Red Hat Enterprise Linux 6

6.5 Release Notes

Release Notes for Red Hat Enterprise Linux 6.5

Edition 5

Red Hat Enterprise Linux 6 6.5 Release Notes

Release Notes for Red Hat Enterprise Linux 6.5

Edition 5

Red Hat Engineering Content Services

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 6.5. For detailed documentation on all changes to Red Hat Enterprise Linux for the 6.5 update, refer to the Technical Notes.

Table of Contents

PREFACE

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The *Red Hat Enterprise Linux 6.5 Release Notes* documents the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release. Detailed notes on changes (that is, bugs fixed, enhancements added, and known issues found) in this minor release are available in the Technical Notes. The Technical Notes document also contains a complete list of all currently available Technology Previews along with packages that provide them.

> **IMPORTANT**
>
> The online *Red Hat Enterprise Linux 6.5 Release Notes* which are located online here, are to be considered the definitive, up-to-date version. Customers with questions about the release are advised to consult the online *Release* and *Technical Notes* for their version of Red Hat Enterprise Linux.

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

CHAPTER 1. KERNEL

The kernel shipped in Red Hat Enterprise Linux 6.5 includes several hundred bug fixes for, and enhancements to the Linux kernel. For details concerning important bugs fixed and enhancements added to the kernel for this release, refer to the kernel section of the Red Hat Enterprise Linux 6.5 Technical Notes.

Support for PMC-Sierra Cards and Controllers

The **pm8001/pm80xx** driver adds support for PMC-Sierra Adaptec Series 6H and 7H SAS/SATA HBA cards as well as PMC Sierra 8081, 8088, and 8089 chip based SAS/SATA controllers.

Configurable Timeout for Unresponsive Devices

In certain storage configurations (for example, configurations with many LUNs), the SCSI error handling code can spend a large amount of time issuing commands such as TEST UNIT READY to unresponsive storage devices. A new **sysfs** parameter, *eh_timeout*, has been added to the SCSI device object, which allows configuration of the timeout value for TEST UNIT READY and REQUEST SENSE commands used by the SCSI error handling code. This decreases the amount of time spent checking these unresponsive devices. The default value of *eh_timeout* is 10 seconds, which was the timeout value used prior to adding this functionality.

Configuration of Maximum Time for Error Recovery

A new **sysfs** parameter *eh_deadline* has been added to the SCSI host object, which enables configuring the maximum amount of time that the SCSI error handling will attempt to perform error recovery, before giving up and resetting the entire host bus adapter (HBA). The value of this parameter is specified in seconds, and the default is zero, which disables the time limit and allows all of the error recovery to take place. In addition to using **sysfs**, a default value can be set for all SCSI HBAs using the *eh_deadline* kernel parameter.

Lenovo X220 Touchscreen Support

Red Hat Enterprise Linux 6.5 now supports Lenovo X220 touchscreen.

New Supported Compression Formats for makedumpfile

In Red Hat Enterprise Linux 6.5, the **makedumpfile** utility supports the LZO and snappy compression formats. Using these compression formats instead of the zlib format is quicker, in particular when compressing data with randomized content.

CHAPTER 2. NETWORKING

Precision Time Protocol
An implementation of the Precision Time Protocol (PTP) according to IEEE standard 1588-2008 for Linux was introduced as a Technology Preview in Red Hat Enterprise Linux 6.4. The PTP infrastructure, both kernel and user space, is now fully supported in Red Hat Enterprise Linux 6.5. Network driver time stamping support now also includes the following drivers: `bnx2x`, `tg3`, `e1000e`, `igb`, `ixgbe`, and `sfc`.

Analyzing the Non-Configuration IP Multicast IGMP Snooping Data
Previously, the bridge module sysfs virtual file system did not provide the ability to inspect the non-configuration IP multicast Internet Group Management Protocol (IGMP) snooping data. Without this functionality, users could not fully analyze their multicast traffic. In Red Hat Enterprise Linux 6.5, users are able to list detected multicast router ports, groups with active subscribers and the associated interfaces.

PPPoE Connections Support in NetworkManager
NetworkManager has been enhanced to support the creation and management of point-to-point protocol over Ethernet (PPPoE) based connections; for example, connections used for DSL, ISDN, and VPN connectivity.

Network Namespace Support for OpenStack
Network namespaces (netns) is a lightweight container-based virtualization technology. A virtual network stack can be associated with a process group. Each namespace has its own loopback device and process space. Virtual or real devices can be added to each network namespace, and the user can assign IP addresses to these devices and use them as a network node.

SCTP Support to Change the Cryptography Hash Function
In Red Hat Enterprise Linux 6.5, users can change the cryptography hash function from MD5 to SHA1 for Stream Control Transmission Protocol (SCTP) connections.

M3UA Measurement Counters for SCTP
Message Transfer Part Level 3 User Adaptation Layer (M3UA) is a protocol defined by the IETF standard for transporting MTP Level 3 user part signaling messages over IP using Stream Control Transmission Protocol (SCTP) instead of using traditional telecommunications networks (ISDN and PSTN).

Managing DOVE Tunnels Using iproute
Distributed Overlay Virtual Ethernet (DOVE) tunnels allow for building of Virtual Extensible Local Area Network (VXLAN), which represents a scalable solution for ISO OSI layer 2 networks used in cloud centers. The **bridge** tool is part of the iproute package and can be used, for example, to manage a forwarding database on VXLAN devices on Linux platform.

WoWLAN Support for Atheros Interfaces
Red Hat Enterprise Linux 6.5 now supports Wake on Wireless LAN (WoWLAN) for Atheros wifi interfaces. The WoWLAN functionality allows users to power up systems remotely, thus ensuring efficient and unattended managing of the systems.

SR-IOV Functionality in the `qlcnic` Driver
Support for Single Root I/O virtualization (SR-IOV) has been added to the `qlcnic` driver as a Technology Preview. Support for this functionality will be provided directly by QLogic, and customers are encouraged to provide feedback to QLogic and Red Hat. Other functionality in the `qlcnic` driver remains fully supported.

Support for Emulex BladeEngine 3 R

Support for the Emulex BladeEngine 3 R (BE3R) controller has been added in Red Hat Enterprise Linux 6.5.

Support for Emulex FCoE CNA 40G

Support for Emulex Fibre Channel over Ethernet (FCoE) Converged Network Adapter (CNA)40G has been added in Red Hat Enterprise Linux 6.5.

SR-IOV Support on Broadcom Controllers

Single root I/O virtualization (SR-IOV) is now supported on these Broadcom controllers: BCM57810S, BCM57810, BCM57712, BCM57800, BCM57810, BCM57840, and BCM57811. This allows a network interface controller (NIC) to be shared by KVM guests on the KVM host.

CHAPTER 3. SECURITY

Changes Related to FIPS 140-2 Certification
In Red Hat Enterprise Linux 6.5, integrity verification is performed when the dracut-fips package is present, regardless of whether the kernel operates in FIPS mode or not. For detailed information on how to make Red Hat Enterprise Linux 6.5 FIPS 140-2 compliant, consult the following Knowledge Base Solution:

https://access.redhat.com/site/solutions/137833

OpenSSL Updated to Version 1.0.1
OpenSSL has been upgraded to upstream version 1.0.1 to add support for multiple new cryptographic algorithms and support for new versions (1.1, 1.2) of the Transport Layer Security (TLS) protocol.

This update adds the following ciphers needed for transparent encryption and authentication support in GlusterFS:

- CMAC (Cipher-based MAC)

- XTS (XEX Tweakable Block Cipher with Ciphertext Stealing)

- GCM (Galois/Counter Mode)

New additional supported algorithms are especially Elliptic curve Diffie–Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA), and Advanced Encryption Standard in Counter with CBC-MAC mode (AES-CCM).

Smartcard Support in OpenSSH
OpenSSH now complies with the PKCS #11 standard, which enables OpenSSH to use smartcards for authentication.

ECDSA Support in OpenSSL
Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses Elliptic Curve Cryptography (ECC). Note that only the `nistp256` and `nistp384` curves are supported.

ECDHE Support in OpenSSL
Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) is supported, which allows for Perfect Forward Secrecy with much lower computational requirements.

Support of TLS 1.1 and 1.2 in OpenSSL and NSS
OpenSSL and NSS now support the latest versions of the Transport Layer Security (TLS) protocol, which increases security of network connections and enables full interoperability with other TLS protocol implementations. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

OpenSSH Support of HMAC-SHA2 Algorithm
In Red Hat Enterprise Linux 6.5, the SHA-2 cryptographic hash function can now be used in producing a hash message authentication code (MAC), which enables data integrity and verification in OpenSSH.

prefix Macro in OpenSSL
The openssl spec file now uses the prefix macro, which allows for rebuilding of the openssl packages in order to relocate them.

NSA Suite B Cryptography Support
Suite B is a set of cryptographic algorithms specified by the NSA as part of its Cryptographic

Modernization Program. It serves as an interoperable cryptographic base for both unclassified information and most classified information. It includes:

- Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits. For traffic flow, AES should be used with either Counter Mode (CTR) for low bandwidth traffic or Galois/Counter Mode (GCM) of operation for high bandwidth traffic and symmetric encryption.

- Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures.

- Elliptic Curve Diffie-Hellman (ECDH) key agreement.

- Secure Hash Algorithm 2 (SHA-256 and SHA-384) message digest.

Shared System Certificates

NSS, GnuTLS, OpenSSL and Java have been enlisted to share a default source for retrieving system certificate anchors and blacklist information to enable a system-wide trust store of static data that is used by crypto toolkits as input for certificate trust decisions. System-level administration of certificates helps ease of use and is required by local system environments and corporate deployments.

LDAP Groups Are Permitted To Contain Local Users Stored in the `/etc/passwd` File

If SSSD is configured to use the RFC 2307 schema, and the central LDAP server lists local users from the `/etc/passwd` file as members of the groups defined centrally, then SSSD properly returns local group members for such groups, when the option is enabled.

ECC Support in NSS

Network Security Services's (NSS) own internal cryptographic module in Red Hat Enterprise Linux 6.5 now supports the National Institute of Standards and Technology (NIST) Suite B set of recommended algorithms for Elliptic curve cryptography (ECC).

Certificate Support in OpenSSH

Red Hat Enterprise Linux 6.5 supports certificate authentication of users and hosts using a new OpenSSH certificate format. Certificates contain a public key, identity information and validity constraints, and are signed with a standard SSH public key using the **ssh-keygen** utility. Note that in **ssh-keygen** shipped with Red Hat Enterprise Linux 6, the `-Z` option is used for specifying the principals. For more information on this functionality, refer to the `/usr/share/doc/openssh-5.3p1/PROTOCOL.certkeys` file.

CHAPTER 4. SUBSCRIPTION MANAGEMENT

Red Hat Support Tool

Red Hat Enterprise Linux 6.5 includes a new package, redhat-support-tool, which provides the Red Hat Support Tool. This tool facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing both the content and services available to them as Red Hat customers. Further, it enables our customers to integrate and automate their helpdesk services with our subscription services. The capabilities of this package include:

- Knowledge Base article and solution viewing from the console (formatted as man pages).

- Viewing, creating, modifying, and commenting on customer cases from the console.

- Attachment uploading directly to a customer case or to ftp://dropbox.redhat.com/ from the console.

- Full proxy support (that is, FTP and HTTP proxies).

- Easy listing and downloading of attachments to customer cases from the console.

- Knowledge Base searching on query terms, log messages, and other parameters, and viewing search results in a selectable list.

- Easy uploading of log files, text files, and other sources to the Shadowman automatic problem determination engine for diagnosis.

- Various other support-related commands.

For more information about the Red Hat Support Tool, refer to the installed documentation in the `/usr/share/doc/redhat-support-tool-`*`version`*`/` directory or the following Knowledge Base article: https://access.redhat.com/site/articles/445443.

Updates of `subscription-manager list`

Among the list of available subscription, the output of the `subscription-manager list -- available` command now contains a new field, `Provides`. This field shows the names of the products that the system is eligible for. In addition, a new field, `Suggested`, has been added to facilitate compliance and provide parity with the graphical user interface (GUI).

CHAPTER 5. VIRTUALIZATION

Virtualization updates in Red Hat Enterprise Linux 6.5 include a number of bug fixes in areas such as live migration, error reporting, hardware and software compatibility. In addition, performance and general stability improvements have been implemented. For the most significant of these changes, see the sections below.

5.1. KVM

Improved Support For the VMDK Image File Format
Red Hat Enterprise Linux 6.5 includes a number of improvements to read-only support for Virtual Machine Disk, or VMDK, image file formats, including its subformats, as created by many VMware products.

Windows Guest Agent Fully Supported
The Windows guest agent is now fully supported and delivered with its own installer in the Supplementary channel together with virtio-win drivers.

Support for the VHDX Image File Format
Red Hat Enterprise Linux 6.5 includes read-only support for Hyper-V virtual hard disk, or VHDX, image formats, as created by Microsoft Hyper-V.

Native Support for GlusterFS in QEMU
Native Support for GlusterFS in QEMU allows native access to GlusterFS volumes using the `libgfapi` library instead of through a locally mounted FUSE file system. This native approach offers considerable performance improvements.

Support for Dumping Metadata of Virtual Disks
This low-level feature uses the newly introduced command option `qemu-img map` to create an index that allows a qcow2 image to be mapped to a block device via LVM. As a result, virtual machine images (with the virtual machine shutdown) can be accessed as block devices. This is useful for backup applications that are now able to read guest image contents without knowing the details of the qcow2 image format.

Enabling and Disabling CPUs in Linux Guests
With this update, it is possible to use the `--guest` option with the `virsh setvcpus` command. This enables or disables virtual CPUs (vCPUs) to set the specified number of vCPUs. Note, however, that this does not add or remove any vCPUs, and will fail if used to set more vCPUs than are currently available on the guest. In addition, to use this feature, the QEMU guest agent must be installed on your system.

Application-Aware `freeze` and `thaw` on Microsoft Windows with VSS Support on `qemu-ga-win`
VSS (Volume Shadow Copy Service) is a Microsoft Windows API that allows, among other things, the notification of applications for proper, consistent freeze and thaw operations. With this feature, snapshots taken while the virtual machine is running are consistent through the whole stack (from the block layer to the guest applications) and can be used for backup purposes. For more information, see the Virtualization Administration Guide

Application-Aware `freeze` and `thaw` on Linux Using qemu-ga Hooks
Similar to the Windows VSS version, application-consistent snapshots can be created with the use of scripts that attach to the QEMU guest agent running on the guest. These scripts can notify applications which would flush their data to the disk during a `freeze` or `thaw` operation, thus allowing consistent snapshots to be taken.

Conversion of VMware OVF and Citrix Xen Guests to KVM Guests

The **virt-v2v** conversion tool has been upgraded to an upstream version to support conversion of VMware Open Virtualization Format (OVF) and Citrix Xen guest conversion to KVM.

Increased KVM Memory Scalability

KVM virtual memory scalability in a single guest has been increased to 4TB.

Support of Volume Control from within Microsoft Windows Guests

Users can now fully control the volume level on Microsoft Windows XP guests using the AC'97 codec.

Opening Connections from a File

It is now possible to set up a **remote-viewer** session from a configuration file associated with a registered MIME type, for example, from the Red Hat Enterprise Virtualization Manager portal. A simple browser link can be used without the need for a browser-specific plug-in or multi-process communication.

Host and Guest Panic Notification in KVM

A new **pvpanic** virtual device can be wired into the virtualization stack such that a guest panic can cause libvirt to send a notification event to management applications. This feature is introduced in Red Hat Enterprise Linux 6.5 as a Technology Preview. Note that enabling the use of this device requires the use of additional **qemu** command line options; this release does not include any supported way for **libvirt** to set those options.

5.2. MICROSOFT HYPER-V

Microsoft Hyper-V Para-Virtualized Drivers

To enhance Red Hat Enterprise Linux support on Microsoft Hyper-V, Synthetic Video Frame Buffer Driver has been added to Red Hat Enterprise Linux 6.5. In addition, the signaling protocol between the host and the guest has been updated. For more information, see Virtualization Administration Guide

5.3. VMWARE

VMware Platform Drivers Updates

The VMware network para-virtualized driver has been updated to the latest upstream version.

CHAPTER 6. STORAGE

Full Support of fsfreeze

The **fsfreeze** tool is fully supported in Red Hat Enterprise Linux 6.5. The `fsfreeze` command halts access to a file system on a disk. **fsfreeze** is designed to be used with hardware RAID devices, assisting in the creation of volume snapshots. For more details on the **fsfreeze** utility, refer to the `fsfreeze(8)` man page.

pNFS File Layout Hardening

pNFS allows traditional NFS systems to scale out in traditional NAS environments, by allowing the compute clients to read and write data directly and in parallel, to and from the physical storage devices. The NFS server is used only to control meta-data and coordinate access, allowing predictably scalable access to very large sets from many clients. Bug fixes to pNFS are being delivered in this release.

Support of Red Hat Storage in FUSE

FUSE (Filesystem in User Space) is a framework that enables development of file systems purely in the user space without requiring modifications to the kernel. Red Hat Enterprise Linux 6.5 delivers performance enhancements for user space file systems that use FUSE, for example, GlusterFS (Red Hat Storage).

Dynamic aggregation of LVM metadata via lvmetad

Most LVM commands require an accurate view of the LVM metadata stored on the disk devices on the system. With the current LVM design, if this information is not available, LVM must scan all the physical disk devices in the system. This requires a significant amount of I/O operations in systems that have a large number of disks.

The purpose of the `lvmetad` daemon is to eliminate the need for this scanning by dynamically aggregating metadata information each time the status of a device changes. These events are signaled to `lvmetad` by `udev` rules. If `lvmetad` is not running, LVM performs a scan as it normally would.

This feature is disabled by default in Red Hat Enterprise Linux 6. To enable it, refer to the *use_lvmetad* parameter in the `/etc/lvm/lvm.conf` file, and enable the `lvmetad` daemon by configuring the `lvm2-lvmetad` init script.

LVM support for (non-clustered) thinly-provisioned snapshots

An implementation of LVM copy-on-write (cow) snapshots, previously available as a Technology Preview, is now fully supported in Red Hat Enterprise Linux 6.5. The main advantage of this implementation, compared to the previous implementation of snapshots, is that it allows many virtual devices to be stored on the same data volume. This implementation also provides support for arbitrary depth of recursive snapshots (snapshots of snapshots of snapshots …). Note that this feature is for use on a single system. It is not available for multi-system access in cluster environments. For more information, refer to the documentation of the `-s, --snapshot` option in the `lvcreate` man page.

LVM support for (non-clustered) thinly-provisioned LVs

Logical Volumes (LVs) can now be thinly provisioned to manage a storage pool of free space to be allocated to an arbitrary number of devices when needed by applications. This allows creation of devices that can be bound to a thinly provisioned pool for late allocation when an application actually writes to the pool. The thinly-provisioned pool can be expanded dynamically if and when needed for cost-effective allocation of storage space. This feature, previously available as a Technology Preview, is now fully supported. You must have the device-mapper-persistent-data package installed to use this feature. For more information, refer to the `lvcreate(8)` man page.

Multipath I/O Updates

Scalability and ease-of-use of **Device Mapper Multipath** have been improved. These improvements include in particular:

- responsiveness of utilities,

- multipath device automatic naming,

- more robust multipath target detection.

Performance Improvements in GFS2

Red Hat Enterprise Linux 6.5 introduces the `Orlov block` allocator that provides better locality for files which are truly related to each other and likely to be accessed together. In addition, when resource groups are highly contended, a different group is used to maximize performance.

TRIM Support in mdadm

The **mdadm** tool now supports the TRIM commands for RAID0, RAID1, and RAID10.

Support For LSI Syncro

Red Hat Enterprise Linux 6 includes code in the `megaraid_sas` driver to enable LSI Syncro CS high-availability direct-attached storage (HA-DAS) adapters. While the `megaraid_sas` driver is fully supported for previously enabled adaptaers, the use of this driver for Syncro CS is available as a Technology Preview. Support for this adapter will be provided directly by LSI, your system integrator, or system vendor. Users deploying Syncro CS on Red Hat Enterprise Linux 6 are encouraged to provide feedback to Red Hat and LSI. For more infomration on LSI Syncro CS solutions, please visit http://www.lsi.com/products/shared-das/pages/default.aspx.

Safe Offline Interface for DASD devices

Red Hat Enterprise Linux 6.5 introduces the safe offline interface for direct access storage devices (DASDs). Instead of setting a DASD device offline and returning all outstanding I/O requests as failed, with this interface, the user can set a DASD device offline and write all outstanding data to the device before setting the device offline.

Support for FBA EAV and EDEV

Red Hat Enterprise Linux 6.5 supports Fixed Block Access (FBA) Extended Address Volumes (EAV) and EDEV installations. FBA Direct Access Storage Devices (DASDs) are mainframe-specific disk devices. In contrast to Extended Count Key Data (ECKD) DASDs, these disks do not require formatting and resemble the Logical Block Addressing (LBA) of non-mainframe disks. Despite this resemblance, the Linux kernel applies special handling during partition detection for FBA DASDs, resulting in a single, immutable partition being reported. While actual FBA DASD hardware is no longer available, the IBM z/VMhypervisor can simulate FBA DASD disks, backed by either ECKD or SCSI devices. EDEV storage then appears to the system as an FBA DASD (with one immutable partition), rather than an ECKD DASD.

CHAPTER 7. CLUSTERING

pcs Fully Supported

The pcs package, previously included as a Technology Preview, is now fully supported. This package provides a command-line tool for configuring and managing the **corosync** and **pacemaker** utilities.

pacemaker Fully Supported

Pacemaker, a scalable high-availability cluster resource manager, which was previously included as a Technology Preview, is now fully supported.

CHAPTER 8. HARDWARE ENABLEMENT

Support of Future Intel SOC Processors

Device support is enabled in the operating system for future Intel System-on-Chip (SOC) processors. These include Dual Atom processors, memory controller, SATA, Universal Asynchronous Receiver/Transmitter, System Management Bus (SMBUS), USB and Intel Legacy Block (ILB - lpc, timers, SMBUS (i2c_801 module)).

Support of 12Gbps LSI SAS Devices

The `mpt3sas` driver adds support for 12Gbps SAS devices from LSI in Red Hat Enterprise Linux.

Support of Dynamic Hardware Partitioning and System Board Slot Recognition

The dynamic hardware partitioning and system board slot recognition features alert high-level system middleware or applications for reconfiguration and allow users to grow the system to support additional workloads without reboot.

Support for future Intel 2D and 3D Graphics

Support for future Intel 2D and 3D graphics has been added to allow systems using future Intel processors to be certified through the Red Hat Hardware Certification program.

Frequency Sensitivity Feedback Monitor

Frequency sensitivity feedback monitor provides the operating system with better information so that it can make better frequency change decisions while saving power.

ECC Memory Support

The Error-correcting code (ECC) memory has been enabled for a future generation of AMD processors. This feature provides the ability to check for performance and errors by accessing ECC memory related counters and status bits.

Support for AMD Systems with More Than 1TB Memory

The kernel now supports memory configurations with more than 1TB of RAM on AMD systems.

CHAPTER 9. INDUSTRY STANDARDS AND CERTIFICATION

FIPS 140 Revalidations

Federal Information Processing Standards (FIPS) publications 140 is a U.S. government security standard that specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive, but unclassified information. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Red Hat Enterprise Linux 6.5 supports NSA Suite B cryptography enhancements and certifications. These cryptographic algorithms provide highly secure networking communication. NSA SUITE B is required for government agencies under NIST 800 - 131. Components of NSA Suite B cryptography include the following:

- Advanced Encryption Standard (AES) encryption GCM mode of operation

- Elliptic Curve Diffie–Hellman (ECDH)

- Secure Hash Algorithm 2 (SHA-256)

The following targets are in the process of validation:

- NSS FIPS-140 Level 1

- Suite B Elliptic Curve Cryptography (ECC)

- OpenSSH (Client and Server)

- Openswan

- dm-crypt

- OpenSSL

- Kernel Crypto

- AES-GCM, AES-CTS, AES-CTR ciphers

CHAPTER 10. DESKTOP AND GRAPHICS

Graphics Updates and New Hardware Support

Graphics updates in Red Hat Enterprise Linux 6.5 include the following:

- Support for future Intel and AMD devices

- Spice improvements

- Improved multi monitor support and touch screen support

Updated gdm

Updates to the **gdm** application include fixes of password expiration messages, mutli-seat support and local interoperability problems.

Upgraded Evolution

The Evolution application has been upgraded to upstream version 2.32 to improve interoperability with Microsoft Exchange. This includes the new Exchange Web Service (EWS), improved meeting support and improved folder support.

Rebased LibreOffice

In Red Hat Enterprise Linux 6.5 release, LibreOffice has been upgraded to upstream version 4.0.4.

Support for AMD GPUs

Support for the latest AMD graphics processor units (GPUs) has been added to Red Hat Enterprise Linux 6.5

Alias Support in NetworkManager

Alias support has been added to NetworkManager. However, users are strongly recommended to use the multiple or secondary IP feature instead.

CHAPTER 11. PERFORMANCE AND SCALABILITY

KSM Enhancements

Kernel Shared Memory (KSM) has been enhanced to consider non-uniform memory access (NUMA) when coalescing pages, which improves performance of the applications on the system. Also, additional page types have been included to increase the density of applications available for Red Hat OpenShift.

tuned updates

tuned profiles have been refined to provide optimum performance for particular scenarios.

CHAPTER 12. COMPILER AND TOOLS

Automatic Bug Reporting Tool (ABRT), Change in the Default Set of Reporters
Running the `abrt-cli --report DIR` command now shows the following choice of reporters:

```
How would you like to report the problem?
 1) New Red Hat Support case
 2) Existing Red Hat Support case
 3) Save to tar archive
```

ABRT Notifications On the Console
Red Hat Enterprise Linux 6.5 provides a new package, abrt-console-notification. With this package installed, users can see warnings on the console if a new problem has been detected by Automatic Bug Reporting Tool (ABRT) since the last login. This was previously not possible and is useful especially for users who do not use the graphical environment, for example, on headless systems. These users could otherwise miss problems detected by ABRT.

APPENDIX A. COMPONENT VERSIONS

This appendix is a list of components and their versions in the Red Hat Enterprise Linux 6.5 release.

Table A.1. Component Versions

Component	Version
Kernel	2.6.32-431
QLogic `qla2xxx` driver	8.05.00.03.06.5-k2
QLogic ql2xxx firmware	ql23xx-firmware-3.03.27-3.1 ql2100-firmware-1.19.38-3.1 ql2200-firmware-2.02.08-3.1 ql2400-firmware-7.00.01-1 ql2500-firmware-7.00.01-1
Emulex `lpfc` driver	8.3.7.21.1p
iSCSI initiator utils	iscsi-initiator-utils-6.2.0.873-10
DM-Multipath	device-mapper-multipath-0.4.9-72
LVM	lvm2-2.02.100-8

APPENDIX B. REVISION HISTORY

Revision 1.0-21   **Tue April 13 2016**   **Jiří Herrmann**
Update of the Red Hat Enterprise Linux 6.5 Release Notes to correct the description for Enabling and Disabling CPUs in Linux Guests.

Revision 1.0-20   **Tue Apr 7 2015**   **Milan Navrátil**
Update of the Red Hat Enterprise Linux 6.5 Release Notes to fix the version of the QLogic qla2xxx driver.

Revision 1.0-18   **Mon Feb 17 2014**   **Eliška Slobodová**
Republished the book to include a note about support for EDEV.

Revision 1.0-16   **Fri Dec 20 2013**   **Eliška Slobodová**
Republished the book to include notes about networking controllers.

Revision 1.0-13   **Fri Dec 13 2013**   **Eliška Slobodová**
Republished the book to include a security note.

Revision 1.0-12   **Thu Nov 21 2013**   **Eliška Slobodová**
Release of the Red Hat Enterprise Linux 6.5 Release Notes.

Revision 1.0-3   **Thu Oct 3 2013**   **Eliška Slobodová**
Release of the Red Hat Enterprise Linux 6.5 Beta Release Notes.