kernel terminated unexpectedly. With this update, the relevant function is extended to support such kind of **`skbs`**, and the kernel no longer crashes. (BZ#1274139)

The `dmesg` log no longer displays 'hw csum failure' with inbound IPv6 traffic

Previously, when IPv6 fragments were received, the cxgb4 Network Interface Card (NIC) calculated wrong internet checksum. As a consequence, the kernel reported the 'hw csum failure' error message in the **`dmesg`** system log when receiving a fragmented IPv6 packet. With this update, the hardware checksum calculation happens only when IPv4 fragments are received. If IPv6 fragments are received, the checksum calculation happens in software. As a result, when IPv6 fragments are received, **`dmesg`** no longer displays the error message in the described scenario. (BZ#1427036)

SCTP now selects the right source address

Previously, when using a secondary IPv6 address, Stream Control Transmission Protocol (SCTP) selected the source address based on the best prefix matching with the destination address. As a consequence, in some cases, a packet was sent through an interface with the wrong IPv6 address. With this update, SCTP uses the address that already exists in the routing table for this specific route. As a result, SCTP uses the expected IPv6 address as the source address when secondary addresses are used on a host. (BZ#1445919)

Improved performance of SCTP

Previously, small data chunks caused the Stream Control Transmission Protocol (SCTP) to account the **`receiver_window (rwnd)`** values incorrectly when recovering from a **`zero-window situation`**. As a consequence, window updates were not sent to the peer, and an artificial growth of **`rwnd`** could lead to packet drops. This update properly accounts such small data chunks and ignores the **`rwnd`** pressure values when reopening a window. As a result, window updates are now sent, and the announced **`rwnd`** reflects better the real state of the receive buffer. (BZ#1492220)

The virtio interface now transmits the Ethernet packets correctly

Previously, when a virtio Network Interface Card (NIC) received a short frame from the guest, the virtio interface stop transmitting any Ethernet packets. As a consequence, packets transmitted by the guest never appeared on the hypervisor virtual network (vnet) device. With this update, the kernel drops truncated packets, and the virtio interface transmits the packets correctly. (BZ#1535024)

CHAPTER 9. SECURITY

SSH connections using libica AES-GCM now work correctly

Previously, unmodified data could be tagged as modified when using decryption with the **AES-GCM** cipher suite. As a consequence, **SSH** connections could not be established when using **AES-GCM**, and with some applications, data encrypted using **AES-GCM** could not be decrypted. With this update, the tag is computed from the ciphertext when decrypting and from the plaintext when encrypting. As a result, **SSH** connections using **AES-GCM** are now successfully established, and it is possible to decrypt data encrypted with **AES-GCM**. (BZ#1490894)

CHAPTER 10. SERVERS AND SERVICES

Restored performance of 32-bit version of GMP

In a previous update of RHEL 6.9, a performance regression was accidentally introduced to the 32-bit version of the GNU Multiple Precision Arithmetic Library (GMP) for AMD and Intel architecture. As a consequence, the 32-bit version of the GMP suffered marginally decreased performance. A fix has been deployed and GMP peformance has been restored to previous values. (BZ#1430873)

PART II. TECHNOLOGY PREVIEWS

This chapter provides a list of all Technology Previews available in Red Hat Enterprise Linux 6.10.

Technology Preview features are currently not supported under Red Hat Enterprise Linux subscription services, may not be functionally complete, and are generally not suitable for production use. However, these features are included as a customer convenience and to provide the feature with wider exposure.

Customers may find these features useful in a non-production environment. Customers are also free to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported. Errata will be provided for high-severity security issues.

During the development of a Technology Preview feature, additional components may become available to the public for testing. It is the intention of Red Hat clustering to fully support Technology Preview features in a future release.

For information on Red Hat scope of support for Technology Preview features, see https://access.redhat.com/support/offerings/techpreview/.

CHAPTER 11. GENERAL UPDATES

A new module helping to upgrade the Tomcat server from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7

This update adds a new module to the preupgrade-assistant-el6toel7 package as a Technology Preview. The module helps to upgrade from Tomcat version 6.0.24 in Red Hat Enterprise Linux 6 to Tomcat version 7.0.x in Red Hat Enterprise Linux 7 and provides information about incompatibilities found in the system configuration. When using the module, which is recommended only on non-production machines, several automatic changes are made to the Tomcat configuration files during the postupgrade phase to prevent certain known issues. Note that in the supported scenario, users should remove the tomcat6 packages before upgrading.

A new module helping to upgrade Java OpenJDK 7 and Java OpenJDK 8 from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7

The preupgrade-assistant-el6toel7 package provides a new module that handles upgrades of Java OpenJDK 7 and Java OpenJDK 8 from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7. The module, available as a Technology Preview, informs users about possible requested actions and installs the expected equivalents of the original Java OpenJDK packages on the target system. Note that Java OpenJDK 6 and earlier versions are not handled by the in-place upgrade, but the module informs users about expected risks and required manual actions.

CHAPTER 12. AUTHENTICATION AND INTEROPERABILITY

Apache Modules for External Authentication

A set of Apache modules was added to Red Hat Enterprise Linux 6.6 as a Technology Preview. The **mod_authnz_pam**, **mod_intercept_form_submit**, and **mod_lookup_identity** Apache modules in the respective packages can be used by Web applications to achieve tighter interaction with external authentication and identity sources, such as Identity Management in Red Hat Enterprise Linux.

Simultaneous maintaining of TGTs for multiple KDCs

Kerberos version 1.10 added a new cache storage type, DIR:, which allows Kerberos to maintain Ticket Granting Tickets (TGTs) for multiple Key Distribution Centers (KDCs) simultaneously and auto-select between them when negotiating with Kerberized resources. Red Hat Enterprise Linux 6.4 and later includes SSSD enhanced to allow the users to select the DIR: cache for users that are logging in using SSSD. This feature is introduced as a Technology Preview.

Package: sssd

Cross-Forest Kerberos Trust Functionality in Identity Management

The Cross-Forest Kerberos Trust functionality provided by Identity Management (IdM) is included as a Technology Preview. This feature allows to create a trust relationship between an IdM and an Active Directory (AD) domain. This means that users from the AD domain can access resources and services from the IdM domain with their AD credentials. No data needs to be synchronized between the IdM and AD domain controllers; AD user are always authenticated against the AD domain controller and information about users is looked up without the need for synchronization.

This feature is provided by the optional ipa-server-trust-ad package. This package depends on features which are only available in **samba4**. Because samba4-* packages conflicts with the corresponding samba-* packages, all samba-* packages must be removed before ipa-server-trust-ad can be installed.

When the ipa-server-trust-ad package is installed, the **ipa-adtrust-install** utility must be run on all IdM servers and replicas to enable IdM to handle trusts. When this is done, a trust can be established from the command line using the **ipa trust-add** command or the IdM web UI. For more information, see the *Identity Management Guide* for Red Hat Enterprise Linux .

Note that Red Hat recommends to connect Red Hat Enterprise Linux 6 IdM clients to a Red Hat Enterprise Linux 7 IdM server for cross-forest trust capability. Trusts are fully supported on servers running Red Hat Enterprise Linux 7. Configuration with Red Hat Enterprise Linux 6 clients connected to a Red Hat Enterprise Linux 7 server for cross-forest trust is fully supported as well. In such setups, it is recommended to use the latest version of Red Hat Enterprise Linux 6 on the client side and the latest version of Red Hat Enterprise Linux 7 on the server side.

Packages: ipa and samba

CHAPTER 13. COMPILER AND TOOLS

System Information Gatherer and Reporter (SIGAR)

The System Information Gatherer and Reporter (SIGAR) is a library and command-line tool for accessing operating system and hardware level information across multiple platforms and programming languages. In Red Hat Enterprise Linux 6.4 and later, SIGAR is considered a Technology Preview package.

Package: sigar

CHAPTER 14. FILE SYSTEMS

FS-Cache

FS-Cache in Red Hat Enterprise Linux 6 enables networked file systems (for example, NFS) to have a persistent cache of data on the client machine.

Package: cachefilesd

CHAPTER 15. KERNEL

Kernel Media support

The following features are presented as Technology Previews:

- The latest upstream video4linux
- Digital video broadcasting
- Primarily infrared remote control device support
- Various webcam support fixes and improvements

Package: kernel

Linux (NameSpace) Container [LXC]

Linux containers provide a flexible approach to application runtime containment on bare-metal systems without the need to fully virtualize the workload. Red Hat Enterprise Linux 6 provides application level containers to separate and control the application resource usage policies through cgroups and namespaces. This release includes basic management of container life-cycle by allowing creation, editing and deletion of containers using the **libvirt** API and the **virt-manager** GUI. Linux Containers are a Technology Preview.

Packages: libvirt, virt-manager

Diagnostic pulse for the fence_ipmilan agent, BZ#655764

A diagnostic pulse can now be issued on the IPMI interface using the **`fence_ipmilan`** agent. This new Technology Preview is used to force a kernel dump of a host if the host is configured to do so. Note that this feature is not a substitute for the **`off`** operation in a production cluster.

Package: fence-agents

CHAPTER 16. NETWORKING

Mellanox SR-IOV Support

Single Root I/O Virtualization (SR-IOV) is now supported as a Technology Preview in the Mellanox **`libmlx4`** library and the following drivers:

- **`mlx_core`**
- **`mlx4_ib`** (InfiniBand protocol)
- **`mlx_en`** (Ethernet protocol)

Package: kernel

QFQ queuing discipline

In Red Hat Enterprise Linux 6, the **tc** utility has been updated to work with the Quick Fair Scheduler (QFQ) kernel features. Users can now take advantage of the new QFQ traffic queuing discipline from userspace. This feature is considered a Technology Preview.

Package: kernel

CHAPTER 17. SECURITY

TPM

TPM (Trusted Platform Module) hardware can create, store and use RSA keys securely (without ever being exposed in memory), verify a platform's software state using cryptographic hashes and more. The trousers and tpm-tools packages are considered a Technology Preview.

Packages: trousers, tpm-tools

CHAPTER 18. STORAGE

dm-era Device Mapper

The device-mapper-persistent-data package now provides tools to help use the new **dm-era** device mapper functionality released as a Technology Preview. The **dm-era** functionality keeps track of which blocks on a device were written within user-defined periods of time called an **era**. This functionality allows backup software to track changed blocks or restore the coherency of a cache after reverting changes.

DIF/DIX support

DIF/DIX, is a new addition to the SCSI Standard and a Technology Preview in Red Hat Enterprise Linux 6. DIF/DIX increases the size of the commonly used 512-byte disk block from 512 to 520 bytes, adding the Data Integrity Field (DIF). The DIF stores a checksum value for the data block that is calculated by the Host Bus Adapter (HBA) when a write occurs. The storage device then confirms the checksum on receive, and stores both the data and the checksum. Conversely, when a read occurs, the checksum can be checked by the storage device, and by the receiving HBA.

The DIF/DIX hardware checksum feature must only be used with applications that exclusively issue ***O_DIRECT*** I/O. These applications may use the raw block device, or the XFS file system in ***O_DIRECT*** mode. (XFS is the only file system that does not fall back to buffered I/O when doing certain allocation operations.) Only applications designed for use with ***O_DIRECT*** I/O and DIF/DIX hardware should enable this feature.

For more information, refer to section *Block Devices with DIF/DIX Enabled* in the Storage Administration Guide.

Package: kernel

LVM Application Programming Interface (API)

Red Hat Enterprise Linux 6 features the new LVM application programming interface (API) as a Technology Preview. This API is used to query and control certain aspects of LVM.

Package: lvm2

CHAPTER 19. VIRTUALIZATION

Performance monitoring in KVM guests

As a Technology Preview, **KVM** can virtualize a performance monitoring unit (vPMU) to allow virtual machines to use performance monitoring. Additionally it supports Intel's “architectural PMU” which can be live-migrated across different host CPU versions, using the **-cpu** host option.

The virtual performance monitoring feature allows virtual machine users to identify sources of performance problems in their guests, using their preferred pre-existing profiling tools that work on the host as well as the guest. Note that this is an addition to the existing ability to profile a KVM guest from the host.

Package:kernel

System monitoring using SNMP

As a Technology Preview, Red Hat Enterprise Linux 6 allows Simple Network Management Protocol (SNMP) to be used for system monitoring. This allows KVM hosts to send SNMP traps on events so that hypervisor events can be communicated to the user via standard SNMP protocol. In addition, SNMP is capable of performing basic virtual networking operations, such as starting and stopping the virtual domain.

Package:libvirt-snmp

Zero-copy compatibility for macvtap-vhost

The *macvtap-vhost* zero-copy capability is available on Red Hat Enterprise Linux 6 as a Technology Preview. This feature allows running networking work loads in very high wire speeds but with low CPU resource consumption, and it does not limit other features such as memory overcommit and guest migration, which is not the case when using PCI device assignment to achieve the wire speed. Note that this feature is disabled by default.

Package:qemu-kvm

vCPU hot unplug

Although hot-plugging a virtual CPU (vCPU) is a supported operation, hot-unplugging a vCPU remains a Technology Preview in Red Hat Enterprise Linux 6, and is strongly recommended not to be used in high-value deployments.

Package:libvirt

CHAPTER 20. DEPRECATED FUNCTIONALITY

This chapter provides an overview of functionality that has been deprecated, or in some cases removed, in all minor releases up to Red Hat Enterprise Linux 6.10.

Deprecated functionality continues to be supported until the end of life of Red Hat Enterprise Linux 6. Deprecated functionality will likely not be supported in future major releases of this product and is not recommended for new deployments. For the most recent list of deprecated functionality within a particular major release, refer to the latest version of release documentation.

Deprecated *hardware* components are not recommended for new deployments on the current or future major releases. Hardware driver updates are limited to security and critical fixes only. Red Hat recommends replacing this hardware as soon as reasonably feasible.

A *package* can be deprecated and not recommended for further use. Under certain circumstances, a package can be removed from a product.Product documentation then identifies more recent packages that offer functionality similar, identical, or more advanced to the one deprecated, and provides further recommendations.

TLS compression support has been removed from nss

To prevent security risks, such as the CRIME attack, support for TLS compression in the **NSS** library has been removed for all TLS versions. This change preserves the API compatibility.

Changes in public web CAs trust

In addition to the regular trust removals and additions that occur in updated versions of Mozilla's CA list, Mozilla has decided to stop maintaining a part of the CA trust list that the recent versions of Mozilla software no longer require.

All CAs that Mozilla had previously declared as trusted to issue code signing certificates, have had that trust attribute removed.

Because Red Hat provides Mozilla's CA trust list at the operating system level and is used by many applications, some environments might potentially use software that depends on the code signing trust attribute to be set for CAs.

To provide backwards compatibility for applications that require it, the ca-certificates package keeps the code signing trust attribute for several CAs, depending on the **`ca-legacy`** configuration.

If the default **`ca-legacy`** configuration is active, and if a CA certificate continues to be trusted by Mozilla for issuing server authentication certificates, and that CA had been previously trusted by Mozilla for issuing code signing certificates, then the ca-certificates package configures that CA as still trusted for issuing code signing certificates.

If the system administrator uses the **`ca-legacy disable`** command to disable the legacy compatibility configuration, then the unmodified Mozilla CA list will be used by the system, and none of the CA certificates provided by the ca-certificates package will be trusted for issuing code signing certificates.

Both *ipt* and *xt* actions deprecated from iproute

Due to various unresolved issues and design flaws, both *ipt* and *xt* actions have been dropped from the iproute in Red Hat Enterprise Linux 6.

Deprecated Drivers

Deprecated device drivers

- 3w-9xxx

- 3w-sas
- 3w-xxxx
- aic7xxx
- i2o
- ips
- megaraid_mbox
- mptbase
- mptctl
- mptfc
- mptlan
- mptsas
- mptscsih
- mptspi
- sym53c8xx
- qla3xxx

The following controllers from the **megaraid_sas** driver have been deprecated:

- Dell PERC5, PCI ID 0x15
- SAS1078R, PCI ID 0x60
- SAS1078DE, PCI ID 0x7C
- SAS1064R, PCI ID 0x411
- VERDE_ZCR, PCI ID 0x413
- SAS1078GEN2, PCI ID 0x78

The following controllers from the **be2iscsi** driver have been deprecated:

- BE_DEVICE_ID1, PCI ID 0x212
- OC_DEVICE_ID1, PCI ID 0x702
- OC_DEVICE_ID2, PCI ID 0x703

Note that other controllers from the mentioned drivers that are not listed here remain unchanged.

Other Deprecated Components

cluster, luci components

The **fence_sanlock** agent and **checkquorum.wdmd**, introduced in Red Hat Enterprise Linux 6.4 as a Technology Preview and providing mechanisms to trigger the recovery of a node using a hardware watchdog device, are considered deprecated.

openswan component

The openswan packages have been deprecated, and libreswan packages have been introduced as a direct replacement for openswan to provide the VPN endpoint solution. openswan is replaced by libreswan during the system upgrade.

seabios component

Native KVM support for the S3 (suspend to RAM) and S4 (suspend to disk) power management states has been discontinued. This feature was previously available as a Technology Preview.

The zerombr yes Kickstart command is deprecated

In some earlier versions of Red Hat Enterprise Linux, the **zerombr yes** command was used to initialize any invalid partition tables during a Kickstart installation. This was inconsistent with the rest of the Kickstart commands due to requiring two words while all other commands require one. Starting with Red Hat Enterprise Linux 6.7, specifying only **zerombr** in your Kickstart file is sufficient, and the old two-word form is deprecated.

Btrfs file system

B-tree file system (Btrfs) is considered deprecated for Red Hat Enterprise Linux 6. Btrfs was previously provided as a Technology Preview, available on AMD64 and Intel 64 architectures.

eCryptfs file system

eCryptfs file system, which was previously available as a Technology Preview, is considered deprecated for Red Hat Enterprise Linux 6.

mingw component

Following the deprecation of Matahari packages in Red Hat Enterprise Linux 6.3, at which time the mingw packages were noted as deprecated, and the subsequent removal of Matahari packages from Red Hat Enterprise Linux 6.4, the mingw packages were removed from Red Hat Enterprise Linux 6.6 and later.

The mingw packages are no longer shipped in Red Hat Enterprise Linux 6 minor releases, nor will they receive security-related updates. Consequently, users are advised to uninstall any earlier releases of the mingw packages from their Red Hat Enterprise Linux 6 systems.

virtio-win component, BZ#1001981

The VirtIO SCSI driver is no longer supported on Microsoft Windows Server 2003 platform.

fence-agents component

Prior to Red Hat Enterprise Linux 6.5 release, the Red Hat Enterprise Linux High Availability Add-On was considered fully supported on certain VMware ESXi/vCenter versions in combination with the fence_scsi fence agent. Due to limitations in these VMware platforms in the area of SCSI-3 persistent reservations, the **fence_scsi** fencing agent is no longer supported on any version of the Red Hat Enterprise Linux High Availability Add-On in VMware virtual machines, except when using iSCSI-based storage. See the Virtualization Support Matrix for High Availability for full details on supported combinations: https://access.redhat.com/site/articles/29440.

Users using **fence_scsi** on an affected combination can contact Red Hat Global Support Services for assistance in evaluating alternative configurations or for additional information.

systemtap component

The systemtap-grapher package has been removed from Red Hat Enterprise Linux 6. For more information, see https://access.redhat.com/solutions/757983.

matahari component

The **Matahari** agent framework (matahari-*) packages have been removed from Red Hat Enterprise Linux 6. Focus for remote systems management has shifted towards the use of the CIM infrastructure. This infrastructure relies on an already existing standard which provides a greater degree of interoperability for all users.

distribution component

The following packages have been deprecated and are subjected to removal in a future release of Red Hat Enterprise Linux 6. These packages will not be updated in the Red Hat Enterprise Linux 6 repositories and customers who do not use the MRG-Messaging product are advised to uninstall them from their system.

- python-qmf
- python-qpid
- qpid-cpp
- qpid-qmf
- qpid-tests
- qpid-tools
- ruby-qpid
- saslwrapper

Red Hat MRG-Messaging customers will continue to receive updated functionality as part of their regular updates to the product.

fence-virt component

The **libvirt-qpid** is no longer part of the fence-virt package.

openscap component

The openscap-perl subpackage has been removed from openscap.

APPENDIX A. LIST OF BUGZILLAS BY COMPONENT

Table A.1. List of Bugzillas by Component

Component	Release Notes		Technical Notes
	New Features	Known Issues	Notable Bug Fixes
bind	BZ#1452639		
binutils			BZ#1427285, BZ#1476412
clufter	BZ#1526494		
freerdp			BZ#1347920
gcc	BZ#1535656		BZ#1104812
gcc-libraries	BZ#1465568		
git		BZ#1430723	
glib2			BZ#1154183
glibc			BZ#1437147
gmp			BZ#1430873
grub		BZ#1227194, BZ#1573121, BZ#1598553	
hwdata			BZ#1489294
initscripts	BZ#1440888		BZ#1436061, BZ#1518429
iproute			BZ#1476664
iptables	BZ#1459673		BZ#1210563

Component	Release Notes		Technical Notes
	New Features	Known Issues	Notable Bug Fixes
kernel		BZ#1073220, BZ#1544565	BZ#1146727, BZ#1212959, BZ#1274139, BZ#1427036, BZ#1445919, BZ#1459263, BZ#1463754, BZ#1488822, BZ#1492220, BZ#1496105, BZ#1535024
libica			BZ#1490894
other		BZ#1497859, BZ#1588352	
pacemaker	BZ#1427643, BZ#1513199		
preupgrade-assistant-el6toel7		BZ#1366671	BZ#1388967
selinux-policy		BZ#1558428	
subscription-manager		BZ#1581359	
systemtap			BZ#1525651

APPENDIX B. REVISION HISTORY

Revision 0.0-3 **Tue Jun 19 2018** **Lenka Špačková**

Release of the Red Hat Enterprise Linux 6.10 Technical Notes.

Revision 0.0-0 **Wed Apr 25 2018** **Lenka Špačková**

Release of the Red Hat Enterprise Linux 6.10 Beta Technical Notes.