Red Hat Enterprise Linux 5
5.6 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.6
Edition 6

Red Hat Inc.

Red Hat Enterprise Linux 5 5.6 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.6
Edition 6

Legal Notice

Copyright © 2011 Red Hat.

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.

Abstract

The Red Hat Enterprise Linux 5.6 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.5 and minor release Red Hat Enterprise Linux 5.6.

Table of Contents

Preface

The Red Hat Enterprise Linux 5.6 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.5 and minor release Red Hat Enterprise Linux 5.6.

For system administrators and others planning Red Hat Enterprise Linux 5.6 upgrades and deployments, the Technical Notes provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the Red Hat Enterprise Linux 5.6 Technical Notes provide a single, organized source for change tracking and compliance testing.

For every user, the Red Hat Enterprise Linux 5.6 Technical Notes provide details of what has changed in this new release.

The Technical Notes also include, as an Appendix, the Red Hat Enterprise Linux Package Manifest: a listing of every changed package in this release.

Chapter 1. Package Updates

1.1. amtu

1.1.1. RHBA-2011:0082: bug fix update

An updated amtu package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Abstract Machine Test Utility (AMTU) is an administrative utility to check whether the underlying protection mechanism of the hardware are still being enforced. This is a requirement of the Controlled Access Protection Profile FPT_AMT.1.

This update fixes the following bug:

* Previously, the amtu memory separation test could fail randomly because the way that it chose memory regions for testing had an off by one error in the address calculation. The memory separation test tries to locate memory regions that are readonly. Because of the miscalculation, it could try writing to a memory location that was writable. Because it was looking for the write to fail, it mistakenly thinks the test had failed. This update corrects this issue and the amtu memory separation test behaves as expected. (BZ#556853)

All amtu users are advised to upgrade to this updated package, which resolves this issue.

1.2. anaconda

1.2.1. RHBA-2011:0030: bug fix and enhancement update

An updated anaconda package that fixes several bugs and adds various enhancements is now available.

Anaconda is the system installer.

This updated package fixes the following bugs:

* Previously, anaconda did not test the validity of the format of IPv4 netmasks entered during network configuration. If a user entered a nonsensical value for the IPv4 netmask (for example, letters instead of numbers), the installer would sometimes crash. Anaconda now tests netmask values and therefore avoids a crash due to a badly formatted netmask. (BZ#440498)

* The swap space required by a system running Red Hat Enterprise Linux 5 varies according to the role of the system. Previously, anaconda recommended that all installations on IBM System z required swap space at least equal to the amount of installed system memory. This recommendation could have misled users to allocate far more swap space than was required for their purposes. Anaconda now warns users only if they have not allocated any swap space at all. Users can therefore allocate swap space appropriate to their systems without potentially misleading warnings from anaconda. (BZ#475358)

* The pkgorder script ensures that kernel packages are included on the first disc of multi-disc sets, but did not previously ensure that dependencies of those packages were also included on the first disc. When kernel dependencies appeared on later discs in the set, installing the kernel became impossible and installation would fail. The pkgorder script now ensures that kernel dependencies appear on the first disc along with the kernel packages themselves and therefore ensures that installation is not prevented by kernel dependency issues. (BZ#491136)

* When anaconda executes the "xconfig --startxonboot" command in a kickstart file, it sets monitor parameters. Previously, anaconda did not test to see that a monitor was attached to the system before it attempted to set these parameters. When a monitor was not present, anaconda crashed. Anaconda now attempts to set monitor parameters only when a monitor is attached to the system and therefore avoids a

crash when the "xconfig --startxonboot" kickstart command is run on a system without a monitor. ([BZ#517051](#))

* Previously, the iscsi kickstart command was not documented in the kickstart-docs.txt file beyond noting its existence and its options, and the iscsiname command and ignoredisk --onlyuse option were not documented at all. Users had to consult documentation outside anaconda itself to learn how to use these commands and options. In this release, the iscsiname command and ignoredisk --onlyuse option are now documented, and the description of the iscsi command is expanded, reducing the requirement for users to resort to other documentation to use these commands and options. ([BZ#525136](#),

[BZ#586576](#))

* Previously, /proc/bus/usb was not mounted as /mnt/sysimage/proc/bus/usb directly after installation. As a consequence, %post scriptlets could not install packages that require /proc/bus/usb. Anaconda now mounts /proc/bus/usb after installation so that packages that %post scriptlets can install packages that require access to this path. ([BZ#532397](#))

* Previously, the network --noipv6 kickstart command configured /etc/sysconfig/network but did not alter modprobe.conf. Therefore, even when --noipv6 was specified, modprobe would still load the kernel IPv6 modules. The --noipv6 option now disables IPv6 in modprobe.conf too, so the IPv6 kernel modules do not load. ([BZ#537887](#))

* When some installation options are specified by a kickstart file, anaconda interactively prompts users for any information not contained in the file. The interactive screens still contain the "Back" buttons, but these might not be meaningful if there were no previous screens. Previously, anaconda did not handle this situation, and when users clicked a "Back" button to a screen that did not exist, anaconda would crash. Anaconda now handles this situation and informs users that they cannot go back, thus avoiding the crash. ([BZ#537889](#))

* Previously, anaconda selected the mkinitrd and rhlp packages for installation after the list of other packages for installation was finalized. Therefore, it was not possible to exclude these packages or their dependencies from installation. Because some of these dependencies are only compiled for i686, it was not possible to install exclusively 64-bit x86 packages on a system. Anaconda now tests these packages against the packages selected for installation, and if the user's package selection would exclude mkinitrd, rhlp, or their dependencies, anaconda excludes them from installation. ([BZ#541323](#))

* Anaconda validates the format of hostnames entered by users during installation. Previously, due to an error in the validation code, anaconda would only accept hostnames that began with a letter, although RFC 1123 permits hostnames that begin with numbers. The validation code has been corrected, and anaconda now accepts hostnames that begin with numbers or letters. ([BZ#559626](#))

* Prior to Red Hat Enterprise Linux 5.5, the --log option in anaconda was not aware of whether %pre and %post scripts in kickstart files were running in a chroot environment or not. Therefore, kickstart files had to provide absolute paths to log files. Improvements to anaconda in Red Hat Enterprise Linux 5.5 made the --log option aware of chroot environments. Consequently, if unmodified kickstart files from Red Hat Enterprise Linux 5.4 were used to install Red Hat Enterprise Linux 5.5, anaconda sometimes crashed and reported that the directory did not exist. The --log option is now further modified to accept either absolute or relative paths. The presence of absolute paths does not prevent the use of kickstart files created for earlier versions of Red Hat Enterprise Linux 5. ([BZ#568861](#))

* Faulty logic in anaconda meant that dhcp domain-name options longer than 64 characters were dropped during the installation process. Consequently, 'search' was not set in the resolv.conf file and remained empty. Anaconda now handles domain names longer than 64 characters correctly, and writes domain-name options set during installation to the resolv.conf file of the installed system. ([BZ#578110](#))

* Previously, faulty logic did not allow anaconda to reach the default gateway on IBM System z if the z/VM was configured to use layer3 vswitch. Installation on this configuration could not then proceed. In this release, the logic that tests the accessibility of the default gateway has been corrected so that anaconda can detect the gateway and continue installation as expected. (BZ#643961)

* Previously, the ks=nfs and method=nfs boot options were not documented in the command-line.txt file. Users had to consult documentation outside anaconda itself to learn how to use these boot options. In this release, the ks=nfs and method=nfs boot options are documented, reducing the requirement for users to resort to other documentation to use these boot options. (BZ#559200)

This update also adds the following enhancements:

* Previously, anaconda automatically ejected optical discs after installation. When users installed Red Hat Enterprise Linux 5 on remote systems with spring-loaded media trays, users were left with no way to close the tray. Anaconda now includes a "noeject" boot option that does not eject optical discs after installation. Users can therefore prevent media trays from opening in situations in which it would be difficult to close them. The new command is documented in command-line.txt. (BZ#477887, BZ#647232)

* Installation of Red Hat Enterprise Linux 5 continues, even when %pre or %post scriptlets fail to install packages. Therefore, it is not necessarily obvious that a problem has occurred. Anaconda now makes error messages about failed package operations from scriptlets more obvious in logs, and presents error messages on screen when it runs in interactive mode. (BZ#531599)

* Previously, anaconda would try only once to download a package for installation from a network source. If the network was unavailable or slow, anaconda report an error. Anaconda now retries ten times with gradually increasing delay before reporting an error. Therefore, anaconda now has a better chance to recover from failure without intervention from users. (BZ#544323)

* Anaconda automatically installs drivers from local storage devices that have the volume label OEMDRV. Previously, anaconda installed these drivers with no confirmation from the user. It was therefore possible for anaconda to install unwanted drivers. Anaconda now prompts users to confirm the installation of drivers that it automatically detects. (BZ#570053)

* Anaconda now includes support for several hardware devices that it did not previously support. Without this support, it was not possible to use these devices during installation. The devices include:

>> Brocade 10G Ethernet controller

>> Chelsio T4 10Gb Ethernet adapter

>> QLogic Corp cLOM8214 1/10Gb Ethernet controller

>> 10Gb EN port on Mellanox Infiniband controller

>> LSI 3ware 97xx SAS/SATA RAID controller

(BZ#549677, BZ#562913, BZ#571895, BZ#635095, BZ#572341)

Users are advised to upgrade to this updated anaconda package, which resolves these issues and adds these enhancements.

1.3. apr

1.3.1. RHBA-2010:0821: bug fix update

Updated apr packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

This update fixes the following bug:

* Previously, the "apr_strtoi64" interface did not clear the "errno" error state. This error state could result in parse errors for applications that use this code. With this update, the error state is cleared and applications that use this code run as expected. (BZ#647121)

All APR users are advised to install this newly released package, which fixes this bug.

1.3.2. RHEA-2010:0642: enhancement update

Enhanced apr packages are now available for Red Hat Enterprise Linux 5.

The Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

This update adds the following enhancement:

The "apr_pool_pre_cleanup_register" interface has been added, which is required to fix crashes at shutdown in JBoss EAP. (BZ#624771)

All APR users are advised to install this newly released package, which adds this enhancement.

1.4. apr-util

1.4.1. RHBA-2010:0700: bug fix update

Updated apr-util packages that fix a bug are now available.

apr-util is a utility library used with the Apache Portable Runtime (APR). It aims to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing, and more.

These updated apr-util packages fix the following bug:

* The "resource list" (reslist) interface did not respect the time-to-live parameter. Use of this interface by Apache httpd's mod_proxy resulted in connections which could outlive the configured "ttl" attribute. With this update, inactive connections do not outlive the configured "ttl" with mod_proxy. (BZ#632096)

All users of apr-util are advised to upgrade to these updated packages, which resolve this issue.

1.5. audit

1.5.1. RHBA-2011:0083: bug fix and enhancement update

An updated audit package that fixes various bugs and provides an enhancement is now available for Red Hat Enterprise Linux 5.

The audit package contains the user space utilities for storing and searching the audit records which have been generated by the audit subsystem in the Linux 2.6 kernel.

This update fixes the following bugs:

* 32-bit systems did not behave correctly when an audit rule with a large inode value was added, because of a signed number conversion. With this update, auditctl treats the inode value as an unsigned number. (BZ#554553)

* The man page and the help interface of the aureport tool contained inconsistencies. Some options were listed on the man pages but not the in help interface, and other options were listed in the help interface but not on the man page. With this update, the appropriate entries are listed on the man page as well as in the help interface of aureport. (BZ#568677)

* When an ignore directive was included in an audit.rules configuration file, the auditctl utility became unresponsive when attempting to load those rules. With this update, the issue is resolved. (BZ#607823)

* If a transmission problem occurred while transferring an audit event to an aggregating server with the audisp-remote program, the server could have shut down unexpectedly. The internal buffers overflowed and leaked memory associated with the event that could not be queued. With this update, if the queue is full, events, which cannot be queued, are discarded. (BZ#649952)

This update also adds the following enhancement:

* With this update, new audit events definitions for the virtualization rebase are added. The new events are VIRT_CONTROL, VIRT_RESOURCE, and VIRT_MACHINE_ID. (BZ#585356)

All audit users are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

1.6. autofs

1.6.1. RHBA-2010:0833: bug fix update

An updated autofs package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon, which automatically mounts, and then unmounts file systems after a period of inactivity. This updated package fixes the following bug: * As it is used quite often, the Network File System (NFS) mount module is pre-opened and cached by the "parse_sun" module, so that it can be accessed by other modules very quickly. However, especially with a high number of simultaneously running threads, it was possible for a race condition to arise, causing the automount daemon to terminate unexpectedly with a segmentation fault (BZ#648411).

All users of the autofs daemon are advised to upgrade to this updated package, which resolves this issue.

1.6.2. RHBA-2010:0791: bug fix update

An updated autofs5 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Problem Description: The autofs utility controls the operation of the automount daemon, which automatically mounts, and then unmounts file systems after a period of inactivity.

This updated package fixes the following bug:

* Previously, Network Information System (NIS) maps failed to work if maps included both file and NIS maps. This was due to problems related to negative caching of non-existent map keys. With this update, the negative cache is corrected and NIS maps work as expected.

All users of the autofs daemon are advised to upgrade to this updated package, which resolves this issue.

1.7. autofs5

1.7.1. RHBA-2010:0626: bug fix update

An updated autofs5 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon, which automatically mounts, and then unmounts file systems after a period of inactivity. File systems can include network file systems, CD-ROMs, diskettes, and other media.

This updated autofs5 package fixes the following bugs:

* previously, when using client certificates with autofs the certificate DN couldn't be used in LDAP ACLs. With this update, the SASL EXTERNAL authentication mechanism is used for maping the certificate DN to an LDAP DN. (bz#615258)

* previously, autofs could occasionally get suspended during expire of mounts stage if there were many automount managed mounts. With this update, autofs runs without suspension even with larger amounts of automount managed mounts. (bz#615259)

All users of autofs5 are advised to upgrade to this updated package, which resolves this issue.

1.8. bind

1.8.1. RHBA-2011:0032: bug fix and enhancement update

Updated bind packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.

This update fixes the following bugs:

* initscript killed all processes with the name "named" when stopping the named daemon. With this update, initscript kills only the one it started. (BZ#500535)

* The bind-chroot-admin script could break the configuration with non-standard chroot layout. With this update, the script terminates without touching the configuration. (BZ#517279)

* The named initscript always returned zero, even if the configuration was incorrect. With this update, the exit code is corrected. (BZ#530214)

* A redundant patch was included in the source rpm. With this update, no more redundant patches are included. (BZ#546477)

* The named daemon, configured as recursive nameserver, could continuously ask for missing DNSKEY keys, which could potentially lead to blocking of DNS queries for particular host from the side of authoritative DNS server due excessive bandwith consumption. With this update, the named daemon caches the DNSKEY and asks for it again only in case, it is not fetched. (BZ#572848)

* The host/dig/nslookup utilities queried only servers from resolv.conf. With this update, the utilities query the servers specified on command line instead of in resolv.conf and the issue is resolved. (BZ#561299)

* The daemon named, started with the "-D" option, could crash if it failed to connect to D-Bus. With this update, the crash no longer occurs and the issue is resolved. (BZ#523052)

* The named_sdb PostgreSQL database backend did not reconnect to the database when the connection failed during named_sdb startup. With this update, the named daemon writes the error message to the system log and tries to reconnect during every lookup. (BZ#533229)

* BIND could have destroyed fetch too early which would end with assertion failure. With this update, this issue is resolved. (BZ#555848)

* The dig utility incorrectly performed recursive resolution when it received responses with referral. With this update, dig does not anymore attempt to recurse. (BZ#625240)

* BIND could have returned SERVFAIL instead of NXDOMAIN responses for nonexistent resource records from the unsigned child zone if the parent zone was signed. (BZ#643012)

* The host utility, started with the '-4' parameter, could have failed to query IPv4 servers listed in /etc/resolv.conf. (BZ#643430)

In addition, this update adds the following enhancements:

* Manual pages for following commands have been added: ldap2zone, named-sdb and zonetodb. (BZ#556798)

* The host utility now honours "debug", "attempts" and "timeout" options in resolv.conf. (BZ#570851)

* A new option, called DISABLE_ZONE_CHECKING, has been added to /etc/sysconfig/named. This option adds the possibility to bypass zone validation via the named-checkzone utility in initscript and allows to start named with misconfigured zones. (BZ#500896)

* Size, MD5 and the modification time of /etc/sysconfig/named configuration file is no longer checked via the `rpm -V bind` command. (BZ#556770)

Users are advised to upgrade to these updated bind packages, which resolve these issues and add these enhancements.

1.9. cman

1.9.1. RHBA-2011:0036: bug-fix and enhancement update

Updated cman packages that fix bugs and add enhancements are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies fixes for the following bugs:

* gfs_controld: fix plock owner in unmount. (BZ#624554)

* gfs_controld: fix plock owner syncing. (BZ#624156)

* fenced: use post_join_delay after cluster join. (BZ#575952)

* group_tool: list more than 64 groups. (BZ#561509)

* Add extended information to 'group_tool dump plocks' (gfs). (BZ#514264)

* fence_ipmilan now supports HP iLO 3 devices. (BZ#548575)

* mkqdisk debug option is no longer position dependent. (BZ#555246)

* cman can now be rebuilt with latest NSS libraries. (BZ#575157)

* gfs_controld: set last_plock_time for ownership operations. (BZ#578632)

* fence_scsi get_scsi_devices() has vastly improved performance. (BZ#564468)

* If ccsd fails to bind to a socket or send to a socket, ccsd fails to report the IP address and port. (BZ#573996)

* fence_ilo throws an exception if the user does not have correct privileges. (BZ#576176)

* fence_ack_manual man page is now up to date. (BZ#578604)

* Fencing agents now return correct return codes. (BZ#583034)

* Standard output is now closed in fence_rsb. (BZ#583040)

* fence_ilo no longer depends on OpenSSL. (BZ#583049)

* Obtaining metadata from fencing agents now works properly. (BZ#583053)

* libcman no longer leaks file descriptors. (BZ#585218)

* fail_to_recv_const has been changed to 2500. (BZ#587080)

* Fence_vmware and fence_vmware_helper syntax errors have been fixed. (BZ#590304)

* Quorum is no longer recalculated after a node abruptly leaves cluster. (BZ#590304)

* fence_apc no longer fails for some port numbers. (BZ#606315)

* Consensus timeout is now optimized based on node count at cluster startup, significantly reducing failure recovery time in clusters with two members. (BZ#611391)

* Qdiskd now gives up on heuristics that do not respond prior to the qdisk timeout. (BZ#589266)

* Multiple mount attempts when mounting the same gfs2 file system no longer fail incorrectly. (BZ#559735)

* Fencing agent parameters now appear in agent metadata output. (BZ#619034)

* 'port' is now a synonym of 'module_name' for fence_drac5. (BZ#619776)

* Some fencing agents do not support login using keys. (BZ#582334)

* The package no longer overwrites users' log files in /var/log/cluster (BZ#659090)

In addition, this update adds the following enhancements:

* Use of clustering is now supported within guest virtual machines managed by Red Hat Enterprise Virtualization (BZ#595458)

* fence_scsi_test can now test preempt-and-abort, enabling administrators to better decide whether their arrays support fence_scsi. (BZ#603838)

* The use of broacast mode is now supported in some configurations. (BZ#629652)

* Fence-Agents: Support non-default TCP ports in fence_wti for the different services (SSH / Telnet). (BZ#572996)

* Two-node clusters may now delay fencing to resolve race-to-fence situations. (BZ#613064)

* IBM IMMv2 devices are now supported by fence_ipmilan. (BZ#614198)

* Adding LUNs to fence_scsi without restarting the cluster is now supported. (BZ#616138)

* A fencing agent for use with Cisco Unified Computing System environments is provided. (BZ#579859)

* A fencing agent for use with Red Hat Enterprise Virtualization Manager is provided. (BZ#595835)

* A fencing agent for use in clusters utilizing certain switches in conjunction with iSCSI storage is provided. (BZ#572863)

* WTI VMR devices no longer require their prompts to be set to "IPS". (BZ#578615)

All cman users are advised to upgrade to these updated packages, which fixes these issues and add these enhancements.

1.9.2. RHEA-2010:0876: enhancement update

Updated cman packages that add enhancements are now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following enhancement:

* Updated support for newer HP iLO3 devices (BZ#642700)

In addition, the following fencing devices:

* Brocade 200E * Brocade 300 * Brocade 4100 * Brocade 5100 * Brocade 4900 are now supported for use with Red Hat Enterprise Linux starting with this release (BZ#643516)

Users of cman are advised to upgrade to these updated packages, which address these issues.

1.9.3. RHBA-2010:0611: bug-fix update

Updated cman packages that fix bugs are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fixes:

* fence_vmware and fence_vmware_helper cannot be executed. (BZ#606664)

* consensus timeout has been optimized. (BZ#618639)

Users of cman are advised to upgrade to these updated packages, which address these issues.

1.9.4. RHBA-2010:0487: bug-fix update

Updated cman packages that fix a bug are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fix: * fence_scsi get_scsi_devices() too slow, maybe hanging (BZ#580158)

Users of cman are advised to upgrade to these updated packages, which address this issue.

1.10. cmirror

1.10.1. RHBA-2011:0057: bug fix update

An updated cmirror package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The cmirror package is necessary for LVM-based mirroring (RAID1) in a cluster environment.

This update fixes the following bugs:

* A data corruption may have occurred when using 3 or more mirrors. With this update, the underlying cluster code has been modified to address this issue, and the data corruption no longer occurs. (BZ#456575, BZ#471291)

* Prior to this update, cmirror did not work properly in a cluster that was composed of systems with different versions of Red Hat Enterprise Linux 5. This has been fixed, and running cmirror in such environment now works as expected. (BZ#533204)

* In a two device allocation, the failure of both the primary and the log device may have caused the sync attempt to fail and mirrors to stop responding to I/O requests. With this update, this error no longer occurs, and such mirrors now respond as expected. (BZ#561984)

* Due to the inclusion of the linux/kdev_t.h header file, the use of "MAJOR" or "MINOR" macros in the source code may have caused a device number to be associated with a wrong device. With this update, this error no longer occurs, and device numbers are now always associated with correct devices. (BZ#631925)

All cmirror users are advised to upgrade to this updated package, which resolves these issues.

1.10.2. RHBA-2010:0883: bug fix update

An updated cmirror package that fixes a bug is now available.

The cmirror package is necessary for LVM-based mirroring (RAID1) in a cluster environment.

This updated cmirror package fixes the following bug:

* Previously, the MAJOR/MINOR macros caused a device number miscalculation, which could result in an association of a given device number with the wrong device. With this update, the miscalculation no longer occurs and the given device number is associated with the right device. (BZ#640912)

All users of cmirror are advised to upgrade to this updated package, which resolves this issue.

1.11. compat-gcc-34

1.11.1. RHBA-2010:0766: bug fix update

Updated compat-gcc-34 packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

The compat-gcc-34 packages include a GCC 3.4.6 compatibility C, C++ and Fortran 77 compilers.

These updated packages fix the following bugs:

* Previously, the compatibility C, C++ and Fortran 77 compilers generated binaries that required text relocations on the Intel Itanium architecture, which SELinux policies disallow by default. With this update, the compatibility C, C++ and Fortran 77 compilers do not anymore generate such binaries. (BZ#462581)

* Previously, compat-gcc-34-g77 %post and %preun rpm scriptlets could fail upon install-info failures. Such failures are now ignored. (BZ#638882)

* Previously, compat-gcc-34-debuginfo couldn't be installed simultaneously with gcc-debuginfo. This has now been fixed. (BZ#638883)

All GCC users are advised to upgrade to these updated packages, which resolve these issues.

1.12. conga

1.12.1. RHBA-2011:0033: bug fix and enhancement update

Updated Conga packages that fix numerous bugs and add enhancements are now available.

The Conga project is a management system for remote workstations. It consists of luci, which is a secure web-based front-end, and ricci, which is a secure daemon that dispatches incoming messages to underlying management modules.

This update applies the following bug fixes:

* Support for configuring the fence_ifmib, fence_cisco_mds, fence_ucs, and fence_ilo_mp fencing agents has been added (BZ#637216, BZ#626817,

BZ#637222, BZ#628102)

* Support for configuring the "power_wait" attribute for fencing agents has been added (BZ#584633)

* Support for designating resources in a service as non-critical has been added (BZ#637259)

* Support for configuring broadcast network operation (instead of multicast) has been added (BZ#525802)

* Support for configuring KVM VM resources has been updated (BZ#603114)

* Support for the fence_vmware fencing agent has been updated (BZ#590311)

* Support for deleting a failover domain has been added (BZ#555862)

* A bug that caused luci to timeout when communicating with ricci clients has been fixed (BZ#564490)

* A bug that caused configuration of fence_drac5 to not populate the cluster.conf correctly has been fixed (BZ#577913)

* The configuration of quorum disk has been updated (BZ#606509)

* A bug that caused adding new cluster nodes to sometimes fail has been fixed (BZ#612300)

* A bug that caused configuring SAP database resources when using the Internet Explorer web browser to fail has been fixed (BZ#513004)

* Support for configuring the Oracle resource type has been updated (BZ#587399)

* A bug that caused some valid hostnames to be rejected when added in the create cluster or add node dialogs has been fixed (BZ#501780)

* A bug that caused the "auth" and "password" attributes to not be stored for the fence_ipmilan fencing agent has been fixed (BZ#533246)

* Help output has been added to ricci (BZ#602459)

* Support for configuring fstype as xfs and ext4 in filesystem resources has been added (BZ#636554)

* Man pages for ricci and luci_admin have been added (BZ#602362)

* Support for the new "orainstance" and "oralistener" resource agents has been added. (BZ#493662)

All Conga users are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.13. Conga

1.13.1. RHBA-2010:0716: bug-fix update

Updated Conga packages that fix two bugs in Red Hat Enterprise Linux 5.5 are now available.

The Conga project is a management system for remote workstations. It consists of luci, a secure web-based front-end; and ricci, a secure daemon that dispatches incoming messages to the underlying management modules.

This update applies the following bug fixes:

* Certain valid hostnames specified as fully qualified domain names (FQDN) were reported as invalid. (BZ#580202)

* An issue with calling 'virsh nodelist' would cause ricci to hang for 30 seconds during most requests, resulting in timeouts to the web interface. (BZ#578954)

All Conga users are advised to upgrade to these updated packages, which resolve these issues.

1.14. coolkey

1.14.1. RHEA-2011:0111: enhancement update

An updated coolkey package that adds support for Gemalto TOPDLGX4 144K CAC cards is now available.

The coolkey package provides support for CoolKey and Common Access Card (CAC) smart card products.

This update adds the following enhancement:

* The coolkey device driver has been updated to follow the new Card Compatibility Container (CCC) specification, so that Gemalto TOPDLGX4 144K CAC cards are now supported. (BZ#593017)

All users of Gemalto TOPDLGX4 144K CAC cards are advised to upgrade to this updated package, which adds this enhancement.

1.15. cpufreq-utils

1.15.1. RHEA-2011:0119: enhancement update

An enhanced cpufreq-utils package is now available.

The cpufreq-utils package provides processor frequency-scaling utilities.

This updated cpufreq-utils package adds the following enhancement:

* The cpufreq-aperf application, which supports calculation of average CPU frequency over a time period, was added. (BZ#568754)

Users of cpufreq-utils are advised to upgrade to this updated package, which adds this enhancement.

1.16. crash

1.16. crash

1.16.1. RHBA-2011:0059: bug fix update

An updated crash package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The crash package provides a self-contained tool that can be used to investigate live systems, and kernel core dumps created from the netdump, diskdump, kdump, and Xen/KVM "virsh dump" facilities from Red Hat Enterprise Linux.

This update fixes the following bugs:

* Under certain circumstances, running the "mach -m" command on x86, Intel 64, and AMD64 architectures may have failed with a segmentation fault. This occurred when the e820 map provided by BIOS contained an Extensible Firmware Interface (EFI) entry with a value that had not been mapped to the "E820" type. With this update, the underlying source code has been modified to target this issue, and the above command now produces the expected output. (BZ#569164)

* Prior to this update, running the "bt" command on an x86 architecture may have failed with the following error message:

bt: cannot resolve stack trace

This occurred when a task that received a non-maskable interrupt (NMI) entered the kernel from user space, but had not called the requested system call function yet, or when the copy_thread() function set the Extended Instruction Pointer (EIP) value of a newly forked task to the "ret_from_fork" entry point. This has been fixed, and the "bt" command now works as expected. (BZ#572605)

* When running the "kmem -s list" command, the crash utility was unable to read the "kmem_cache_s.name" string. To resolve this issue, the utility has been adjusted to skip the "list_head", and the above command now displays the actual "kmem_cache" names or addresses only. (BZ#580589)

* On a PowerPC architecture, booting a kernel with the "smt-enabled=off" option caused the initial system information, as well as the "sys" and "mach" commands to display an incorrect CPU count. This error has been fixed, and the crash utility now always displays the correct number of available CPUs. (BZ#580599)

* On Intel 64 and AMD64 architectures, running the "bt" command may have failed to produce a correct backtrace when an NMI-interrupted task did not manage to switch its stack pointer from the user-space to kernel stack yet. This error no longer occurs, and the "bt" command now produces the correct output. (BZ#593066)

* The crash utility has been updated to recognize the "__rhel5" marker that flags the difference between the upstream and Red Hat KVM "virsh dump" CPU device format in the dump file header. (BZ#603027)

* Prior to this update, the "bt" command failed to make the transition from the NMI exception stack to the process stack when a task had just entered the kernel, but had not switched its stack pointer from the user-space per-thread stack to the relevant kernel stack yet. This has been fixed, and such transition is made as expected. (BZ#608171)

* The "bt" command was unable to make the transition from the soft IRQ stack to the process stack when a task had taken a clock interrupt and crashed in the subsequent soft IRQ handler. With this update, such transition no longer fails. (BZ#608714)

* On an x86 architecture, the "bt" command may have occasionally failed to produce the backtrace of an NMI-interrupted idle task. This error has been fixed, and the correct output is now displayed as expected. (BZ#653288)

* Previously, using the "bt" command to backtrace the VCPU of a Xen hypervisor may have failed to return the correct result. This happened when the VCPU received an NMI interrupt while it was running in a particular location in the hypercall entry point, and in certain interrupt handlers. This error has been fixed, and using "bt" to backtrace such VCPU now produces the expected output. (BZ#653823)

* When running the "kmem -s" command on a large, active live system, a glibc error may have caused the utility to terminate with a segmentation fault. With this update, an upstream patch has been applied to target this issue, and the segmentation fault no longer occurs. (BZ#659593)

Users of crash are advised to upgrade to this updated package, which resolves these issues.

1.16.2. RHBA-2010:0523: bug fix update

Updated crash packages that fix various bugs are now available.

crash is a self-contained tool that can be used to investigate live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

These updated packages fix the following bugs:

* the "bt" subcommand of the crash tool occasionally did not output the backtrace correctly. The error appeared in x86_64 NMI-interrupted tasks which had not yet switched their stack pointer from the user-space stack to the kernel stack. This issue has been resolved. (BZ#601081)

* a segmentation violation happened when running the "mach -m" command option on x86 or x86_64 systems whose BIOS-provided e820 map contained an EFI-related memory type value that has previously not been mapped to an E820 type. This issue has been resolved. (BZ#601082).

* the "kmem -s list" subcommand in crash couldn't read the kmem_cache_s.name string. This issue has been resolved. The list now skips the list_head and only displays the actual kmem_cache names/addresses. (BZ#601084)

* if a ppc64 kernel was booted with "smt-enabled=off", the initial system banner and the "sys" and "mach" commands displayed an incorrect CPU count. They have been changed to display the number of cpus online. (BZ#601088)

* the "bt" subcommand of crash could not resolve the stack trace when an x86 NMI-interrupted task had just entered the kernel from user-space, but had not yet called the requested system call function. The same issue occurred when the resumption EIP address value of a newly forked x86 task was set to the "ret_from_fork" entry point by copy_thread(). This issue has been resolved in both cases. (BZ#601089)

1.17. ctdb

1.17.1. RHBA-2011:0055: bug fix update

An updated ctdb package that fixes various bugs is now available.

CTDB is a clustered database based on Samba's Trivial Database (TDB). The ctdb package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

This updated ctdb package includes fixes for the following bugs:

* When installing the ctdb package, the tdb-tools package needs to be installed manually. This dependency issue will be addressed in a future release. (BZ#526479)

* With this update, the ctdb package version matches the version of the samba3x package. (BZ#611854)

Please note that it is not possible to do a rolling update of a cluster (i.e. update one server while the others are online) from the previous version ctdb-1.0.82 to the current ctdb-1.0.112. All nodes of a cluster must be shut down before the update. After all nodes are updated, the cluster can be started again.

All users of ctdb are advised to upgrade to this updated package, which resolves these issues.

1.18. cups

1.18.1. RHBA-2011:0095: bug fix update

Updated cups packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.

These updated cups packages provide fixes for the following bugs:

* CUPS printed page labels in the text area and the page labels thus covered the text of plain text documents. Page labels are printed at the edge of the imageable area and the outer text border. (BZ#527187)

* Document printing could be delayed when the user sent a document to a network printer with the socket URI scheme. The delay occurred because the socket back-end waited for pending back-channel data, even though the wait time option was set to zero. This update removes the pertinent wait_bc() function call, and the printing is no longer delayed. (BZ#561946)

* When the class members were changed, /etc/cups/classes.conf was not always updated accordingly. This issue has been resolved, and the configuration file is now always updated as expected. (BZ#565823)

* Previously, when a printer was removed from a class, the list of class members was not updated properly. As a result, if the user attempted to add the printer with the same name to the class the following error message occurred:

Printer [printer] is already a member of class [class]

With this update, the member list is updated as expected, and re-adding the previously removed printer no longer causes the above error. (BZ#565829)

* In some circumstances, the standard CUPS back ends, which transfer data to printers, got into an endless loop, which consumed all CPU cycles. With this update, the main data processing loop shared by all back ends is adjusted and the problem no longer occurs. (BZ#605584)

* The unsupported-character-set error message used the formatting: "Unsupported character set [host.name] from host [character.set]! Clients must use us-ascii or utf-8." This was due to a mistake in the error message formatting. With this update, the parameters are swapped and the error message uses the correct parameter order. (BZ#608016)

* The CUPS mailto notifier got in a loop consuming CPU cycles if an SMTP mail server failed while the notifier was sending an email message. This update fixes the SMTP response parsing code of the notifier and the loop occurs no longer. (BZ#608392)

* It was not possible to print with the samba3x package. This was due to a missing RPM trigger in the CUPS back-end directory. The update adds a trigger, which creates a symbolic link for the samba3x package. (BZ#621932)

* A domain name service failure caused a printer queue to stop, because failure to lookup a hostname was treated as a hard error and the ErrorPolicy for the queue was not followed. With this update, the DNS failures are no longer considered permanent failures and if such a failure occurs, the set ErrorPolicy is applied. (BZ#651945)

All users of cups are advised to upgrade to these updated packages, which resolve these issues.

1.18.2. RHBA-2010:0614: bug fix update

Updated cups packages that fix various bugs are now available.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems. The CUPS "texttops" filter converts text files to PostScript.

These updated cups packages fix the following bugs:

* previously, when the printer was removed from the class, the list of class members was not updated properly. As a result, adding the printer of the same name to the class resulted in the following error message:

Printer <printer> is already a member of class <class>

With this update, the member list is now updated as expected, and re-adding the previously removed printer no longer results in the above error. (BZ#581902)

* when the class members were changed, /etc/cups/classes.conf was not always updated accordingly. This issue has been resolved, and the configuration file is now always updated as expected. (BZ#594621)

* previously, sending a document to a network printer using the socket URI scheme could cause the actual printing to be delayed. This was due to the fact that the socket back-end used to wait for any pending back-channel data, even though the wait time option was set to zero. With this update, the pertinent "wait_bc" function call has been removed, and printing the document is no longer delayed. (BZ#612964)

Users of CUPS are advised to upgrade to these updated packages, which resolve these issues. After installing this update, the cupsd daemon will be restarted automatically.

1.19. dapl

1.19.1. RHBA-2010:0886: and compat-dapl bug fix update

Updated dapl and compat dapl packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

dapl and compat-dapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.

This update fixes the following bugs:

* Previously, an error in the code path in the uDAPL layer did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. With this update, the entry is cleaned up correctly and subsequent connections work as expected. (BZ#638594)

* Previously, dapl could leak file descriptors, which could cause an application crash. With this update, the leak is closed and dapl behaves as expected. (BZ#638595)

* Previously, verbs CQ and completion channels were not correctly disconnected and freed, which could cause an application crash. With this update, verbs CQ and completion channels behave as expected. (BZ#638860)

* Previously, an error in the code path in the compat-dapl layer did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. With this update, the entry is cleaned up correctly and subsequent connections work as expected. (BZ#638862)

All users of dapl or compat-dapl are advised to upgrade to these updated packages which resolve these issues.

1.20. db4

1.20.1. RHBA-2010:0517: bug fix update

Updated db4 packages that fix a database verification bug are now available.

The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.

This update fixes the following bug:

* IDs (ID lists) are stored as "duplicate" nested btrees. When such a list grew big enough enough to require internal pages, the dbverify utility reported spurious out-of-order errors as follows (note: the page and entry numbers are context dependent):

db_verify: Page 7: out-of-order key at entry 6

These errors presented because dbverify did not distinguish between the main database tree and off-page-duplicate trees. With this update, dbverify now distinguishes between such trees and the spurious errors no longer occur. (BZ#589880)

All users should upgrade to these updated packages, which resolve this issue.

1.21. device-mapper

1.21.1. RHBA-2011:0051: bug fix and enhancement update

Updated device-mapper packages that fix several bugs and add an enhancement are now available.

The device-mapper packages provide a library required by logical volume management utilities such as LVM2 and dmraid.

These updated device-mapper packages provide fixes for the following bugs:

* Filtering with many regular expressions (for example when using lvm commands to filter devices) could have caused performance problems. This update improves the parsing process for regular expressions and the processing performance. (BZ#581830)

* After you issued the command for deactivation of logical volumes (lvchange -an) and the command failed, the system could have deleted the symlink to the device in /dev/VGNAME/LVNAME. With this update, the device deactivation function fails if the device is open and the issue no longer occurs. (BZ#583646)

* The devmapper.pc file contained a wrong dependency on SELinux 'Requires.private: libselinux' and other tools could not resolve this dependency. With this update, the dependency was reverted to 'Libs.private: lselinux' and the dependency problem no longer occurs. (BZ#632298)

* Previously, due to the output limit in reporting functions (vgs, lvs), tags seized to be displayed in longer reports. With this update, the output lines in these reports are limited by available memory only. (BZ#649710)

* Filtering with regular expressions (for example when using lvm commands to filter devices) could have failed. This was due to an error in removing a common suffix. With this update, the optimization for common suffixes works correctly. (BZ#651349)

In addition, these updated packages provides the following enhancement:

* The device-mapper package was upgraded to version 1.02.55. The upgraded version: - adds the manual page for the dmeventd service, - improves the 'dmsetup' manual page and adds descriptions of the 'clear' command and the '--showkeys' option, - adds the '--help' option as an alternative to the 'help' command, - allows use of the device-mapper header file in C++. (BZ#627539)

Users are advised to upgrade to these updated device-mapper packages, which resolve these issues and add this enhancement.

1.21.2. RHBA-2010:0431: bug fix update

Updated device-mapper packages that fix various bugs are now available.

The device-mapper packages provide a library required by logical volume management utilities such as LVM2 and dmraid.

This update applies the following bug fixes:

* fixes the device deactivation function so that the function fails if the device is open. This fixes a problem that occurred when a device remained active but the symbolic link was unexpectedly removed. (BZ#583900)

* optimizes regular expression parsing for shared character prefixes. This shortens processing of lvm2 filters with many devices with a shared prefix. (BZ#584345)

All users of device-mapper should upgrade to these updated packages, which resolve these issues and include these enhancements.

1.22. device-mapper-multipath

1.22.1. RHEA-2011:0074: bug fix and enhancement update

Updated device-mapper-multipath packages that fix several bugs and add various enhancements are now available.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug fixes:

* The kernel driver of device-mapper multipath appeared to be old and SAN boot could fail, because the version testing of the driver was incorrect. Version testing is now implemented correctly. (BZ#517951)

* On a non-disruptive upgrade (NDU), all paths of EMC Symmetric arrays failed and the application suddenly terminated. The default configurations for EMC Symmetric are added and the issue no longer occurs. (BZ#562967)

* device-mapper multipath failed to update its maps after a path state transition. multipathd now automatically updates the path groups when a path priority changes. (BZ#566685)

* Because of a udev race, partitions on multipath devices were not always created. The udev rules now wait for device-mapper multipath to finish the device creation. (BZ#568127)

* If a multipath device configured with queue_if_no_path with no working paths was created while booting, the machine hung. multipath no longer enables queuing before multipathd is started. (BZ#579789)

* If a default configuration used /bin/true for the priority callout, booting from a multipathed root file system stopped responding. Now the default values of the respective configurations are set to "none" and booting succeeds. (BZ#580729)

* To resize a multipath device, you had to run "multipathd -k'resize map [mapname]'", as running "multipath" caused it to get stuck in the SUSPENDED state. In this state, all I/O to the device hung. You can now resize the device with either command. (BZ#584742)

* The "show config" command displayed only values differing from the default values. Now, the command prints the complete configuration. (BZ#585225)

* If you added and removed a path in quick succession, the path was removed while multipathd was still using it, resulting in a segmentation fault. multipathd no longer crashes. (BZ#597789)

* If all paths to a device failed and were recovered, in some cases multipath was unable to recover the path immediately. multipath now detects recovered paths. (BZ#599053)

* Since the HWTABLE cannot be overridden, the "defaults" section of the multipath.conf man page no longer implies that anything in the section becomes default and overrides the implied settings. (BZ#599686)

* The kernel could send a spurious remove uevent for a multipath device and a valid multipath device was removed. uevents are now sent only after a device is removed. (BZ#614966)

* Restoring paths on a group_by_prio multipath device could cause the pathgroups to be misconfigured. Multipathd now refreshes all path priorities after paths are restored, which solves the issue. (BZ#660238)

Enhancements:

* CCISS devices are now supported. (BZ#484419)

* Multipath for storage devices mounted as read-only with the 'nodev' option is added. (BZ#559852)

* The multipath and multipathd commands print warning messages in case of an invalid configuration parameter in multipath.conf. (BZ#560892)

* The default configuration for IBM Virtual SCSI ALUA, HP EVA 3000/5000 and P2000, EUROLOGC FC2502 devices is provided. (BZ#647358, BZ#565579,

BZ#573495)

* The "pg_prio_calc" option was added to multipath.conf default options. By default, the option is set to "sum" and group priority is calculated as the sum of its path priorities. If set to "avg", multipath calculates priorities using the average priority of the paths in the group. (BZ#570513)

* The "log_checker_err" option was added to the multipath.conf defaults option. By default, the option is set to "always" and a path checker error is logged continuously. If set to "once", multipathd logs the path checker error once at logging level 2. Any later errors are logged at level 3, until the device is restored. (BZ#574813)

* Virtio block devices can be multipathed. (BZ#576600)

Users should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.22.2. RHBA-2010:0728: bug fix update

Updated device-mapper-multipath packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

These updated packages provide a fix for the following bug:

* Due to a race condition between udev and Device-Mapper, kpartx may have attempted to create partitions on a multipath device before it was completely initialized, causing no Device-Mapper partitions to be created. With this update, udev now waits for the multipath device to be completely initialized before attempting to create partitions on it. (BZ#634903)

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve this issue.

1.22.3. RHBA-2010:0696: bug fix update

Updated device-mapper-multipath packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

These updated packages provide a fix for the following bug:

* when multipathd occassionally received spurious remove uevents from the kernel, multipathd incorrectly removed the multipath device. Since remove uevents are only supposed to be generated after a device has been already removed, multipath no longer removes a multipath device when it receives a remove uevent. Instead, it simply cleans up its internal state if the device has been removed. (BZ#624772)

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve this issue.

1.22.4. RHBA-2010:0532: bug fix update

Updated device-mapper-multipath packages that fix multiple bugs are now available.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-multipath" kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

This update fixes the following bugs:

* due to the inability of multipathd (a path monitoring daemon) to distinguish between deleted and recently added but not yet fully initialized devices, it used to take more than a minute to remove a dead path and reload the device with a new one. This has been fixed and multipathd now removes the deleted devices immediately. (BZ#603616)

* previously, to resize a multipath device, users had to run the command "multipathd -k'resize map <mapname>'", as running "multipath" instead caused the multipath to become stuck in the SUSPENDED state. In this state, all input/output to the device hung. Now users can resize the device with either command, and the multipath device will no longer get stuck in the SUSPENDED state. (BZ#607487)

* adding and removing a path in quick succession could have caused it to be removed while the multipathd was still using it, which used to lead to a segmentation fault. This has been resolved, and multipathd no longer crashes when the path is added and quickly removed again. ([BZ#607911](#))

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve these issues.

1.22.5. RHBA-2010:0415: bug fix update

Updated device-mapper-multipath packages that fix two bugs are now available.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the device-mapper multipath kernel module instructions on what to do, as well as by managing the creation and removal of partitions for device-mapper devices.

This update addresses the following bug:

* During bootup, multipath was setting up queue_if_no_path on devices that asked for it before multipathd was started. If paths to the device existed, but were all unusable, multipath would queue all IO until multipathd started up. This caused kpartx to hang when trying to read the partition table off the device. The end result was that the entire machine would hang during bootup. Multipath now does not enable queueing on newly created devices if multipathd has not started up yet. This can be overridden with the new -q option. Multipathd will enable queuing on the appropriate devices when it starts up. ([BZ#584344](#))

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve this issue.

1.23. dhcp

1.23.1. RHBA-2010:0664: bug fix update

An updated dhcp package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp package provides a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

These updated packages provide a fix for the following bug:

* previously, dhcpd sometimes started to give "INIT" clients new leases rather than presently active ones. That led to premature exhaustion of available leases for new clients. With this update, the server's "by client-id" and "by hardware address" hash table lists are sorted according to the preference to re-allocate that lease to returning clients. This should eliminate pool starvation problems.

All users of dhcp are advised to upgrade to these updated packages, which resolve this issue.

1.23.2. RHBA-2010:0612: bug fix update

An updated dhcp package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp package provides a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

These updated packages provide a fix for the following bug:

* previously, moving the server from communication-interrupted into partner-down state didn't force dhcpd to take over the partner's leases. With this update, a partner-down failover server no longer sends 'peer holds all free leases' if it is able to newly-allocate one of the peer's leases.

All users of dhcp are advised to upgrade to these updated packages, which resolve this issue.

1.24. dhcpv6

1.24.1. RHBA-2011:0034: bug fix update

Updated dhcpv6 packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

The dhcpv6 packages implement the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks, in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). DHCP is a protocol that allows individual devices on an IP network to get their own network configuration information. It consists of: dhcp6c(8), the DHCPv6 client daemon; dhcp6s(8), the DHCPv6 server daemon; and dhcp6r(8), the DHCPv6 relay agent.

These updated packages provide fixes for the following bugs:

* previously, if the server sent a NotOnLink error in it's Reply message during the Solicit/Advertise/Request/Reply process, the client restarted the process by sending a Solicit message, but then ignored the Advertise message sent by the server. With this update, the client doesn't ignore the subsequent Advertise message and correctly sends Request message to server. (BZ #511323)

* previously, if the server received a Relay-Forward message in which the Relay Message Option comes before the Interface-Id Option the server didn't correctly parse the message and failed with an error. With this update, the server parses the Relay-Forward message correctly. (BZ #512399)

* previously, when more than one 'range' statement was defined in the server's configuration file (dhcp6s.conf), the server always sent NotOnLink status in the Reply message. That forced clients to restart the DHCP server discovery process. With this update, the setting of the status code in the Reply message is fixed. (BZ #598439)

All users of dhcpv6 are advised to upgrade to these updated packages, which resolve these issues.

1.25. dump

1.25.1. RHBA-2010:0684: bug fix update

Updated dump packages that fix various bugs are now available.

The dump package contains both dump and restore commands. The dump command examines files in a file system, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a file system. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups.

These updated dump packages fix the following bugs:

* errors in calculating offsets from which to continue file restoration meant that, if a file was split across multiple tapes during a backup, the split file was corrupted and presented with a different md5sum hash to the original when restoration was attempted. This update corrects the offset calculations and allows restoration of split files as expected. (BZ#563532)

* previously, the restore command attempted to restore extended attributes of a file after the immutable flag had been set. As a result, the attributes were not fully restored, and a warning message was displayed on standard error (STDERR). With this update, these operations are now performed in the correct order, and the restore command no longer fails to set the extended attributes. (BZ#494303)

All dump users should upgrade to these updated packages, which resolve these issues.

1.26. dvgrab

1.26.1. RHBA-2011:0120: bug fix update

An updated dvgrab package that fixes a bug is now available.

The dvgrab package is used to save video files from DV-capable FireWire devices (usually camcorders) and DV-capable USB Video Class devices.

This updated dvgrab package fixes the following bug: * Previously, dvgrab could stop responding and only be killed by signal 9 when attempting to save video data from a UVC (USB Video Class) device that is not DV-capable. With this update, an error appears and dvgrab exits cleanly. (BZ#477183)

All users of dvgrab are advised to upgrade to this updated package, which resolves this issue.

1.27. e2fsprogs

1.27.1. RHBA-2010:0868: bug fix and enhancement update

Updated e2fsprogs packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The e2fsprogs packages contain a number of utilities that create, check, modify, and correct inconsistencies in second extended (ext2) file systems. This includes e2fsck (which repairs file system inconsistencies after an unclean shutdown), mke2fs (which initializes a partition to contain an empty ext2 file system), tune2fs (which modifies file system parameters), and most of the other core ext2fs file system utilities.

This update fixes the following bugs:

* Prior to this update, a corrupted journal on an ext3 file system may not have been properly repaired by the e2fsck utility. This was caused by the fact that the utility was unable to detect or repair the problem when the journal appeared to be a sparse file, which led to a journaling failure and file system shut down. With this update, the process_journal_block() function has been adjusted to mark sparse journal as invalid, and e2fsck utility now works as expected. (BZ#621836)

* Under certain circumstances, the blkid utility may have produced an empty output when the /etc/blkid/blkid.tab file contained multiple stale entries with the same label. Consequent to this, an attempt to check the file system or mount it may have failed, preventing the system from booting. This error has been fixed, and the underlying source code has been modified to ensure that blkid always returns the expected result. (BZ#640584)

All users are advised to upgrade to these updated packages, which resolve these issues.

1.28. e4fsprogs

1.28.1. RHBA-2011:0076: bug fix and enhancement update

Updated e4fsprogs packages that fix a bug and add an enhancement are now available for Red Hat Enterprise Linux 5.

The e4fsprogs packages contain a number of utilities for creating, checking, modifying, and correcting inconsistencies in fourth extended (ext4 and ext4dev) file systems. e4fsprogs contains e4fsck (used to repair file system inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 file system), tune4fs (used to modify file system parameters), and most other core ext4fs file system utilities.

This update fixes the following bug:

* To ensure the file system was recently checked, users were required to use the fsck utility before running the "resize4fs -P" (minimum size query) command, even though this is not actually necessary. With this update, the underlying source code has been modified to target this issue, and running fsck before querying the minimum size of the file system is no longer required. (BZ#643945)

As well, this update adds the following enhancement:

* The e4fsprogs package has been updated to the upstream version 1.41.12. (BZ#604809)

All e4fsprogs users are advised to upgrade to these updated packages, which resolve this issue, and add this enhancement.

1.29. exim

1.29.1. RHBA-2010:0522: bug fix update

Updated exim packages that resolve an issue with deliveries on systems configured with multiple routers and duplicate addresses are now available.

Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. It is freely available under the terms of the GNU General Public Licence. In style it is similar to Smail 3, but its facilities are more general. There is a great deal of flexibility in the way mail can be routed, and there are extensive facilities for checking incoming mail. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

These updated exim packages provides fix for the following bug:

* when exim is configured to use multiple routers (eg a remote archiving smtp router and the default localuser router) and duplicate addresses exist (eg a list in /etc/aliases includes users also extant on the local system), if any messages sent to a duplicated address are deferred (eg because the user's mailbox is locked), these messages end up not being delivered. In this circumstance, exim was correctly marking the address as a duplicate but incorrectly marking it as "done". With this update, exim still checks for duplicate addresses in these circumstances but now only marks unique addresses as "done", ensuring deferred messages are still listed as undelivered until they are, in fact, delivered. (BZ#609083)

All exim users of should upgrade to these updated packages, which resolve this issue.

1.30. expat

1.30.1. RHBA-2010:0672: bug fix update

Updated expat packages that fix a bug are now available for Red Hat Enterprise Linux 5.

expat is a C library for parsing XML documents.

These updated expat packages fix the following bug:

* due to a regression introduced by the fix for CVE-2009-3560 the parser could fail when parsing a document with an external DTD (Document Type Definition). This issue is now resolved and such documents will parse correctly. (BZ#618744)

All expat users are advised to upgrade to these updated packages, which resolve this issue.

1.31. gcc

1.31.1. RHSA-2011:0025: Low security and bug fix update

Updated gcc packages that fix two security issues and several compiler bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The gcc packages include C, C++, Java, Fortran, Objective C, and Ada 95 GNU compilers, along with related support libraries. The libgcj package provides fastjar, an archive tool for Java Archive (JAR) files.

Two directory traversal flaws were found in the way fastjar extracted JAR archive files. If a local, unsuspecting user extracted a specially-crafted JAR file, it could cause fastjar to overwrite arbitrary files writable by the user running fastjar. (CVE-2010-0831, CVE-2010-2322)

This update also fixes the following bugs:

* The option -print-multi-os-directory in the gcc --help output is not in the gcc(1) man page. This update applies an upstream patch to amend this. (BZ#529659)

* An internal assertion in the compiler tried to check that a C++ static data member is external which resulted in errors. This was because when the compiler optimizes C++ anonymous namespaces the declarations were no longer marked external as everything on anonymous namespaces is local to the current translation. This update corrects the assertion to resolve this issue. (BZ#503565, BZ#508735, BZ#582682)

* Attempting to compile certain .cpp files could have resulted in an internal compiler error. This update resolves this issue. (BZ#527510)

* PrintServiceLookup.lookupPrintServices with an appropriate DocFlavor failed to return a list of printers under gcj. This update includes a backported patch to correct this bug in the printer lookup service. (BZ#578382)

* GCC would not build against xulrunner-devel-1.9.2. This update removes gcjwebplugin from the GCC RPM. (BZ#596097)

* When a SystemTap generated kernel module was compiled, gcc reported an internal compiler error and gets a segmentation fault. This update applies a patch that, instead of crashing, assumes it can point to anything. (BZ#605803)

* There was a performance issue with libstdc++ regarding all objects derived from or using std::streambuf because of lock contention between threads. This patch ensures reload uses the same value from _S_global for the comparison, _M_add_reference () and _M_impl member of the class. (BZ#635708)

All gcc users should upgrade to these updated packages, which contain backported patches to correct these issues.

1.32. gcc44

1.32. gcc44

1.32.1. RHBA-2011:0102: bug fix update

Updated gcc44 packages that fix several bugs are now available.

The gcc44 packages provide the GNU Compiler Collection (GCC), which includes GNU compilers and related support libraries for C, C++, and Fortran programming languages. These packages also include libgomp, the GNU implementation of the OpenMP Application Programming Interface for multi-platform shared-memory parallel programming.

These updated gcc44 packages provide fixes for the following bugs:

* Prior to this update, irregularities in the debuginfo package prevented the user from seeing local variables in a debugger. This was caused by overlapping entries in the '.debug_ranges' variable. This update fixes the aforementioned issue so that using a debbuger now works as expected. (BZ#510958)

* Under certain circumstances, compiling a program with g++ caused a segmentation fault. This was caused by a flaw in the 'dynamic_cast' code. With this update, the aforementioned fault has been fixed and the crash no longer occurs. (BZ#519517)

* A common block thread private variable was out of scope inside the OpenMP parallel region. Since the variable was thread private, it should have pointed to different addresses in each of the different threads in the common block, but, failed to do so. The variable also exposed a different error where the address of the variable could not be found by gdb. This update fixes the aforementioned flaws. (BZ#533183)

* Under certain circumstances, compiling with the "g++44 -m32 -O2" command on Red Hat Enterprise Linux 5.4 resulted in the following error:

internal compiler error: in emit_swap_insn, at reg-stack.c:827

This update fixes the issue above, and compilation now works as expected. (BZ#548384)

* Compiling certain programs with the '-O2' option resulted in the following error:

error: unable to find a register to spill in class

This error is no longer returned with this update, and the operation now completes as expected. (BZ#558549)

* Passing a variable reference of type 'const' to a function caused the compiler to crash and return an error. This update fixes the flaw in the code so that passing variable references now works as expected. (BZ#593060)

* A certain test case did not compile due to the xor instructions in the code being optimized out. With this update, the aforementioned issue has been fixed and no longer occurs. (BZ#593117)

Users are advised to upgrade to these updated gcc44 packages, which resolve these issues.

1.33. gdb

1.33.1. RHBA-2011:0099: bug fix update

An updated gdb package that fixes various bugs is now available.

GDB, the GNU debugger, allows debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and then printing their data.

This update fixes the following bugs:

* When the gcore utility created a core file for any executable which was compiled with the "-Wl,-z,relro" parameter, GDB was unable to open the core file because it did not contain the list of shared libraries. This is fixed in this update and the core files of executables created with the "-Wl,-z,relro" parameter can be opened in GDB as expected. (BZ#623749)

* GDB terminated unexpectedly when an inferior shared library list changed during an inferior function call, for example by the dlopen() function. GDB now remains stable in this case. (BZ#623219)

* GDB displayed invalid content of some variables. Separate debuginfo files installed for executables caused this behavior when the prelink program optimized the executable with copy relocations. GDB now displays the contents of all the variables correctly. (BZ#614806)

* GDB could have failed to backtrace some functions of binaries. This occurred when some of the source files of a single binary were compiled with debug information (gcc -g), and some without it. With this update, GDB finds all Call Frame Information (CFI) present in the binary and backtraces correctly. (BZ#614028)

* When debugging a C++ program, GDB displayed values of simple data types as they were implemented. With the Python Pretty-Printers feature, GDB is now able to display such values in a human-readable format. (BZ#609157)

* For C++ classes, the ptype command did not display types defined with typedef in a class. The ptype command now displays class data fields, methods, and types defined in a class. To ensure that typedefs are located inside a templated class, the "-fno-eliminate-unused-debug-types" option must be passed to g++ when compiling the program to be debugged. Note that this feature is only available for executables compiled with GCC provided with Red Hat Enterprise Linux 5. (BZ#602355)

* An SIGILL signal could have terminated a multithreaded program while the programs were being debugged in GDB. GDB processed a queued SIGILL signal even if the user deleted the signal's breakpoint. In such case, the SIGILL signal could break the inferior. GDB now recognizes these cases at the moment when signaled by the target program and ignores the SIGILL signal for a deleted breakpoint. (BZ#601709)

* GDB could have lost important debugging information provided by the siginfo_t part of a POSIX signal during the debugging process. GDB now preserves the associated siginfo_t information, and debugging is now transparent to the application, even in multithreaded programs with the setuid() function. (BZ#592031)

* A failed assertion could have occurred when a user activated GDB's Text User Interface (TUI). With this update, GDB's TUI works correctly. (BZ#586566)

* The gstack shell script caused the omission of the first line of backtraces. This has been fixed in this update. (BZ#579793)

* GDB returned an error message when the user attempted to quit. The error message appeared if GDB loaded an executable file and a core file, and the execution was not finished when the user attempted to quit. With this update, GDB automatically removes the core file when starting another inferior execution. (BZ#575232)

* GDB automatically reloads changed binary files from the disk before creating a new instance of the inferior. However, GDB could have terminated unexpectedly when doing so. With this update, this no longer occurs. (BZ#569235)

* When running the gcore command, GDB could have prompted the user to allow pagination and then fail. This occurred if the terminal window was too small for the output returned by the external gcore program. With this update, the gcore standalone command runs non-interactively. (BZ#555076)

All users of gdb are advised to upgrade to this updated package, which resolves these issues.

1.33.2. RHBA-2010:0599: bug fix update

Updated gdb packages that resolve an issue with threads on ia64 are now available.

The GNU debugger, gdb, allows the debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

This update resolves the following issue:

* multi-threaded target programs could get terminated by the SIGILL (Illegal instruction) signal when being debugged using gdb and the breakpoint was deleted before the second SIGILL was reported to the user. The updated gdb package now recognizes these cases already when they get signaled by the target program and the breakpoint is still in place. (BZ#616315)

All gdb users are advised to upgrade to this updated package, which resolves this issue.

1.33.3. RHBA-2010:0417: bug fix update

Updated gdb packages that resolve an issue in the gstack shell script are now available.

The GNU debugger, gdb, allows the debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

This update resolves the following issue:

* a bug in the gstack shell script suppressed the first line of a backtrace. The first line uses frame identification #0 and lists the current execution point (PC address). (Note: gstack can also be executed under the name "pstack".) This update corrects /usr/bin/gstack which now prints the entire backtrace including the first line. (BZ#580833)

All gdb users are advised to upgrade to these updated packages, which resolve this issue.

1.34. gettext

1.34.1. RHEA-2011:0047: enhancement update

An enhanced gettext package updated to version 0.17 is now available for Red Hat Enterprise Linux.

The GNU gettext package provides a set of tools and documentation for producing multi-lingual messages in programs.

This update adds the following enhancement:

* Since the previous version of gettext no longer works with a large number of newer software projects, this updated package installs gettext version 0.17, which allows packages that require modern gettext to build successfully. (BZ#523713)

Note: The Java and libintl.jar support has been discontinued.

All users of gettext are advised to upgrade to this updated package, which adds this enhancement.

1.35. gfs-kmod

1.35.1. RHBA-2011:0089: bug fix update

Updated gfs-kmod packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The gfs-kmod packages contain modules that provide the ability to mount and use Global File System (GFS).

This update fixes the following bugs:

* When a Global File System (GFS) was exported as a Network File System (NFS) service, relocating the service could cause the data on the file system to be corrupted. This error has been fixed, and using NFS along with GFS now works as expected. (BZ#245024)

* Under certain circumstances, using a Network File System (NFS) protocol with a Global File System (GFS) could fail with the following error:

GFS: fsid=axqa01:gfstest.0: fatal: assertion "!bd->bd_pinned && !buffer_busy(bh)" failed

With this update, a complex patch has been applied to resolve this issue, and the above error no longer occurs. (BZ#491369)

* Prior to this update, a kernel panic may have occurred when copying data from an mmapped sparse file on a Global File System (GFS) to a file on a different GFS storage. With this update, this error has been fixed, and GFS no longer causes kernel panics during this workload. (BZ#617339)

* When a Global File System (GFS) does not have enough journals, an attempt to mount it can fail, and an error message is written to standard error. However, this message was not very informative, and did not include important information required to determine the cause of the problem. With this update, the kernel now returns the "-EUSERS" error code, which allows the mount.gfs utility to recognize this error, and display more informative message. (BZ#635023)

All users of gfs-kmod are advised to upgrade to these updated packages, which resolve these issues.

1.36. gfs-utils

1.36.1. RHBA-2011:0088: bug fix update

An updated gfs-utils package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The gfs-utils package provides various user-space tools that are necessary to mount, create, maintain, and test Global File Systems (GFS).

This update fixes the following bugs:

* Prior to this update, an attempt to use the gfs_jadd utility on a symbolic link to a block device failed with the following error message:

GFS Filesystem /dev/vg0/gfs not found

With this update, the underlying source code has been modified to target this issue, and both symbolic links to block devices and block devices themselves can now be used interchangeably. (BZ#555363)

* Due to an incorrect use of the log_err() function, running the "gfs_fsck -q" command may have caused the utility to display the confirmation message multiple times. With this update, the relevant function call has been corrected, so that the gfs_fsck utility no longer produces duplicate messages. (BZ#567657)

All users of gfs-utils are advised to upgrade to this updated package, which resolves these issues.

1.37. gfs2-utils

1.37.1. RHBA-2011:0135: bug fix update

An updated gfs2-utils package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The gfs2-utils package provides the user-space tools necessary to mount, create, maintain and test GFS2 file systems.

This update fixes the following bugs:

* If you try to mount a gfs file system without enough journals, the error messages were misleading. The error reporting was improved. (BZ#537201)

* The file system checker for GFS2 (fsck.gfs2) was extremely slow compared to other fsck utilities. The program was made faster, more thorough and more correct. (BZ#455300)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was segfaulting when converting filesystems of block size 512 bytes.(BZ#568852)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was using too much memory for journaled data (jdata) conversion. (BZ#571876)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was not properly handling context-dependant path names (CDPNs). (BZ#573795)

* The gfs2 file system checker (fsck.gfs2) was segfaulting if the statfs system file was missing. (BZ#575968)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) wasn't converting indirectly-pointed extended attributes correctly. (BZ#576040)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was not able to convert full gfs1 filesystems. (BZ#585081)

* The gfs2 quota program (gfs2_quota) was sometimes allowing the quota file length to become misaligned. (BZ#585085)

* Some RPM build problems were corrected. (BZ#589815)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) wasn't converting the quota files. (BZ#589820)

* If the gfs2_grow tool was run on a device rather than a mount point it was improperly failing rather than determining the mount point. (BZ#595488)

* The gfs2 file system checker (fsck.gfs2) was sometimes ending improperly during journal recovery. (BZ#606468)

* The gfs2_edit tool was returning a good return code (0) when errors occurred with the restoremeta option. (BZ#607229)

* The gfs2 file system checker (fsck.gfs2) was exiting improperly with "unaligned access" errors on Itanium architecture. (BZ#608158)

* The gfs2 file system checker (fsck.gfs2) was segfaulting if journals were missing. (BZ#620384)

* The gfs2 file system checker (fsck.gfs2) was improperly deleting directories if they got too big. (BZ#624689)

* Attempts to unmount a GFS2 file system failed when other filesystems were mounted on the same mount point. (BZ#627723)

* The gfs2 file system checker (fsck.gfs2) was improperly truncating directories with more than 100,000 entries. (BZ#629010)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was corrupting file systems when directories got unusually big (internal structure di_height of 3). (BZ#643099)

As well, this update adds the following enhancements:

* The man page and documentation pertaining to gfs2_convert was updated. (BZ#588374)

* The tool to convert from gfs1 to gfs2 (gfs2_convert) was enhanced to better handle resuming after an interrupted conversion. (BZ#636157)

All users of gfs2-utils should upgrade to this updated package, which resolves these issues.

1.38. ghostscript

1.38.1. RHBA-2011:0137: bug fix and enhancement update

Updated ghostscript packages that fix various bugs and add an enhancement are now available.

The Ghostscript suite provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for PDF files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

This update fixes the following bugs:

* Previously, including a large JBIG2 compressed image in the PDF input file may have caused the pdf2ps conversion utility to terminate unexpectedly with a segmentation fault. This was caused by the fact that the result of the "jbig2_image_new" function call was not always checked properly. This error has been fixed, and the inclusion of JBIG2 images no longer results in a segmentation fault. (BZ#501710)

* Although the recent security bug fix resolved a vulnerability in Ghostscript's International Color Consortium Format Library (icclib), it also changed the limit for "clutPoints" to 100, causing the icclib to reject most ICC profiles. With this update, the limit has been increased to 255, and ICC profiles are now handled as expected. (BZ#514723)

* Due to the incorrect page size handling, converting a PDF file to PostScript may have caused the correct page size information to be lost. As a result, the printed output may have been misplaced or partially visible only. With this update, the conversion from PDF to PostScript works as expected. (BZ#524250)

* When converting a PDF 1.5 document to PNG, running the gs command resulted in the following error message:

ERROR: /undefined in /BXlevel

This has been fixed, and the conversion from PDF 1.5 to PNG no longer fails with the above error. (BZ#545821)

* Due to an error in the pxlmono driver, an incorrect page size may have been used when attempting to print a document with a size other than the default US Letter. With this update, Ghostscript now always retains the correct page size. (BZ#565776)

* Previously, using certain fonts in a PDF document could cause the gs command to terminate with the following error message:

ERROR: /invalidfont in --charpath--

This has been fixed, and gs now processes these PDF files as expected. (BZ#566832)

* A series of imprecise rounding may have caused some elements in a PostScript document to be wrongly positioned when rendered. This has been fixed, and Ghostscript now renders PostScript files correctly. (BZ#599615)

* Attempting to process a PDF file generated by Xerox WorkCentre resulted in an empty output. This was caused by the fact that in these documents, the segment data length field of the last segment is set to "-1", which was not handled correctly. With this update, PDF files generated by Xerox WorkCentre are now rendered as expected. (BZ#605219)

* Due to an incorrect object management, Ghostscript may have attempted to read from uninitialized memory, which could have lead to a segmentation fault. This has been fixed by back-porting a patch from a newer version. (BZ#629563)

This update also adds the following enhancement:

* OPVP 1.0 support has been added. (BZ#560096)

All users of Ghostscript are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

1.38.2. RHBA-2010:0646: bug fix update

Updated ghostscript packages that fix various bugs and add an enhancement are now available.

The Ghostscript suite provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for PDF files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

This update fixes the following bug:

* due to the incorrect page size handling, converting a PDF file to PostScript may have caused the correct page size information to be lost. As a result, the printed output may have been misplaced or partially visible only. With this update, the conversion from PDF to PostScript works as expected. (BZ#592962)

All users of Ghostscript are advised to upgrade to these updated packages, which resolve this issue.

1.39. glibc

1.39.1. RHBA-2011:0109: bug fix and enhancement update

Updated glibc packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

These updated glibc packages provide fixes for the following bugs:

* Executing the 'memusage' command (provided by the memusage utility, which is a part of the glibc-devel package) could cause a segmentation fault. This update fixes the found deficiency and the 'memusage' command works as expected. (BZ#531576)

* Prior to this update, a DNS resolver could fail to report an appropriate error when the supplied buffer was too small. This resulted in a truncated response instead of asking the caller to resize the buffer and try again. With this update, small buffers are handled correctly and the DNS resolver no longer fails. (BZ#533367)

* A deadlock that could cause an application to hang could occur when the 'dlclose' function was called. This resulted in the cancellation of a thread. With this update, a deadlock no longer occurs when calling the 'dlclose' function. (BZ#549813)

* This update limits the amount of stack usage when adding an environment variable with a long name or value. (BZ#559974)

* Submitting an AIO (Asynchronous Input/Output) write request requires a creation of a helper thread to handle the request. If the creation of this thread failed, a corruption of the glibc internal data structures could occur. This resulted in a crash when the next AIO request was submitted. This update corrects this issue by making sure the internal data structures remain consistent. (BZ#566712)

* Previously, there was an error in the POWER6 implementation of the 'memcpy' and 'memset' functions. As a result, using Concurrent Versions System (CVS) with Kerberos authentication on the 32-bit PowerPC architecture may have failed with a segmentation fault. This error has been fixed, and both 'memcpy' and 'memset' functions now work as expected. (BZ#579011)

* Due to a race in the 'free()' function, enabling 'MALLOC_CHECK_' could cause a segmentation fault. This update adds proper locking in the 'free()' function to prevent the aforementioned segmentation fault. (BZ#585674)

* Under certain conditions, cancellation of a thread did not invoke a cleanup handler. This update adds more complete information to the unwind library for glibc, thus, when canceling a thread, a cleanup handler is invoked before the thread is terminated under all circumstances. (BZ#593047)

* Under certain circumstances, unloading a module could leave the remaining modules' symbol search list in an inconsistent state. Consequent to this inconsistency, symbol lookups could spuriously fail to find the symbol. This update corrects this: module unloading no longer produces inconsistent state in the symbol search list. (BZ#593675)

* Previously, pattern matching of specific digraphs was not consistent across all architectures. This was caused by a misinterpretation of the locale's collation information. With this update, the digraphs are correctly recognized and properly collated. (BZ#601294)

* A race condition between module loading and stack unwinding could result in a crash. With this update, a crash no longer occurs in the aforementioned case. (BZ#649956)

In addition, these updated glibc packages provide the following enhancement:

* The name service cache daemon (nscd) now prepends a timestamp to its log messages. (BZ#527558)

* Support for POWER7 and Power ISA v.2.06 architectures has been added. (BZ#563563), (BZ#563599)

Users are advised to upgrade to these updated glibc packages, which resolve these issues and add this enhancement.

1.39.2. RHBA-2010:0769: bug fix update

Updated glibc packages that resolve an issue are now available.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

These updated glibc packages fix the following bug:

* When the 'MALLOC_CHECK_' feature was enabled, a race condition in the 'free' function resulted in an internal heap corruption in a multi-threaded application. With this update, proper locking was added to prevent the corruption. (BZ#637067)

All users of glibc are advised to upgrade to these updated packages, which resolve this issue.

1.39.3. RHBA-2010:0562: bug fix update

Updated glibc packages that fix various bugs are now available.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

This update fixes the following bugs:

* under certain circumstances, unloading a module could leave the remaining modules' symbol search list in an inconsistent state. Consequent to this inconsistency, symbol lookups could spuriously fail to find the symbol. This update corrects this: module unloading no longer produces inconsistent state in the symbol search list. (BZ#604193)

* previously, there was an error in the POWER6 implementation of the "memcpy" and "memset" functions. As a result, using Concurrent Versions System (CVS) with Kerberos authentication on the 32-bit PowerPC architecture may have failed with a segmentation fault. This error has been fixed, and both "memcpy" and "memset" functions now work as expected. (BZ#614546)

All users are advised to upgrade to these updated packages, which resolve these issues.

1.39.4. RHBA-2010:0450: bug fix update

Updated glibc packages that fix two bugs are now available.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

This update applies the following bug fixes:

* submitting an AIO write request initially requires creating a helper thread to handle the request. If the creation of this thread fails, a corruption of glibc internal data structures can result which can cause a crash when the next AIO request is submitted. This update corrects this by making sure the internal structures remain consistent. (BZ#589871)

* missing unwind information can cause pthread cleanup handlers to be missed when a thread is canceled. This update adds unwind information to all functions in the standard C library, even on platforms that do not emit such information by default. (BZ#593047)

All users are advised to upgrade to these updated packages, which resolve these issue.

1.40. gnome-screensaver

1.40.1. RHBA-2010:0944: bug fix update

An updated gnome-screensaver package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with a GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

A recent bug fix introduced in RHBA-2010:0826 uncovered a latent bug in gnome-screensaver's PAM

message handling. This update fixes the following manifestations of that bug:

* An attempt to unlock a locked screen using the smart card authentication failed. With this update, this error no longer occurs, and unlocking a screen with the smart card authentication no works as expected. (BZ#656924)

* When using cached credentials with the System Security Services Daemon (SSSD), an attempt to unlock a locked screen in the "offline mode" could fail. With this update, this error has been fixed, and such attempt no longer fails. (BZ#657044)

Users of gnome-screensaver should upgrade to this updated package, which resolves these issues.

1.40.2. RHBA-2010:0826: bug fix update

An updated gnome-screensaver package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with a GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

This update fixes the following bug:

* When unlocking the screen, clicking the "Cancel" button may have caused the following message to appear in the /var/log/secure log:

gnome-screensaver-dialog: pam_unix(gnome-screensaver:auth): auth could not identify password for [user]

This was due to authentication dialog attempting to log in, even though no such action was requested. With this update, this error has been fixed, and clicking "Cancel" no longer attempts to authenticate a user. (BZ#644823)

Users of gnome-screensaver should upgrade to this updated package, which resolves this issue.

1.41. gnome-session

1.41.1. RHBA-2010:0709: bug fix update

An updated gnome-session package that fixes a bug is now available.

The gnome-session package manages the GNOME desktop session. It starts up other core components of GNOME and handles logouts and saving of the sessions.

This updated gnome-session package fixes the following bug:

* gnome-session, also referred to as the GNOME Session Manager, remembers information such as which applications were open at the time of logout (among other session details), and restores these applications upon logging in again. The session properties dialog which ships with gnome-session previously presented a non-functional "Ask on logout" session saving checkbox. This update replaces that checkbox with a "Save the current session" button. (BZ#432538)

All users of gnome-session are advised to upgrade to this updated package, which resolves this issue.

1.42. gnome-vfs2

1.42.1. RHBA-2010:0436: bug fix update

Updated gnome-vfs2 packages that fix a regression from Red Hat Enterprise Linux 5.4 are now available.

GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.

This update addresses the following regression from Red Hat Enterprise Linux 5.4:

* when extracted from the Uniform Resource Identifier, gnome-vfs returned escaped file paths. If the path, as stored in the URI, contained non-ASCII characters or some ASCII characters which are parsed as something other than file path (eg spaces), the escaped path was inaccurate and could lead gnome-vfs to error.

For example, if an unescaped path contained a space -- eg /home/user/work folder/letter.odt -- trying to move "letter.odt" to the Trash using Nautilus resulted in an alert box presenting as follows:

Error "Not on the same file system" while deleting

Clicking the default "Retry" button did not result in the file being moved to the Trash. The practical consequence: this bug meant files with paths that included spaces could not be deleted using Nautilus.

With this update, gnome-vfs properly properly unescapes paths when the path is required for a system call. The paths are, consequently, parsed properly and errors such as the example above no longer occur. (BZ#589874)

Users should upgrade to these updated packages, which resolve this issue.

1.43. gnupg

1.43.1. RHBA-2010:0513: bug fix update

An updated gnupg package that fixes a bug is now available.

GnuPG is a utility for encrypting data and creating digital signatures.

This package addresses the following bug:

* compressed, old-style Modification Detection Code (MDC) packets do not include length information and the decompressor uses an implicit end point. In some circumstances (message length was likely the determining circumstance) this could result in more bytes being supplied to the decompressor than were needed. This resulted in GnuPG failing to decrypt the file and returning an error as follows:

gpg: [don't know]: invalid packet (ctb=14)

With this update, the packet parsing was changed: MDC packets are now decoded independently and are no longer passed to the packet parser that lead to the errors. (BZ#592845).

GnuPG users should upgrade to this updated package, which resolves this issue.

1.44. gtk2

1.44.1. RHBA-2010:0913: bug fix update

An updated gtk2 package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.

* Previously, the file chooser dialog in GTK+ did not open the default selected file by pressing the Enter key when the location field was visible. With this update, the default selected file opens regardless of the visibility of the location. (BZ#648555)

* Previously, the file chooser dialog in GTK+ did not change into the default directory by pressing the Enter key when the location field was visible. With this update, the default selected directory opens regardless of the visibility of the location. (BZ#648557)

All GTK+ users are advised to upgrade to this updated package, which resolves these issues.

1.45. hal

1.45.1. RHBA-2011:0108: bug fix and enhancement update

Updated hal packages that fix two bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The HAL daemon collects and maintains information about the hardware on the system from several sources, and provides a live device list through D-BUS.

This update fixes the following bugs:

* Prior to this update, the "noexec" option was enforced when mounting CDs, preventing scripts on that media from being run automatically. However, this also prevented applications that rely on executing from media from working correctly. Since the intended level of protection provided by this feature is minimal, and there are other ways to achieve it, the feature has been removed and the "noexec" option is no longer enforced. (BZ#480716)

* Previously, it was possible to mount both data CDs and DVDs, even though the "storage.policy.should_mount" option was set to "false". As a result, system administrators were unable to disable mounting of such media. This error has been fixed, and the "storage.policy.should_mount" option now works as expected. (BZ#454923)

As well, this update adds the following enhancement:

* System administrators can now set additional command line options that are passed to the daemon by creating the /etc/sysconfig/haldaemon file. This allows users to increase the child timeout value if a large number of devices are attached to the system. (BZ#576045)

Users of are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

1.46. hplip

1.46.1. RHBA-2011:0058: bug fix update

Updated hplip packages that resolve several issues are now available.

The hplip (Hewlett-Packard Linux Imaging and Printing Project) provides drivers for HP printers and multi-function peripherals. These updated hplip packages fix the following bugs:

* The libsane-hpaio package no longer depends on the hpijs package. (BZ#457440)

* Some Python scripts used the interpreter line '#!/usr/bin/env python' and during the execution, they might have been using an incorrect Python version. With this update, the interpreter line is changed and uses the path /usr/bin/python. (BZ#521857)

All hplip users are advised to upgrade to these updated packages, which resolve these issues.

1.47. httpd

1.47.1. RHBA-2011:0130: bug fix update

Updated httpd packages that resolve several issues are now available.

The Apache HTTP Server is a popular web server.

These updated packages provide fixes for the following bugs:

* In a reverse proxy configuration, the Date field in the response headers sent by an upstream server was replaced by a Date header using the local time at the proxy server. This could result in inappropriate caching of the response in browsers or downstream caches. The Date header is no longer replaced in a reverse proxy configuration and caching is correct. (BZ#565865)

* Due to a bug in the filter initialization process, filters configured using the "mod_filter" module were not handled correctly if a "sub-request" took place. For example, using the "FilterChain" directive to configure the "DEFLATE" compression filter with a Server-Side-Include page could result in pages which were only partially compressed. With this update filters used with mod_filter operate correctly. (BZ#570628)

* If using a WebDAV repository, uploading new content with the "PUT" HTTP method could remove an existing resource if an error occurred during the upload. This was caused by a bug in failure handling. With this update the content remains in place. (BZ#572910)

* The output of the "mod_deflate" module could have contained corrupted or empty HTTP responses when either response compression was enabled, or when acting as a proxy, expansion of compressed responses from upstream servers. The compressed responses are now fixed. (BZ#593715, BZ#612211)

* If the "mod_dbd" module was used, due to a memory lifetime issue in the module, an error message from glibc concerning "double free or corruption" could be raised when the httpd daemon was stopped, and the daemon would terminate unexpectedly. This update fixes the memory lifetime issues. The error message no longer appears and the server exits normally. (BZ#633955)

* When executing "service httpd stop", a 10-seconds timeout is used before terminating the httpd parent process in case of error. If this timeout was insufficient, resources did not allow the parent process to terminate cleanly and could be leaked. The "STOP_TIMEOUT" environment variable has been introduced which can be used in the "/etc/sysconfig/httpd" configuration file to change the timeout. This can be used to allow a longer delay and fix resource leaks if the httpd parent is slow to terminate. (BZ#644223)

* If arguments passed to the "ab" benchmarking program triggered a memory allocation failure, ab could terminate with a Segmentation Fault error. The memory allocation failure is now trapped earlier, and the program exits gracefully with an error message. (BZ#645845)

All httpd users are advised to upgrade to these updated packages, which resolve these issues.

1.48. hwdata

1.48.1. RHEA-2011:0048: enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 5.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

This update adds the following enhancements:

* The usb.ids database has been updated to include the information about the Intel Corporation Rate Matching Hub (RMH) device. (BZ#516932)

* The pci.ids database has been updated to include the support for the NetXen P3+ based Converged Network Adapter (CNA) from QLogic. (BZ#571899)

* In the pci.ids database, the vendor name for the Virtio driver has been changed from "Qumranet, Inc." to "Red Hat, Inc." (BZ#591790)

* The pci.ids database has been updated according to the latest upstream changes. (BZ#627930)

Users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

1.49. icu

1.49.1. RHBA-2011:0127: bug fix update

Updated icu packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

This update fixes the following bugs:

* Due to a bug in the ICU library, when the "Kartika.ttf" font was installed, selecting "Format Cells" from the menu caused OpenOffice.org Calc to terminate unexpectedly. With this update, this error has been fixed, and the presence of "Kartika.ttf" no longer causes OpenOffice.org Calc to crash. (BZ#457656)

* On 64-bit PowerPC architectures, an attempt to load the "intl" module for PHP 5.3 could be incorrectly denied by SELinux. These updated packages no longer trigger the SELinux denial, and the "intl" module can now be loaded as expected. (BZ#654590)

Users of icu should upgrade to these updated packages, which resolve these issues.

1.50. ImageMagick

1.50.1. RHBA-2010:0784: bug fix update

Updated ImageMagick packages that fix a bug are now available for Red Hat Enterprise Linux 5.

ImageMagick is an image display and manipulation tool for the X Window System that can read and write multiple image formats.

This update fixes the following bug:

* Previously, converting an image to PostScript by running the convert utility with the "-page" command line option caused the utility to produce an invalid output with a wrong page size. With this update, the page size is counted properly, and the convert utility now produces the expected output. (BZ#640587)

Users of ImageMagick are advised to upgrade to these updated packages, which resolve this issue.

1.51. initscripts

1.51.1. RHBA-2011:0075: bug fix update

An updated initscripts package that fixes various bugs is now available.

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

This updated initscripts package includes fixes for the following bugs:

* Stale PID files in /var/run/dovecot/ were not removed upon system start-up. Consequently, this caused Dovecot to fail to start. With this update, all files in /var/run/dovecot/ are removed upon boot. (BZ#492994)

* The documentation for the 'DHCP_HOSTNAME' parameter in 'ifcfg' configuration files was missing. With this update, the documentation for 'DHCP_HOSTNAME' was added to the sysconfig.txt file. (BZ#498052)

* For non-root partitions, issuing a 'forcequotacheck' did not run a 'quotacheck' on LVM partitions. With this update, the 'quotacheck' now runs after the local file systems have been mounted. (BZ#499207)

* Due to an incorrect loading of the bonding driver module, certain systems may not have been able to activate a bonding interface. The bonding driver is now correctly loaded when an 'ifcfg' script contains the 'BONDING_OPTS' option. (BZ#516569)

* Until the 'restorecond' service was started, the /var/run/utmp* and /var/log/wtmp* files had the wrong SELinux context. With this update, the correct SELinux context is set right after the aforementioned files are created. (BZ#519748)

* On system start-up, the 'rc.sysinit' script tried to activate individual 'dmraid' subsets. This operation lead to a failure and a display of error messages. With this update, the 'dmraid' tool is queried with different options to prevent the aforementioned behavior. (BZ#524356)

* The 'xend' daemon could not be started on a read-only root system because the daemon was not present in the /etc/rwtab configuration file. With this update, an entry was added to the /etc/rwtab file, which mounts a writable directory on a tmpfs file system. (BZ#526046)

* Calling the 'ifup' command with a network interface, where the name of the network interface is a substring of an already active interface, resulted in an error. With this update, the checks to test whether an interface is already active have been fixed so that an active interface can be activated now. (BZ#538863)

* The 'unicode_start' process was called with the wrong setting which resulted in an incorrect Unicode font display. With this update, 'unicode_start' is now started with $UNIMAP instead of $SYSFONTACM, thus, fixing the issue. (BZ#557089)

* When running the daemon() function from an initscript and using the '--user' option, the daemon ran /sbin/runuser to execute. This command clears the environment by default. This could cause a problem because some initscripts set environment variables for their programs' use. With this update, the daemon() function does not start a login shell anymore, thus fixing the aforementioned the issue. (BZ#564093)

* Upon interactive startup, some of the displayed shortcut keys did not work. With this update, a correction of the translation files has fixed the aforementioned issue. (BZ#566579)

* If SELinux was in enforcing mode, the 'racoon' daemon could not be signaled to reload its configuration. This was caused by the killall signal being called with the full path to the 'racoon' daemon. This resulted in SELinux denying the access to /proc/[pid]/exe and the 'racoon' daemon not getting a HUP signal. With this update, the killall signal is called without the full path, resulting in a correctly reloaded configuration file. (BZ#567295)

* An attempt to reboot or shut down a system with a running iSCSI daemon could cause the system to stop responding. This was caused by the system waiting for iSCSI devices to sync, even though the network was already shut down. With this update, the /etc/rc.d/init.d/network startup script has been modified and the system can be shut down or rebooted as expected. (BZ#583218)

All users of initscripts are advised to upgrade to this updated package, which resolves these issues.

1.51.2. RHBA-2010:0885: bug fix update

An updated initscripts package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

This update fixes the following bugs:

* Prior to this update, an attempt to reboot or shut down a system with a running Internet Small Computer System Interface (iSCSI) daemon may have caused the system to stop responding. This was caused by the fact that the system was waiting for iSCSI devices to sync, even though the network was already shut down. With this update, the /etc/rc.d/init.d/network startup script has been modified not to deactivate network interfaces when the iSCSI daemon is running, and the system can be shut down or rebooted as expected. (BZ#630538)

* Due to an incorrect loading of the bonding driver module, certain systems may not have been able to activate a bonding interface. This error has been fixed, and the bonding driver is now correctly loaded when an ifcfg script contains the "BONDING_OPTS" option. (BZ#652250)

All users are advised to upgrade to this updated package, which resolves these issues.

1.52. iprutils

1.52.1. RHEA-2011:0092: bug fix and enhancement update

An updated iprutils package that fixes a bug and provides an enhancement is now available.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the ipr SCSI storage device driver.

This updated iprutils package fixes the following bug:

* The manual page for iprdbg tool was missing. This update adds the manual page. (BZ#555777)

In addition, this updated iprutils package provides the following enhancement:

* The iprutils package supports 64-bit PCI-E x8 Gen2 6Gb SAS adapters. (BZ#563573)

Users are advised to upgrade to this updated iprutils package, which resolves this issue and adds this enhancement.

1.53. ipsec-tools

1.53.1. RHBA-2010:0645: bug fix update

An updated ipsec-tools package that fixes various bugs is now available.

The ipsec-tools package contains configuration and management tools for IPsec.

This updated ipsec-tools package resolves the following bugs:

* when clients connected and disconnected under load the racoon daemon stopped responding for a few minutes due to a race condition in the code handling dumps of the Security Association Database (SAD) from the kernel through a pfkey socket. The updated package uses a separate pfkey socket for the SA database dumps effectively removing the possibility for the race condition. (BZ#609084)

* when receiving a delete notification for the IKE SA the racoon daemon incorrectly deleted also the IPsec SA associated with the IKE SA. The updated package just expires the IKE SA and waits for the IPsec SAs to expire before the IKE SA is purged from the racoon memory. (BZ#609085)

* when looking at the security policy database entries the racoon daemon used to match inexact entries even if there was an exact entry in the database. The updated package matches the exact entry before falling back to inexact matching. (BZ#609087)

* when dumping the pfkey database the kernel used to return only part of the database due to the small socket buffer size. When racoon was deployed on a system with a large number of network security policy entries, the racoon could not find all of the security policy entries in the database. The updated package supports a new configuration option pfkey_buffer to the racoon.conf file that allows to set the buffer size as appropriate for the deployment requirements. (BZ#609090)

All users of IPsec Tools are advised to upgrade to this updated package, which resolves these issues.

1.54. ipvsadm

1.54.1. RHEA-2011:0086: enhancement update

An enhanced ipvsadm package is now available.

This updated ipvsadm package adds the following enhancement:

* UDP packets were treated as if being connected: if multiple UDP packets reached the load balancer within a short period of time, all packets were sent to the same real server. This update adds One-Packet Scheduler, which load-balances the UDP packets. One-Packet Scheduler treats every UDP packet as a new connection, and picks a server based on the scheduling algorithm. (BZ#633636)

Users of ipvsadm are advised to upgrade to this updated package, which adds this enhancement.

1.55. iscsi-initiator-utils

1.55.1. RHBA-2011:0072: bug fix update

An updated iscsi-initiator-utils package that fixes various bugs is now available for Red Hat Enterprise 5.

The iscsi-initiator-utils package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol (IP) networks.

This update fixes the following bugs:

* Previously, the iSCSI offload login did not consistently work with the Broadcom iSCSI offload driver bnx2i. With this update, the iSCSI offload login works consistently. (BZ#580743)

* When the "stop" operation was invoked, the iscsid init script did not remove the process identifier (PID) file. This update modifies the iscsid script to remove the PID file during the stop operation. (BZ#583086)

* Previously, the open-iscsi administration utility (iscsiadm) interface update operation returned an error code, even though the operation was successful. This error has been fixed, the error detection code has been corrected, and the interface update now behaves as expected. (BZ#588990)

* Since the iscsi init script did not detect if the iscsid service successfully started, running it with the "start" command returned an invalid code. To resolve this issue, this update uses different return values for starting the daemon and for the start operation. (BZ#608074)

* Due to iscsid sharing the "semarg" structure between multiple devices, a deadlock may have occurred when logging was initiated. With this update, each process is assigned its own structure, so that such deadlocks no longer occur. (BZ#624344)

* When encountering a multi-PDU sequence, the open-iscsi administration utility (iscsiadm) sent incorrect initiator task tags (ITT), causing the discovery to fail. With this update, the ITT initialization and allocation sends the correct tags, and iscsiadm works as expected. (BZ#633122) * A host removal could become suspended when the bnx2i, cxgb3i, or be2iscsi drivers were used and iSCSI sessions could not be cleaned up. With this update, the iSCSI daemon has been corrected to handle the error event, and a host removal behaves as expected. (BZ#640111)

This update also adds the following new features:

* Previously, the target portal management in the iSCSI ecosystem was very time consuming. This update adds iSNS and SCN support to the iscsi-initiator-utils tool to simplify management tasks. (BZ#521222, BZ#629400) * This update contains the current IP-0.5.15 Broadcom user-space daemon, and adds VLAN support for iSCSI. (BZ#568517)

* This update adds components to support IPv6, VLAN, and the new Broadcom BCM57712 10G device. (BZ#568609)

All users of iscsi-initiator-utils are advised to upgrade to this updated package, which resolves these issues.

1.55.2. RHBA-2010:0721: bug fix update

An updated iscsi-initiator-utils package that fixes a bug is now available.

The iscsi-initiator-utils package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

This updated iscsi-initiator-utils package fixes the following bug:

* Previously, iscsiadm did not contain a discovery mode with an update option. This prevented vdsm to discover targets with CHAP (Challenge-Handshake Authentication Protocol) authentication. This update adds a iscsiadm discoverydb mode ('iscsiadm -m discoverydb') which fixes this issue and can be used to create, store and edit discovery records. (BZ#604649)

* Previously, iscsid shared the 'semarg' structure between multiple devices and thus caused a deadlock to occur when logging was initiated. With this update, each process is assigned its own structure and deadlocks no longer occurs during the logging process. (BZ#632094)

All users of iscsi-initiator-utils are advised to upgrade to this updated package, which resolves this issue.

1.56. isns-utils

1.56.1. RHBA-2011:0070: bug fix update

An updated isns-utils package that supports SCNs is now available for Red Hat Enterprise Linux 5.

The iSNS package contains the daemon and tools to setup a iSNS server, and iSNS client tools. The Internet Storage Name Service (iSNS) protocol allows automated discovery, management and configuration of iSCSI and Fibre Channel devices (using iFCP gateways) on a TCP/IP network.

* Previously, the iSNS server's state change notification (SCN) support did not conform to iSNS RFC. As a result, the server did neither send nor handle SCNs. With this update, the server conforms to iSNS RFC and SCNs are handled correctly. (BZ#521221)

* This update adds the upstream SCN changes. (BZ#629399)

All iSNS users are advised to upgrade to this updated package, which resolves this issue.

1.57. java-1.6.0-openjdk

1.57.1. RHEA-2010:0621: enhancement update

A new set of OpenJDK packages that update Daylight Saving Time observations for Egypt is now available.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. The Java Runtime Environment (JRE) contains the software and tools that users need to run applications written using the Java programming language.

These updated packages address the following change to Daylight Saving Time (DST) observations:

* During Ramadan, that is, during the period between 2010-08-11 and 2010-09-08, Egypt will suspend DST. The DST period will be officially restored on 2010-09-09. (BZ#622836)

All users, especially those in the locale affected by this time change and users interacting with people or systems in the affected locale, are advised to upgrade to these packages, which add this enhancement.

1.58. jwhois

1.58.1. RHBA-2010:0745: bug fix and enhancement update

An updated jwhois package that provides fixes for bugs and contains enhancements is now available for Red Hat Enterprise Linux 5.

The jwhois package is a whois client which is used to obtain information about domain names and IP addresses from whois servers.

This updated jwhois package provides fixes for the following bugs:

* previously, jwhois on machines with IPv4 connection did not work correctly when querying whois server with both IPv4 and IPv6 addresses. This issue is fixed in this updated jwhois package. (BZ#415491)

* previously, jwhois did not follow referral whois for .com and .net domains. This issue is fixed in this updated jwhois package. (BZ#479061)

This updated jwhois package provides the following enhancements:

* previously, jwhois did not contain whois server details for .ae domains. Whois queries for these domains would be directed to whois.uaenic.ae. Because whois.uaenic.ae does not contain information on .ae domains, the query would fail. The configuration file contained in this updated jwhois package was updated and directs queries for .ae domains to whois.aeda.net.ae. (BZ#509475)

* previously, jwhois did not contain whois server details for .im domains. Whois queries for these domains would be directed to www.nic.im. The configuration file contained in this updated jwhois package directs queries for .im domains to whois.nic.im. (BZ#512930)

All whois client users are advised to upgrade to this updated package, which resolves this issue and addresses the latest known whois server changes.

1.59. kdebase

1.59.1. RHBA-2010:0806: bug fix update

Updated kdebase packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase packages include core applications for the K Desktop Environment.

These updated kdebase packages fix the following bug:

* Previously, the 'kdesktop_lock' process did not run on multi-user systems when another user had already ran an instance of 'kdesktop_lock'. This update allows 'kdesktop_lock' to work on multi-user systems when multiple single users are logged in. (BZ#499442)

All users of kdebase are advised to upgrade to these updated packages, which resolve this issue.

1.60. kernel

1.60.1. RHSA-2011:0927 - Important: kernel security and bug fix update

> **Important**
>
> This update has already been released as the security errata RHSA-2011:0927

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

* An integer overflow flaw in `ib_uverbs_poll_cq()` could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2010-4649, Important)

* A race condition in the way new InfiniBand connections were set up could allow a remote user to cause a denial of service. (CVE-2011-0695, Important)

* A flaw in the Stream Control Transmission Protocol (SCTP) implementation could allow a remote attacker to cause a denial of service if the `sysctl` *`net.sctp.addip_enable`* and *`auth_enable`* variables were turned on (they are off by default). (CVE-2011-1573, Important)

* Flaws in the `AGPGART` driver implementation when handling certain IOCTL commands could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2011-1745, CVE-2011-2022, Important)

* An integer overflow flaw in `agp_allocate_memory()` could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2011-1746, Important)

* A flaw allowed **napi_reuse_skb()** to be called on VLAN (virtual LAN) packets. An attacker on the local network could trigger this flaw by sending specially-crafted packets to a target system, possibly causing a denial of service. (CVE-2011-1576, Moderate)

* An integer signedness error in **next_pidmap()** could allow a local, unprivileged user to cause a denial of service. (CVE-2011-1593, Moderate)

* A flaw in the way the Xen hypervisor implementation handled CPUID instruction emulation during virtual machine exits could allow an unprivileged guest user to crash a guest. This only affects systems that have an Intel x86 processor with the Intel VT-x extension enabled. (CVE-2011-1936, Moderate)

* A flaw in **inet_diag_bc_audit()** could allow a local, unprivileged user to cause a denial of service (infinite loop). (CVE-2011-2213, Moderate)

* A missing initialization flaw in the XFS file system implementation could lead to an information leak. (CVE-2011-0711, Low)

* A flaw in **ib_uverbs_poll_cq()** could allow a local, unprivileged user to cause an information leak. (CVE-2011-1044, Low)

* A missing validation check was found in the signals implementation. A local, unprivileged user could use this flaw to send signals via the **sigqueueinfo** system call, with the **si_code** set to *SI_TKILL* and with spoofed process and user IDs, to other processes. Note: This flaw does not allow existing permission checks to be bypassed; signals can only be sent if your privileges allow you to already do so. (CVE-2011-1182, Low)

* A heap overflow flaw in the EFI GUID Partition Table (GPT) implementation could allow a local attacker to cause a denial of service by mounting a disk containing specially-crafted partition tables. (CVE-2011-1776, Low)

* Structure padding in two structures in the Bluetooth implementation was not initialized properly before being copied to user-space, possibly allowing local, unprivileged users to leak kernel stack memory to user-space. (CVE-2011-2492, Low)

Red Hat would like to thank Jens Kuehnel for reporting CVE-2011-0695; Vasiliy Kulikov for reporting CVE-2011-1745, CVE-2011-2022, and CVE-2011-1746; Ryan Sweat for reporting CVE-2011-1576; Robert Swiecki for reporting CVE-2011-1593; Dan Rosenberg for reporting CVE-2011-2213 and CVE-2011-0711; Julien Tinnes of the Google Security Team for reporting CVE-2011-1182; Timo Warns for reporting CVE-2011-1776; and Marek Kroemeke and Filip Palian for reporting CVE-2011-2492.

Bug fixes:

BZ#709767

Prior to this update, a race in the GFS2 glock state machine could cause nodes to become unresponsive. Specifically, all nodes but one would hang, waiting for a particular glock. All the waiting nodes had the **W** (*Waiting*) bit set. The remaining node had the glock in the *Exclusive Mode* (**EX**) with no holder records. The race was caused by the **Pending Demote** bit, which could be set and then immediately reset by another process. With this update, the **Pending Demote** bit is properly handled, and GFS2 nodes no longer hang.

BZ#711519

Multiple GFS2 nodes attempted to unlink, rename, or manipulate files at the same time, causing various forms of file system corruption, panics, and withdraws. This update adds multiple checks for **dinode**'s *i_nlink* value to assure inode operations such as link, unlink, or rename no longer cause the aforementioned problems.

BZ#713948

Under certain circumstances, a command could be left unprocessed when using either the `cciss` or the `hpsa` driver. This was because the HP Smart Array controller considered all commands to be completed when, in fact, some commands were still left in the completion queue. This could cause the file system to become read-only or panic and the whole system to become unstable. With this update, an extra read operation has been added to both of the aforementioned drivers, fixing this issue.

BZ#707899

Hot removing a PCIe device and, consequently, hot plugging it again caused kernel panic. This was due to a PCI resource for the SR-IOV Virtual Function (vf) not being released after the hot removing, causing the memory area in the *pci_dev* struct to be used by another process. With this update, when a PCIe device is removed from a system, all resources are properly released; kernel panic no longer occurs.

BZ#710426

The event device (`evdev`) failed to lock data structures when adding or removing input devices. As a result, kernel panic occurred in the `evdev_release` function during a system restart. With this update, locking of data structures works as expected, and kernel panic no longer occurs.

BZ#703056

Running a reboot test on an iSCSI root host resulted in kernel panic. When the `iscsi_tcp` module is destroying a connection it grabs the `sk_callback_lock` and clears the `sk_user_data/conn` pointer to signal that the callback functions should not execute the operation. However, some functions were not grabbing the lock, causing a NULL pointer kernel panic when `iscsi_sw_tcp_conn_restore_callbacks` was called and, consequently, one of the callbacks was called. With this update, the underlying source code has been modified to address this issue, and kernel panic no longer occurs.

BZ#712034

The `mpt fusion` driver has been upgraded to version 3.4.17, which provides a number of bug fixes and enhancements over the previous version.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.60.2. RHSA-2011:0833 - Important: kernel security and bug fix update

> **Important**
>
> This update has already been released as the security errata RHSA-2011:0833

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

* A flaw in the `dccp_rcv_state_process()` function could allow a remote attacker to cause a denial of service, even when the socket was already closed. (CVE-2011-1093, Important)

* Multiple buffer overflow flaws were found in the Linux kernel's Management Module Support for Message Passing Technology (MPT) based controllers. A local, unprivileged user could use these flaws to cause a denial of service, an information leak, or escalate their privileges. (CVE-2011-1494, CVE-2011-1495, Important)

* A missing validation of a null-terminated string data structure element in the `bnep_sock_ioctl()` function could allow a local user to cause an information leak or a denial of service. (CVE-2011-1079, Moderate)

* Missing error checking in the way page tables were handled in the Xen hypervisor implementation could allow a privileged guest user to cause the host, and the guests, to lock up. (CVE-2011-1166, Moderate)

* A flaw was found in the way the Xen hypervisor implementation checked for the upper boundary when getting a new event channel port. A privileged guest user could use this flaw to cause a denial of service or escalate their privileges. (CVE-2011-1763, Moderate)

* The start_code and end_code values in `/proc/<pid>/stat` were not protected. In certain scenarios, this flaw could be used to defeat Address Space Layout Randomization (ASLR). (CVE-2011-0726, Low)

* A missing initialization flaw in the `sco_sock_getsockopt()` function could allow a local, unprivileged user to cause an information leak. (CVE-2011-1078, Low)

* A missing validation of a null-terminated string data structure element in the `do_replace()` function could allow a local user who has the CAP_NET_ADMIN capability to cause an information leak. (CVE-2011-1080, Low)

* A buffer overflow flaw in the DEC Alpha OSF partition implementation in the Linux kernel could allow a local attacker to cause an information leak by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1163, Low)

* Missing validations of null-terminated string data structure elements in the `do_replace()`, `compat_do_replace()`, `do_ipt_get_ctl()`, `do_ip6t_get_ctl()`, and `do_arpt_get_ctl()` functions could allow a local user who has the **CAP_NET_ADMIN** capability to cause an information leak. (CVE-2011-1170, CVE-2011-1171, CVE-2011-1172, Low)

* A heap overflow flaw in the Linux kernel's EFI GUID Partition Table (GPT) implementation could allow a local attacker to cause a denial of service by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1577, Low)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2011-1494 and CVE-2011-1495; Vasiliy Kulikov for reporting CVE-2011-1079, CVE-2011-1078, CVE-2011-1080, CVE-2011-1170, CVE-2011-1171, and CVE-2011-1172; Kees Cook for reporting CVE-2011-0726; and Timo Warns for reporting CVE-2011-1163 and CVE-2011-1577.

Bug fixes:

BZ#689699

Under certain circumstances, a deadlock could occur between the **khubd** process of the USB stack and the **modprobe** of the **usb-storage** module. This was because the **khubd** process, when attempting to delete a usb device, waited for the reference count of **knode_bus** to be of value **0**. However, **modprobe**, when loading the **usb-storage** module, scans all USB devices and increments the reference count, preventing the **khubd** process to continue. With this update, the underlying source code has been modified to address this issue, and a deadlock no longer occurs in the aforementioned case.

BZ#690795

The **ext4** file system could end up corrupted after a power failure occurred even when file system barriers and local write cache was enabled. This was due to faulty barrier flag setting in **WRITE_SYNC** requests. With this update, this issue has been fixed, and **ext4** file system corruption no longer occurs.

BZ#688855

Due to incorrect ordering of **glock**s, a deadlock could occur in the code which reclaims unlinked inodes when multiple nodes were trying to deallocate the same unlinked inode. This update resolves the lock ordering issue, and unlinked inodes are now properly deallocated under all circumstances.

BZ#699609

In a four node cluster environment, a deadlock could occur on machines in the cluster when the nodes accessed a GFS2 file system. This resulted in memory fragmentation which caused the number of network packet fragments in requests to exceed the network hardware limit. The network hardware firmware dropped the network packets exceeding this limit. With this update, the network packet fragmentation was reduced to the limit of the network hardware, no longer causing problems during memory fragmentation.

BZ#692370

Previously, some IBM storage arrays (IBM 1745 and 1746) could have stopped responding or fail to load to the device list of the **scsi_dh_rdac** kernel module. This occurred because the **scsi_dh_rdac** device list did not contain these storage arrays. With this update, the arrays have been added to the list, and they are now detected and operate as expected.

BZ#693755

In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by non-NFS users of the server. An application on a client may then be able to open the file at its old location (read old cached data from it and perform read locks on it), long after the file no longer exists at that location on the server. To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing the value **0** to the **/proc/sys/fs/leases-enable** file (ideally on boot, before the NFS server is started). This change prevents NFSv4 delegations from being given out, restoring correctness at the expense of some performance.

BZ#696503

Under certain circumstances, a command could be left unprocessed when using either the **cciss** or the **hpsa** driver. This was because the HP Smart Array controller considered all commands to be completed when, in fact, some commands were still left in the completion queue. This could cause the file system to become read-only or panic and the whole system to become unstable. With this update, an extra read operation has been added to both of the aforementioned drivers, fixing this issue.

BZ#696136

This update fixes a bug in the way isochronous input data was returned to user space for **usbfs** (USB File System) transfers, resolving various audio issues.

BZ#690134

Previously, on VMware, the time ran too fast on virtual machines with more than 4GHz TSC (Time Step Counter) processor frequency if they were using PIT/TSC based timekeeping. This was due to a calculation bug in the **get_hypervisor_cycles_per_sec** function. This update fixes the

calculation, and timekeeping works correctly for such virtual machines

BZ#[689808](), BZ#[689805]()

For certain NICs, the **operstate** state (stored in, for example, the
/sys/class/net/eth0/operstate file) was showing the **unknown** state even though the NIC
was working properly. This was due to the fact that at the end of a probe operation, the
netif_carrier_off was not being called. With this update, the **netif_carrier_off** is
properly called after a probe operation, and the **operstate** state now correctly displays the
operational state of an NIC.

BZ#[688156]()

Under certain circumstances, a crash in the kernel could occur due to a race condition in the
lockd_down function, which did not wait for the **lockd** process to come down. With this update,
the **lockd_down** function has been fixed, and the kernel no longer crashes.

BZ#[693751]()

Enabling the Header Splitting mode on all Intel 82599 10 Gigabit Ethernet hardware could lead to
unpredictable behavior. With this update, the Header Splitting mode is never enabled on the
aforementioned hardware. Additionally, this update fixes VM pool allocation issues based on MAC
address filtering, and limits the scope of VF access to promiscuous mode.

BZ#[689700]()

Prior to this update, if a CT/ELS pass-through command timed out, the QLogic 8Gb Fibre Channel
adapter created a firmware dump. With this update, firmware dumps are no longer created when
CT/ELS pass-through requests time out as a firmware dump is not necessary in this case.

BZ#[701222]()

Configuring a network bridge with no STP (Spanning Tree Protocol) and a **0** forwarding delay could
result in the flooding of all packets on the link for 20 seconds due to various issues in the source
code. With this update, the underlying source code has been modified to address this issue, and a
traffic flood on the network bridge no longer occurs.

BZ#[699808]()

Setting a DASD (Direct Access Storage Device) device offline while another process is trying to
open that device caused a race in the **dasd_open** function. The **dasd_open** function tried to read
a pointer from the **private_data** field after the structure has already been freed, resulting in a
dereference of an invalid pointer. With this update, the aforementioned pointer is now stored in a
different structure; thus, preventing the race condition.

BZ#[690239]()

GFS2 (Global File System 2) keeps track of the list of resource groups to allow better performance
when allocating blocks. Previously, when the user created a large file in **GFS2**, **GFS2** could have run
out of allocation space because it was confined to the recently-used resource groups. With this
update, **GFS2** uses the MRU (Most Recently Used) list instead of the list of the recently-used
resource groups. The MRU list allows **GFS2** to use all available resource groups and if a large span
of blocks is in use, **GFS2** uses allocation blocks of another resource group.

BZ#[696908]()

A cpu mask that is being waited on after an IPI call was not the same cpu mask that was being
passed into the IPI call function. This could result in not up-to-date values being stored in the
cache. The loop in the **flush_tlb_others()** function waited for the cpu mask to be cleared,

however, that cpu mask could have been incorrect. As a result, the system could become unresponsive. With this update, the cpu mask being waited on is the same cpu mask used in the IPI call function, and the system no longer hangs.

BZ#689339

A buffer overflow flaw was found in the Linux kernel's Cluster IP hashmark target implementation. A local, unprivileged user could trigger this flaw and cause a local denial of service by editing files in the **/proc/net/ipt_CLUSTERIP/** directory. Note: On Red Hat Enterprise MRG, only root can write to files in the **/proc/net/ipt_CLUSTERIP/** directory by default. This update corrects this issue as a preventative measure in case an administrator has changed the permissions on these files. Red Hat would like to thank Vasiliy Kulikov for reporting this issue.

BZ#696181

Prior to this update, a FW/SW semaphore collision could lead to an link establishment failure on an SFP+ (Small Form-factor Pluggable) transceiver module. With this update, the underlying source code has been modified to address this issue, and SFP+ modules work as expected.

BZ#699610

The **kdump** kernel could fail when handling an IPI (Inter-processor interrupt) that was in-flight as the initial kernel crashed. This was due to an IPI-related data structure within **kdump**'s kernel not being properly initialized, resulting in a dereference of an invalid pointer. This update addresses this issue, and the **kdump** kernel no longer fails upon encountering an in-flight IPI.

BZ#679304

Prior to this update, a collection of world-writable **sysfs** and **procfs** files allowed an unprivileged user to change various settings, change device hardware registers, and load certain firmware. With this update, permissions for these files have been changed.

BZ#697448

An NFS server uses reference-counted structures, called **auth_domains**, to identify which group of clients (for example, 192.168.0.0/24 or *.foo.edu) the client who sent an RPC request belongs to. The server NLM code incorrectly took an extra reference of the **auth_domain** associated with each NLM RPC request, and never dropped that reference. The reference count is an unsigned 32-bit value, so after 232 (about 4 billion) lock operations from the same client or group of clients, the reference count would overflow to 0, and the kernel would incorrectly think that the **auth_domain** should be freed. As a result, the kernel would panic. This update removes the extra reference-count increment from the server NLM code, and the kernel no longer panics.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.60.3. RHSA-2011:0429 - Moderate: kernel security and bug fix update

Important

This update has already been released as the security errata RHSA-2011:0429

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

* A missing boundary check was found in the `dvb_ca_ioctl()` function in the Linux kernel's `av7110` module. On systems that use old DVB cards that require the `av7110` module, a local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges. (CVE-2011-0521, Important)

* An inconsistency was found in the interaction between the Linux kernel's method for allocating NFSv4 (Network File System version 4) ACL data and the method by which it was freed. This inconsistency led to a kernel panic which could be triggered by a local, unprivileged user with files owned by said user on an NFSv4 share. (CVE-2011-1090, Moderate)

* A NULL pointer dereference flaw was found in the Generic Receive Offload (GRO) functionality in the Linux kernel's networking implementation. If both GRO and promiscuous mode were enabled on an interface in a virtual LAN (VLAN), it could result in a denial of service when a malformed VLAN frame is received on that interface. (CVE-2011-1478, Moderate)

* A missing security check in the Linux kernel's implementation of the `install_special_mapping()` function could allow a local, unprivileged user to bypass the mmap_min_addr protection mechanism. (CVE-2010-4346, Low)

* An information leak was found in the Linux kernel's `task_show_regs()` implementation. On IBM S/390 systems, a local, unprivileged user could use this flaw to read `/proc/<PID>/status` files, allowing them to discover the CPU register values of processes. (CVE-2011-0710, Low)

* A missing validation check was found in the Linux kernel's `mac_partition()` implementation, used for supporting file systems created on Mac OS operating systems. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains specially-crafted partitions. (CVE-2011-1010, Low)

Red Hat would like to thank Ryan Sweat for reporting CVE-2011-1478; Tavis Ormandy for reporting CVE-2010-4346; and Timo Warns for reporting CVE-2011-1010.

Bug fixes:

BZ#675909

> Deleting a file on a GFS2 file system caused the inode, which the deleted file previously occupied, to not be freed. Specifically, this only occurred when a file was deleted on a different inode than the inode that created it. The mechanism for ensuring that inodes are correctly deallocated when the final close occurs was dependent on a previously corrected bug (BZ#504188). In order to ensure that iopen glocks are not cached beyond the lifetime of the inode, and thus prevent deallocation by another inode in the cluster, this update marks the iopen glock as not to be cached during the inode disposal process.

BZ#684128

> A call to the *HP_GETHOSTINFO* ioctl (I/O Control) in the `mptctl` module could result in the MPT (Message Passing Technology) fusion driver being reset due to erroneous detection of completed ioctl commands. With this update, the message context sent to the `mptctl` module is stored (previously, it was zeroed). When an ioctl command completes, the saved message context is used to recognize the completion of the message, thus resolving the faulty detection.

BZ#675664

A bug was discovered in the bonding driver that occurred when using **netpoll** and changing, adding or removing slaves from a bond. The misuse of a per-cpu flag in the bonding driver during these operations at the wrong time could lead to the detection of an invalid state in the bonding driver, triggering kernel panic. With this update, the use of the aforementioned per-cpu flag has been corrected and a kernel panic no longer occurs.

BZ#679747

The fix introduced with BZ#560013 added a check for detection of the **northbridge** device into the **amd_fixup_dcm()** function to make Red Hat Enterprise Linux 5 guests boot on a 5.4.z Xen hypervisor. However, the added check caused a kernel panic due to missing multi-node CPU topology detection on AMD CPU family 0x15 systems. To preserve backwards compatibility, the check has not been removed but is triggered only on AMD Magny-Cours systems. AMD family 0x15 systems do not require the aforementioned check because they are not supported as 5.4 Xen hypervisor hosts. For Xen hypervisor 5.5, this issue has been fixed, which makes the check obsolete.

BZ#674774

The **bnx2i** drive could cause a system crash on IBM POWER7 systems. The driver's page tables were not set up properly on Big Endian machines, causing extended error handling (EEH) errors on PowerPC machines. With this update, the page tables are properly set up and a system crash no longer occurs in the aforementioned case.

BZ#675665

Booting Red Hat Enterprise Linux 5 with the *crashkernel=X* parameter enabled for the kdump kernel does not always succeed. This is because the kernel may not be able to find a suitable memory range for the crashkernel due to the fragmentation of the physical memory. Similarly, if a user specifies the starting address of the reserved memory, the specified memory range may be occupied by other parts of the kernel (in this case, the **initrd**, i.e. initial ramdisk). This update adds two debugging kernel parameters (*bootmem_debug* and *ignore_loglevel*) which allow to diagnose what causes the crashkernel to not be assigned enough memory.

BZ#680350

Prior to this update, the following message was displayed when booting a Red Hat Enterprise Linux 5 system on a virtual guest:

```
WARNING calibrate_APIC_clock: the APIC timer calibration may be
wrong.
```

This was due to the *MAX_DIFFERENCE* parameter value (in the APIC calibration loop) of 1000 cycles being too aggressive for virtual guests. APIC (Advanced Programmable Interrupt Controllers) and TSC (Time Stamp Counter) reads normally take longer than 1000 cycles when performed from inside a virtual guest, due to processors being scheduled away from and then back onto the guest. With this update, the *MAX_DIFFERENCE* parameter value has been increased to 10,000 for virtual guests.

BZ#681795

For a device that used a Target Portal Group (TPG) ID which occupied the full 2 bytes in the RTPG (Report Target Port Groups) response (with either byte exceeding the maximum value that may be stored in a signed char), the kernel's calculated TPG ID would never match the *group_id* that it should. As a result, this signed char overflow also caused the ALUA handler to incorrectly identify

the AAS (Asymmetric Access State) of the specified device as well as incorrectly interpret the supported AAS of the target. With this update, the aforementioned issue has been addressed and no longer occurs.

BZ#680043

Setting the capture levels on the Line-In capture channel when using an ARX USB I/O sound card for recording and playback did not work properly. The set values were not persistent. With this update, the capture values are now cached in the **usb-audio** driver leaving the set capture levels unchanged.

BZ#683443

A race could occur when an internal **multipath** structure (**pgpath**) was freed before it was used to signal the path group initialization was complete (via **pg_init_done**). This update includes a number of fixes that address this issue. **multipath** is now increasingly robust when multipathd restarts are combined with I/O operations to **multipath** devices and storage failures.

BZ#677173

Calling the **mptctl_fasync()** function to enable async notification caused the *fasync_struct* data structure, which was allocated, to never be freed. *fasync_struct* remained on the event list of the **mptctl** module even after a file was closed and released. After the file was closed, *fasync_struct* had an invalid file pointer which was dereferenced when the **mptctl** module called the **kill_fasync()** function to report any events. The use of the invalid file pointer could result in a deadlock on the system because the **send_sigio()** function tried to acquire the *rwlock* in the *f_owner* field of the previously closed file. With this update, a release callback function has been added for the file operations in the **mptctl** module. *fasync_struct* is now properly freed when a file is closed, no longer causing a deadlock.

BZ#677172

If an application opened a file with the *O_DIRECT* flag on an NFS client and performed write operations on it of size equal to *wsize* (size of the blocks of data passed between the client and the server), the NFS client sent two RPCs (Remote Procedure Calls) when only one RPC needed to be send. Write operations of size smaller than *wsize* worked as expected. With this update, write operations of size equal to *wsize* now work as expected and no longer cause the NFS client to send out unnecessary RPCs.

BZ#682673

Booting a Red Hat Enterprise Linux 5.4 or later kernel failed (the system became unresponsive) due to the zeroing out of extra bytes of memory of the reset vector. The reset vector is comprised of two 16-bit registers (high and low). Instead of zeroing out 32-bits, the kernel was zeroing out 64-bits. On some machines this overwritten memory was used during the boot process, resulting in a hang. With this update, the **long** data type has been changed to the unsigned 32-bit data type; thus, resolving the issue. The Red Hat Enterprise Linux 5.4 and later kernel now boot as expected on the machines affected by this bug.

BZ#688312

Prior to this update, a segmentation fault occurred when an application called VDSO's **gettimeofday** function due to erroneous exporting of the *wall_to_monotonic* construct. With this update, the *wall_to_monotonic* construct is correctly exported, and a crash no longer occurs.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.60.4. RHSA-2011:0303 - Moderate: kernel security and bug fix update

> **Important**
>
> This update has already been released as the security errata RHSA-2011:0303

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

* A flaw was found in the Linux kernel's garbage collector for **AF_UNIX** sockets. A local, unprivileged user could use this flaw to trigger a denial of service (out-of-memory condition). (CVE-2010-4249, Moderate)

* A flaw was found in the Linux kernel's networking subsystem. If the number of packets received exceeded the receiver's buffer limit, they were queued in a backlog, consuming memory, instead of being discarded. A remote attacker could abuse this flaw to cause a denial of service (out-of-memory condition). (CVE-2010-4251, Moderate)

* A missing initialization flaw was found in the **ethtool_get_regs()** function in the Linux kernel's **ethtool IOCTL** handler. A local user who has the **CAP_NET_ADMIN** capability could use this flaw to cause an information leak. (CVE-2010-4655, Low)

Red Hat would like to thank Vegard Nossum for reporting CVE-2010-4249, and Kees Cook for reporting CVE-2010-4655.

Bug fixes:

BZ#672253

Prior to this update, the **/proc/diskstats** file showed erroneous values. This occurred when the kernel merged two I/O operations for adjacent sectors which were located on different disk partitions. Two merge requests were submitted for the adjacent sectors, the first request for the second partition and the second request for the first partition, which was then merged to the first request. The first submission of the merge request incremented the **in_flight** value for the second partition. However, at the completion of the merge request, the **in_flight** value of a different partition (the first one) was decremented. This resulted in the erroneous values displayed in the **/proc/diskstats** file. With this update, the merging of two I/O operations which are located on different disk partitions has been fixed and works as expected.

BZ#669300

When selecting a new window, the **tcp_select_window()** function tried not to shrink the offered window by using the maximum of the remaining offered window size and the newly calculated window size. The newly calculated window size was always a multiple of the window scaling factor, however, the remaining window size was not since it depended on **rcv_wup/rcv_nxt**. As a result, a window was shrunk when it was scaled down. With this update, aligning the remaining window to the window scaling factor assures a window is no longer shrunk.

BZ#674273

Prior to this update, the **be2net** driver failed to work with bonding, causing "flapping" errors (the interface switches between states *up* and *down*) in the active interface. This was due to the fact that the *netdev->trans_start* pointer in the **be_xmit** function was not updated. With this update, the aforementioned pointer has been properly updated and "flapping" errors no longer occur.

BZ#[670824](#)

Outgoing packets were not fragmented after receiving the icmpv6 pkt-too-big message when using the **IPSecv6** tunnel mode. This was due to the lack of **IPv6** fragmentation support over an **IPsec** tunnel. With this update, **IPv6** fragmentation is fully supported and works as expected when using the **IPSecv6** tunnel mode.

BZ#[668976](#)

Using the **cciss** driver, when a TUR (Test Unit Ready) was executed, the *rq->bio* pointer in the **blk_rq_bytes** function was of value **null**, which resulted in a null pointer dereference, and, consequently, kernel panic occurred. With this update, the *rq->bio* pointer is used only when the **blk_fs_request(rq)** condition is true, thus, kernel panic no longer occurs.

BZ#[670807](#)

While bringing down an interface, the **e1000** driver failed to properly handle IRQs (Interrupt Requests), resulting in the reception of the following messages:

```
irq NN: nobody cared...
```

With this update, the driver's *down* flag is set later in the process of bringing down an interface, specifically, after all timers have exited, preventing the IRQ handler from being called and exiting early without handling the IRQ.

BZ#[671340](#)

A formerly introduced patch that provided extended **PCI** config space access on AMD systems caused the **lpfc** driver to fail when it tried to initialize hardware. On kernel-xen, Hypervisor trapped the aforementioned accesses and truncated them, causing the **lpfc** driver to fail to initialize hardware. Note that this issue was only observed when using the **lpfc** driver with the following parameters: *Vendor_ID=0x10df*, *Device_ID=0xf0e5*. With this update, the part of the patch related to kernel-xen that was causing the failures was removed and the **lpfc** driver now works as expected.

BZ#[670797](#)

Prior to this update, kernel panic occurred in the **kfree()** due to a race condition in the **acpi_bus_receive_event()** function. The **acpi_bus_receive_event()** function left the *acpi_bus_event_list* list attribute unlocked between checking it whether it was empty and calling the **kfree()** function on it. With this update, a check was added after the lock has been lifted in order to prevent the race and the calling of the **kfree()** function on an empty list.

BZ#[673984](#)

Prior to this update, a **rhev-agent** could not be started due to missing a /dev/virtio-ports/ directory. This was due to the fact that the **udev** utility does not parse the *KOBJ_CHANGE* event. With this update, the *KOBJ_ADD* event is invoked instead and so that symlinks in **/dev/virtio-ports** are created when a port name is obtained.

BZ#[678613](#)

VDSO (Virtual Dynamically-linked Shared Object) kernel variables must be exported in **vextern.h**, otherwise they end up as undefined pointers. When calling the VDSO **gettimeofday()** function in Red Hat Enterprise Linux 5, a missing declaration lead to a segmentation fault. With this update, the **sysctl_vsyscall** system call is properly exported and segmentation faults no longer occur.

BZ#**673983**

Using a **virtio** serial port from an application, filling it until the **write** command returns **-EAGAIN** and then executing a **select** command for the **write** command caused the **select** command to not return any values, when using the **virtio** serial port in a *non-blocking* mode. When used in a *blocking* mode, the **write** command waited until the host indicated it used up the buffers. This was due to the fact that the poll operation waited for the *port->waitqueue* pointer, however, nothing woke the *waitqueue* when there was room again in the queue. With this update, the queue is woken via host notifications so that buffers consumed by the host can be reclaimed, the queue freed, and the application **write** operations may proceed again.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.60.5. RHSA-2011:0017 - Important: Red Hat Enterprise Linux 5.6 kernel security and bug fix update

> **Important**
>
> This update has already been released as the security errata RHSA-2011:0017

Updated kernel packages that fix multiple security issues, address several hundred bugs, and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the sixth regular update.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

* A NULL pointer dereference flaw was found in the **igb** driver in the Linux kernel. If both the Single Root I/O Virtualization (SR-IOV) feature and promiscuous mode were enabled on an interface using **igb**, it could result in a denial of service when a tagged VLAN packet is received on that interface. (CVE-2010-4263, Important)

* A missing sanity check was found in **vbd_create()** in the Xen hypervisor implementation. As CD-ROM drives are not supported by the **blkback** back-end driver, attempting to use a virtual CD-ROM drive with **blkback** could trigger a denial of service (crash) on the host system running the Xen hypervisor. (CVE-2010-4238, Moderate)

* A flaw was found in the Linux kernel **execve()** system call implementation. A local, unprivileged user could cause large amounts of memory to be allocated but not visible to the OOM (Out of Memory) killer, triggering a denial of service. (CVE-2010-4243, Moderate)

* A flaw was found in **fixup_page_fault()** in the Xen hypervisor implementation. If a 64-bit para-virtualized guest accessed a certain area of memory, it could cause a denial of service on the host system

running the Xen hypervisor. (CVE-2010-4255, Moderate)

* A missing initialization flaw was found in the **bfa** driver used by Brocade Fibre Channel Host Bus Adapters. A local, unprivileged user could use this flaw to cause a denial of service by reading a file in the **/sys/class/fc_host/host#/statistics/** directory. (CVE-2010-4343, Moderate)

* Missing initialization flaws in the Linux kernel could lead to information leaks. (CVE-2010-3296, CVE-2010-3877, CVE-2010-4072, CVE-2010-4073, CVE-2010-4075, CVE-2010-4080, CVE-2010-4081, CVE-2010-4158, Low)

Red Hat would like to thank Kosuke Tatsukawa for reporting CVE-2010-4263; Vladymyr Denysov for reporting CVE-2010-4238; Brad Spengler for reporting CVE-2010-4243; Dan Rosenberg for reporting CVE-2010-3296, CVE-2010-4073, CVE-2010-4075, CVE-2010-4080, CVE-2010-4081, and CVE-2010-4158; Vasiliy Kulikov for reporting CVE-2010-3877; and Kees Cook for reporting CVE-2010-4072.

Bug Fixes:

BZ#659571

A flaw was found in the Linux kernel where, if used in conjunction with another flaw that can result in a kernel Oops, could possibly lead to privilege escalation. It does not affect Red Hat Enterprise Linux 5 as the **sysctl** *panic_on_oops* variable is turned on by default. However, as a preventive measure if the variable is turned off by an administrator, this update addresses the issue. Red Hat would like to thank Nelson Elhage for reporting this vulnerability.

BZ#647297

Performing a Direct IO write operation to a file on an NFS mount did not work. With this update, the minor error in the source code was fixed and the Direct IO operation works as expected.

BZ#638753

Previously, writing multiple files in parallel could result in uncontrollable fragmentation of the files. With this update, the methods of controlling fragmentation work as expected.

BZ#637764

In an active/backup bonding network interface with vlans on top of it, when a link failed over, it took a minute for the multicast domain to be rejoined. This was caused by the driver not sending any IGMP join packets. With this update, the driver sends IGMP join packets and the multicast domain is rejoined immediately.

BZ#636198

With this update, the upper limit of the *log_mtts_per_seg* variable was increased from five to seven, increasing the amount of memory that can be registered. Machines with larger memory are now able to register more memory.

BZ#630129

Recently applied patch introduced a bug, which caused the Xen guest networking not to work properly on 64-bit Itanium processors. However, this bug also revealed an issue, which may have led to a data corruption. With this update, both errors have been fixed, and Xen virtual guest networking now works as expected.

BZ#629773

Previously, migrating a hardware virtual machine (HVM) guest with both, UP and PV drivers, may have caused the guest to stop responding. With this update, HVM guest migration works as expected.

BZ#624068

Running the Virtual Desktop Server Manager (VDSM) and performing an **lvextend** operation during an intensive Virtual Guest power up caused this operation to fail. Since **lvextend** was blocked, all components became non-responsive: **vgs** and **lvs** commands froze the session, Virtual Guests became Paused or Not Responding. This was caused by a faulty use of a lock. With this update, performing an **lvextend** operation works as expected.

BZ#620508

Previously, running the **dd** command on an iSCSI device with the **qla3xxx** driver may have caused the system to crash. This error has been fixed, and running the **dd** command on such device no longer crashes the system.

BZ#620502

Previously, a large number of Red Hat Enterprise Linux NFS clients mounting a NFSv4 share from a server would show the following log messages repeatedly and could no longer access the share from the server:

```
NFS: v4 server returned a bad sequence-id error!
```

With this update, the error is no longer returned.

BZ#619466

Prior to this update, **ccw_device_set_options()** in **dasd_generic_probe()** unset the **CWDEV_ALLOW_FORCE** flag set in **dasd_eckd_probe()**. As a result, the unconditional reserve was not allowed on ECKD direct access storage devices (DASDs). With this update, the flags are set only in discipline specific probe functions.

BZ#619465

To build the CCW requests, the direct access storage device (DASD) reserve and release ioctl system calls use a preallocated memory pool of the respective device. Previously, this pool may have been emptied due to lack of memory, causing such system calls to fail. With this update, a memory is preallocated for each of these requests, and ioctl calls now work as expected.

BZ#619070

Previously, using 802.3ad link aggregation did not work properly when using the ixgbe driver. This was caused due to an inability to form 802.3ad-based bonds. With this update, the issue causing 802.3ad link aggregation to not work properly has been fixed.

BZ#608109

Previously, disks were spinning up for devices in an Active/Passive array on standby path side. This caused long boot up times which resulted in SD devices to be all created before multipath was ready. With this update, a disk is not spun up if returning *NOT_READY* on standby path.

BZ#602402

Upon startup, the **bnx2x** network driver experienced a panic dump when more than one network interface was configured to start up at boot time. With this update, statistics counter initialization for function IDs greater than **1** has been disabled, with the result that **bnx2x** no longer panic dumps when more than one interface has the *ONBOOT=yes* directive set.

BZ#601391

Previously, receiving eight or more different types of ICMP packets corrupted the kernel memory. This was caused by a flaw in the `net/ipv4/proc.c` file. With this update, kernel memory is no longer corrupted when receiving eight or more different types of ICMP packets.

BZ#590763

Input/output errors can occur due to temporary failures, such as multipath errors or losing network contact with an iSCSI server. In these cases, virtual memory attempts to retry the `readpage()` function on the memory page. However, the `do_generic_file_read()` function did not clear *PG_error*, which resulted in the system being unable to use the data in the page cache page, even if subsequent `readpage()` calls succeeded. With this update, the `do_generic_file_read()` function properly clears *PG_error* so that the page cache can be utilized in the case of input/output errors.

BZ#586416

The **e1000** and **e1000e** drivers for Intel PRO/1000 network devices were updated with an enhanced algorithm for adaptive interrupt modulation in the Red Hat Enterprise Linux 5.1 release. When *InterruptThrottleRate* was set to **1** (thus enabling the new adaptive mode), certain traffic patterns could have caused high CPU usage. This update provides a way to set *InterruptThrottleRate* to **4**, which switches the mode back to the simpler and non-adaptive algorithm. Doing so may decrease CPU usage by the **e1000** and **e1000e** drivers depending on traffic patterns.

Note: you can change the *InterruptThrottleRate* setting using the ethtool utility by running the following command:

```
ethtool -C ethX rx-usecs 4
```

BZ#582321

When an NFS server exported a file system with an explicit *fsid=[file_system_ID]*, an NFS client mounted that file system on one mount point and a subdirectory of that file system on a separate mount point, then if the server re-exported that file system after un-exporting and unmounting it, it was possible for the NFS client to unmount those mount points and receive the following error message:

```
"VFS: Busy inodes after unmount..."
```

Additionally, it was possible to crash the NFS client's kernel in this situation.

BZ#579711

The `timer_interrupt()` routine did not scale lost real ticks to logical ticks correctly. This could have caused time drift for 64-bit Red Hat Enterprise Linux 5: KVM (Kernel-based Virtual Machine) guests that were booted with the *divider=x* kernel parameter set to a value greater than 1. *warning: many lost ticks* messages may have been logged on the affected guest systems.

BZ#578531

An attempt to create a VLAN interface on a bond of two **bnx2** adapters in two switch configurations resulted in a soft lockup after a few seconds. This was caused by an incorrect use of a bonding pointer. With this update, soft lockups no longer occurs and creating a VLAN interface works as expected.

BZ#578261

When the Stream Control Transmission Protocol (SCTP) kernel code attempted to check a non-blocking flag, it could have dereferenced a **NULL** file pointer due to the fact that in-kernel sockets created with the **sock_create_kern()** function may not have a file structure and descriptor allocated to them. The kernel would crash as a result of the dereference. With this update, SCTP ensures that the file is valid before attempting to set a timeout, thus preventing a possible **NULL** dereference and consequent kernel crash.

BZ#576709

A host could crash during an SAN (storage area network) installation when using the Cisco **fnic** driver. During driver initialization, an error in the **fnic** driver caused it to flush the wrong queue. The flush code could then incorrectly access the memory and crash the host. With this update, the error in the **fnic** driver has been fixed and crashed no longer occur.

BZ#576246

When the **power_meter** module was unloaded or its initialization failed, a backtrace message was written to **/var/log/dmesg** that warned about a missing **release()** function. This error was harmless, and no longer occurs with this update.

BZ#575799

Attempting to boot the x86 kernel on AMD Magny-Cours systems could result in a kernel panic. This was caused by the inability to handle kernel **NULL** pointer dereference in a virtual address. This update fixes the aforementioned issue and kernel panic no longer occurs on AMD Magny-Cours systems.

BZ#571544

Hot-adding memory to a system with 4 GB of RAM caused problems with 32-bit DMA devices, which led to the system becoming unresponsive. With this update, the user is warned that more than 4 GB of RAM is being added to the system; however, memory exceeding 4 GB is not registered by the system.

BZ#570824

Red Hat Enterprise Linux 5.4 SMP guests running on the Red Hat Enterprise Virtualization Hypervisor may have experienced inconsistent time, such as the clock drifting backwards. This could have caused some applications to become unresponsive.

BZ#570645

When a system was configured using channel bonding in *mode=0* (round-robin balancing) with multicast, IGMP traffic was transmitted via a single interface. If that interface failed (due to a port, NIC or cable failure, for example), IGMP was not transmitted via another port in the group, thus resulting in packets for the previously-registered multicast group not being routed correctly.

BZ#570000

On certain platforms, the **mptsas** driver could return the following kernel warning messages:

```
kernel unaligned access to 0xe0000034f327f0ff, ip=0xa0000002040c4870
kernel unaligned access to 0xe0000034f327cbff, ip=0xa0000002040c4870
kernel unaligned access to 0xe00000300c9581ff, ip=0xa0000002040c4870
```

These messages did not indicate a serious error. With this update, the data alignment issue has been fixed and the aforementioned kernel warning messages are no longer returned.

BZ#567479

The Red Hat Enterprise Linux 5.5 kernel contained a fix for Bugzilla issue number 548657 which introduced a regression in file locking behavior that presented with the General Parallel File System (GPFS). This update removes the redundant locking code.

BZ#567428

Kernel panic occurred on a Red Hat Enterprise Linux 5.5 FC host with a QLogic 8G FC adapter (QLE2562) while running IO with target controller faults. With this update, kernel panic no longer occurs in the aforementioned case.

BZ#564249

A bug was found in the way the **megaraid_sas** driver (for SAS based RAID controllers) handled physical disks and management IOCTLs (Input/Output Control). All physical disks were exported to the disk layer, allowing an oops in **megasas_complete_cmd_dpc()** when completing the IOCTL command if a timeout occurred. One possible trigger for this bug was running mkfs. This update resolves this issue by updating the megaraid_sas driver to version 4.31.

BZ#563546

Some BIOS implementations initialized interrupt remapping hardware in a way that Xen did not expect. Consequently, a system could hang during boot, returning the following error message:

```
(XEN) [VT-D]intremap.c:73: remap_entry_to_ioapic_rte: index (74) is
larger than remap table entry size (55)!
```

This update introduces an array to record the index for each IOAPIC pin, thus, the *format* bit (which was causing the unexpected interrupt remapping) does not need to be checked. As a result, the system no longer hangs during boot.

BZ#560540

Previously, system board iomem resources, which were enumerated using the PNP Motherboard resource descriptions, were not recognized and taken into consideration when gathering resource information. This could have caused MMIO-based requests to receive allocations that were not valid. With this update, system board iomem resources are correctly recognized when gathering resource information.

BZ#554706

The **cnic** parts resets could cause a deadlock when the **bnx2** device was enslaved in a bonding device and that device had an associated VLAN.

BZ#504188

In a two node cluster, moving 100 files between two folders using the lock master was nearly instantaneous. However, not using the lock master resulted in a considerably worse performance on both, GFS1 (Global File System 1) and GFS2 (Global File System 2) file systems. With this update, not using the lock master does not lead to worsened performance on either of the aforementioned file systems.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.61. kexec-tools

1.61.1. RHBA-2011:0061: bug fix update

An updated kexec-tools package that fixes various bugs is now available

kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

This update fixes the following bugs:

* The setting of the path line on /etc/kdump.conf was not reflected. Now, this script is corrected. (BZ#379521)

* Certain systems became unresponsive because Kdump could not handle receipts of dhcp NAK frames. This update resolves this issue. (BZ#515208)

* Mkdumprd failed because the temporary file was not created when root was read-only. Now, the command "mkdumprd" works as expected. (BZ#530265)

* Mkdumprd failed when the using a network bridge. Now, kdump works as expected.(BZ#558733)

* Kdump failed to dump vmcore on Nehalem EX machine. Now, kdump dumps vmcore as expected.(BZ#559928)

* Systems could fail to perform a core dump due to DNS problems on AMD64 or Intel64 based hardware on the x86 PAE kernel. This update resolves this issue. (BZ#559928)

* A reference to deprecated .ssh/authorized_keys2, not .ssh/authorized_keys was hardcoded in kdump. Now, the key is configurable. (BZ#567708)

* In the kexec initrd environment, the request_module() failed. Now, request_module() loads the requested module. (BZ#576075)

* Kdump did not save vmcore on machines with 1TB memory. Now, kdump saves vmcore. (BZ#585979)

* Mkdumprd regenerated the ld.so.cache. This removed any symlinks to shared libs which reside on autofs managed filesystems. Now, mkdumprd restores the ld.so.cache to return the original cache even if network filesystems aren't available. (BZ#589768)

* Kexec could not dump vmcore through NFS on PowerPC systems due to issues with DNS lookups. Now, dumps to NFS locations succeed. (BZ#601273)

* The kexec kernel attempted to load inside xen-guest and could panic the central processing unit. Now, kexec-tools prevent the kexec kernel from loading in xen-guest. (BZ#608322)

* Kdump would not start on ppc servers with 256 Gigbytes of memory enabled. This update fixes this problem. (BZ#625828)

* The call to kdump_pre was missing from the kdump init script. Now, kdump_pre is part of the kdump init script. (BZ#640577)

* Kdump saved the vmcore to the Network File System too slow. This update improves the performance. (BZ#642552)

* The ld.so.cache could not be restored in read-only root. This issue is resolved. (BZ#642921)

* The ssh key did not propagate. Now, kdump uses '.ssh/authorized_keys' instead of '.ssh/authorized_keys2'. (BZ#643325)

* Depmod in mkdumprd failed on dom0 with memory bigger than 4 Gigabytes. This update resolves this issue. (BZ#646791)

* Systems became unresponsive when a forced crash occured due the hugepages=X boot option. Now, the system exits and produces a core. (BZ#647046)

* The system was not rebooted after dumping. Now, kdump reboots to normal system if no "default" action is available. (BZ#647627)

* Due to DNS problems nfs dumping failed on dom0. This update resolves this problem. (BZ#648416)

* Errors occured during ssh dumping. Now, ssh dumping works as expected. (BZ#648766)

* While loading shared libraries: libc.so.6, ssh dumping failed because ifup did not have all the variables for lo/inet. This update resolves this issue. (BZ#648771)

* Warning messages echoed when starting kdump service. Now, kdump service behaves as expected. (BZ#652500) * The system would reboot when dhcp failed to read IPs. Now, the system enters use-space and saves the vmcore. (BZ#654997)

* The vmcore was wrongly named vmcore.flat due problems with 'core_collector cp'. This update resolves this issue. (BZ#657198)

This update also adds the following enhancement:

* This update adds the opption "poweroff" to 'default' in /etc/kdump.conf. (BZ#543336)

All users are advised to upgrade to this updated kexec-tools package, which resolves these issues and adds this enhancement.

1.61.2. RHBA-2010:0776: bug fix update

An updated kexec-tools package that fixes a bug is now available.

The kexec-tools package provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot.

This updated kexec-tools package fixes the following bug:

* Previously, "/sbin/kexec" could run out of buffer on a PowerPC, when the PowerPC's memory was large, due to the buffer size limit for devtree. This caused kdump to fail to start. With this update, the buffer size is increased, thus, segmentation faults no longer occur and kdump is able to start as expected. (BZ#639303)

All users of kexec-tools are advised to upgrade to this updated package, which resolves this issue.

1.61.3. RHBA-2010:0438: bug fix update

An updated kexec-tools package that fixes a bug that prevented kexec from capturing a vmcore on 64-bit systems with more than 1TB of RAM is now available.

kexec-tools provides the /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

This update addresses the following issue:

* the physical address space supported by the Red Hat Enterprise Linux 5 kernel was out of sync with the physical address space the kexec binary assumed the kernel supported. As a consequence, kexec could not successfully capture a vmcore on AMD64 or Intel 64 systems with more than 1TB of RAM. This update brings the kernel and kexec utility view of the supported memory boundary into sync, obviating the problem. (BZ#590547)

All users are advised to upgrade to this updated kexec-tools package, which fixes this bug.

1.61.4. RHBA-2010:0375: bug fix update

An updated kexec-tools package that fixes various bugs is now available.

kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the user-space component of the kernel's kexec feature.

This updated kexec-tools package fixes the following bug:

* systems running a 32-bit kernel with the PAE (Physical Address Extension) feature enabled restrict the range of accessible memory to 64 GB, even when the system contains more physical RAM than 64 GB. On such a system, the kernel exports all of the detected memory via /proc/iomem, not just the amount of accessible memory. The kexec user-space tools use /proc/iomem to determine the amount of system memory in order to format its vmcore file so that all memory is accessible. However, on systems with more than 64 GB of RAM, the value read by kexec from /proc/iomem did not represent the amount of actual memory used by the system, which resulted in /proc/vmcore read errors when the kdump mechanism activated.

This update restricts the size of the vmcore file on 32-bit systems to 64 GB, thus preventing /proc/vmcore read errors due to an incorrectly-sized vmcore file. (BZ#582349)

All users of kexec-tools are advised to upgrade to this updated package, which resolves this issue.

1.62. krb5

1.62.1. RHBA-2011:0098: bug fix and enhancement update

Updated krb5 packages that fix several bugs and provide two new features are now available for Red Hat Enterprise Linux 5.

Kerberos is a network authentication system which allows clients and servers to authenticate each other with the help of a trusted third party, the Key Distribution Center (KDC).

This update addresses these issues:

* Servers which were not able to determine to which realm they belonged may have failed to accept authentication from clients. (BZ#450122)

* Log files were not rotated on KDCs. (BZ#462658)

* Replicated servers could not use master key stash files generated on a KDC of different endianness. (BZ#514741)

* Authentication to GSSAPI-enabled FTP servers could have failed if the server was known by multiple names and the client knew the server by a name other than the server's configured host name. (BZ#538075)

* Some applications that attempted to obtain initial credentials for a user could have crashed if the user's password had expired. (BZ#555875)

* The default kdc.conf configuration file did not list AES encryption types in the included example. (BZ#565941)

* When the credentials used to establish a GSSAPI context expired, communication using the context began to fail. (BZ#605367)

* The Kerberos-aware version of rshd unnecessarily failed if the name of the local user account being accessed was more than 16--but less than 32--characters long. ([BZ#611713](#))

* The password expiration time recorded in a user entry in a realm database accessed using LDAP was always ignored if the user entry had an associated password policy. ([BZ#627038](#))

This update also provides these features:

* A realm database can now be stored in an LDAP directory server. ([BZ#514362](#))

* The k5login_authoritative setting can be used to adjust the logic of the commonly-used krb5_kuserok() function to allow access to a user account when the principal name can be mapped to user's name, but the principal name is not explicitly listed in the user's .k5login file. ([BZ#539423](#))

Users should upgrade to these updated packages, which resolve these issues and add these enhancements.

1.62.2. RHBA-2010:0560: bug fix update

Kerberos is a trusted-third-party authentication system in which allows clients and servers to authenticate to each other using symmetric encryption and the trusted third party, the KDC.

The krb5-workstation includes a utility, ksu, which can be used to grant privileged shell access to unprivileged users using Kerberos authentication. It can also be used to grant access to shells running as unprivileged users.

These updated packages resolve the following issues:

* ksu used perform PAM account and session management for the target user after switching to the privileges of the target user. As a result, if that user did not have sufficient privileges, some modules which PAM could be configured to use would not function properly.This update performs PAM account and session management before assuming the privileges of the target user, fixing these bugs. ([BZ#602967](#) and [BZ#615261](#))

Users of krb5-workstation are advised to upgrade to these updated packages, which resolve these issues.

1.63. ksh

1.63.1. RHEA-2010:0694: enhancement update

An updated Ksh package that brings enhanced ulimit support is now available for Red Hat Enterprise Linux 5.

KornShell is a shell programming language which is also compatible with "sh", the original Bourne Shell. KSH-93 is the most recent version of the KornShell by David Korn of AT&TBell Laboratories.

This updated ksh package adds the following enhancement:

* previously the ksh ulimit builtin lacked support for RLIMIT_RTPRIO and RLIMIT_NICE. This did not allow full usage of ksh by script writers. With this update, the ksh package adds the ability to read and set both RLIMIT_RTPRIO and RLIMIT_NICE with the ulimit builtin. ([BZ#626790](#))

KornShell users, especially those who require RLIMIT_RTPRIO or RLIMIT_NICE, are advised to upgrade to this updated package, which adds this enhancement.

1.64. kudzu

1.64.1. RHBA-2011:0133: bug fix update

An updated kudzu package is available that fixes an incompatibility with the current version of pciutils.

pciutils has been upgraded to version 3.1.7 in Red Hat Enterprise Linux 5.6. This update changed the ABI of the static libpci library. Any application that links against the new libpci and the older libkudzu would crash.

Previously, the presence of an unsupported sound card could cause kudzu to list the available sound devices in unpredictable order. As a result, the /etc/modprobe.conf configuration file could contain a line with an incorrect "index" parameter for the sound module. With this update, unsupported sound cards no longer affect the order of sound devices, and the "index" parameter is now set correctly.(BZ#579852)

When the information associated with a network device changed, kudzu incorrectly recognized the device as a new one, even though its Media Access Control (MAC) address remained the same. When this happened, kudzu corrupted the Ethernet configuration. This update ensures that devices with the same MAC address are treated as identical regardless of their associated information, and a change to these information no longer affects the Ethernet configuration.(BZ#636263)

This update rebuilds kudzu to match the current libpci. (BZ#663395)

All users are advised to upgrade to these updated packages, which resolve these issues.

1.64.2. RHBA-2011:0010: bug fix update

An updated kudzu package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The kudzu package provides a hardware probing tool that is run at boot time to determine what hardware has been added or removed from the system.

This update fixes the following bugs:

* Previously, the presence of an unsupported sound card could cause kudzu to list the available sound devices in unpredictable order. As a result, the /etc/modprobe.conf configuration file could contain a line with an incorrect "index" parameter for the sound module. With this update, unsupported sound cards no longer affect the order of sound devices, and the "index" parameter is now set correctly. (BZ#656926)

* When the information associated with a network device changed, kudzu incorrectly recognized the device as a new one, even though its Media Access Control (MAC) address remained the same. When this happened, kudzu corrupted the Ethernet configuration. This update ensures that devices with the same MAC address are treated as identical regardless of their associated information, and a change to these information no longer affects the Ethernet configuration. (BZ#656927)

All users are advised to upgrade to this updated package, which resolves these issues.

1.65. kvm

1.65.1. RHSA-2011:0028: Low security and bug fix update

Updated kvm packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

A data structure field in kvm_vcpu_ioctl_x86_get_vcpu_events() in QEMU-KVM was not initialized properly before being copied to user-space. A privileged host user with access to "/dev/kvm" could use this flaw to leak kernel stack memory to user-space. (CVE-2010-4525)

Red Hat would like to thank Stephan Mueller of atsec information security for reporting this issue.

These updated packages also fix several bugs. Documentation for these bug fixes will be available shortly in the "kvm" section of the Red Hat Enterprise Linux 5.6 Technical Notes, linked to in the References.

All KVM users should upgrade to these updated packages, which resolve this issue as well as fixing the bugs noted in the Technical Notes. Note: The procedure in the Solution section must be performed before this update will take effect.

1.65.2. RHBA-2010:0714: bug fix update

Updated kvm packages that resolve several issues are now available.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems.

These updated kvm packages provide fixes for the following bugs:

* When a new virtual guest was created from a template, using Red Hat Enterprise Virtualization Manager on NFS storage, which was mounted remotely, it was handled by the qemu-img command. This operation took a considerable amount of time, about an hour for a 5-10GB image. With this update, the convert operation no longer results in poor performance and works as expected. (BZ#629574)

* Previously, the debug info package was missing from kvm-qemu-img-83-164.el5_5.12. With this update, it is included. (BZ#629635)

All KVM users should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.65.3. RHBA-2010:0536: bug fix update

Updated kvm packages that resolve several issues are now available.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems.

These updated kvm packages provide fixes for the following bugs:

* the virtio-blk back end for qemu-kvm performed unnecessary zeroing of memory on every I/O request, which reduced virtual guest performance. With this update, the virtio-blk back end avoids spurious zeroing of request structures on each I/O request, with the result that guest performance is increased. (BZ#604159)

* in the kvm kernel module, some internal KVM memory slots were incorrectly being handled by copy-on-write after a fork() function call, which caused issues when qemu-kvm ran child processes. This update fixes the handling of internal KVM memory slots on fork() to avoid those issues. (BZ#610341)

* when using the Network File System (NFS), lseek(SEEK_END) operations resulted in a GETATTR command being sent to th eserver, with the result that performance was reduced on disk images over NFS. With this update, the pread() and pwrite() functions are used instead of lseek(), read() and write(), with the result that performance is increased when using NFS. (BZ#610344)

* following writing metadata to a QCOW2 disk image, metadata was not flushed, which could have potentially caused the disk image to become corrupted in the event of system disruption (such as a power outage). With this update, metadata is flushed after being written, thus increasing QCOW2 image integrity, and decreasing the likelihood of image corruption. (BZ#612507)

* when using QCOW2 disk images, certain I/O operation or disk space depletion errors could potentially have caused image corruption or a virtual guest to stop running. This was due to the improper error-handling code for QCOW2 disk images. This has been fixed with this update so that the aforementioned types of errors are handled correctly, thus increasing QCOW2 disk integrity in such situations. (BZ#612508)

All KVM users should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.65.4. RHBA-2010:0479: bug fix update

Updated kvm packages that address several issues are now available.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems.

These updated packages fix the following bugs:

* it was found that qemu-img rebase could corrupt output images under certain conditions, due to clusters being taken from the backing file rather than the COW file. qemu-image rebase now always gives clusters in the COW file priority over those in the backing file, resolving this issue. (BZ#596378)

* for particular workloads, KVM would become stuck in an infinite loop while updating a guest page table entry (PTE). The qemu process used by qemu-kvm could not be killed, but continues to consume resources. This issue has been resolved. (BZ#596381)

* a rare theoretical race condition was found in the pvclock code for setting the wallclock. An unprotected global variable was used to hold version data, allowing guests to interfere with one another if they would both write wallclock data at the same time. The race condition has been removed, and this issue is now resolved. (BZ#596625)

* an error in a rarely used code path in the refcount table growth code of qcow2 caused inconsistencies in the metadata, which could lead to real data corruption later on. The corruption after refblock allocation was fixed, and this issue is now resolved. (BZ#602363)

* after saving a guest snapshot and restarting it, guests failed to boot and suffered a kernel panic. This issue only occurred when guests used virtio block drivers and ran multiple requests at the same time. The qcow2 block driver lacked a synchronous version, which has been added, and the issue is now resolved. (BZ#604188)

All KVM users should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.65.5. RHBA-2010:0419: bug fix update

Updated kvm packages that address several issues are now available.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems.

These updated packages fix the following bugs:

* when run on SMP systems, 64-bit Windows 2003 Server and 64-bit Windows 2008 Server only use the boot CPU for time-keeping, despite configuring the RTC interrupt for broadcast. KVM cannot tell, therefore, if the RTC interrupt can be used for time-keeping purposes or not. Consequently, 64-bit Windows 2003 Server and 64-bit Windows 2008 Server showed significant clock drift when run as guests on SMP systems. With this update, KVM now checks the RTC interrupt only on vcpu0, the 64-bit Windows 2003 Server and 64-bit Windows 2008 Server boot CPU when they run as SMP guests under KVM. (BZ#577266)

* some Linux-based para-virtualised guests (eg Fedora 11 and Fedora 12) which accessed para-virtualised (PV) MMU page tables crashed during startup when launched on AMD-based hosts which had Rapid Virtualization Indexing (RVI, formerly known as Nested Page Tables or NPT) disabled. (RVI is AMD's hardware-assisted virtualization technology for allowing guests to modify their own MMU page tables. It was called NPT during development.)

The crash occurred because a system call made by such guests (via the hypercall driver) attempted to write to a read-only page. With this update, the PV MMU reporting capability was disabled and Linux-based guests which make these calls no longer cause KVM to inject a page fault and crash. (BZ#578579)

* an error in irq_source_id size verification meant guest operating systems with eight assigned virtual functions (VF) hung on boot. This update corrects the error: verification is now done using bit numbers, not bytes and guests with eight VFs bound to the pci-stub driver boot (and can use the assigned virtual devices) as expected. (BZ#579863)

* in some circumstances, memory was reported as still SwapCached and Cached even after all virtual machines were quit and all the processes whose memory had been swapped out were no longer running. Although this memory is eventually reclaimed by the system, available free memory is a factor in deciding which host to use when launching a virtual machine: inaccurately reported memory could result in sub-optimal host allocation. With this update, kvm explicitly removes old pages from swapcache if they are the last mapped page, ensuring reported free memory is accurate. (BZ#581764)

* as part of the qcow2 image format, each cluster has an associate reference count (refcount) that takes two values: zero (free) and not-zero (in use). These refcounts are stored in a refcount block which, itself, has a refcount. Previously, the refcount of this refcount block was only updated after cluster refcount allocation had finished. If an I/O error occurred during refcount allocation, however, the not updated refcount block refcount could cause the qcow2 image to corrupt. With this update, the refcount block's refcount is automatically changed as cluster refcount allocation occurs, ensuring it is always accurate and protecting the qcow2 image in the event of I/O errors. (BZ#581766)

* an abort() call was incorrectly added to an I/O error condition. As a consequence, in some circumstances, if a guest was writing a file and an I/O error occurred, the entire guest would crash. This update removes the call and corrects this regression. If the equivalent I/O error now occurs, the guest stops trying to write the file (and a "free_clusters failed" error is logged) but otherwise continues unaffected. (BZ#586246)

All KVM users should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.66. less

1.66.1. RHBA-2010:0805: bug fix update

An updated less package that fixes a bug in documentation is now available for Red Hat Enterprise Linux 5.

The less utility is a text file browser that resembles the more browser, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because the less utility does not need to read the entire input file before it starts, it starts up more quickly than text editors (vi, for example).

This updated package fixes the following bug:

* Previously, the less --help contained incorrect descriptions of some options. With this update, all options are described correctly. (BZ#578289)

All users of the less text file browser are advised to upgrade to this updated package, which fixes this bug.

1.67. libbonobo

1.67.1. RHBA-2010:0789: bug fix update

A new libbonobo package that fixes various issues is now available for Red Hat Enterprise Linux 5.

Bonobo is a component system based on CORBA, used by the GNOME desktop.

This update fixes the following bug:

Previously, the activation server didn't exit with the session. This update provides a new environment variable, BONOBO_ACTIVATION_RUN_SERVER_PER_SESSION, which allows the bonobo-activation-server to start per-session and exit with each session.

All GNOME users are advised to upgrade to this updated package which resolves this issue.

1.68. libhugetlbfs

1.68.1. RHBA-2010:0820: bug fix update

An updated libhugetlbfs package that fixes a bug is now available.

The libhugetlbfs library interacts with the Linux Huge TLB file system to make large pages available to applications in a transparent manner.

* Due to several arithmetic errors in the huge page size computation, the huge_page_setup_helper.py script may have failed with the following error message:

IndexError: list index out of range

This has been fixed, and the script no longer terminates unexpectedly. (BZ#616799)

Users of libhugetlbfs are advised to upgrade to this updated package, which resolves this issue.

1.69. libselinux

1.69.1. RHBA-2011:0029: bug fix update

Updated libselinux packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

libselinux is the core library of an SELinux system. It is used by all applications that are SELinux-aware.

This update fixes the following bugs:

* Under certain circumstances, when SELinux was enabled, an attempt to start a customized version of the httpd service (that is, other than the one that is shipped with Red Hat Enterprise Linux 5) could fail with a segmentation fault. With this update, a patch has been applied to target this issue, and SELinux no longer prevents httpd from starting. (BZ#537040)

* Due to missing functions in the selinux.h header file, sVirt, an integrated solution for securing Linux-based virtualization using SELinux, was not fully supported. This has been fixed, selinux.h have been updated to contain both selinux_virtual_domain_context_path() and selinux_virtual_image_context_path(), and sVirt support now works as expected. (BZ#582612)

Users are advised to upgrade to these updated packages, which resolve these issues.

1.70. libvirt

1.70.1. RHEA-2011:0060: bug fix and enhancement update

Updated libvirt packages that upgrade the libvirt library to upstream version 0.8.2, add sVirt support, and fix a number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remotely managing virtualized systems.

These updated packages upgrade the libvirt library for Red Hat Enterprise Linux 5 to upstream version 0.8.2, which contains a large number of enhancements and bug fixes over the previous version. Importantly, with this libvirt update, Red Hat Enterprise Linux 5.6 now provides support for sVirt, which brings mandatory access control to the KVM hypervisor. (BZ#544303)

1.70.2. RHSA-2010:0615: Low security and bug fix update

Updated libvirt packages that fix two security issues and three bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remotely managing virtualized systems.

It was found that libvirt did not set the user-defined backing store format when creating a new image, possibly resulting in applications having to probe the backing store to discover the format. A privileged guest user could use this flaw to read arbitrary files on the host. (CVE-2010-2239)

It was found that libvirt created insecure iptables rules on the host when a guest system was configured for IP masquerading, allowing the guest to use privileged ports on the host when accessing network resources. A privileged guest user could use this flaw to access network resources that would otherwise not be accessible to the guest. (CVE-2010-2242)

Red Hat would like to thank Jeremy Nickurak for reporting the CVE-2010-2242 issue.

This update also fixes the following bugs:

* a Linux software bridge assumes the MAC address of the enslaved interface with the numerically lowest MAC address. When the bridge changes its MAC address, for a period of time it does not relay packets across network segments, resulting in a temporary network "blackout". The bridge should thus avoid changing its MAC address in order not to disrupt network communications.

The Linux kernel assigns network TAP devices a random MAC address. Occasionally, this random MAC address is lower than that of the physical interface which is enslaved (for example, eth0 or eth1), which causes the bridge to change its MAC address, thereby disrupting network communications for a period of time.

With this update, libvirt now sets an explicit MAC address for all TAP devices created using the configured MAC address from the XML, but with the high bit set to 0xFE. The result is that TAP device MAC addresses are now numerically greater than those for physical interfaces, and bridges should no longer attempt to switch their MAC address to that of the TAP device, thus avoiding potential spurious network disruptions. (BZ#617243)

* a memory leak in the libvirt driver for the Xen hypervisor has been fixed with this update. (BZ#619711)

* the xm and virsh management user interfaces for virtual guests can be called on the command line to list the number of active guests. However, under certain circumstances, running the "virsh list" command resulted in virsh not listing all of the virtual guests that were active (that is, running) at the time. This update incorporates a fix that matches the logic used for determining active guests with that of "xm list", such that both commands should now list the same number of active virtual guests under all circumstances. (BZ#618200)

All users of libvirt are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the system must be rebooted for the update to take effect.

1.70.3. RHBA-2010:0524: bug fix update

Updated libvirt packages that resolve an issue are now available.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remotely managing virtualized systems.

These updated libvirt packages fix the following bug:

* previously, libvirt set CPU affinity only for the Virtual CPU (vCPU) threads, leaving the main QEMU thread and any I/O threads unpinned and able to use any CPU on the host. This update corrects this: libvirt now sets CPU affinity for the whole QEMU process and all its threads before memory allocation occurs. (BZ#599570)

All libvirt users are advised to upgrade to these updated packages, which resolve this issue.

1.71. libxml2

1.71.1. RHBA-2010:0764: bug fix update

Updated libxml2 packages that fix an erratic behavior of the XPath implementation.

libxml2 is a library for parsing and manipulating XML files. It includes support for reading, modifying, and writing XML and HTML files. Libxml2 implements the XPath specification which is a language for addressing parts of an XML document.

This update fixes the following bug:

* Due to an uninitialized field in one of the private libxml2 XPath data structures, the XPath evaluation may have return incorrect results. This error has been fixed, the field is now initialized properly, and XPath evaluation returns expected results. (BZ#640191)

Users of libxml2 are advised to upgrade to these updated packages, which resolve this issue.

1.72. linuxwacom

1.72.1. RHEA-2011:0123: enhancement update

An enhanced linuxwacom package is now available for Red Hat Enterprise Linux 5.

The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.Org XInput drivers.

This updated linuxwacom package adds the following enhancements:

* Red Hat Enterprise Linux 5.6 now supports the Wacom Cintiq 21UX 2 devices. (BZ#639091)

* Red Hat Enterprise Linux 5.6 now supports the Wacom Intuos4 devices. (BZ#573748)

All linuxwacom users are advised to upgrade to this updated package, which adds these enhancements.

1.73. logrotate

1.73.1. RHBA-2010:0827: bug fix update

An updated logrotate package that fixes a bug is now available.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

* Previously, using the "compressoptions" directive in the configuration file, /etc/logrotate.conf, caused logrotate to crash. With this update, the relevant part of the source code has been updated to use the popt library, and logrotate now works as expected. (BZ#646762)

All users of logrotate are advised to upgrade to this updated package, which resolves this issue.

1.73.2. RHBA-2010:0772: bug fix update

An updated logrotate package that fixes a bug is now available.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

* Previously, when there was an error in one of the logrotate's configuration files, logrotate stopped the whole rotation process. With this update, logrotate only skips broken configuration files, and rotates logs defined in other configuration files as usual. (BZ#642255)

All users of logrotate are advised to upgrade to this updated package, which resolves this issue.

1.74. lvm2

1.74.1. RHBA-2011:0052: bug fix and enhancement update

Updated lvm2 packages that fix bugs and add enhancements are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

This update applies the following bug fixes:

* Fixes incorrect removal of symlinks after LV deactivation fails.

* Fixes vgremove to allow removal of VG with missing PVs.

* Requires --restorefile when using pvcreate --uuid.

* Never scans internal LVM devices directly to avoid deadlock.

* Fixes allocation of wrong number of mirror logs with 'remove' fault policy.

* Checks if LV with specified name already exists when splitting a mirror.

* Fixes possible hang when all mirror images of a mirrored log fail.

* Ensures region_size of mirrored log does not exceed its full size.

* Does not return error code when using -o help with LVM reports.

* Requires partial option in lvchange --refresh for partial LVs.

* Do not merge old device cache after we run full scan to properly update cache

* Fixes truncated total size displayed by pvscan.

* Disallows the addition of mirror images while a conversion is happening.

* Disallows primary mirror image removal when mirror is not in-sync.

* Fixes return code of pvmove --abort PV.

* Fixes pvmove --abort to remove even for empty pvmove LV.

* Fixes pvmove allocation to take existing parallel stripes into account.

* Fixes --alloc contiguous policy only to allocate one set of parallel areas.

* Avoids scanning all pvs in the system if operating on a device with metadata areas.

* Suppresses repeated errors about the same missing PV uuids.

* Bypasses full device scans when using internally-cached VG metadata.

* Runs only do one full device scan during each read of text format metadata.

* Stops dmeventd trying to access already-removed snapshots.

* Fixes allocation code not to stop at the first area of a PV that fits.

* Keeps log type consistent when changing mirror image count.

* Corrects activated or deactivated text in vgchange summary message.

* Fixes lvm shell crash when input is entirely whitespace.

* Fixes fsadm command to properly handle user's break action and --dry-run option.

* Fails with correct error message when creating a too-small snapshot.

As well, this update adds the following enhancements:

* Adds "devices/default_data_alignment" to lvm.conf.

* Allows aborting if MD/swap signature is found in pvcreate.

* Detects LUKS signature in pvcreate.

* Allows to set limit for repeated access to broken devices by disable_after_error_count option in to lvm.conf.

* Adds --norestorefile option to pvcreate.

* Use built-in rule for device aliases which prefers more user friendly device names.

* Handles failure of all mirrored log devices and all but one mirror leg.

* Makes vgck warn about missing PVs.

* Adds metadata/vgmetadatacopies to lvm.conf and --[vg]metadatacopies option to allow metadata balancing (select number of mdas to use in a VG).

* Adds --metadataignore to pvcreate,pvchange and vgextend to set metadata ignore bit.

* Adds vg_mda_copies, pv_mda_used_count and vg_mda_used_count to reports.

* Adds man pages for lvmconf and non-existent lvmsadc and lvmsar tools.

* Adds --force, --nofsck and --resizefs to lvresize/extend/reduce man pages.

* Adds --sysinit compound option to vgchange and lvchange.

* Allows incomplete mirror restore in lvconvert --repair upon insufficient space.

* Allows VGs with active LVs to be renamed.

* Permits mirror image LVs to be striped in lvcreate, lvresize and lvconvert.

* Adds ability to create mirrored logs for mirror LVs.

* Adds --monitor and --ignoremonitoring to lvcreate.

* Adds default alternative to mlockall using mlock to reduce pinned memory size.

* Adds --splitmirrors to lvconvert to split off part of a mirror.

* Adds --poll flag to vgchange and lvchange to control background daemon launch.

* Removes PVs flagged as missing in vgreduce --removemissing --force.

* Adds vgextend --restoremissing to enable reappeared PVs.

Users of lvm2 are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.74.2. RHBA-2010:0510: bug fix update

Updated lvm2 packages that fix various bugs are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

These updated lvm2 packages include fixes for the following bugs:

* the command lvchange --refresh used to cause unexpected partial mapping if some PVs were missing. lvchange --refresh requires a partial flag for missing PVs. This problem is resolved and lvchange --refresh recognizes now --partial. (BZ#601078)

* the lvm command used to fail when the log file specified in lvm.conf was not available. This problem is now resolved and the commands simply log the error and continue as if there was no log file specified at all. (BZ#601079)

All users are advised to upgrade to these updated packages, which resolve these issues.

1.74.3. RHBA-2010:0433: bug fix update

Updated lvm2 packages that fix various bugs are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

These updated lvm2 package include fixes for the following bugs:

* fixes a crash in pvs -a command if some device in Volume Group is missing. (BZ#583995)

* avoids repeated full device scans if using internally-cached VG metadata (which happens on system with missing device in Volume Group). (BZ#584705)

* disallows removal of primary mirror image (using lvconvert) if the mirror is not fully synchronised yet. (BZ#584801)

* fixes unexpected symbolic link removal if device is still active after deactivation failure. (BZ#580831)

All users are advised to upgrade to this updated package, which resolves these issues.

1.74.4. RHBA-2010:0368: bug fix update

An updated lvm2 package that fixes various bugs is now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

This updated lvm2 package includes fixes for the following bugs:

* updating the Red Hat Enterprise Linux 5.5 kernel package while clvmd (the cluster LVM daemon) was running caused LVM commands to subsequently fail, with the result that it was not possible to boot into the new kernel, though booting into an older kernel worked as expected. This issue was caused by an incompatible flag in the cluster lock request. This update properly masks this flag so that LVM is again able to communicate with the running clvmd daemon. With this update, LVM works as expected after installing the Red Hat Enterprise Linux 5.5 kernel.

Important: a workaround for this issue was described in the Red Hat Knowledgebase article linked to in the References. This workaround is not needed after installing this lvm2 update. (BZ#582218)

* running certain LVM commands, such as "vgremove", simultaneously on two different volume groups occasionally caused one of the commands to fail. This was caused by a race condition that resulted in the following error message:

flock failed: Resource temporarily unavailable Can't get lock for orphan PVs This update includes a fix for the race condition that ensures that commands can be run in parallel without failure. (BZ#582232)

All users are advised to upgrade to this updated package, which resolves these issues.

1.75. lvm2-cluster

1.75.1. RHBA-2011:0053: bug fix and enhancement update

Updated lvm2-cluster packages that fix several bugs and add enhancements are now available.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This update ensures that the bugs fixed by the lvm2 advisory are also fixed in a clustered environment.

This update applies the following bug fixes:

* Changes the clvmd initscript to provide a standard exit status code (4) when executed by a non-root user.

* Changes the clvmd initscript restart command to start the daemon if it was not running.

* Changes the clvmd initscript never to deactivate non-clustered logical volumes.

* Changes the clvmd initscript now to report only clustered logical volumes during activation.

* Avoids a crash in clvmd -R if no response is received from the daemon.

* Disallows vgchange --clustered if there are active mirrors or snapshots.

* Fixes a crash during automatic target module loading.

* Avoids a deadlock discovered during clvmd stress testing. ([BZ#561226](#))

* Fixes 'lvconvert --splitmirrors' in cluster operation.

* Fixes a data corruption bug in cluster mirrors.

* Disallows 'mirrored' log type for cluster mirrors.

* Disallows lvchange --ignoremonitoring for clustered volumes.

* Avoids file conflicts when installing both lvm2 and lvm2-cluster debuginfo packages. ([BZ#586980](#))

This update adds the following enhancements:

* Adds -S command to clvmd to restart the daemon preserving exclusive locks.

* Ensures the cluster log daemon is running before allowing the creation of a clustered mirror.

* Provides a manual page for lvmconf(8). ([BZ#498436](#))

Users of lvm2-cluster are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.75.2. RHBA-2010:0432: bug fix update

Updated lvm2-cluster packages that fix various bugs are now available.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This update ensures that the bugs fixed by the lvm2 advisory are also fixed in a clustered environment, namely these bugs:

* avoids repeated full device scans if using internally-cached VG metadata (which happens on systems with a missing device in a Volume Group). ([BZ#584705](#))

* fixes unexpected symbolic link removal if device is still active after deactivation failure. ([BZ#580831](#))

This update also applies the following clustered lvm only bug fixes:

* fixes thread race which can happen if clvmd is under high load and leads to clvmd hangs. ([BZ#584706](#))

* fixes clvmd init script info to properly shutdown Logical Volumes if GFS is used on them. ([BZ#591524](#))

* fixes vgscan to refresh device cache if cluster locking is used and device filter in lvm.conf is changed. ([BZ#592220](#))

Users of lvm2-cluster are advised to upgrade to these updated packages, which resolve these issues.

1.76. m2crypto

1.76.1. RHBA-2011:0019: bug fix and enhancement update

An updated m2crypto package that fixes some bugs and provides an enhancement is now available.

m2crypto is a Python wrapper for OpenSSL. It makes it possible to call OpenSSL functions from Python scripts.

This updated m2crypto package fixes the following bugs:

* Example scripts used "/usr/bin/env python" as the script interpreter path. With this update, the example scripts use "/usr/bin/python" as the script interpreter path to make sure the scripts are executed by the system Python interpreter, not a locally built interpreter. (BZ#521887)

* When a M2Crypto.SSL.Connection object was created without setting up a connection, an SSL object was allocated and never freed. Over time, this could result in a significant memory leak. This update ensures the memory is correctly deallocated. (BZ#660292)

In addition, this updated package provides the following enhancement:

* Previously, m2crypto did not allow users to override the certificate hostname checks performed by default. With this update, users can disable the hostname checks. (BZ#524855)

Users are advised to upgrade to this updated m2crypto package, which resolves these issues and adds this enhancement.

1.76.2. RHBA-2010:0993: bug fix update

An updated m2crypto package that fixes a memory leak is now available for Red Hat Enterprise Linux 5.

m2crypto is a Python wrapper for OpenSSL. It makes it possible to call OpenSSL functions from Python scripts.

This updated m2crypto package fixes the following bug:

* When an "M2Crypto.SSL.Connection" object was created without setting up a connection, an SSL object was allocated and never freed. Over time, this could result in a significant memory leak. This update ensures the memory is correctly deallocated. (BZ#661869)

Users of m2crypto are advised to upgrade to this updated package, which resolves this issue.

1.77. mailman

1.77.1. RHBA-2010:0726: bug fix update

An updated mailman package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

Mailman is a program used to help manage email discussion lists.

This updated mailman package includes fixes for the following bugs:

* Previously, the /etc/smrsh/mailman symbolic link used an absolute path, which may have not work properly in a chroot environment. This error has been fixed, and the symbolic link now uses a relative path. (BZ#290661)

* When an email could not be parsed, it may have been lost and the remaining messages may have been stuck in the queue. With this update, such problematic messages are preserved, and the message queue is processed as expected. (BZ#453377)

* If the original Cc: field contained an address that spanned across multiple lines, mailman was not able to parse it correctly, causing the resulting address to be invalid. This error has been fixed, and email addresses are now parsed as expected. (BZ#461707)

* When changing an email address using the web interface, confirming the change may have caused the subscribed user to be presented with a traceback error. This has been corrected, and an informative message is now displayed instead. (BZ#515157)

* In accordance with current guidelines, all Python executables have been updated to use "#!/usr/bin/python" instead of "#!/usr/bin/env python". (BZ#521888)

Users are advised to upgrade to this updated package, which resolves these issues.

1.78. man-pages

1.78.1. RHBA-2010:0571: bug fix update

An updated man-pages package that corrects documentation errors and omissions is now available for Red Hat Enterprise Linux 5.

The man-pages package provides manual pages from the Linux Documentation Project.

This updated manual pages package fixes the following bugs:

* previously, the manual page for 'rt_sigprocmask' contained inconsistencies with the manual page for rt_sigaction in the synopsis (oset instead of oact). Now the manual page is consistent. (BZ#530570)

* previously, numerous manual pages mentioned the wrong URLs for kernel documentation. Now, the manual pages correctly point to /usr/share/doc/kernel-doc-2.6.18. (BZ#532634)

* previously, several available options were not described on the manual page for iconv. The updated package now describes all options. (BZ#544142)

* previously, the manual page for /etc/nscd.conf did not mention the configuration options max-db-size and auto-propagate. The updated package adds documentation for these options to the manual page. (BZ#566303)

* previously, the getrusage manual page did not describe the option RUSAGE_THREAD. The updated package resolves this issue and mentions this option. (BZ#572194)

* the previous package contained manual pages for several Source Code Control System (SCCS) commands. These manual pages were removed because the SCCS commands are not included in Red Hat Enterprise Linux. (BZ#582119)

All users of manual pages are advised to upgrade to this updated package, which resolves these issues.

1.79. man-pages-ja

1.79.1. RHBA-2010:0592: bug fix update

An updated man-pages-ja package that fixes documentation errors is now available for Red Hat Enterprise Linux 5.

The man-pages-ja package contains Japanese translations of the Linux Documentation Project man pages.

This updated package fixes the following bugs:

* the old Japanese manual page of the 'tail' command contained the obsolete option '+N'.The updated package removes this issue. (BZ#551471)

* the old Japanese manual page of the 'less' command did not mention the '&pattern' command from the English version. The updated package adds the description of the '&pattern' command. (BZ#583520)

* the Japanese manual page of the 'passwd' command was translated against the wrong English version of the 'passwd' command. As a result,the page mentioned the wrong options. The updated package resolves this issue and synchronizes the text with the correct English version of the passwd man page. (BZ#601127)

All man-pages-ja users are advised to upgrade to this updated package, which resolves these issues.

1.80. metacity

1.80.1. RHBA-2011:0107: bug fix update

An updated metacity package that fixes various bugs is now available.

Metacity is the default window manager for the GNOME desktop.

Important: the RHBA-2010:0245 - metacity bug fix and enhancement update introduced two new GConf preferences, no_focus_windows and new_windows_always_on_top. This update enhances the capabilities provided by these preferences.

This updated metacity package includes fixes for the following bugs:

* In order to prevent the system from focusing new windows of applications automatically, you needed to define the applications in the no_focus_windows option. With this update, if the no_focus_windows option is activated, only new windows of the currently-focused application are focused and new windows of any other application are ignored. (BZ#591944)

* Previously, if the new_windows_always_on_top setting was activated, any new window was focused. This could have cause unwanted changes of window focus. With this update, if the new_windows_always_on_top option is activated, new windows of other than the currently-focused application are brought to the foreground; however, these windows are not focused. (BZ#582769)

All metacity users are advised to upgrade to this updated package, which resolves these issues.

1.81. microcode_ctl

1.81.1. RHEA-2011:0126: enhancement update

An enhanced microcode_ctl package is now available.

microcode_ctl provides utility code and the microcode data itself -- supplied by Intel -- to assist the kernel in updating the CPU microcode at system boot time. This microcode supports all current Intel x86- and Intel 64-based CPU models and takes advantage of the mechanism built-in to Linux that allows microcode to be updated after system boot. When loaded, the updated microcode corrects the behavior of various Intel

processors, as described in processor specification updates issued by Intel for those processors.

This updated microcode_ctl package adds the following enhancement:

* The Intel CPU microcode file is updated to version 20101123. As of November 23, 2010, this is the most recent version of the microcode available from Intel. (BZ#627798)

Note: To apply the changes, reboot the system after update.

Users of microcode_ctl are advised to upgrade to this updated package, which adds this enhancement.

1.82. mkinitrd

1.82.1. RHBA-2011:0110: bug fix update

Updated mkinitrd packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

This update fixes the following bugs:

* Previously, network devices could be set up more than once with iSCSI when the system had two partitions on a single iscsi device. With this update, the network is only configured once. This issue could be resolved thanks to the patch contributed made by Thomas Chenault. (BZ#499781)

* Previously, the symlink /sbin/dmraid.static was missing when the kernel-debug and kernel packages were installed. With this update, the installation of these packages behaves as expected. (BZ#513961)

* Previously, virtual machines using iscsi could not boot correctly after installation. With this update booting works correctly. (BZ#568325)

* Previously, the command "mkinitrd" failed due to a regression. As a result, no initial RAM disk could be created. With this update, command "mkinitrd" creates initial RAM disks without errors. (BZ#578236)

* Previously, mkinitrd did not support the option multipath-tools bindings_file. This update does support this option (BZ#593050)

* Previously, the installation of Red Hat Enterprise Linux 5.6 Snap5 failed when root was installed on iSCSI multipath'd LUN. This update installs the operating system successfully with root (/) FS on an iSCSI multipath'd LUN. (BZ#664389)

All mkinitrd users are advised to upgrade to these updated packages, which resolve these issues.

1.82.2. RHBA-2010:0541: bug fix update

Updated mkinitrd packages that resolve an issue are now available.

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

These updated mkinitrd packages resolve the following issue:

* previously, when using the bindings_file configuration directive in /etc/multipath.conf, mkinitrd failed to copy the bindings file from the location specified in /etc/multipath.conf to the corresponding relative path inside the initramfs image. This issue is now resolved and mkinitrd uses the bindings_file configuration directive without problems.

All mkinitrd users are advised to upgrade to these updated packages, which resolve this issue. (BZ#596134)

1.82.3. RHBA-2010:0390: bug fix update

Updated mkinitrd packages that fix a regression introduced by RHBA-2010:0295 are now available.

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

These updated mkinitrd packages fix the following bug:

* a previous mkinitrd update, released as RHBA-2010:0295, included a fix for BZ#540641. This bug saw mkinitrd copy the symbolic link of a bootpath driver instead of the actual bootpath driver and, as a fix, mkinitrd was set to check the full path of symbolically linked drivers.

The fix included for BZ#540641 also introduced a regression, however. This regression could cause mkinitrd to fall into an infinite loop if checking the full path involved parsing a looped symbolic link. This update corrects the error in the readlink() function call that caused the regression. Looped symbolic links in driver paths no longer prevent mkinitrd from creating RAM disks as expected. (BZ#583901)

All mkinitrd users should upgrade to these updated packages, which resolve this issue.

1.83. mod_authz_ldap

1.83.1. RHBA-2010:0880: bug fix update

An updated mod_authz_ldap package that fixes a bug is now available for Red Hat Enterprise Linux 5.

mod_authz_ldap is a module for the Apache HTTP Server. This module provides support for authenticating users against an LDAP database.

This update fixes the following bug:

* Previously, memory leaks occurred when running mod_authz_ldap. With this update, the issue is resolved.

All users of mod_authz_ldap are advised to upgrade to this updated package, which resolves this issue.

1.84. mod_nss

1.84.1. RHBA-2011:0049: bug fix update

An updated mod_nss package that fixes various bugs is now available.

This updated mod_nss package includes fixes for the following bugs:

* Some hardware readers did not work because mod_nss initialized NSS and only then forked its child listeners. This process was not compliant with the PKCS#11 specification of public-key cryptography standards (PKCS). With this update, mod_nss initializes NSS after Apache HTTP Server forks as it is defined in the PKCS specification. (BZ#498542)

* The httpd daemon failed to start if Apache HTTP Server loaded the mod_nss module without the mod_nss configuration. With this update, the httpd daemon starts as expected. (BZ#513367)

* During mod_nss installation the following message appeared:

mod_nss certificate database generated.

With this update, the message no longer appears. (BZ#529164)

* The httpd daemon terminated unexpectedly if the stored token password did not match the database password. With this update, the problem no longer occurs. (BZ#588858)

* Large POST request caused the mod_nss module to get into an infinite loop. This update fixes the problem and the loop no longer occurs. (BZ#634685)

* Server experienced performance issues when starting up. The server searched for the certificates for every configured virtual server. With this update, a server pulls the list of certificates and caches the list. (BZ#635324)

All users of mod_nss are advised to upgrade to this updated package, which resolves these issues.

1.85. module-init-tools

1.85.1. RHBA-2010:0759: bug fix update

An updated module-init-tools package that provides a bug fix is now available.

The module-init-tools package provides various utilities used to manage the loading and administration of Linux Kernel Modules.

This updated package addresses the following bug:

* When a Driver Update package (that is, one of the various "kmod" packages) is updated, a symbolic link is recreated in the weak-updates directory to correlate with the compatible kernel. However, previous version of the module-init-tools package introduced a bug, which caused it not to create these links again once they were removed during the update process. This update ensures that such weak links are created properly, and upgrading Driver Update packages now works as expected. (BZ#638855)

Users are advised to upgrade to this updated package, which resolves this issue.

1.86. net-snmp

1.86.1. RHBA-2010:0422: bug fix update

Updated net-snmp packages that resolve an issue are now available.

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-snmp packages include various SNMP tools:an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl MIB browser.

These updated net-snmp packages fix the following bug:

* snmpd, the SNMP daemon, could have leaked file descriptors periodically when retrieving data for RMON-MIB. This leak could have exhausted file descriptors for the snmpd process and rendered the daemon unable to respond to SNMP requests. With this update, all unnecessary file descriptors are appropriately closed so that snmpd thus no longer leaks file descriptors. (BZ#585202)

All users of net-snmp are advised to upgrade to these updated packages, which resolve this issue.

1.87. NetworkManager

1.87.1. RHBA-2010:0933: bug fix update

Updated NetworkManager packages that fix a bug are now available for Red Hat Enterprise Linux 5.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and PPPoE devices, and provides VPN integration with a variety of different VPN services.

This update fixes the following bug:

* Prior to this update, stopping the messagebus service (either manually, or during a routine system shutdown) may have caused certain NetworkManager components to terminate unexpectedly with a segmentation fault. With this update, the underlying source code has been modified to target this issue, and NetworkManager components now exit with 0 return code when the messagebus service is stopped. (BZ#653345)

Users are advised to upgrade to these updated packages, which resolve this issue.

1.88. new

1.88.1. RHEA-2011:0069: packages: php53

New php53 packages are now available for Red Hat Enterprise Linux 5.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

The php53 packages provide the current PHP 5.3.x release series for Red Hat Enterprise Linux 5, superseding the 5.1.x series provided by the php packages.

php53 is provided for those users who wish to migrate to a more current PHP release. (BZ#577688)

The php53 and php packages cannot be installed concurrently on the same system. In order to install the php53 packages, you must first remove the php packages if they are installed on your system.

All users requiring PHP 5.3 should install these new packages.

1.88.2. RHEA-2011:0044: packages: sssd

New packages which provide SSSD to Red Hat Enterprise Linux 5 are now available.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system, and a pluggable back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

These new packages provide upstream SSSD version 1.2.1 to Red Hat Enterprise Linux 5. (BZ#579840)

All users requiring SSSD should install these newly-released packages.

1.88.3. RHEA-2011:0035: packages: bind97

New bind97 packages that provide BIND version 9.7.0 are now available for Red Hat Enterprise Linux 5.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a Domain Name System (DNS) server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.

This update adds the following new feature:

* These new bind97 packages support the new Domain Name System Security Extensions (DNSSEC), algorithms (NSEC3, RSA-SHA2), and HMAC-SHA2 TSIGs (Transaction SIGnatures). (BZ#570611)

This update also allows for improved scalability on multiprocessor systems.

All users who require BIND 9.7.0 are advised to install these new packages, which add this new feature.

1.89. New

1.89.1. RHEA-2011:0041: package: libtdb

A new libtdb package, which contains the Trivial Database development library, is now available for Red Hat Enterprise Linux 5.

A new development library, libtdb, is now available. TDB is the small Trivial Database, and is conceptually similar to Gnu dbm and FreeBSD's DB, with the exception that it uses internal locking to allow multiple simultaneous writers.

libtdb is a library that implements a trivial database.

All users requiring libtdb should install this newly-released package, which adds this enhancement.

1.90. nfs-utils

1.90.1. RHBA-2011:0125: bug fix and enhancement update

An enhanced nfs-utils package that fixes various bugs and provides an enhancement is now available.

The nfs-utils package provides a daemon for the kernel NFS (Network File System) server and related tools, which provides better performance than the traditional Linux NFS server. This package also contains the mount.nfs, umount.nfs and showmount programs. Showmount queries the mount daemon on a remote host for information about the NFS server on the remote host. For example, showmount can display the clients which are mounted on that host

This updated nfs-utils package includes fixes for the following bugs:

* NFS mount options could be lost when mounting with the "bg" option. This occurred, due to an incorrect behavior, if the first try_mount() attempt failed. With this update, the failure of try_mount() is handled correctly and the mount options are preserved. (BZ#529370)

* The rpc.statd and rpc.mountd deamons could be using the same UDP port. With this update, the problem occurs no longer. (BZ#541892)

In addition, this updated nfs-utils package provides the following enhancement:

* The nfsiostat and mountstats scripts were added. (BZ#648529)

All users of nfs-utils are advised to upgrade to this updated package, which resolves these issues and provides this enhancement.

1.90.2. RHBA-2011:0011: bug fix update

An updated nfs-utils package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

This update fixes the following bug:

* Previously, the rpc.statd and rpc.mountd daemons could under circumstances use the same UDP port, because the SO_REUSEADDR option is used for the for UDP socket. This update resolves this issue and the daemons no longer use the same UDP port. (BZ#648822)

All nfs-utils users should upgrade to this updated package, which resolves this issue.

1.90.3. RHBA-2010:0604: bug fix update

An updated nfs-utils package that fixes a bug that presented in some circumstances when NFS file system mounts were attempted in the background is now available.

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

This updated package fixes the following bug:

* when an Network File System (NFS) client attempts to mount an NFS exported file system the try_mount() function is called once and two variables -- mount_opts and extra_opts -- are setup to handle any options sent with the mount command. One option -- bg -- sets the command to fork and continue attempting to mount the file system in the background should the initial attempt fail. In some circumstances, when the bg option was used and the initial call to try_mount() failed, options set in the extra_opts variable were lost when the try_mount() function was called again. This update fixes this: using the bg option now works as expected, with all specified and default options honored when an NFS export is mounted in the background. (BZ#614491)

All nfs-utils users should upgrade to this updated package, which resolves this issue.

1.91. nspluginwrapper

1.91.1. RHBA-2010:0445: bug fix update

An updated nspluginwrapper package that fixes a bug is now available.

nspluginwrapper is a utility which allows 32-bit plug-ins to run in a 64-bit browser environment (a common example is Adobe's browser plug-in for presenting proprietary Flash files embedded in web pages). It includes the plug-in viewer and a tool for managing plug-in installations and updates.

This updated nspluginwrapper package fixes the following bug:

* the "spice-xpi" package provides a Firefox plugin that allows for the graphical administration of a KVM virtual machine over the SPICE protocol within the browser. However, the nspluginwrapper compatibility wrapper for plugins caused the Firefox plugin not to be able to open a SPICE session. This update instructs nspluginwrapper to ignore the Firefox SPICE plugin so that it works as expected. (BZ#575058)

All users of nspluginwrapper are advised to upgrade to this updated package, which resolves this issue.

1.92. nss

1.92.1. RHBA-2010:0526: bug fix update

Updated nss packages that resolve an issue are now available.

NSS is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS

#11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.

These updated nss packages fix the following bug:

* a header, 'prlink.h', caused compiler warnings when it was included in an application built with the strict prototype checking enabled (i.e. when "-Wstrict-prototypes" was included in the 'CFLAGS'). If such warnings were treated as errors in the compiler flags (i.e. if "-Werror" was used), the affected application would not compile. The affected applications did not, in fact, need 'prlink.h', they were including it indirectly via another header. This update fixes the header so that it does not expose the faulty header and enables nss client software to build with strict prototype checking enabled, as expected. (BZ#587546)

All users of NSS are advised to upgrade to these updated packages, which resolve this issue.

1.93. nss_ldap

1.93.1. RHBA-2011:0097: bug fix update

An updated nss_ldap package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The nss_ldap package contains the nss_ldap and pam_ldap modules. The nss_ldap module is a plug-in which allows applications to retrieve information about users and groups from a directory server. The pam_ldap module allows a directory server to be used by PAM-aware applications to verify user passwords.

This update fixes the following bugs:

* When looking up host names and addresses, the 'gethostbyname_r' function did not return a proper value for the 'errno_p' parameter when the length of the name or the address was less than was required. This resulted in the host name and the address being overlooked and not returned. With this update, the aforementioned function has been fixed and works as expected. (BZ#468807)

* Under certain conditions, an application which spawned a new child process would begin exhibiting undefined behavior. This was caused by the 'free()' function being called in the 'fork()' function which resulted in a race and hung the application. This update fixes the race issue and the application no longer hangs. (BZ#474181)

* Prior to this update, some processes would trigger SELinux policy denials when attempting to use a connection to a directory server which its parent process had opened. This was caused by a leaked file descriptor. With this update, file descriptors are no longer leaked, thus, SELinux policy denials are no longer triggered. (BZ#500397)

* When using pluggable authentication modules (PAM), selected modules can be loaded and unloaded upon each authentication attempt. However, unloading the pam_ldap module could cause the memory that is allocated by libraries on which it depends to be lost. Consequent to this, multiple authentication attempts may have led to a significant memory loss. To prevent this, the pam_ldap module is no longer unloaded. (BZ#511238)

* When authenticating users using a directory server which provides a password aging policy, a user whose password will expire in less than a day would not be warned of the impending expiration. With this update, a password expiry warning is shown that reminds the user of the impending password expiration. (BZ#537358)

* When the "/etc/ldap.conf" configuration file contained an incomplete configuration or a setting with too large a value, a process which attempted to use nss_ldap could crash. With this update, a crash no longer occurs and an appropriate error is returned. (BZ#538498)

* Adding a large amount of users (multiple kilobytes of usernames) to the 'nss_initgroups_ignoreusers' option in the "/etc/ldap.conf" configuration file resulted in an "Assertion failed" error when executing any nss_ldap related commands. With this update, adding multiple users to the 'nss_initgroups_ignoreusers' option works as expected. (BZ#584157)

* When an LDAP context has been established, obtaining the list of groups a user belongs to could result in a memory leak. With this update, a patch has been applied to address this issue, and such memory leaks no longer occur. (BZ#654650)

* Under certain circumstances, the nss_ldap module may have been unable to correctly process LDAP entries with a large number of group members. This was due to an error number being accidentally overwritten before the control was returned to the caller. When this happened, various utilities failed to produce expected results. With this update, this error has been fixed, the error number is no longer overwritten, and affected utilities now work properly. (BZ#661630)

All users of nss_ldap are advised to upgrade to this updated package, which resolves these issues.

1.93.2. RHBA-2010:0992: bug fix update

An updated nss_ldap package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The nss_ldap package contains the nss_ldap and pam_ldap modules. The nss_ldap module is a plug-in which allows applications to retrieve information about users and groups from a directory server. The pam_ldap module allows a directory server to be used by PAM-aware applications to verify user passwords.

This update fixes the following bugs:

* When using pluggable authentication modules (PAM), selected modules can be loaded and unloaded upon each authentication attempt. However, unloading the pam_ldap module could cause the memory that is allocated by libraries on which it depends to be lost. Consequent to this, multiple authentication attempts may have led to a significant memory loss. To prevent this, the pam_ldap module is no longer unloaded. (BZ#660236)

* When an LDAP context has been established, obtaining the list of groups a user belongs to could result in a memory leak. With this update, a patch has been applied to address this issue, and such memory leaks no longer occur. (BZ#660456)

* Under certain circumstances, the nss_ldap module may have been unable to correctly process LDAP entries with a large number of group members. This was due to an error number being accidentally overwritten before the control was returned to the caller. When this happened, various utilities failed to produce expected results. With this update, this error has been fixed, the error number is no longer overwritten, and affected utilities now work properly. (BZ#662939)

All users of nss_ldap are advised to upgrade to this updated package, which resolves these issues.

1.94. oddjob

1.94.1. RHBA-2010:0668: bug fix update

An updated oddjob package is now available for Red Hat Enterprise Linux 5.

oddjob is a D-BUS service which performs particular tasks for clients which connect to it and issue requests using the system-wide message bus.

This updated package provides patches for the following bugs:

* previously, the configuration settings between systems which support both 32-bit and 64-bit binaries could not be shared. This was because the locations of the oddjob "mkhomedir" helper binary differed between 32-bit and 64-bit versions of the package on such systems. With this update, the helper binary has been moved to the same location on all architectures. (BZ#476255)

* previously, the oddjob_request and pam_oddjob_mkhomedir.so clients would print an error message, when running on systems on which SELinux had been disabled. This was because these clients could not determine the SELinux context of the running oddjobd daemon. With this update, the clients do not attempt to do so anymore and the issue is resolved. (BZ#510457)

All users of D-BUS are advised to upgrade to this updated package, which resolves these issues.

1.95. openais

1.95.1. RHBA-2011:0100: bug fix update

An updated openais package that fixes various bugs is now available.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files, and an init script.

This updated openais package includes fixes for the following bugs:

* Previously, openais crashed with a segmentation fault if it received an unknown message (this could happen when upgrading openais). Unknown messages are now ignored so that openais no longer crashes in these circumstances. (BZ#606028)

* When an Openais client process sent an event to the server (aisexec), the server stopped working. When the client process tried to send the event using the saEvtEventPublish() function, it hung indefinitely on a semaphore (semop()) operation. Even when the server was restarted, the blocked client process was still blocked. The client process no longer hangs indefinitely and is unblocked after a set period of time. (BZ#579081)

* When the openais server was stopped, server clients may have encountered a segmentation fault because of an invalid return code in an internal function. This crash no longer occurs. (BZ#596359)

* Previously, the Closed Process Group (CPG) interface returned the wrong result, which could have led to incorrect behavior in some situations. With this update, the CPG interface now behaves as expected. (BZ#599654)

* An incorrectly-configured network could have casued the openais server to enter a continuous FAILED TO RECEIVE/GATHER loop. (BZ#533383)

* A gather operation which interrupted synchronization could have caused cluster lockup. (BZ#586519)

* A memmove() operation on a high-loss network could have caused possible stack corruption resulting in stack protector abort due to an incorrectly-calculated length in the memmove() operation. (BZ#588489)

* The retransmit list is now properly-typed so as not to confuse the compiler. (BZ#588494)

* In high-loss networks, an assert based on a constant value for the retransmit message queue size could have caused a some nodes to receive SIGABRT signals, and therefore terminate. This constant value has been increased to correspond to the maximum number of entries, thus resolving the issue. (BZ#588500)

* An internal timer variable was reset on each token retransmission rather than only on original token transmission; this has been fixed in this updated package. (BZ#614222)

* OpenAIS has been enabled to work in network environments wherein multicast messages are slightly delayed when compared to token messages. (BZ#619536)

* In high loss networks, all nodes in a cluster experienced a buffer overflow and aborted when a threshold of unprocessed/not transmitted packets was reached. With this update, even when a significant number of packets is unprocessed/not transmitted, all nodes in a cluster work as expected and do not abort. (BZ#594480)

* Isolating a node and then removing the isolation potentially resulted in membership misbehavior. (BZ#611129)

* When a checkpoint name was not terminated with the NULL character, the aisexec process may have terminated unexpectedly with a segmentation fault, causing a cluster outage. With this update, the underlying source code has been modified to resolve this issue, and such strings no longer cause aisexec to crash. (BZ#625947)

* In rare circumstances, an invalid CPG member was delivered in a configuration change callback. (BZ#568650)

* An internal protocol variable was set on retransmission when it should only have been set on the first transmission. With this update, the aforementioned variable is only set on the first transmission. (BZ#598689)

* The receipt of out-of-order messages could have resulted in token loss. (BZ#619570)

All users of openais are advised to upgrade to this updated package, which resolves these issues.

1.95.2. RHBA-2010:0983: bug fix update

An updated openais package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files, and an init script.

This updated openais package provides a fix for the following bug:

* When a checkpoint name was not terminated with the NULL character, the aisexec process may have terminated unexpectedly with a segmentation fault, causing a cluster outage. With this update, the underlying source code has been modified to resolve this issue, and such strings no longer cause aisexec to crash. (BZ#638609)

All users of openais are advised to upgrade to this updated package, which resolves this issue.

1.95.3. RHBA-2010:0708: bug fix update

An updated openais package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files, and an init script.

This updated openais package provides fixes for the following bugs:

* previously, an internal protocol variable was set on retransmission when it should only have been set on the first transmission. With this update, this variable is only set on the first transmission. (BZ#601077)

* previously, multicast could be delayed while sending unicast packets due to the bahavior of many hardware switches. With this update, only required messages are retransmitted. (BZ#621264)

All users of OpenAIS are advised to upgrade to this updated package, which resolves these issues.

1.95.4. RHBA-2010:0629: bug fix update

An updated openais package that fixes various bugs is now available.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

This updated openais package provides fixes for the following bugs:

* in high loss networks, all nodes in a cluster experienced a buffer overflow and aborted when a threshold of unprocessed/not transmitted packets was reached. With this update, even when a significant number of packets is unprocessed/not transmitted, all nodes in a cluster work as expected and do not abort. (BZ#601086)

* when an Openais client process sent an event to the server (aisexec), the server stopped working. When the client process tried to send the event using the saEvtEventPublish() function, it hanged indefinitely on a semaphore (semop()) operation. Even when the server was restarted, the blocked client process was still blocked. With this update, the client process no longer hangs indefinitely and is unblocked after a set period of time. (BZ#603615)

* when the openais server was stopped, server clients may have encountered a segmentation fault because of an invalid return code in an internal function. With this update, the segmentation fault no longer occurs. (BZ#603623)

* previously, CPG API returned the wrong results when a cluster component failed that was using openais. With this update, the correct results are returned. (BZ#618766)

* previously, openais returned a segmentation fault if it received a CPQ message. With this update, new message IDs are introduced into the CPQ service so that the CPQ messages no longer cause a segmentation fault in openais. (BZ#611931)

All users of openais are advised to upgrade to this updated package, which resolves these issues.

1.95.5. RHBA-2010:0486: bug fix update

An updated openais package that fixes various bugs is now available.

The Application Interface Specification (AIS) is an API and set of policies for developing applications that maintain service during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais packages contain the openais executable, OpenAIS service handlers, default configuration files and init script.

This updated openais package provides fixes for the following bugs:

* due to the very low queue limit, openais could receive a SIGABRT signal when the 500 messages threshold was reached on high loss networks, resulting in the termination of some nodes. With this update, the limit has been increased to a maximum of 16384 messages to avoid receiving the abort signal. (BZ#588627)

* on high loss networks, entering the "gather" state could interrupt the recovery and cause an improper message delivery or even a segmentation fault. This update ensures that the internal data element is being restored properly, so that the sync process is no longer affected. (BZ#588628)

* on high loss networks, an unexpected stack corruption could cause stack protector to send a SIGABRT signal and terminate the node. This update fixes this error and the stack corruption no longer occurs. (BZ#588895)

* the use of an incorrect data type could lead to an internal data corruption. This error has been fixed and the data type is now set properly. (BZ#588897)

All users of openais are advised to upgrade to this updated package, which resolves these issues.

1.95.6. RHBA-2010:0403: bug fix update

Updated openais packages that resolve a bug are now available for Red Hat Enterprise Linux 5.5 Extended Update Support.

The Application Interface Specification (AIS) is an API and set of policies for developing applications that maintain service during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais packages contain the openais executable, OpenAIS service handlers, default configuration files and init script.

These updated openais packages provide a fix for the following bug:

* When a multicast message was not received by a node in the cluster at the end of the total order, the protocol used in OpenAIS failed to recover this last message. This most often occurred in lightly-loaded, bonded networks, and resulted in the message "FAILED TO RECV" appearing in the system logs. (BZ#577887)

All users of openais are advised to upgrade to these updated packages, which resolve this issue.

1.96. openCryptoki

1.96.1. RHBA-2010:0699: bug fix update

Updated openCryptoki packages that resolve an issue are now available.

The openCryptoki package contains version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z).

These updated openCryptoki packages provide fix for the following bug:

* previously, the overall performance of cryptographic operations degraded exponentially with the number of objects per token or open sessions per process. This was caused by the fact that OpenCryptoki used linked-lists to track objects and sessions in memory, thus, performing an exhaustive search in practically every PKCS#11 call. With this update, the overall performance remains constant. (BZ#627560)

All users of openCryptoki are advised to upgrade to these updated packages, which resolve this issue.

1.97. OpenIPMI

1.97.1. RHBA-2011:0096: bug fix and enhancement update

Updated OpenIPMI packages that fix several bugs and add various enhancements are now available.

OpenIPMI (Intelligent Platform Management Interface) provides command line tools and utilities to access

platform information, allowing system administrators to monitor system health and manage systems.

The updated OpenIPMI packages fixes the following bugs:

* The command 'ipmitool sol payload' accepted incorrect argument values. With this update, argument values are validated. (BZ#514218)

* The command 'ipmitool sel' accepted incorrect argument values. Argument values are now validated. (BZ#514237)

* When the BMC (baseboard management controller) sends sensor data, the second event state byte is optional. The 'ipmitool sensor list' command sometimes displayed misleading data. When the BMC did not send the second (optional) event state byte, 'ipmitool' displayed the received data incorrectly. The 'ipmitool' command now checks the length of the incoming state field properly and displays the received data correctly. (BZ#541263)

* If the user called 'ipmitool tsol' on a serial console over LAN on Tyan hardware, the application terminated unexpectedly. This happened due to a mistake in serial-over-lan on Tyan hardware. Now this issue is fixed. (BZ#546386)

* The command 'ipmitool sensor list' failed when reading a sensor with invalid units. The ipmitool utility now processes invalid readings and reports 'Unknown' units. (BZ#550120)

* In the lanplus interface, the 'ipmitool' command displayed unclear error messages when the user provided a wrong username or password. The 'ipmitool' command now displays a notification that the username or password is incorrect. (BZ#552458)

* When setting user privileges with the command 'ipmitool user priv', the ipmitool utility automatically enabled IPMI messaging for the user. The updated ipmitool no longer enables IPMI messaging automatically. To enable IPMI messaging, use the command 'ipmitool channel setaccess'. (BZ#552459)

* A serial console connected through LAN and activated with the command 'ipmitool sol activate' could consume all available memory resources. This update package fixes the issue. (BZ#576004)

* The command 'ipmitool sensor elist' terminated unexpectedly when receiving an error. The updated ipmitool utility now parses the incoming packets properly and recovers from unexpected error messages. (BZ#580087)

* The pkgconfig script contained incorrect link options. This could have resulted in linking errors when compiling software that used the OpenIPMI libraries. This update fixes the pkgconfig script and software correctly links to the OpenIPMI libraries. (BZ#591646)

* When listing sensors, the ipmitool utility incorrectly showed the 15th bit of event state of a discrete sensor. The 15th bit of event state of a discrete sensor is now ignored as defined in the IPMI specification and it is hidden in the output. (BZ#616546)

* The command 'service ipmi start' returned an error if the service was already running. The updated package fixes the service init script and reports subsequent service start as successful. (BZ#619143)

* The 'ipmitool sensor' command failed to report hardware temperatures. This occurred on hardware with unusual IPMB (Intelligent Platform Management Bus) addresses where ipmitool bridged messages to the BMC. The 'ipmitool' utility now recognizes all IPMB addresses properly and does not bridge requests to the BMC, and reports temperatures as expected. (BZ#636854)

These updated OpenIPMI packages provide the following enhancements:

* This update adds the 'channel kgset' subcommand to the 'ipmitool' command, which allows for KG key configuration. (BZ#503039)

* These packages add a Dell-specific IPMI extension, which adds the "delloem" subcommand to the 'ipmitool' command. The extension allows users to browse the list of network interfaces, read the LCD panel and set its options, and monitor system power consumption. (BZ#568676)

Users are advised to upgrade to these updated OpenIPMI packages, which resolve these issues and add these enhancements.

1.98. openldap

1.98.1. RHBA-2010:0914: bug fix update

Updated OpenLDAP packages that fix a bug are now available for Red Hat Enterprise Linux 5.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

These updated packages provide a fix for the following bug:

* Due to an error introduced in one of the previous updates, initializing a connection to a slapd server may have caused the CPU usage to reach 100% and the server to become unresponsive for about 3 seconds. With this update, an existing upstream patch has been applied to target this issue, and the OpenLDAP suite now works as expected. (BZ#653910)

All users of OpenLDAP are advised to upgrade to these updated packages, which resolve this issue.

1.98.2. RHBA-2010:0617: bug fix update

Updated OpenLDAP packages that provides a fix for a bug are now available for Red Hat Enterprise Linux 5.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

These updated packages provide a fix for the following bug:

* previously, slapd could unexpectedly abort during replication using LDAP protocol replication. This issue is now resolved and no more crashes occur when slapd adds or deletes user data. (BZ#620621)

All users of OpenLDAP are advised to upgrade to these updated packages, which resolve this issue.

1.99. openmotif

1.99.1. RHBA-2010:0822: bug fix update

An updated openmotif package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The openmotif package includes the Motif shared libraries needed to run applications that are dynamically linked against Motif, as well as the Motif Window Manager (MWM).

This update fixes the following bug:

* Due to 32-bit time stamp issues, attempting to copy and paste on a 64-bit architecture using the clipboard may have failed occasionally. With this update, the underlying source code has been modified to ensure the time stamp always contains a "CARD32" value, so that copy and paste on 64-bit architectures works as expected. (BZ#647399)

All users of openmotif are advised to upgrade to this updated package, which resolves this issue.

1.99.2. RHBA-2010:0667: bug fix update

Updated openmotif packages that fix a bug are now available.

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

These updated openmotif packages fix the following bug:

* previously, when the icon box in MWM was enabled, placing a window over the icon box and removing the window afterwards caused a graphics corruption of the icons. With this update, icons in the icon box are no longer corrupt.

All users of openmotif are advised to upgrade to these updated packages, which resolve this issue.

1.100. openssh

1.100.1. RHBA-2011:0018: bug fix and enhancement update

Updated openssh packages that fix various bugs and add enhancements are now available for Red Hat Enterprise Linux 5.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

These updated packages fix the following bugs:

* When the ~/.bashrc startup file contained a command that produced an output to standard error (STDERR), the sftp utility was unable to log in to that account. This bug has been fixed, and the output to STDERR no longer prevents sftp from establishing the connection. (BZ#576765)

* Due to the limitations of the data type that was used to store user identifier (UID), the lastlog record was not created for users with UID larger than 2147483647. With this update, this data type has been changed to unsigned long integer, and the /var/log/lastlog database is now updated as expected. (BZ#616396)

* Although the OpenSSH update RHSA-2009:1287 mentioned the change of the cipher preference, the openssh packages did not actually include this adjustment. This update changes the cipher preference as announced, so that CTR mode ciphers are now preferred to CBC mode. (BZ#661716)

As well, this update adds the following enhancements:

* The "ForceCommand" directive has been added as a valid /etc/ssh/sshd_config option, making it possible to force the execution of the supplied command regardless of user input. (BZ#532559)

* The OpenSSL dynamic engine loading support has been added, so that the ibmca engine can now use Central Processor Assist for Cryptographic Function (CPACF). (BZ#594815)

* When a key authentication is used to log in to a machine, the same information as the one that is logged when using Pluggable Authentication Modules (PAM) is written to the log file, including the information about the key type and size, and a fingerprint. Additionally, when an encrypted tunnel is being established, the sshd daemon now logs the result of the cipher negotiation, that is, the type and the key size. (BZ#632402,

BZ#659242, BZ#661669)

All OpenSSH users are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

1.100.2. RHEA-2010:0683: enhancement update

Updated openssh packages that add an enhancement are now available.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

These updated packages add the following enhancement:

* The OpenSSL dynamic engine loading support has been added, so that the ibmca engine can now use Central Processor Assist for Cryptographic Function (CPACF). (BZ#629509)

All OpenSSH users are advised to upgrade to these updated packages, which add this enhancement.

1.101. openssl-ibmca

1.101.1. RHBA-2010:0655: bug fix update

New openssl-ibmca packages that fix a bug are now available for Red Hat Enterprise Linux 5.

openssl-ibmca is a shared object OpenSSL dynamic engine for the IBM eServer Cryptographic Accelerator (ICA).

This updated package provides a fix for the following bug:

* previously, the dynamically loaded ibmca engine for OpenSSL failed because key length 4096 for RSA in the engine was not supported. With this update, the ibmca engine uses the Hardware accelerator for key lengths smaller than or equal to 2048 and falls back to software implementation directly from OpenSSL for key lengths greater than 2048. (BZ#597394)

All openssl-ibmca users are advised to upgrade to this updated package, which resolves this issue.

1.102. Openswan

1.102.1. RHEA-2010:0444: enhancement update

Updated openswan packages that implement Diffie-Hellman groups 22, 23 and 24 from RFC 5114 are now available.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) for Linux. IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the IPsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network, or VPN.

These packages contain the daemons and userland tools for setting up openswan. They support the NETKEY/XFRM IPsec stack in the default Linux kernel. The openswan 2.6.x-series also supports IKEv2 as described in RFC 4309.

This update adds the following enhancement:

* RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, adds eight Diffie-Hellman groups (three prime modulus groups and five elliptic curve groups) to the extant 21 groups set out in previous RFCs (eg RFCs 2409, 3526 and 4492) for use with IKE, TLS, SSH and so on.

This update implements groups 22, 23 and 24: a 1024-bit MODular exPonential (MODP) Group with 160-bit Prime Order Subgroup; a 2048-bit MODP Group with 224-bit Prime Order Subgroup; and a 2048-bit MODP Group with 256-bit Prime Order Subgroup respectively. (BZ#591104)

Note: implementation of group 24 (a 2048-bit MODP Group with 256-bit Prime Order Subgroup) is required for US National Institute of Standards and Technology (NIST) IPv6 compliance and ongoing FIPS-140 certification.

All openswan users should install these updated packages, which add this enhancement.

1.103. pam_krb5

1.103.1. RHBA-2010:0746: bug fix update

An updated pam_krb5 package that fixes a bug and provides an enhancement is now available.

The pam_krb5 module allows Pluggable Authentication Modules (PAM) aware applications to use Kerberos to verify user identities by obtaining user credentials at log in time.

This updated pam_krb5 package fixes the following bug:

* Previously, the verify_ap_req_nofail setting in /etc/krb5.conf's "libdefaults" section was ignored when pam_krb5 verified initial credentials. With this update, the credential verification part of the module recognizes the verify_ap_req_nofail setting. (BZ#541177)

In addition, this updated package provides the following enhancement:

* Previously, pam_krb5 messages and prompts were only available in English. With this update, pam_krb5 is available in various languages thus able to match the language of your desired locale. (BZ#526067)

Users are advised to upgrade to this updated pam_krb5 package, which resolves this issue and adds this enhancement.

1.104. passwd

1.104.1. RHBA-2010:0620: bug fix update

Updated passwd packages that fix bugs are now available for Red Hat Enterprise Linux 5.

The passwd packages contain the system utility passwd which changes passwords and displays password status information using Pluggable Authentication Modules (PAM) and Libuser libraries.

These updated passwd packages provide fixes for the following bugs:

* while building the packages, the debuginfo packages were not correctly generated which rendered the passwd utility unable to be debugged. With this update, the passwd-debuginfo contains debugging symbols and the passwd utility can now be debugged. (BZ#500615)

* previously, the description of the passwd command in the passwd(1) manual page contained formatting errors which caused parts of the text to be missing. It also contained inaccurate information. With this update, these errors are corrected. (BZ#545668)

* passwd -S was not able to display the correct password types for the new password hashes. It also returned nonzero exit values even when the password status was displayed successfully. With this update, the correct password type is shown in the output. (BZ#578534)

All passwd users are advised to upgrade to these updated passwd packages, which resolve these issues.

1.105. patch

1.105.1. RHBA-2010:0656: bug fix update

An updated patch package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The patch package is used to apply changes, such as those from diff files, to text files.

This updated package package provides a fix for the following bug:

* previously, SELinux file contexts were not preserved on patched files. This has been corrected. (BZ#229329)

* previously, patches for files whose names contain spaces could not be applied. A change has been backported to allow filenames with spaces. (BZ#431887)

* The "-g" option was not handled correctly by the patch command. This has been fixed. (BZ#553624)

All users of patch are advised to upgrade to this updated package, which resolves this issue.

1.106. pciutils

1.106.1. RHEA-2011:0045: enhancement and bug fix update

An enhanced pciutils package that fixes various bugs and provides an enhancement is now available.

The pciutils package contains various utilities for inspecting and manipulating devices connected to the PCI bus.

This updated pciutils package has been enhanced by being upgraded to upstream version 3.1.7, which provides fixes for the following bugs:

* Several pciutils utilities were unable to recognize newer PCIe capabilities, and therefore returned an "UNKNOWN" message instead of a proper description. With this update, the PCI utilities are now aware of PCIe capabilities, and return a proper description. (BZ#511992)

* The lspci command was unable to report which PCI slot a certain device was plugged into. With this updated package, lspci reports which PCI slot a device is using given that the information is available. (#563286)

All users of pciutils are advised to upgrade to this updated package, which resolves these issues and provides this enhancement.

1.107. pcre

1.107.1. RHEA-2011:0022: enhancement update

An enhanced pcre package is now available for Red Hat Enterprise Linux 5.

PCRE is a Perl-compatible regular expression library.

This updated pcre package adds the following enhancement:

* Unicode properties have been enabled to support \p{..}, \P{..}, and \X escape sequences. (BZ#457064)

Users of pcre are advised to upgrade to this updated package, which adds this enhancement.

1.108. perl

1.108.1. RHBA-2010:0712: bug fix update

Updated perl packages that fix a bug in threading are now available.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

This update fixes the following bug:

* Previously, joining a thread variable or calling the "undef" function on it in a Perl script resulted in the following error message:

Attempt to free unreferenced scalar: SV 0x7b7dcb0, Perl interpreter: 0x7b4cfb0 during global destruction.

This error has been fixed, and using the above functions now works as expected. ([BZ#629935](#))

Users of threads in Perl programs are advised to upgrade to these updated packages, which resolve this issue.

1.109. perl-Archive-Tar

1.109.1. RHBA-2010:0595: bug fix update

An updated perl-Archive-Tar package that fixes a bug is now available.

The Archive::Tar module provides a mechanism for Perl scripts to manipulate tar archive files.

This updated perl-Archive-Tar package fixes the following bug:

* when using the Archive::Tar Perl module, when the $VERSION variable was referenced, a warning message similar to the following was printed to standard output:

Argument "1.39_01" isn't numeric in subroutine entry at -e line 1.

This was caused by the presence of an underscore in the $VERSION variable. With this update, the Archive::Tar module no longer outputs this warning message. ([BZ#614408](#))

Note: this regression was caused by a change to the module's version number, and was introduced by the RHSA-2010:0505 perl-Archive-Tar security update.

All users of perl-Archive-Tar are advised to upgrade to this updated package, which corrects this issue. All applications using the Archive::Tar module must be restarted for this update to take effect.

1.110. perl-Sys-Virt

1.110.1. RHBA-2011:0117: bug fix update

Updated perl-Sys-Virt packages, that support new libvirt APIs, are now available for Red Hat Enterprise Linux 5.

The perl-Sys-Virt package provides an API for managing virtual machines from Perl, using the libvirt library.

This update fixes the following bug:

Previously, perl-Sys-Virt was not able to authenticate with libvirt ESX driver connections. This update fixes the compatibility with ESX driver and introduces support for new APIs in the rebased libvirt package. (BZ#63200)

All users of Perl or Perl-based tools, which use virtual machine management, are advised to upgrade to this updated package which fixes this bug.

1.111. piranha

1.111.1. RHBA-2011:0091: bug fix update

Updated piranha packages that fix several bugs are now available for Red Hat Enterprise 5.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. It includes various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

This update fixes the following bugs: * Previously, timeout values for both TCP and UDP sessions returned to the default when both load directors were rebooted simultaneously. With this update, an option to delay the start of LVS is introduced. (BZ#453451)

* Previously, the pulse daemon failed to parse the load average using "load_monitor = ruptime". With this update, pulse parses the load average correctly. (BZ#550126)

* Previously, piranha did not work when SELinux was enabled. With this update, piranha runs as expected with SELinux. (BZ#604742)

All piranha users are advised to upgrade to these updated packages, which resolve these issues.

1.112. pirut

1.112.1. RHBA-2011:0132: bug fix update

An updated pirut package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The pirut package provides a set of graphical tools for managing software.

This update fixes the following bug:

* Due to an error in the Slovak translation, working with a package that was signed with an unknown GPG key caused pirut to terminate unexpectedly with a traceback. This update corrects the Slovak translation, and pirut no longer crashes. (BZ#661278)

All users are advised to upgrade to this updated package, which resolves this issue.

1.113. poppler

1.113.1. RHBA-2010:0658: bug fix update

An updated poppler package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Poppler is a Portable Document Format (PDF) rendering library, used by applications such as Evince.

This update provides a fix for the following bug:

* previously, poppler was unable to open some PDFs created with Adobe Acrobat due to incorrect determination of the position in the JBIG2 stream. With this update, such PDFs open correctly. (BZ#624702)

All users of poppler and applications that rely on poppler are advised to upgrade to this updated package, which resolves this issue.

1.114. ppc64-utils

1.114.1. RHEA-2011:0087: bug fix and enhancement update

An enhanced ppc64-utils package that fixes several bugs is now available.

The ppc64-utils package is a collection of utilities for Linux running on 64-bit PowerPC platforms.

This updated ppc64-utils package adds the following enhancements:

* The lsvpd utility that lists hardware Vital Product Data (VPD), such as, vendor, version, revision level, and serial number, was upgraded to upstream version 1.6.8. (BZ#565612)

* The libvpd library, which is a library for lsvpd, was upgraded to upstream version 2.1.2. (BZ#566271)

* The package provides support for partition hibernation. (BZ#579800)

In addition, this updated ppc64-utils package provides fixes for the following bugs:

* Previously, several man pages were missing. This update adds the missing pages. (BZ#555781)

* On the ofpathname manual page, "PoowerPC-64" was changed into PowerPC-64". (BZ#577338)

* The ofpathname manual page did not show the "-a" and "-V" options, and the "-?" option was displayed for the "--help" option. The missing "-a" and "-V" options were added and the short option for "--help", "-?", was changed to "-h" and the manual page shows all options as expected. (BZ#578516)

* Previously, the ofpathname command could not properly convert a logical name to an Open Firmware device path name for SAN disk. With this update, ofpathname converts the logical name properly. (BZ#580992)

* Previously, the drmgr tool does not support PCI DLPAR remove operations on the Jupiter and Juno Power platforms. With this update, drmgr supports remove operations. (BZ#655087)

* After the ppc64-utils installation, the install.log file contained the following error message:

error reading information on service vpdupdater: No such file or directory

With this update, the error message is no longer in the log file. (BZ#638513)

Users of ppc64-utils are advised to upgrade to this updated package, which adds these enhancements and resolves these issues.

1.115. python

1.115.1. RHSA-2011:0027: Low security, bug fix, and enhancement update

Updated python packages that fix multiple security issues, several bugs, and add two enhancements are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Python is an interpreted, interactive, object-oriented programming language.

It was found that many applications embedding the Python interpreter did not specify a valid full path to the script or application when calling the PySys_SetArgv API function, which could result in the addition of the current working directory to the module search path (sys.path). A local attacker able to trick a victim into running such an application in an attacker-controlled directory could use this flaw to execute code with the victim's privileges. This update adds the PySys_SetArgvEx API. Developers can modify their applications to use this new API, which sets sys.argv without modifying sys.path. (CVE-2008-5983)

Multiple flaws were found in the Python rgbimg module. If an application written in Python was using the rgbimg module and loaded a specially-crafted SGI image file, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2009-4134, CVE-2010-1449, CVE-2010-1450)

Multiple flaws were found in the Python audioop module. Supplying certain inputs could cause the audioop module to crash or, possibly, execute arbitrary code. (CVE-2010-1634, CVE-2010-2089)

This update also fixes the following bugs:

* When starting a child process from the subprocess module in Python 2.4, the parent process could leak file descriptors if an error occurred. This update resolves the issue. (BZ#609017)

* Prior to Python 2.7, programs that used "ulimit -n" to enable communication with large numbers of subprocesses could still monitor only 1024 file descriptors at a time, which caused an exception:

ValueError: filedescriptor out of range in select()

This was due to the subprocess module using the "select" system call. The module now uses the "poll" system call, removing this limitation. (BZ#609020)

* Prior to Python 2.5, the tarfile module failed to unpack tar files if the path was longer than 100 characters. This update backports the tarfile module from Python 2.5 and the issue no longer occurs. (BZ#263401)

* The email module incorrectly implemented the logic for obtaining attachment file names: the get_filename() fallback for using the deprecated "name" parameter of the "Content-Type" header erroneously used the "Content-Disposition" header. This update backports a fix from Python 2.6, which resolves this issue. (BZ#644147)

* Prior to version 2.5, Python's optimized memory allocator never released memory back to the system. The memory usage of a long-running Python process would resemble a "high-water mark". This update backports a fix from Python 2.5a1, which frees unused arenas, and adds a non-standard sys._debugmallocstats() function, which prints diagnostic information to stderr. Finally, when running under Valgrind, the optimized allocator is deactivated, to allow more convenient debugging of Python memory usage issues. (BZ#569093)

* The urllib and urllib2 modules ignored the no_proxy variable, which could lead to programs such as "yum" erroneously accessing a proxy server for URLs covered by a "no_proxy" exclusion. This update backports fixes of urllib and urllib2, which respect the "no_proxy" variable, which fixes these issues. (BZ#549372)

As well, this update adds the following enhancements:

* This update introduces a new python-libs package, subsuming the majority of the content of the core python package. This makes both 32-bit and 64-bit Python libraries available on PowerPC systems. (BZ#625372)

* The python-libs.i386 package is now available for 64-bit Itanium with the 32-bit Itanium compatibility mode. (BZ#644761)

All Python users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

1.115.2. RHBA-2010:0871: bug fix update

Updated python packages that resolve an issue with the "email" module are now available.

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

These updated python packages provide fixes for the following bug:

* Prior to this update, the "email" module incorrectly implemented part of the logic for obtaining file names of attachments, and as a result, get_filename()'s fallback for using the "Content-Type" header's deprecated "name" parameter erroneously used the "Content-Disposition" header instead. This update applies a patch from Python 2.6, fixing this problem. (BZ#649250)

All users of Python are advised to upgrade to these updated packages, which resolve this issue.

1.115.3. RHBA-2010:0724: bug fix update

Updated python packages that resolve several issues are now available.

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

These updated python packages provide fixes for the following bugs:

* Previously, Python 2.4's "subprocess" module contained a bug where a Python process could leak file descriptors if an error occurred when starting a child process. With this update, the Python process no longer leaks file descriptors. (BZ#630663)

* Prior to Python 2.7, the "subprocess" module used the "select" system call when connecting to the streams of child processes. This operation failed with a ValueError exception (ValueError: filedescriptor out of range in select()) when more file descriptors were open in the python process than the limit defined by the FD_SETSIZE macro in the <sys/select.h> header (typically 1024). With this update, the module was ported to use the "poll" system call, removing this limit. (BZ#630832)

* Prior to Python 2.5, the "tarfile" module would fail to unpack tar files with a path longer than 100 characters. This update backports Python 2.5's "tarfile" module, fixing this problem. (BZ#631816)

All users of python are advised to upgrade to these updated packages, which resolve these issues.

1.116. python-dmidecode

1.116.1. RHBA-2010:0695: bug fix update

An updated python-dmidecode package that fixes a bug is now available.

The python-dmidecode module is a Python extension that uses the code-base of the dmidecode utility, and presents the DMI data as Python dictionaries or XML utilizing libxml2.

This update provides fixes for the following bugs:

* previously, the Python script would be stopped because of a assertion failure. This was due to the DMI tables on certain hardware with which unexpectedly returned NULL values instead of a string. With this update, the script does not anymore encounter assertion faults and processes NULL values correctly as empty strings. (RH BZ#596133)

* previously a segmentation fault occured when trying to identify the processor type via string comparison. This was due to the DMI tables on certain hardware which did not report the CPU processor information as a string and returned NULL instead. This update adds additional checks for NULL values before doing this string comparison. (RH BZ#621837)

* previously, a large amount of duplicated warnings could appear in the output. This was due to the DMI tables on certain hardware where the length description did not match the length of the tables found on the system. With this update, the logging function has been improved to avoid unnecessary duplication of warnings. (RH BZ#621895)

All users of the python-dmidecode module are advised to upgrade to this updated package, that addresses these issues.

1.117. python-urlgrabber

1.117.1. RHBA-2011:0038: bug fix update

An updated python-urlgrabber package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The python-urlgrabber is a high-level cross-protocol url-grabber for python supporting HTTP, FTP and file locations. Features include keepalive, byte ranges, throttling, authentication, proxies and more.

This updated package provides fixes for the following bugs:

* previously, messages were truncated when downloading packages. As a result, the lines were truncated so they didn't show the names of the packages that were being downloaded. With this update, the complete package information is printed when packages are being downloaded and this issue is resolved. (BZ#500912)

* previously, the python-urlgrabber could not handle the character '@' or '%40' as login in username or password when authenticating. With this update, the information for username and password is encoded correctly, username and password fields are unquoted after splitting from the host portion, and this issue is resolved. (BZ#576651)

All python-urlgrabber users are advised to upgrade to this updated package, which resolves these issues.

1.118. python-virtinst

1.118.1. RHBA-2011:0078: bug fix and enhancement update

An updated python-virtinst package that fixes bugs and adds enhancements is now available for Red Hat Enterprise Linux 5.

The python-virtinst utility is a module that helps build and install libvirt based virtual machines.

This update fixes the following bugs:

* Previously, the command "rpmbuild -bp" failed if a recent rpm was used and the patch flags were changed so that patch backup files were not created in some backup directory, because 0.400.3-unicode-fix.patch modified the backup file of previous patches. With this update, rpmbuild -bp works as expected. (BZ#579976)

* Previously, the virt-install man page wrongly showed the default QEMU/KVM MAC address as beginning with 54:52... . With this update, the correct sequence 52:54 ... is shown. (BZ#620838)

This update also adds the following enhancement:

* Previously, virt-install ignored the passed arguments when the -x option was used with local install media instead of URL installs. This update adds the ability for virt-install to recognize passed arguments in the -x option with local install media and prints errors for these. (BZ#593410)

All users of python-virtinst are advised to upgrade to this updated python-virtinst package which resolves these issues.

1.118.2. RHBA-2010:0763: bug fix update

An updated python-virtinst package that fixes a bug in the virt-clone tool, is now available for Red Hat Enterprise Linux 5.

python-virtinst is a module that helps build and install libvirt based virtual machines. virt-clone is a command line tool that clones existing virtual machine images with the "libvirt" library.

* Previously, the virt-clone tool prevented cloning existing virtual machines to a block device. This was caused by a flawed validation check of the clone destination that would exit the virt-clone tool with an error if the clone destination file already existed. With this update, virt-clone skips this check if the clone destination is a block device. (BZ#628458)

Users of python-virtinst, who clone virtual machines to a block device, are advised to upgrade to this updated package, which resolves this issue.

1.119. qffmpeg

1.119.1. RHBA-2010:0559: bug fix update

An updated qffmpeg package that fixes an SELinux incompatibility is now available.

qffmpeg provides video codecs for the Spice remote desktop protocol.

This update addresses the following issue:

* shared libraries at /usr/lib/libqavcodec.so.51 required a text relocation (a reference to an object with a variable address at runtime using an absolute addressing mode). This is a potential security problem and, consequently, when a Spice session attempted to load these libraries an SELinux exception triggered and Spice failed to launch with the following error:

spicec: error while loading shared libraries: /usr/lib/libqavcodec.so.51:

cannot restore segment prot after reloc: Permission denied

This update corrects the affected qffmpeg assembly: text relocation is no longer required and the exception is no longer triggered. (BZ#576564)

Note: a workaround existed. The file context and default file context of "/usr/lib/libqavcodec.so.51.71.0" could be changed as follows to allow the library to load:

chcon -t textrel_shlib_t '/usr/lib/libqavcodec.so.51.71.0'

semanage fcontext -a -t textrel_shlib_t '/usr/lib/libqavcodec.so.51.71.0'

This workaround is no longer necessary. If the workaround was used prior to this update's release, undoing these changes is recommended.

All Spice users should install this updated package which fixes this bug.

1.120. qspice

1.120.1. RHBA-2010:0579: bug fix update

Updated qspice packages that fix a bug are now available.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor, or on Red Hat Enterprise Virtualization Hypervisor.

These updated qspice packages fix the following bug:

* after a live migration of a virtual machine with multiple monitors, not being reset properly at the client side, the palette cache was not always synchronized between the server and the client, which could cause the client to terminate unexpectedly. With this update, the target server always sends the "RESET" instruction to the client for all monitors, and the client now works as expected. (BZ#609582)

Users requiring remote display capabilities for KVM hypervisors are advised to upgrade to these updated qspice packages, which resolve the above issue.

1.121. quagga

1.121.1. RHBA-2010:0420: bug fix update

Updated quagga packages that fix a bug are now available.

Quagga manages the TCP/IP based routing protocol. It takes multi-server and multi-thread approaches to resolve the current complexity of the Internet. Quagga supports BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng. Quagga is intended to be used as a Route Server and a Route Reflector.

This update fixes the following bug:

* several declarations were missing from zebra.h, including the zebra_route_string() function. As a consequence, if the "show ip protocol" command was issued to a running zebra sever, zebra segfaulted rather than present the two column "Protocol : route-map" table. This update adds the missing declarations to zebra.h and issuing the "show ip protocal" command now works as expected. (BZ #576903)

All quagga users should upgrade to these updated packages, which resolve this issue.

1.122. quota

1.122.1. RHBA-2011:0023: bug fix and enhancement update

An updated quota package that fixes several bugs and adds various enhancements, including ext4, remote quota limits, and LDAP address lookup, is now available.

The quota package contains system administration tools for monitoring and limiting user and group disk usage on file systems.

This updated quota package provides fixes for the following bugs:

* The quotaon(8) man page also serves as the manual documentation for the quotaoff command; however, the quotaoff(8) man page was not correctly linked to it. With this update, this error has been corrected and quotaoff(8) man page is now redirected to the quotaon(8). (BZ#574804)

* When a user reached the hard quota limit (the maximal disk usage a user cannot exceed), the quota command did not display the remaining grace period (the remaining time before enforcing the limits) in its output. With this update, quota always displays the amount of time remaining in the grace period when the user has exceeded or met their hard or soft disk usage limit. (BZ#589472)

* The warnquota(8) man page implied that the warnquota command checks the disk quota for all file systems, whereas it actually only checks local file systems. It does not, for example, check NFS-mounted file systems (i.e. those mounted by the Network File System) with quotas enabled. The man page has been clarified in this regard and no longer contains misleading information. (BZ#589523)

* The quota package contained the xqmstat(8) man page despite the fact that Red Hat Enterprise Linux 4 does not support XFS quotas. The man page has been removed from the package to avoid confusion. (BZ#589578)

* The manual page for the remote quota server was found under rquotad(8), even though the actual command is "rpc.rquotad". To avoid possible confusion, the man page has also been made accessible under the more intuitive name "rpc.quotad(8)". (BZ#595729)

* The quotactl(2) manual page has been updated to refer to correct structure names. (BZ#656827)

In addition, this updated package provides the following enhancements:

* When a user reaches their quota limit, the warnquota utility can send a warning email to that user. This update enables support for LDAP so that warnquota can now be configured to obtain a user's email address from an LDAP directory instead of simply delivering the quota usage warning email to the local host. (BZ#459494, BZ#447780)

* The superuser is now able to use the '-r' (remote) option to edit quota limits on a remote system via remote procedure call (RPC) using the standard quota limit utilities. This enables quota limits on file systems which are mounted oven the network. (BZ#469753)

* The rquotad(8) man page referred to the rpc(3N) man page; however, the "3N" manual section is not provided. This update changes all "rpc" referencs to correctly refer to rpc(3). (BZ#474836)

* Quota limits for the ext4 file system are newly supported with this updated package. (BZ#500231)

Users are advised to upgrade to this updated quota package, which resolves these issues and adds these enhancements.

1.123. redhat-lsb

1.123.1. RHBA-2011:0084: bug fix update

Updated redhat-lsb packages that resolve several issues are now available.

The Linux Standards Base (LSB) is an attempt to develop a set of standards that will increase compatibility among Linux distributions. The redhat-lsb package provides utilities needed for LSB Compliant Applications. It also contains requirements that will ensure all components required by the LSB that are provided by Red Hat Linux are installed on the system.

These updated redhat-lsb packages provide fixes for the following bugs:

* Executing the lsb_start_daemon command caused an infinite loop as the daemon was not able to handle option flags properly. The update fixes this issue and output usage statement with option flags are parsed correctly. (BZ#503749)

* The redhat-lsb support package reported support for LSB version 3.2 and earlier versions. However, Red Hat Enterprise Linux 5 complies with LSB 4.0. This update fixes the package metadata and the package reports it supports LSB version 4.0. (BZ#570063)

All users of redhat-lsb are advised to upgrade to these updated packages, which resolve these issues.

1.124. redhat-release-notes

1.124.1. RHEA-2011:0131: enhancement update

An updated redhat-release-notes package is now available.

An updated version of the redhat-release-notes package is now available as part of ongoing support and maintenance of Red Hat Enterprise Linux 5.

This package contains the Release Notes for Red Hat Enterprise Linux 5.6

1.125. rgmanager

1.125.1. RHBA-2011:0134: bug fix and enhancement update

Updated rgmanager packages that provide a fix for a bug and add an enhancement are now available for Red Hat Enterprise Linux 5.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update addresses the following bugs:

* HA-LVM now resolves volume group names correctly (BZ#506587)

* HA-LVM can now protect from metadata changes by utilizing CLVM; logging has also been improved (BZ#509368 BZ#572311 BZ#583769 BZ#585229)

* The NetBIOS name stored in the automatically generated smb.conf files for services now has spaces removed (BZ#531098)

* It is now possible to stop rgmanager before CMAN finishes starting (BZ#545229)

* Failover domains are now documented in the rgmanager.8 man page (BZ#557562)

* SAPInstance and SAPDatabase resource agents no longer leave extraneous temporary files (BZ#565363)

* Rgmanager now retries the operation if it tries to relocate a service to another node before that node has reread the cluster configuration file (BZ#568126)

* fs.sh no longer sleeps unnecessarily if the file system is already unmounted during a stop operation (BZ#573705)

* Postgres-8 agent will now stop correctly if there are active clients connected (BZ#587735)

* Restricted failover domain boundaries are now honored when performing virtual machine migrations (BZ#592380)

* Temporary files created when using NFS lock code are now deleted (BZ#595455)

* Live migrations now use the correct interfaces when using migration mappings (BZ#596016)

* Errors from tomcat.sh have been addressed (BZ#591003)

* Previously, clusters failed to recover from a clurgmgrd crash if the reboot() system call failed. With this update, the rgmanager watchdog process now uses a more robust method to reboot the machine if the main rgmanager process crashes. (BZ#608397)

* clustat no longer returns 255 if rgmanager is not running (BZ#620730)

* If openais dies, rgmanager now halts services and exits (BZ#639961)

* Handling of CIFS mount points mounted from the netfs agents has been improved (BZ#640676)

* User-specified migration URIs work correctly with the fix for BZ#569016 (BZ#659477)

* The postgres-8 resource agent now correctly places IP netmask information into the configuration files it generates (BZ#614456)

This update also contains the following enhancements:

* Previously, vm.sh only checked the status of the VM itself, not the status of any services inside. With this update, administrators may now use a newly provided status check program which checks the availability of services within virtual machines running Red Hat Enterprise Virtualization Manager. Timeouts for starting and stopping virtual machines are now configurable in cluster.conf. The start timeout is based on the status check program. (BZ#583788)

* Independent subtrees may now be flagged as 'non-critical', meaning they may fail and have their components manually restarted without the entire service being affected (BZ#605733)

* The file system agent will now accept 'vxfs' as the file system type (BZ#531843)

* The file system agent will now accept 'ext4' as the file system type (BZ#636550)

* Users of Oracle database may now separate the listener from the database instance and have multiples of each resource type in a single cluster. This feature is offered as a Technical Preview and is not supported in production environments. (BZ#629208)

All users of Red Hat Resource Group Manager are advised to upgrade to these updated packages, which address these issues and add these enhancements.

1.125.2. RHBA-2010:0647: bug fix and enhancement update

Updated rgmanager packages that provide a fix for a bug and add an enhancement are now available for Red Hat Enterprise Linux 5.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update provides a fix for the following bug:

* previously, clusters failed to recover from clurgmgrd crash. With this update, the rgmanager watchdog process now uses a more robust method to reboot the machine if the main rgmanager process crashes. (BZ#609182)

This update contains also the following enhancement:

* previously, vm.sh only checked the status of the VM itself, not the status of any services inside. With this

update, administrators may now use a newly provided status check program which checks the availability of services within virtual machines running Red Hat Enterprise Virtualization Manager. Timeouts for starting and stopping virtual machines are now configurable in cluster.conf. The start timeout is based on the status check program. (BZ#594476)

All users of Red Hat Resource Group Manager are advised to upgrade to these updated packages, which address this issue and add this enhancement.

1.126. rhn-client-tools

1.126.1. RHBA-2010:0328: bug fix update

Updated rhn-client-tools packages that fix an entitlement issue are now available.

Red Hat Network Client Tools provide programs and libraries that allow your system to receive software updates from Red Hat Network (RHN).

This update includes a fix for an issue where XEN full-virt guests consumed regular entitlements instead of inherited entitlements provided by 'Virtualization' or 'Virtualization Platform' or the Flex Guest Entitlement channel (BZ#576637).

All users of rhn-client-tools are advised to upgrade to these updated packages, which resolve this issue.

1.127. rhnlib

1.127.1. RHBA-2011:0113: bug fix update

An updated rhnlib package that provides bug fixes is now available for Red Hat Enterprise Linux 5.

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

This update fixes the following bugs:

* Previously, the HTTP redirections were not handled correctly, which caused infinite loops.This update resolves this issue and redirections are now handled as expected. (BZ#583020)

* Previously, the nonblocking mode tried to use nonexistent fcntl constants. This update corrects this error and the constructor of the NonBlockingFile now behaves as expected. (BZ#583980)

* Previously, the registration of RHEL 4 systems failed if dmidecode returned BIOS information that contained non-XMLRPC-compliant characters. This update uses a XMLRPC-compliant set of characters. (BZ#618250)

All users of rhnlib are advised to upgrade to this updated package, which addresses these issues.

1.127.2. RHBA-2010:0790: and rhn-client-tools bug fix update

Updated rhn-client-tools and rhnlib packages, that fix a bug that caused the Red Hat Network and Red Hat Network Satellite registration to fail when the Desktop Management Interface (DMI) contained a control character, or when the hardware name contained a non-ASCII character, are now available.

The rhnlib and rhn-client-tools packages contain a collection of Python modules that are used by the Red Hat Network (RHN) software.

This update fixes the following bug:

* Previously, the presence of less commonly used characters from Latin-1 and UTF-8 character sets in the hardware name rendered the system unable to register to both Red Hat Network and Red Hat Network Satellite Server. This error has been fixed, and the system registration now works as expected. (BZ#639226)

All users of rhnlib and rhn-client-tools are advised to upgrade to these updated packages, which resolve this issue.

1.128. rng-utils

1.128.1. RHBA-2011:0116: bug fix update

Updated rng-utils packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The rng-utils package contains the random number generator user space utilities such as the rng daemon.

This update fixes the following bugs:

* Previously, rng-utils did not support the Trusted Platform Module (TPM). This update adds TPM rng support to use the random number generator inside the TPM. (BZ#461716)

* Previously, the release number of the rng-utils package was missing. This update resolves this issue and the release number is now available. (BZ#640725)

All users of rng-utils are advised to upgrade to this updated package, which resolves these issues.

1.129. rpm

1.129.1. RHBA-2011:0124: bug fix and enhancement update

Updated rpm packages that fix several bugs and add an enhancement are now available.

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

These updated rpm packages provide fixes for the following bugs:

* A memory leak in the communication between RPM and the Security-Enhanced Linux (SELinux) subsystem could have caused extensive memory consumption. In reported cases, this issue was triggered by running rhn_check when errata were scheduled to be applied. (BZ#627630)

* When installing the libgnome package, an error was displayed:

gconftool-2: command not found

This was due to a bug in dependency ordering on multilib systems, which caused failures of package scriptlets. With this update, the package dependencies are fixed and the problem no longer occurs. (BZ#641892)

In addition, these updated rpm packages provide the following enhancement:

* RPM accepts GPG keys saved on Windows operating system with Windows native line endings. (BZ#530212)

Users are advised to upgrade to these updated rpm packages, which resolve these issues and add this enhancement.

1.130. rsyslog

1.130. rsyslog

1.130.1. RHBA-2010:0980: bug fix update

Updated rsyslog packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. Rsyslog is compatible with stock sysklogd, and can be used as a drop-in replacement. It is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.

This update fixes the following bugs:

* Although the previous release of the rsyslog packages replaced rklogd, a daemon that provided kernel logging, with a loadable module, it did not enable this functionality in the configuration. Consequent to this, rsyslog did not log the kernel messages at all. With this update, the /etc/rsyslog.conf configuration file has been corrected to include the "$ModLoad imklog" directive, and the kernel messages are now logged as expected. (BZ#661147, BZ#661149)

* The previous rsyslog release introduced a new format of the message timestamps. However, certain utilities such as logwatch may have been unable to parse this new format properly. To prevent this, the "$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat" directive has been added to the /etc/rsyslog.conf configuration file to ensure that the old format is used by default. (BZ#661148)

All users of rsyslog are advised to upgrade to these updated packages, which resolve these issues. Note that if the /etc/rsyslog.conf configuration file contains local modifications, it is necessary to add these configuration directives manually.

1.131. s390utils

1.131.1. RHBA-2011:0081: bug fix and enhancement update

An updated s390utils package that fixes multiple bugs and adds two enhancements is now available.

The s390utils package contains utilities related to Linux for the IBM System z architecture.

This update fixes the following bugs:

* Previously, the online help for chsh documented "panic" as a valid state, although the command should not be used in this way. The online help could therefore have misled users. In this release, "panic" is no longer documented in the online help and does not therefore suggest that "panic" is a valid state for the chsh command. (BZ#561153)

* Previously, the online help for the zipl command omitted the --force option. Users were therefore not informed about this option unless they referred to additional documentation. The --force option for zipl is now documented in the online help, reducing the need for users to refer to additional documentation. (BZ#577321)

* Previously, due to faulty logic, non-zero values were returned even when particular utilities finished successfully. The affected utilities were:

>> lstape, using the -h option

>> ziomon, using the -h or -v options

>> ziorep, using the -h or -v options

The logic is corrected in this release, and these utilities now correctly return 0 when they complete successfully. (BZ#556916, BZ#556917, BZ#623252)

* When cmm_min is commented out in the cpuplugd configuration file, a value of -1 is assigned to cmm_min and cpuplugd should not run. Previously, cpuplugd did not test whether the value of cmm_min was less than 0 and therefore cpuplugd would run even with cmm_min set to -1. Cpuplugd now tests wether cmm_min is less than 0 and therefore does not run if cmm_min is commented out in the configuration file. (BZ#511379)

* On systems with more than 30 CPUs, NULL termination of a read buffer in cpuplugd could lead to a stack overwrite if a previous read had filled the whole buffer. Cpuplugd now reads no more than the maximum buffer size less 1 byte, and therefore avoids a stack overwrite on subsequent reads. (BZ#601850)

* Previously, cpu_min was set to 2 by default in the cpuplugd configuration file. This setting could produce expensive and unnecessary CPU signaling when a workload was spread across two under-worked CPUs. Cpu_min is now set to 1 by default and therefore avoids wastage of system resources in this way. (BZ#611789)

* Previously, cpuplugd only ran some of its tests for cmm_min and cmm_max values if it was started with the -V option or when cmm_pages was manually set to a value other than the default value. Therefore, cpuplugd did not always honor the cmm_min and cmm_max values specified in its configuration file. The tests for cmm_min and cmm_max are now independent of the -V option and the cmm_pages test and cpuplugd therefore enforces cmm_min and cmm_max correctly as specified in its configuration file. (BZ#611792)

* Previously, zipl did not handle situations when I/O channels were unresponsive; for example, when a subchannel showed a "busy" or "status pending" condition, or when a DASD showed an unexpected status during SSCH. In these situations, zipl would terminate IPL and place the system in disabled wait. Now, zipl retries unresponsive channels and can clear the status of channels when it encounters errors. IPL is therefore more likely to succeed. (BZ#537139, BZ#561155)

* Previously, lszfcp examined all ccw devices beneath $SYSFS/devices/css0/* when it generated its reports. As a result, the command was very slow on LPAR. Now, lsfcp focuses on zfcp devices -- those below $SYSFS/bus/ccw/drivers/zfcp/ -- and therefore produces its reports more quickly. (BZ#518669)

* Because the HDIO_GETGEO ioctl does not reliably report the correct number of cylinders on a DASD, dasdview and fdasd previously computed the number of cylinders from the device size. However, for unformatted devices the device size is zero and thus, the computation previously ended with a floating point exception. Now, dasdview and fdasd obtain the number of cylinders from the BIODASDINFO ioctl. Because dasdview and fdasd no longer compute the number of cylinders, the floating point exception no longer occurs when these commands are run on an unformatted device. (BZ#536846)

* Previously, lsreipl lacked a test for NSS as an IPL type. Therefore, when lsreipl was run on a booted NSS, lsreipl did not print any information. Lsreipl now includes a test for NSS and when lsreipl runs on an NSS, it prints the NSS name. (BZ#546298)

* Previosuly, ziomon did not initialize mp_arr correctly as an empty array. Therefore, the output of multipath -l could not be stored in mp_arr and when ziomon was run on a valid multipath device, it would report "The following devices do not seem to exist." Now, mp_arr is initialized as an empty array and ziomon detects multipath devices correctly. (BZ#533958)

* The code that ziomon previously used to parse the output of the multipath command could not handle all the characters that might appear in the output of the multipath command. Therefore, the number of LUNs reported by ziomon would not necessarily match the number of devices present. This release includes more robust parsing code for ziomon that reliably handles the output of the multipath command and therefore reports the correct number of LUNs. (BZ#577319)

* Previously, the progress_bar variable in vmconvert was not initialized correctly. Consequently, control characters appeared in the display of the progress bar. The untidy appearance of the progress bar might have misled users to think that there was a problem with the conversion process. With the variable correctly initialized, the control characters no longer appear and users can be confident that conversion is proceding

correctly. (BZ#567688)

* Previously, faulty logic in zipl meant that incorrect partition information might be written to zipl.conf when configuring the zfcp dump partition. With the logic corrected, the partition information written to zipl.conf is now reliable. (BZ#572312)

* Previously, faulty logic in qethconf matched only subchannels set to 0. Therefore, qethconf could not detect devices with subchannels set to values other than 0. With the logic corrected, qethconf now processes devices with subchannels set to values other than 0. (BZ#627690)

* Previously, iucvtty passeed the z/VM user ID of the originating guest virtual machine as an argument to the to the -h option of the login program. However, the -h option makes some login programs obtain an FQDN for the system to which [uw]tmp records should be written. The time taken to obtain this FQDN might exceed the time limit in which the login program waits for user input. Under these circumstances, users cannot log in. Iucvtty no longer specifies a user ID as an argument to login -h. The scenario in which users might not be able to log in is therefore avoided. (BZ#636203)

* The options set for the df command used by ziomon previously allowed long device names to be split across multiple lines, therefore preventing device names from being parsed properly. Ziomon now runs df with the -m option to keep device names on the one line. (BZ#575830)

* Previously, the path for ziorep_config was hard coded. However, because different distributions store these configuration files in different directories, ziomon might not always find the ziorep_config file. The path to ziorep_config is now read from PATH to ensure that ziomon can always find it. (BZ#576575)

* Previously, lsqeth did not clear its print array before it collected information for a qeth device. Therefore, when lsqeth printed information on a level2 device, it would sometimes include information from a previously displayed level3 device. Lsqeth now clears its print array before it collects information for a device and therefore avoids mixing information from more than one device. (BZ#588356)

As well, this update adds the following enhancements:

* The sclp_cpi sysfs interface allows a set of descriptive data called "Control Program Identification" (CPI) to be associated with an operating system instance (currently LPAR only). This information is not persistent and has to be set once per IPL. The s390utils package now allows users of IBM System z to specify the following CPI data:

> /sys/firmware/cpi/system_name -- arbitrary, user-specified system name as a string (for example, LPAR12)

> /sys/firmware/cpi/sysplex_name -- arbitrary, user-specified sysplex name as a string (for example, SYSPLEX1)

Additionally, certain CPI data is set automatically:

> /sys/firmware/cpi/system_type String: operating system type identifier as a string (set to "LINUX")

> /sys/firmware/cpi/system_level -- operating system version information as a hexadecimal value in the form 0x0000000000aabbcc, where aa=kernel version, bb=kernel patch level, and cc=kernel sublevel. For example, Linux kernel 2.6.26 is represented as 0x000000000002061a

(BZ#476011)

* ts-shell previously used a regular expression to limit group names to alphanumeric characters. This limitation was arbitrary, however, as any character that is not a whitespace should be usable as a group name. In this release, the regular expression is modified to allow any non- whitespace character in group names. (BZ#598636)

IBM System z users should install this updated package which addresses these issues and adds these enhancements.

1.132. samba3x

1.132.1. RHBA-2011:0054: bug fix and enhancement update

Updated samba3x packages that fix several bugs and add various enhancements are now available.

Samba is a suite of programs used by machines for authentication, and file and printer sharing.

These updated samba3x packages provide fixes for the following bugs:

* Users of trusted child domains were not authenticated correctly. As a result, some users of such domains did not appear as members of the parent domain even if the child domain allowed full inheriting from the parent domain. With this update, all users of a trusted child domain are authenticated successfully. (BZ#459842)

* The smb.conf manual page contained an ambiguous description of the 'default case' parameter. With this update, the description is updated and gives a clear description. (BZ#480405)

* Service principal names were not always created correctly and as a result, the system was attempting to acquire a service ticket using a wrong hostname. This caused the Kerberos authentication to fail. With this update, service principal names are created correctly. (BZ#560239)

* CUPS printing could fail in an Active Directory environment with Kerberos. With this update, regular users can print in such environment. (BZ#565774)

* When the 'normalize names' setting was enabled, the winbindd service could have failed after user authentication. With this update, authentication is successful. (BZ#565915)

* Packages requiring samba cannot recognize samba3x as an updated samba version. With this update, dependent packages recognize samba3x as the new samba version. (BZ#582756)

* Some remote users could not authenticate from workstations running Windows. This occurred, because the winbind service failed to authenticate to Windows Server 2008 using the "ntlm-server-1" ntm_auth protocol. With this update, the service works correctly. (BZ#590766)

* In the offline mode, the winbind service could have logged the following message: "Exceeding 200 client connections, no idle connection found." With this update, the error no longer occurs and you can set the client limit manually with the command 'winbind max clients'. (BZ#604081)

* The winbindd client limit was set to 200 and could not be changed. With this update, you can set the client limit manually with the command 'winbind max clients'. (BZ#641379)

* Previously, the samba3x package considered any samba package a conflicting package. With this update, samba3x checks for possible non-conflicting versions of the samba package. (BZ#609578)

* When using non-standard character sets, the command 'wbinfo' displayed user and group names with accented characters incorrectly. With this update, those names are displayed correctly with all supported character sets. (BZ#649708)

* Samba could have failed to connect to workstations running Windows 7 with Live Essentials installed due to a SPNEGO parsing failure. With this update, the connection succeeds. (BZ#651722)

In addition, these updated packages provide the following enhancements:

* Interoperation with Windows 7 and Windows Server 2008 was fixed. Secure channel connections to servers with Windows Server 2008 R2 and interdomain trusts with Windows Server 2008 domains are now supported. Previously also, due to errors in the secure channel to Windows 7 and Windows Server 2008 R2, the winbind daemon could corrupt the secure channel. With this update, this no longer occurs. (BZ#527997)

* In Red Hat Enterprise Linux 5.6, the samba3x package no longer provides the libtalloc library. The library is now provided in a separate source RPM. (BZ#596883)

* In Red Hat Enterprise Linux 5.6, the samba3x package no longer provides the libtdb library. The library is now provided in a separate source RPM. (BZ#596886)

Users are advised to upgrade to these updated samba3x packages, which resolve these issues and add these enhancements.

1.133. sblim

1.133.1. RHBA-2011:0090: bug fix and enhancement update

Updated sblim packages that fix various bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

SBLIM stands for Standards-Based Linux Instrumentation for Manageability. It consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

This update fixes the following bugs:

* Previously, running the reposdump utility from the sblim-gather package with no additional arguments failed with a segmentation fault. With this update, this error no longer occurs, and reposdump now works as expected. (BZ#565487)

* Due to a typing error in a post-installation script, a registration of a provider could fail. This error has been fixed, the typing error has been corrected, and the registration no longer fails. (BZ#633248)

* Prior to this update, the sfcbrepos utility used getopt as a dependency. However, the sblim-sfcb package that provides this utility could be installed before the util-linux package that includes getopt. Consequent to this, the following error message could appear in the install.log file:

/usr/bin/sfcbrepos: line 8: getopt: command not found

Since getopt is actually not required for the script to perform its work, its absence is no longer logged in the install.log file. (BZ#638555)

As well, this update adds the following enhancement:

* The sblim-gather packages have been updated to the latest upstream version. (BZ#605317)

All users are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

1.134. screen

1.134.1. RHBA-2011:0118: bug fix update

An updated screen package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The screen utility allows multiple logins on a single terminal. This is especially useful for users who telnet into a machine or are connected using a terminal that does not provide this functionality, but want to use more than one login.

This update fixes the following bugs:

* During a screen session, running certain commands such as "who am i", "w", or "logname" as a superuser did not produce the expected output or failed. This was caused by the fact that the package was built without the utempter support. With this update, the utility has been updated to include this support, and the above commands now work as expected. (BZ#474896)

* Due to several unrelated bugs, the screen utility did not pass the Common Criteria certification requirements. With this update, various parts of the underlying source code have been modified to target these issues. (BZ#644070)

All users of screen are advised to upgrade to this updated package, which resolves these issues.

1.135. scsi-target-utils

1.135.1. RHBA-2011:0071: bug fix update

An updated scsi-target-utils package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The scsi-target-utils package contains the daemon and tools to setup and monitor targets for The Small Computer System Interface (SCSI). Currently, iSCSI software targets are supported.

This update fixes the following bugs:

* Previously, targetadmin (tgtadm) encountered a segmentation fault and the target daemon (tgtd) could not shut down when users attempted to close an open connection with ongoing input/output. With this update, tgtadm shuts down the connection or exits gracefully with an error. (BZ#511002) * Previously, the target daemon (tgtd) failed under load. With this update, /var/log/messages contains no more errors and tgtd continues to respond. (BZ#513241)

* Previously, the target daemon (tgtd) and target admin (tgtadm) supported iSNS, but tgt-admin and tgtd.conf did not, which made the iSNS setup difficult. This update rebases the scsi-target-utils to the tgt-1.0.8 release which incorporated iSNS support in tgtd.conf configuration file parsing. (BZ#627053)

All users of scsi-target-utils are advised to upgrade to this updated package, which resolves these issues.

1.136. selinux-policy

1.136.1. RHBA-2011:0026: selinux-policy bug fix and enhancement update

Updated *selinux-policy* packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The *selinux-policy* packages contain the rules that govern how confined processes run on the system.

These updated packages provide fixes for the following bugs:

> **BZ#477103**
>
>> When a user upgraded from Red Hat Enterprise Linux 4 Workstation to 5 Server, the **OpenOffice.org** suite no longer worked correctly with SELinux. This was because the Red Hat Enterprise Linux version of **OpenOffice.org** is built using an incorrect library, and as a result,

SELinux prevented it from accessing any shared libraries, thus causing it to fail. With this update, the SELinux context has been updated to address this issue, and **OpenOffice.org** no longer fails.

BZ#514506

Prior to this update, SELinux prevented the `httpd` service from loading the `/usr/lib/libnnz11.so` (or `/usr/lib64/libnnz11.so` on a 64-bit system) library, which requires a text relocation. With this update, the SELinux context for this particular library has been changed from the default to `textrel_shlib_t`, so that the library can now be loaded as expected.

BZ#525859

When a **Samba** server, **smbd**, attempted to access the content of the `/var/lib/mysql/` directory, SELinux denied this access, and reported this event in the audit log. However, this access is not necessary for **Samba** to work properly. With this update, appropriate SELinux rules have been added to address this issue, and such access denial is no longer logged.

BZ#533500

Various SELinux policy issues were discovered by a customer during the configuration of Red Hat Enterprise Linux 5 hosts. These updated packages include several SELinux rules that resolve these issues.

BZ#551380

With SELinux running in the enforcing mode, the **Prelude Manager** was unable to connect to a **MySQL** server, and did not work properly. With this update, the SELinux rules have been updated to permit such connection, so that the **Prelude Manager** can access the server as expected.

BZ#570481

Previously, the `httpd_can_network_connect_db` boolean did not allow the `httpd` service to connect to **Microsoft SQL Server** (MSSQL). This error has been fixed, the boolean has been modified, and the relevant policy code has been added to define `mssql` port.

BZ#571319

When running SELinux in the enforcing mode, various **SpamAssassin** operations may have been denied, and multiple denial messages could be written to the `/var/log/messages` log file. This error has been fixed, and *selinux-policy* packages now contain updated SELinux rules, which permit appropriate operations.

BZ#575203

When SELinux was enabled, an attempt to generate a key pair from an init script using the following command failed with an error:

```
ssh-keygen -t rsa -f /root/.ssh/id_rsa -P ""
```

These updated *selinux-policy* packages provide corrected SELinux rules that allow the `ssh_keygen_t` domain to search the content of the `/root/.ssh/` directory, so that the key pair creation no longer fails.

BZ#576059

Due to an incorrect SELinux policy, an attempt to connect to VPN from **NetworkManager** could fail. With this update, the relevant policy has been corrected, and such connections can now be established as expected.

BZ#578187

A new version of *Berkeley Internet Name Domain* (**BIND**) required various additional changes in SELinux policy. These updated packages introduce the adjusted SELinux rules, and add the SELinux context for the `/var/named/data/` and `/var/named/slaves/` directories.

BZ#579105

When the `httpd` service was configured to use the `mod_auth_pam` module with `winbind`, users were denied access, even though the `allow_httpd_mod_auth_pam` and `httpd_can_network_connect` booleans were set to **on**. With this update, `allow_httpd_mod_auth_pam` has been corrected, and users are no longer denied access with this configuration.

BZ#579497

After upgrading to Red Hat Enterprise Linux 5.5, the **Xen hypervisor** was unable to auto-start domains linked to in the `/etc/xen/auto/` directory. This was caused by the default Red Hat Enterprise Linux 5.5 SELinux policy preventing the `xm` daemon from reading symbolic links in the `/etc/xen/auto/` directory, with the result that the `xm` daemon could not start virtual guests. These updated *selinux-policy* packages contain an updated SELinux policy that allows the `xm` daemon to correctly read the symbolic links in `/etc/xen/auto/`. The `xm` service is now able to auto-start virtual guests upon system startup.

BZ#579547

When SELinux was configured to run in the permissive mode, and the **snmpd** service attempted to access removable devices, this access was denied and relevant AVC messages were written to the audit log. Since this access is not necessary for **snmpd** to work properly, appropriate SELinux rules have been added to prevent these denials from being logged.

BZ#582613

Due to missing SELinux policy rules, **sVirt**, an integrated solution for securing Linux-based virtualization using SELinux, was not fully supported. With this update, relevant sVirt policy rules have been included in the *selinux-policy* packages to provide this support.

BZ#584447

Prior to this update, SELinux did not support **Piranha**, a set of miscellaneous tools to administer and configure the Linux Virtual server, as well as heartbeating and failover components. Consequent to this, users of **Piranha** with SELinux running in the enforcing mode could encounter various issues. With this update, a new SELinux policy for these tools have been added, resolving these issues.

BZ#588902

Due to an error in the SELinux rules, when SELinux was running in the enforcing mode, a dead cluster node could not be fenced, rendering **rgmanager** unable to migrate a resource. To address this issue, relevant SELinux rules have been updated, and such cluster node is now fenced as expected, allowing **rgmanager** to migrate the resource.

BZ#591975

During an **Openswan** connection, SELinux did not allow the access to the socket, and relevant AVC messages were written to the audit log. With this update, a patch has been applied to add required SELinux rules, so that SELinux no longer denies this access.

BZ#592752

Previously, SELinux prevented the **Postfix** mail transfer agent from creating a *chroot* environment. This issue has been resolved, and relevant rules have been added to permit this operation.

BZ#592805

Due to an error in SELinux rules, the **vsftpd** daemon may have been unable to write to a file or create a directory inside **~/public_html/**, reporting the following error message:

```
550 Create directory operation failed.
```

This update fixes the SELinux rules, and **vsftpd** now works as expected.

BZ#593139

With SELinux running in the enforcing mode, an attempt to run the **rsyslogd** service with GnuTLS modules enabled could fail with the following error message:

```
Starting system logger: Fatal: no entropy gathering module detected
```

With this update, relevant rules have been modified to resolve this issue, and **rsyslogd** no longer fails to run.

BZ#598646

When a system was configured to use **winbind** for authentication using the **winbind refresh tickets = true** configuration option, several issues may have occurred, preventing this configuration from working properly. This update fixes the SELinux rules for **winbind**, so that the above configuration works as expected.

BZ#612823

When SELinux was running in the enforcing mode, the **snmpd** daemon was incorrectly denied access to the **/var/net-snmp/snmpd.conf** configuration file. With this update, the SELinux context for the **/var/net-snmp/** directory has been corrected.

BZ#613551

Recently, the **OpenAIS** Standards-Based Cluster Framework, an open implementation of the *Application Interface Specification* (AIS), started using POSIX semaphores instead of the SysV semaphores. With this update, relevant SELinux rules have been adjusted to reflect this change.

BZ#614796

With SELinux running in the enforcing mode, an attempt to start the **qpidd** service when the **aisexec** was already running failed, and the following error message was written to the **qpidd.log**:

```
Unexpected error: Timed out waiting for daemon (If store recovery is
in progress, use longer wait time)
```

This was caused by SELinux incorrectly denying **qpidd** the access to OpenAIS. This update corrects the SELinux policy, resolving this issue.

BZ#616793

Previously, the **/etc/oddjobd.conf** configuration file for the **oddjobd** service was not portable between different architectures. To resolve this issue, the proper SELinux context for the **oddjob** libraries has been added, so that the configuration file can be ported to different architectures as expected.

BZ#617763

Prior to this update, the **xm_t** domain was not allowed to search directories with the **autofs_t** security context. Consequent to this, virtual machines could not be stored on automatically mounted file systems. With this update, the SELinux rules have been adjusted to permit such search, so that the virtual machines can now be stored on an automatically mounted file system as expected.

BZ#621057

The SELinux policy for **rpc.quotad** has been adjusted in order to make it work properly.

BZ#621885

Since certain Oracle libraries require a text relocation, the SELinux context for libraries in the **/usr/lib/oracle/** directory has been changed to **textrel_shlib_t**.

BZ#625498

The **ftpd_selinux** manual page describes how to allow **FTP** servers to read from and write to the **/var/ftp/incoming/** directory. However, these instructions contained an error, and running the **restorecon** command with the recommended command line options did not produce the expected results. With this update, the manual page has been corrected, and no longer contains misleading information.

BZ#626858

The SELinux policy has been updated to reflect the latest changes in the *hplip* (Hewlett-Packard Linux Imaging and Printing Project) packages.

BZ#633705

With SELinux running in the enforcing mode, using the **postfix set-permissions** command failed with the following error message:

```
/etc/postfix/postfix-script: line 263: /etc/postfix/post-install:
Permission denied
```

With this update, the **postfix_domtrans_master(unconfined_t)** transition has been removed, and the above command no longer fails to run.

BZ#633901

Due to an incorrect SELinux policy, the **aisexec** service was unable to use shared memory segments as an unprivileged user. This error has been fixed, the relevant SELinux policy has been corrected, and **aisexec** now works as expected.

BZ#637843

Prior to this update, several messages were written to the audit log when **Sendmail** leaked file descriptors. To prevent this, the SELinux policy has been corrected, and these events are no longer logged.

BZ#639259

Due to an error in a SELinux policy, messages similar to the following could be written to the **/var/log/messages** log file:

```
restorecon: /etc/selinux/targeted/contexts/files/file_contexts:
Multiple same specifications for
/etc/NetworkManager/dispatcher\.d(/.*).
```

These updated packages correct this error, and the above message no longer appears in the log.

BZ#641872

All *selinux-policy* subpackages now provide versioned *selinux-policy-base*.

BZ#643824

When using SELinux in the enforcing mode, the **Postfix** services were unable to retrieve information about the network state. With this update, the SELinux rules have been updated to allow the required access.

BZ#644276

With SELinux running in the enforcing mode, using a pass-through PCI device with sVirt rendered **KVM** (Kernel-based Virtual Machine) unable to start a virtual machine. With this update, the **virt_use_sysfs** boolean has been updated to resolve this issue, and virtual machines no longer fail to start.

BZ#644333

Under certain circumstances, SELinux could report that **Internet Protocol Security** (IPsec) management tools require read access to the content of a user's home directory. This error no longer occurs, and an appropriate SELinux rule has been added to resolve this issue.

BZ#646731

Due to an error in an SELinux policy, the **system-config-printer** utility could terminate unexpectedly with the following message written to the standard error:

```
ImportError: /usr/lib64/python2.4/site-packages/cups.so: undefined
symbol: _cupsAdminGetServerSettings
```

To resolve this issue, relevant SELinux rules have been corrected, so that the **system-config-printer** utility no longer crashes.

BZ#646801

By setting the **fail_action** option to **halt**, the **audisp-remote** plug-in can be configured to shut down the system when an error is reported. However, consequent to an error in the SELinux rules, when a network connection failed, SELinux incorrectly denied the **halt** action. With this update, the SELinux rules have been corrected, and **audisp-remote** is now allowed to shut down the system as expected.

BZ#649492

With SELinux running in the enforcing mode, the **smbcontrol** utility was unable to ping **Samba** services such as **smbd**, **nmbd**, or **winbindd**. This error no longer occurs, and **smbcontrol** now works as expected.

BZ#649691

Prior to this update, performing certain **iscsiadm** actions could cause AVC messages to be written to the audit log. With this update, the SELinux rules have been corrected to address this issue.

BZ#650141

Previously, SELinux prevented the **winbindd** service from connecting to MS-RPC. This has been fixed, appropriate SELinux rules have been added, and **winbindd** is now allowed to establish a connection with MS-RPC as expected.

BZ#652074

Under certain circumstances, a system may have been unable to automatically load certain modules at a boot time. When this happened, network interfaces may not have been started during the boot, and had to be started manually. With this update, several rules have been added to the SELinux MLS (Multilevel Security) policy to allow the use of shared memory, resolving this issue.

BZ#652199

With SELinux enabled, the **winbindd** service was unable to connect to the port **135**. This error has been fixed, and relevant SELinux rules have been added to allow such connections.

BZ#652644

Due to an error in the SELinux policy, SELinux prevented the **qemu-kvm** command from accessing **HugeTLBfs** devices. This update corrects the SELinux rules to allow this access.

BZ#652660

Previously, running the **sa1** command from the *sysstat* package caused various denial messages to be written in the audit log. This update addresses this issue, and the above command now works as expected.

BZ#656255

With SELinux enabled, an attempt to run the **run_init** command in single user mode failed with the following error message:

```
sh: /usr/sbin/run_init: permission denied
```

This update adds SELinux rules to address this issue, and the **run_init** command no longer fails to run.

BZ#656290

When SELinux was running in the enforcing mode, an SELinux MLS policy did not allow the **udevmonitor** to create a socket. As a result, an attempt to run this command in single user mode failed with the following error message:

```
error getting socket: Permission denied
```

With this update, the SELinux policy has been fixed to permit the creation of such socket, and **udevmonitor** can now be run as expected.

BZ#656809

Under certain circumstances, using SELinux with the MLS policy in the permissive mode could cause the following messages to appear at a boot time:

```
/dev/mapper/control: open failed: Permission denied
Failure to communicate with kernel device-mapper driver.
```

With this update, appropriate SELinux rules have been added to address this issue, and the system now boots without these errors.

BZ#657262

Previously, the SELinux MLS policy prevented the **udevinfo** command from producing the expected results. This update fixes the relevant policy, so that the command no longer fails.

BZ#657268

Due to the SELinux MLS policy, the **udevcontrol** command failed to run, and a denial message was written to the audit log. With this update, this issue has been resolved, and SELinux no longer prevents **udevcontrol** from running.

BZ#657271

With the SELinux MLS policy enabled, running the **semodule** command could cause various AVC messages to be written to the log. This error has been fixed, and **semodule** no longer causes such messages to appear.

BZ#657365

Due to an error in the SELinux MLS policy, running the **run_init service cpuspeed start** command in single user mode caused an AVC message to appear in the audit log. With this update, the SELinux MLS policy has been corrected, so that the above command works as expected.

BZ#658145

Due to an error in an SELinux policy, pre-installation and post-installation scripts in RPM packages were unable to write to a pipe. This has been fixed, and SELinux no longer prevents these scripts from performing their work.

BZ#658436

When the **snmpd** service attempted to change the *user identifier* (UID) or *group identifier* (GID), SELinux denied this action, and an appropriate message was written to the audit log. These updated *selinux-policy* packages provide corrected SELinux rules that permit this operation, and SELinux no longer prevents **snmpd** from changing the user and group identifier.

BZ#659372

Previously, running the **vbetool** utility could cause AVC messages to be written to the audit log. With this update, the SELinux policy has been updated to address this issue, and such messages no longer appear.

BZ#659777

An updated SELinux rule for the **consoletype** command has been backported from Red Hat Enterprise Linux 6.

BZ#661368

Prior to this update, the SELinux MLS policy prevented **modprobe** from reading an SHM (shared memory) object. This update corrects the SELinux policy, and **modprobe** now works as expected.

As well, these updated packages add the following enhancement:

> **BZ#637182**
>
>> The **httpd_setrlimit** boolean has been added to allow the **httpd** service to change its maximum limit of the file descriptors.

All users of *selinux-policy* are advised to upgrade to these updated packages, which resolve these issues, and add this enhancement.

1.136.2. RHBA-2010:0832: bug fix update

Updated selinux-policy packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

This update fixes the following bug:

* Due to incorrect SELinux policy, cmirror was unable to start properly, and as a result, cluster mirrors could not be started at all. This error has been fixed, and SELinux no longer prevents cluster mirrors from being started. (BZ#644821)

All users of selinux-policy are advised to upgrade to these updated packages, which resolve this issue.

1.136.3. RHBA-2010:0561: bug fix update

Updated selinux-policy packages that resolve an issue are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

These updated selinux-policy packages fix the following bug:

* after upgrading to Red Hat Enterprise Linux 5.5, the Xen hypervisor was unable to auto-start domains linked to in the /etc/xen/auto/ directory. This was caused by the default Red Hat Enterprise Linux 5.5 SELinux policy preventing the xm daemon from reading the symlinks in the /etc/xen/auto directory, with the result that the xm daemon could not start the virtual guests. These updated selinux-policy packages contain an updated SELinux policy that allows the xm daemon to correctly read the symbolic links in /etc/xen/auto. The xm service is now able to auto-start virtual guests upon system startup. (BZ#617169)

All users of selinux-policy are advised to upgrade to these updated packages, which resolve this issue.

1.137. sg3_utils

1.137.1. RHBA-2011:0093: bug fix update

Updated sq3_utils packages that resolve an issue are now available.

The sg3_utils package contains a collection of tools for SCSI devices that use the Linux SCSI generic (sg) interface. It includes utilities for database copying based on 'dd' syntax and semantics (the sg_dd, sgp_dd and sgm_dd commands), INQUIRY data checking and associated pages (sg_inq), mode and log page checking (sg_modes and sg_logs), disk spinning (sg_start) and self-tests (sg_senddiag), as well as other utilities. It also contains the rescan-scsi-bus.sh script.

These updated sq3_utils packages fix the following bug:

* If no device existed with a Logical Unit Number (LUN) of "0", then the rescan-scsi-bus.sh shell script failed to detect any other devices as well.

In a separate issue, the rescan-scsi-bus.sh shell script did not always detect all LUNs due to a timing issue while checking the device's online status.

With this update, the rescan-scsi-bus.sh script detects all devices even if there is no device with LUN of "0", and the "rescan" command successfully receives the device's online status. (BZ#529654)

All users of sq3_utils are advised to upgrade to these updated packages, which resolve this issue.

1.138. shadow-utils

1.138.1. RHBA-2011:0094: bug fix update

An updated shadow-utils package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The shadow-utils package includes programs for converting UNIX password files to the shadow password format, as well as tools for managing user and group accounts.

This update fixes the following bugs:

* Previously, extended Attributes and extended access control lists (ACLs) on files and directories under /etc/skel were dropped when a new user was created. With this update, the files are successfully copied and the extended ACL's are preserved. (BZ#513055)

* Previously, the description of the option -K in the Japanese man page of groupadd could cause confusion. With this update, the content of the man page is corrected and the description is clear and logical. (BZ#537011)

* Previously, the maximum number of character for username and groupname was limited to 31. With this update Maximum size of username and groupname is set to 32 characters. (BZ#586861)

* Previously, the command "faillog" failed to print the User Identification (UID) when the faillog file was empty. This update prints the UID of the users who had a login failure and no more underflow occurs. (BZ#603692)

* Previously, the command "faillog" printed the faillog records of all users when it was run without arguments. With this update, the log prints only the records of the users who had a login failure, as described in the manual page. (BZ#619713)

All users of shadow-utils are advised to upgrade to this updated package, which resolves these issues.

1.139. sox

1.139.1. RHBA-2010:0916: bug fix update

An updated sox package that fixes a bug is now available for Red Hat Enterprise Linux 5.

SoX (Sound eXchange) is a sound file format converter that allows a user to convert between many different digitized sound formats, as well as to use simple sound manipulation functions, including sound effects.

This update fixes the following bug:

* Previously, an attempt to convert an Audio Interchange File Format (AIFF) file that contained the MARK chunk may have failed with the following error:

sox: Failed reading file.aiff: AIFF: no sound data on input file

With this update, the underlying source code has been modified to target this issue, and such files are now converted as expected. (BZ#651404)

All users of sox are advised to upgrade to this updated package, which resolves this issue.

1.140. spice-usb-share

1.140.1. RHBA-2011:0122: and kspiceusb-kmod bug fix update (was spice-usb-redirector)

Updated spice-usb-share and kspiceusb-kmod packages that fix various bugs and replace spice-usb-redirector, are now available.

spice-usb-share is a non-free USB drivers package which is used to share USB devices with a guest operating system connected via SPICE. kspiceusb-kmod provides the kernel module that helps enable spice-usb-share functionality.

The spice-usb-share and kspiceusb-kmod packages provide USB-over-network capabilities when working with a SPICE client. The package include 3 components: a kernel module, a service daemon to handle the devices and a controller utility which intermediates between SPICE and the USB service daemon.

Users that are using SPICE to access a remote virtual machine (VM) managed by Red Hat Enterprise Virtualization Manager and wanting their client machine operating systems to make USB devices available to guest operating systems should install/update these new packages.

1.141. strace

1.141.1. RHBA-2010:0453: bug fix update

An updated strace package that fixes a bug is now available.

The strace program intercepts and records the system calls called and received by a running process. It can print a record of each system call, its arguments and its return value.

This update also fixes the following bug:

* when detaching from a process, a misinterpreted status caused strace to always leave the process being traced in a stopped state. With this update, the process is left in the correct state after detaching. (BZ#594616)

Users are advised to upgrade to this updated strace package, which resolves this issue.

1.142. subversion

1.142.1. RHEA-2011:0039: enhancement update

Enhanced subversion packages are now available.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes.

These updated subversion packages add the following enhancements:

* The Subversion package has been upgraded to version 1.6.11 and supports now merge tracking and interactive conflict resolution. (BZ#497036, BZ#488810)

* A SysV init script for the svnserve command is available. (BZ#564073)

Users of subversion are advised to upgrade to these updated packages, which add these enhancements.

1.143. sudo

1.143.1. RHBA-2011:0079: bug fix update

An updated sudo package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

This update fixes the following bugs:

* Due to an incorrect definition of a lexical analyzer rule, using a negated user-specific "Defaults" directive failed with a parse error. With this update, such directives are now parsed as expected. (BZ#580438)

* Prior to this update, the manual page for sudoers.ldap was not installed, even though it contains important information on how to set up an LDAP sudoers source and other documents refer to it. This error no longer occurs, and the manual page is now properly included in the package. Additionally, various POD files have been removed from the package, as they are required for build purposes only. (BZ#583644)

* A comment regarding the "visiblepw" option of the "Defaults" directive has been added to the default /etc/sudoers file to clarify its usage. (BZ#583911)

* A typing error in the sudoers manual page has been corrected. (BZ#602022)

* When the /etc/sudoers file contained entries with multiple hosts, running the "sudo -l" command incorrectly reported that a certain user does not have permissions to use sudo on the system. With this update, the underlying source code has been modified to target this issue, and running the "sudo -l" command now produces the correct output. (BZ#603819)

* Due to an incorrect handling of mixed case in user and group names, fetching the information from Active Directory may have failed with a cache error. With this update, an upstream patch has been applied to target this issue, and sudo now works as expected. (BZ#615179)

All users of sudo are advised to upgrade to this updated package, which resolves these issues.

1.143.2. RHBA-2010:0777: bug fix update

An updated sudo package that fixes a bug is now available.

The sudo (super user do) utility allows system administrators to give certain users the ability to run commands as root with logging.

This updated sudo package fixes the following bug:

* Previously, 'sudo' returned a 'cache error' whenever a mixed cased user name or a mixed cased group name was fetched from an Active Directory via LDAP (Lightweight Directory Access Protocol) or QAS (Quest Authentication Services). With this update, the case of a user name or a group name is ignored and 'sudo' no longer returns a 'cache error'. (BZ#632235)

All users of sudo are advised to upgrade to this updated package, which resolves this issue.

1.144. sysstat

1.144.1. RHBA-2010:0552: bug fix and enhancement update

An updated sysstat package that provides several bug fixes and adds an enhancement is now available.

The sysstat package provides the sar and iostat commands. These commands enable system monitoring of disk, network, and other I/O activity.

This updated sysstat package provide fixes for the following bugs:

* sar data set the maximum number of days in log files too high, which appended data from the previous month to the next one instead of replacing it. This updated package resolves this issue and sets the maximum to 25 days. (BZ#609819)

* sysstat's programs such as mpstat wrongly interpreted the /proc data and showed information about one fictive cpu. This update resolves this issue and these fictive data are not displayed anymore. (BZ#609821)

* the "sar -d " command used to output invalid data. This issue is resolved and the updated package recognizes disk reregistration and disk statistic overflow better. Now, only relevant data is displayed. (BZ#609824)

* on ia64 machines, the output of sar -I ALL/XALL wrongly showed information about interruptions. This issue is resolved and the updated package does not use sar -I for this type of architecture. (BZ#609826)

* iostat -n used invalid data to create the statistic. The updated package resolves this issue and the data source is now changed. Additionally, one new column has been added. (BZ#609991)

* though function write() executed successful, the return value wasn't equal to the supposed write size. So, p_write_error() ran and the following message appeared: "Cannot write data to system activity file: Success". In this updated package, the sadc utility successfully writes the remaining input, thus resolving this issue. (BZ#609994)

All sysstat users are advised to upgrade to this updated package, which resolves these issues.

1.145. system-config-cluster

1.145.1. RHBA-2011:0101: bug fix update

An updated system-config-cluster package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The system-config-cluster package contains a utility that allows the management of cluster configuration in a graphical setting.

This update fixes the following bugs:

* Previously, system-config-cluster failed to parse logging tags and related children because the cluster.ng file did not contain those tags. This update adds the tags for the logger parent and its children. (BZ#520886)

* Previously, system-config-cluster did not populate the ip correctly when editing the ip resource with no subnet mask. With this update, the ip is populated correctly. (BZ#546747)

* Previously, XFS as a filesystem resource option was not available in system-config-cluster. This update uses the existing support for XFS in /usr/share/cluster/fs.sh to add xfs as a fs option for existing and already configured xfs fs resources. (BZ#632599)

All users of the system-config-cluster utility are advised to upgrade to this updated package, which resolves these issues.

1.145.2. RHBA-2010:0747: bug fix update

An updated system-config-cluster package that fixes a bug is now available.

The system-config-cluster package contains a utility that allows management of cluster configuration in a graphical setting.

This updated system-config-cluster package fixes the following bug:

* The cluster configuration schema was out-of-date and did not represent several logging-related constructs, which could have caused validation failures with certain cluster configurations. The cluster configuration schema, cluster.ng, has been updated so that all correct configurations validate successfully. (BZ#629083)

All users of system-config-cluster are advised to upgrade to this updated package, which resolves this issue.

1.146. system-config-lvm

1.146.1. RHBA-2011:0103: bug fix update

An updated system-config-lvm package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

system-config-lvm is a utility for graphically configuring logical volumes.

This update fixes the following bugs:

* Prior to this update, using the system-config-lvm utility to edit the properties of a logical volume may have changed the order of lines in the /etc/fstab file. To prevent potential errors upon a subsequent system startup, system-config-lvm has been updated to preserve the original line order. (BZ#548057)

* Under certain circumstances, an attempt to remove a snapshot of a logical volume may have failed with an error. With this update, an upstream patch to target this issue has been applied, and such snapshots can now be removed as expected. (BZ#567464)

* Due to an error in the implementation, deactivating an existing snapshot of a logical volume rendered the system-config-lvm utility unable to start. This error no longer occurs, and unused snapshots no longer prevent the utility from starting. (BZ#569498)

* Due to the use of incorrect utilities, system-config-lvm was unable to resize ext4 partitions. This error has been fixed, and system-config-lvm now correctly uses the ext4 utilities. (BZ#571995)

* When running a non-English translation of the application, the initial window was not completely translated and still contained English messages. With this update, the underlying source code has been corrected to respect the localization settings, and all messages are now translated as expected. (BZ#578827)

* Previously, extending a logical volume may have caused the relevant line in the /etc/fstab file to be duplicated. This no longer occurs, and /etc/fstab is now processed as expected. (BZ#586553)

* Prior to this update, an attempt to adjust the size of a logical volume failed, and a traceback was written to standard error. With this update, the size changes are applied, and relevant volumes are correctly remounted. (BZ#586555)

Users of system-config-lvm are advised to upgrade to this updated package, which resolves these issues.

1.147. system-config-securitylevel

1.147.1. RHBA-2010:0686: bug fix update

Updated system-config-securitylevel packages that fix several bugs are now available for Red Hat Enterprise

Linux 5.

system-config-securitylevel is a graphical program for configuring firewall and SELinux settings.

These updated packages provide fixes for the following bugs:

* previously, the focus of the add port dialog was not on the port entry if the dialog was used before. This update places the focus on the port entry every time gets opened. (BZ#352401)

* previously, adding ports entries could result in loss of the entries if there was a predefined service also using this port but with a different protocol. This update solves this issue. (BZ#474100)

* disabling a running firewall resulted in no firewall settings for IPv4, but the IPv6 firewall was still active. This update solves this issue. (BZ#526477)

All users are advised to upgrade to these updated packages, which resolve these issues.

1.148. systemtap

1.148.1. RHEA-2011-0037: systemtap bug fix and enhancement update

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

This update re-bases SystemTap to upstream version 1.3 (BZ#606726). This re-base applies several upstream enhancements, highlights of which include:

- A new integrated compile-server client is now available as part of **stap**.

- A new option, **--ldd**, automatically adds any additional shared libraries needed by probed or "**-d**"-listed userspace binaries to the **-d** list; this enables symbolic backtracing through them. Similarly, the new **--all-modules** option automatically adds any currently loaded kernel modules (listed in **/proc/modules**) to the **-d** list.

- By default the **systemtap-runtime** RPM builds now includes a shared library: **staplog.so**. This library allows **crash** to extract systemtap data from a **vmcore** image.

- This re-base also introduces backward-compatibility flags and a deprecation policy, which is useful in preventing future tapset/language changes from breaking valid scripts.

- The **<sys/sdt.h>** user-space markers no longer default to an implicit **MARKER_NAME_ENABLED()** semaphore check for each marker. To check for enabled markers use a **.d** declaration file, then:

```
if (MARKER_NAME_ENABLED()) MARKER_NAME()
```

- A new **stap** option, **-G VAR=VALUE**, allows users to override global variables by passing the settings to **staprun** as module options.

- Iterating with **foreach** can now explicitly save the value for the loop.

- A new operator, **@entry**, is available for automatically saving an expression at entry time for use in a **.return** probe.

This update also applies the following fixes:

❧ The **stap-prep** script, packaged with SystemTap, requires **yumdownloader** (supplied by **yum-utils**). However, **yum-utils** is not a dependency of SystemTap. With this update, **yum-utils** is now a dependency of SystemTap. ([BZ#513672](#))

❧ Whenever SystemTap invoked **useradd**, it did so without specifying a UID; as such, any such invocations could result in a 'BAD level' warning. With this update, **stap-server** checks the existence of a system UID/GID before invoking an **adduser**/**groupadd** command. A 155:155 static UID:GID pair will then be assigned to the **stap-server** user without UID/GID reservation. In the rare case that such a user already exists on the system, dynamic UID/GID allocation will be used. ([BZ#555808](#))

❧ When loading a module, **stap** executes **stapio** to handle interactions. A bug in **runtime/staprun/mainloop.c** made it possible for **stapio** to fail in executing a module control file even after successfully opening it. When this occurred, **stapio** returned an "ERROR: unexpected EOF" when loading/unloading a kernel module concurrently. This update applies an upstream patch to **runtime/staprun/mainloop.c** that instructs **stapio** to quit (instead of retrying) when a read error occurs, avoiding a loop. ([BZ#557165](#))

❧ When running **rpm -V systemtap systemtap-server**, TPS reported two verification failures: **systemtap-server.ppc64: /var/log/stap-server.log .M...UG. [tps:B]** and **systemtap.ppc64: /usr/share/systemtap/runtime/uprobes .M....G. [tps:B]**. This update applies an upstream patch that corrects this. ([BZ#559633](#))

❧ The Red Hat Enterprise Linux 5.4 version of SystemTap contained a **stap-prep** script that is missing in 5.5. This update returns the **stap-prep** script. ([BZ#573031](#))

❧ When running multiple **stap** engines simultaneously, it was possible for SystemTap to unload the **stap** module before running all **utrace** callback handlers. This could result in the kernel calling code in an unloaded module, which would result in a crash. To prevent this from occurring, this update patches **runtime/itrace.c** and **runtime/task_finder.c** accordingly, adding a loop that checks for running handlers. SystemTap will now only unload a module when it is safe to do so. ([BZ#602706](#))

❧ When running **service systemtap restart** on a previously stopped script, the script remained halted instead of restarting. This was because the SystemTap initscript incorrectly defined the **SCRIPTS** variable. With this update, SystemTap makes local copies of the **$SCRIPTS** global variable. This update also adds **force-reload**, **reload**, **condrestart**, and **try-restart** commands. ([BZ#607232](#))

❧ The **prelink** utility is no longer a SystemTap dependency on Itanium. This dependency was added in previous releases for specific SystemTap test cases. ([BZ#629190](#))

❧ The **-I** option when running **stap** terminated abnormally with a segmentation fault because of the string literal at the end of the file. This update provides a workaround by adding a semi-colin (;) after the string literal, and a fix in **parse.cxx** that only inspets the next token if there is one. ([BZ#648420](#))

The following fixes were previously released in a separate, asynchronous errata:

❧ Due to a string copy being used instead of a formatted string copy, the argstring of the socketpair system call had a wrong "UNKNOWN VALUE". This issue is now resolved. ([BZ#560720](#))

❧ Although the kernel in Red Hat Enterprise Linux 5.5 for the Itanium architecture introduced a new pipe system call handler, **sys_ia64_pipe**, the function was not added to the SystemTap tapset. As a result, probing the system call from the script via **probe syscall.pipe** did not succeed. This error has been fixed, the new function has been added to the tapset, and the pipe system call should now be probed correctly. ([BZ#568032](#))

❧ Previously, a change in register contents (such as **$return**) on the Itanium architecture caused a crash due to a flaw in the way the values in the memory were set. Now, a change in register contents no longer results in a crash. ([BZ#598615](#))

For a more detailed list of upstream enhancements and bug fixes applied by the re-base, refer to the following link:

http://sourceware.org/ml/systemtap/2010-q3/msg00098.html

All SystemTap users are advised to apply this update.

1.148.2. RHBA-2010:0608: bug fix update

Updated systemtap packages that resolve two bugs are now available for Red Hat Enterprise Linux 5.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

This update resolves the following bugs:

* due to a string copy being used instead of a formatted string copy, the argstring of the socketpair system call had a wrong "UNKNOWN VALUE". This issue is now resolved. (BZ#617099)

* previously, a change in register contents (such as $return) on Itanium caused a crash due to a flaw in the way the values in the memory were set. Now, no crash happens when register contents change. (BZ#617100)

All SystemTap users are advised to upgrade to these updated packages, which fix these bugs.

1.148.3. RHBA-2010:0525: bug fix update

Updated systemtap packages that fix a bug are now available.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

This update fixes the following bug:

* although the kernel in Red Hat Enterprise Linux 5.5 for the Itanium architecture introduced a new pipe system call handler, "sys_ia64_pipe", the function was not added to the SystemTap tapset. As a result, probing the system call from the script via "probe syscall.pipe" did not succeed. This error has been fixed, the new function has been added to the tapset, and the pipe system call should now be probed correctly. (BZ#604022)

Affected SystemTap users should upgrade to these updated packages, which resolve this issue.

1.149. tcsh

1.149.1. RHBA-2010:0823: bug fix update

An updated tcsh package that fixes a bugs is now available.

Tcsh is an enhanced and compatible version of the C shell (csh). It is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

This updated tcsh package fixes the following bugs:

* Previously, under certain circumstances, a null pointer may have been incorrectly dereferenced, causing the tcsh shell to terminate unexpectedly. With this update, the pointer is now checked properly and tcsh no longer crashes. (#631815)

* Previously, when command substitution with backquotes was used, extra fork() was performed. With this update, only one fork() is performed. (#640251)

* Previously, if printexitvalue was set, tcsh returns the exit code as part of the command output, rendering the output unusable. With this update, output of command is correct. (#640252)

All users of tcsh are advised to upgrade to this updated package, which resolves these issues.

1.150. tetex

1.150.1. RHBA-2010:0816: bug fix update

Updated teTeX packages that fix a bug are now available.

TeTeX is an implementation of TeX. TeX takes a text file and a set of formatting commands as input, and creates a typesetter-independent DeVice Independent (DVI) file as output.

This update fixes the following bug:

* Previously, attempting to convert an Encapsulated PostScript (EPS) file containing a BoundingBox caused the epstopdf utility to fail with an unrecoverable error. This error no longer occurs, and such files are now converted as expected. (BZ#635666)

All users are advised to upgrade to these updated packages, which resolve this issue.

1.151. thunderbird

1.151.1. RHBA-2010:0900: bug fix update

An updated thunderbird package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Mozilla Thunderbird is a standalone mail and newsgroup client.

This updated package fixes the following bug:

* Previously, clicking the "Load" button in the Device Manager configuration dialog did not not open an appropriate dialog window, rendering user unable to load a PKCS#11 (Public-Key Cryptography Standard) device. This error has been fixed, and PKCS#11 devices can now be loaded as expected. (BZ#649251)

Users of Thunderbird are advised to upgrade to this updated package, which resolves this issue.

1.152. tmpwatch

1.152.1. RHBA-2010:0619: bug fix update

An updated tmpwatch package that fixes various bugs is now available.

The tmpwatch utility recursively searches through specified directories and removes files which have not been accessed in a specified period of time. tmpwatch is usually used to clean up directories containing temporary files (for example, /tmp).

This updated package fixes the following bugs:

* tmpwatch automatically deletes temporary directories, which previously broke some Java management functionality. With this update, this issue has been resolved and the newly added option --exclude-pattern is now used to preserve these directories. (BZ#527425)

* previously, tmpwatch called fuser (1) incorrectly, which lead to unexpected error messages when encountering a file name starting with '-' character. This issue has now been resolved and tmpwatch now calls fuser (1) correctly even for file names starting with the '-' character. (BZ#548932)

Users are advised to upgrade to this updated tmpwatch package, which resolves this issue.

1.153. tog-pegasus

1.153.1. RHBA-2010:0869: bugfix update

An updated tog-pegasus package that fixes a bug is now available for Red Hat Enterprise 5.

OpenPegasus Web-Based Enterprise Management (WBEM) Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent Distributed Management Task Force (DMTF) standard that defines a common information model (CIM) and communication protocol for monitoring and controlling resources from diverse sources.

This update fixes the following bug:

* Previously, not all array elements, which were cloned by the OpenPegasus CIM server, were released together with the Common Manageability Programming Interface Array(CMPIArray) by calling their respective release functions. This resulted in memory leak. With this update, the new flag isCloned handles the release for cloned CMPIArray. (BZ#644839)

This patch also resolves memory leaks in sample CMPIInstanceProvider.

Users of OpenPegasus are advised to upgrade to this updated package, which resolves this issue.

1.154. tomcat5

1.154.1. RHBA-2011:0138: bug fix update

Updated tomcat5 packages that resolve several issues are now available.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

These updated tomcat5 packages provide fixes for the following bugs:

* Fetching a data source from Java Naming and Directory Interface (JNDI) failed with a ClassNotFoundException. This happened because the naming-factory-dbcp library referred to a missing class when calling data source. This update adds the system property javax.sql.DataSource.Factory to JAVA_OPTS and data source fetching works as expected. (BZ#217630)

* After upgrading to tomcat5-5.5.23-0jpp.9.el5_5, the system throws a StackOverflowError. This happened due to a typographical error in the patch. With this update, the error is fixed. (BZ#620996)

* After upgrading to tomcat5-5.5.23-0jpp.9.el5_5, a NullPointerException occurred after starting the Tomcat service. This was due to an error in the context.xml validation. This update corrects validation of the context.xml file. (BZ#623465)

* Tomcat 5 failed to start due to incorrect file permissions. Permissions have been corrected in the installation script and the problem no longer occurs. (BZ#551267)

All tomcat5 users are advised to upgrade to these updated packages, which resolve these issues.

1.154.2. RHBA-2010:0744: bug fix update

Updated tomcat5 packages that resolve several issues are now available.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

These updated tomcat5 packages provide fixes for the following bugs:

* Previously, when Tomcat was starting up, it failed to undeploy applications and returned a 'StackOverflowError' exception. This was caused by an infinite loop that eventually caused Tomcat to run out of memory. The infinite loop was a result of a faulty check that searched for directory traversal attempts in WAR archives. With this update, the undeploying of applications works as expected and no longer returns a stack overflow error. (BZ#623254)

* During Tomcat's startup process, applications that used the 'context.xml' configuration file would occasionally fail with a 'NullPointerException' exception or a 'ConcurrentModificationException' exception, leaving the 'tomcat5' process running, but not working. With this update, applications no longer fail and no longer return the aforementioned exceptions. (BZ#627507)

All users of tomcat5 are advised to upgrade to these updated packages, which resolve these issues.

1.155. udev

1.155.1. RHBA-2011:0073: bug fix and enhancement update

Updated udev packages that fix several bugs and add various enhancements are now available.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user-space, dynamically creates and removes devices, provides consistent naming, and a user-space API. udev replaces devfs, providing greater hot plug functionality.

These updated udev packages provide fixes for the following bugs:

* Previously, the udev helper application 'vol_id' ran several times if a device was unreadable. This caused a massive delay for the bootup process on some machines. With this update, 'vol_id' checks whether a device is readable only once and no longer causes a delay. (BZ#456447)

* Previously, 'cciss' devices did not have an entry in the udev database. This was caused by the fact that these devices do not provide information in the /sys file system, making it hard to create persistent symbolic links in '/dev/disk'. With this update, the 'scsi_id' utility is used to query the ID of 'cciss' devices, so that udev can create the database entries as expected. (BZ#515566)

* Prior to this update, renaming a network device with udev rules could fail. This was caused by a faulty retry-loop in the code. With this update, renaming a network device works as expected. (BZ#520453)

* The udev daemon could die with an unhandled SIGBUS error if a 'rules' file was removed while udev was reading it. This was caused by a race condition between the 'fstat/mmap/loop' process and another process that is modifying the file. With this update, the race condition is removed and udev no longer fails. (BZ#521318)

* Updating the udev packages caused udev not to run after the update. This was caused by the udevd process not being shut down cleanly before the update. When the new udevd process attempted to start, it failed because the original udevd process was still running. With this update, the update mechanism works as expected. (BZ#567406)

* Setting a 'umask' to a non-default value could cause some devices to not be readable by other processes. This update sets an explicit 'umask' for the udev daemon. (BZ#596774)

* Prior to this update, udev renamed the '/dev/sr*' device nodes to '/dev/scd*'. This caused some sr* devices nodes (referenced by kernel information such as '/proc/sys/dev/cdrom/info') to be missing. This update creates symbolic links to /dev/scd* and creates the /dev/sr* device nodes. (BZ#610897)

In addition, these updated packages provide the following enhancements:

* Previously, udev did not create '/dev/tape/by-path' symbolic links for tape devices. With this update, the 'by-path' symbolic links are created. (BZ#611664)

* The virtio-console driver has been updated to handle generic communication in Red Hat Enterprise Linux 5.6. For any named virtio-serial ports, this update now creates symbolic links in '/dev/virtio-ports/'. (BZ#624928)

Users are advised to upgrade to these updated udev packages, which resolve these issues and add these enhancements.

1.155.2. RHBA-2010:0593: bug fix update

Updated udev packages that fix a bug are now available.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user-space, dynamically creates and removes devices, provides consistent naming, and a user-space API. udev replaces devfs, providing greater hot plug functionality.

These updated packages fix the following bug:

* previously, cciss devices did not have an entry in the udev database. This was caused by the fact that these devices do not provide information in the /sys file system, making it hard to create persistent symbolic links in /dev/disk. With this update, the scsi_id utility is used to query the ID of cciss devices, so that udev can create the database entries as expected. (BZ#615270)

Users of udev are advised to upgrade to these updated packages, which resolve this issue.

1.156. util-linux

1.156.1. RHBA-2011:0085: bug fix update

Updated util-linux packages that fix various bugs are now available.

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, util-linux contains the fdisk configuration tool and the login program.

The updated packages include the following fixes:

* The fdisk(8) command showed wrong partition name on device-mapper-multipath devices. (BZ#448919)

* The ipcs(1) command returned wrong return code on errors. (BZ#465911)

* The man page for blockdev(8) was not up to date. (BZ#470497)

* The 'mount -a' command was not able to detect that some pseudo filesystems (e.g. tmpfs) are already mounted. (BZ#475509)

* The "~/.hushlogin" file was invisible for the login(1) command if the home directory was on NFS. (BZ#488192)

* The PAM configuration of the login(1) command initialized the keyring at an inconvenient time. (BZ#245578)

* The man page for login(1) had obsolete information about users switching. (BZ#495192)

* The script(1) command didn't log to the utmp database. (BZ#490693)

* The fdisk(8) and sfdisk(8) commands used unnecessary sleep(2) calls. (BZ#502639)

* The fdisk(8) command was not able create partition with starting beyond 1 TiB. (BZ#471369)

* The sfdisk(8) command didn't ensure writes make it to disk. (BZ#565946)

* The flock(1) command faulted when file name is not given.(BZ#513369)

* The man page for mount(8) didn't describe all vfat options for non-UTF8 locale. (BZ#515149)

* The remount of bind mounts wasn't properly documented in the man page for mount(8). (BZ#568194)

* The 'cal -3' command generated improperly formatted output. (BZ#458055)

* The /etc/udev/rules.d/60-raw.rules file was trashed by util-linux update. (BZ#612423)

* The mount(8) command produced spurious warning when /bin/mount wasn't set-uid. (BZ#559302)

Users of util-linux should upgrade to these updated packages, which resolve these issues.

1.157. vim

1.157.1. RHBA-2010:0685: bug fix update

Updated vim packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

VIM (VIsual editor iMproved) is an updated and improved version of the vi editor.

These updated vim packages provide fixes for the following bugs:

* the menu entry for gvim was previously in the Development menu. With this update, it moved to the "Accessories" menu because gvim isn't a developer-only application. (BZ#506442)

* previously, when editing a script which contained the control character "\c", vim reported a syntax error. This was due to a incorrect "." after "c" in the regex for shSpecial. With this release, this issue is resolved and no syntax error appears. (BZ#512265)

* when running vim in ex mode, running comments previously returned an error at end-of-file. With this update, only empty lines return an error, not comments. (BZ#572157)

All users of vim are advised to upgrade to these updated packages, which resolve these issues.

1.158. virt-manager

1.158.1. RHBA-2011:0077: bug fix update

An updated virt-manager package that fixes two bugs and adds an enhancement is now available for Red Hat Enterprise Linux 5.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. virt-manager can start, stop, add or remove virtualized devices, connect to a graphical or serial

console, and see resource usage statistics for existing virtualized guests on local or remote machines. It uses the libvirt API.

This update fixes the following bugs:

* Due to various errors in some of the translations, users of Virtual Machine Manager in non-English languages may have encountered superfluous characters or even untranslated strings. These errors have been fixed, and the application is now correctly translated to all available languages. (BZ#513324)

* Since version 5.4, KVM (Kernel-based Virtual Machine) supports memory overcommitment, which allows virtualized guests to use more than 100% of the memory that is currently available on a host system. However, when this feature was in use, Virtual Machine Manager did not display the total memory usage correctly. With this update, the underlying source code has been adjusted to check whether the memory is overcommitted, so that the "Memory Usage" field reports the correct value. (BZ#521754)

As well, this update adds the following enhancement:

* URL installation options for fully virtualized guests have been enabled in Virtual Machine Manager. This is accomplished by fetching a boot.iso disc image from the URL install tree. (BZ#612676)

All users of virt-manager are advised to upgrade to this updated package, which resolves these issues, and adds this enhancement.

1.159. virtio-win

1.159.1. RHBA-2011:0106: bug fix and enhancement update

An updated virtio-win package that fixes a bug and adds an enhancement is now available for Red Hat Enterprise Linux 5.

Para-virtualized drivers are virtualization-aware drivers used by fully virtualized guests running on Red Hat Enterprise Linux. Fully-virtualized guests using the para-virtualized drivers gain significantly better I/O performance than fully-virtualized guests running without the drivers.

The virtio-win package provides para-virtualized network drivers for the following guest operating systems:

32-bit Windows XP 32-bit Windows Server 2003 64-bit Windows Server 2008 32-bit Windows Server 2008 64-bit Windows Server 2008 R2 32-bit Windows 7

The virtio-win package also provides para-virtualized disk (block) drivers for the following guest operating systems:

32-bit Windows XP 32-bit Windows Server 2003 64-bit Windows Server 2008 32-bit Windows Server 2008 64-bit Windows Server 2008 R2 32-bit Windows 7

This update fixes the following bug:

* When installing the VirtIO driver, the relevant dialog window did not offer Windows 7 as the target operating system. With this update, Windows 7 has been added to the list of supported operating systems, and this error no longer occurs. (BZ#605334)

As well, this update adds the following enhancement:

* The content of the Virtual Floppy Disk (VFD) is now distributed as a part of the package installation, and can be found in the /usr/share/virtio-win/drivers directory. (BZ#636516)

All users running fully-virtualized instances of Windows on Red Hat Enterprise Linux-based KVM hosts are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

1.160. vnc

1.160.1. RHBA-2010:0563: bug fix update

Updated vnc packages that fix various bugs are now available.

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

These updated vnc packages resolve the following issues:

* libvnc.so module to Xorg wasn't able to wake up the main Xorg process when entered to the DPMS standby mode. Now, when libvnc.so receives keyboard or mouse event over network, it wakes up the Xorg and turns down running screensaver. (BZ#607566)

* the VNC server script didn't accept +option switches when specified before [:X] display number. This issue is now resolved. (BZ#607567)

All VNC Users are advised to upgrade to these updated VNC packages, which resolve those issues.

1.160.2. RHBA-2010:0421: bug fix update

A vnc package that fixes a bug is now available.

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

This updated vnc package provides fix for the following bug:

* The Java VNC viewer failed to send the "tab" key to the VNC server correctly. (BZ#576905)

All users of vnc are advised to upgrade to this updated package, which resolves this issue.

1.161. vsftpd

1.161.1. RHBA-2010:0410: bug fix update

An updated vsftpd package that fixes two bugs is now available.

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

This updated vsftpd package includes fixes for the following bugs:

* when the "connect_from_port_20" directive in the vsftp.conf configuration file was set to "NO", and other directives were set to certain values, the vsftpd daemon would disconnect clients immediately after establishing the connection. With this update, setting "connect_from_port_20=NO" in vsftpd.conf no longer results in such disconnects, and clients are again able to successfully establish connections. (BZ#580055)

* when the "background" directive in the vsftpd.conf configuration file is set to "YES", the vsftpd startup script forks, creating a child process (the vsftpd daemon) which immediately sends the SIGUSR1 signal to its parent process, which exits upon receiving it. When "background=NO" was specified in vsftpd.conf, the startup script did not fork, but still sent the SIGUSR1 signal to its parent process, which could have been any process that started the vsftpd process. A parent process which did not explicitly handle SIGUSR1 would exit upon receiving this signal. This update ensures that when "background=NO" is specified in vsftpd.conf, the vsftpd process running in the foreground does not send the SIGUSR1 signal to its parent process, thus

avoiding potentially causing that process to exit. (BZ#580396)

All users of vsftpd are advised to upgrade to this updated package, which resolves these issues.

1.162. wacomexpresskeys

1.162.1. RHBA-2011:0129: bug fix and enhancement update

An updated wacomexpresskeys package that fixes a bug and adds an enhancement is now available for Red Hat Enterprise Linux 5.

The wacomexpresskeys package provides a configuration utility that allows a user to map Wacom tablet ExpressKeys and Touch Strips to other events.

This update fixes the following bug:

* Due to an error in the Wacom Cintiq 21UX support, ExpressKeys did not work properly on such devices. This error has been fixed, the underlying source code has been modified to target this issue, and ExpressKeys on Wacom Cintiq21UX devices now work as expected. (BZ#589684)

As well, this update adds the following enhancement:

* The wacomexpresskeys utility has been updated to support Wacom Cintiq 21UX2 devices. (BZ#652743)

Users of Wacom Cintiq 21UX or Wacom Cintiq 21UX2 devices are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

1.163. wdaemon

1.163.1. RHBA-2011:0128: bug fix and enhancement update

An updated wdaemon package that fixes a bug and adds an enhancement is now available for Red Hat Enterprise Linux 5.

wdaemon is a helper application that emulates persistent input devices for Wacom tablets. This allows such devices to be plugged in and unplugged while an X Window System server is running.

This update fixes the following bug:

* On a tablet PC that is detected as a tablet by wdaemon, the presence of a serial tablet caused the "wacom - a" command to fail with the following error:

Error retrieving device id: Invalid argument

With this update, an upstream patch has been applied to correct the detection of such device, and running the above command now produces the expected results. (BZ#504332)

As well, this update adds the following enhancement:

* The wdaemon package has been updated to add the support for Wacom Cintiq 21UX2 devices. (BZ#652740)

Users of Wacom Cintiq 21UX2 devices are advised to upgrade to this updated package, which adds this enhancement.

1.164. xen

1.164.1. RHBA-2011:0031: bug fix and enhancement update

Updated xen packages that fix several bugs and add enhancements are now available.

The xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

These updated packages include numerous bug fixes for and enhancements to the xen packages. Space precludes documenting each of these changes in this advisory and users are directed to the Virtualization chapter in the Red Hat Enterprise Linux 5.6 Technical Notes:

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.6_Relea se_Notes/ar01s02.html

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which fix the bugs and add the enhancements noted in the Red Hat Enterprise Linux 5.6 Technical Notes. The system must be rebooted for this update to take effect.

1.164.2. RHBA-2010:0572: bug fix update

Updated Xen packages that fix a bug are now available for Red Hat Enterprise Linux.

Xen is a high performance and secure open source virtualization framework. Virtualization lets users run guest operating systems in virtual machines on top of a host operating system.

These updated Xen packages resolve the following issue:

* xenstore slowly but consistently leaked memory. This caused problems on systems that ran for a long time. These packages remove this leak. (BZ#616091)

All Xen users are advised to install these updates, which resolve this issue.

1.164.3. RHBA-2010:0515: bug fix update

Updated xen packages that add support for the HLT instruction emulation and the assignment of the Intel 82599 Virtual Function to the Hardware Virtual Machine (HVM) guest.

Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bugs:

* due to the missing HLT (halt) instruction emulation in the VMXAssist real-mode emulator, certain versions of the SYSLINUX boot loader could have caused the guest operating system (domU) to stop responding. With this update, the HLT instruction emulation has been added, and all versions of SYSLINUX now boot properly. (BZ#593230)

* previously, the PCIe Capability Structure was set to 0. As a result, it was impossible to assign the Niantic Virtual Function (VF) to the Hardware Virtual Machine (HVM) guest. This has been fixed, and the Niantic VF can now be assigned as expected. (BZ#599018)

All Xen users should install this update, which addresses these issues.

1.164.4. RHBA-2010:0456: bug fix update

An updated xen package that fixes a problem with broadcast packets not travelling from dom0 to domU instances is now available.

Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bug:

* when the xen bridge ran on an arp-monitored bond device, the local routing table did not properly flush IP addresses. Consequently, broadcast packets sent from dom0 were not received by domUs running on the same system. With this update the routing table is cleaned up properly and packets from dom0 are received by domU instances as expected. (BZ#592219)

All Xen users, particularly those running guest instances of Windows, should install this update, which addresses this issue.

1.164.5. RHBA-2010:0418: bug fix update

An updated xen package that changes some PCI device classes, ensuring the Storage Query Property test (part of the Windows Logo test) are passed, is now available.

Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bug:

* previously, some para-virtualized drivers returned a STORAGE_BUS_TYPE (SCSI in this case) that was inconsistent with its PCI class code. They, consequently, failed the Storage Query Property test (part of the Windows Logo test). With this update, these drivers' class and sub-class were changed from "Unclassified" and "Other" to "Storage" and "SCSI" respectively. This is consistent with their STORAGE_BUS_TYPE and they now pass the Storage Query Property test. (BZ#580398)

All Xen users, particularly those running guest instances of Windows, should install this update, which addresses this issue.

1.165. xorg-x11-drv-ati

1.165.1. RHBA-2011:0080: bug fix and enhancement update

An updated xorg-x11-drv-ati package that fixes a bug and adds an enhancement is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-ati package provides a driver for the X.Org implementation of the X Window System, for ATI cards.

This update fixes the following bug:

* On certain Dell machines with ATI RN50 video controllers, an internal error (IERR) may have occurred when switching between a virtual terminal (VT) and an X session. This was caused by the driver incorrectly resetting a component of the graphics processing unit (GPU). With this update, the driver no longer attempts to reset that component, and switching between an X session and a virtual terminal now works as expected. (BZ#608894)

As well, this updated package adds the following enhancement:

* The driver has been updated to support mode-setting on the HD5xxx (Evergreen) series of the ATI Radeon GPUs. (BZ#573063)

All users of xorg-x11-drv-ati are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

1.165.2. RHBA-2010:0715: bug fix update

An updated xorg-x11-drv-ati package that fixes a bug is now available.

The xorg-x11-drv-ati package provides a driver for ATI cards for the X.Org implementation of the X Window System.

This updated xorg-x11-drv-ati package fixes the following bug:

* previously, on certain Dell servers, VT switching on RN50 cards caused an internal error (IERR). This was caused by the driver incorrectly resetting a component of the GPU on a VT switch. With this update, the driver no longer attempts to reset that component. (BZ#627510)

All users of xorg-x11-drv-ati are advised to upgrade to this updated package, which resolves this issue.

1.166. xorg-x11-drv-mga

1.166.1. RHEA-2011:0104: enhancement update

An updated xorg-x11-drv-mga package is now available for Red Hat Enterprise Linux 5.

xorg-x11-drv-mga is a video driver for the X.Org implementation of the X Window System that provides a support for Matrox G-series chips.

This update adds the following enhancement:

* The video driver has been extended to support Matrox G200eH application-specific integrated circuits (ASICs). These chips are typically used in servers and server management products. (BZ#569554)

All users of the xorg-x11-drv-mga driver should upgrade to this updated package, which adds this enhancement.

1.167. xorg-x11-drv-nv

1.167.1. RHBA-2011:0121: bug fix update

An updated xorg-x11-drv-nv package that fixes a bug is now available for Red Hat Enterprise Linux 5.

xorg-x11-drv-nv is a video driver for the X.Org implementation of the X Window System that provides a support for NVIDIA cards.

This update fixes the following bug:

* Currently, the nv driver for NVIDIA graphics devices does not fully support the DisplayPort digital display interface. To prevent possible issues, this update disables this driver on the following chips that are known to have DisplayPort outputs:

FX4800 (PCI device ID 0x05fe) FX1800 (PCI device ID 0x0638) FX380 (PCI device ID 0x0658) FX580 (PCI device ID 0x0659) NVS450 (PCI device ID 0x06fa) NVS295 (PCI device ID 0x06fd)

Users with these chips may still use the nv driver by explicitly enabling it in the X.Org configuration, otherwise the vesa fallback driver will be used instead. (BZ#566228)

All users of the xorg-x11-drv-nv driver should upgrade to this updated package, which resolves this issue.

1.168. xorg-x11-drv-sis

1.168.1. RHEA-2011:0105: enhancement update

An updated xorg-x11-drv-sis package is now available for Red Hat Enterprise Linux 5.

xorg-x11-drv-sis is a video driver for the X.Org implementation of the X Window System that provides a support for Silicon Integrated Systems (SiS) graphics chips.

This update adds the following enhancement:

* The video driver has been extended to support XGI Volari Z9s application-specific integrated circuits (ASICs). These chips are typically used in servers and server management products. (BZ#483568)

Note: On new installations of Red Hat Enterprise Linux 5.6, this updated package will use the appropriate driver automatically. On existing systems, it may be necessary to switch to the "xgi" driver after the updated package is installed. To do this, run the following command as root:

system-config-display --reconfig

All users of the xorg-x11-drv-sis driver should upgrade to this updated package, which adds this enhancement.

1.169. xorg-x11-server

1.169.1. RHBA-2010:0722: bug fix update

Updated xorg-x11-server packages that resolve an issue are now available.

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality upon which full fledged graphical user interfaces such as GNOME and KDE are designed.

These updated xorg-x11-server packages fix the following bug:

* the 'miDbePositionWindow' function allocates two pixmaps: a front buffer, and a back buffer. If the buffers are supposed to be initialized, it validates a graphic context (GC) against the front buffer, then uses it to fill and/or copy both the front buffer and the back buffer, without revalidating. If the acceleration architecture needed different GC functions for the two pixmaps, for example if allocation of the front buffer exhausted video memory, then this caused crashes because the GC was not validated for the back buffer pixmap. With this update, the crashes no longer occur and GC validation works as expected. (BZ#626328)

All users of xorg-x11-server are advised to upgrade to these updated packages, which resolve this issue.

1.170. yaboot

1.170.1. RHBA-2010:0815: bug fix update

An updated yaboot package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

This update fixes the following bug:

* Prior to this update, attempting to load a kernel with the CONFIG_RELOCATABLE option enabled failed with the following error:

/vmlinuz: Not a valid ELF image

This option changes the ELF file format to ET_DYN. With this update, the underlying code has been modified to allow this format, and relocatable kernel images can now be loaded as expected. (BZ#647777)

All users of yaboot are advised to upgrade to this updated package, which resolves this issue.

1.171. yum

1.171.1. RHBA-2011:0136: bug fix update

An updated yum package that fixes several problems and adds an enhancement is now available for Red Hat Enterprise Linux 5.

Yum is a utility that can check for, automatically download, and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.

This update fixes the following bugs:

* Previously, yum checked the configured server host name with the name in the server's SSL certificate when connecting to HTTPS yum repositories, even when SSL verification was disabled, which is the default setting. With this update yum will only check names when SSL verification is enabled. Note: yum-rhn-plugin always disables name checks even for non-RHN repositories. (BZ#500721)

* Previously, installing obsolete packages resulted in installing the package of the incorrect arch. With this update, Yum selects the correct arch and the issue is resolved. (BZ#593349)

* Previously, running yum failed when /proc was not mounted. With this update, yum uses the generic result instead of trying to narrow down the architecture of the Central Processing Unit (CPU). (BZ#623955)

* Previously, when getting unique metadata from RHN yum would only delete the downloaded files and not the generated (.sqlite) files. This meant that /var/cache/yum would grow without bound. With this update, yum will delete the generated files as well. (BZ#628963)

* Previously, the yum.conf manual page did not document options for setting SSL verification parameters for HTTPS yum repositories. With this update, these options are documented. (BZ#637146)

This update also adds the following enhancement:

* With this update, yum can parse more fields in the updateinfo.xml metadata and provides these fields to other applications. (BZ#634119)

Yum users are advised to upgrade to this updated package which resolves these issues.

1.171.2. RHBA-2010:0814: bug fix update

An updated yum package that fixes a bug in the cache control mechanism is now available for Red Hat Enterprise Linux 5.

Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically, prompting the user for permission as necessary.

This updated package provides fixes for the following bug:

* Previously, when getting unique metadata from Red Hat Network (RHN), yum would only delete the downloaded files and not the generated (.sqlite) files. This meant that /var/cache/yum would grow without bound. With this update, yum will delete the generated files as well. (BZ#646982)

All users are advised to upgrade to this updated package, which resolves this issue.

1.172. yum-rhn-plugin

1.172.1. RHEA-2011:0112: and rhn-client-tools bug fix and enhancement update

Updated rhn-client-tools and yum-rhn-plugin packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network (RHN). yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

This update fixes the following bugs:

* When the "networkRetries" configuration option was not set to a valid integer value, network operation did not time out at all. With this update, invalid values are now interpreted as a single attempt, and network operations time out as expected. (BZ#554693)

* Due to a typing error, the manual page for rhn-profile-sync incorrectly referred to /etc/sysconfig/rhn/update, even though the file is actually called /etc/sysconfig/rhn/up2date. This has been corrected, and the manual page no longer contains misleading information. (BZ#559797)

* On a PowerPC system, running the rhn_register utility did not subscribe a user to all relevant channels associated with the installation number. As a result, affected users had to subscribe to these channels manually. This error no longer occurs, and all users are now subscribed to appropriate channels as expected. (BZ#574404)

* Prior to this update, KVM and Xen fully virtualized guests may have incorrectly consumed regular entitlements. This error has been fixed, and such guests now use Flex Guest Entitlement as expected. (BZ#575127,

BZ#624780)

* Several files related to the graphical user interface (GUI) were removed from the rhn-setup package, and are now installed as a part of rhn-setup-gnome. (BZ#584779)

* Under certain circumstances, clicking the "back" button in a GUI version of the rhn_register utility may have caused the cursor to remain busy. This error has been fixed, and the cursor is now properly restored. (BZ#595679)

* Due to an error in the architecture checking, the rhn_register utility failed to update packages when their architecture had changed from "noarch" to "multiarch" or vice versa. With this update, the underlying source code has been modified to target this issue, and such packages are now updated as expected. (BZ#603028)

* The number of CPUs is now reported correctly on IBM System z. (BZ#621135)

* Previously, using the hash sign (that is, "#") in a proxy password caused yum to fail with the following error:

Error communicating with server. The message was: Proxy Authentication Required

With this update, this error no longer occurs, and the use of this character no longer prevents yum from working. (BZ#650520)

As well, this update adds the following enhancement:

* The rhn-client-tools package has been updated to support the Red Hat Network Satellite Server Maintenance Window. (BZ#626737)

All users of rhn-client-tools and yum-rhn-plugin are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

1.173. yum-utils

1.173.1. RHBA-2010:0509: bug fix update

An updated yum-utils package that fixes a bug in yum-complete-transaction that could, potentially, render a system inoperable, is now available.

yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use.

These updated yum-utils packages fix the following bug:

* the yum-complete-transaction utility finds incomplete or aborted yum transactions on a system and then attempts to complete them. Following dependency analysis, yum-complete-transaction could, in some circumstances, mark essential system packages for removal. If the operation was continued, resulting in the removal of said packages, it was entirely possible to make the system inoperable as a result.

With this update, yum-complete-transaction analyzes the list of packages to be removed more thoroughly. If it finds the transaction size has changed (the precipitating state that caused essential system packages to be marked for removal) it aborts the operation and returns a "Transaction size changed" error with suggestions for further action. (BZ#574389)

All yum-utils users should upgrade to these updated packages, which resolve this issue.

1.174. zsh

1.174.1. RHBA-2010:0804: bug fix update

An updated zsh package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The zsh shell is a command interpreter which can be used as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

This updated package provides fixes the following bugs:

* Previously, zsh could fail when searching the history in vi mode. With this update, searching the history in vi mode works as expected and the issue is resolved. (BZ#610505)

* Previously, running zsh in ksh mode caused incorrect error messages during syntax only check. With this update, zsh in ksh mode behaves as expected and no more incorrect messages appear during syntax only check. (BZ#488943)

Users of zsh are advised to upgrade to this updated package, which resolves these issues.

Chapter 2. New Packages

New Packages

2.1. RHBA-2011:0046: c-ares

The c-ares package is now available for Red Hat Enterprise Linux 5.

This new package provides a library of asynchronous DNS operations and is an SSSD dependency (BZ#621002).

All users requiring c-ares should install this newly-released package, which adds this enhancement.

2.2. RHEA-2011:0056: certmonger

The certmonger package is now available for Red Hat Enterprise Linux 5.

Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.

This new package provides the certmonger utility which can monitor certificates and warn the system administrator when those certificates are no longer valid. If it has access to a private key which corresponds to a certain certificate, and the certificate was issued by a CA which it supports, certmonger can be told to automatically request a new certificate in case the certificate expires. (BZ#578204)

All users requiring certmonger should install this newly-released package, which adds this enhancement.

2.3. RHBA-2011:0024: dropwatch

The dropwatch package is now available for Red Hat Enterprise Linux 5.

The dropwatch package provides packet monitoring services.

This new package provides the dropwatch utility, which shows the symbolic instruction pointer of the dropped packet detected by DROP_MONITOR. (BZ#494311)

All users requiring dropwatch should install this newly-released package, which adds this enhancement.

2.4. RHEA-2011:0062: ebtables

A new ebtables package is now available for Red Hat Enterprise Linux 5.

Ethernet bridge tables is a firewalling tool to transparently filter network traffic passing a bridge. The filtering possibilities are limited to link layer filtering and some basic filtering on higher network layers.

This package is now available for general use in Red Hat Enterprise Linux 5. (BZ#583146)

All users requiring firewalling for Ethernet bridge tables should install this newly released package, which adds this functionality.

2.5. RHEA-2011:0114: hplip3

New hplip3 packages that provide drivers for HP printers and multi-function peripherals are now available.

The HPLIP (Hewlett-Packard Linux Imaging and Printing Project) package provides drivers for HP printers and multi-function peripherals.

These packages provide a newer version of HPLIP that can be installed alongside the version provided in Red Hat Enterprise Linux 5. The relevant command line utilities are prefixed with "hp3" instead of "hp", for example, "hp3-setup". (BZ#506645, BZ#629009)

All users requiring HPLIP drivers should install these new packages, which add this enhancement. Note that no additional action is required to use these drivers when using the system-config-printer utility or the CUPS web interface to add or modify printer queues.

2.6. RHEA-2011:0063: ipa-client

A new ipa-client package is now available for Red Hat Enterprise Linux 5.

IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

The ipa-client package provides a tool to enroll a machine to an IPA server version 2, and is not backward compatible with version 1 of the server. (BZ#607772)

All users requiring ipa-client should install this newly released package, which adds this enhancement.

2.7. RHEA-2011:0065: ipa-gothic-fonts

A new ipa-gothic-fonts package is now available.

IPA Font is a JIS X 0213:2004 compliant Japanese OpenType font provided by Information-technology Promotion Agency, Japan. The ipa-gothic-fonts package contains the Gothic (sans-serif) style font.

This new package enhances the Japanese support, and adds a JIS X 0213:2004 compliant Gothic font to Red Hat Enterprise Linux 5. (BZ#606201)

All users requiring the JIS X 0213:2004 character set support should install this newly released package, which adds this enhancement.

2.8. RHEA-2011:0066: ipa-mincho-fonts

A new ipa-mincho-fonts package is now available.

IPA Font is a JIS X 0213:2004 compliant Japanese OpenType font provided by Information-technology Promotion Agency, Japan. The ipa-mincho-fonts package contains the Mincho-style font.

This new package enhances the Japanese support, and adds a JIS X 0213:2004 compliant Mincho font to Red Hat Enterprise Linux 5. (BZ#606202)

All users requiring the JIS X 0213:2004 character set support should install this newly released package, which adds this enhancement.

2.9. RHEA-2011:0067: ipa-pgothic-fonts

A new ipa-pgothic-fonts package is now available.

IPA Font is a JIS X 0213:2004 compliant Japanese OpenType font provided by Information-technology Promotion Agency, Japan. The ipa-pgothic-fonts package contains the Proportional Gothic (sans-serif) style font.

This new package enhances the Japanese support, and adds a JIS X 0213:2004 compliant Proportional Gothic font to Red Hat Enterprise Linux 5. (BZ#606203)

All users requiring the JIS X 0213:2004 character set support should install this newly released package, which adds this enhancement.

2.10. RHEA-2011:0068: ipa-pmincho-fonts

A new ipa-pmincho-fonts package is now available.

IPA Font is a JIS X 0213:2004 compliant Japanese OpenType font provided by Information-technology Promotion Agency, Japan. The ipa-pmincho-fonts package contains the Proportional Mincho-style font.

This new package enhances the Japanese support, and adds a JIS X 0213:2004 compliant Proportional Mincho font to Red Hat Enterprise Linux 5. (BZ#606204)

All users requiring the JIS X 0213:2004 character set support should install this newly released package, which adds this enhancement.

2.11. RHEA-2011:0043: libldb

New libldb packages are now available for Red Hat Enterprise Linux 5.

libldb is an extensible library that implements an LDAP-like API to access remote LDAP servers, or use local TDB databases.

These packages are required by the System Security Services Daemon (SSSD). (BZ#579841)

All users requiring libldb should install these new packages, which provide this functionality.

2.12. RHEA-2011:0040: libtalloc

New libtalloc packages are now available for Red Hat Enterprise Linux 5.

The libtalloc package provides a library that implements a hierarchical memory allocator with destructors.

These packages are required by libtevent, libldb, samba3x, and sssd packages. (BZ#579846)

All users requiring libtalloc are advised to install these newly released packages, which add this enhancement.

2.13. RHEA-2011:0042: libtevent

A new development library, libtevent, is now available.

A new development library, libtevent, is now available.

Tevent is an event system based on the talloc memory management library. It has support for many event types, including timers, signals, and the classic file descriptor events. Tevent also provide helpers to deal with asynchronous code providing the tevent_req (Tevent Request) functions. (BZ#579844)

Libtevent provides the core event system used in Samba and also provides the event-driven main loop for projects such as SSSD and LDB. Anyone using these applications and developers needing to link programs against the Tevent library should install this package.

2.14. RHEA-2011:0050: mod_revocator

A new mod_revocator package is now available for Red Hat Enterprise Linux 5.

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server without a need for a restart or user intervention. It can be configured to retrieve CRLs from remote servers at periodic intervals or when a CRL expires, and make them available to the Apache Secure Sockets Layer (SSL) module, mod_nss. Additionally, it can be configured to stop the Apache server from accepting requests if a CRL retrieval fails.

This package is required for IPA and Certificate System. ([BZ#591244](BZ#591244))

All users requiring mod_revocator should install this new package, which adds this enhancement.

2.15. RHEA-2011:0115: python-pycurl

A new python-pycurl package is now available.

python-pycurl is a Python interface to libcurl. It can be used to fetch objects identified by a URL from a Python program, similar to the urllib Python module. python-pycurl is mature, very fast, and supports a lot of features.

This new package is required by the new fence agents, fence_rhev and fence_cisco_ucs. ([BZ#637830](BZ#637830))

All users requiring python-pycurl should install this new package, which adds this enhancement.

2.16. RHEA-2010:0492: qspice-client

A new qspice-client package is now available.

[Update 23 August 2010] The channel list in this erratum has been corrected. No changes have been made to the packages.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments. SPICE users can view a virtualized desktop or server from the local system or any system with network access to the server. SPICE is available for a variety of machine architectures and operating systems. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

This new package provides the client side of the SPICE protocol. ([BZ#575631](BZ#575631))

Note: the spice client, accessible as /usr/libexec/spicec or by using Red Hat Enterprise Virtualization Manager (RHEV-M) from an administrative portal or user portal, requires a running spice-server daemon that allows the client to access the remote server. If RHEV-M is used, spice-xpi is also required.

All prospective users of the Red Hat Enterprise Virtualization Manager should install this newly-released package, which provides this enhancement.

2.17. RHEA-2011:0020: redhat-release

A new redhat-release package is now available for Red Hat Enterprise Linux 5.6.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.6.

Users of Red Hat Enterprise Linux 5 should upgrade to this updated package.

2.18. RHEA-2010:0460: spice-usb-redirector

A new package, spice-usb-redirector, which enables host operating systems to share USB devices with guest operating systems, is now available.

spice-usb-redirector is a non-free USB driver used to share USB devices with a guest operating system.

The spice-usb-redirector provides USB-over-network capabilities when working with a SPICE client. The package include 3 components: a kernel module, a service daemon to handle the devices and a controller utility which intermediates between SPICE and the USB service daemon. ([BZ#574386](#))

Users wanting host operating systems to make USB devices available to guest operating systems should install this new package.

2.19. RHEA-2010:0493: spice-xpi

A new package, spice-xpi, is now available.

[Update 23 August 2010] The channel list in this erratum has been corrected. No changes have been made to the packages.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments. SPICE users can view a virtualized desktop or server from the local system or any system with network access to the server. SPICE is available for a variety of machine architectures and operating systems. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

This new package provides a Mozilla add-on that allows the SPICE client to run from within Firefox. ([BZ#573586](#))

Note: The SPICE client, accessible as /usr/libexec/spicec or by using Red Hat Enterprise Virtualization Manager (RHEV-M) from an admin portal or user portal, requires a running spice-server that allows the client to access the remote server. If RHEV-M is used, spice-xpi is a required package.

Anyone planning to use the Red Hat Enterprise Virtualization Manager should install spice-xpi.

2.20. RHEA-2011:0064: xmlrpc-c

New xmlrpc-c packages are now available for Red Hat Enterprise Linux 5.

XML-RPC is a way to make remote procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML.

These packages provide a modular implementation of XML-RPC for C and C++. ([BZ#582721](#))

All users requiring XML-RPC are advised to install these newly released packages, which add this enhancement.

2.21. RHEA-2011:0021: zd1211-firmware

2.21. RHEA-2011:0021: zd1211-firmware

A zd1211-firmware package that matches the zd1211rw driver in the latest Red Hat Enterprise Linux kernels is now available.

The zd1211rw driver requires firmware loaded on the device in order to function. This package provides the firmware required by that driver.

Users of the zd1211rw driver are advised to install this new package, which provides this enhancement.

Chapter 3. Detailed Technical Notes

3.1. Red Hat Enterprise Linux 5 and 4 kilobyte sector disks

Until recently all standard harddisks had 512 byte in a sector, but as the capacity of harddisks grows, the 512 bytes per sector limitation is causing issues. To resolve these issues, harddisks with 4 kilobyte sectors are now available, and most firmware (BIOS-es, etc.) and software (operating systems) need to be modified to be able to work with these new disks.

There are 2 versions of 4 kilobytes sector harddisks:

4 kilobyte physical sectors, 512 byte logical sectors harddisk

Disks with 4 kilobyte physical sectors and 512 byte logical sectors are currently the most common 4 kilobyte sector harddrive available. These disks use 4 kilobytes sectors, but present themselves to the firmware and operating system as a 512 byte harddisk. No special support is needed for these, but care must be taken when formatting these to ensure optimal performance.

4 kilobyte physical sectors, 4 kilobyte logical sector harddisks

4 kilobyte physical sectors, 4 kilobyte logical sector harddisks require firmware and software modifications to function. This type of 4 kilobytes sector disks is currently not supported in Red Hat Enterprise Linux 5

3.1.1. Ensuring optimal performace with 4 kilobyte sector disks

When using a 4 kilobyte physical, 512 bytes logical sector harddisk on Red Hat Enterprise Linux 5, the partitions must be aligned to 4k boundaries to ensure optimal performance. If the partitions are not properly aligned the drive needs to do a read / modify / write cycle internally for each 4 kilobyte filesystem block written, leading to serious write performance degradation.

The partition tools do not have support for doing the necessary alignment automatically. When adding one of these disks to an existing Red Hat Enterprise Linux 5 system, the partitions need to be manually aligned during the partition process. Additionally, the installer does not have support for doing the necessary alignment automatically. The disks must be manually partitioned before starting the installation and the pre-created partitions used during installation.

3.1.2. Partitioning a 4 kilobyte sector harddisk for optimal performance

To partition these disks for optimal performance, **parted** must be used and the start and end of the partitions must be given in sectors, not in kilobytes, mega or gigabytes. Specify the start / size in sectors by adding an "s" to the end of the number. Generally, it is a good idea to align the partitions to a multiple of one MB (1024x1024 bytes). To achieve alignment, start sectors of partitions should always be a multiple of 2048, and end sectors should always be a multiple of 2048, minus 1. Note that the first partition can not start at sector 0, use sector 2048 instead.

For example, to create 2 partitions, one of 250 megabytes and one of 500 megabytes, the 250 megabyte partition would then start at sector 2048 and end at sector 514047 (2048 + 250 * 2048 - 1 = 514047). The 500 megabyte partition would start at 514048 (the end of the 250 megabyte partition + 1) and end at 1538047 (514048 + 500 * 2048 - 1 = 1538047).

Using **parted** this would be achieved as follows:

```
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mklabel msdos
```

```
(parted) mkpart p ext2 2048s 514047s
(parted) mkpart p ext2 514048s 1538047s
(parted) p
Partition Table: msdos

Number  Start   End     Size    Type     File system  Flags
 1      1049kB  263MB   262MB   primary
 2      263MB   787MB   524MB   primary

(parted) unit s p
Partition Table: msdos

Number  Start    End       Size      Type     File system  Flags
 1      2048s    514047s   512000s   primary
 2      514048s  1538047s  1024000s  primary
```

Chapter 4. Technology Previews

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. Erratas 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 to fully support Technology Preview features in a future release.

DFS

Starting with Red Hat Enterprise Linux 5.3, CIFS supports Distributed File System (DFS) as a Technology Preview.

CDTB

CTDB is a clustered database based on Samba's Trivial Database (TDB). The *ctdb* package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

Brocade BFA Fibre-Channel/FCoE driver

the `bfa` driver for Brocade Fibre Channel Host Bus adapters is considered a Technology Preview in Red Hat Enterprise Linux 5.6 BZ#475695

FreeIPMI

FreeIPMI is now included in this update as a Technology Preview. FreeIPMI is a collection of Intelligent Platform Management IPMI system software. It provides in-band and out-of-band software, along with a development library conforming to the Intelligent Platform Management Interface (IPMI v1.5 and v2.0) standards.

For more information about FreeIPMI, refer to http://www.gnu.org/software/freeipmi/

TrouSerS and tpm-tools

TrouSerS and `tpm-tools` are included in this release to enable use of *Trusted Platform Module* (TPM) hardware.TPM hardware features include (among others):

> Creation, storage, and use of RSA keys securely (without being exposed in memory)

> Verification of a platform's software state using cryptographic hashes

TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use TrouSerS to write applications that make use of TPM hardware. `tpm-tools` is a suite of tools used to manage and utilize TPM hardware.

For more information about TrouSerS, refer to http://trousers.sourceforge.net/.

eCryptfs

eCryptfs is a stacked cryptographic file system for Linux. It mounts on individual directories in existing mounted lower file systems such as EXT3; there is no need to change existing partitions or file systems in order to start using **eCryptfs**.

With this release, **eCryptfs** has been re-based to upstream version 56, which provides several bug fixes and enhancements. In addition, this update provides a graphical program to help configure **eCryptfs** (`ecryptfs-mount-helper-gui`).

This update also changes the syntax of certain **eCryptfs** mount options. If you choose to update to this version of **eCryptfs**, you should update any affected mount scripts and **/etc/fstab** entries. For information about these changes, refer to **man ecryptfs**.

The following caveats apply to this release of **eCryptfs**:

> Note that the **eCryptfs** file system will only work properly if the encrypted file system is mounted once over the underlying directory of the same name. For example:

```
mount -t ecryptfs /mnt/secret /mnt/secret
```

> The secured portion of the file system should not be exposed, i.e. it should not be mounted to other mount points, bind mounts, and the like.

> **eCryptfs** mounts on networked file systems (e.g. NFS, Samba) will not work properly.

> This version of the **eCryptfs** kernel driver requires updated userspace, which is provided by **ecryptfs-utils-56-4.el5** or newer.

For more information about **eCryptfs**, refer to http://ecryptfs.sf.net. You can also refer to http://ecryptfs.sourceforge.net/README and http://ecryptfs.sourceforge.net/ecryptfs-faq.html for basic setup information.

Stateless Linux

Stateless Linux, included as a Technology Preview, is a new way of thinking about how a system should be run and managed, designed to simplify provisioning and management of large numbers of systems by making them easily replaceable. This is accomplished primarily by establishing prepared system images which get replicated and managed across a large number of stateless systems, running the operating system in a read-only manner (refer to **/etc/sysconfig/readonly-root** for more details).

In its current state of development, the Stateless features are subsets of the intended goals. As such, the capability remains as Technology Preview.

Red Hat recommends that those interested in testing stateless code join the stateless-list@redhat.com mailing list.

The enabling infrastructure pieces for Stateless Linux were originally introduced in Red Hat Enterprise Linux 5.

AIGLX

AIGLX is a Technology Preview feature of the otherwise fully supported X server. It aims to enable GL-accelerated effects on a standard desktop. The project consists of the following:

> A lightly modified X server.

> An updated Mesa package that adds new protocol support.

By installing these components, you can have GL-accelerated effects on your desktop with very few changes, as well as the ability to enable and disable them at will without replacing your X server. AIGLX also enables remote GLX applications to take advantage of hardware GLX acceleration.

FireWire

The **firewire-sbp2** module is still included in this update as a Technology Preview. This module enables connectivity with FireWire storage devices and scanners.

At present, FireWire does not support the following:

> ❯ IPv4

> ❯ *pcilynx* host controllers

> ❯ multi-LUN storage devices

> ❯ non-exclusive access to storage devices

In addition, the following issues still exist in FireWire:

> ❯ a memory leak in the **SBP2** driver may cause the machine to become unresponsive.

> ❯ a code in this version does not work properly in big-endian machines. This could lead to unexpected behavior in PowerPC.

SGPIO Support for dmraid

Serial General Purpose Input Output (SGPIO) is an industry standard communication method used between a main board and a variety of internal and external hard disk drive bay enclosures. This method can be used to control LED lights on an enclosure through the AHCI driver interface.

In this release, SGPIO support in **dmraid** is included as a technology preview. This will allow **dmraid** to work properly with disk enclosures.

Kernel Tracepoint Facility

In this update, a new kernel marker/tracepoint facility has been implemented as a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

kerbors security for CIFS

NEED CONTENT

Kernel Tracepoint Facility

In this update, a new kernel marker/tracepoint facility has been implemented as a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

Software based Fibre Channel over Ethernet (FCoE)

The Fibre Channel over Ethernet (FCoE) driver (fcoe.ko), along with libfc, provides the ability to run FCoE over a standard Ethernet card. This capability is provided as a Technology Preview in Red Hat Enterprise Linux 5.6.

To enable this feature, you must login by writing the network interface name to the **/sys/module/fcoe/parameters/create** file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/create
```

To logout, write the network interface name to the **/sys/module/fcoe/parameters/destroy** file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/destroy
```

For further information on software based FCoE refer to: http://www.open-fcoe.org/openfc/wiki/index.php/FCoE_Initiator_Quickstart.

Red Hat Enterprise Linux 5.6 provides full support for FCoE on three specialized hardware implementations. These are: Cisco **fnic** driver, the Emulex **lpfc** driver, and the Qlogic **qla2xx** driver.

iSER Support

iSER support, allowing for block storage transfer across a network, has been added to the **scsi-target-utils** package as a Technology Preview. In this release, single portal and multiple portals on different subnets are supported. There are known bugs when using multiple portals on the same subnet.

To set up the iSER target component install the scsi-target-utils and libibverbs-devel RPM. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to Red Hat Bugzilla #470627 for more information on this issue.

cman fence_virsh fence agent

The fence_virsh fence agent is provided in this release of Red Hat Enterprise Linux as a Technology Preview. fence_virsh provides the ability for one guest (running as a domU) to fence another using the libvirt protocol. However, as fence_virsh is not integrated with cluster-suite it is not supported as a fence agent in that environment.

glibc new MALLOC behaviour

The upstream glibc has been changed recently to enable higher scalability across many sockets and cores. This is done by assigning threads their own memory pools and by avoiding locking in some situations. The amount of additional memory used for the memory pools (if any) can be controlled using the environment variables MALLOC_ARENA_TEST and MALLOC_ARENA_MAX.

MALLOC_ARENA_TEST specifies that a test for the number of cores is performed once the number of memory pools reaches this value. MALLOC_ARENA_MAX sets the maximum number of memory pools used, regardless of the number of cores.

The glibc in the Red Hat Enterprise Linux 5.6 release has this functionality integrated as a Technology Preview of the upstream malloc. To enable the per-thread memory pools the environment variable MALLOC_PER_THREAD needs to be set in the environment. This environment variable will become obsolete when this new malloc behaviour becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

Intel Patsburg device controllers

The enablement of Intel Patsburg device controllers is considered a Technology Preview in Red Hat Enterprise Linux 5.6

ipa-client

The ipa-client package provides a tool to enroll a machine to an IPA server version 2, and is not backward compatible with version 1 of the server. ipa-client is considered a Technology Preview in Red Hat Enterprise Linux 5.6

Note, however that SSSD needs to be manually configured for use with IPA.

Configuring NSS to fetch user and group information

SSSD provides the nss_sss NSS module. To use this module, configure NSS to use the sss name database in addition to the UNIX file database. Edit /etc/nsswitch.conf, adding the following lines:

```
passwd:      files sss
group:       files sss
```

Configuring PAM for authentication

> ⚠️ **Warning**
>
> Errors when editing the PAM configuration file can lock you out of the system. Always back up the configuration file and keep another session open to revert changes if an error is made.

Change the PAM config file to:

```
auth         required       pam_env.so
auth         sufficient     pam_unix.so nullok try_first_pass
auth         requisite      pam_succeed_if.so uid >= 500 quiet
auth         sufficient     pam_sss.so use_first_pass
auth         required       pam_deny.so

account      required       pam_unix.so broken_shadow
account      sufficient     pam_localuser.so
account      sufficient     pam_succeed_if.so uid < 500 quiet
account      [default=bad success=ok user_unknown=ignore]
pam_sss.so
account      required       pam_permit.so

password     requisite      pam_cracklib.so try_first_pass
retry=3
password     sufficient     pam_unix.so sha512 shadow nullok
try_first_pass
use_authtok
password     sufficient     pam_sss.so use_authtok
password     required       pam_deny.so

session      optional       pam_keyinit.so revoke
session      required       pam_limits.so
session      [success=1 default=ignore] pam_succeed_if.so
service in crond quiet
use_uid
session      required       pam_unix.so
session      optional       pam_sss.so
```

Chapter 5. Known Issues

5.1. anaconda

The anaconda package contains the program which was used to install your system.

The following are the Known Issues that apply to the anaconda package in Red Hat Enterprise Linux 5

» anaconda sometimes crashes while attempting to install on a disk containing partitions or filesystems used by other operating systems. To workaround this issue, clear the existing partition table using the command:

```
clearpart --initlabel [disks]
```

BZ#530465

» Performing a System z installation when the install.img is located on direct access storage device (DASD) disk, will cause the installer to crash, returning a backtrace. anaconda is attempting to re-write (commit) all disk labels when partitioning is complete, but is failing because the partition is busy. To work around this issue, a non-DASD source should be used for install.img. BZ#455929

» When installing to an ext3 or ext4 file system, anaconda disables periodic filesystem checking. Unlike ext2, these filesystems are journaled, removing the need for a periodic filesystem check. In the rare cases where there is an error detected at runtime or an error while recovering the filesystem journal, the file system check will be run at boot time. (BZ#513480)

» Red Hat Enterprise Linux 5 does not support having a separate /var on a network filesystem (nfs, iscsi disk, nbd, etc.) This is because /var contains the utilities required to bring up the network, for example /var/lib/dhcp. However, you may have /var/spool, /var/www or the like on a separate network disk, just not the complete /var filesystem. BZ#485478

» When using rescue mode on an installation which uses iscsi drives which were manually configured during installation, the automatic mounting of the root filesystem will not work and you need to configure iscsi and mount the filesystems manually. This only applies to manual configured iscsi drives, iscsi drives which are automatically detected through ibft are fully supported in rescue mode.

To rescue a system which has / on a non ibft configured iscsi drive, choose to skip the mounting of the root fs when asked and then follow the steps below.

```
$TARGET_IP: IP address of the iscsi target (drive)
$TARGET_IQN: name of the iscsi target as printed by the discovery command
$ROOT_DEV: devicenode (/dev/.....) where your root fs lives
```

» Define an initiator name.

```
$ mkdir /etc/iscsi
$ cat << EOF>> /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.fedora:d62f2d7c09f
EOF
```

» Start iscsid

```
$ iscsid
```

» Discover and login to target:

```
$ iscsiadm -m discovery -t st -p $TARGET_IP
$ iscsiadm -m node -T $TARGET_IQN -p $TARGET_IP --login
```

 » If the iSCSI LUN is part of a LVM Logical volume group

```
$ lvm vgscan
$ lvm vgchange -ay
```

 » Now mount your '/' partition

```
$ mount /dev/path/to/root /mnt/sysimage
$ mount -t bind /dev /mnt/sysimage/dev
$ mount -t proc proc /mnt/sysimage/proc
$ mount -t sysfs sysfs /mnt/sysimage/sys
```

 » Now you can chroot to the root fs of your installation if wanted

```
$ chroot /mnt/sysimage /bin/su -
```

(BZ#248022)

 » When installing KVM or Xen guests, always create a partition for the guest disk, or create an LVM volume. Guests should not be installed to block devices or raw disk devices. Anaconda includes disk label duplication avoidance code, but when installing within a VM, it has no visibility to the disk labels elsewhere on the host and cannot detect duplicates.

 If guest filesystems, especially the root filesystem, are directly visible to the host, a host OS reboot may inadvertantly parse the partition table and mount the guest filesystems. This can lead to highly undesirable outcomes. (BZ#518461)

 » The minimum memory requirement when installing all Red Hat Enterprise Linux packages (i.e. '*' or '@everything' is listed in the %packages section of the kickstart file) on a fully virtualized Itanium guest is 768MB. After installation, the memory allocated to the guest can be lowered to the desired amount. (BZ#507891)

 » Upgrading a system using Anaconda is not possible if the system is installed on disks attached using zFCP or iSCSI (unless booted from the disk using a network adaptor with iBFT). Such disks are activated after Anaconda scans for upgradable installations and are not found. To update please use the Red Hat Network with the hosted Web user interface, a Red Hat Network Satellite, the local graphical Updater, or the yum command line. (BZ#494033)

 » Anaconda's graphical installer fails to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. To work around this issue, ensure anaconda uses a higher resolution by passing the parameters **resolution=1024x768** or **resolution=1280x1024**" to the installer using the boot command line.

 » The NFS default for RHEL5 is "locking". Therefore, to mount nfs shares from the %post section of anaconda, use the **mount -o nolock,udp** command to start the locking daemon before using nfs to mount shares. (BZ#426053)

 » If you are using the Virtualized kernel when upgrading from Red Hat Enterprise Linux 5.0 to a later 5.x release, you must reboot after completing the upgrade. You should then boot the system using the updated Virtualized kernel.

The hypervisor ABI changes in an incompatible way between Red Hat Enterprise Linux 5 and 5.1. If you do not boot the system after upgrading from RHEL 5.0 using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)

» When upgrading from Red Hat Enterprise Linux 4.6 to Red Hat Enterprise Linux 5.1 or later, gcc4 may cause the upgrade to fail. As such, you should manually remove the gcc4 package before upgrading. (BZ#432773)

» When provisioning guests during installation, the **RHN tools for guests** option will not be available. When this occurs, the system will require an additional entitlement, separate from the entitlement used by **dom0**.

To prevent the consumption of additional entitlements for guests, install the **rhn-virtualization-common** package manually before attempting to register the system to Red Hat Network. (BZ#431648)

» When installing Red Hat Enterprise Linux 5 on a guest, the guest is configured to explicitly use a temporary installation kernel provided by **dom0**. Once installation finishes, it can then use its own bootloader. However, this can only be achieved by forcing the guest's first reboot to be a shutdown.

As such, when the **Reboot** button appears at the end of the guest installation, clicking it shuts down the guest, but does not reboot it. This is an expected behavior.

Note that when you boot the guest after this it will then use its own bootloader. (BZ#328471)

» Using the **swap --grow** parameter in a kickstart file without setting the **--maxsize** parameter at the same time makes anaconda impose a restriction on the maximum size of the swap partition. It does not allow it to grow to fill the device.

For systems with less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB. (BZ#462734)

» Existing encrypted block devices that contain **vfat** file systems will appear as type **foreign** in the partitioning interface; as such, these devices will not be mounted automatically during system boot. To ensure that such devices are mounted automatically, add an appropriate entry for them to **/etc/fstab**. For details on how to do so, refer to **man fstab**. (BZ#467202)

» when using anaconda's automatic partitioning on an IBM System p partition with multiple harddisks containing different Linux distributions, the anaconda installer may overwrite the bootloaders of the other Linux installations although their harddisks have been unchecked. To work around this, choose manual partitioning during the installation process.(BZ#519795)

The following note applies to PowerPC Architectures:

» The minimum RAM required to install Red Hat Enterprise Linux 5.2 is 1GB; the recommended RAM is 2GB. If a machine has less than 1GB RAM, the installation process may hang.

Further, PowerPC-based machines that have only 1GB of RAM experience significant performance issues under certain RAM-intensive workloads. For a Red Hat Enterprise Linux 5.2 system to perform RAM-intensive processes optimally, 4GB of RAM is recommended. This ensures the system has the same number of physical pages as was available on PowerPC machines with 512MB of RAM running Red Hat Enterprise Linux 4.5 or earlier. (BZ#209165)

The following note applies to s390x Architectures:

» Installation on a machine with existing Linux or non-Linux filesystems on DASD block devices may cause the installer to halt. If this happens, it is necessary to clear out all existing partitions on the DASD devices you want to use and restart the installer. (BZ#289631)

The following note applies to the ia64 Architecture:

- If your system only has 512MB of RAM, attempting to install Red Hat Enterprise Linux 5.4 may fail. To prevent this, perform a base installation first and install all other packages after the installation finishes. (BZ#435271)

5.2. cmirror

The cmirror packages provide user-level utilities for managing cluster mirroring.

- Due to limitations in the cluster infrastructure, cluster mirrors greater than 1.5TB cannot be created with the default region size. If larger mirrors are required, the region size should be increased from its default (512kB), for example:

  ```
  # -R <region_size_in_MiB>
  lvcreate -m1 -L 2T -R 2 -n mirror vol_group
  ```

  Failure to increase the region size will result in the LVM creation process hanging and may cause other LVM commands to hang. (BZ#514814)

5.3. compiz

Compiz is an OpenGL-based window and compositing manager.

- Running **rpmbuild** on the **compiz** source RPM will fail if any KDE or **qt** development packages (for example, **qt-devel**) are installed. This is caused by a bug in the **compiz** configuration script.

  To work around this, remove any KDE or **qt** development packages before attempting to build the **compiz** package from its source RPM. (BZ#444609)

5.4. device-mapper-multipath

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

- By default, the multipathd service starts up before the iscsi service. This provides multipathing support early in the bootup process and is necessary for multipathed ISCSI SAN boot setups. However, once started, the multipathd service adds paths as informed about them by udev. As soon as the multipathd service detects a path that belongs to a multipath device, it creates the device. If the first path that multipathd notices is a passive path, it attempts to make that path active. If it later adds a more optimal path, multipathd activates the more optimal path. In some cases, this can cause a significant overhead during a startup.

  If you are experiencing such performance problems, define the multipathd service to start after the iscsi service. This does not apply to systems where the root device is a multipathed ISCSI device, since it the system would become unbootable. To move the service start time run the following commands:

  ```
  # mv /etc/rc5.d/S06multipathd /etc/rc5.d/S14multipathd
  # mv /etc/rc3.d/S06multipathd /etc/rc3.d/S14multipathd
  ```

  To restore the original start time, run the following command:

  ```
  # chkconfig multipathd resetpriorities
  ```

➤ When using **dm-multipath**, if **features "1 queue_if_no_path"** is specified in **/etc/multipath.conf** then any process that issues I/O will hang until one or more paths are restored.

To avoid this, set **no_path_retry [N]** in **/etc/multipath.conf** (where **[N]** is the number of times the system should retry a path). When you do, remove the **features "1 queue_if_no_path"** option from **/etc/multipath.conf** as well.

If you need to use **"1 queue_if_no_path"** and experience the issue noted here, use **dmsetup** to edit the policy at runtime for a particular LUN (i.e. for which all the paths are unavailable).

To illustrate: run **dmsetup message [device] 0 "fail_if_no_path"**, where **[device]** is the multipath device name (e.g. **mpath2**; do not specify the path) for which you want to change the policy from **"queue_if_no_path"** to **"fail_if_no_path"**. (BZ#419581)

➤ When a LUN is deleted on a configured storage system, the change is not reflected on the host. In such cases, **lvm** commands will hang indefinitely when **dm-multipath** is used, as the LUN has now become *stale*.

To work around this, delete all device and **mpath** link entries in **/etc/lvm/.cache** specific to the stale LUN.

To find out what these entries are, run the following command:

ls -l /dev/mpath | grep [stale LUN]

For example, if **[stale LUN]** is 3600d0230003414f30000203a7bc41a00, the following results may appear:

```
lrwxrwxrwx 1 root root 7 Aug  2 10:33 /3600d0230003414f30000203a7bc41a00 -
> ../dm-4
lrwxrwxrwx 1 root root 7 Aug  2 10:33 /3600d0230003414f30000203a7bc41a00p1
-> ../dm-5
```

This means that 3600d0230003414f30000203a7bc41a00 is mapped to two **mpath** links: **dm-4** and **dm-5**.

As such, the following lines should be deleted from **/etc/lvm/.cache**:

```
/dev/dm-4
/dev/dm-5
/dev/mapper/3600d0230003414f30000203a7bc41a00
/dev/mapper/3600d0230003414f30000203a7bc41a00p1
/dev/mpath/3600d0230003414f30000203a7bc41a00
/dev/mpath/3600d0230003414f30000203a7bc41a00p1
```

(BZ#238421)

➤ Running the **multipath** command with the **-ll** option can cause the command to hang if one of the paths is on a blocking device. Note that the driver does not fail a request after some time if the device does not respond.

This is caused by the cleanup code, which waits until the path checker request either completes or fails. To display the current **multipath** state without hanging the command, use **multipath -l** instead. (BZ#214838)

5.5. dmraid

The dmraid packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

» The **/etc/cron.d/dmeventd-logwatch** crontab file does not specify the user that the logwatch process should be executed by. To work around this issue, the functional portion of this crontab must be changed to:

```
* * * * * root /usr/sbin/logwatch --service dmeventd --range today --
detail med
```

(BZ#516892)

» The installation procedure stores the name of RAID volume and partition in an initscript. When the system boots, dmraid enables the RAID partition (that are named implicitly in the init script. This action functions until the volume and partition names are changed. In these cases, the system may not boot, and the user is given an option to reboot system and start the rebuild procedure in OROM.

OROM changes the name of RAID volume (as seen by dmraid) and dmraid cannot recognize the array identified by previous name stored in initscript. The system no longer boots from RAID partition, since it is not enabled by dmraid. In case of RAID 1 (mirror), the system may be booted from disk that is part of RAID volume. However, dmraid does not allow to active or rebuild the volume which component in mounted.

To work around this issue, do not rebuild the RAID array in OROM. Start the rebuild procedure by dmraid in the operating system, which performs all the steps of rebuilding. dmraid does not change the RAID volume name, therefore the system can be booted from RAID array without the need of init script modification.

To modify init script after OROM has started rebuild:

>> Start the system in rescue mode from the installation disk, skip finding and mounting previous installations.

>> At the command line, find and enable the raid volume that is to be booted from (the RAID volume and partitions will be activated)

```
dmraid -ay isw_effjffhbi_Volume0
```

>> Mount the root partition:

```
mkdir /tmp/raid
mount /dev/mapper/isw_effjffhbi_Volume0p1 /tmp/raid
```

>> Decompress the boot image:

```
mkdir /tmp/raid/tmp/image
cd /tmp/raid/tmp/image
gzip -cd /tmp/raid/boot/inird-2.6.18-155.el5.img | cpio -imd –quiet
```

>> Change the names of the RAID volumes in the initscript to use the new names of RAID:

```
dmraid –ay –I –p –rm_partition "/dev/mapper/isw_effjffhbi_Volume0"
kpartx –a –p p "/dev/mapper/isw_effjffhbi_Volume0"
mkrtootdev –t ext3 –o defaults,ro
/dev/mapper/isw_effjffhbi_Volume0p1
```

> compress and copy initrd image with the modified init script to the boot directory

```
cd /tmp/raid/tmp/image
find . –print | cpio –c –o | gzip -9 > /tmp/raid/boot/inird-2.6.18-
155.el5.img
```

> unmount the raid volume and reboot the system:

```
umount /dev/mapper/isw_effjffhbi_Volume0p1
dmraid -an
```

5.6. dogtail

dogtail is a GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.

> Attempting to run **sniff** may result in an error. This is because some required packages are not installed with **dogtail**. (BZ#435702)
>
> To prevent this from occurring, install the following packages manually:
>
> - librsvg2
>
> - ghostscript-fonts
>
> - pygtk2-libglade

5.7. firstboot

The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

The following notes apply to s390x Architectures:

> The *IBM System z* does not provide a traditional Unix-style physical console. As such, Red Hat Enterprise Linux 5.2 for the *IBM System z* does not support the *firstboot* functionality during initial program load.
>
> To properly initialize setup for Red Hat Enterprise Linux 5.2 on the *IBM System z*, run the following commands after installation:
>
> - **/usr/bin/setup** — provided by the **setuptool** package.
>
> - **/usr/bin/rhn_register** — provided by the **rhn-setup** package.
>
> (BZ#217921)

5.8. gfs2-utils

The gfs2-utils packages provide the user-level tools necessary to mount, create, maintain and test GFS2 file systems.

If gfs2 is used as the root file system, the first boot attempt will fail with the error message "**fsck.gfs2: invalid option -- a**". To work around this issue:

1. Enter the root password when prompted

2. Mount the root file system manually:

```
mount -o remount,rw /dev/VolGroup00/LogVol00 /
```

3. Edit the /etc/fstab file from:

```
/dev/VolGroup00/LogVol00 / gfs2 defaults 1 1
```

to

```
/dev/VolGroup00/LogVol00 / gfs2 defaults 1 0
```

4. Reboot the system.

> **Important**
>
> Note, however that using GFS2 as the root filesystem is unsupported.

5.9. gnome-volume-manager

The GNOME Volume Manager monitors volume-related events and responds with user-specified policy. The GNOME Volume Manager can automount hot-plugged drives, automount inserted removable media, autorun programs, automatically play audio CDs and video DVDs, and automatically import photos from a digital camera.

» Removable storage devices (such as CDs and DVDs) do not automatically mount when you are logged in as root. As such, you will need to manually mount the device through the graphical file manager. (BZ#209362)

Alternatively, you can run the following command to mount a device to **/media**:

```
mount /dev/[device name] /media
```

5.10. initscripts

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

» On systems with more than two encrypted block devices, anaconda has a option to provide a global passphrase. The init scripts, however, do not support this feature. When booting the system, entering each individual passphrase for all encrypted devices will be required. (BZ#464895)

» Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5.3. (BZ#223446, BZ#210136)

5.11. iscsi-initiator-utils

5.11. iscsi-initiator-utils

The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

≫ iSCSI iface binding is not supported during install or boot. The initiator only supports the ability to log into target portals using the default behavior where the initiator uses the network routing table to decide which NIC to use.

To work around this limitation, booting or installation can be done using the default behavior. After the iscs and iscsid services start, the iscsi service can log into the target using iSCSI iface binding. This however, will leave an extra session using the default behavior, and it has to be manually logged out using the following command:

```
iscsiadm -m node -T target -p ip -I default -u
```

(BZ#500273)

5.12. kernel-xen

≫ A virtual function NIC might fail to get an IP address after several iterations of creating and destroying a guest. To work around this issue, diable interrupt remapping in the system BIOS for **kernel-xen**.

≫ On Intel platforms with VT-d enabled, the frame buffer of a fully-virtualized Xen guest with 4GB or more RAM might not be displayed correctly. To work around this issue, create the guest with additional memory (e.g. 2GB more than desired), close the guest, then recreate the guest with the desired amount of RAM. (BZ#511398)

≫ Xen guests will not boot using configurations that bind multiple virtualized CPUs to a single CPU. (BZ#570056)

≫ The Xen hypervisor will not start when booting from an iSCSI disk. To work around this issue, disable the Xen hypervisor's EDD feature with the "edd=off" kernel parameter. For example:

```
kernel /xen.gz edd=off
```

(BZ#568336)

≫ blktap may not function as expected, resulting in slow disk I/O causing the guest to operate slowly also. To work around this issue guests should be installed using a physical disk (i.e. a real partition or a logical volume). (BZ#545692)

≫ When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.6 Xen, the domain may fail to start if more than 2047MB of memory is configured for the domain. To work around this issue, pass the "**nogbpages**" parameter on the guest kernel command-line. (BZ#502826)

≫ Boot parameters are required to enable SR/IOV Virtual Function devices. SR/IOV Virtual Function devices can only be accessed if the parameter pci_pt_e820_access=on is added to the boot stanza in the /boot/grub/grub.conf file. For example:

```
title Red Hat Enterprise Linux Server (2.6.18-152.el5xen)
        root (hd0,1)
        kernel /xen.gz-2.6.18-152.el5 com1=115200,8n1 console=com1
iommu=1
```

```
        module /vmlinuz-2.6.18-152.el5xen ro root=LABEL=/
console=ttyS0,115200
pci_pt_e820_access=on
```

This enables the MMCONF access method for the PCI configuration space, a requirement for VF device support

» When using Single Root I/O Virtualization (SR-IOV) devices under Xen, a single Hardware Virtual Machine (HVM) guest is limited to 12 Virtual Function (VF) assignments. (BZ#511403)

» Diskette drive media will not be accessible when using the virtualized kernel. To work around this, use a USB-attached diskette drive instead.

   Note that diskette drive media works well with other non-virtualized kernels. (BZ#401081)

» Formatting a disk when running **Windows 2008** or **Windows Vista** as a guest can crash when the guest has been booted with multiple virtual CPUs. To work around this, boot the guest with a single virtual CPU when formatting. (BZ#441627)

» Fully virtualized guests cannot correct for time lost due to the domain being paused and unpaused. Being able to correctly track the time across pause and unpause events is one of the advantages of paravirtualized kernels. This issue is being addressed upstream with replaceable timers, so fully virtualized guests will have paravirtualized timers. Currently, this code is under development upstream and should be available in later versions of Red Hat Enterprise Linux. (BZ#422531)

The following note applies to x86_64 Architectures:

» Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.2 may render existing Red Hat Enterprise Linux 4.5 SMP paravirtualized guests unbootable. This is more likely to occur when the host system has more than 4GB of RAM.

   To work around this, boot each Red Hat Enterprise Linux 4.5 guest in single CPU mode and upgrade its kernel to the latest version (for Red Hat Enterprise Linux 4.5.z). (BZ#253087, BZ#251013)

The following note applies to the ia64 Architecture:

» On some *Itanium* systems configured for console output to VGA, the **dom0** virtualized kernel may fail to boot. This is because the virtualized kernel failed to properly detect the default console device from the *Extensible Firmware Interface* (EFI) settings.

   When this occurs, add the boot parameter **console=tty** to the kernel boot options in **/boot/efi/elilo.conf**. (BZ#249076)

» On some *Itanium* systems (such as the *Hitachi Cold Fusion 3e*), the serial port cannot be detected in **dom0** when VGA is enabled by the EFI Maintenance Manager. As such, you need to supply the following serial port information to the **dom0** kernel:

   ▫ Speed in bits/second

   ▫ Number of data bits

   ▫ Parity

   ▫ **io_base** address

These details must be specified in the **append=** line of the **dom0** kernel in **/boot/efi/elilo.conf**. For example:

```
append="com1=19200,8n1,0x3f8 -- quiet rhgb console=tty0
console=ttyS0,19200n8"
```

In this example, **com1** is the serial port, **19200** is the speed (in bits/second), **8n1** specifies the number of data bits/parity settings, and **0x3f8** is the **io_base** address. [(BZ#433771)](#)

» Virtualization does not work on some architectures that use Non-Uniform Memory Access (NUMA). As such, installing the virtualized kernel on systems that use NUMA will result in a boot failure.

Some installation numbers install the virtualized kernel by default. If you have such an installation number and your system uses NUMA and does not work with kernel-xen, deselect the Virtualization option during installation. [(BZ#293071)](#)

5.13. kernel

The Kernel

» NUMA class systems should not be booted with a single memory node configuration. Configuration of single node NUMA systems will result in contention for the memory resources on all of the non-local memory nodes. As only one node will have local memory the CPUs on that single node will starve the remaining CPUs for memory allocations, locks, and any kernel data structure access. This contention will lead to the "CPU#n stuck for 10s!" error messages. This configuration can also result in NMI watchdog timeout panics if a spinlock is acquired via spinlock_irq() and held for more than 60 seconds. The system can also hang for indeterminate lengths of time

To minimize this problem NUMA class systems need to have their memory evenly distributed between nodes. NUMA information can be obtained from dmesg output as well as from the numastat command.

» When upgrading from Red Hat Enterprise Linux 5.0, 5.1 or 5.2 to more recent releases, the gfs2-kmod may still be installed on the system. This package must be manually removed or it will override the (newer) version of GFS2 which is built into the kernel. Do not install the **gfs2-kmod** package on later versions of Red Hat Enterprise Linux. **gfs2-kmod** is not required since GFS2 is built into the kernel from 5.3 onwards. The content of the gfs2-kmod package is considered a Technology Preview of GFS2, and has not received any updates since Red Hat Enterprise Linux 5.3 was released.

Note that this note only applies to GFS2 and not to GFS, for which the gfs-kmod package continues to be the only method of obtaining the required kernel module.

» Issues might be encountered on a system with 8Gb/s LPe1200x HBAs and firmware version 2.00a3 when the Red Hat Enterprise Linux 5.6 kernel is used with the in-box LPFC driver. Such issues include loss of LUNs and/or fiber channel host hangs during fabric faults with multipathing.

To work around these issues, it is recommended to either:

▫ Downgrade the firmware revision of the 8Gb/s LPe1200x HBA to revision [1.11a5](#), or

▫ Modify the LPFC driver's **lpfc_enable_npiv** module parameter to zero.

When loading the LPFC driver from the initrd image (i.e. at system boot time), add the line

```
options lpfc_enable_npiv=0
```

to **/etc/modprobe.conf** and re-build the initrd image.

When loading the LPFC driver dynamically, include the **lpfc_enable_npiv=0** option in the insmod or modprobe command line.

For additional information on how to set the LPFC driver module parameters, refer to the Emulex Drivers for Linux User Manual.

▷ If AMD IOMMU is enabled in BIOS on ProLiant DL165 G7 systems, the system will reboot automatically when IOMMU attempts to initalize. To work around this issue, either disable IOMMU, or update the BIOS to version **2010.09.06** or later.

▷ As of Red Hat Enterprise Linux 5.6 the ext4 file system is fully supported. However, provisioning ext4 file systems with the anaconda installer is not supported, and ext4 file systems need to be provisioned manually after the installation.

▷ In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by other clients, or by non-NFS users of the server. An application on a client may then be able to open the file at its old pathname (and read old cached data from it, and perform read locks on it), long after the file no longer exists at that pathname on the server.

To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing **0** to **/proc/sys/fs/leases-enable** (ideally on boot, before the nfs server is started). This change prevents NFSv4 delegations from being given out, restore correctness at the expense of some performance.

▷ Some laptops may generate continuous events in response to the lid being shut. Consequently, the gnome-power-manager utility will consume CPU resources as it responds to each event.

▷ A kernel panic may be triggered by the lpfc driver when multiple Emulex OneConnect Universal Converged Network Adapter initiators are included in the same Storage Area Network (SAN) zone. Typically, this kernel panic will present after a cable is pulled or one of the systems is rebooted. To work around this issue, configure the SAN to use single initiator zoning. (BZ#574858)

▷ If a Huawei USB modem is unplugged from a system, the device may not be detected when it is attached again. To work around this issue, the usbserial and usb-storage driver modules need to be reloaded, allowing the system to detect the device. Alternatively, the if the system is rebooted, the modem will be detected also. (BZ#517454)

▷ Memory on-line is not currently supported with the Boxboro-EX platform. (BZ#515299)

▷ Unloading a PF (SR-IOV Physical function) driver from a host when a guest is using a VF (virtual function) from that device can cause a host crash. A PF driver for an SR-IOV device should not be unloaded until after all guest virtual machines with assigned VFs from that SR-IOV device have terminated. (BZ#514360)

▷ Data corruption on NFS filesystems might be encountered on network adapters without support for error-correcting code (ECC) memory that also have TCP segmentation offloading (TSO) enabled in the driver. Note: data that might be corrupted by the sender still passes the checksum performed by the IP stack of the receiving machine A possible work around to this issue is to disable TSO on network adapters that do not support ECC memory. BZ#504811

▷ After installation, a System z machine with a large number of memory and CPUs (e.g. 16 CPU's and 200GB of memory) might may fail to IPL. To work around this issue, change the line

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img
```

to

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img,0x02000000
```

The command **zipl -V** should now show **0x02000000** as the starting address for the inital RAM disk (initrd). Stop the logigal partiton (LPAR), and then manually increase the the storage size of the LPAR.

❊ On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run

```
chkconfig --del iscsi
chkconfig --del iscsid
```

On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.

❊ In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO_PROCESS" does not set the priority of child threads. (BZ#472251)

❊ Physical CPUs cannot be safely placed offline or online when the 'kvm_intel' or 'kvm_amd' module is loaded. This precludes physical CPU offline and online operations when KVM guests that utilize processor virtualization support are running. It also precludes physical CPU offline and online operations without KVM guests running when the 'kvm_intel' or 'kvm_amd' module is simply loaded and not being used.

If the kmod-kvm package is installed, the 'kvm_intel' or 'kvm_amd' module automatically loads during boot on some systems. If a physical CPU is placed offline while the 'kvm_intel' or 'kvm_amd' module is loaded a subsequent attempt to online that CPU may fail with an I/O error.

To work around this issue, unload the 'kvm_intel' or 'kvm_amd' before performing physical CPU hot-plug operations. It may be necessary to shut down KVM guests before the 'kvm_intel' or 'kvm_amd' will successfully unload.

For example, to offline a physical CPU 6 on an Intel based system:

```
# rmmod kvm_intel
# echo 0 > /sys/devices/system/cpu/cpu6/online
# modprobe kvm_intel
```

(BZ#515557)

❊ A change to the cciss driver in Red Hat Enterprise Linux 5.4 made it incompatible with the "echo disk > /sys/power/state" suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

```
Stopping tasks:
==================================================================
 stopping tasks timed out after 20 seconds (1 tasks remaining):
  cciss_scan00
Restarting tasks...<6> Strange, cciss_scan00 not stopped
 done
```

(BZ#513472)

❊ The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (anaconda) to refresh the CD. (BZ#510632)

❧ Applications attempting to **malloc** memory approximately larger than the size of the physical memory on the node on a NUMA system may hang or appear to stall. This issue may occur on a NUMA system where the remote memory distance, as defined in SLIT, is greater than 20 and RAM based filesystem like **tmpfs** or **ramfs** is mounted.

To work around this issue, unmount all RAM based filesystems (i.e. tmpfs or ramfs). If unmounting the RAM based filesystems is not possible, modify the application to allocate lesser memory. Finally, if modifying the application is not possible, disable NUMA memory reclaim by running:

```
sysctl vm.zone_reclaim_mode=0
```

> **Important**
>
> Turning NUMA reclaim negatively effects the overall throughput of the system.

(BZ#507360)

❧ Configuring IRQ SMP affinity has no effect on some devices that use message signalled interrupts (MSI) with no MSI per-vector masking capability. Examples of such devices include *Broadcom NetXtreme* Ethernet devices that use the **bnx2** driver.

If you need to configure IRQ affinity for such a device, disable MSI by creating a file in **/etc/modprobe.d/** containing the following line:

```
options bnx2 disable_msi=1
```

Alternatively, you can disable MSI completely using the kernel boot parameter **pci=nomsi**. (BZ#432451)

❧ The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)

❧ *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To avoid this, boot the system with the argument **acpi_sleep=s3_bios**. (BZ#439006)

❧ The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

Because of this limitation, successive resets (via consecutive **ifdown**/**ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. (BZ#276891)

❧ Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). (BZ#213262)

❧ Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. (BZ#251934)

» The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

To work around this, add a script named **hal-system-power-suspend** to **/usr/share/hal/scripts/** containing the following lines:

```
chvt 1
radeontool light off
radeontool dac off
```

This script will ensure that the *IBM T41* laptop enters **Suspend Mode** properly. To ensure that the system resumes normal operations properly, add the script **restore-after-standby** to the same directory as well, containing the following lines:

```
radeontool dac on
radeontool light on
chvt 7
```

(BZ#227496)

» If the **edac** module is loaded, BIOS memory reporting will not work. This is because the **edac** module clears the register that the BIOS uses for reporting memory errors.

The current Red Hat Enterprise Linux Driver Update Model instructs the kernel to load all available modules (including the **edac** module) by default. If you wish to ensure BIOS memory reporting on your system, you need to manually blacklist the **edac** modules. To do so, add the following lines to **/etc/modprobe.conf**:

```
blacklist edac_mc
blacklist i5000_edac
blacklist i3000_edac
blacklist e752x_edac
```

(BZ#441329)

» Due to outstanding driver issues with hardware encryption acceleration, users of Intel WiFi Link 4965, 5100, 5150, 5300, and 5350 wireless cards are advised to disable hardware accelerated encryption using module parameters. Failure to do so may result in the inability to connect to Wired Equivalent Privacy (WEP) protected wireless networks after connecting to WiFi Protected Access (WPA) protected wireless networks.

To do so, add the following options to **/etc/modprobe.conf**:

```
alias wlan0 iwlagn
options iwlagn swcrypto50=1 swcrypto=1
```

(where wlan0 is the default interface name of the first Intel WiFi Link device)

[(BZ#468967)](#)

The following note applies to PowerPC Architectures:

» The size of the PPC kernel image is too large for OpenFirmware to support. Consequently, network booting will fail, resulting in the following error message:

```
Please wait, loading kernel...
/pci@8000000f8000000/ide@4,1/disk@0:2,vmlinux-anaconda: No such file or
directory
boot:
```

To work around this:

» Boot to the OpenFirmware prompt, by pressing the '8' key when the IBM splash screen is displayed.

» Run the following command:

```
setenv real-base 2000000
```

» Boot into System Managment Services (SMS) with the command:

```
0> dev /packages/gui obe
```

[(BZ#462663)](#)

5.14. kexec-tools

kexec-tools provides the /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature

» Executing **kdump** on an *IBM Bladecenter QS21* or *QS22* configured with NFS root will fail. To avoid this, specify an NFS dump target in **/etc/kdump.conf**. [(BZ#368981)](#)

» Some **forcedeth** based devices may encounter difficulty accessing memory above 4GB during operation in a **kdump** kernel. To work around this issue, add the following line to the **/etc/sysconfig/kdump** file:

```
KDUMP_COMMANDLINE_APPEND="dma_64bit=0"
```

This work around prevents the forcedeth network driver from using high memory resources in the kdump kernel, allowing the network to function properly.

» The system may not successfully reboot into a **kexec**/**kdump** kernel if X is running and using a driver other than *vesa*. This problem only exists with *ATI Rage XL* graphics chipsets.

If X is running on a system equipped with *ATI Rage XL*, ensure that it is using the *vesa* driver in order to successfully reboot into a **kexec**/**kdump** kernel. [(BZ#221656)](#)

❧ **kdump** now serializes drive creation registration with the rest of the **kdump** process. Consequently, **kdump** may hang waiting for IDE drives to be initialized. In these cases, it is recommended that IDE disks not be used with **kdump**. (BZ#473852)

❧ It is possible in rare circumstances, for **makedumpfile** to produce erroneous results but not have them reported. This is due to the fact that **makedumpfile** processes its output data through a pipeline consisting of several stages. If **makedumpfile** fails, the other stages will still succeed, effectively masking the failure. Should a vmcore appear corrupt, and makedumpfile is in use, it is recommended that the core be recorded without makedumpfile and a bug be reported. (BZ#475487)

❧ kdump now restarts when CPUs or DIMMs are hot-added to a system. If multiple items are added at the same time, several sequential restarts may be encountered. This behavior is intentional, as it minimizes the time-frame where a crash may occur while memory or processors are not being tracked by kdump. (BZ#474409)

The following note applies to ia64 Architecture:

❧ Some *Itanium* systems cannot properly produce console output from the **kexec purgatory** code. This code contains instructions for backing up the first 640k of memory after a crash.

While **purgatory** console output can be useful in diagnosing problems, it is not needed for **kdump** to properly function. As such, if your *Itanium* system resets during a **kdump** operation, disable console output in **purgatory** by adding **--noio** to the **KEXEC_ARGS** variable in **/etc/sysconfig/kdump**. (BZ#436426)

5.15. kvm

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the libvirt virtualization tools (virt-manager and virsh).

❧ Booting a Linux guest causes 1.5 to 2 second time drift from the host time when the default hwclock service starts. It is recommended to disable the hwclock service. Alternatively, enable the ntp service so ntp can correct the time once the ntp service starts.

❧ By default, KVM virtual machines created in Red Hat Enterprise Linux 5.6 have a virtual Realtek 8139 (rtl8139) network interface controller (NIC). The rtl8139 virtual NIC works fine in most environments, but may suffer from performance degradation issues on some networks for example, a 10 GigE (10 Gigabit Ethernet) network.

One workaround for this issue is switch to a different type of virtual NIC, for example, Intel PRO/1000 (e1000) or virtio (a virtual I/O driver for Linux that can talk to the hypervisor).

To switch to e1000:

   ❧ Shutdown the guest OS

   ❧ Edit the guest OS definition with the command-line tool virsh:

   ```
   virsh edit GUEST
   ```

   ❧ Locate the network interface section and add a model line as shown:

```
<interface type='network'>
 ...
 <model type='e1000' />
</interface>
```

» Save the changes and exit the text editor

» Restart the guest OS

Alternatively, if you're having trouble installing the OS on the virtual machine because of the rtl8139 NIC (for example, because you're installing the OS over the network), you can create a virtual machine from scratch with an e1000 NIC. This method requires you to have at least one virtual machine already created (possibly installed from CD or DVD) to use as a template.

» Create an XML template from an existing virtual machine:

```
virsh dumpxml GUEST > /tmp/guest.xml
```

» Copy and edit the XML file and update the unique fields: virtual machine name, UUID, disk image, MAC address, etc. NOTE: you can delete the UUID and MAC address lines and virsh will generate a UUID and MAC address.

```
cp /tmp/guest.xml /tmp/new-guest.xml
vi /tmp/new-guest.xml
```

» Locate the network interface section and add a model line as shown:

```
<interface type='network'>
 ...
 <model type='e1000' />
</interface>
```

» Create the new virtual machine:

```
virsh define /tmp/new-guest.xml
virsh start new-guest
```

» Currently, KVM cannot disable virtualization extensions on a CPU while it is being taken down. Consequently, suspending a host running KVM-based virtual machines may cause the host to crash. (BZ#509809)

» The KSM module shipped in this release is a different version from the KSM module found on the latest upstream kernel versions. Newer features, such as exporting statistics on the /sys filesystem, that are implemented upstream are not in the version shipped in this release.

» The mute button in the audio control panel on a Windows virtual machine does not mute the sound. BZ#482570

» When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. (BZ#516029)

» the application binary interface (ABI) between the KVM userspace (e.g. qemu-kvm) and the KVM kernel modules may change in future updates. Using the latest upstream qemu-kvm package is unsupported due to ABI differences. (BZ#515549)

❯ Devices using the qlge driver cannot be assigned to a KVM guest using KVM's PCI Device Driver assignment. (BZ#507689)

❯ the use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)

❯ 64-bit versions of Windows 7 do not have support for the AC'97 Audio Codec. Consequently, the virtualized sound device Windows 7 kvm guests will not function. (BZ#563122)

❯ Hotplugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)

❯ Windows 2003 32-bit guests with more than 4GB of RAM may crash on reboot with the default qemu-kvm CPU settings. To work around this issue, configure a different CPU model on the management interface. (BZ#516762)

❯ The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-203.el5. If kmod-kvm is updated and an older kernel is kept installed, error messages similar to the following will be returned if attempting to install these modules on older kernels:

```
WARNING: /lib/modules/2.6.18-194.el5/weak-updates/kmod-kvm/ksm.ko needs
unknown symbol kvm_ksm_spte_count
```

(BZ#509361)

❯ The KVM modules available in the **kmod-kvm** package are loaded automatically at boot time if the kmod-kvm package is installed. To make these KVM modules available after installing the **kmod-kvm** package the system either needs to be rebooted or the modules can be loaded manually by running the **/etc/sysconfig/modules/kvm.modules** script. (BZ#501543)

❯ Some Linux-based guests that use virtio virtual block devices may abort during installation, returning the error message: unhandled vm exit: 0x31 vcpu_id 0 To work around this issue, consider utilizing a different interface (other than virtio) for the guest virtual disk. (BZ#518081)

❯ The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (ie. Remote Installation Services (RIS) or Windows Deployment Services (WDS)). (BZ#497692)

❯ The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)

  ◦ smb user directories

  ◦ scsi emulation

  ◦ "isapc" machine type

  ◦ nested KVM guests

  ◦ usb mass storage device emulation

  ◦ usb wacom tablet emulation

  ◦ usb serial emulation

  ◦ usb network emulation

  ◦ usb bluetooth emulation

  ◦ device emulation for vmware drivers

- sb16, es1370, and ac97 sound card emulation

- bluetooth emulation

5.16. mesa

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

The following note applies to x86_64 Architectures:

- On an *IBM T61* laptop, Red Hat recommends that you refrain from clicking the **glxgears** window (when **glxgears** is run). Doing so can lock the system.

  To prevent this from occurring, disable the tiling feature. To do so, add the following line in the **Device** section of **/etc/X11/xorg.conf**:

  ```
  Option "Tiling" "0"
  ```

  (BZ#444508)

5.17. mkinitrd

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

- When using an encrypted device, the following error message may be reported during bootup:

  ```
  insmod: error inserting '/lib/aes_generic.ko': -1 File exists
  ```

  This message can safely be ignored. (BZ#466296)

- Installation using a Multiple Device (MD) RAID on top of multipath will result in a machine that cannot boot. Multipath to Storage Area Network (SAN) devices which provide RAID internally are not affected. (BZ#467469)

The following note applies to s390x Architectures:

- When installing Red Hat Enterprise Linux 5.4, the following errors may be returned in **install.log**:

  ```
  Installing kernel-2.6.18-158.el5.s390x
  cp: cannot stat `/sbin/dmraid.static': No such file or directory
  ```

  This message can be safely ignored.

- iSCSI root devices do not function correctly if used over an IPv6 network connection. While the installation will appear to succeed, the system will fail to find the root filesystem during the first boot. (BZ#529636)

5.18. openib

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP hardware diagnostic utilities, the Infiniband fabric management daemon, Infiniband/iWARP kernel module loader, and libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for

Infiniband/iWARP/RDMA hardware support.

The following note applies to the ia64 Architectures:

◈ Running **perftest** will fail if different CPU speeds are detected. As such, you should disable CPU speed scaling before running **perftest**. (BZ#433659)

5.19. openmpi

Open MPI, MVAPICH, and MVAPICH2 are all competing implementations of the Message Passing Interface (MPI) standard. MVAPICH implements version 1 of the MPI standard, while Open MPI and MVAPICH2 both implement the later, version 2 of the MPI standard.

◈ **mvapich** and **mvapich2** in Red Hat Enterprise Linux 5 are compiled to support only *InfiniBand/iWARP* interconnects. Consequently, they will not run over ethernet or other network interconnects. (BZ#466390)

◈ When upgrading openmpi using yum, the following warning may be returned:

```
cannot open `/tmp/openmpi-upgrade-version.*' for reading: No such file or
directory
```

The message is harmless and can be safely ignored. (BZ#463919)

◈ A bug in previous versions of **openmpi** and **lam** may prevent you from upgrading these packages. This bug manifests in the following error (when attempting to upgrade **openmpi** or **lam**:

```
error: %preun(openmpi-[version]) scriptlet failed, exit status 2
```

As such, you need to manually remove older versions of **openmpi** and **lam** in order to install their latest versions. To do so, use the following **rpm** command:

rpm -qa | grep '^openmpi-\|^lam-' | xargs rpm -e --noscripts --allmatches
(BZ#433841)

5.20. pm-utils

The pm-utils package contains utilities and scripts for power management.

◈ nVidia video devices on laptops can not be correctly re-initialized using VESA in Red Hat Enterprise Linux 5. Attempting to do so results in a black laptop screen after resume from suspend.

5.21. qspice

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows users to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

◈ Occasionally, the video compression algorithm used by SPICE starts when the guest is accessing text instead of video or moving content. This causes the text to appear blurry or difficult to read. (BZ#493375)

5.22. systemtap

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows

users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other evens that occur in both kernel-space and user-space.

The following are the Known Issues that apply to the systemtap package in Red Hat Enterprise Linux 5.4

» Running some user-space probe test cases provided by the **systemtap-testsuite** package fail with an **Unknown symbol in module** error on some architectures. These test cases include (but are not limited to):

- **systemtap.base/uprobes.exp**

- **systemtap.base/bz10078.exp**

- **systemtap.base/bz6850.exp**

- **systemtap.base/bz5274.exp**

Because of a known bug in the latest SystemTap update, new SystemTap installations do not unload old versions of the **uprobes.ko** module. Some updated user-space probe tests provided by the systemtap-testsuite package use symbols available only in the latest **uprobes.ko** module (also provided by the latest SystemTap update). As such, running these user-space probe tests result in the error mentioned earlier.

If you encounter this error, simply run **rmmod uprobes** to manually remove the older **uprobes.ko** module before running the user-space probe test again.(BZ#499677)

» SystemTap currently uses GCC to probe user-space events. GCC is, however, unable to provide debuggers with precise location list information for parameters. In some cases, GCC also fails to provide visibility on some parameters. As a consequence, SystemTap scripts that probe user-space may return inaccurate readings. (BZ#239065)

5.23. vdsm22

» If an ISO domain includes a CD-ROM image that uses spaces or other special shell characters, a virtual machine that is configured to boot with the image attached will fail to start. To avoid this, use only alphanumeric names for image names.

5.24. virtio-win

VirtIO para-virtualized Windows(R) drivers for 32-bit and 64-bit Windows (R) guests.

» Low performance with UDP messages larger than 1024 is a known Microsoft issue: http://support.microsoft.com/default.aspx/kb/235257. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.

(BZ#496592)

» Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally. BZ#513160

5.25. xorg-x11-drv-i810

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

❧ Running a screensaver or resuming a suspended laptop with an external monitor attached may result in a blank screen or a brief flash followed by a blank screen. If this occurs with the screensaver, the prompt for your password is being obscured, the password can still be entered blindly to get back to the desktop. To work around this issue, physically disconnect the external monitor and then press the video hotkey (usually Fn-F7) to rescan the available outputs, before suspending the laptop.

The following notes apply to x86_64 Architectures:

❧ If your system uses an *Intel 945GM* graphics card, do not use the `i810` driver. You should use the default `intel` driver instead. (BZ#468218)

❧ On dual-GPU laptops, if one of the graphics chips is Intel-based, the Intel graphics mode cannot drive any external digital connections (including HDMI, DVI, and DisplayPort). This is a hardware limitation of the Intel GPU. If you require external digital connections, configure the system to use the discrete graphics chip (in the BIOS). (BZ#468259)

5.26. xorg-x11-drv-nv

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

❧ Improvements have been made to the 'nv' driver, enhancing suspend and resume support on some systems equipped with nVidia GeForce 8000 and 9000 series devices. Due to technical limitations, this will not enable suspend/resume on all hardware. (BZ#414971)

❧ The nv driver for NVIDIA graphics devices does not fully support the DisplayPort digital display interface. Connections from DisplayPort video devices to DisplayPort monitors are unsupported by the nv driver. Internal laptop and notebook displays that use Embedded DisplayPort (eDP) are also unsupported. Other connections, such as VGA, DVI, HDMI and the use of DisplayPort to DVI adapters are supported by the nv driver. To work around this limitation, it is recommended that the "vesa" driver be used. (BZ#566228)

The following note applies to x86_64 Architectures:

❧ Some machines that use *NVIDIA* graphics cards may display corrupted graphics or fonts when using the graphical installer or during a graphical login. To work around this, switch to a virtual console and back to the original X host. (BZ#222737, BZ#221789)

5.27. xorg-x11-drv-vesa

xorg-x11-drv-vesa is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

The following note applies to x86 Architectures:

❧ When running the bare-metal (non-Virtualized) kernel, the X server may not be able to retrieve `EDID` information from the monitor. When this occurs, the graphics driver will be unable to display resolutions highers than 800x600.

To work around this, add the following line to the `ServerLayout` section of `/etc/X11/xorg.conf`:

```
Option "Int10Backend" "x86emu"
```

(BZ#236416)

5.28. yaboot

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

‣ If the string that represents the path to kernel (or ramdisk) is greater than 63 characters, network booting an IBM Power5 series system may result in the following error:

```
FINAL File Size = 8948021 bytes.
load-base=0x4000
real-base=0xc00000
DEFAULT CATCH!, exception-handler=fff00300
```

The firmware for IBM Power6 and IBM Power7 systems contains a fix for this issue. (BZ#550086)

5.29. xen

‣ There are only 2 virtual slots (00:06.0 and 00:07.0) that are available for hotplug support in a virtual guest.

‣ As of Red Hat Enterprise Linux 5.4, PCI devices connected to a single PCI-PCI bridge can no longer be assigned to different PV guests. If the old, unsafe behaviour is required, disable pci-dev-assign-strict-check in /etc/xen/xend-config.sxp. (BZ#508310)

‣ In live migrations of paravirtualized guests, time-dependent guest processes may function improperly if the corresponding hosts' (dom0) times are not synchronized. Use NTP to synchronize system times for all corresponding hosts before migration. (BZ#426861)

‣ When running x86_64 Xen, it is recommended to set dom0-min-mem in /etc/xen/xend-config.sxp to a value of 1024 or higher. Lower values may cause the dom0 to run out of memory, resulting in poor performance or out-of-memory situations. (BZ#519492)

‣ The Red Hat Enterprise Linux 3 kernel does not include SWIOTLB support. SWIOTLB support is required for Red Hat Enterprise Linux 3 guests to support more than 4GB of memory on AMD Opteron and Athlon-64 processors. Consequently, Red Hat Enterprise Linux 3 guests are limited to 4GB of memory on AMD processors. (BZ#504187)

‣ When setting up interface bonding on **dom0**, the default **network-bridge** script may cause bonded network interfaces to alternately switch between **unavailable** and **available**. This occurrence is commonly known as *flapping*.

To prevent this, replace the standard **network-script** line in **/etc/xen/xend-config.sxp** with the following line:

```
(network-script network-bridge-bonding netdev=bond0)
```

Doing so will disable the *netloop* device, which prevents Address Resolution Protocol (ARP) monitoring from failing during the address transfer process. (BZ#429154, BZ#429154)

‣ The Hypervisor outputs messages regarding attempts by any guest to write to an MSR. Such messages contain the statement **Domain attempted WRMSR**. These messages can be safely ignored; furthermore, they are rate limited and should pose no performance risk. (BZ#477647)

The following note applies to x86_64 Architectures:

▷ Installing Red Hat Enterprise Linux 3.9 on a fully virtualized guest may be extremely slow. In addition, booting up the guest after installation may result in **`hda: lost interrupt`** errors.

To avoid this bootup error, configure the guest to use the SMP kernel. (BZ#249521)

Appendix A. Package Manifest

This appendix is a list of all package changes since the release of Red Hat Enterprise Linux 5.4

A.1. Client

A.1.1. Added Packages

bind97-9.7.0-6.P2.el5

- ❧ Group: System Environment/Daemons

- ❧ Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server

- ❧ Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

c-ares-1.6.0-5.el5

- ❧ Group: System Environment/Libraries

- ❧ Summary: A library that performs asynchronous DNS operations

- ❧ Description: c-ares is a C library that performs DNS requests and name resolves asynchronously. c-ares is a fork of the library named 'ares', written by Greg Hudson at MIT.

certmonger-0.30-4.el5

- ❧ Group: System Environment/Daemons

- ❧ Summary: Certificate status monitor and PKI enrollment client

- ❧ Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.

dropwatch-1.2-2.el5

- ❧ Group: Applications/System

- ❧ Summary: Kernel dropped packet monitor

- ❧ Description: dropwatch is an utility to interface to the kernel to monitor for dropped network packets.

ebtables-2.0.9-5.el5

- ❧ Group: System Environment/Base

- ❧ Summary: Ethernet Bridge frame table administration tool

- ❧ Description: Ethernet bridge tables is a firewalling tool to transparently filter network traffic passing a bridge. The filtering possibilities are limited to link layer filtering and some basic filtering on higher network layers. This tool is the userspace control for the bridge and ebtables kernel components. The ebtables tool can be used together with the other Linux filtering tools, like iptables. There are no known incompatibility issues.

gsl-1.13-3.el5

- Group: System Environment/Libraries

- Summary: The GNU Scientific Library for numerical analysis

- Description: The GNU Scientific Library (GSL) is a collection of routines for numerical analysis, written in C.

hplip3-3.9.8-11.el5

- Group: System Environment/Daemons

- Summary: HP Linux Imaging and Printing Project

- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.

ipa-client-2.0-10.el5

- Group: System Environment/Base

- Summary: IPA authentication for use on clients

- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).

ipa-gothic-fonts-003.02-3.1.el5

- Group: User Interface/X

- Summary: Japanese Gothic-typeface OpenType font by IPA

- Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Gothic (sans-serif) style font.

ipa-mincho-fonts-003.02-2.1.el5

- Group: User Interface/X

- Summary: Japanese Mincho-typeface OpenType font by IPA

- Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Mincho style font.

ipa-pgothic-fonts-003.02-3.1.el5

- Group: User Interface/X

- Summary: Japanese Proportional Gothic-typeface OpenType font by IPA

- Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Proportional Gothic (sans-serif) style font.

ipa-pmincho-fonts-003.02-2.1.el5

- Group: User Interface/X

≫ Summary: Japanese Proportional Mincho-typeface OpenType font by IPA

≫ Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Proportional Mincho style font.

libldb-0.9.10-33.el5

≫ Group: Development/Libraries

≫ Summary: A schema-less, ldap like, API and database

≫ Description: An extensible library that implements an LDAP like API to access remote LDAP servers, or use local tdb databases.

libtalloc-2.0.1-11.el5

≫ Group: System Environment/Daemons

≫ Summary: A hierarchical memory allocator

≫ Description: A library that implements a hierarchical allocator with destructors.

libtdb-1.2.1-5.el5

≫ Group: System Environment/Daemons

≫ Summary: The tdb library

≫ Description: A library that implements a trivial database.

libtevent-0.9.8-10.el5

≫ Group: System Environment/Daemons

≫ Summary: Talloc-based, event-driven mainloop

≫ Description: Tevent is an event system based on the talloc memory management library. Tevent has support for many event types, including timers, signals, and the classic file descriptor events. Tevent also provide helpers to deal with asynchronous code providing the tevent_req (Tevent Request) functions.

mod_revocator-1.0.3-5.el5

≫ Group: System Environment/Daemons

≫ Summary: CRL retrieval module for the Apache HTTP server

≫ Description: The mod_revocator module retrieves and installs remote Certificate Revocate Lists (CRLs) into an Apache web server.

php53-5.3.3-1.el5

≫ Group: Development/Languages

≫ Summary: PHP scripting language for creating dynamic web sites

≫ Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP

coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.

python-pycurl-7.15.5.1-8.el5

» Group: Development/Languages

» Summary: A Python interface to libcurl

» Description: PycURL is a Python interface to libcurl. PycURL can be used to fetch objects identified by a URL from a Python program, similar to the urllib Python module. PycURL is mature, very fast, and supports a lot of features.

qspice-client-0.3.0-4.el5_5

» Group: User Interface/Desktops

» Summary: Implements the client side of the SPICE protocol

» Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package provides the client side of the SPICE protocol

spice-xpi-2.2-2.3.el5_5

» Group: Applications/Internet

» Summary: SPICE extension for Mozilla

» Description: SPICE extension for mozilla allows the client to be used from a web browser.

sssd-1.2.1-39.el5

» Group: Applications/System

» Summary: System Security Services Daemon

» Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

xmlrpc-c-1.16.24-1206.1840.el5

» Group: System Environment/Libraries

» Summary: A lightweight RPC library based on XML and HTTP

» Description: XML-RPC is a quick-and-easy way to make procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML. This library provides a modular implementation of XML-RPC for C.

A.1.2. Updated Packages

ImageMagick-6.2.8.0-4.el5_1.1 - ImageMagick-6.2.8.0-4.el5_5.3

» Group: Applications/Multimedia

❧ Summary: An X application for displaying and manipulating images.

❧ Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

NetworkManager-0.7.0-10.el5 - NetworkManager-0.7.0-10.el5_5.2

❧ Group: System Environment/Base

❧ Summary: Network connection manager and user applications

❧ Description: NetworkManager attempts to keep an active network connection available at all times. It is intended only for the desktop use-case, and is not intended for usage on servers. The point of NetworkManager is to make networking configuration and setup as painless and automatic as possible. If using DHCP, NetworkManager is intended to replace default routes, obtain IP addresses from a DHCP server, and change nameservers whenever it sees fit.

❧ Added Dependencies:

 ▫ dbus-glib-devel >= 0.73-10

❧ Removed Dependencies:

 ▫ dbus-glib-devel >= 0.73-6

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

OpenIPMI-2.0.16-7.el5 - OpenIPMI-2.0.16-11.el5

> Group: System Environment/Base

> Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools

> Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

amtu-1.0.6-1.el5 - amtu-1.0.6-2.el5

> Group: System Environment/Base

> Summary: Abstract Machine Test Utility (AMTU)

> Description: Abstract Machine Test Utility (AMTU) is an administrative utility to check whether the underlying protection mechanism of the hardware are still being enforced. This is a requirement of the Controlled Access Protection Profile FPT_AMT.1, see http://www.radium.ncsc.mil/tpep/library/protection_profiles/CAPP-1.d.pdf

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

anaconda-11.1.2.209-1 - anaconda-11.1.2.224-1

> Group: Applications/System

> Summary: Graphical system installer

> Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.

> Added Dependencies:

- kudzu-devel >= 1.2.57.1.26-1

- pciutils-devel >= 3.1.7-3

- Removed Dependencies:

  - kudzu-devel >= 1.2.57.1.18

  - pciutils-devel

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

apr-1.2.7-11.el5_3.1 - apr-1.2.7-11.el5_5.3

- Group: System Environment/Libraries

- Summary: Apache Portable Runtime library

- Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines, forming a system portability layer to as many operating systems as possible, including Unices, MS Win32, BeOS and OS/2.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

apr-util-1.2.7-11.el5 - apr-util-1.2.7-11.el5_5.2

- Group: System Environment/Libraries

- Summary: Apache Portable Runtime Utility library

- Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing and more.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

audit-1.7.17-3.el5 - audit-1.7.18-2.el5

- Group: System Environment/Daemons

- Summary: User space tools for 2.6 kernel auditing

- Description: The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

autofs-5.0.1-0.rc2.143.el5 - autofs-5.0.1-0.rc2.143.el5_5.6

- Group: System Environment/Daemons

- Summary: A tool for automatically mounting and unmounting filesystems.

- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

avahi-0.6.16-7.el5 - avahi-0.6.16-9.el5_5

> ≫ Group: System Environment/Base

> ≫ Summary: Local network service discovery

> ≫ Description: Avahi is a system which facilitates service discovery on a local network -- this means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind of technology is already found in MacOS X (branded 'Rendezvous', 'Bonjour' and sometimes 'ZeroConf') and is very convenient.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

bind-9.3.6-4.P1.el5_4.2 - bind-9.3.6-16.P1.el5

> ≫ Group: System Environment/Daemons

> ≫ Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.

> ≫ Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

bzip2-1.0.3-4.el5_2 - bzip2-1.0.3-6.el5_5

> ≫ Group: Applications/File

> ≫ Summary: A file compression utility.

> ≫ Description: Bzip2 is a freely available, patent-free, high quality data compressor. Bzip2 compresses files to within 10 to 15 percent of the capabilities of the best techniques available. However, bzip2 has the added benefit of being approximately two times faster at compression

and six times faster at decompression than those techniques. Bzip2 is not the fastest compression utility, but it does strike a balance between speed and compression capability. Install bzip2 if you need a compression utility.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

cman-2.0.115-34.el5 - cman-2.0.115-68.el5

- Group: System Environment/Base

- Summary: cman - The Cluster Manager

- Description: cman - The Cluster Manager

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

compat-gcc-34-3.4.6-4 - compat-gcc-34-3.4.6-4.1

- Group: Development/Languages

- Summary: Compatibility GNU Compiler Collection

- Description: This package includes a GCC 3.4.6-RH compatibility compiler.

- Added Dependencies:

  - /lib/libc.so.6

  - /lib64/libc.so.6

  - /usr/lib/libc.so

  - /usr/lib64/libc.so

- No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

coolkey-1.1.0-14.el5 - coolkey-1.1.0-15.el5

≫ Group: System Environment/Libraries

≫ Summary: CoolKey PKCS #11 module

≫ Description: Linux Driver support for the CoolKey and CAC products.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

cpufreq-utils-005-1.el5 - cpufreq-utils-005-3.el5

≫ Group: System Environment/Base

≫ Summary: CPU Frequency changing related utilities

≫ Description: cpufreq-utils contains several utilities that can be used to control the cpufreq interface provided by the kernel on hardware that supports CPU frequency scaling.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

crash-4.1.2-4.el5 - crash-4.1.2-8.el5

» Group: Development/Debuggers

» Summary: crash utility for live systems; netdump, diskdump, kdump, LKCD or mcore dumpfiles

» Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

cups-1.3.7-18.el5 - cups-1.3.7-26.el5

» Group: System Environment/Daemons

» Summary: Common Unix Printing System

» Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

dapl-2.0.25-2.el5 - dapl-2.0.25-2.el5_5.1

» Group: System Environment/Libraries

» Summary: Library providing access to the DAT 1.2 and 2.0 APIs

» Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.

» No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

db4-4.3.29-10.el5 - db4-4.3.29-10.el5_5.2

➤ Group: System Environment/Libraries

➤ Summary: The Berkeley DB database library (version 4) for C.

➤ Description: The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

dbus-glib-0.73-8.el5 - dbus-glib-0.73-10.el5_5

➤ Group: System Environment/Libraries

➤ Summary: GLib bindings for D-Bus

➤ Description: D-Bus add-on library to integrate the standard D-Bus library with the GLib thread abstraction and main loop.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

devhelp-0.12-20.el5 - devhelp-0.12-21.el5

➤ Group: Development/Tools

➤ Summary: API document browser

➤ Description: An API document browser for GNOME 2.

➤ Added Dependencies:

  ▪ gecko-devel-unstable >= 1.9.2

➤ Removed Dependencies:

  ▪ gecko-devel-unstable >= 1.9

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

device-mapper-1.02.39-1.el5 - device-mapper-1.02.55-2.el5

➤ Group: System Environment/Base

➤ Summary: device mapper library

➤ Description: This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

device-mapper-multipath-0.4.7-34.el5 - device-mapper-multipath-0.4.7-42.el5

➤ Group: System Environment/Base

» Summary: Tools to manage multipath devices using device-mapper.

» Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

dhcp-3.0.5-23.el5 - dhcp-3.0.5-23.el5_5.2

» Group: System Environment/Daemons

» Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.

» Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

dhcpv6-1.0.10-18.el5 - dhcpv6-1.0.10-20.el5

» Group: System Environment/Daemons

» Summary: DHCPv6 - DHCP server and client for IPv6

» Description: Implements the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Consists of dhcp6s(8), the server DHCP daemon, and dhcp6r(8), the

DHCPv6 relay agent. Install this package if you want to support dynamic configuration of IPv6 addresses and parameters on your IPv6 network.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

dump-0.4b41-4.el5 - dump-0.4b41-5.el5

❧ Group: Applications/Archiving

❧ Summary: Programs for backing up and restoring ext2/ext3 filesystems

❧ Description: The dump package contains both dump and restore. Dump examines files in a filesystem, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a filesystem. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups. Install dump if you need a system for both backing up filesystems and restoring filesystems after backups.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

dvgrab-3.0-1.el5 - dvgrab-3.0-1.1.el5

❧ Group: Applications/Multimedia

❧ Summary: Utility to capture video from a DV camera

❧ Description: The dvgrab utility will capture digital video from a DV source on the firewire (IEEE-1394) bus.

❧ No added dependencies

❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

e2fsprogs-1.39-23.el5 - e2fsprogs-1.39-23.el5_5.1

> ❧ Group: System Environment/Base

> ❧ Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems

> ❧ Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

e4fsprogs-1.41.9-3.el5 - e4fsprogs-1.41.12-2.el5

> ❧ Group: System Environment/Base

> ❧ Summary: Utilities for managing the fourth extended (ext4) filesystem

> ❧ Description: The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 filesystem.

- ❧ No added dependencies

- ❧ No removed dependencies

- ❧ No added provides

- ❧ No removed provides

- ❧ No added conflicts

- ❧ No removed conflicts

- ❧ No added obsoletes

- ❧ No removed obsoletes

esc-1.1.0-11.el5 - esc-1.1.0-12.el5

- ❧ Group: Applications/Internet

- ❧ Summary: Enterprise Security Client Smart Card Client

- ❧ Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.

- ❧ Added Dependencies:

  - ▫ xulrunner >= 1.9.2

  - ▫ xulrunner-devel >= 1.9.2

- ❧ Removed Dependencies:

  - ▫ xulrunner

  - ▫ xulrunner-devel

- ❧ No added provides

- ❧ No removed provides

- ❧ No added conflicts

- ❧ No removed conflicts

- ❧ No added obsoletes

- ❧ No removed obsoletes

exim-4.63-5.el5 - exim-4.63-5.el5_5.2

- ❧ Group: System Environment/Daemons

- ❧ Summary: The exim mail transfer agent

- ❧ Description: Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. It is freely available under the terms of the GNU General Public Licence. In style it is similar to Smail 3, but its facilities are more general. There is a great deal of flexibility in the way mail can be routed, and there are extensive facilities for checking incoming mail. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

expat-1.95.8-8.3.el5_4.2 - expat-1.95.8-8.3.el5_5.3

❯ Group: System Environment/Libraries

❯ Summary: A library for parsing XML.

❯ Description: This is expat, the C library for parsing XML, written by James Clark. Expat is a stream oriented XML parser. This means that you register handlers with the parser prior to starting the parse. These handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

firefox-3.0.18-1.el5_4 - firefox-3.6.13-2.el5

❯ Group: Applications/Internet

❯ Summary: Mozilla Firefox Web browser

❯ Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

❯ Added Dependencies:

  ▪ xulrunner-devel >= 1.9.2.13-3

❯ Removed Dependencies:

  ▪ xulrunner-devel >= 1.9.0.18-1

  ▪ xulrunner-devel-unstable >= 1.9.0.18-1

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

freetype-2.2.1-21.el5_3 - freetype-2.2.1-28.el5_5.1

❯ Group: System Environment/Libraries

❯ Summary: A free and portable font rendering engine

❯ Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

gcc-4.1.2-48.el5 - gcc-4.1.2-50.el5

❯ Group: Development/Languages

❯ Summary: Various compilers (C, C++, Objective-C, Java, ...)

❯ Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

gcc44-4.4.0-6.el5 - gcc44-4.4.4-13.el5

➤ Group: Development/Languages

➤ Summary: Preview of GCC version 4.4

➤ Description: The gcc44 package contains preview of the GNU Compiler Collection version 4.4.

➤ Added Dependencies:

◦ gdb

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

gdb-7.0.1-23.el5 - gdb-7.0.1-32.el5

➤ Group: Development/Debuggers

➤ Summary: A GNU source-level debugger for C, C++, Java and other languages

➤ Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.

➤ Added Dependencies:

◦ libstdc++

◦ python-devel

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

gettext-0.14.6-4.el5 - gettext-0.17-1.el5

➤ Group: Development/Tools

➤ Summary: GNU libraries and utilities for producing multi-lingual messages

➤ Description: The GNU gettext package provides a set of tools and documentation for producing

multi-lingual messages in programs. Tools include a set of conventions about how programs should be written to support message catalogs, a directory and file naming organization for the message catalogs, a runtime library which supports the retrieval of translated messages, and stand-alone programs for handling the translatable and the already translated strings. Gettext provides an easy to use library and tools for creating, using, and modifying natural language catalogs and is a powerful and simple method for internationalizing programs.

❯❯ Added Dependencies:

- autoconf

- automake

- expat-devel

❯❯ Removed Dependencies:

- /usr/bin/fastjar

- gcc-java

- libgcj

- unzip

- zip

❯❯ No added provides

❯❯ No removed provides

❯❯ No added conflicts

❯❯ No removed conflicts

❯❯ No added obsoletes

❯❯ No removed obsoletes

gfs2-utils-0.1.62-20.el5 - gfs2-utils-0.1.62-28.el5

❯❯ Group: System Environment/Kernel

❯❯ Summary: Utilities for managing the global filesystem (GFS)

❯❯ Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.

❯❯ No added dependencies

❯❯ No removed dependencies

❯❯ No added provides

❯❯ No removed provides

❯❯ No added conflicts

❯❯ No removed conflicts

❯❯ No added obsoletes

➣ No removed obsoletes

ghostscript-8.15.2-9.11.el5 - ghostscript-8.70-6.el5

➣ Group: Applications/Publishing

➣ Summary: A PostScript(TM) interpreter and renderer.

➣ Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

glibc-2.5-49 - glibc-2.5-58

➣ Group: System Environment/Libraries

➣ Summary: The GNU libc libraries.

➣ Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

gnome-python2-extras-2.14.2-6.el5 - gnome-python2-extras-2.14.2-7.el5

- ≫ Group: Development/Languages

- ≫ Summary: The sources for additional. PyGNOME Python extension modules.

- ≫ Description: The gnome-python-extra package contains the source packages for additional Python bindings for GNOME. It should be used together with gnome-python.

- ≫ Added Dependencies:

  - ▫ gecko-devel-unstable >= 1.9.2

- ≫ Removed Dependencies:

  - ▫ gecko-devel-unstable >= 1.9

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

gnome-screensaver-2.16.1-8.el5 - gnome-screensaver-2.16.1-8.el5_5.2

- ≫ Group: Amusements/Graphics

- ≫ Summary: GNOME Screensaver

- ≫ Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

gnome-session-2.16.0-7.el5 - gnome-session-2.16.0-8.el5

- ≫ Group: User Interface/Desktops

- ≫ Summary: GNOME session manager

- ≫ Description: gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

gnome-vfs2-2.16.2-6.el5 - gnome-vfs2-2.16.2-6.el5_5.1

» Group: System Environment/Libraries

» Summary: The GNOME virtual file-system libraries

» Description: GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

gnupg-1.4.5-14 - gnupg-1.4.5-14.el5_5.1

» Group: Applications/System

» Summary: A GNU utility for secure communication and data storage.

» Description: GnuPG (GNU Privacy Guard) is a GNU utility for encrypting data and creating digital signatures. GnuPG has advanced key management capabilities and is compliant with the proposed OpenPGP Internet standard described in RFC2440. Since GnuPG doesn't use any patented algorithm, it is not compatible with any version of PGP2 (PGP2.x uses only IDEA for symmetric-key encryption, which is patented worldwide).

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gnupg2-2.0.10-3.el5 - gnupg2-2.0.10-3.el5_5.1

- Group: Applications/System

- Summary: Utility for secure communication and data storage

- Description: GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440 and the S/MIME standard as described by several RFCs. GnuPG 2.0 is the stable version of GnuPG integrating support for OpenPGP and S/MIME. It does not conflict with an installed 1.x OpenPGP-only version. GnuPG 2.0 is a newer version of GnuPG with additional support for S/MIME. It has a different design philosophy that splits functionality up into several modules. Both versions may be installed simultaneously without any conflict (gpg is called gpg2 in GnuPG 2). In fact, the gpg version from GnuPG 1.x is able to make use of the gpg-agent as included in GnuPG 2 and allows for seamless passphrase caching. The advantage of GnupG 1.x is its smaller size and no dependency on other modules at run and build time.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gnutls-1.4.1-3.el5_3.5 - gnutls-1.4.1-3.el5_4.8

- Group: System Environment/Libraries

- Summary: A TLS protocol implementation.

- Description: GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer. Currently the GnuTLS library implements the proposed standards by the IETF's TLS working group.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gtk2-2.10.4-20.el5 - gtk2-2.10.4-21.el5_5.6

- Group: System Environment/Libraries

- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X

- Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

hal-0.5.8.1-59.el5 - hal-0.5.8.1-62.el5

- Group: System Environment/Libraries

- Summary: Hardware Abstraction Layer

- Description: HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

hplip-1.6.7-4.1.el5_2.4 - hplip-1.6.7-6.el5

- Group: System Environment/Daemons

- Summary: HP Linux Imaging and Printing Project

> ≫ Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

httpd-2.2.3-43.el5 - httpd-2.2.3-45.el5

> ≫ Group: System Environment/Daemons

> ≫ Summary: Apache HTTP Server

> ≫ Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

hwdata-0.213.18-1.el5.1 - hwdata-0.213.22-1.el5

> ≫ Group: System Environment/Base

> ≫ Summary: Hardware identification and configuration data

> ≫ Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

▹ No added obsoletes

▹ No removed obsoletes

icu-3.6-5.11.4 - icu-3.6-5.16

▹ Group: System Environment/Libraries

▹ Summary: International Components for Unicode

▹ Description: The International Components for Unicode (ICU) libraries provide robust and full-featured Unicode services on a wide variety of platforms. ICU supports the most current version of the Unicode standard, and they provide support for supplementary Unicode characters (needed for GB 18030 repertoire support). As computing environments become more heterogeneous, software portability becomes more important. ICU lets you produce the same results across all the various platforms you support, without sacrificing performance. It offers great flexibility to extend and customize the supplied services.

▹ No added dependencies

▹ No removed dependencies

▹ No added provides

▹ No removed provides

▹ No added conflicts

▹ No removed conflicts

▹ No added obsoletes

▹ No removed obsoletes

initscripts-8.45.30-2.el5 - initscripts-8.45.33-1.el5

▹ Group: System Environment/Base

▹ Summary: The inittab file and the /etc/init.d scripts.

▹ Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.

▹ No added dependencies

▹ No removed dependencies

▹ No added provides

▹ No removed provides

▹ No added conflicts

▹ No removed conflicts

▹ No added obsoletes

▹ No removed obsoletes

ipsec-tools-0.6.5-13.el5_3.1 - ipsec-tools-0.6.5-14.el5_5.5

- Group: System Environment/Base

- Summary: Tools for configuring and using IPSEC

- Description: This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds: - setkey, a program to directly manipulate policies and SAs - racoon, an IKEv1 keying daemon

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

iscsi-initiator-utils-6.2.0.871-0.16.el5 - iscsi-initiator-utils-6.2.0.872-6.el5

- Group: System Environment/Daemons

- Summary: iSCSI daemon and utility programs

- Description: The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5 - java-1.6.0-openjdk-1.6.0.0-1.16.b17.el5

- Group: Development/Languages

- Summary: OpenJDK Runtime Environment

- Description: The OpenJDK runtime environment.

- Added Dependencies:

  - autoconf

  - automake

- java-1.6.0-openjdk-devel

- Removed Dependencies:

  - openmotif-devel

  - prelink

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

jwhois-3.2.3-8.el5 - jwhois-3.2.3-11.el5

- Group: Applications/Internet

- Summary: Internet whois/nicname client.

- Description: A whois client that accepts both traditional and finger-style queries.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

kdebase-3.5.4-20.el5 - kdebase-3.5.4-22.el5

- Group: User Interface/Desktops

- Summary: K Desktop Environment - core files

- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).

- Added Dependencies:

  - libsmbclient-devel

- Removed Dependencies:

  - samba >= 2.2.3a-5

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

kdegraphics-3.5.4-15.el5_4.2 - kdegraphics-3.5.4-17.el5_5.1

- Group: Applications/Multimedia

- Summary: K Desktop Environment - Graphics Applications

- Description: Graphics applications for the K Desktop Environment. Includes: kdvi (displays TeX .dvi files) kghostview (displays postscript files) kcoloredit (palette editor and color chooser) kiconedit (icon editor) kolourpaint (a simple drawing program) ksnapshot (screen capture utility) kview (image viewer for GIF, JPEG, TIFF, etc.) kooka (scanner application) kruler (screen ruler and color measurement tool) kpdf (display pdf files)

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

kernel-2.6.18-194.el5 - kernel-2.6.18-238.el5

- Group: System Environment/Kernel

- Summary: The Linux kernel (the core of the Linux operating system)

- Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

- No added dependencies

- Removed Dependencies:

  - rpmlib(VersionedDependencies) <= 3.0.3-1

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

kexec-tools-1.102pre-96.el5 - kexec-tools-1.102pre-126.el5

- Group: Applications/System

- Summary: The kexec/kdump userspace component.

- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

krb5-1.6.1-36.el5_4.1 - krb5-1.6.1-55.el5

- Group: System Environment/Libraries

- Summary: The Kerberos network authentication system.

- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.

- Added Dependencies:

    - openldap-devel

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

ksh-20100202-1.el5 - ksh-20100202-1.el5_5.1

» Group: Applications/Shells

» Summary: The Original ATT Korn Shell

» Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

kudzu-1.2.57.1.24-1 - kudzu-1.2.57.1.26-1

» Group: Applications/System

» Summary: The Red Hat Linux hardware probing tool.

» Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the system.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

kvm-83-164.el5 - kvm-83-224.el5

» Group: Development/Tools

» Summary: Kernel-based Virtual Machine

» Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.

➢ Added Dependencies:

  ▫ kernel-debug-devel = 2.6.18-237.el5

  ▫ kernel-devel = 2.6.18-237.el5

  ▫ libgcrypt-devel

➢ Removed Dependencies:

  ▫ kernel-devel

  ▫ kernel-devel-x86_64 = 2.6.18-191.el5

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

less-436-2.el5 - less-436-7.el5

➢ Group: Applications/Text

➢ Summary: A text file browser similar to more, but better.

➢ Description: The less utility is a text file browser that resembles more, but has more capabilities. Less allows you to move backwards in the file as well as forwards. Since less doesn't have to read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

lftp-3.7.11-4.el5 - lftp-3.7.11-4.el5_5.3

➢ Group: Applications/Internet

➢ Summary: A sophisticated file transfer program

➤ Description: LFTP is a sophisticated ftp/http file transfer program. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

libbonobo-2.16.0-1.fc6 - libbonobo-2.16.0-1.1.el5_5.1

➤ Group: System Environment/Libraries

➤ Summary: Bonobo component system

➤ Description: Bonobo is a component system based on CORBA, used by the GNOME desktop.

➤ Added Dependencies:

  ▪ dbus-glib-devel

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

libhugetlbfs-1.3-7.el5 - libhugetlbfs-1.3-8.2.el5

➤ Group: System Environment/Libraries

➤ Summary: Library to access the Huge TLB Filesystem

➤ Description: The libhugetlbfs library interacts with the Linux hugetlbfs to make large pages available to applications in a transparent manner.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

libpng-1.2.10-7.1.el5_3.2 - libpng-1.2.10-7.1.el5_5.3

> ≫ Group: System Environment/Libraries

> ≫ Summary: A library of functions for manipulating PNG image format files

> ≫ Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG format image files.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

> ≫ No removed conflicts

> ≫ No added obsoletes

> ≫ No removed obsoletes

libselinux-1.33.4-5.5.el5 - libselinux-1.33.4-5.7.el5

> ≫ Group: System Environment/Libraries

> ≫ Summary: SELinux library and simple utilities

> ≫ Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libselinux provides an API for SELinux applications to get and set process and file security contexts and to obtain security policy decisions. Required for any applications that use the SELinux API.

> ≫ No added dependencies

> ≫ No removed dependencies

> ≫ No added provides

> ≫ No removed provides

> ≫ No added conflicts

- » No removed conflicts

- » No added obsoletes

- » No removed obsoletes

libtiff-3.8.2-7.el5_3.4 - libtiff-3.8.2-7.el5_5.5

- » Group: System Environment/Libraries

- » Summary: Library of functions for manipulating TIFF format image files

- » Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image files.

- » No added dependencies

- » No removed dependencies

- » No added provides

- » No removed provides

- » No added conflicts

- » No removed conflicts

- » No added obsoletes

- » No removed obsoletes

libvirt-0.6.3-33.el5 - libvirt-0.8.2-15.el5

- » Group: Development/Libraries

- » Summary: Library providing a simple API virtualization

- » Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).

- » Added Dependencies:

  - ▪ audit-libs-devel

  - ▪ autoconf

  - ▪ automake

  - ▪ curl-devel

  - ▪ device-mapper

  - ▪ libselinux-devel >= 1.33.4-5.6

  - ▪ libxslt

- » Removed Dependencies:

  - ▪ libselinux-devel

  - ▪ python

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

libxml2-2.6.26-2.1.2.8 - libxml2-2.6.26-2.1.2.8.el5_5.1

➤ Group: Development/Libraries

➤ Summary: Library providing XML and HTML support

➤ Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

linuxwacom-0.7.8.3-8.el5 - linuxwacom-0.7.8.3-10.el5

➤ Group: User Interface/X Hardware Support

➤ Summary: Wacom Drivers from Linux Wacom Project

➤ Description: The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

logrotate-3.7.4-9 - logrotate-3.7.4-9.el5_5.2

- Group: System Environment/Base

- Summary: Rotates, compresses, removes and mails system log files.

- Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your system.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

lvm2-2.02.56-8.el5 - lvm2-2.02.74-5.el5

- Group: System Environment/Base

- Summary: Userland logical volume management tools

- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.

- Added Dependencies:

  - device-mapper >= 1.02.55-2

- Removed Dependencies:

  - device-mapper >= 1.02.39-1

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

m2crypto-0.16-6.el5.6 - m2crypto-0.16-6.el5.8

➤ Group: System Environment/Libraries

➤ Summary: Support for using OpenSSL in python scripts

➤ Description: This package allows you to call OpenSSL functions from python scripts.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

mailman-2.1.9-4.el5 - mailman-2.1.9-6.el5

➤ Group: Applications/Internet

➤ Summary: Mailing list manager with built in Web access.

➤ Description: Mailman is software to help manage email discussion lists, much like Majordomo and Smartmail. Unlike most similar products, Mailman gives each mailing list a webpage, and allows users to subscribe, unsubscribe, etc. over the Web. Even the list manager can administer his or her list entirely from the Web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail <-> news gateways, and so on. Documentation can be found in: /usr/share/doc/mailman-2.1.9 When the package has finished installing, you will need to perform some additional installation steps, these are described in: /usr/share/doc/mailman-2.1.9/INSTALL.REDHAT

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

man-pages-2.39-15.el5 - man-pages-2.39-17.el5

➤ Group: Documentation

≫ Summary: Man (manual) pages from the Linux Documentation Project.

≫ Description: A large collection of man pages (documentation) from the Linux Documentation Project (LDP).

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

man-pages-ja-20060815-13.el5 - man-pages-ja-20060815-14.el5

≫ Group: Documentation

≫ Summary: Japanese man (manual) pages from the Japanese Manual Project

≫ Description: Japanese Manual pages, translated by JM-Project (Japanese Manual Project).

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

metacity-2.16.0-15.el5 - metacity-2.16.0-16.el5

≫ Group: User Interface/Desktops

≫ Summary: Metacity window manager

≫ Description: Metacity is a simple window manager that integrates nicely with GNOME 2.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

microcode_ctl-1.17-1.50.el5 - microcode_ctl-1.17-1.52.el5

- ≫ Group: System Environment/Base

- ≫ Summary: Tool to update x86/x86-64 CPU microcode.

- ≫ Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

mikmod-3.1.6-38.1 - mikmod-3.1.6-39.el5_5.1

- ≫ Group: Applications/Multimedia

- ≫ Summary: A MOD music file player.

- ≫ Description: MikMod is one of the best and most well known MOD music file players for UNIX-like systems. This particular distribution is intended to compile fairly painlessly in a Linux environment. MikMod uses the OSS /dev/dsp driver including all recent kernels for output, and will also write .wav files. Supported file formats include MOD, STM, S3M, MTM, XM, ULT, and IT. The player uses ncurses for console output and supports transparent loading from gzip/pkzip/zoo archives and the loading/saving of playlists. Install the mikmod package if you need a MOD music file player.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

mkinitrd-5.1.19.6-61 - mkinitrd-5.1.19.6-68.el5

❧ Group: System Environment/Base

❧ Summary: Creates an initial ramdisk image for preloading modules.

❧ Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

mod_authz_ldap-0.26-9.el5 - mod_authz_ldap-0.26-9.el5_5.1

❧ Group: System Environment/Daemons

❧ Summary: LDAP authorization module for the Apache HTTP Server

❧ Description: The mod_authz_ldap package provides support for authenticating users of the Apache HTTP server against an LDAP database. mod_authz_ldap features the ability to authenticate users based on the SSL client certificate presented, and also supports password aging, and authentication based on role or by configured filters.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

mod_nss-1.0.3-8.el5 - mod_nss-1.0.8-3.el5

❧ Group: System Environment/Daemons

❧ Summary: SSL/TLS module for the Apache HTTP server

➢ Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security library.

➢ Added Dependencies:

  ▪ httpd-devel

  ▪ nspr-devel

  ▪ nss-devel >= 3.12.6

➢ Removed Dependencies:

  ▪ httpd-devel >= 0:2.0.52

  ▪ nspr-devel >= 4.6

  ▪ nss-devel >= 3.11

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

module-init-tools-3.3-0.pre3.1.60.el5 - module-init-tools-3.3-0.pre3.1.60.el5_5.1

➢ Group: System Environment/Kernel

➢ Summary: Kernel module management utilities.

➢ Description: The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

mysql-5.0.77-4.el5_4.2 - mysql-5.0.77-4.el5_5.4

➢ Group: Applications/Databases

➢ Summary: MySQL client programs and shared libraries

❧ Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

net-snmp-5.3.2.2-9.el5 - net-snmp-5.3.2.2-9.el5_5.1

❧ Group: System Environment/Daemons

❧ Summary: A collection of SNMP protocol tools and libraries.

❧ Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

nfs-utils-1.0.9-44.el5 - nfs-utils-1.0.9-50.el5

❧ Group: System Environment/Daemons

❧ Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.

❧ Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries

the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.

≫ No added dependencies

≫ Removed Dependencies:

  ▪ nfs-utils-lib-devel >= 1.0.8-2

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

nspluginwrapper-1.3.0-8.el5 - nspluginwrapper-1.3.0-9.el5

≫ Group: Networking/WWW

≫ Summary: A compatibility layer for Netscape 4 plugins

≫ Description: nspluginwrapper makes it possible to use Netscape 4 compatible plugins compiled for ppc into Mozilla for another architecture, e.g. x86_64. This package consists in: * npviewer: the plugin viewer * npwrapper.so: the browser-side plugin * nspluginplayer: stand-alone NPAPI plugin player * mozilla-plugin-config: a tool to manage plugins installation and update

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

nspr-4.7.6-1.el5_4 - nspr-4.8.6-1.el5

≫ Group: System Environment/Libraries

≫ Summary: Netscape Portable Runtime

≫ Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.

≫ No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

nss-3.12.3.99.3-1.el5_3.2 - nss-3.12.8-1.el5

- Group: System Environment/Libraries

- Summary: Network Security Services

- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.

- Added Dependencies:

  - nspr-devel >= 4.8.6

- Removed Dependencies:

  - nspr-devel >= 4.6.99

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

nss_db-2.2-35.3 - nss_db-2.2-35.4.el5_5

- Group: System Environment/Libraries

- Summary: An NSS library for the Berkeley DB.

- Description: Nss_db is a set of C library extensions which allow Berkeley Databases to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Install nss_db if your flat name service files are too large and lookups are slow.

- No added dependencies

- No removed dependencies

- No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

nss_ldap-253-25.el5 - nss_ldap-253-37.el5

➤ Group: System Environment/Base

➤ Summary: NSS library and PAM module for LDAP.

➤ Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

oddjob-0.27-9.el5 - oddjob-0.27-11.el5

➤ Group: System Environment/Daemons

➤ Summary: A D-BUS service which runs odd jobs on behalf of client applications

➤ Description: oddjob is a D-BUS service which performs particular tasks for clients which connect to it and issue requests using the system-wide message bus.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

openCryptoki-2.2.4-22.el5_4.2 - openCryptoki-2.2.4-22.el5_5.1

➤ Group: Productivity/Security

➤ Summary: Implementation of Cryptoki v2.11 for IBM Crypto Hardware

➤ Description: The PKCS#11 Version 2.11 api implemented for the IBM Crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded) and the IBM eServer Cryptographic Accelerator (FC 4960 on pSeries)

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

openais-0.80.6-16.el5 - openais-0.80.6-28.el5

➤ Group: System Environment/Base

➤ Summary: The openais Standards-Based Cluster Framework executive and APIs

➤ Description: This package contains the openais executive, openais service handlers, default configuration files and init script.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

openldap-2.3.43-12.el5 - openldap-2.3.43-12.el5_5.3

➤ Group: System Environment/Daemons

➤ Summary: The configuration files, libraries, and documentation for OpenLDAP.

➤ Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the

Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

 ❧ No added dependencies

 ❧ No removed dependencies

 ❧ No added provides

 ❧ No removed provides

 ❧ No added conflicts

 ❧ No removed conflicts

 ❧ No added obsoletes

 ❧ No removed obsoletes

openmotif-2.3.1-2.el5_4.1 - openmotif-2.3.1-5.el5_5.1

 ❧ Group: System Environment/Libraries

 ❧ Summary: Open Motif runtime libraries and executables.

 ❧ Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".

 ❧ No added dependencies

 ❧ No removed dependencies

 ❧ No added provides

 ❧ No removed provides

 ❧ No added conflicts

 ❧ No removed conflicts

 ❧ No added obsoletes

 ❧ No removed obsoletes

openoffice.org-3.1.1-19.5.el5 - openoffice.org-3.1.1-19.5.el5_5.1

 ❧ Group: Applications/Productivity

 ❧ Summary: OpenOffice.org comprehensive office suite.

 ❧ Description: OpenOffice.org is an Open Source, community-developed, multi-platform office productivity suite. It includes the key desktop applications, such as a word processor, spreadsheet, presentation manager, formula editor and drawing program, with a user interface and feature set similar to other office suites. Sophisticated and flexible, OpenOffice.org also works transparently with a variety of file formats, including Microsoft Office. Usage: Simply type "ooffice" to run OpenOffice.org or select the requested component (Writer, Calc, Impress, etc.) from your desktop menu. On first start a few files will be installed in the user's home, if necessary.

 ❧ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

openssh-4.3p2-41.el5 - openssh-4.3p2-72.el5

❯ Group: Applications/Internet

❯ Summary: The OpenSSH implementation of SSH protocol versions 1 and 2

❯ Description: SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.

❯ Added Dependencies:

  ▫ audit-libs-devel >= 1.7.18

❯ Removed Dependencies:

  ▫ audit-libs-devel

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

openssl-0.9.8e-12.el5_4.6 - openssl-0.9.8e-12.el5_5.7

❯ Group: System Environment/Libraries

❯ Summary: The OpenSSL toolkit

❯ Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.

❯ No added dependencies

❯ No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

openssl097a-0.9.7a-9.el5_2.1 - openssl097a-0.9.7a-9.el5_4.2

- Group: System Environment/Libraries

- Summary: The OpenSSL toolkit

- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

openswan-2.6.21-5.el5_4.2 - openswan-2.6.21-5.el5_5.3

- Group: System Environment/Daemons

- Summary: Openswan IPSEC implementation

- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4309)

- Added Dependencies:

  - nss-devel >= 3.12.6-2

- Removed Dependencies:

  - nss-devel >= 3.12.3-2

- No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

pam-0.99.6.2-6.el5_4.1 - pam-0.99.6.2-6.el5_5.2

➤ Group: System Environment/Base

➤ Summary: A security tool which provides authentication for applications

➤ Description: PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

pam_krb5-2.2.14-15 - pam_krb5-2.2.14-18.el5

➤ Group: System Environment/Base

➤ Summary: A Pluggable Authentication Module for Kerberos 5.

➤ Description: This is pam_krb5, a pluggable authentication module that can be used with Linux-PAM and Kerberos 5. This module supports password checking, ticket creation, and optional TGT verification and conversion to Kerberos IV tickets. The included pam_krb5afs module also gets AFS tokens if so configured.

➤ Added Dependencies:

   ▪ gettext-devel

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

> ❧ No removed obsoletes

pango-1.14.9-6.el5 - pango-1.14.9-8.el5

> ❧ Group: System Environment/Libraries

> ❧ Summary: System for layout and rendering of internationalized text

> ❧ Description: Pango is a system for layout and rendering of internationalized text.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

passwd-0.73-1 - passwd-0.73-2

> ❧ Group: System Environment/Base

> ❧ Summary: The passwd utility for setting/changing passwords using PAM

> ❧ Description: The passwd package contains a system utility (passwd) which sets and/or changes passwords, using PAM (Pluggable Authentication Modules). To use passwd, you should have PAM installed on your system.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

patch-2.5.4-29.2.3.el5 - patch-2.5.4-31.el5

> ❧ Group: Development/Tools

> ❧ Summary: The GNU patch command, for modifying/upgrading files.

> ❧ Description: The patch program applies diff files to originals. The diff command is used to compare an original to a changed file. Diff lists the changes made to the file. A person who has the original file can then use the patch command with the diff file to add the changes to their original file (patching the file). Patch should be installed because it is a common way of

upgrading applications.

≫ Added Dependencies:

   ▪ libselinux-devel

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

pciutils-2.2.3-8.el5 - pciutils-3.1.7-3.el5

≫ Group: Applications/System

≫ Summary: PCI bus related utilities

≫ Description: The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

pcre-6.6-2.el5_1.7 - pcre-6.6-6.el5

≫ Group: System Environment/Libraries

≫ Summary: Perl-compatible regular expression library

≫ Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.

≫ No added dependencies

≫ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

pcsc-lite-1.4.4-1.el5 - pcsc-lite-1.4.4-4.el5_5

➤ Group: System Environment/Daemons

➤ Summary: PC/SC Lite smart card framework and applications

➤ Description: The purpose of PC/SC Lite is to provide a Windows(R) SCard interface in a very small form factor for communicating to smartcards and readers. PC/SC Lite uses the same winscard API as used under Windows(R). This package includes the PC/SC Lite daemon, a resource manager that coordinates communications with smart card readers and smart cards that are connected to the system, as well as other command line tools.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

perl-5.8.8-27.el5 - perl-5.8.8-32.el5_5.2

➤ Group: Development/Languages

➤ Summary: The Perl programming language

➤ Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

- ➤ No added conflicts

- ➤ No removed conflicts

- ➤ No added obsoletes

- ➤ No removed obsoletes

perl-Archive-Tar-1.30-1.fc6 - perl-Archive-Tar-1.39.1-1.el5_5.2

- ➤ Group: Development/Libraries

- ➤ Summary: A module for Perl manipulation of .tar files

- ➤ Description: Archive::Tar provides an object oriented mechanism for handling tar files. It provides class methods for quick and easy files handling while also allowing for the creation of tar file objects for custom manipulation. If you have the IO::Zlib module installed, Archive::Tar will also support compressed or gzipped tar files.

- ➤ No added dependencies

- ➤ No removed dependencies

- ➤ No added provides

- ➤ No removed provides

- ➤ No added conflicts

- ➤ No removed conflicts

- ➤ No added obsoletes

- ➤ No removed obsoletes

perl-Sys-Virt-0.2.0-6.el5 - perl-Sys-Virt-0.2.4-1.el5

- ➤ Group: Development/Libraries

- ➤ Summary: Perl bindings for the libvirt library

- ➤ Description: The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.

- ➤ Added Dependencies:

    - ▫ libvirt-devel >= 0.8.1

- ➤ Removed Dependencies:

    - ▫ libvirt-devel >= 0.6.1

- ➤ No added provides

- ➤ No removed provides

- ➤ No added conflicts

- ➤ No removed conflicts

- ➤ No added obsoletes

➤ No removed obsoletes

php-5.1.6-27.el5 - php-5.1.6-27.el5_5.3

➤ Group: Development/Languages

➤ Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)

➤ Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

pidgin-2.6.6-1.el5 - pidgin-2.6.6-5.el5_5

➤ Group: Applications/Internet

➤ Summary: A Gtk+ based multiprotocol instant messaging client

➤ Description: Pidgin allows you to talk to anyone using a variety of messaging protocols including AIM, MSN, Yahoo!, Jabber, Bonjour, Gadu-Gadu, ICQ, IRC, Novell Groupwise, QQ, Lotus Sametime, SILC, Simple and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor. Pidgin supports many common features of other clients, as well as many unique features, such as perl scripting, TCL scripting and C plugins. Pidgin is not affiliated with or endorsed by America Online, Inc., Microsoft Corporation, Yahoo! Inc., or ICQ Inc.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

pirut-1.3.28-17.el5 - pirut-1.3.28-19.el5

- Group: Applications/System

- Summary: Package Installation, Removal and Update Tools

- Description: pirut (pronounced "pirate") provides a set of graphical tools for managing software.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

poppler-0.5.4-4.4.el5_4.11 - poppler-0.5.4-4.4.el5_5.14

- Group: Development/Libraries

- Summary: PDF rendering library

- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

postgresql-8.1.18-2.el5_4.1 - postgresql-8.1.22-1.el5_5.1

- Group: Applications/Databases

- Summary: PostgreSQL client programs and libraries.

- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as

well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

➤ No added dependencies

➤ Removed Dependencies:

  ▪ rpmlib(VersionedDependencies) <= 3.0.3-1

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

postgresql84-8.4.2-5.el5 - postgresql84-8.4.5-1.el5_5.1

➤ Group: Applications/Databases

➤ Summary: PostgreSQL client programs

➤ Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

python-2.4.3-27.el5 - python-2.4.3-43.el5

➤ Group: Development/Languages

❧ Summary: An interpreted, interactive, object-oriented programming language.

❧ Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.

❧ Added Dependencies:

  ▪ valgrind-devel

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

python-dmidecode-3.10.8-4.el5 - python-dmidecode-3.10.13-1.el5_5.1

❧ Group: System Environment/Libraries

❧ Summary: Python module to access DMI data

❧ Description: python-dmidecode is a python extension module that uses the code-base of the 'dmidecode' utility, and presents the data as python data structures or as XML data using libxml2.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

python-urlgrabber-3.1.0-5.el5 - python-urlgrabber-3.1.0-6.el5

❧ Group: Development/Libraries

❧ Summary: A high-level cross-protocol url-grabber

> Description: A high-level cross-protocol url-grabber for python supporting HTTP, FTP and file locations. Features include keepalive, byte ranges, throttling, authentication, proxies and more.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

python-virtinst-0.400.3-9.el5 - python-virtinst-0.400.3-11.el5

> Group: Development/Libraries

> Summary: Python modules and utilities for installing virtual machines

> Description: virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

qffmpeg-0.4.9-0.15.20080908.el5 - qffmpeg-0.4.9-0.16.20080908.el5_5

> Group: Applications/Multimedia

> Summary: Stripped-down fork of ffmpeg for libspice

> Description: This is a stripped down version of upstream FFMPEG including only the codecs used by SPICE in order to avoid inadvertantly bundling or shipping any encumbered code or binaries.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

qspice-0.3.0-54.el5 - qspice-0.3.0-54.el5_5.2

> Group: User Interface/Desktops

> Summary: An implementation of the Simple Protocol for Independent Computing Environments

> Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

quagga-0.98.6-5.el5 - quagga-0.98.6-5.el5_5.2

> Group: System Environment/Daemons

> Summary: Routing daemon

> Description: Quagga is a free software that manages TCP/IP based routing protocol. It takes multi-server and multi-thread approach to resolve the current complexity of the Internet. Quagga supports BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng. Quagga is intended to be used as a Route Server and a Route Reflector. It is not a toolkit, it provides full routing power under a new architecture. Quagga by design has a process for each protocol. Quagga is a fork of GNU Zebra.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

- No added obsoletes

- No removed obsoletes

quota-3.13-1.2.5.el5 - quota-3.13-4.el5

- Group: System Environment/Base

- Summary: System administration tools for monitoring users' disk usage.

- Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.

- Added Dependencies:

  - openldap-devel

  - openssl-devel

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

redhat-lsb-3.1-12.3.EL - redhat-lsb-4.0-2.1.4.el5

- Group: System Environment/Base

- Summary: LSB base libraries support for Red Hat Enterprise Linux

- Description: The Linux Standard Base (LSB) is an attempt to develop a set of standards that will increase compatibility among Linux distributions. The redhat-lsb package provides utilities needed for LSB Compliant Applications. It also contains requirements that will ensure that all components required by the LSB that are provided by Red Hat Linux are installed on the system.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

redhat-release-5Client-5.5.0.2 - redhat-release-5Client-5.6.0.3

➢ Group: System Environment/Base

➢ Summary: Red Hat Enterprise Linux release file

➢ Description: Red Hat Enterprise Linux release files

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

redhat-release-notes-5Client-31 - redhat-release-notes-5Client-34

➢ Group: System Environment/Base

➢ Summary: Red Hat Enterprise Linux release notes files

➢ Description: Red Hat Enterprise Linux release notes files.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

rhn-client-tools-0.4.20-33.el5 - rhn-client-tools-0.4.20-46.el5

➢ Group: System Environment/Base

➢ Summary: Support programs and libraries for Red Hat Network

➢ Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rhnlib-2.5.22-3.el5 - rhnlib-2.5.22-5.el5

- Group: Development/Libraries

- Summary: Python libraries for the RHN project

- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rng-utils-2.0-1.14.1.fc6 - rng-utils-2.0-4.el5

- Group: System Environment/Base

- Summary: Random number generator related utilities

- Description: Hardware random number generation tools.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rpm-4.4.2.3-18.el5 - rpm-4.4.2.3-22.el5

- Group: System Environment/Base

- Summary: The RPM package management system

❧ Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

rsyslog-3.22.1-3.el5 - rsyslog-3.22.1-3.el5_5.1

❧ Group: System Environment/Daemons

❧ Summary: Enhanced system logging and kernel message trapping daemon

❧ Description: Rsyslog is an enhanced multi-threaded syslogd supporting, among others, MySQL, syslog/tcp, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is quite compatible to stock sysklogd and can be used as a drop-in replacement. Its advanced features make it suitable for enterprise-class, encryption protected syslog relay chains while at the same time being very easy to setup for the novice user.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

samba-3.0.33-3.28.el5 - samba-3.0.33-3.29.el5_5.1

❧ Group: System Environment/Daemons

❧ Summary: The Samba SMB server.

❧ Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides

an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

samba3x-3.3.8-0.51.el5 - samba3x-3.5.4-0.70.el5

» Group: System Environment/Daemons

» Summary: Server and Client software to interoperate with Windows machines

» Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

» Added Dependencies:

  ▪ libtalloc-devel >= 2.0.1

  ▪ libtdb-devel >= 1.2.1

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

sblim-1-40.el5 - sblim-1-47.el5

» Group: Applications/System

» Summary: Standards Based Linux Instrumentation for Manageability

» Description: SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules

that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

- No added dependencies

- Removed Dependencies:

  - sblim-cmpi-devel

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

screen-4.0.3-1.el5_4.1 - screen-4.0.3-3.el5

- Group: Applications/System

- Summary: A screen manager that supports multiple logins on one terminal

- Description: The screen utility allows you to have multiple logins on just one terminal. Screen is useful for users who telnet into a machine or are connected via a dumb terminal, but want to use more than just one login. Install the screen package if you need a screen manager that can support multiple logins on one terminal.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

selinux-policy-2.4.6-279.el5 - selinux-policy-2.4.6-300.el5

- Group: System Environment/Base

- Summary: SELinux policy configuration

- Description: SELinux Reference Policy - modular.

- No added dependencies

- No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

sg3_utils-1.25-4.el5 - sg3_utils-1.25-5.el5

≫ Group: Utilities/System

≫ Summary: Utils for Linux's SCSI generic driver devices + raw devices

≫ Description: Collection of Linux utilities for devices that use the SCSI command set. Includes utilities to copy data based on "dd" syntax and semantics (called sg_dd, sgp_dd and sgm_dd); check INQUIRY data and VPD pages (sg_inq); check mode and log pages (sginfo, sg_modes and sg_logs); spin up and down disks (sg_start); do self tests (sg_senddiag); and various other functions. See the README, CHANGELOG and COVERAGE files. Requires the linux kernel 2.4 series or later. In the 2.4 series SCSI generic device names (e.g. /dev/sg0) must be used. In the 2.6 series other device names may be used as well (e.g. /dev/sda). Warning: Some of these tools access the internals of your system and the incorrect usage of them may render your system inoperable.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

shadow-utils-4.0.17-15.el5 - shadow-utils-4.0.17-18.el5

≫ Group: System Environment/Base

≫ Summary: Utilities for managing accounts and shadow password files.

≫ Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.

≫ Added Dependencies:

  - libacl-devel

  - libattr-devel

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

sox-12.18.1-1 - sox-12.18.1-1.el5_5.1

- Group: Applications/Multimedia

- Summary: A general purpose sound file conversion tool.

- Description: SoX (Sound eXchange) is a sound file format converter SoX can convert between many different digitized sound formats and perform simple sound manipulation functions, including sound effects.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

strace-4.5.18-5.el5_4.1 - strace-4.5.18-5.el5_5.5

- Group: Development/Debuggers

- Summary: Tracks and displays system calls associated with a running process

- Description: The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.

- No added dependencies

- No removed dependencies

- No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

subversion-1.4.2-4.el5_3.1 - subversion-1.6.11-7.el5

❧ Group: Development/Tools

❧ Summary: Modern Version Control System designed to replace CVS

❧ Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.

❧ Added Dependencies:

  ▪ cyrus-sasl-devel

  ▪ java-devel-gcj

  ▪ unzip

  ▪ zip

❧ Removed Dependencies:

  ▪ java-1.4.2-devel

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

sudo-1.7.2p1-5.el5 - sudo-1.7.2p1-10.el5

❧ Group: Applications/System

❧ Summary: Allows restricted root access for specified users.

❧ Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.

❧ No added dependencies

- ❯ No removed dependencies

- ❯ No added provides

- ❯ No removed provides

- ❯ No added conflicts

- ❯ No removed conflicts

- ❯ No added obsoletes

- ❯ No removed obsoletes

sysstat-7.0.2-3.el5 - sysstat-7.0.2-3.el5_5.1

- ❯ Group: Applications/System

- ❯ Summary: The sar and iostat system monitoring commands.

- ❯ Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.

- ❯ No added dependencies

- ❯ No removed dependencies

- ❯ No added provides

- ❯ No removed provides

- ❯ No added conflicts

- ❯ No removed conflicts

- ❯ No added obsoletes

- ❯ No removed obsoletes

system-config-lvm-1.1.5-4.el5 - system-config-lvm-1.1.5-8.el5

- ❯ Group: Applications/System

- ❯ Summary: A utility for graphically configuring Logical Volumes

- ❯ Description: system-config-lvm is a utility for graphically configuring Logical Volumes

- ❯ No added dependencies

- ❯ No removed dependencies

- ❯ No added provides

- ❯ No removed provides

- ❯ No added conflicts

- ❯ No removed conflicts

- ❯ No added obsoletes

- ❯ No removed obsoletes

system-config-securitylevel-1.6.29.1-5.el5 - system-config-securitylevel-1.6.29.1-6.el5

➤ Group: System Environment/Base

➤ Summary: A graphical interface for modifying the system security level

➤ Description: system-config-securitylevel is a graphical user interface for setting basic firewall rules.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

systemtap-1.1-3.el5 - systemtap-1.3-4.el5

➤ Group: Development/System

➤ Summary: Instrumentation System

➤ Description: SystemTap is an instrumentation system for systems running Linux 2.6. Developers can write instrumentation to collect data on the operation of the system.

➤ Added Dependencies:

  ▪ avahi-devel

  ▪ glibc-headers

  ▪ rpm-devel

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

tcsh-6.14-17.el5 - tcsh-6.14-17.el5_5.2

➤ Group: System Environment/Shells

➤ Summary: An enhanced version of csh, the C shell.

❯ Description: Tcsh is an enhanced but completely compatible version of csh, the C shell. Tcsh is a command language interpreter which can be used both as an interactive login shell and as a shell script command processor. Tcsh includes a command line editor, programmable word completion, spelling correction, a history mechanism, job control and a C language like syntax.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

tetex-3.0-33.8.el5 - tetex-3.0-33.8.el5_5.6

❯ Group: Applications/Publishing

❯ Summary: The TeX text formatting system.

❯ Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

thunderbird-2.0.0.24-2.el5_4 - thunderbird-2.0.0.24-13.el5_5

❯ Group: Applications/Internet

❯ Summary: Mozilla Thunderbird mail/newsgroup client

❯ Description: Mozilla Thunderbird is a standalone mail and newsgroup client.

❯ No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

tmpwatch-2.9.7-1.1.el5.2 - tmpwatch-2.9.7-1.1.el5.5

- Group: System Environment/Base

- Summary: A utility for removing files based on when they were last accessed.

- Description: The tmpwatch utility recursively searches through specified directories and removes files which have not been accessed in a specified period of time. Tmpwatch is normally used to clean up directories which are used for temporarily holding files (for example, /tmp). Tmpwatch ignores symlinks, won't switch filesystems and only removes empty directories and regular files.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

tog-pegasus-2.9.1-2.el5 - tog-pegasus-2.9.1-2.el5_5.1

- Group: Systems Management/Base

- Summary: OpenPegasus WBEM Services for Linux

- Description: OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

tomcat5-5.5.23-0jpp.7.el5_3.2 - tomcat5-5.5.23-0jpp.16.el5

> Group: Networking/Daemons

> Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API

> Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

totem-2.16.7-6.el5 - totem-2.16.7-7.el5

> Group: Applications/Multimedia

> Summary: Movie player for GNOME 2

> Description: Totem is simple movie player for the Gnome desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as a pretty complete keyboard navigation.

> Added Dependencies:

>> gecko-devel-unstable >= 1.9.2

> Removed Dependencies:

>> gecko-devel-unstable >= 1.9

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

tzdata-2010e-1.el5 - tzdata-2010l-1.el5

> ❧ Group: System Environment/Base

> ❧ Summary: Timezone data

> ❧ Description: This package contains data files with rules for various time zones around the world.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

udev-095-14.21.el5 - udev-095-14.24.el5

> ❧ Group: System Environment/Base

> ❧ Summary: A userspace implementation of devfs

> ❧ Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

util-linux-2.13-0.52.el5_4.1 - util-linux-2.13-0.56.el5

> ❧ Group: System Environment/Base

> ❧ Summary: A collection of basic system utilities.

> ❧ Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.

➤ Added Dependencies:

  ▪ libutempter-devel

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

vim-7.0.109-6.el5 - vim-7.0.109-7.el5

➤ Group: Applications/Editors

➤ Summary: The VIM editor.

➤ Description: VIM (VIsual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.

➤ No added dependencies

➤ Removed Dependencies:

  ▪ rpmlib(VersionedDependencies) <= 3.0.3-1

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

virt-manager-0.6.1-12.el5 - virt-manager-0.6.1-13.el5

➤ Group: Applications/Emulators

➤ Summary: Virtual Machine Manager

➤ Description: Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.

➤ No added dependencies

➤ No removed dependencies

- ❧ No added provides

- ❧ No removed provides

- ❧ No added conflicts

- ❧ No removed conflicts

- ❧ No added obsoletes

- ❧ No removed obsoletes

vnc-4.1.2-14.el5_3.1 - vnc-4.1.2-14.el5_5.4

- ❧ Group: User Interface/Desktops

- ❧ Summary: A remote display system.

- ❧ Description: Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package contains a client which will allow you to connect to other desktops running a VNC server.

- ❧ No added dependencies

- ❧ No removed dependencies

- ❧ No added provides

- ❧ No removed provides

- ❧ No added conflicts

- ❧ No removed conflicts

- ❧ No added obsoletes

- ❧ No removed obsoletes

vsftpd-2.0.5-16.el5_4.1 - vsftpd-2.0.5-16.el5_5.1

- ❧ Group: System Environment/Daemons

- ❧ Summary: vsftpd - Very Secure Ftp Daemon

- ❧ Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.

- ❧ No added dependencies

- ❧ No removed dependencies

- ❧ No added provides

- ❧ No removed provides

- ❧ No added conflicts

- ❧ No removed conflicts

- ❧ No added obsoletes

- ❧ No removed obsoletes

w3m-0.5.1-15.el5 - w3m-0.5.1-17.el5_5

- Group: Applications/Internet

- Summary: A pager with Web browsing abilities.

- Description: The w3m program is a pager (or text file viewer) that can also be used as a text-mode Web browser. W3m features include the following: when reading an HTML document, you can follow links and view images using an external image viewer; its internet message mode determines the type of document from the header; if the Content-Type field of the document is text/html, the document is displayed as an HTML document; you can change a URL description like 'http://hogege.net' in plain text into a link to that URL. If you want to display the inline images on w3m, you need to install w3m-img package as well.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

wacomexpresskeys-0.4.1-1.el5 - wacomexpresskeys-0.4.1-2.el5

- Group: System Environment/Base

- Summary: Wacom ExpressKeys and Touch Strips configuration utility

- Description: Configuration utility to bind Wacom tablet's ExpressKeys and Touch Strips to generate other input events.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

wdaemon-0.14-5 - wdaemon-0.14-7

- Group: User Interface/X Hardware Support

- Summary: Hotplug helper for Wacom X.org driver

➤ Description: Helper application which emulates persistent input devices for Wacom tablets so they can be plugged and unplugged while X.org server is running. This should go away as soon X.org properly supports hotplugging.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

wireshark-1.0.8-1.el5_3.1 - wireshark-1.0.15-1.el5_5.1

➤ Group: Applications/Internet

➤ Summary: Network traffic analyzer

➤ Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ package.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

xen-3.0.3-105.el5 - xen-3.0.3-120.el5

➤ Group: Development/Libraries

➤ Summary: Xen is a virtual machine monitor

➤ Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.

➤ No added dependencies

› No removed dependencies

› No added provides

› No removed provides

› No added conflicts

› No removed conflicts

› No added obsoletes

› No removed obsoletes

xorg-x11-drv-ati-6.6.3-3.27.el5 - xorg-x11-drv-ati-6.6.3-3.32.el5

› Group: User Interface/X Hardware Support

› Summary: Xorg X11 ati video driver

› Description: X.Org X11 ati video driver.

› No added dependencies

› No removed dependencies

› No added provides

› No removed provides

› No added conflicts

› No removed conflicts

› No added obsoletes

› No removed obsoletes

xorg-x11-drv-mga-1.4.10-7.el5 - xorg-x11-drv-mga-1.4.13-1.el5

› Group: User Interface/X Hardware Support

› Summary: Xorg X11 mga video driver

› Description: X.Org X11 mga video driver.

› No added dependencies

› No removed dependencies

› No added provides

› No removed provides

› No added conflicts

› No removed conflicts

› No added obsoletes

› No removed obsoletes

xorg-x11-drv-nv-2.1.15-3.el5 - xorg-x11-drv-nv-2.1.15-4.el5

≫ Group: User Interface/X Hardware Support

≫ Summary: Xorg X11 nv video driver

≫ Description: X.Org X11 nv video driver.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

xorg-x11-drv-sis-0.9.1-7.1.el5 - xorg-x11-drv-sis-0.9.1-7.3.el5

≫ Group: User Interface/X Hardware Support

≫ Summary: Xorg X11 sis video driver

≫ Description: X.Org X11 sis video driver.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

xorg-x11-server-1.1.1-48.76.el5 - xorg-x11-server-1.1.1-48.76.el5_5.2

≫ Group: User Interface/X

≫ Summary: X.Org X11 X server

≫ Description: X.Org X11 X server

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

xulrunner-1.9.0.18-1.el5_4 - xulrunner-1.9.2.13-3.el5

⯈ Group: Applications/Internet

⯈ Summary: XUL Runtime for Gecko Applications

⯈ Description: XULRunner provides the XUL Runtime environment for Gecko applications.

⯈ Added Dependencies:

- alsa-lib-devel

- autoconf213

- bzip2-devel

- libnotify-devel

- nspr-devel >= 4.8

- nss-devel >= 3.12.8

- startup-notification-devel

⯈ Removed Dependencies:

- cairo-devel >= 0.5

- curl-devel

- desktop-file-utils

- libpng-devel

- nspr-devel >= 4.7.6

- nss-devel >= 3.11.99.5

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

yelp-2.16.0-22.el5 - yelp-2.16.0-26.el5

⯈ Group: Applications/System

⯈ Summary: A system documentation reader from the Gnome project

- Description: Yelp is the Gnome 2 help/documentation browser. It is designed to help you browse all the documentation on your system in one central tool.

- Added Dependencies:

    - gecko-devel-unstable >= 1.9.2

- Removed Dependencies:

    - gecko-devel-unstable >= 1.9

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

yum-3.2.22-26.el5 - yum-3.2.22-33.el5

- Group: System Environment/Base

- Summary: RPM installer/updater

- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

yum-rhn-plugin-0.5.4-15.el5 - yum-rhn-plugin-0.5.4-17.el5

- Group: System Environment/Base

- Summary: RHN support for yum

- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.

- No added dependencies

- No removed dependencies

- No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

yum-utils-1.1.16-13.el5 - yum-utils-1.1.16-13.el5_4.1

≫ Group: Development/Tools

≫ Summary: Utilities based around the yum package manager

≫ Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-manager.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

zsh-4.2.6-3.el5 - zsh-4.2.6-5.el5

≫ Group: System Environment/Shells

≫ Summary: A powerful interactive shell

≫ Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

A.2. Server

A.2.1. Added Packages

bind97-9.7.0-6.P2.el5

> ❧ Group: System Environment/Daemons

> ❧ Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server

> ❧ Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

c-ares-1.6.0-5.el5

> ❧ Group: System Environment/Libraries

> ❧ Summary: A library that performs asynchronous DNS operations

> ❧ Description: c-ares is a C library that performs DNS requests and name resolves asynchronously. c-ares is a fork of the library named 'ares', written by Greg Hudson at MIT.

certmonger-0.30-4.el5

> ❧ Group: System Environment/Daemons

> ❧ Summary: Certificate status monitor and PKI enrollment client

> ❧ Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.

dropwatch-1.2-2.el5

> ❧ Group: Applications/System

> ❧ Summary: Kernel dropped packet monitor

> ❧ Description: dropwatch is an utility to interface to the kernel to monitor for dropped network packets.

ebtables-2.0.9-5.el5

> ❧ Group: System Environment/Base

> ❧ Summary: Ethernet Bridge frame table administration tool

> ❧ Description: Ethernet bridge tables is a firewalling tool to transparently filter network traffic passing a bridge. The filtering possibilities are limited to link layer filtering and some basic filtering on higher network layers. This tool is the userspace control for the bridge and ebtables kernel components. The ebtables tool can be used together with the other Linux filtering tools, like iptables. There are no known incompatibility issues.

hplip3-3.9.8-11.el5

❧ Group: System Environment/Daemons

❧ Summary: HP Linux Imaging and Printing Project

❧ Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.

ipa-client-2.0-10.el5

❧ Group: System Environment/Base

❧ Summary: IPA authentication for use on clients

❧ Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).

ipa-gothic-fonts-003.02-3.1.el5

❧ Group: User Interface/X

❧ Summary: Japanese Gothic-typeface OpenType font by IPA

❧ Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Gothic (sans-serif) style font.

ipa-mincho-fonts-003.02-2.1.el5

❧ Group: User Interface/X

❧ Summary: Japanese Mincho-typeface OpenType font by IPA

❧ Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Mincho style font.

ipa-pgothic-fonts-003.02-3.1.el5

❧ Group: User Interface/X

❧ Summary: Japanese Proportional Gothic-typeface OpenType font by IPA

❧ Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Proportional Gothic (sans-serif) style font.

ipa-pmincho-fonts-003.02-2.1.el5

❧ Group: User Interface/X

❧ Summary: Japanese Proportional Mincho-typeface OpenType font by IPA

❧ Description: IPA Font is a Japanese OpenType fonts that is JIS X 0213:2004 compliant, provided by Information-technology Promotion Agency, Japan. This package contains Proportional Mincho style font.

libldb-0.9.10-33.el5

❧ Group: Development/Libraries

❧ Summary: A schema-less, ldap like, API and database

➢ Description: An extensible library that implements an LDAP like API to access remote LDAP servers, or use local tdb databases.

libtalloc-2.0.1-11.el5

➢ Group: System Environment/Daemons

➢ Summary: A hierarchical memory allocator

➢ Description: A library that implements a hierarchical allocator with destructors.

libtdb-1.2.1-5.el5

➢ Group: System Environment/Daemons

➢ Summary: The tdb library

➢ Description: A library that implements a trivial database.

libtevent-0.9.8-10.el5

➢ Group: System Environment/Daemons

➢ Summary: Talloc-based, event-driven mainloop

➢ Description: Tevent is an event system based on the talloc memory management library. Tevent has support for many event types, including timers, signals, and the classic file descriptor events. Tevent also provide helpers to deal with asynchronous code providing the tevent_req (Tevent Request) functions.

mod_revocator-1.0.3-5.el5

➢ Group: System Environment/Daemons

➢ Summary: CRL retrieval module for the Apache HTTP server

➢ Description: The mod_revocator module retrieves and installs remote Certificate Revocate Lists (CRLs) into an Apache web server.

php53-5.3.3-1.el5

➢ Group: Development/Languages

➢ Summary: PHP scripting language for creating dynamic web sites

➢ Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.

python-pycurl-7.15.5.1-8.el5

➢ Group: Development/Languages

➢ Summary: A Python interface to libcurl

➢ Description: PycURL is a Python interface to libcurl. PycURL can be used to fetch objects identified by a URL from a Python program, similar to the urllib Python module. PycURL is mature, very fast, and supports a lot of features.

sssd-1.2.1-39.el5

⪼ Group: Applications/System

⪼ Summary: System Security Services Daemon

⪼ Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

xmlrpc-c-1.16.24-1206.1840.el5

⪼ Group: System Environment/Libraries

⪼ Summary: A lightweight RPC library based on XML and HTTP

⪼ Description: XML-RPC is a quick-and-easy way to make procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML. This library provides a modular implementation of XML-RPC for C.

A.2.2. Updated Packages

ImageMagick-6.2.8.0-4.el5_1.1 - ImageMagick-6.2.8.0-4.el5_5.3

⪼ Group: Applications/Multimedia

⪼ Summary: An X application for displaying and manipulating images.

⪼ Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.

⪼ No added dependencies

⪼ No removed dependencies

⪼ No added provides

⪼ No removed provides

⪼ No added conflicts

⪼ No removed conflicts

⪼ No added obsoletes

⪼ No removed obsoletes

NetworkManager-0.7.0-10.el5 - NetworkManager-0.7.0-10.el5_5.2

⪼ Group: System Environment/Base

➤ Summary: Network connection manager and user applications

➤ Description: NetworkManager attempts to keep an active network connection available at all times. It is intended only for the desktop use-case, and is not intended for usage on servers. The point of NetworkManager is to make networking configuration and setup as painless and automatic as possible. If using DHCP, NetworkManager is intended to replace default routes, obtain IP addresses from a DHCP server, and change nameservers whenever it sees fit.

➤ Added Dependencies:

  ▪ dbus-glib-devel >= 0.73-10

➤ Removed Dependencies:

  ▪ dbus-glib-devel >= 0.73-6

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

OpenIPMI-2.0.16-7.el5 - OpenIPMI-2.0.16-11.el5

➤ Group: System Environment/Base

➤ Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools

➤ Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

amtu-1.0.6-1.el5 - amtu-1.0.6-2.el5

➤ Group: System Environment/Base

➤ Summary: Abstract Machine Test Utility (AMTU)

≫ Description: Abstract Machine Test Utility (AMTU) is an administrative utility to check whether the underlying protection mechanism of the hardware are still being enforced. This is a requirement of the Controlled Access Protection Profile FPT_AMT.1, see http://www.radium.ncsc.mil/tpep/library/protection_profiles/CAPP-1.d.pdf

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

anaconda-11.1.2.209-1 - anaconda-11.1.2.224-1

≫ Group: Applications/System

≫ Summary: Graphical system installer

≫ Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.

≫ Added Dependencies:

  ▪ kudzu-devel >= 1.2.57.1.26-1

  ▪ pciutils-devel >= 3.1.7-3

≫ Removed Dependencies:

  ▪ kudzu-devel >= 1.2.57.1.18

  ▪ pciutils-devel

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

apr-1.2.7-11.el5_3.1 - apr-1.2.7-11.el5_5.3

≫ Group: System Environment/Libraries

≫ Summary: Apache Portable Runtime library

➤ Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines, forming a system portability layer to as many operating systems as possible, including Unices, MS Win32, BeOS and OS/2.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

apr-util-1.2.7-11.el5 - apr-util-1.2.7-11.el5_5.2

➤ Group: System Environment/Libraries

➤ Summary: Apache Portable Runtime Utility library

➤ Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing and more.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

audit-1.7.17-3.el5 - audit-1.7.18-2.el5

➤ Group: System Environment/Daemons

➤ Summary: User space tools for 2.6 kernel auditing

➤ Description: The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

autofs-5.0.1-0.rc2.143.el5 - autofs-5.0.1-0.rc2.143.el5_5.6

- Group: System Environment/Daemons

- Summary: A tool for automatically mounting and unmounting filesystems.

- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

avahi-0.6.16-7.el5 - avahi-0.6.16-9.el5_5

- Group: System Environment/Base

- Summary: Local network service discovery

- Description: Avahi is a system which facilitates service discovery on a local network -- this means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind of technology is already found in MacOS X (branded 'Rendezvous', 'Bonjour' and sometimes 'ZeroConf') and is very convenient.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

bind-9.3.6-4.P1.el5_4.2 - bind-9.3.6-16.P1.el5

» Group: System Environment/Daemons

» Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.

» Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

bzip2-1.0.3-4.el5_2 - bzip2-1.0.3-6.el5_5

» Group: Applications/File

» Summary: A file compression utility.

» Description: Bzip2 is a freely available, patent-free, high quality data compressor. Bzip2 compresses files to within 10 to 15 percent of the capabilities of the best techniques available. However, bzip2 has the added benefit of being approximately two times faster at compression and six times faster at decompression than those techniques. Bzip2 is not the fastest compression utility, but it does strike a balance between speed and compression capability. Install bzip2 if you need a compression utility.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

cman-2.0.115-34.el5 - cman-2.0.115-68.el5

» Group: System Environment/Base

» Summary: cman - The Cluster Manager

- Description: cman - The Cluster Manager

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

cmirror-1.1.39-8.el5 - cmirror-1.1.39-10.el5

- Group: System Environment/Base

- Summary: cmirror - The Cluster Mirror Package

- Description: cmirror - Cluster Mirroring

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

compat-gcc-34-3.4.6-4 - compat-gcc-34-3.4.6-4.1

- Group: Development/Languages

- Summary: Compatibility GNU Compiler Collection

- Description: This package includes a GCC 3.4.6-RH compatibility compiler.

- Added Dependencies:

  - /lib/libc.so.6

  - /lib64/libc.so.6

  - /usr/lib/libc.so

  - /usr/lib64/libc.so

- No removed dependencies

- No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

conga-0.12.2-12.el5 - conga-0.12.2-24.el5

⯈ Group: System Environment/Base

⯈ Summary: Remote Management System

⯈ Description: Conga is a project developing management system for remote stations. It consists of luci, https frontend, and ricci, secure daemon that dispatches incoming messages to underlying management modules.

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

coolkey-1.1.0-14.el5 - coolkey-1.1.0-15.el5

⯈ Group: System Environment/Libraries

⯈ Summary: CoolKey PKCS #11 module

⯈ Description: Linux Driver support for the CoolKey and CAC products.

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

cpufreq-utils-005-1.el5 - cpufreq-utils-005-3.el5

⯈ Group: System Environment/Base

➤ Summary: CPU Frequency changing related utilities

➤ Description: cpufreq-utils contains several utilities that can be used to control the cpufreq interface provided by the kernel on hardware that supports CPU frequency scaling.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

crash-4.1.2-4.el5 - crash-4.1.2-8.el5

➤ Group: Development/Debuggers

➤ Summary: crash utility for live systems; netdump, diskdump, kdump, LKCD or mcore dumpfiles

➤ Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

ctdb-1.0.82-1.el5 - ctdb-1.0.112-1.el5

➤ Group: System Environment/Daemons

➤ Summary: A Clustered Database based on Samba's Trivial Database (TDB)

➤ Description: CTDB is a cluster implementation of the TDB database used by Samba and other projects to store temporary data. If an application is already using TDB for temporary data it is very easy to convert that application to be cluster aware and use CTDB instead.

➤ No added dependencies

➤ No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

cups-1.3.7-18.el5 - cups-1.3.7-26.el5

- Group: System Environment/Daemons

- Summary: Common Unix Printing System

- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

dapl-2.0.25-2.el5 - dapl-2.0.25-2.el5_5.1

- Group: System Environment/Libraries

- Summary: Library providing access to the DAT 1.2 and 2.0 APIs

- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

db4-4.3.29-10.el5 - db4-4.3.29-10.el5_5.2

➤ Group: System Environment/Libraries

➤ Summary: The Berkeley DB database library (version 4) for C.

➤ Description: The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

dbus-glib-0.73-8.el5 - dbus-glib-0.73-10.el5_5

➤ Group: System Environment/Libraries

➤ Summary: GLib bindings for D-Bus

➤ Description: D-Bus add-on library to integrate the standard D-Bus library with the GLib thread abstraction and main loop.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

devhelp-0.12-20.el5 - devhelp-0.12-21.el5

➤ Group: Development/Tools

➤ Summary: API document browser

➤ Description: An API document browser for GNOME 2.

➣ Added Dependencies:

⬛ gecko-devel-unstable >= 1.9.2

➣ Removed Dependencies:

⬛ gecko-devel-unstable >= 1.9

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

device-mapper-1.02.39-1.el5 - device-mapper-1.02.55-2.el5

➣ Group: System Environment/Base

➣ Summary: device mapper library

➣ Description: This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

device-mapper-multipath-0.4.7-34.el5 - device-mapper-multipath-0.4.7-42.el5

➣ Group: System Environment/Base

➣ Summary: Tools to manage multipath devices using device-mapper.

➣ Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

dhcp-3.0.5-23.el5 - dhcp-3.0.5-23.el5_5.2

» Group: System Environment/Daemons

» Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.

» Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

dhcpv6-1.0.10-18.el5 - dhcpv6-1.0.10-20.el5

» Group: System Environment/Daemons

» Summary: DHCPv6 - DHCP server and client for IPv6

» Description: Implements the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Consists of dhcp6s(8), the server DHCP daemon, and dhcp6r(8), the DHCPv6 relay agent. Install this package if you want to support dynamic configuration of IPv6 addresses and parameters on your IPv6 network.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

297

➤ No added obsoletes

➤ No removed obsoletes

dump-0.4b41-4.el5 - dump-0.4b41-5.el5

➤ Group: Applications/Archiving

➤ Summary: Programs for backing up and restoring ext2/ext3 filesystems

➤ Description: The dump package contains both dump and restore. Dump examines files in a filesystem, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a filesystem. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups. Install dump if you need a system for both backing up filesystems and restoring filesystems after backups.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

dvgrab-3.0-1.el5 - dvgrab-3.0-1.1.el5

➤ Group: Applications/Multimedia

➤ Summary: Utility to capture video from a DV camera

➤ Description: The dvgrab utility will capture digital video from a DV source on the firewire (IEEE-1394) bus.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

e2fsprogs-1.39-23.el5 - e2fsprogs-1.39-23.el5_5.1

➤ Group: System Environment/Base

> ⸎ Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems

> ⸎ Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.

> ⸎ No added dependencies

> ⸎ No removed dependencies

> ⸎ No added provides

> ⸎ No removed provides

> ⸎ No added conflicts

> ⸎ No removed conflicts

> ⸎ No added obsoletes

> ⸎ No removed obsoletes

e4fsprogs-1.41.9-3.el5 - e4fsprogs-1.41.12-2.el5

> ⸎ Group: System Environment/Base

> ⸎ Summary: Utilities for managing the fourth extended (ext4) filesystem

> ⸎ Description: The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 filesystem.

> ⸎ No added dependencies

> ⸎ No removed dependencies

> ⸎ No added provides

> ⸎ No removed provides

> ⸎ No added conflicts

> ⸎ No removed conflicts

> ⸎ No added obsoletes

> ⸎ No removed obsoletes

esc-1.1.0-11.el5 - esc-1.1.0-12.el5

- ≫ Group: Applications/Internet

- ≫ Summary: Enterprise Security Client Smart Card Client

- ≫ Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.

- ≫ Added Dependencies:

  - ▫ xulrunner >= 1.9.2

  - ▫ xulrunner-devel >= 1.9.2

- ≫ Removed Dependencies:

  - ▫ xulrunner

  - ▫ xulrunner-devel

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

exim-4.63-5.el5 - exim-4.63-5.el5_5.2

- ≫ Group: System Environment/Daemons

- ≫ Summary: The exim mail transfer agent

- ≫ Description: Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. It is freely available under the terms of the GNU General Public Licence. In style it is similar to Smail 3, but its facilities are more general. There is a great deal of flexibility in the way mail can be routed, and there are extensive facilities for checking incoming mail. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

expat-1.95.8-8.3.el5_4.2 - expat-1.95.8-8.3.el5_5.3

➤ Group: System Environment/Libraries

➤ Summary: A library for parsing XML.

➤ Description: This is expat, the C library for parsing XML, written by James Clark. Expat is a stream oriented XML parser. This means that you register handlers with the parser prior to starting the parse. These handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

firefox-3.0.18-1.el5_4 - firefox-3.6.13-2.el5

➤ Group: Applications/Internet

➤ Summary: Mozilla Firefox Web browser

➤ Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

➤ Added Dependencies:

   ▫ xulrunner-devel >= 1.9.2.13-3

➤ Removed Dependencies:

   ▫ xulrunner-devel >= 1.9.0.18-1

   ▫ xulrunner-devel-unstable >= 1.9.0.18-1

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

freetype-2.2.1-21.el5_3 - freetype-2.2.1-28.el5_5.1

➤ Group: System Environment/Libraries

» Summary: A free and portable font rendering engine

» Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

gcc-4.1.2-48.el5 - gcc-4.1.2-50.el5

» Group: Development/Languages

» Summary: Various compilers (C, C++, Objective-C, Java, ...)

» Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

gcc44-4.4.0-6.el5 - gcc44-4.4.4-13.el5

» Group: Development/Languages

» Summary: Preview of GCC version 4.4

» Description: The gcc44 package contains preview of the GNU Compiler Collection version 4.4.

» Added Dependencies:

  ▫ gdb

» No removed dependencies

» No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

gdb-7.0.1-23.el5 - gdb-7.0.1-32.el5

≫ Group: Development/Debuggers

≫ Summary: A GNU source-level debugger for C, C++, Java and other languages

≫ Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.

≫ Added Dependencies:

◻ libstdc++

◻ python-devel

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

gettext-0.14.6-4.el5 - gettext-0.17-1.el5

≫ Group: Development/Tools

≫ Summary: GNU libraries and utilities for producing multi-lingual messages

≫ Description: The GNU gettext package provides a set of tools and documentation for producing multi-lingual messages in programs. Tools include a set of conventions about how programs should be written to support message catalogs, a directory and file naming organization for the message catalogs, a runtime library which supports the retrieval of translated messages, and stand-alone programs for handling the translatable and the already translated strings. Gettext provides an easy to use library and tools for creating, using, and modifying natural language catalogs and is a powerful and simple method for internationalizing programs.

≫ Added Dependencies:

◻ autoconf

◻ automake

◻ expat-devel

≫ Removed Dependencies:

  ▫ /usr/bin/fastjar

  ▫ gcc-java

  ▫ libgcj

  ▫ unzip

  ▫ zip

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

gfs-kmod-0.1.34-12.el5 - gfs-kmod-0.1.34-15.el5

≫ Group: System Environment/Kernel

≫ Summary: gfs kernel modules

≫ Description: gfs - The Global File System is a symmetric, shared-disk, cluster file system.

≫ Added Dependencies:

  ▫ kernel-devel-ia64 = 2.6.18-223.el5

  ▫ kernel-xen-devel-ia64 = 2.6.18-223.el5

≫ Removed Dependencies:

  ▫ kernel-devel-ia64 = 2.6.18-192.el5

  ▫ kernel-xen-devel-ia64 = 2.6.18-192.el5

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

gfs-utils-0.1.20-7.el5 - gfs-utils-0.1.20-8.el5

≫ Group: System Environment/Kernel

≫ Summary: Utilities for managing the global filesystem (GFS)

➢ Description: The gfs-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

gfs2-utils-0.1.62-20.el5 - gfs2-utils-0.1.62-28.el5

➢ Group: System Environment/Kernel

➢ Summary: Utilities for managing the global filesystem (GFS)

➢ Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

ghostscript-8.15.2-9.11.el5 - ghostscript-8.70-6.el5

➢ Group: Applications/Publishing

➢ Summary: A PostScript(TM) interpreter and renderer.

➢ Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.

➢ No added dependencies

➢ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

glibc-2.5-49 - glibc-2.5-58

- ≫ Group: System Environment/Libraries

- ≫ Summary: The GNU libc libraries.

- ≫ Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

gnome-python2-extras-2.14.2-6.el5 - gnome-python2-extras-2.14.2-7.el5

- ≫ Group: Development/Languages

- ≫ Summary: The sources for additional. PyGNOME Python extension modules.

- ≫ Description: The gnome-python-extra package contains the source packages for additional Python bindings for GNOME. It should be used together with gnome-python.

- ≫ Added Dependencies:

  - ▣ gecko-devel-unstable >= 1.9.2

- ≫ Removed Dependencies:

  - ▣ gecko-devel-unstable >= 1.9

- ≫ No added provides

- ≫ No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gnome-screensaver-2.16.1-8.el5 - gnome-screensaver-2.16.1-8.el5_5.2

- Group: Amusements/Graphics

- Summary: GNOME Screensaver

- Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gnome-session-2.16.0-7.el5 - gnome-session-2.16.0-8.el5

- Group: User Interface/Desktops

- Summary: GNOME session manager

- Description: gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

gnome-vfs2-2.16.2-6.el5 - gnome-vfs2-2.16.2-6.el5_5.1

- Group: System Environment/Libraries

- Summary: The GNOME virtual file-system libraries

❯ Description: GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

gnupg-1.4.5-14 - gnupg-1.4.5-14.el5_5.1

❯ Group: Applications/System

❯ Summary: A GNU utility for secure communication and data storage.

❯ Description: GnuPG (GNU Privacy Guard) is a GNU utility for encrypting data and creating digital signatures. GnuPG has advanced key management capabilities and is compliant with the proposed OpenPGP Internet standard described in RFC2440. Since GnuPG doesn't use any patented algorithm, it is not compatible with any version of PGP2 (PGP2.x uses only IDEA for symmetric-key encryption, which is patented worldwide).

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

gnupg2-2.0.10-3.el5 - gnupg2-2.0.10-3.el5_5.1

❯ Group: Applications/System

❯ Summary: Utility for secure communication and data storage

❯ Description: GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440 and the S/MIME standard as described by several RFCs. GnuPG 2.0 is the stable version of GnuPG integrating support for OpenPGP and S/MIME. It does not conflict with an installed 1.x OpenPGP-only version. GnuPG 2.0 is a newer version of GnuPG with additional

support for S/MIME. It has a different design philosophy that splits functionality up into several modules. Both versions may be installed simultaneously without any conflict (gpg is called gpg2 in GnuPG 2). In fact, the gpg version from GnuPG 1.x is able to make use of the gpg-agent as included in GnuPG 2 and allows for seamless passphrase caching. The advantage of GnupG 1.x is its smaller size and no dependency on other modules at run and build time.

- » No added dependencies

- » No removed dependencies

- » No added provides

- » No removed provides

- » No added conflicts

- » No removed conflicts

- » No added obsoletes

- » No removed obsoletes

gnutls-1.4.1-3.el5_3.5 - gnutls-1.4.1-3.el5_4.8

- » Group: System Environment/Libraries

- » Summary: A TLS protocol implementation.

- » Description: GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer. Currently the GnuTLS library implements the proposed standards by the IETF's TLS working group.

- » No added dependencies

- » No removed dependencies

- » No added provides

- » No removed provides

- » No added conflicts

- » No removed conflicts

- » No added obsoletes

- » No removed obsoletes

gtk2-2.10.4-20.el5 - gtk2-2.10.4-21.el5_5.6

- » Group: System Environment/Libraries

- » Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X

- » Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.

- » No added dependencies

- » No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

hal-0.5.8.1-59.el5 - hal-0.5.8.1-62.el5

- ≫ Group: System Environment/Libraries

- ≫ Summary: Hardware Abstraction Layer

- ≫ Description: HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

hplip-1.6.7-4.1.el5_2.4 - hplip-1.6.7-6.el5

- ≫ Group: System Environment/Daemons

- ≫ Summary: HP Linux Imaging and Printing Project

- ≫ Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

httpd-2.2.3-43.el5 - httpd-2.2.3-45.el5

- Group: System Environment/Daemons

- Summary: Apache HTTP Server

- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

hwdata-0.213.18-1.el5.1 - hwdata-0.213.22-1.el5

- Group: System Environment/Base

- Summary: Hardware identification and configuration data

- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

icu-3.6-5.11.4 - icu-3.6-5.16

- Group: System Environment/Libraries

- Summary: International Components for Unicode

- Description: The International Components for Unicode (ICU) libraries provide robust and full-featured Unicode services on a wide variety of platforms. ICU supports the most current version of the Unicode standard, and they provide support for supplementary Unicode characters (needed for GB 18030 repertoire support). As computing environments become more heterogeneous, software portability becomes more important. ICU lets you produce the same results across all the various platforms you support, without sacrificing performance. It offers great flexibility to extend and customize the supplied services.

- No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

initscripts-8.45.30-2.el5 - initscripts-8.45.33-1.el5

➣ Group: System Environment/Base

➣ Summary: The inittab file and the /etc/init.d scripts.

➣ Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

➣ No removed obsoletes

iprutils-2.2.18-1.el5 - iprutils-2.3.0-2.el5

➣ Group: System Environment/Base

➣ Summary: Utilities for the IBM Power Linux RAID adapters

➣ Description: Provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.

➣ No added dependencies

➣ No removed dependencies

➣ No added provides

➣ No removed provides

➣ No added conflicts

➣ No removed conflicts

➣ No added obsoletes

≫ No removed obsoletes

ipsec-tools-0.6.5-13.el5_3.1 - ipsec-tools-0.6.5-14.el5_5.5

≫ Group: System Environment/Base

≫ Summary: Tools for configuring and using IPSEC

≫ Description: This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds: - setkey, a program to directly manipulate policies and SAs - racoon, an IKEv1 keying daemon

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

ipvsadm-1.24-10 - ipvsadm-1.24-12.el5

≫ Group: Applications/System

≫ Summary: Utility to administer the Linux Virtual Server

≫ Description: ipvsadm is a utility to administer the IP Virtual Server services offered by the Linux kernel.

≫ Added Dependencies:

  ▪ popt

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

iscsi-initiator-utils-6.2.0.871-0.16.el5 - iscsi-initiator-utils-6.2.0.872-6.el5

≫ Group: System Environment/Daemons

≫ Summary: iSCSI daemon and utility programs

≫ Description: The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using

SCSI commands sent over Internet Protocol networks.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

isns-utils-0.91-0.1.el5 - isns-utils-0.93-1.0.el5

‣ Group: System Environment/Daemons

‣ Summary: The iSNS daemon and utility programs

‣ Description: The iSNS package contains the daemon and tools to setup a iSNS server, and iSNS client tools. The Internet Storage Name Service (iSNS) protocol allows automated discovery, management and configuration of iSCSI and Fibre Channel devices (using iFCP gateways) on a TCP/IP network.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5 - java-1.6.0-openjdk-1.6.0.0-1.16.b17.el5

‣ Group: Development/Languages

‣ Summary: OpenJDK Runtime Environment

‣ Description: The OpenJDK runtime environment.

‣ Added Dependencies:

  ▪ autoconf

  ▪ automake

  ▪ java-1.6.0-openjdk-devel

‣ Removed Dependencies:

- openmotif-devel

- prelink

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

jwhois-3.2.3-8.el5 - jwhois-3.2.3-11.el5

≫ Group: Applications/Internet

≫ Summary: Internet whois/nicname client.

≫ Description: A whois client that accepts both traditional and finger-style queries.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

kdebase-3.5.4-20.el5 - kdebase-3.5.4-22.el5

≫ Group: User Interface/Desktops

≫ Summary: K Desktop Environment - core files

≫ Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).

≫ Added Dependencies:

- libsmbclient-devel

≫ Removed Dependencies:

- samba >= 2.2.3a-5

≫ No added provides

- ❥ No removed provides

- ❥ No added conflicts

- ❥ No removed conflicts

- ❥ No added obsoletes

- ❥ No removed obsoletes

kernel-2.6.18-194.el5 - kernel-2.6.18-238.el5

- ❥ Group: System Environment/Kernel

- ❥ Summary: The Linux kernel (the core of the Linux operating system)

- ❥ Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

- ❥ No added dependencies

- ❥ Removed Dependencies:

  - ▫ rpmlib(VersionedDependencies) <= 3.0.3-1

- ❥ No added provides

- ❥ No removed provides

- ❥ No added conflicts

- ❥ No removed conflicts

- ❥ No added obsoletes

- ❥ No removed obsoletes

kexec-tools-1.102pre-96.el5 - kexec-tools-1.102pre-126.el5

- ❥ Group: Applications/System

- ❥ Summary: The kexec/kdump userspace component.

- ❥ Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.

- ❥ No added dependencies

- ❥ No removed dependencies

- ❥ No added provides

- ❥ No removed provides

- ❥ No added conflicts

- ❥ No removed conflicts

- ❥ No added obsoletes

≫ No removed obsoletes

krb5-1.6.1-36.el5_4.1 - krb5-1.6.1-55.el5

≫ Group: System Environment/Libraries

≫ Summary: The Kerberos network authentication system.

≫ Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.

≫ Added Dependencies:

  ▪ openldap-devel

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

ksh-20100202-1.el5 - ksh-20100202-1.el5_5.1

≫ Group: Applications/Shells

≫ Summary: The Original ATT Korn Shell

≫ Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

kudzu-1.2.57.1.24-1 - kudzu-1.2.57.1.26-1

≫ Group: Applications/System

≫ Summary: The Red Hat Linux hardware probing tool.

≫ Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the system.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

kvm-83-164.el5 - kvm-83-224.el5

≫ Group: Development/Tools

≫ Summary: Kernel-based Virtual Machine

≫ Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.

≫ Added Dependencies:

  ▫ kernel-debug-devel = 2.6.18-237.el5

  ▫ kernel-devel = 2.6.18-237.el5

  ▫ libgcrypt-devel

≫ Removed Dependencies:

  ▫ kernel-devel

  ▫ kernel-devel-x86_64 = 2.6.18-191.el5

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

less-436-2.el5 - less-436-7.el5

≫ Group: Applications/Text

≫ Summary: A text file browser similar to more, but better.

≫ Description: The less utility is a text file browser that resembles more, but has more capabilities. Less allows you to move backwards in the file as well as forwards. Since less doesn't have to

read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

lftp-3.7.11-4.el5 - lftp-3.7.11-4.el5_5.3

❧ Group: Applications/Internet

❧ Summary: A sophisticated file transfer program

❧ Description: LFTP is a sophisticated ftp/http file transfer program. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

libbonobo-2.16.0-1.fc6 - libbonobo-2.16.0-1.1.el5_5.1

❧ Group: System Environment/Libraries

❧ Summary: Bonobo component system

❧ Description: Bonobo is a component system based on CORBA, used by the GNOME desktop.

❧ Added Dependencies:

  ▪ dbus-glib-devel

❧ No removed dependencies

❧ No added provides

❧ No removed provides

>> No added conflicts

>> No removed conflicts

>> No added obsoletes

>> No removed obsoletes

libhugetlbfs-1.3-7.el5 - libhugetlbfs-1.3-8.2.el5

>> Group: System Environment/Libraries

>> Summary: Library to access the Huge TLB Filesystem

>> Description: The libhugetlbfs library interacts with the Linux hugetlbfs to make large pages available to applications in a transparent manner.

>> No added dependencies

>> No removed dependencies

>> No added provides

>> No removed provides

>> No added conflicts

>> No removed conflicts

>> No added obsoletes

>> No removed obsoletes

libpng-1.2.10-7.1.el5_3.2 - libpng-1.2.10-7.1.el5_5.3

>> Group: System Environment/Libraries

>> Summary: A library of functions for manipulating PNG image format files

>> Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG format image files.

>> No added dependencies

>> No removed dependencies

>> No added provides

>> No removed provides

>> No added conflicts

>> No removed conflicts

>> No added obsoletes

>> No removed obsoletes

libselinux-1.33.4-5.5.el5 - libselinux-1.33.4-5.7.el5

➤ Group: System Environment/Libraries

➤ Summary: SELinux library and simple utilities

➤ Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libselinux provides an API for SELinux applications to get and set process and file security contexts and to obtain security policy decisions. Required for any applications that use the SELinux API.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

libtiff-3.8.2-7.el5_3.4 - libtiff-3.8.2-7.el5_5.5

➤ Group: System Environment/Libraries

➤ Summary: Library of functions for manipulating TIFF format image files

➤ Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image files.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

libvirt-0.6.3-33.el5 - libvirt-0.8.2-15.el5

➤ Group: Development/Libraries

➤ Summary: Library providing a simple API virtualization

❧ Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).

❧ Added Dependencies:

- audit-libs-devel

- autoconf

- automake

- curl-devel

- device-mapper

- libselinux-devel >= 1.33.4-5.6

- libxslt

❧ Removed Dependencies:

- libselinux-devel

- python

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

libxml2-2.6.26-2.1.2.8 - libxml2-2.6.26-2.1.2.8.el5_5.1

❧ Group: Development/Libraries

❧ Summary: Library providing XML and HTML support

❧ Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

linuxwacom-0.7.8.3-8.el5 - linuxwacom-0.7.8.3-10.el5

≫ Group: User Interface/X Hardware Support

≫ Summary: Wacom Drivers from Linux Wacom Project

≫ Description: The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

logrotate-3.7.4-9 - logrotate-3.7.4-9.el5_5.2

≫ Group: System Environment/Base

≫ Summary: Rotates, compresses, removes and mails system log files.

≫ Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your system.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

lvm2-2.02.56-8.el5 - lvm2-2.02.74-5.el5

≫ Group: System Environment/Base

‣ Summary: Userland logical volume management tools

‣ Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.

‣ Added Dependencies:

  ▪ device-mapper >= 1.02.55-2

‣ Removed Dependencies:

  ▪ device-mapper >= 1.02.39-1

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

lvm2-cluster-2.02.56-7.el5 - lvm2-cluster-2.02.74-3.el5

‣ Group: System Environment/Base

‣ Summary: Cluster extensions for userland logical volume management tools

‣ Description: Extensions to LVM2 to support clusters.

‣ Added Dependencies:

  ▪ device-mapper >= 1.02.55-2

‣ Removed Dependencies:

  ▪ device-mapper >= 1.02.39-1

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

m2crypto-0.16-6.el5.6 - m2crypto-0.16-6.el5.8

‣ Group: System Environment/Libraries

‣ Summary: Support for using OpenSSL in python scripts

‣ Description: This package allows you to call OpenSSL functions from python scripts.

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

mailman-2.1.9-4.el5 - mailman-2.1.9-6.el5

⯈ Group: Applications/Internet

⯈ Summary: Mailing list manager with built in Web access.

⯈ Description: Mailman is software to help manage email discussion lists, much like Majordomo and Smartmail. Unlike most similar products, Mailman gives each mailing list a webpage, and allows users to subscribe, unsubscribe, etc. over the Web. Even the list manager can administer his or her list entirely from the Web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail <-> news gateways, and so on. Documentation can be found in: /usr/share/doc/mailman-2.1.9 When the package has finished installing, you will need to perform some additional installation steps, these are described in: /usr/share/doc/mailman-2.1.9/INSTALL.REDHAT

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

man-pages-2.39-15.el5 - man-pages-2.39-17.el5

⯈ Group: Documentation

⯈ Summary: Man (manual) pages from the Linux Documentation Project.

⯈ Description: A large collection of man pages (documentation) from the Linux Documentation Project (LDP).

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

man-pages-ja-20060815-13.el5 - man-pages-ja-20060815-14.el5

- Group: Documentation

- Summary: Japanese man (manual) pages from the Japanese Manual Project

- Description: Japanese Manual pages, translated by JM-Project (Japanese Manual Project).

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

metacity-2.16.0-15.el5 - metacity-2.16.0-16.el5

- Group: User Interface/Desktops

- Summary: Metacity window manager

- Description: Metacity is a simple window manager that integrates nicely with GNOME 2.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

microcode_ctl-1.17-1.50.el5 - microcode_ctl-1.17-1.52.el5

- Group: System Environment/Base

- Summary: Tool to update x86/x86-64 CPU microcode.

❧ Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

mikmod-3.1.6-38.1 - mikmod-3.1.6-39.el5_5.1

❧ Group: Applications/Multimedia

❧ Summary: A MOD music file player.

❧ Description: MikMod is one of the best and most well known MOD music file players for UNIX-like systems. This particular distribution is intended to compile fairly painlessly in a Linux environment. MikMod uses the OSS /dev/dsp driver including all recent kernels for output, and will also write .wav files. Supported file formats include MOD, STM, S3M, MTM, XM, ULT, and IT. The player uses ncurses for console output and supports transparent loading from gzip/pkzip/zoo archives and the loading/saving of playlists. Install the mikmod package if you need a MOD music file player.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

mkinitrd-5.1.19.6-61 - mkinitrd-5.1.19.6-68.el5

❧ Group: System Environment/Base

❧ Summary: Creates an initial ramdisk image for preloading modules.

❧ Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used.

The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

mod_authz_ldap-0.26-9.el5 - mod_authz_ldap-0.26-9.el5_5.1

- Group: System Environment/Daemons

- Summary: LDAP authorization module for the Apache HTTP Server

- Description: The mod_authz_ldap package provides support for authenticating users of the Apache HTTP server against an LDAP database. mod_authz_ldap features the ability to authenticate users based on the SSL client certificate presented, and also supports password aging, and authentication based on role or by configured filters.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

mod_nss-1.0.3-8.el5 - mod_nss-1.0.8-3.el5

- Group: System Environment/Daemons

- Summary: SSL/TLS module for the Apache HTTP server

- Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security library.

- Added Dependencies:

  - httpd-devel

- nspr-devel

- nss-devel >= 3.12.6

» Removed Dependencies:

- httpd-devel >= 0:2.0.52

- nspr-devel >= 4.6

- nss-devel >= 3.11

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

module-init-tools-3.3-0.pre3.1.60.el5 - module-init-tools-3.3-0.pre3.1.60.el5_5.1

» Group: System Environment/Kernel

» Summary: Kernel module management utilities.

» Description: The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

mysql-5.0.77-4.el5_4.2 - mysql-5.0.77-4.el5_5.4

» Group: Applications/Databases

» Summary: MySQL client programs and shared libraries

» Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

net-snmp-5.3.2.2-9.el5 - net-snmp-5.3.2.2-9.el5_5.1

» Group: System Environment/Daemons

» Summary: A collection of SNMP protocol tools and libraries.

» Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

nfs-utils-1.0.9-44.el5 - nfs-utils-1.0.9-50.el5

» Group: System Environment/Daemons

» Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.

» Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.

» No added dependencies

» Removed Dependencies:

- nfs-utils-lib-devel >= 1.0.8-2

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

nspluginwrapper-1.3.0-8.el5 - nspluginwrapper-1.3.0-9.el5

» Group: Networking/WWW

» Summary: A compatibility layer for Netscape 4 plugins

» Description: nspluginwrapper makes it possible to use Netscape 4 compatible plugins compiled for ppc into Mozilla for another architecture, e.g. x86_64. This package consists in: * npviewer: the plugin viewer * npwrapper.so: the browser-side plugin * nspluginplayer: stand-alone NPAPI plugin player * mozilla-plugin-config: a tool to manage plugins installation and update

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

nspr-4.7.6-1.el5_4 - nspr-4.8.6-1.el5

» Group: System Environment/Libraries

» Summary: Netscape Portable Runtime

» Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

> ❯ No removed conflicts

> ❯ No added obsoletes

> ❯ No removed obsoletes

nss-3.12.3.99.3-1.el5_3.2 - nss-3.12.8-1.el5

> ❯ Group: System Environment/Libraries

> ❯ Summary: Network Security Services

> ❯ Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.

> ❯ Added Dependencies:

>> ▫ nspr-devel >= 4.8.6

> ❯ Removed Dependencies:

>> ▫ nspr-devel >= 4.6.99

> ❯ No added provides

> ❯ No removed provides

> ❯ No added conflicts

> ❯ No removed conflicts

> ❯ No added obsoletes

> ❯ No removed obsoletes

nss_db-2.2-35.3 - nss_db-2.2-35.4.el5_5

> ❯ Group: System Environment/Libraries

> ❯ Summary: An NSS library for the Berkeley DB.

> ❯ Description: Nss_db is a set of C library extensions which allow Berkeley Databases to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Install nss_db if your flat name service files are too large and lookups are slow.

> ❯ No added dependencies

> ❯ No removed dependencies

> ❯ No added provides

> ❯ No removed provides

> ❯ No added conflicts

> ❯ No removed conflicts

> ❯ No added obsoletes

≫ No removed obsoletes

nss_ldap-253-25.el5 - nss_ldap-253-37.el5

≫ Group: System Environment/Base

≫ Summary: NSS library and PAM module for LDAP.

≫ Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

oddjob-0.27-9.el5 - oddjob-0.27-11.el5

≫ Group: System Environment/Daemons

≫ Summary: A D-BUS service which runs odd jobs on behalf of client applications

≫ Description: oddjob is a D-BUS service which performs particular tasks for clients which connect to it and issue requests using the system-wide message bus.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

openCryptoki-2.2.4-22.el5_4.2 - openCryptoki-2.2.4-22.el5_5.1

≫ Group: Productivity/Security

≫ Summary: Implementation of Cryptoki v2.11 for IBM Crypto Hardware

➤ Description: The PKCS#11 Version 2.11 api implemented for the IBM Crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded) and the IBM eServer Cryptographic Accelerator (FC 4960 on pSeries)

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

openais-0.80.6-16.el5 - openais-0.80.6-28.el5

➤ Group: System Environment/Base

➤ Summary: The openais Standards-Based Cluster Framework executive and APIs

➤ Description: This package contains the openais executive, openais service handlers, default configuration files and init script.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

openldap-2.3.43-12.el5 - openldap-2.3.43-12.el5_5.3

➤ Group: System Environment/Daemons

➤ Summary: The configuration files, libraries, and documentation for OpenLDAP.

➤ Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

➤ No added dependencies

➤ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

openmotif-2.3.1-2.el5_4.1 - openmotif-2.3.1-5.el5_5.1

- ≫ Group: System Environment/Libraries

- ≫ Summary: Open Motif runtime libraries and executables.

- ≫ Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".

- ≫ No added dependencies

- ≫ No removed dependencies

- ≫ No added provides

- ≫ No removed provides

- ≫ No added conflicts

- ≫ No removed conflicts

- ≫ No added obsoletes

- ≫ No removed obsoletes

openssh-4.3p2-41.el5 - openssh-4.3p2-72.el5

- ≫ Group: Applications/Internet

- ≫ Summary: The OpenSSH implementation of SSH protocol versions 1 and 2

- ≫ Description: SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.

- ≫ Added Dependencies:

  - ▪ audit-libs-devel >= 1.7.18

- ≫ Removed Dependencies:

  - ▪ audit-libs-devel

- ≫ No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

openssl-0.9.8e-12.el5_4.6 - openssl-0.9.8e-12.el5_5.7

» Group: System Environment/Libraries

» Summary: The OpenSSL toolkit

» Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

openssl-ibmca-1.0.0.rc2-1.el5.4 - openssl-ibmca-1.0.0.rc2-2.el5

» Group: System Environment/Libraries

» Summary: A dynamic OpenSSL engine for IBMCA

» Description: A dynamic OpenSSL engine for IBMCA crypto hardware on IBM zSeries machines.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

openssl097a-0.9.7a-9.el5_2.1 - openssl097a-0.9.7a-9.el5_4.2

- Group: System Environment/Libraries

- Summary: The OpenSSL toolkit

- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

openswan-2.6.21-5.el5_4.2 - openswan-2.6.21-5.el5_5.3

- Group: System Environment/Daemons

- Summary: Openswan IPSEC implementation

- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4309)

- Added Dependencies:

  - nss-devel >= 3.12.6-2

- Removed Dependencies:

  - nss-devel >= 3.12.3-2

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

pam-0.99.6.2-6.el5_4.1 - pam-0.99.6.2-6.el5_5.2

- Group: System Environment/Base

⯈ Summary: A security tool which provides authentication for applications

⯈ Description: PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.

⯈ No added dependencies

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

pam_krb5-2.2.14-15 - pam_krb5-2.2.14-18.el5

⯈ Group: System Environment/Base

⯈ Summary: A Pluggable Authentication Module for Kerberos 5.

⯈ Description: This is pam_krb5, a pluggable authentication module that can be used with Linux-PAM and Kerberos 5. This module supports password checking, ticket creation, and optional TGT verification and conversion to Kerberos IV tickets. The included pam_krb5afs module also gets AFS tokens if so configured.

⯈ Added Dependencies:

　　▢ gettext-devel

⯈ No removed dependencies

⯈ No added provides

⯈ No removed provides

⯈ No added conflicts

⯈ No removed conflicts

⯈ No added obsoletes

⯈ No removed obsoletes

pango-1.14.9-6.el5 - pango-1.14.9-8.el5

⯈ Group: System Environment/Libraries

⯈ Summary: System for layout and rendering of internationalized text

⯈ Description: Pango is a system for layout and rendering of internationalized text.

⯈ No added dependencies

⯈ No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

passwd-0.73-1 - passwd-0.73-2

- Group: System Environment/Base

- Summary: The passwd utility for setting/changing passwords using PAM

- Description: The passwd package contains a system utility (passwd) which sets and/or changes passwords, using PAM (Pluggable Authentication Modules). To use passwd, you should have PAM installed on your system.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

patch-2.5.4-29.2.3.el5 - patch-2.5.4-31.el5

- Group: Development/Tools

- Summary: The GNU patch command, for modifying/upgrading files.

- Description: The patch program applies diff files to originals. The diff command is used to compare an original to a changed file. Diff lists the changes made to the file. A person who has the original file can then use the patch command with the diff file to add the changes to their original file (patching the file). Patch should be installed because it is a common way of upgrading applications.

- Added Dependencies:

  - libselinux-devel

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

pciutils-2.2.3-8.el5 - pciutils-3.1.7-3.el5

- Group: Applications/System
- Summary: PCI bus related utilities
- Description: The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pcre-6.6-2.el5_1.7 - pcre-6.6-6.el5

- Group: System Environment/Libraries
- Summary: Perl-compatible regular expression library
- Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pcsc-lite-1.4.4-1.el5 - pcsc-lite-1.4.4-4.el5_5

- Group: System Environment/Daemons

≫ Group: System Environment/Daemons

≫ Summary: PC/SC Lite smart card framework and applications

≫ Description: The purpose of PC/SC Lite is to provide a Windows(R) SCard interface in a very small form factor for communicating to smartcards and readers. PC/SC Lite uses the same winscard API as used under Windows(R). This package includes the PC/SC Lite daemon, a resource manager that coordinates communications with smart card readers and smart cards that are connected to the system, as well as other command line tools.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

perl-5.8.8-27.el5 - perl-5.8.8-32.el5_5.2

≫ Group: Development/Languages

≫ Summary: The Perl programming language

≫ Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

perl-Archive-Tar-1.30-1.fc6 - perl-Archive-Tar-1.39.1-1.el5_5.2

≫ Group: Development/Libraries

≫ Summary: A module for Perl manipulation of .tar files

≫ Description: Archive::Tar provides an object oriented mechanism for handling tar files. It

provides class methods for quick and easy files handling while also allowing for the creation of tar file objects for custom manipulation. If you have the IO::Zlib module installed, Archive::Tar will also support compressed or gzipped tar files.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

perl-Sys-Virt-0.2.0-6.el5 - perl-Sys-Virt-0.2.4-1.el5

➤ Group: Development/Libraries

➤ Summary: Perl bindings for the libvirt library

➤ Description: The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.

➤ Added Dependencies:

  ▪ libvirt-devel >= 0.8.1

➤ Removed Dependencies:

  ▪ libvirt-devel >= 0.6.1

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

php-5.1.6-27.el5 - php-5.1.6-27.el5_5.3

➤ Group: Development/Languages

➤ Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)

➤ Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

piranha-0.8.4-16.el5 - piranha-0.8.4-19.el5

❯ Group: System Environment/Base

❯ Summary: Cluster administation tools

❯ Description: Various tools to administer and configure the Linux Virtual Server as well as heartbeating and failover components. The LVS is a dynamically adjusted kernel routing mechanism that provides load balancing primarily for web and ftp servers though other services are supported.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

pirut-1.3.28-17.el5 - pirut-1.3.28-19.el5

❯ Group: Applications/System

❯ Summary: Package Installation, Removal and Update Tools

❯ Description: pirut (pronounced "pirate") provides a set of graphical tools for managing software.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

- No added obsoletes

- No removed obsoletes

poppler-0.5.4-4.4.el5_4.11 - poppler-0.5.4-4.4.el5_5.14

- Group: Development/Libraries

- Summary: PDF rendering library

- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

postgresql-8.1.18-2.el5_4.1 - postgresql-8.1.22-1.el5_5.1

- Group: Applications/Databases

- Summary: PostgreSQL client programs and libraries.

- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

- No added dependencies

- Removed Dependencies:

    - rpmlib(VersionedDependencies) <= 3.0.3-1

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

postgresql84-8.4.2-5.el5 - postgresql84-8.4.5-1.el5_5.1

❧ Group: Applications/Databases

❧ Summary: PostgreSQL client programs

❧ Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

ppc64-utils-0.11-14.el5 - ppc64-utils-0.13-7.el5

❧ Group: System Environment/Base

❧ Summary: Linux/PPC64 specific utilities

❧ Description: A collection of utilities for Linux on PPC64 platforms.

❧ Added Dependencies:

  ▪ sqlite-devel

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

> ❧ No removed obsoletes

python-2.4.3-27.el5 - python-2.4.3-43.el5

> ❧ Group: Development/Languages

> ❧ Summary: An interpreted, interactive, object-oriented programming language.

> ❧ Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.

> ❧ Added Dependencies:

> > ❧ valgrind-devel

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

python-dmidecode-3.10.8-4.el5 - python-dmidecode-3.10.13-1.el5_5.1

> ❧ Group: System Environment/Libraries

> ❧ Summary: Python module to access DMI data

> ❧ Description: python-dmidecode is a python extension module that uses the code-base of the 'dmidecode' utility, and presents the data as python data structures or as XML data using libxml2.

> ❧ No added dependencies

> ❧ No removed dependencies

> ❧ No added provides

> ❧ No removed provides

> ❧ No added conflicts

> ❧ No removed conflicts

> ❧ No added obsoletes

> ❧ No removed obsoletes

python-urlgrabber-3.1.0-5.el5 - python-urlgrabber-3.1.0-6.el5

» Group: Development/Libraries

» Summary: A high-level cross-protocol url-grabber

» Description: A high-level cross-protocol url-grabber for python supporting HTTP, FTP and file locations. Features include keepalive, byte ranges, throttling, authentication, proxies and more.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

python-virtinst-0.400.3-9.el5 - python-virtinst-0.400.3-11.el5

» Group: Development/Libraries

» Summary: Python modules and utilities for installing virtual machines

» Description: virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

qffmpeg-0.4.9-0.15.20080908.el5 - qffmpeg-0.4.9-0.16.20080908.el5_5

» Group: Applications/Multimedia

» Summary: Stripped-down fork of ffmpeg for libspice

» Description: This is a stripped down version of upstream FFMPEG including only the codecs used by SPICE in order to avoid inadvertantly bundling or shipping any encumbered code or binaries.

» No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

qspice-0.3.0-54.el5 - qspice-0.3.0-54.el5_5.2

➤ Group: User Interface/Desktops

➤ Summary: An implementation of the Simple Protocol for Independent Computing Environments

➤ Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

quagga-0.98.6-5.el5 - quagga-0.98.6-5.el5_5.2

➤ Group: System Environment/Daemons

➤ Summary: Routing daemon

➤ Description: Quagga is a free software that manages TCP/IP based routing protocol. It takes multi-server and multi-thread approach to resolve the current complexity of the Internet. Quagga supports BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng. Quagga is intended to be used as a Route Server and a Route Reflector. It is not a toolkit, it provides full routing power under a new architecture. Quagga by design has a process for each protocol. Quagga is a fork of GNU Zebra.

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

quota-3.13-1.2.5.el5 - quota-3.13-4.el5

➢ Group: System Environment/Base

➢ Summary: System administration tools for monitoring users' disk usage.

➢ Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.

➢ Added Dependencies:

   ▫ openldap-devel

   ▫ openssl-devel

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

➢ No removed obsoletes

redhat-lsb-3.1-12.3.EL - redhat-lsb-4.0-2.1.4.el5

➢ Group: System Environment/Base

➢ Summary: LSB base libraries support for Red Hat Enterprise Linux

➢ Description: The Linux Standard Base (LSB) is an attempt to develop a set of standards that will increase compatibility among Linux distributions. The redhat-lsb package provides utilities needed for LSB Compliant Applications. It also contains requirements that will ensure that all components required by the LSB that are provided by Red Hat Linux are installed on the system.

➢ No added dependencies

➢ No removed dependencies

➢ No added provides

➢ No removed provides

➢ No added conflicts

➢ No removed conflicts

➢ No added obsoletes

❯ No removed obsoletes

redhat-release-5Server-5.5.0.2 - redhat-release-5Server-5.6.0.3

❯ Group: System Environment/Base

❯ Summary: Red Hat Enterprise Linux release file

❯ Description: Red Hat Enterprise Linux release files

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

redhat-release-notes-5Server-31 - redhat-release-notes-5Server-34

❯ Group: System Environment/Base

❯ Summary: Red Hat Enterprise Linux release notes files

❯ Description: Red Hat Enterprise Linux release notes files.

❯ No added dependencies

❯ No removed dependencies

❯ No added provides

❯ No removed provides

❯ No added conflicts

❯ No removed conflicts

❯ No added obsoletes

❯ No removed obsoletes

rgmanager-2.0.52-6.el5 - rgmanager-2.0.52-9.el5

❯ Group: System Environment/Base

❯ Summary: Open Source HA Resource Group Failover for Red Hat Enterprise Linux

❯ Description: Red Hat Resource Group Manager provides high availability of critical server applications in the event of planned or unplanned system downtime.

❯ No added dependencies

❯ No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rhn-client-tools-0.4.20-33.el5 - rhn-client-tools-0.4.20-46.el5

- Group: System Environment/Base

- Summary: Support programs and libraries for Red Hat Network

- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rhnlib-2.5.22-3.el5 - rhnlib-2.5.22-5.el5

- Group: Development/Libraries

- Summary: Python libraries for the RHN project

- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rng-utils-2.0-1.14.1.fc6 - rng-utils-2.0-4.el5

- Group: System Environment/Base

- Summary: Random number generator related utilities

- Description: Hardware random number generation tools.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rpm-4.4.2.3-18.el5 - rpm-4.4.2.3-22.el5

- Group: System Environment/Base

- Summary: The RPM package management system

- Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

rsyslog-3.22.1-3.el5 - rsyslog-3.22.1-3.el5_5.1

- Group: System Environment/Daemons

- Summary: Enhanced system logging and kernel message trapping daemon

- Description: Rsyslog is an enhanced multi-threaded syslogd supporting, among others, MySQL, syslog/tcp, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is quite compatible to stock sysklogd and can be used as a drop-in replacement. Its advanced features make it suitable for enterprise-class, encryption protected syslog relay chains while at the same time being very easy to setup for the novice user.

- No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

s390utils-1.8.1-8.el5 - s390utils-1.8.1-11.el5

❧ Group: System Environment/Base

❧ Summary: Linux/390 specific utilities

❧ Description: This package contains utilities related to Linux for S/390. The most important programs contained in this package are: - The cmstools suite to list, check, copy and cat files from a CMS volume. - chccwdev, a script to generically change attributes of a ccw device. - dasdfmt, which is used to low-level format eckd-dasds with either the classic linux disk layout or the new z/OS compatible disk layout. - dasdview, which displays DASD and VTOC information and dumps the content of a DASD to the console. - fdasd, which is used to create or modify partitions on eckd-dasds formatted with the z/OS compatible disk layout. - osasnmpd, a subagent for net-snmp to access the OSA hardware. - qetharp to query and purge address data in the OSA and HiperSockets hardware - qethconf to configure IBM QETH function IPA, VIPA and Proxy ARP. - src_vipa.sh to start applications using VIPA capabilities - tunedasd, a tool to adjust tunable parameters on DASD devices - vmconvert, a tool to convert vm dumps to lkcd compatible dumps. - vmcp, a tool to send CP commands from a Linux guest to the VM. - vmur, a tool to work with z/VM spool file queues (reader, punch, printer). - zipl, which is used to make either dasds or tapes bootable for system IPL or system dump. - zdump, which is used to retrieve system dumps from either tapes or dasds. - ziomon tools to collect data for zfcp performance analysis and report. - iucvterm, a z/VM IUCV terminal applications. - cpuplugd, a daemon that manages CPU and memory resources based on a set of rules. - dumpconf, the dump device used for system dump in case a kernel panic occurs. - mon_statd, pair of Linux - z/VM monitoring daemons. - ipl_tools, tool set to configure and list reipl and shutdown actions. - cpi, a service to set the system and sysplex names from the Linux guest to the HMC/SE using the Control Program Identification feature.

❧ No added dependencies

❧ No removed dependencies

❧ No added provides

❧ No removed provides

❧ No added conflicts

❧ No removed conflicts

❧ No added obsoletes

❧ No removed obsoletes

samba-3.0.33-3.28.el5 - samba-3.0.33-3.29.el5_5.1

❧ Group: System Environment/Daemons

≫ Summary: The Samba SMB server.

≫ Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

samba3x-3.3.8-0.51.el5 - samba3x-3.5.4-0.70.el5

≫ Group: System Environment/Daemons

≫ Summary: Server and Client software to interoperate with Windows machines

≫ Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

≫ Added Dependencies:

  ▪ libtalloc-devel >= 2.0.1

  ▪ libtdb-devel >= 1.2.1

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

sblim-1-40.el5 - sblim-1-47.el5

- Group: Applications/System

- Summary: Standards Based Linux Instrumentation for Manageability

- Description: SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

- No added dependencies

- Removed Dependencies:

  - sblim-cmpi-devel

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

screen-4.0.3-1.el5_4.1 - screen-4.0.3-3.el5

- Group: Applications/System

- Summary: A screen manager that supports multiple logins on one terminal

- Description: The screen utility allows you to have multiple logins on just one terminal. Screen is useful for users who telnet into a machine or are connected via a dumb terminal, but want to use more than just one login. Install the screen package if you need a screen manager that can support multiple logins on one terminal.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

scsi-target-utils-0.0-6.20091205snap.el5_4.1 - scsi-target-utils-1.0.8-0.el5

- Group: System Environment/Daemons

- Summary: The SCSI target daemon and utility programs

≫ Description: The SCSI target package contains the daemon and tools to setup a SCSI targets. Currently, software iSCSI targets are supported.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

selinux-policy-2.4.6-279.el5 - selinux-policy-2.4.6-300.el5

≫ Group: System Environment/Base

≫ Summary: SELinux policy configuration

≫ Description: SELinux Reference Policy - modular.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

sg3_utils-1.25-4.el5 - sg3_utils-1.25-5.el5

≫ Group: Utilities/System

≫ Summary: Utils for Linux's SCSI generic driver devices + raw devices

≫ Description: Collection of Linux utilities for devices that use the SCSI command set. Includes utilities to copy data based on "dd" syntax and semantics (called sg_dd, sgp_dd and sgm_dd); check INQUIRY data and VPD pages (sg_inq); check mode and log pages (sginfo, sg_modes and sg_logs); spin up and down disks (sg_start); do self tests (sg_senddiag); and various other functions. See the README, CHANGELOG and COVERAGE files. Requires the linux kernel 2.4 series or later. In the 2.4 series SCSI generic device names (e.g. /dev/sg0) must be used. In the 2.6 series other device names may be used as well (e.g. /dev/sda). Warning: Some of these tools access the internals of your system and the incorrect usage of them may render your system inoperable.

≫ No added dependencies

≫ No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

shadow-utils-4.0.17-15.el5 - shadow-utils-4.0.17-18.el5

» Group: System Environment/Base

» Summary: Utilities for managing accounts and shadow password files.

» Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.

» Added Dependencies:

  ▪ libacl-devel

  ▪ libattr-devel

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

sox-12.18.1-1 - sox-12.18.1-1.el5_5.1

» Group: Applications/Multimedia

» Summary: A general purpose sound file conversion tool.

» Description: SoX (Sound eXchange) is a sound file format converter SoX can convert between many different digitized sound formats and perform simple sound manipulation functions, including sound effects.

» No added dependencies

» No removed dependencies

» No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

strace-4.5.18-5.el5_4.1 - strace-4.5.18-5.el5_5.5

- Group: Development/Debuggers

- Summary: Tracks and displays system calls associated with a running process

- Description: The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

subversion-1.4.2-4.el5_3.1 - subversion-1.6.11-7.el5

- Group: Development/Tools

- Summary: Modern Version Control System designed to replace CVS

- Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.

- Added Dependencies:

  - cyrus-sasl-devel

  - java-devel-gcj

  - unzip

  - zip

- Removed Dependencies:

  - java-1.4.2-devel

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

sudo-1.7.2p1-5.el5 - sudo-1.7.2p1-10.el5

» Group: Applications/System

» Summary: Allows restricted root access for specified users.

» Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

sysstat-7.0.2-3.el5 - sysstat-7.0.2-3.el5_5.1

» Group: Applications/System

» Summary: The sar and iostat system monitoring commands.

» Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

- No added obsoletes

- No removed obsoletes

system-config-cluster-1.0.57-3 - system-config-cluster-1.0.57-7

- Group: Applications/System

- Summary: system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.

- Description: system-config-cluster is a utility which allows you to manage cluster configuuration in a graphical setting.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

system-config-lvm-1.1.5-4.el5 - system-config-lvm-1.1.5-8.el5

- Group: Applications/System

- Summary: A utility for graphically configuring Logical Volumes

- Description: system-config-lvm is a utility for graphically configuring Logical Volumes

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

system-config-securitylevel-1.6.29.1-5.el5 - system-config-securitylevel-1.6.29.1-6.el5

- Group: System Environment/Base

- Summary: A graphical interface for modifying the system security level

- Description: system-config-securitylevel is a graphical user interface for setting basic firewall rules.

* No added dependencies

* No removed dependencies

* No added provides

* No removed provides

* No added conflicts

* No removed conflicts

* No added obsoletes

* No removed obsoletes

systemtap-1.1-3.el5 - systemtap-1.3-4.el5

* Group: Development/System

* Summary: Instrumentation System

* Description: SystemTap is an instrumentation system for systems running Linux 2.6. Developers can write instrumentation to collect data on the operation of the system.

* Added Dependencies:

  * avahi-devel

  * glibc-headers

  * rpm-devel

* No removed dependencies

* No added provides

* No removed provides

* No added conflicts

* No removed conflicts

* No added obsoletes

* No removed obsoletes

tcsh-6.14-17.el5 - tcsh-6.14-17.el5_5.2

* Group: System Environment/Shells

* Summary: An enhanced version of csh, the C shell.

* Description: Tcsh is an enhanced but completely compatible version of csh, the C shell. Tcsh is a command language interpreter which can be used both as an interactive login shell and as a shell script command processor. Tcsh includes a command line editor, programmable word completion, spelling correction, a history mechanism, job control and a C language like syntax.

* No added dependencies

* No removed dependencies

* No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

tetex-3.0-33.8.el5 - tetex-3.0-33.8.el5_5.6

> Group: Applications/Publishing

> Summary: The TeX text formatting system.

> Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

> No added conflicts

> No removed conflicts

> No added obsoletes

> No removed obsoletes

tmpwatch-2.9.7-1.1.el5.2 - tmpwatch-2.9.7-1.1.el5.5

> Group: System Environment/Base

> Summary: A utility for removing files based on when they were last accessed.

> Description: The tmpwatch utility recursively searches through specified directories and removes files which have not been accessed in a specified period of time. Tmpwatch is normally used to clean up directories which are used for temporarily holding files (for example, /tmp). Tmpwatch ignores symlinks, won't switch filesystems and only removes empty directories and regular files.

> No added dependencies

> No removed dependencies

> No added provides

> No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

tog-pegasus-2.9.1-2.el5 - tog-pegasus-2.9.1-2.el5_5.1

- Group: Systems Management/Base

- Summary: OpenPegasus WBEM Services for Linux

- Description: OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

tomcat5-5.5.23-0jpp.7.el5_3.2 - tomcat5-5.5.23-0jpp.16.el5

- Group: Networking/Daemons

- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API

- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

» No removed obsoletes

totem-2.16.7-6.el5 - totem-2.16.7-7.el5

» Group: Applications/Multimedia

» Summary: Movie player for GNOME 2

» Description: Totem is simple movie player for the Gnome desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as a pretty complete keyboard navigation.

» Added Dependencies:

▪ gecko-devel-unstable >= 1.9.2

» Removed Dependencies:

▪ gecko-devel-unstable >= 1.9

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

tzdata-2010e-1.el5 - tzdata-2010l-1.el5

» Group: System Environment/Base

» Summary: Timezone data

» Description: This package contains data files with rules for various time zones around the world.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

udev-095-14.21.el5 - udev-095-14.24.el5

» Group: System Environment/Base

» Summary: A userspace implementation of devfs

- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

util-linux-2.13-0.52.el5_4.1 - util-linux-2.13-0.56.el5

- Group: System Environment/Base

- Summary: A collection of basic system utilities.

- Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.

- Added Dependencies:

  - libutempter-devel

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

vim-7.0.109-6.el5 - vim-7.0.109-7.el5

- Group: Applications/Editors

- Summary: The VIM editor.

- Description: VIM (VIsual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.

- No added dependencies

- Removed Dependencies:

  - rpmlib(VersionedDependencies) <= 3.0.3-1

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

virt-manager-0.6.1-12.el5 - virt-manager-0.6.1-13.el5

- Group: Applications/Emulators

- Summary: Virtual Machine Manager

- Description: Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

vnc-4.1.2-14.el5_3.1 - vnc-4.1.2-14.el5_5.4

- Group: User Interface/Desktops

- Summary: A remote display system.

- Description: Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package contains a client which will allow you to connect to other desktops running a VNC server.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

vsftpd-2.0.5-16.el5_4.1 - vsftpd-2.0.5-16.el5_5.1

≫ Group: System Environment/Daemons

≫ Summary: vsftpd - Very Secure Ftp Daemon

≫ Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

w3m-0.5.1-15.el5 - w3m-0.5.1-17.el5_5

≫ Group: Applications/Internet

≫ Summary: A pager with Web browsing abilities.

≫ Description: The w3m program is a pager (or text file viewer) that can also be used as a text-mode Web browser. W3m features include the following: when reading an HTML document, you can follow links and view images using an external image viewer; its internet message mode determines the type of document from the header; if the Content-Type field of the document is text/html, the document is displayed as an HTML document; you can change a URL description like 'http://hogege.net' in plain text into a link to that URL. If you want to display the inline images on w3m, you need to install w3m-img package as well.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

wacomexpresskeys-0.4.1-1.el5 - wacomexpresskeys-0.4.1-2.el5

≫ Group: System Environment/Base

≫ Summary: Wacom ExpressKeys and Touch Strips configuration utility

≫ Description: Configuration utility to bind Wacom tablet's ExpressKeys and Touch Strips to generate other input events.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

wdaemon-0.14-5 - wdaemon-0.14-7

≫ Group: User Interface/X Hardware Support

≫ Summary: Hotplug helper for Wacom X.org driver

≫ Description: Helper application which emulates persistent input devices for Wacom tablets so they can be plugged and unplugged while X.org server is running. This should go away as soon X.org properly supports hotplugging.

≫ No added dependencies

≫ No removed dependencies

≫ No added provides

≫ No removed provides

≫ No added conflicts

≫ No removed conflicts

≫ No added obsoletes

≫ No removed obsoletes

wireshark-1.0.8-1.el5_3.1 - wireshark-1.0.15-1.el5_5.1

≫ Group: Applications/Internet

≫ Summary: Network traffic analyzer

≫ Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ package.

≫ No added dependencies

≫ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

xen-3.0.3-105.el5 - xen-3.0.3-120.el5

‣ Group: Development/Libraries

‣ Summary: Xen is a virtual machine monitor

‣ Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

xorg-x11-drv-ati-6.6.3-3.27.el5 - xorg-x11-drv-ati-6.6.3-3.32.el5

‣ Group: User Interface/X Hardware Support

‣ Summary: Xorg X11 ati video driver

‣ Description: X.Org X11 ati video driver.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

xorg-x11-drv-mga-1.4.10-7.el5 - xorg-x11-drv-mga-1.4.13-1.el5

‣ Group: User Interface/X Hardware Support

‣ Summary: Xorg X11 mga video driver

‣ Description: X.Org X11 mga video driver.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

xorg-x11-drv-nv-2.1.15-3.el5 - xorg-x11-drv-nv-2.1.15-4.el5

‣ Group: User Interface/X Hardware Support

‣ Summary: Xorg X11 nv video driver

‣ Description: X.Org X11 nv video driver.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

‣ No removed provides

‣ No added conflicts

‣ No removed conflicts

‣ No added obsoletes

‣ No removed obsoletes

xorg-x11-drv-sis-0.9.1-7.1.el5 - xorg-x11-drv-sis-0.9.1-7.3.el5

‣ Group: User Interface/X Hardware Support

‣ Summary: Xorg X11 sis video driver

‣ Description: X.Org X11 sis video driver.

‣ No added dependencies

‣ No removed dependencies

‣ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

xorg-x11-server-1.1.1-48.76.el5 - xorg-x11-server-1.1.1-48.76.el5_5.2

➤ Group: User Interface/X

➤ Summary: X.Org X11 X server

➤ Description: X.Org X11 X server

➤ No added dependencies

➤ No removed dependencies

➤ No added provides

➤ No removed provides

➤ No added conflicts

➤ No removed conflicts

➤ No added obsoletes

➤ No removed obsoletes

xulrunner-1.9.0.18-1.el5_4 - xulrunner-1.9.2.13-3.el5

➤ Group: Applications/Internet

➤ Summary: XUL Runtime for Gecko Applications

➤ Description: XULRunner provides the XUL Runtime environment for Gecko applications.

➤ Added Dependencies:

- alsa-lib-devel

- autoconf213

- bzip2-devel

- libnotify-devel

- nspr-devel >= 4.8

- nss-devel >= 3.12.8

- startup-notification-devel

➤ Removed Dependencies:

- cairo-devel >= 0.5

- curl-devel

- desktop-file-utils

- libpng-devel

- nspr-devel >= 4.7.6

- nss-devel >= 3.11.99.5

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

yaboot-1.3.13-10.el5 - yaboot-1.3.13-10.el5_5.1

» Group: System Environment/Base

» Summary: Linux bootloader for Power Macintosh "New World" computers.

» Description: yaboot is a bootloader for PowerPC machines which works on New World ROM machines (Rev. A iMac and newer) and runs directly from Open Firmware, eliminating the need for Mac OS. yaboot can also bootload IBM pSeries machines.

» No added dependencies

» No removed dependencies

» No added provides

» No removed provides

» No added conflicts

» No removed conflicts

» No added obsoletes

» No removed obsoletes

yelp-2.16.0-22.el5 - yelp-2.16.0-26.el5

» Group: Applications/System

» Summary: A system documentation reader from the Gnome project

» Description: Yelp is the Gnome 2 help/documentation browser. It is designed to help you browse all the documentation on your system in one central tool.

» Added Dependencies:

- gecko-devel-unstable >= 1.9.2

» Removed Dependencies:

- gecko-devel-unstable >= 1.9

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

yum-3.2.22-26.el5 - yum-3.2.22-33.el5

- Group: System Environment/Base

- Summary: RPM installer/updater

- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

yum-rhn-plugin-0.5.4-15.el5 - yum-rhn-plugin-0.5.4-17.el5

- Group: System Environment/Base

- Summary: RHN support for yum

- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.

- No added dependencies

- No removed dependencies

- No added provides

- No removed provides

- No added conflicts

- No removed conflicts

- No added obsoletes

- No removed obsoletes

yum-utils-1.1.16-13.el5 - yum-utils-1.1.16-13.el5_4.1

 ❯ Group: Development/Tools

 ❯ Summary: Utilities based around the yum package manager

 ❯ Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-manager.

 ❯ No added dependencies

 ❯ No removed dependencies

 ❯ No added provides

 ❯ No removed provides

 ❯ No added conflicts

 ❯ No removed conflicts

 ❯ No added obsoletes

 ❯ No removed obsoletes

zsh-4.2.6-3.el5 - zsh-4.2.6-5.el5

 ❯ Group: System Environment/Shells

 ❯ Summary: A powerful interactive shell

 ❯ Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

 ❯ No added dependencies

 ❯ No removed dependencies

 ❯ No added provides

 ❯ No removed provides

 ❯ No added conflicts

 ❯ No removed conflicts

 ❯ No added obsoletes

 ❯ No removed obsoletes

Appendix B. Revision History

Revision 1-1.402	Fri Oct 25 2013	Rüdiger Landmann

Rebuild with Publican 4.0.0

Revision 1-1	Mon Jun 4 2012	Martin Prpič

Fixed Stateless Linux description and removed outdated reference to Fedora page.

Revision 0-0	Tue Nov 30 2010	Ryan Lerch

inital release of the Technical Notes