Red Hat Enterprise Linux 7

7.3 Release Notes

Release Notes for Red Hat Enterprise Linux 7.3

Last Updated: 2018-04-17

Red Hat Enterprise Linux 7 7.3 Release Notes

Release Notes for Red Hat Enterprise Linux 7.3

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

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 7.3 and document known problems in this release, as well as notable bug fixes, Technology Previews, deprecated functionality, and other details.

Table of Contents

PREFACE

Red Hat Enterprise Linux minor releases are an aggregation of individual security, enhancement, and bug fix errata. The *Red Hat Enterprise Linux 7.3 Release Notes* document describes the major changes made to the Red Hat Enterprise Linux 7 operating system and its accompanying applications for this minor release, as well as known problems and a complete list of all currently available Technology Previews.

Capabilities and limits of Red Hat Enterprise Linux 7 as compared to other versions of the system are available in the Red Hat Knowledgebase article available at https://access.redhat.com/articles/rhel-limits.

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

CHAPTER 1. OVERVIEW

Security

- The SELinux userspace has been rebased and provides various enhancements and performance improvements. Notably, the new SELinux module store supports priorities, and the SELinux Common Intermediate Language (CIL) has been introduced.
- OpenSCAP workbench now provides a new SCAP Security Guide integration dialog and enables modification of SCAP policies using a graphical tool.
- The OpenSCAP suite now includes support for scanning containers using the **`atomic scan`** command.
- Upgraded **`firewalld`** starts and restarts significantly faster due to a new transaction model. It also provides improved management of connections, interfaces, and sources, a new default logging option, and **`ipset`** support.
- The **`audit`** daemon introduces a new flush technique, which significantly improves performance. Audit policy, configuration, and logging have been enhanced and now support a number of new options.
- Media Access Control Security (MACsec) encryption over Ethernet is now supported.

See Chapter 15, *Security* for more information on security enhancements.

Identity Management

The highlighted new features and improvements related to Identity Management (IdM) include:

- Improved performance of both IdM servers and clients in large customer environments
- Enhanced topology management and replica installation
- Extended smart card support for Active Directory (AD) users
- Fine-grained configuration of one-time password (OTP) authentication
- Improved troubleshooting capabilities of IdM clients.

Red Hat Enterprise Linux 7.2 introduced the Ipsilon identity provider service for federated single sign-on (SSO). Subsequently, Red Hat has released Red Hat Single Sign-On as a web SSO solution based on the Keycloak community project. Red Hat Single Sign-On provides greater capabilities than Ipsilon and is designated as the standard web SSO solution across the Red Hat product portfolio.

For details on Red Hat Single Sign-On, see:

- Red Hat Single Sign-On product page
- Red Hat Single Sign-On Release Notes

Note that Red Hat does not plan to upgrade Ipsilon from Technology Preview to a fully supported feature. The ipsilon packages will be removed from Red Hat Enterprise Linux in a future minor release.

Entitlements to Red Hat Single Sign-On are currently available using Red Hat JBoss Middleware or OpenShift Container Platform subscriptions.

For detailed information on changes in IdM, refer to Chapter 5, *Authentication and Interoperability*.

Core Kernel

- Support for Checkpoint/Restore in User space (CRIU) has been expanded to the the little-endian variant of IBM Power Systems architecture.
- Heterogeneous memory management (HMM) feature has been introduced as a Technology Preview.

For more kernel features, refer to Chapter 12, *Kernel*. For information about Technology Previews related to kernel, see Chapter 42, *Kernel*.

Networking

- Open vSwitch now uses kernel lightweight tunnel support.
- Bulking in the memory allocator subsystem is now supported.
- **NetworkManager** now supports new device types, improved stacking of virtual devices, LLDP, stable privacy IPv6 addresses (RFC 7217), detects duplicate IPv4 addresses, and controls a host name through **`systemd-hostnamed`**. Additionally, the user can set a DHCP timeout property and DNS priorities.

For more networking features, see Chapter 14, *Networking*.

Platform Hardware Enablement

- Support for the Coherent Accelerator Processor Interface (CAPI) flash block adapter has been added. For detailed information, see Chapter 10, *Hardware Enablement*.

Real-Time Kernel

- A new scheduler policy, **`SCHED_DEADLINE`** has been introduced as Technology Preview. This new policy is available in the upstream kernel and shows promise for certain Realtime use cases. For details, see Chapter 43, *Real-Time Kernel*.

Storage and File Systems

- Support for Non-Volatile Dual In-line Memory Module (NVDIMM) persistent memory architecture has been added, which includes the addition of the **`libnvdimm`** kernel subsystem. NVDIMM memory can be accessed either as a block storage device, which is fully supported in Red Hat Enterprise Linux 7.3, or in Direct Access (DAX) mode, which is provided by the ext4 and XFS file systems as a Technology Preview in Red Hat Enterprise Linux 7.3. For more information, see Chapter 17, *Storage* and Chapter 12, *Kernel* in the New Features part, and Chapter 39, *File Systems* in the Technology Previews part.
- A new Ceph File System (CephFS) kernel module, introduced as a Technology Preview, enables Red Hat Enterprise Linux Linux nodes to mount Ceph File Systems from Red Hat Ceph Storage clusters. For more information, see Chapter 39, *File Systems*.
- Support for pNFS SCSI file sharing has been introduced as a Technology Preview. For details, refer to Chapter 39, *File Systems*.
- LVM2 support for RAID-level takeover, the ability to switch between RAID types, is now available as a Technology Preview. See Chapter 45, *Storage* for more information.

Clustering

For Red Hat Enterprise Linux 7.3, the Red Hat High Availability Add-On supports the following major enhancements:

- The ability to better configure and trigger notifications when the status of a managed cluster changes with the introduction of enhanced pacemaker alerts.
- The ability to configure **Pacemaker** to manage multi-site clusters across geo-locations for disaster recovery and scalability through the use of the Booth ticket manager. This feature is provided as a Technology Preview.
- The ability to configure **Pacemaker** to manage stretch clusters using a separate quorum device (QDevice), which acts as a third-party arbitration device for the cluster. This functionality is provided as a Technology Preview, and its primary use is to allow a cluster to sustain more node failures than standard quorum rules allow.

For more information on enhancements to the Red Hat High Availability Add-On, see Chapter 6, *Clustering* in the New Features Part and Chapter 38, *Clustering* in the Technology Previews part.

Desktop

- A new instant messaging client, **pidgin**, has been introduced, which supports off-the-record (OTR) messaging and the Microsoft Lync instant messaging application.

For more information regarding changes in desktop, refer to Chapter 8, *Desktop*.

Internet of Things

- Red Hat Enterprise Linux 7.3 provides latest Bluetooth support, including support for connecting to Bluetooth Low Energy (LE) devices; see Chapter 14, *Networking*.
- Controller Area Network (CAN) device drivers are now supported, see Chapter 12, *Kernel* for more information.
- Red Hat Enterprise Linux 7 kernel is now able to use the embedded MMC (eMMC) interface version 5.0. For details, refer to Chapter 10, *Hardware Enablement*.

Linux Containers

- The System Security Services Daemon (SSSD) container is now available for Red Hat Enterprise Linux Atomic Host as Technology Preview. See Chapter 37, *Authentication and Interoperability* for details.

See also the Red Hat Enterprise Linux Atomic Host and Containers Release Notes.

Red Hat Insights

Since Red Hat Enterprise Linux 7.2, the *Red Hat Insights* service is available. Red Hat Insights is a proactive service designed to enable you to identify, examine, and resolve known technical issues before they affect your deployment. Insights leverages the combined knowledge of Red Hat Support Engineers, documented solutions, and resolved issues to deliver relevant, actionable information to system administrators.

The service is hosted and delivered through the customer portal at https://access.redhat.com/insights/ or through Red Hat Satellite. To register your systems, follow the Getting Started Guide for Insights. For further information, data security, and limits, refer to https://access.redhat.com/insights/splash/.

Red Hat Customer Portal Labs

Red Hat Customer Portal Labs is a set of tools in a section of the Customer Portal available at https://access.redhat.com/labs/. The applications in Red Hat Customer Portal Labs can help you improve performance, quickly troubleshoot issues, identify security problems, and quickly deploy and configure complex applications. Some of the most popular applications are:

- Kickstart Configurator
- Registration Assistant
- NFS Helper
- Linter for Dockerfile
- Multipath Helper
- iSCSI Helper
- Code Browser

CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 7.3 is available as a single kit on the following architectures: [1]

- 64-bit AMD
- 64-bit Intel
- IBM POWER7+ and POWER8 (big endian) [2]
- IBM POWER8 (little endian) [3]
- IBM z Systems [4]

---

[1] Note that the Red Hat Enterprise Linux 7.3 installation is supported only on 64-bit hardware. Red Hat Enterprise Linux 7.3 is able to run 32-bit operating systems, including previous versions of Red Hat Enterprise Linux, as virtual machines.

[2] Red Hat Enterprise Linux 7.3 (big endian) is currently supported as a KVM guest on Red Hat Enterprise Virtualization for Power, and on PowerVM.

[3] Red Hat Enterprise Linux 7.3 (little endian) is currently supported as a KVM guest on Red Hat Enterprise Virtualization for Power, on PowerVM and PowerNV (bare metal).

[4] Note that Red Hat Enterprise Linux 7.3 supports IBM zEnterprise 196 hardware or later; IBM z10 Systems mainframe systems are no longer supported and will not boot Red Hat Enterprise Linux 7.3.

CHAPTER 3. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel shipped with Red Hat Enterprise Linux 7.3. These changes include added or updated **proc** entries, **sysctl**, and **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

apic_extnmi=[APIC,X86]

Provides external Nonmaskable Interrupt (NMI) delivery setting.

Format: { bsp (default) | all | none }.

bsp: External NMI is delivered only to CPU 0.

all: External NMIs are broadcast to all CPUs as a backup of CPU 0.

none: External NMI is masked for all CPUs. This is useful so that a dump capture kernel will not be shot down by NMI.

bau=[X86_UV] Enable the BAU on SGI UV

The default behavior is to disable the BAU (i.e. bau=0).

Format: { "0" | "1" }

0 - Disable the BAU.

1 - Enable the BAU.

unset - Disable the BAU.

cpu_init_udelay=N [X86]

Sets delay of N microseconds between assert and de-assert of **APIC INIT** to start processors. This delay occurs on every CPU online, such as boot, and resume from suspend.

Default value: 10000

hardlockup_all_cpu_backtrace=[KNL]

The hard-lockup detector generates backtraces on all cpus.

Format: integer

intel_iommu=[DMAR] Intel iommu driver (DMAR) option [...]

ecs_off [Default Off]

By default, extended context tables are supported if the hardware advertises that it has support both for the extended tables themselves, and also **PASID** support. With this option set, extended tables will not be used even on hardware which claims to support them.

kernelcore=nn[KMG] [KNL,X86,IA-64,PPC]

This parameter

kernelcore=[KNL,X86,IA-64,PPC]

Format: **nn[KMGTPE]** | "mirror"

Instead of specifying the amount of memory **nn[KMGTPE]**, users can specify "mirror" option. In case "mirror" option is specified, mirrored memory is used for non-movable allocations and remaining memory is used for movable pages. Both **nn[KMGTPE]** and "mirror" option are exclusive. Users are not allowed to specify **nn[KMGTPE]** and "mirror" option at the same time.

libata.force=[LIBATA]

* [no]ncqtrim: Turn off queued **DSM TRIM**.

memmap=nn[KMG]!ss[KMG] [KNL,X86]

Marks specific memory as protected. Region of memory to be used, from ss to ss+nn. The memory region should be marked as e820 type 12 (0xc) and is NVDIMM or ADR memory.

module_blacklist=[KNL]

Does not load a comma-separated list of modules. This feature is useful for debugging problem modules.

nfs4.layoutstats_timer=[NFSv4.2]

Changes the rate at which the kernel sends the layout statistics to the pNFS metadata server.

Setting this value to zero causes the kernel to use whatever value is the default set by the layout driver. Any non-zero value sets the minimum interval in seconds between the transmissions of layout statistics.

nmi_watchdog=[KNL,BUGS=X86]

Debugging features for SMP kernels.

Format: [panic,][nopanic,][num]

Valid num: 0 or 1

0 - turn nmi_watchdog off

1 - turn nmi_watchdog on

nohugeiomap [KNL,x86]

Disables kernel huge I/O mappings.

soft_watchdog

This parameter can be used to control the soft lockup detector.

0 - disable the soft lockup detector

1 - enable the soft lockup detector

The soft lockup detector monitors CPUs for threads that are hogging the CPUs without rescheduling voluntarily, thus preventing the **watchdog/N** threads from running. The mechanism depends on the CPUs ability to respond to timer interrupts which are needed for the **watchdog/N** threads to be

woken up by the watchdog timer function, otherwise the NMI watchdog - if enabled - can detect a hard lockup condition.

watchdog

This parameter disables or enables the soft lockup detector and the hard lockup detector ensured by NMI watchdog at the same time.

0 - disables both lockup detectors

1 - enables both lockup detectors

The soft lockup detector and the NMI watchdog can also be disabled or enabled individually, using the soft_watchdog and nmi_watchdog parameters. If the watchdog parameter is read, for example by executing the cat /proc/sys/kernel/watchdog command, the output value of this command, which is 0 or 1, shows the logical OR of soft_watchdog and nmi_watchdog.

noxsaveopt [X86]

Disables xsaveopt used in saving x86 extended register states. The kernel falls back to use xsave to save the states. By using this parameter, performance of saving the states is lowered because xsave does not support modified optimization, while xsaveopt supports it on xsaveopt enabled systems.

noxsaves [X86]

Disables xsaves and xrstors used in saving and restoring x86 extended register state in compacted form of xsave area. The kernel falls back to use xsaveopt and xrstor to save and restore the states in standard form of xsave area. By using this parameter, xsave area per process can occupy more memory on xsaves enabled systems.

nompx [X86]

Disables Intel Memory Protection Extensions.

See Documentation/x86/intel_mpx.txt for more information about the feature.

nowatchdog [KNL]

Disables both lockup detectors: soft-lockup and NMI watchdog (hard-lockup).

watchdog_cpumask

This value is used to set which CPUs are available for watchdog to run. The default cpumask is all possible cores, but if **`NO_HZ_FULL`** is enabled in the kernel config, and cores are specified with the nohz_full=boot argument, those cores are excluded by default. Offline cores can be included in this mask. If the core is later brought online, watchdog is started based on the mask value. This value can only be touched in the nohz_full case to re-enable cores that by default were not running watchdog, if a kernel lockup was suspected on those cores. The argument value is the standard cpulist format for cpumasks.

Example:

To enable the watchdog on cores 0, 2, 3, and 4 use this command:

echo 0,2-4 **`/proc/sys/kernel/watchdog_cpumask`**

watchdog_thresh

This value is used to set the frequency of hrtimer and NMI events and the soft and hard lockup thresholds. The default threshold is 10 seconds. The softlockup threshold is 2 * watchdog_thresh. Setting of this parameter to zero will disable lockup detection altogether.

schedstats=[KNL,X86]

Enables or disables scheduler statistics.

Allowed values are enable and disable.

This feature incurs a small amount of overhead in the scheduler, but it is useful for debugging and performance tuning.

usbcore.usbfs_snoop_max=[USB]

Sets maximum number of bytes to snoop in each USB Request Block (URB). The default value is 65536.

usb-storage.quirks=[...]

j = NO_REPORT_LUNS

Does not use report luns command, UAS only.

workqueue.watchdog_thres

If **`CONFIG_WQ_WATCHDOG`** is configured, workqueue can warn stall conditions and dump internal state to help debugging. Value 0 disables workqueue stall detection. Otherwise, it is the stall threshold duration in seconds.The default value is 30 and it can be updated at runtime by writing to the corresponding sysfs file.

workqueue.power_efficient

Per-cpu work queues are generally preferred because they have better performance due to cache locality, but they consume more power than unbound work queues. This kernel parameter makes the per-cpu work queues which were observed to contribute significantly to power consumption unbound, leading to significantly lower power usage at the cost of small performance overhead.

perf_event_paranoid

Controls use of the performance events system by unprivileged users who do not have CAP_SYS_ADMIN.

The default value is 1.

-1 - Allows use of all events by all users.

>=0 - Disallows raw tracepoint access by users without CAP_IOC_LOCK.

>=1 - Disallow CPU event access by users without CAP_SYS_ADMIN.

>=2 - Disallow kernel profiling by users without CAP_SYS_ADMIN

`/proc/sys/fs`

pipe-user-pages-hard:

Sets maximum total number of pages that a non-privileged user can allocate for pipes.

Once this limit is reached, no new pipes can be allocated until usage returns below the limit again. When set to 0, no limit is applied, which is the default setting.

pipe-user-pages-soft:

Sets maximum total number of pages that a non-privileged user can allocate for pipes before the pipe size gets limited to a single page. Once this limit is reached, new pipes are limited to a single page in size for this user in order to limit total memory usage. Trying to increase the total number of pages using the fcntl() function is denied until usage drops below the limit again. The default value allows to allocate up to 1024 pipes at their default size. When set to 0, no limit is applied.

`/proc/sys/kernel`

hardlockup_all_cpu_backtrace:

This value controls the hard lockup detector behavior regarding gathering further debug information. If enabled, arch-specific all-CPU stack dumping is initiated.

0 - do nothing. This is the default behavior.

1 - on detection capture more debug information.

PART I. NEW FEATURES

This part documents new features in Red Hat Enterprise Linux 7.3.

CHAPTER 4. GENERAL UPDATES

New variable for disabling colored output for `systemd`

This update introduces the **`SYSTEMD_COLORS`** environment variable for **`systemd`**, which enables turning on or off **`systemd`** color output. **`SYSTEMD_COLORS`** should be set to a valid boolean value. (BZ#1265749)

`systemd` units can now be enabled using aliases

The **`systemd`** init system uses aliases. Aliases are symbolic links to the service files, and can be used in commands instead of the actual names of services. For example, the package providing the **`/usr/lib/systemd/system/nfs-server.service`** service file also provides an alias **`/usr/lib/systemd/system/nfs.service`**, which is a symbolic link to the **`nfs-server.service`**. This enables, for example, using the **`systemctl status nfs.service`** command instead of **`systemctl status nfs-server.service`**.

Previously, running the **`systemctl enable`** command using an alias instead of the real service name failed with an error. With this update, the bug is fixed, and **`systemctl enable`** successfully enables units referred to by their aliases. (BZ#1142378)

New `systemd` option: `RandomizedDelaySec`

This update introduces the **`RandomizedDelaySec`** option for **`systemd`** timers, which schedules an event to occur later by a random number of seconds. For example, setting the option to 10 will postpone the event by a random number of seconds between 0 and 10. The new option is useful for spreading workload over a longer time period to avoid several events executing at the same time. (BZ#1305279)

CHAPTER 5. AUTHENTICATION AND INTEROPERABILITY

Server performance has improved in many areas

Some operations in Identity Management run much faster now. For example, this enhancement enables better scalability in large deployments exceeding 50,000 users and hosts. Most notably, the improvements include:

- Faster adding of users and hosts
- Faster Kerberos authentication for all commands
- Faster execution of the **`ipa user-find`** and **`ipa host-find`** commands

For information on how to reduce the time required for provisioning of a large number of entries, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#performance-tuning

Note that to make the find operations faster, the **`ipa *-find`** commands no longer show membership by default. To display the membership, add the **`--all`** option to **`ipa *-find`** or, alternatively, use the **`ipa *-show`** commands. (BZ#1298288, BZ#1271321, BZ#1268449, BZ#1346321)

Enhanced IdM topology management

Information about the Identity Management (IdM) topology is now maintained at a central location in the shared tree. As a result, you can now manage the topology from any IdM server using the command line or the web UI.

Additionally, some topology management operations have been simplified, notably:

- Topology commands have been integrated into the IdM command-line interface, so that you can perform all replica operations using the native IdM command-line tools.
- You can manage replication agreements in the web UI or from the command line using a new and simplified workflow.
- The web UI includes a graph of the IdM topology, which helps visualize the current state of replica relationships.
- IdM includes safety measures that prevent you from accidentally deleting the last certificate authority (CA) master from the topology or isolating a server from the other servers.
- Support for server roles as a simpler way of determining which server in the topology hosts which services as well as installing these services onto a server.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#managing-topology

Note that the new functionality requires raising the domain level to **`1`**. See https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#domain-level (BZ#1298848, BZ#1199516)

Simplified replica installation

Installing a replica no longer requires you to log in to the initial server, use the Directory Manager (DM) credentials, and copy the replica information file from the initial server to the replica. For example, this allows for easier provisioning using an external infrastructure management system, while retaining a reasonable level of security.

In addition, the **ipa-replica-install** utility can now also promote an existing client to a replica.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#install-replica

Note that the new functionality requires raising the domain level to **1**. See https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#domain-level (BZ#837369)

IdM now supports smart card authentication for AD users

This update extends smart card support in Identity Management (IdM). Users from a trusted Active Directory (AD) can now authenticate using a smart card both remotely using **ssh** as well as locally. The following methods are supported for local authentication:

- Text console
- Graphical console, such as the Gnome Display Manager (GDM)
- Local authentication services, like **su** or **sudo**

Note that IdM only supports the above-mentioned local authentication services and **ssh** for smart card authentication. Other services, such as FTP, are not supported.

The smart card certificate for AD users can be stored directly in AD, or in an IdM override object for the AD user.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Windows_Integration_Guide/index.html#smart-cards (BZ#1298966, BZ#1290378)

IdM now supports TGS authorization decisions

In an Identity Management (IdM) environment, users can optionally log in using multi-factor authentication. The Kerberos ticket from the ticket granting server (TGS) now contains an indicator if two-factor authentication using a standard password in combination with a one-time password (OTP) was used. This enables the administrator to set server-side policies for resources, and the users are allowed to access based upon the type of their logins. For example, the administrator can now allow the user to log in to the desktop either using one- or two-factor authentication, but require two-factor authentication for virtual private networks (VPN) logins.

By default, all services accept all tickets. To activate this granularity, you have to manage the policies in the IdM web user interface or use the **ipa service-*** and **ipa host-*** commands. (BZ#1224057, BZ#1340304, BZ#1292153)

sssd now provides optional two-factor authentication

The System Security Services Daemon (SSSD) now allows users with two-factor authentication enabled to authenticate to services either by using a standard password and a one-time password (OTP), or using only a standard password. Optional two-factor authentication enables administrators to configure local logins using a single factor, while other services, like access to VPN gateways, can request both factors. As a result, during the login, the user can enter either both factors, or optionally only the password. The Kerberos ticket then uses authentication indicators to list the used factors. (BZ#1325809)

New SSSD control and status utility

The **sssctl** utility provides a simple and unified way to obtain information about the System Security Services Daemon's (SSSD) status. For example, you can query status information about active server, auto-discovered servers, domains, and cached objects. Additionally, the **sssctl** utility enables you to manage SSSD data files to troubleshoot SSSD in a safe way while the service is running.

The options supported by **sssctl** include **client-data-backup** and **cache-remove** to back up and remove the SSSD cache. Previously, when it was necessary to start SSSD without any cached data, the administrator had to remove the cache files manually.

For more information about the features the utility provides, run **sssctl --help**.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/System-Level_Authentication_Guide/index.html#sssctl (BZ#879333)

SSSD configuration file validation

Previously, the System Security Services Daemon (SSSD) did not provide a tool to manually check the **/etc/sssd/sssd.conf** file. As a consequence, the administrator had to find the problem in the configuration file if the service failed to start. This update provides the **config-check** option of the **sssctl** command to locate problems in the configuration file. Additionally, SSSD automatically checks the validity of the configuration file after the service starts, and shows level 0 debug messages for incorrect settings. (BZ#988207, BZ#1072458)

The pki cert-find command now supports revocation strings

The **pki cert-find** command has been enhanced and now supports revocation reasons in string format. As a result, you can pass strings, such as **Key_compromise**, to the **--revocationReason** option, instead of the corresponding numeric values. For the list of supported revocation strings, see

```
# pki cert-find --help
```

(BZ#1224365)

IdM now supports setting individual Directory Server options during server or replica installation

The Identity Management (IdM) **ipa-server-install** and **ipa-replica-install** commands have been enhanced. The new **--dirsrv-config-file** parameter enables the administrator to change default Directory Server settings used during and after the IdM installation. For example, to disable secure LDAP binds in the mentioned situation:

Create a text file with the setting in LDIF format:

```
dn: cn=config
changetype: modify
replace: nsslapd-require-secure-binds
nsslapd-require-secure-binds: off
```

Start the IdM server installation by passing the **--dirsrv-config-file** parameter and file to the installation script:

```
# ipa-server-install --dirsrv-config-file filename.ldif
```

(BZ#825391)

IdM now enables the admin group and ipaservers host group

Identity Management (IdM) now introduces two new groups:

- User group **admins** - Members have full administrative permissions in IdM.
- Host group **ipaservers** - Hosts in this group can be promoted to a replica by users without full administrative permissions. All IdM servers are members of this group. (BZ#1211595)

IdM now supports OTP generation in the Web UI

Identity Management (IdM) now supports one-time password (OTP) generation when adding a host in the Web UI. Select the **`Generate OTP`** check box in the **`Add host`** dialog. After adding the host, a window displays the generated OTP. You can use this password to join the host to the domain. This procedure simplifies the process and provides a strong OTP. To override the OTP, navigate to the host's details page, click, **`Action`** and select **`Reset One-Time-Password`**. (BZ#1146860)

New sss_cache option to mark sudo rules as expired

This update enhances the **`sss_cache`** command from the System Security Services Daemon (SSSD). The options **`-r`** and **`-R`** have been added to mark one or all **sudo** rules as expired. This enables the administrator to force a refresh of new rules on the next **sudo** lookup. Please note that the **sudo** rules are refreshed using a different algorithm than the user and group entities. For more information about the mechanism, see the sssd-sudo(5) man page. (BZ#1031074)

New packages: custodia, python-jwcrypto

This update adds the custodia packages and their dependency python-jwcrypto to Red Hat Enterprise Linux 7.

Custodia is an HTTP-based pipeline to request and distribute secrets. It handles the authentication, authorization, request handling, and storage stages of secrets management. Custodia is currently only supported as an internal subsystem of Red Hat Identity Management.

The package python-jwcrypto is an implementation of the JavaScript object signing and encryption (JOSE) web standards in Python. It is installed as a dependency of Custodia. (BZ#1206288)

New package: python-gssapi

This update adds the python-gssapi package to Red Hat Enterprise Linux 7. It provides a generic security services API (GSSAPI) that is compatible with Python 2 and 3. Identity Management (IdM) uses the package as a replacement for python-krbV and python-pykerberos, which only support Python 2 (BZ#1292139)

New package: python-netifaces

This update adds the python-netifaces package to Red Hat Enterprise Linux 7. This Python module makes it possible to read information about the system network interfaces from the operating system. It has been added as a dependency for Red Hat Identity Management (IdM). (BZ#1303046)

New package: mod_auth_openidc

This update adds the mod_auth_openidc package to Red Hat Enterprise Linux 7. It enables the Apache HTTP server to act as an OpenID Connect Relying Party for single sign-on (SSO) or as an OAuth 2.0 Resource Server. Web applications can use the module to interact with a variety of OpenID Connect server implementations including the **`Keycloak`** open source project and Red Hat Single Sign-On (SSO) products. (BZ#1292561)

IdM now supports DNS locations

This update adds support for DNS location management to the Identity Management (IdM) integrated DNS server to improve cross-site implementations. Previously, clients using DNS records to locate IdM servers could not distinguish local servers from servers located in remote geographical locations. This update enables clients using DNS discovery to find the nearest servers, and to use the network in an optimized way. As a result, administrators can manage DNS locations and assign servers to them in the IdM web user interface and from the command line.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#dns-locations (BZ#747612)

IdM now supports establishing an external trust to an AD domain

Red Hat Enterprise Linux Identity Management (IdM) now supports establishing an external trust to an Active Directory (AD) domain in a forest. An external trust is non-transitive and can be established to any domain in an AD forest. This allows to limit a trusted relationship to a specific domain rather than trusting the whole AD forest. (BZ#1314786)

IdM now supports logging in with alternative UPNs

In an Active Directory (AD) forest, it is possible to associate a different user principal name (UPN) suffix with the user name instead of the default domain name. Identity Management (IdM) now allows users from a trusted AD forest to log on with an alternative UPN.

Additionally, the System Security Services Daemon (SSSD) now detects whether the IdM server supports alternative UPNs. If they are supported, SSSD activates this feature automatically on the client.

When you add or remove UPN suffixes in a trusted AD forest, run **`ipa trust-fetch-domains`** on an IdM master to refresh the information for the trusted forest in the IdM database.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Windows_Integration_Guide/index.html#UPN-in-a-trust (BZ#1287194, BZ#1211631)

IdM now supports sub-CAs

Previously, Identity Management (IdM) only supported one certificate authority (CA) that was used to sign all certificates issued within the IdM domain. Now, you can use lightweight sub-CAs for better control over the purpose for which a certificate can be used. For example, a Virtual Private Network (VPN) server can be configured to only accept certificates issued by a sub-CA created for that purpose, rejecting certificates issued by other sub-CAs, such as a smart card CA.

To support this functionality, you can now specify an IdM lightweight sub-CA when requesting a certificate with certmonger.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#lightweight-sub-cas (BZ#1200731, BZ#1345755)

SSSD now supports automatic Kerberos host keytab renewal

Previously, the System Security Services Daemon (SSSD) did not support the automatic renewal of Kerberos host keytab files in an Active Directory (AD). In environments that, for security reasons, do not allow using passwords that never expire, the files had to be manually renewed. With this update, SSSD is able to automatically renew Kerberos host keytab files.

SSSD checks once per day if the machine account password is older than the configured number of days in the **`ad_maximum_machine_account_password_age`** parameter of the **`/etc/sssd/sssd.conf`** file.

For details, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/System-Level_Authentication_Guide/index.html#sssd-auto-keytab-renewal (BZ#1310877)

IdM supports user principal aliases

Previously, Identity Management (IdM) supported only the authentication using the user name. However, in some environments it is a requirement to authenticate with an email address or alias name. IdM has been enhanced and now supports principal aliases. The System Security Services Daemon (SSSD) has also been updated to support this functionality.

To add the aliases **`ualias`** and **`user@example.com`** to the account **`user`**, run the following command:

```
# ipa user-add-principal user ualias user\\@example.com
```

Use the **-C** option to the **kinit** command when with an alias, and the **-E** option when using an enterprise principal name:

```
# kinit -C ualias
# kinit -E user@example.com
```

(BZ#1328552, BZ#1309745)

SSSD cache update performance improvement

Previously, the System Security Services Daemon (SSSD) always updated all cached entries after the cache validity timeout passed. This consumed unnecessarily resources on the client and the server, for entries that have not been changed. SSSD has been enhanced and now checks if the cached entry requires an update. The time stamp values are increased for unchanged entries and stored in the new SSSD database **/var/lib/sss/db/timestamps_$domain.ldb**. This enhancement improves the performance for entries that rarely change on the server side, such as groups. (BZ#1290380)

SSSD now supports sudo rules stored in the IdM schema

Previously, the System Security Services Daemon (SSSD) used the **ou=sudoers** container, generated by the compatibility plug-in, to fetch sudo rules. SSSD has been enhanced to support sudo rules in the **cn=sudo** container that are stored in the Identity Management (IdM) directory schema.

To enable this feature, unset the **ldap_sudo_search_base** parameter in the **/etc/sssd/sssd.conf** file. (BZ#789477)

SSSD now automatically adjusts the ID ranges for AD clients in environments with high RID numbers

The automatic ID mapping mechanism included in the System Security Services Daemon (SSSD) service is now able to merge ID range domains. The SSSD default size of ID ranges is 200,000. In large Active Directory (AD) installations, the administrator had to manually adjust the ID range assigned by SSSD if the Active Directory relative ID (RID) increased 200,000 to correspond with the RID.

With this enhancement, for AD clients having ID mapping enabled, SSSD automatically adjusts the ID ranges in the described situation. As a result, the administrator does not have to adjust the ID range manually, and the default ID mapping mechanism works in large AD installations. (BZ#1059972)

New sssctl option remove-cache

This update adds the **remove-cache** option to the **sssctl** utility. The option removes the local System Security Services Daemon's (SSSD) database contents, and restarts the **sssd** service. This enables the administrator to start from a clean state with SSSD and avoid the need to manually remove cache files. (BZ#1007969)

Password changes on legacy IdM clients

Previously, Red Hat Enterprise Linux contained a version of slapi-nis that does not enable user to change their passwords on legacy Identity Management (IdM) clients. As a consequence, users logged in to clients via the slapi-nis compatibility tree could only update their password using the IdM web UI or directly in Active Directory (AD). A patch has been applied to and as a result, users are now able to change their password on legacy IdM clients. (BZ#1084018)

The `ldapsearch` command can now return all operational attributes

LDAP searches can now return all operational attributes as described in IETF RFC 3673. Using the **+** character in a search will yield all operational attributes to which the bound Distinguished Name (DN) has access. The returned results may be limited depending on applicable Access Control Instructions (ACIs).

An example search might look similar to the following:

```
ldapsearch -LLLx -h localhost -p 10002 -b ou=people,dc=example,dc=com -s
base '+'
dn: ou=People,dc=example,dc=com
```

See https://tools.ietf.org/html/rfc3673 for additional information about this feature. (BZ#1290111)

Increased accuracy of log time stamps

This update increases the accuracy of time stamps in Directory Server logs from one second precision to nanosecond precision by default. This enhancement allows for a more detailed analysis of events in Directory Server, and enables external log systems to correctly rebuild and interweave logs from Directory Server.

Previously, log entries contained time stamps as shown in the following example:

```
[21/Mar/2016:12:00:59 +1000] conn=1 op=0 BIND dn="cn=Directory Manager"
method=128 version=3
```

With this update, the same log entry contains a more accurate time stamp:

```
[21/Mar/2016:12:00:59.061886080 +1000] conn=1 op=0 BIND dn="cn=Directory
Manager" method=128 version=3
```

To revert to the old time stamp format, set the **nsslapd-logging-hr-timestamps-enabled** attribute to **false** in **cn=config**. (BZ#1273549)

Changing a user password now always updates the shadowLastChange attribute

Previously, some ways of changing a user's password could update the **passwordExpirationTime** attribute but not the **shadowLastChange** attribute. Some systems which can interface with Directory Server, such as Active Directory, expect both attributes to be updated, and therefore this behavior could lead to synchronization errors. With this update, any change to a user password updates both attributes, and synchronization problems no longer occur. (BZ#1018944)

ns-slapd now logs failed operations in the audit log

Previously, **ns-slapd** only logged successful changes to the directory. This update adds support for also logging failed changes, their contents, and the reason for the failure. This allows for easier debugging of applications failing to alter directory content as well as detecting possible attacks. (BZ#1209094)

New utility for displaying status of Directory Server instances

Directory Server now provides the **status-dirsrv** command line utility, which outputs the status of one or all instances. Use the following command to obtain a list of all existing instances:

```
status-dirsrv
```

To display the status of a specific instance, append the instance name to the command. See the **status-dirsrv(8)** man page for additional details and a list of return codes. (BZ#1209128)

IdM now supports up to 60 replicas

Previously, Identity Management (IdM) supported up to 20 replicas per IdM domain. This update increases the support limit to 60 replicas per IdM domain.

For detailed replica topology recommendations, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/replica-considerations.html#replica-topology-recommendations (BZ#1274524)

SSSD now reads optional *.conf files from `/etc/sssd/conf.d/`

The System Security Services Daemon (SSSD) has been enhanced to read *.conf files from the **`/etc/sssd/conf.d/`** directory. This enables you to use a general **`/etc/sssd/sssd.conf`** file on all clients and to add additional settings in further configuration files to suit individual clients. SSSD first reads the common **`/etc/sssd/sssd.conf`** file, and then in alphabetical order the other files in **`/etc/sssd/conf.d/`**. The daemon uses the last read configuration parameter if the same one appears multiple times in different files. (BZ#790113)

New option to enable use of quotes in schema

This update introduces the **`LDAP_SCHEMA_ALLOW_QUOTED`** environment variable which adds support for older style schema using quotes in the schema directory. To enable this functionality, set the following variable in the **`/etc/sysconfig/dirsrv-INSTANCE`** configuration file:

```
LDAP_SCHEMA_ALLOW_QUOTED=on
```

(BZ#1368484)

OpenLDAP now supports SHA2 password hashes

The OpenLDAP server in Red Hat Enterprise Linux 7.3 now provides a module for SHA2 support. To load the **`pw-sha2`** module, add the following line to your **`/etc/openldap/slapd.conf`** file: moduleload pw-sha2

As a result, you can store passwords in OpenLDAP using the following hashes:

- SSHA-512
- SSHA-384
- SSHA-256
- SHA-512
- SHA-384
- SHA-256 (BZ#1292568)

The `pki cert-request-find` command now displays the serial number for completed revocation requests

With this update, the **`pki`** subcommand **`cert-request-find`** now displays the certificate ID of revoked certificates for completed revocation requests. (BZ#1224642)

The IdM password policy now enables never-expiring passwords

Previously, all user passwords in Identity Management (IdM) were required to have an expiration date defined. With this update, the administrator can configure user passwords to be valid indefinitely by setting the password policy **`Max lifetime`** value to **`0`**.

Note that new password policy settings apply to new passwords only. For the change to take effect, existing users must update their passwords. (BZ#826790)

`ipa-getkeytab` can now automatically detect the IdM server

When running the **`ipa-getkeytab`** utility on an Identity Management (IdM) server, you are no longer required to specify the server name using the **`-s`** option. The **`ipa-getkeytab`** utility detects the IdM server automatically in this situation. (BZ#768316)

Enhanced sub-commands in the `ipa-replica-manage` utility

The **`ipa-replica-manage`** utility has been enhanced and now additionally supports the **`o=ipaca`** back end in the following sub-commands:

- list-ruv
- clean-ruv
- abort-clean-ruv

Additionally, the **`clean-dangling-ruv`** sub-command has been added to the **`ipa-replica-manage`** utility. This enables the administrator to automatically remove dangling replica update vectors (RUV). (BZ#1212713)

samba rebased to version 4.4.4

The samba packages have been upgraded to upstream version 4.4.4, which provides a number of bug fixes and enhancements over the previous version:

- The WINS nsswitch module now uses the **`libwbclient`** library for WINS queries. Note that the **`winbind`** daemon must be running to resolve WINS names that use the module.
- The default value of the **`winbind expand groups`** option has been changed from **`1`** to **`0`**.
- The **`-u`** and **`-g`** options of the **`smbget`** command have been replaced with the **`-U`** option to match other Samba command's parameter. The **`-U`** option accepts a **`username[%password]`** value. Additionally, the **`username`** and **`password`** parameters in the **`smbgetrc`** configuration file have been replaced with the **`user`** parameter.
- The **`-P`** parameter of the **`smbget`** command has been removed.
- Printing using the **`CUPS`** back end with Kerberos credentials now requires to install the samba-krb5-printing package and to configure CUPS appropriately.
- It is now possible to configure Samba as a print server by using the CUPS back end with Kerberos credentials. To do so, install the samba-krb5-printing package and configure CUPS appropriately.
- Samba and CTDB header files are no longer installed automatically when you install samba.

Samba automatically updates its tdb database files when the **`smbd`**, **`nmbd`**, or **`winbind`** daemon starts. Back up the databases files before starting Samba. Note that Red Hat does not support downgrading tdb database files.

Note that using the Linux kernel CIFS module with SMB protocol 3.1.1 is currently experimental and the functionality is unavailable in kernels provided by Red Hat.

For further information about notable changes, read the upstream release notes before updating:

- https://www.samba.org/samba/history/samba-4.3.0.html
- https://www.samba.org/samba/history/samba-4.4.0.html (BZ#1303076)

New `net ads join` option to prevent AD DNS update

The **`net ads join`** command now provides the **`--no-dns-updates`** option that prevents updating the DNS server with the machine name when joining a client to the Active Directory (AD). This option enables the administrator to bypass the DNS registration if the DNS server does not allow client updates

and thus the DNS update would fail with an error message. (BZ#1263322)

New `realm join` option to set NetBIOS name

The **`realm join`** command now provides the **`--computer-name`** option to set an individual NetBIOS name. This enables the administrator to join a machine to a domain using a different name than the host name. (BZ#1293390)

DRMTool renamed to KRATool

The Data Recovery Manager (DRM) component of Certificate System (CS) is now called Key Recovery Authority (KRA). For consistency with this change, this update renames the DRMTool utility to KRATool. Note that to ease the transition, compatibility symbolic links are provided. The links help ensure that, for example, scripts referencing DRMTool continue working. (BZ#1305622)

Explicit dependency on OpenJDK 1.8.0

The current PKI code has only been verified to work with OpenJDK 1.8.0. Previously, PKI depended on a generic **`java`** link provided by alternatives and assumed that the link would point to OpenJDK 1.8.0. Since the alternatives settings could change for various reasons, it could cause some problems to PKI.

To ensure that PKI always works properly, PKI has been changed to depend more specifically on **`jre_1.8.0_openjdk`** link which will always point to the latest update of OpenJDK 1.8.0 regardless of other Java installation. (BZ#1347466)

The `ipa *-find` commands no longer display member entries

The new default setting in Identity Management (IdM) **`ipa *-find`** commands no longer displays member entries, such as for host groups. Resolving a large number of member entries is resource intensive and the output of the commands can get long and unreadable. As a result, the default was changed. To display members entries, use the **`--all`** option to the **`ipa *-find`** command. For example:

```
# ipa hostgroup-find --all
```

(BZ#1354626)

Certificate System now supports setting a start ID for CRL

The Red Hat Certificate System now supports setting a start ID for certificate revocation lists (CRL) using the **`pki_ca_starting_crl_number`** option in the **`/etc/pki/default.cfg`** file. This enables administrators to migrate certificate authorities (CA) which already have CRLs issued to the Certificate System. (BZ#1358439)

New `pki-server` subcommand to add the issuer DN to a certificate

An enhancement in the Certificate Server now stores the issuer DN in new certificate records and the REST API certificate search enables support for filtering certificates by the issuer DN. To add the issuer DN to existing certificate records, run:

```
# pki-server db-upgrade
```

(BZ#1305992)

Certificate System now removes old CRLs

Previously, if the file based certificate revocation list (CRL) publishing feature was enabled in the Certificate System, the service regularly created new CRL files without removing old ones. As a consequence, the system running Certificate System could eventually run out of space. To address the problem, two new configuration options were added to the **`/etc/pki/pki-tomcat/ca/CS.cfg`** file:

- **`maxAge`** - Sets the number of days after which files expire and be purged. Default is **`0`** (never).
- **`maxFullCRLs`** - Sets the maximum number of CRLs to keep. When new files are published, the oldest file is purged. Default is **`0`** (no limit).

As a result, you can now configure how the Certificate System handles old CRL files. (BZ#1327683)

Specifying certificate nick names in `pkispawn` configuration for cloning

During clone installation, the clone imports the system certificates from the PKCS #12 file specified in the **`pki_clone_pkcs12_path`** parameter in the **`pkispawn`** configuration file. Previously, it was not necessary to specify the nick names of the certificates in the PKCS #12 file.

Due to new IPA requirements, the certificate import mechanism had to be changed. With this update, to ensure that the certificates are imported with the proper trust attributes, the nick names of the CA signing certificate and the audit signing certificate in the PKCS #12 file have to be specified in the following parameters:

- pki_ca_signing_nickname
- pki_audit_signing_nickname (BZ#1321491)

Deploying the Certificate System using an existing CA certificate and key

Previously, the Certificate System generated the key for the certificate authority (CA) certificate internally. With this update, the key generation is optional and the Certificate System now supports reusing an existing CA certificate and key which can be provided by using a PKCS#12 file or a hardware security module (HSM). This mechanism enables the administrator to migrate from an existing CA to the Certificate System. (BZ#1289323)

Separate cipher lists for instances acting as a client

Prior to this feature, the cipher list specified in the **`server.xml`** file was used when a Certificate System instance was acting as a server as well as a client. In some cases, certain ciphers could be not desired or did not work. This update gives administrators tighter control as it allows the administrator to specify an allowed list of SSL ciphers when the server is acting as a client for communication between two Certificate System subsystems. This cipher list is separate from the one stored on the server. (BZ#1302136)

Support for PKCS #7 certificate chains with the `BEGIN/END PKCS7` label

To comply with RFC 7468, PKI tools now accept and generate PKCS #7 certificate chains with the **`BEGIN/END PKCS7`** label instead of the **`BEGIN/END CERTIFICATE CHAIN`** label. (BZ#1353005)

krb5 rebased to version 1.14.1

The krb5 packages have been updated to upstream version 1.14.1, which provides a number of enhancements, new features, and bug fixes. Notably, it implements authentication indicators support to increase security. For further details, see http://web.mit.edu/kerberos/krb5-latest/doc/admin/auth_indicator.html (BZ#1292153)

The Kerberos client now supports configuration snippets

The **`/etc/krb5.conf`** file now loads configuration snippets from the **`/etc/krb5.conf.d/`** directory. This enables compliance with existing distribution configuration standards and crypto policies management. As a result, users can now split configuration files and store the snippets in the **`/etc/krb5.conf.d/`** directory. (BZ#1146945)

IdM rebased to version 4.4.0

The ipa* packages have been upgraded to upstream version 4.4.0, which provide a number of bug fixes and enhancements over the previous version:

- Improved Identity Management (IdM) server performance, such as faster provisioning, Kerberos authentication, and user and group operations with many members.
- DNS locations to enable clients in a branch office to contact only local servers with the possibility to fall back to remote servers.
- Central replication topology management.
- The number of supported replication partners has been increased from 20 to 60 replicas.
- Authentication indicator support for one-time passwords (OTP) and RADIUS. Authentication indicators can be enabled for hosts and services individually.
- Sub-CA support enables the administrator to create individual certificate authorities to issue certificates for specific services.
- Enhanced smart card support for Active Directory (AD) users enables the administrator to store smart card certificates in AD or IdM overrides.
- IdM server API versioning.
- Support for establishing external trusts with AD.
- Alternative AD user principal names (UPN) suffixes. (BZ#1292141)

SSSD now enables fetching autofs maps from an AD server

You can now use the **`autofs_provider=ad`** setting in the [domain] section of the **`/etc/sssd/sssd.conf`** file. With this setting, the System Security Services Daemon (SSSD) fetches **`autofs`** maps from an Active Directory (AD) server.

Previously, when it was required to store **`autofs`** maps in AD, the AD server administrator had to use the **`autofs_provider=ldap`** setting and manually configure the LDAP provider, including the bind method, search base, and other parameters. With this update, it is only required to set **`autofs_provider=ad`** in **`sssd.conf`**.

Note that SSSD expects the **`autofs`** maps stored in AD to follow the format defined in RFC2307: https://tools.ietf.org/html/rfc2307 (BZ#874985)

The `dyndns_server` option enables specifying the DNS server to receive dynamic DNS updates

The System Security Services Daemon (SSSD) now supports the **`dyndns_server`** option in the **`/etc/sssd/sssd.conf`** file. The option specifies the DNS server that is automatically updated with DNS records when the **`dyndns_update`** option is enabled.

The option is useful, for example, in environments where the DNS server is different from the identity server. In such cases, you can use **`dyndnds_server`** to enable SSSD to update the DNS records on the specified DNS server. (BZ#1140022)

SSSD now supports using `full_name_format=%1$s` to set the output name of AD trusted users to a shortname

Previously, in trust setups, certain System Security Services Daemon (SSSD) features required using the default value for the **`full_name_format`** option in the **`/etc/sssd/sssd.conf`** file. Using **`full_name_format=%1$s`** to set the output format of trusted Active Directory (AD) users to a shortname broke other functionality.

This update decouples the internal representation of a user name from the output format. You can now use **`full_name_format=%1$s`** without breaking other SSSD functionality.

Note that the input name must still be qualified, except for when the **`default_domain_suffix`** option is used in **`sssd.conf`**. (BZ#1287209)

Documentation now describes configuration and limitations of IdM clients using an AD DNS host name

The Identity Management (IdM) documentation has been enhanced and now describes the configuration of IdM clients located in the DNS name space of a trusted Active Directory (AD) domain. Note that this is not a recommended configuration and has some limitations. For example, only password authentication is available to access these clients instead of single sign-on. Red Hat recommends to always deploy IdM clients in a DNS zone different from the ones owned by AD and access IdM clients through their IdM host names.

For detailed information, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/ipa-in-ad-dns.html. (BZ#1320838)

Certificate System now supports setting SSL ciphers for individual installation

Previously, if an existing Certificate Server had customized cipher set that did not overlap with the default ciphers used during the installation, a new instance could not be installed to work with existing instances. With this update, Certificate System enables you to customize the SSL cipher using a two-step installation, which avoids this problem. To set the ciphers during a Certificate System instance installation:

1. Prepare a deployment configuration file that includes the **`pki_skip_configuration=True`** option.

2. Pass the deployment configuration file to the **`pkispawn`** command to start the initial part of the installation.

3. Set the ciphers in the **`sslRangeCiphers`** option in the **`/var/lib/pki/<instance>/conf/server.xml`** file.

4. Replace the **`pki_skip_configuration=True`** option with **`pki_skip_installation=True`** in the deployment configuration file.

5. Run the same **`pkispawn`** command to complete the installation. (BZ#1303175)

New attribute for configuring replica release timeout

In a multi-master replication environment where multiple masters receive updates at the same time, it was previously possible for a single master to obtain exclusive access to a replica and hold it for a very long time due to problems such as a slow network connection. During this time, other masters were blocked from accessing the same replica, which considerably slowed down the replication process.

This update adds a new configuration attribute, **`nsds5ReplicaReleaseTimeout`**, which can be used to specify a timeout in seconds. After the specified timeout period passes, the master releases the replica, allowing other masters to access it and send their updates. (BZ#1349571)

CHAPTER 6. CLUSTERING

`Pacemaker` now supports alert agents

You can now create **`Pacemaker`** alert agents to take some external action when a cluster event occurs. The cluster passes information about the event to the agent by means of environment variables. Agents can do anything desired with this information, such as send an email message, log to a file, or update a monitoring system. For information on configuring alert agents, see the Red Hat Enterprise Linux 7 High Availability Add-On Reference: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/index.html. (BZ#1315371)

`Pacemaker` now supports `SBD` fencing configuration

The **`SBD`** daemon integrates with **`Pacemaker`**, a watchdog device, to arrange for nodes to reliably self-terminate when fencing is required. This update adds the **`pcs stonith sbd`** command to configure **`SBD`** in **`Pacemaker`**, and it is now also possible to configure **`SBD`** from the web UI. **`SBD`** fencing can be particularly useful in environments where traditional fencing mechanisms are not possible. For information on using **`SBD`** with **`Pacemaker`**, see the following Red Hat Knowledgebase article: https://access.redhat.com/articles/2212861. (BZ#1164402)

Graceful migration of resources when the `pacemaker_remote` service is stopped on an active Pacemaker Remote node

If the **`pacemaker_remote`** service is stopped on an active Pacemaker Remote node, the cluster will gracefully migrate resources off the node before stopping the node. Previously, Pacemaker Remote nodes were fenced when the service was stopped (including by commands such as **`yum update`**), unless the node was first explicitly taken out of the cluster. Software upgrades and other routine maintenance procedures are now much easier to perform on Pacemaker Remote nodes.

Note: All nodes in the cluster must be upgraded to a version supporting this feature before it can be used on any node. (BZ#1288929)

A `Pacemaker` cluster resource that is used to create a guest node may now be a member of a resource group

Previous **`Pacemaker`** versions did not support including a guest node in a group. As of Red Hat Enterprise Linux 7.3, a **`Pacemaker`** cluster resource such as **`VirtualDomain`** that is used to create a guest node may now be a member of a resource group. This can be useful, for example, to associate a virtual machine with its storage. (BZ#1303765)

`pcsd` now supports setting SSL options and ciphers

Previously, the **`pcsd`** service did not enable the user to easily disable a cipher or a particular version of the SSL or TSL protocol if a vulnerability was found of if the protocol version or the cipher was considered weak for some reason. With this update, the user can easily configure SSL options and ciphers in **`pcsd`**, and RC4 ciphers as well as TLS protocol version 1.1 and earlier are disabled by default. (BZ#1315652)

`pcs` now supports setting expected votes on a live cluster

When nodes fail in a cluster, user sometimes needs to manually lower expected votes in order to recover the cluster. You can now use the **`pcs quorum expected-votes`** command to set expected votes on a live cluster. (BZ#1327739)

Support added for configuring Pacemaker utilization attributes

You can now configure Pacemaker utilization attributes with the **`pcs`** command and the **`pcsd`** Web UI. This allows you to configure the capacity a particular node provides, the capacity a particular resource requires, and an overall strategy for placement of resources. For information on utilization and placement

strategy, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/index.html. (BZ#1158500)

CHAPTER 7. COMPILER AND TOOLS

Support for new instructions in IBM z Systems z13

The new version of GCC brings support for the new hardware instructions of the IBM z Systems z13, along with support for SIMD instructions. The **`-march=z13`** command-line option is needed to enable the new intrinsics. (BZ#1182152)

GCC now generates optimal code for POWER8

On the PowerPC 64 LE architecture, the GCC compiler is now configured with the **`--with-cpu=power8`** and **`--with-tune=power8`** parameters, to make GCC generate optimal code for POWER8 platforms. (BZ#1213268)

Support for Intel Memory Protection Keys (IMPK)

This update to the GCC compiler provides support for IMPK - the compiler can now generate the new PKU instructions. The new instructions can be enabled by using the **`-mpku`** command-line option. (BZ#1304449)

gcc-libraries rebased

The gcc-libraries package has been rebased to the latest GCC 5 version to include various bug fixes and enhancements from the upstream version. (BZ#1265252)

GDB now supports IBM z13 features

This update provides a GDB extension for debugging code utilizing IBM z13 features. This includes disassembling extended IBM z13 instructions and supporting SIMD instructions using 128-bit wide vector registers **`v0-v31`**. Code optimized for IBM z13 can be now debugged by GDB displaying correct instruction mnemonics, vector registers, and retrieving and passing vector register content during inferior calls. (BZ#1182151)

binutils rebased to version 2.25.1

The highlights of the new rebased binutils package include:

- The **`strings`** program now has a **`--data`** command-line option which only prints strings in loadable, initialized data sections. The default behaviour has been changed to match the **`--all`** command-line option.
- The **`strings`** program now has a **`--include-all-whitespace`** command-line option which treats any non-displaying ASCII character as part of the string. This includes carriage return and new line characters which otherwise would be considered to be line terminators.
- The **`objcopy`** program now has a **`--dump-section`** command-line option to extract the contents of named sections and copy them into separate files.
- The **`objcopy`** program now supports wildcard characters in command-line options that take section names.
- The **`as`** assembler now has a **`--gdwarf-sections`** command-line option to enable the generation of per-code-section **`DWARF.debug_line`** sections. This facilitates the removal of those sections when their corresponding code section is removed by linker garbage collection. (BZ#1341730)

Support for the z13 extensions to IBM z Systems architecture.

This update provides multiple upstream patches combined into a single patch and applied to the Red Hat Enterprise Linux 7 binutils package. The z13 extensions are now supported. (BZ#1364516)

Support for `MWAITX`

The updated binutils package for the 32-bit AMD and Intel architecture now provides support for the **MWAITX** instruction. (BZ#1335684)

Support for Zeppelin

The updated binutils package for the 32-bit AMD and Intel architecture now provides support for the **Zeppelin** extensions. (BZ#1335313)

Support for the Large System Extensions

The updated binutils package now provides support for the Large System Extensions to the AArch64 assembler. In addition, support for the **.arch_extension** pseudo-operation has also been added. (BZ#1276755)

elfutils rebased to version 0.166

The elfutils packages contain a number of utilities and libraries related to the creation and maintenance of executable code. The package has been upgraded to version 0.166. Highlighted improvements include:

- **strip**, **unstrip** - These utilities can now handle ELF files with merged strtab/shstrtab tables.
- **elfcompress** - A new utility to compress or decompress ELF sections.
- **readelf** - A new **-z,--decompress** option.
- New functions have been added to **libelf** and **libdw** to handle compressed ELF sections: **elf_compress**, **elf_compress_gnu**, **elf32_getchdr**, **elf64_getchdr**, and **gelf_getchdr**.
- **libdwelf** - a new **dwelf_scn_gnu_compressed_size()** function.
- New **libelf** and **libdw** pkgconfig (package configuration) files.

(BZ#1296313)

valgrind rebased to version 3.11.0

Valgrind is an instrumentation framework that is used for debugging memory, detecting memory leaks, and profiling applications. The package has been upgraded to upstream version 3.11.0. Highlighted improvements include:

- The JIT's register allocator is now significantly faster, making JIT-intensive activities, for example program startup, approximately 5% faster.
- Intel AVX2 support is now more complete for 64-bit targets. On AVX2-capable hosts, the simulated CPUID will now indicate AVX2 support.
- The default value for the **--smc-check** option has been changed from **stack** to **all-non-file** on targets that provide automatic D-I cache coherence. The result is to provide, by default, transparent support for JIT generated and self-modifying code on all targets.

Highlighted new features in the **Memcheck** utility include:

- The default value for the **--leak-check-heuristics** option has been changed from **none** to **all**. This helps to reduce the number of possibly lost blocks, in particular for C++ applications.
- The default value for the **--keep-stacktraces** option has been changed from **malloc-then-free** to **malloc-and-free**. This has a small cost in memory but allows **Memcheck** to show the 3 stack traces of a dangling reference: where the block was allocated, where it was

freed, and where it is accessed after being freed.

- The default value for the **--partial-loads-ok** option has been changed from **no** to **yes**, to avoid false-positive errors resulting from certain vectorised loops.
- A new gdb monitor command **xb [addr] [len]** shows the validity bits of **[len]** bytes at **[addr]**. The monitor command **xb** is easier to use than **get_vbits** when you need to associate byte data value with their corresponding validity bits.
- The **block_list** gdb monitor command has been enhanced: it can print a range of loss records; it now accepts an optional argument, **limited [max_blocks]**, to control the number of printed blocks; if a block has been found using a heuristic, then **block_list** now shows the heuristic after the block size; the loss records/blocks to print can be limited to the blocks found via specified heuristics.
- A new **--expensive-definedness-checks=yes|no** command-line option has been added. This is useful for avoiding occasional invalid uninitialized-value errors in optimized code. Beware of potential runtime degradation, as this can be up to 25%. The slowdown is highly application-specific though. The default value is **no**.

(BZ#1296318)

Interception of user-defined allocation functions in valgrind

Some applications do not use the **glibc** allocator. Consequently, it was not always convenient to run such applications under **valgrind**. With this update, **valgrind** tries to automatically intercept user-defined memory allocation functions as if the program used the normal **glibc** allocator, making it possible to use memory tracing utilities such as **memcheck** on those programs out of the box. (BZ#1271754)

systemtap rebased to version 3.0

The systemtap packages have been updated to upstream version 3.0, which provides a number of bug fixes and enhancements. For example, the translator has been improved to require less memory, produce faster code, support more function callee probing, print improved diagnostics, include language extensions for function overloading and private scoping, and introduce experimental **--monitor** and **--interactive** modes. (BZ#1289617)

Support for the 7th-generation Core i3, i5, and i7 Intel processors

This update provides a complete set of performance monitoring events for the 7th-generation Core i3, i5, and i7 Intel processors (Kabylake-U/Y). (BZ#1310950)

Support for the 7th-generation Core i3, i5, and i7 Intel processors

This update provides a complete set of performance monitoring events for the 7th-generation Core i3, i5, and i7 Intel processors (Kabylake-H/S). (BZ#1310951)

libpfm rebased to version 4.7.0

The libpfm package has been upgraded to version 4.7.0. This version provides support for the following 32-bit AMD and Intel architectures:

- Intel Skylake core PMU
- Intel Haswell-EP uncore PMUs
- Intel Broadwell-DE
- Intel Broadwell (desktop core)

- Intel Haswell-EP (core)
- Intel Haswell-EP (core)
- Intel Ivy Bridge-EP uncore PMUs (all boxes)
- Intel Silvermont core PMU
- Intel RAPL events support
- Intel SNB, IVB, HSW event table updates
- Major update on Intel event tables
- AMD Fam15h Northbridge PMU

(BZ#1321051)

gssproxy now supports RELRO and PIE

The GSS-API **gssproxy** daemon is now built using the security-related **RELRO** and **PIE** compile-time flags to harden the daemon. As a result, gssproxy provides a higher security against loader memory area overwrite attempts and memory corruption attacks. (BZ#1092515)

iputils rebased to version 20160308

The iputils packages have been upgraded to upstream version 20160308, which provides a number of bug fixes and enhancements over the previous version. Notably, the **ping** command is now dual stack aware. It can be used for probing both IPv4 and IPv6 addresses. The old **ping6** command is now a symbolic link to the **ping** command and works the same way as before. (BZ#1273336)

Logging capabilities of the `tftp` server have been enhanced

As a result of improved logging, the Trivial File Transfer Protocol (TFTP) server can now track successes and failures. For example, a log event is now created when a client successfully finishes downloading a file, or the **file not found** message is provided in case of a failure. (BZ#1311092)

New option for arpwatch: `-p`

This update introduces option **-p** for the **arpwatch** command of the **arpwatch** network monitoring tool. This option disables promiscuous mode. (BZ#1291722)

The `chrt` utility now has new options

This update introduces new command-line options for the **chrt** utility: **--deadline**, **--sched-runtime**, **--sched-period**, and **--sched-deadline**. These options take advantage of the kernel **SCHED_DEADLINE** scheduler and provide full control of deadline scheduling policy for scripts and when using the command line. (BZ#1298384)

New command-line utility: `lsipc`

This update introduces the **lsipc** utility that lists information about inter-process communication (IPC) facilities. In comparison with the old **ipcs** command, **lsipc** provides more details, is easier to use in scripts, and is more user-friendly. This results into better control of the output on IPC information for scripts and when using the command line. (BZ#1153770)

Searching using `libmount` and `findmnt` is now more reliable

Overlay filesystem's **st_dev** does not provide possibility for reliable searching to the **libmount** library and the **findmnt** utility. With this update, **libmount** and **findmnt** search in mount tables by other means than with **st_dev** in some cases, achieving better reliability. (BZ#587393)

New `--family` option for the `alternatives` utility

This update introduces the new **`--family`** option for the **`alternatives`** utility. The software packager can use this option to group similar alternative packages from the same group into families. Families inside groups ensure that if the currently used alternative is removed, and it belonged to a family, then the current alternative will change to package with the highest priority within the same family, and not outside the family.

For example, a system has four packages installed in the same **`alternatives`** group: a1, a2, a3, b (listed in increasing priority). Packages a1, a2, and a3 belong to the same family. a1 is the currently used alternative. If a1 is removed, then the currently used alternative will change to a3. It will not be b, because b is outside the family of a1, and it will not be a2, because a2 has lower priority than a3.

This option is useful when just setting priorities for each alternative is not enough. For example, all openjdk packages can be put into the same family to ensure that if one of them is uninstalled, the alternative will switch to another openjdk package, and not to the java-1.7.0-oracle package (if another openjdk package is installed). (BZ#1291340)

sos rebased to version 3.3

The sos package has been updated to upstream version 3.3, which provides a number of enhancements, new features, and bug fixes, including:

- Support for OpenShift Enterprise 3.x
- Improved and expanded OpenStack plug-ins
- Enhanced support for Open vSwitch
- Enhanced Kubernetes data collection
- Improved support for **`systemd`** journal collection
- Enhanced display manager and 3D acceleration data capture
- Improved support for Linux clusters, including Pacemaker
- Expanded CPU and NUMA topology collection
- Expanded mainframe (IBM z Systems) coverage
- Collection of multipath topology (BZ#1293044)

ethtool rebased to version 4.5

The ethtool utility enables querying and changing settings such as speed, port, auto-negotiation, PCI locations, and checksum offload on many network devices, especially Ethernet devices. The package has been upgraded to upstream version 4.5. Notable improvements include:

- SFP serial number and date are now included in EEPROM dump (option **`-m`**)
- Added missing Advertised speeds, some combinations of 10GbE and 56GbE
- Added register dump support for VMware vmxnet3 (option **`-d`**)
- Added support for setting the default **`Rx`** flow indirection table (option **`-X`**)

(BZ#1318316)

pcp rebased to version 3.11.3

Performance Co-Pilot (PCP) is a suite of tools, services, and libraries for acquisition, archiving, and analysis of system-level performance measurements. The package has been upgraded to version 3.11.3. Highlighted improvements include:

- **pcp-ipcs** - new command to show inter-process communication
- **pcp-atopsar** - new PMAPI sar command based on http://atoptool.nl
- **pcp-vmstat** - wrapper for **pmstat** modified to more closely resemble **vmstat**
- **libpcp** - new **fetchgroup** API
- **pmdamic** - new PMDA for Intel MIC card metrics
- **pmdaslurm** - new PMDA exporting HPC scheduler metrics
- **pmdapipe** - command output event capture PMDA
- **pmdaxfs** - support for per-device XFS metrics
- **pmdavmware** - updated to work with current VMWare Perl API
- **pmdaperfevent** - variety of improvements surrounding derived metrics; added reference clock cycles for NHM and WSM
- **pmdaoracle** - Oracle database metrics available and updated
- **pmdads389** - added normalized dn cache metrics
- **pmdalinux** - added metrics for per numa node memory bandwidth, shared memory segments, IPC, MD driver stats, transparent-huge-page zero page alloc counters, NVME devices, IPv6 metrics
- **pmdaelasticsearch** - restrict to local node metrics by default and adjust to **elasticsearch** API change
- **pmdaxfs** - support for per-device XFS metrics
- **pmrep** - powerful and versatile metric-reporting utility
- **pmlogconf** - support for automatic recording of Oracle database, nginx, elasticsearch, memcache, and application metrics supplied by **mmv**
- **zbxpcp** - Zabbix Agent loadable module for **PCP** metrics supporting Zabbix v2 and v3 simultaneously
- **pmcd** - support for starting PMDAs via **pmdaroot**, allowing restart on PMDA failure without restarting **pmcd** itself
- **sar2pcp** - support for additional **mem.util** metrics and sysstat-11.0.1 commands
- **pmmgr** - added general monitor-program launching option
- **pcp-atop** - updated with latest **atop** features (especially NFS-related)

- **libpcp** - allowed the name of a server certificate to be customized; added support for permanent, global derived metrics, and multi-archive contexts
- **pmdaproc** - **cgroup blkio** throttle throughput and IOPS metrics
- **pcp-iostat** - added the **-R** flag for device-name matching using regular expressions and the **-G** flag for **sum**, **avg**, **min**, or **max statistics**
- **pmieconf** - new rule to automate restarting of unresponsive PMDAs

(BZ#1284307)

OpenJDK 8 now supports ECC

With this update, support for Elliptic Curve Cryptography (ECC) and associated ciphers for TLS connections has been added to **OpenJDK 8**. In most cases, ECC is preferable to older cryptographic solutions for establishing secure network connections. (BZ#1245810)

pycurl now provides options to require TLSv1.1 or 1.2

With this update, **pycurl** has been enhanced to support options that make it possible to require the use of the 1.1 or 1.2 versions of the TLS protocol, which improves the security of communication. (BZ#1260407)

Perl Net:SSLeay now supports elliptic curve parameters

Support for elliptic-curve parameters has been added to the Perl **Net:SSLeay** module, which contains bindings to the OpenSSL library. Namely, the **EC_KEY_new_by_curve_name()**, **EC_KEY_free*()**, **SSL_CTX_set_tmp_ecdh()**, and **OBJ_txt2nid()** subroutines have been ported from upstream. This is required for the support of the Elliptic Curve Diffie–Hellman Exchange (ECDHE) key exchange in the **IO::Socket::SSL** Perl module. (BZ#1316379)

Perl IO::Socket::SSL now supports ECDHE

Support for Elliptic Curve Diffie–Hellman Exchange (ECDHE) has been added to the **IO::Socket::SSL** Perl module. The new **SSL_ecdh_curve** option can be used for specifying a suitable curve by the Object Identifier (OID) or Name Identifier (NID). As a result, it is now possible to override the default elliptic curve parameters when implementing a TLS client using **IO::Socket:SSL**. (BZ#1316377)

tcsh now uses system allocation functions

The **tcsh** command language interpreter now uses allocation functions from the **glibc** library instead of built-in allocation functions. This eliminates earlier problems with the **malloc()** library call. (BZ#1315713)

Python performance enhancement

The **CPython** interpreter now uses computed **goto** statements at the main **switch** statement, which executes **Python** bytecode. This enhancement allows the interpreter to avoid a bounds check that is required by the C99 standard for the **switch** statement, and allows the CPU to perform more efficient branch prediction, which reduces pipeline flushes. As a result of this enhancement, **Python** code is interpreted significantly faster than before. (BZ#1289277)

telnet now accepts -i to use an IP address when calling login

When a computer on a network has multiple IP addresses, it was previously possible to use one address to connect to the **telnet** server, but the other addresses were saved in the **/var/run/utmp** file. To prevent the **telnet** utility from performing a DNS lookup and ensure that **telnet** uses a particular IP

address when calling the **login** utility, you can now use the **-i** option. Note that **-i** works in the same way as the **-N** option on Debian systems. (BZ#1323094)

sg3_utils rebased to version 1.37-7

The sg3_utils packages provide command-line utilities for devices that use the Small Computer System Interface (SCSI) command sets. With this update, the **sg_inq** and **sg_vpd** utilities allow decoding of more feature information on storage devices. Additionally, the presentation of date and software version information is now displayed correctly. The **sg_rdac** utility has been fixed as well and now supports 10-byte Command Descriptor Block (CDB) mode, which allows management of up to 256 logical unit numbers (LUN). (BZ#1170719)

New configuration options for SSL/TLS certificate verification for the HTTP clients in the Python standard library

New per-application and per-process configuration options for SSL/TLS certificate verification have been added for the HTTP clients in the Python standard library. The options are described in the 493 Python Enhancement Proposal (https://www.python.org/dev/peps/pep-0493/). The default global setting continues to be to not verify certificates. For details, see https://access.redhat.com/articles/2039753. (BZ#1315758)

`glibc` now supports the BIG5-HKSCS-2008 character set

Previously, **glibc** supported an earlier version of the Hong Kong Supplementary Character Set, BIG5-HKSCS-2004. The BIG5-HKSCS character set map has been updated to the HKSCS-2008 revision of the standard. This allows Red Hat Enterprise Linux customers to write applications processing text that is encoded with this version of the standard. (BZ#1211823)

memtest86+ rebased to version 5.01

The memtest86+ package has been upgraded to upstream version 5.01, which provides a number of bug fixes and enhancements over the previous version. Notable changes include the following:

- Support for up to 2 TB of RAM on AMD64 and Intel 64 CPUs
- Support for new Intel and AMD CPUs, for example Intel Haswell
- Experimental SMT support up to 32 cores

For detailed changes, see http://www.memtest.org/#change (BZ#1280352)

mcelog rebased to version 136

The mcelog packages have been upgraded to upstream version 136, which provides a number of bug fixes and enhancements over the previous version. Notably, support for various 5th and 6th generation Intel Core processors (Broadwell-DE/SoC, Broadwell-EP, Broadwell-EX, and Skylake Client) has been included. (BZ#1336431)

xz rebased to version 5.2.2

The xz packages have been upgraded to upstream version 5.2.2, which provides several optimization fixes, fixes for race conditions, translations, portability fixes, and also a new stabilized API previously available only for testing. Additionally, this update introduces a new experimental feature controlled by the **--flush-timeout** option (by default off). When compressing, if more than timeout milliseconds (a positive integer) have passed since the previous flush and reading more input would be blocked, all the pending input data is flushed from the encoder and made available in the output stream. This can be useful if the **xz** utility is used for compressing data that is streamed over a network. (BZ#1160193)

`tapestat` has been added to sysstat

The sysstat packages now provide the **tapestat** utility, which can be used to monitor performance of tape drives. (BZ#1332662)

sysstat now supports a larger number of processors

The sysstat packages now support the maximum number of processors supported by the Linux kernel, which is 8192 at the time of Red Hat Enterprise Linux 7.3 release. Previously, sysstat could not handle more than 2048 processors. (BZ#1258990)

ruby rebased to version 2.0.0.648

The ruby packages have been upgraded to upstream version 2.0.0.648, which provides a number of bug and security fixes. This is the last upstream stable release of **Ruby 2.0.0** as it has been deprecated in upstream. More recent versions of Ruby are available in Red Hat Software Collections. (BZ#1197720)

Enhancements to abrt reporting workflow

The problem-reporting workflow in **abrt** has been enhanced to improve the overall crash-reporting experience and customer-case creation. The enhancements include:

- The **Provide additional information** screen now allows you to select whether the problem happens repeatedly, and also contains an additional input field for providing steps to reproduce the problem.
- A new reporting workflow **Submit anonymous report**, which should be used when the reported problem is not critical and no Red Hat support team assistance is required.
- New tests have been added to the internal logic to ensure that users only open cases for critical problems and software released by Red Hat. (BZ#1258482)

abrt can now exclude specific programs from generating a core dump

Previously, ignoring crashes of blacklisted programs in **abrt** did not prevent it from creating their core dumps, which were written to disk and then deleted. This approach allowed **abrt** to notify system administrators of a crash while not using disk space to store unneeded crash dumps. However, creating these dumps only to delete them later was unnecessarily wasting system resources. This update introduces a new configuration option **IgnoredPaths** in the **/etc/abrt/plugins/CCpp.conf** configuration file, which allows you to specify a comma-separated list of file system path patterns, for which core dump will not be generated at all. (BZ#1277848)

User and group whitelisting added to abrt

Previously, **abrt** allowed all users to generate and collect core dumps, which could potentially enable any user to maliciously generate a large number of core dumps and waste system resources. This update adds a whitelisting functionality to **abrt**, and you can now only allow specific users or groups to generate core dumps. Use the new **AllowedUsers = user1, user2, ...** and **AllowedGroups = group1, group2, ...** options in the **/etc/abrt/plugins/CCpp.conf** configuration file to restrict core dump generation and collection to these users or groups, or leave these options empty to configure **abrt** to process core dumps for all users and groups. (BZ#1277849)

Format of emails sent by ABRT is now configurable

You can now configure the format of emails sent by **ABRT** using the new **-F FORMAT_FILE** command-line option of the **reporter-mailx** utility. This option allows you to define your own format. Without the **-F** option, **reporter-mailx** uses the default format, which sorts all important elements by importance. For more information about the format of formatting files, see the **reporter-mailx(1)** man page. (BZ#1281312)

The Oracle ACFS is now included among known file systems

Previously, the Oracle ASM Cluster file system (ACFS) was not listed among known file systems for the **stat** and **tail** utilities. As a consequence, the **tail** utility printed an error message stating that the file system was not recognized. ACFS has been added to the list of known file systems, and the error message no longer appears in the described situation.

In addition, other file systems recognized by upstream have been added to the list of known file systems as well, namely **bpf_fs**, **btrfs_test**, **configfs**, **hfs+**, **hfsx**, **ibrix**, **logfs**, **m1fs**, **nsfs**, **overlayfs**, **prl_fs**, and **tracefs**. (BZ#1280357)

Support for Octave 3.8 used by swig

Previously, the Octave code generated by **swig** 2.0.10 did not work with Octave 3.8, because it contained deprecated bits such as variables and macros. This update ensures that **swig** produces code which works with Octave of versions 3.0.5, 3.2.4, 3.4.3, 3.6.4, and 3.8.0. (BZ#1136487)

The sos `cluster` plug-in has been divided into type-specific plug-ins

The **cluster** plug-in in the sos package has been divided into several plug-ins (**cman**, **dlm**, **gfs2**, and **pacemaker**). The new plug-in organization reflects that there are two different types of cluster (**cman** and **pacemaker**) and prevents certain commands from needing to be run multiple times. (BZ#1187258)

libvpd rebased to version 2.2.5

The libvpd packages have been updated to upstream version 2.2.5, which provides a number of bug fixes and enhancements over the previous version. Notably, it also implements several security fixes, including the buffer overflow and memory allocation validation. (BZ#1182031)

Man pages for `pchrt` and `ptaskset` added to python-schedutils

This update adds man pages for the **pchrt** and **ptaskset** utilities, which are provided by the python-schedutils package. (BZ#948381)

The socket timeout value for SSL connections of the `subscription-manager` client is now configurable

Previously, the socket timeout value for SSL connections to an entitlement server was hard-coded. With this update, users can configure a custom SSL timeout value in the **/etc/rhsm/rhsm.conf** file. Setting a larger SSL timeout helps ensure that expensive operations involving many subscriptions have enough time to complete. (BZ#1346417)

`redhat-uep.pem` CA certificate moved to a `python-rhsm-certificates` package

The **/etc/rhsm/ca/redhat-uep.pem** certificate authority (CA) certificate was previously included in the **python-rhsm** package. This update moves this certificate into a simplified **python-rhsm-certificates** package that provides only the certificate. As a result, container images can now be built only with **python-rhsm-certificates** without all the package dependencies required by **python-rhsm**, specifically the **python** package. (BZ#1104332)

gfs2-utils rebased to version 3.1.9

The gfs2-utils package has been updated to upstream version 3.1.9, which provides a number of enhancements, new features, and bug fixes, including the following:

- fsck.gfs2 now uses less memory
- Improvements and fixes to the extended attributes and resource group checking of fsck.gfs2
- mkfs.gfs2 reports progress so that the user can tell it is still active during a long mkfs operation
- The **-t** option of mkfs.gfs2 now accepts a longer cluster name and file system name
- A udev helper script is now installed to suspend the device on withdraw, which prevents hangs
- Support for the de_rahead and de_cookie dirent fields has been added
- gfs2_edit savemeta performance improvements

- The glocktop utility has been added to help analyze locking-related performance problems
- The mkfs.gfs2(8) man page has been reworked
- The **rgrplbv** and **loccookie** mount options have been added to the gfs2(5) man page
- Fixes for out-of-tree builds and testing (BZ#1271674)

system-switch-java rebased to version 1.7

The system-switch-java package, which provides an easy-to-use tool to select the default Java toolset for the system, has been updated to version 1.7. The new version has been rewritten to support modern JDK packages. The main enhancements include support for multiple Java installations, addition of -debug packages, and support for JDK 9. (BZ#1283904)

Optional branch predictor optimization for certain Intel micro-architectures

The branch predictor in the 2nd generation Xeon Phi and 3rd generation Atom micro-architectures only supports 32-bit offsets between branch and branch targets. If a branch and its target were further apart than 4 GiB, performance was very poor.

With this update, **glibc** maps the main program and shared objects into the first 31 bits of the address space if the **LD_PREFER_MAP_32BIT_EXEC** environment variable is set, improving performance on the described architectures. Note that this improvement reduces address space layout randomization (ASLR) and is therefore not enabled by default. (BZ#1292018)

Optimized memory routines for Intel hardware using AVX 512

This update provides optimized memory copying routines to the core C library (glibc) for Intel hardware using AVX 512. These optimized routines are automatically selected when applications use the C library **memcpy()**, **memmove()**, or **memset()** function on AVX 512-enabled hardware.

The AVX 512-enabled memory copying routine provides the best possible performance on the latest Intel hardware that supports this feature, particularly on the second-generation Xeon Phi systems. (BZ#1298526)

Better-performance `memset()` routine

This update provides a key optimization to the core C library **memset()** routine for Intel Xeon v5 server hardware. The existing **memset()** routine for AMD64 and Intel 64 architectures made extensive use of non-temporal stores, a hardware feature which does not provide uniform performance across hardware variants. The new **memset()** provides better performance across hardware variants, including Intel Xeon v5 hardware. (BZ#1335286)

Support for the `--instLangs` option in `glibc`

The glibc-common packages provide a large locale archive containing data for all locales supported by **glibc**. Typical installations only need a subset of these locales, and installing all of them is wasteful. With this update, it is possible to create system installations and container images which only include required locales, greatly reducing image size. (BZ#1296297)

Optimizations in `glibc` for IBM POWER8

With this update, all libraries provided by **glibc** have been compiled for optimal execution on POWER8 hardware. Optimized memory and string manipulation routines for 64-bit IBM POWER7 and POWER8 hardware have been added to the core C library (glibc). These optimized routines are automatically selected when applications use C library routines like **strncat()** or **strncmp()**. These POWER7 and POWER8-enabled routines provide the best possible performance on the latest IBM hardware. (BZ#1213267, BZ#1183088, BZ#1240351)

Optimizations in `glibc` for IBM z Systems z13

The core C library (glibc) has been enhanced to provide optimized support for IBM z Systems z13 hardware. Core string and memory manipulation routines such as **`strncpy()`** or **`memcpy()`** have all been optimized. The z13-enabled routines provide the best possible performance on the latest IBM hardware. (BZ#1268008)

`Origin` plug-in added to the sos package

The **`origin`** plug-in has been added to the sos package. The plug-in collects information about **`OpenShift Origin`** and related products, such as **`Atomic Platform`** or **`OpenShift Enterprise 3`** and higher. This allows users to gather information about **`OpenShift Origin`** deployments. (BZ#1246423)

gssproxy now supports krb5 1.14

The gssproxy packages, which provide a daemon to manage access to GSSAPI credentials, as well as a GSSAPI interposer plug-in, have been updated to upstream version 0.4.1-10. gssproxy now supports the krb5 packages in version 1.14. (BZ#1292487)

A possibility to configure optional SSH key files for the ABRT `reporter-upload` tool has been added

This update adds the possibility to configure an SSH key in the **`reporter-upload`** utility of Automatic Bug Reporting Tool (ABRT). To specify the key file, choose one of the following ways:

- Using the **`SSHPublicKey`** and **`SSHPrivateKey`** options in the **`/etc/libreport/plugins/upload.conf`** configuration file
- Using the **`-b`** and **`-r`** command-line options for the public and private key, respectively
- Setting the **`Upload_SSHPublicKey`** and **`Upload_SSHPrivateKey`** environment variables, respectively.

If none of these options or variables are specified, **`reporter-upload`** uses the default SSH key from the user's **`~/.ssh/`** directory. (BZ#1289513)

CHAPTER 8. DESKTOP

New packages: pidgin and pidgin-sipe

This update adds:

- The **pidgin** instant messaging client, which supports off-the-record (OTR) messaging and the Microsoft Lync instant messaging application.
- The **pidgin-sipe** plug-in, which contains a back-end code that implements support for Lync.

The users need both the application and the plug-in to use Microsoft Lync. (BZ#1066457, BZ#1297461)

Scroll wheel increment configurable in GNOME terminal

With this update, the _gnome-terminal packages have been upgraded so that the scroll wheel setting is now configurable in the GNOME terminal. The scrolling preferences include a checkbutton and a spinbutton, which allow to choose between dynamic or fixed scrolling increment. The default option is dynamic scrolling increment, which is based on the number of visible rows. (BZ#1103380)

Vinagre user experience improvements

The Vinagre remote desktop viewer introduces the following user experience enhancements:

- A minimize button is available in the fullscreen toolbar, which makes access to custom options easier.
- It is now possible to scale Remote Desktop Protocol (RDP) sessions. You can set the session size in the Connect dialog.
- You can now use the secrets service to safely store and retrieve remote credentials. (BZ#1291275)

Custom titles for the terminal tabs or windows

This update allows users to set custom titles for terminal windows or tabs in **gnome-terminal**. The titles can be changed directly in the **gnome-terminal** user interface. (BZ#1296110)

Separate menu items for opening tabs and windows restored

This update restores separate menu items for opening tabs and windows in **gnome-terminal**. It is now easier to open a mix of tabs and windows without being familiar with keyboard shortcuts. (BZ#1300826)

Native Gnome/GTK+ look for Qt applications

Previously, the default Qt style did not provide consistency for Qt applications, causing them not to fit into Gnome desktop. A new **adwaita-qt** style has been provided for those applications and the visual differences between the Qt and GTK+ applications are now minimal. (BZ#1306307)

rhythmbox rebased to version 3.3.1

Rhythmbox is the GNOME default music player. It is easy to use and includes features such as playlists, podcast playback, and audio streaming. The rhythmbox packages have been upgraded to upstream version 3.3.1. The most notable changes include:

- Better support for Android devices
- New task progress display below the track list
- Support for the composer, disc, and track total tags
- New style for playback controls and the source list

- A number of bug fixes for various warnings and unexpected termination errors (BZ#1298233)

libreoffice rebased to version 5.0.6.2

The libreoffice packages have been upgraded to upstream version 5.0.6.2, which provides a number of bug fixes and enhancements over the previous version, notably:

- The status bar and various sidebar decks have been improved.
- Various toolbars and context menus have been cleaned up or rearranged for better usability.
- The color selector has been reworked.
- New templates have been created.
- Templates now appear directly in the Start Center and can be picked from there.
- libreoffice now displays an information bar to indicate visibly when a document is being opened in read-only mode.
- The possibility to embed libreoffice in certain web browsers by using the deprecated NPAPI has been removed.
- It is possible to connect to SharePoint 2010 and 2013 and OneDrive directly from libreoffice.
- Support for converting formulas into direct values, Master Document templates, reading Adobe Swatch Exchange color palettes in the **`.ase`** format, importing Adobe PageMaker documents, and for exporting digitally signed PDF files.
- It is now possible to specify references to entire columns or rows using the A:A or 1:1 notation.
- Interoperability with Microsoft Office document formats has been improved.

For a complete list of bug fixes and enhancements provided by this upgrade, see https://wiki.documentfoundation.org/ReleaseNotes/4.4 and https://wiki.documentfoundation.org/ReleaseNotes/5.0. (BZ#1290148)

GNOME boxes support for Windows Server 2012 R2, Windows 10, and Windows 8.1

GNOME boxes now supports creating virtual machines with Windows Server 2012 R2, Windows 10, and Windows 8.1. (BZ#1257865, BZ#1257867, BZ#1267869)

The `vmware` graphics driver now supports 3D acceleration in VMware Workstation 12

Previously, the **`vmware`** graphics driver in Red Hat Enterprise Linux did not support 3D acceleration in VMware Workstation 12 virtual machines (VM). As a consequence, the GNOME desktop was rendered on the host's CPU instead of the GPU. The driver has been updated to support the VMware Workstation 12 virtual graphics adapter. As a result, the GNOME desktop is now rendered using 3D acceleration. (BZ#1263120)

libdvdnav rebased to version 5.0.3

The **`libdvdnav`** library allows you to navigate DVD menus on any operating system. The libdvdnav packages have been upgraded to version 5.0.3. The most notable changes include:

- Fixed a bug on menu-less DVDs
- Fixed playback issues on multi-angle DVDs

- Fixed unexpected termination when playing a DVD from different region than currently set in the DVD drive
- Fixed memory bugs when reading certain DVDs (BZ#1068814)

GIMP rebased to version 2.8.16

The GNU Image Manipulation Program (GIMP) has been upgraded to version 2.8.16, which provides a number of bug fixes and enhancements over the previous version. Notable changes include the following:

Core:

- More robust loading of XCF files
- Improved performance and behavior when writing XCF files

GUI:

- The widget direction automatically matches the direction of language set for GUI
- Larger scroll area for tags
- Fixed switching of dock tabs by drag and drop (DND) hovering
- DND works between images in one dockable
- No unexpected termination problem in the save dialog

Plug-ins:

- Improved security of the script-fu server
- Fixed reading and writing of files in the BMP format
- Fixed exporting of fonts in the PDF plug-in
- Support of layer groups in OpenRaster files
- Fixed loading of PSD files with layer groups (BZ#1298226)

gimp-help rebased to version 2.8.2

The gimp-help package has been upgraded to upstream version 2.8.2, which provides a number of bug fixes and enhancements over the previous version. Notably, it also implements a complete translation to Brazilian Portuguese. (BZ#1370595)

Qt5 added to Red Hat Enterprise Linux 7

A new version of the **Qt** library (Qt5) has been added to Red Hat Enterprise Linux 7. This version of **Qt** brings number of features for developers as well as support for mobile devices, which was missing in the previous version. (BZ#1272603)

Improved UI message when setting a new language in system-config-language

Previously, if you selected a new language to install in the **Language** graphical tool (the system-config-language package), and the selected language group was not available, the error message that was displayed was not clear enough. For example, if you selected **Italian (Switzerland)**, the message displayed was:

```
Due to comps cleanup italian-support group got removed and no longer
```

```
exists. Therefore only setting the default system language
```

With this update, the message is updated and will look similar to the following example:

```
Due to comps cleanup, italian-support group no longer exists and its
language packages will not be installed. Therefore only setting Italian as
the default system language.
```

The new message means that the new language has been enabled without having to install any new packages. After the next reboot, the system will boot in the selected language. (BZ#1328068)

New packages: pavucontrol

This update adds the pavucontrol packages, which contain PulseAudio Volume Control, a GTK-based volume control application for the PulseAudio sound server. This application enables to send the output of different audio streams to different output devices, such as headsets or speakers. Individual routing is impossible with the default audio control panel, which sends all audio streams to the same output device. (BZ#1210846)

libdvdread rebased to version 5.0.3

The libdvdread packages have been rebased to version 5.0.3. The most notable changes include:

- Fixes for numerous crashes, assertions and corruptions
- Fixed compilation in C++ applications
- Removed the unused feature to remap .MAP files
- Removed the **`dvdnavmini`** library
- Added the **`DVDOpenStream`** API

Because of API change, .so version also changed. Third-party software dependent on libdvdread needs to be recompiled against this new version. (BZ#1326238)

New weather service for `gnome-weather`

Previously, the **`gnome-weather`** application used the METAR services provided by the National Oceanic and Atmospheric Administration (NOAA). However, NOAA stopped to provide the METAR service. This update introduces a new METAR service provided by the Aviation Weather Center (AWC) and **`gnome-weather`** now works as expected. (BZ#1371550)

libosinfo rebased to version 0.3.0

The libosinfo packages have been updated to version 0.3.0. Notable changes over the previous version include improving operating system data for several recent versions of Red Hat Enterprise Linux and Ubuntu, and fixing several memory leaks. (BZ#1282919)

CHAPTER 9. FILE SYSTEMS

XFS runtime statistics are available per file system in the `/sys/fs/` directory

The existing XFS global statistics directory has been moved from the **`/proc/fs/xfs/`** directory to the **`/sys/fs/xfs/`** directory while maintaining compatibility with earlier versions with a symbolic link in **`/proc/fs/xfs/stat`**. New subdirectories will be created and maintained for statistics per file system in **`/sys/fs/xfs/`**, for example **`/sys/fs/xfs/sdb7/stats`** and **`/sys/fs/xfs/sdb8/stats`**. Previously, XFS runtime statistics were available only per server. Now, XFS runtime statistics are available per device. (BZ#1269281)

A progress indicator has been added to `mkfs.gfs2`

The **`mkfs.gfs2`** tool now reports its progress when building journals and resource groups. As **`mkfs.gfs2`** can take some time to complete with large or slow devices, it was not previously clear if mkfs.gfs2 was working correctly until a report was printed. A progress bar has been added to **`mkfs.gfs2`** indicate progress. (BZ#1196321)

fsck.gfs2 has been enhanced to require considerably less memory on large file systems

Prior to this update, the Global File System 2 (GFS2) file system checker, fsck.gfs2, required a large amount of memory to run on large file systems, and running fsck.gfs2 on file systems larger than 100 TB was therefore impractical. With this update, fsck.gfs2 has been enhanced to run in considerably less memory, which allows for better scalability and makes running fsck.gf2 practical to run on much larger file systems. (BZ#1268045)

GFS2 has been enhanced to allow better scalability of its glocks

In the Global File System 2 (GFS2), opening or creating a large number of files, even if they are closed again, leaves a lot of GFS2 cluster locks (glocks) in slab memory. When the number of glocks was in the millions, GFS2 previously started to slow down, especially with file creates: GFS2 became gradually slower to create files. With this update, the GFS2 has been enhanced to allow better scalability of its glocks, and the GFS2 can now therefore maintain good performance across millions of file creates. (BZ#1172819)

xfsprogs rebased to version 4.5.0

The xfsprogs packages have been upgraded to upstream version 4.5.0, which provides a number of bug fixes and enhancements over the previous version. The Red Hat Enterprise Linux 7.3 kernel RPM requires the upgraded version of xfsprogs because the new default on-disk format requires special handling of log cycle numbers when running the **`xfs_repair`** utility. Notable changes include:

- Metadata cyclic redundancy checks (CRCs) and directory entry file types are now enabled by default. To replicate the older **`mkfs`** on-disk format used in earlier versions of Red Hat Enterprise Linux 7, use the **`-m crc=0 -n ftype=0`** options on the **`mkfs.xfs`** command line.

- The **`GETNEXTQUOTA`** interface is now implemented in **`xfs_quota`**, which allows fast iteration over all on-disk quotas even when the number of entries in the user database is extremely large.

Also, note the following differences between upstream and Red Hat Enterprise Linux 7.3:

- The experimental sparse inode feature is not available.

- The free inode btree (finobt) feature is disabled by default to ensure compatibility with earlier Red Hat Enterprise Linux 7 kernel versions. (BZ#1309498)

The CIFS kernel module rebased to version 6.4

The Common Internet File System (CIFS) has been upgraded to upstream version 6.4, which provides a number of bug fixes and enhancements over the previous version. Notably:

- Support for Kerberos authentication has been added.
- Support for **MFSymlink** has been added.
- The **mknod** and **mkfifo** named pipes are now allowed.

Also, several memory leaks have been identified and fixed. (BZ#1337587)

quota now supports suppressing warnings about NFS mount points with unavailable quota RPC service

If a user listed disk quotas with the **quota** tool, and the local system mounted a network file system with an NFS server that did not provide the **quota** RPC service, the **quota** tool returned the **error while getting quota from server** error message. Now, the **quota** tools can distinguish between unreachable NFS server and a reachable NFS server without the **quota** RPC service, and no error is reported in the second case. (BZ#1155584)

The /proc/ directory now uses the red-black tree implementation to improve the performance

Previously, the **/proc/** directory entries implementation used a single linked list, which slowed down the manipulation of directories with a large number of entries. With this update, the single linked list implementation has been replaced by a red-black tree implementation, which improves the performance of directory entries manipulation. (BZ#1210350)

CHAPTER 10. HARDWARE ENABLEMENT

Support added for the CAPI flash block adapter

The Coherent Accelerator Processor Interface (CAPI) is a technology that enables I/O adapters to coherently access host memory, and thus ensures improved performance. This update adds the **cxlflash** driver, which provides support for IBM's CAPI flash block adapter. (BZ#1182021)

MMC kernel rebased to version 4.5

With this update, the Multimedia Card (MMC) kernel subsystem has been upgraded to upstream version 4.5, which fixes multiple bugs and also enables the Red Hat Enterprise Linux 7 kernel to use the embedded MMC (eMMC) interface version 5.0. In addition, the update improves the suspend and resume functionality of MMC devices, as well as their general stability. (BZ#1297039)

iWarp mapper service added

This update adds support for the internet Wide Area RDMA Protocol (iWARP) mapper to Red Hat Enterprise Linux 7. The iWARP mapper is a user-space service that enables the following iWARP drivers to claim TCP ports using the standard socket interface:

- Intel i40iw
- NES
- Chelsio cxgb4

Note that both the **iw_cm** and **ib_core** kernel modules need to be loaded for the iWarp mapper service (iwpmd) to start successfully. (BZ#1331651)

New package: memkind

This update adds the memkind package, which provides a user-extensible heap manager library, built as an extension of the **jemalloc** memory allocator. This library enables partitioning of the memory heap located between memory types that are defined when the operating system policies are applied to virtual address ranges. In addition, memkind enables the user to control memory partition features and allocate memory with a specified set of memory features selected. (BZ#1210910)

Per-port MSI-X support for the AHCI driver

The driver for the Advanced Host Controlled Interface (AHCI) has been updated for per-port message-signaled interrupt (MSI-X) vectors. Note that this applies only to controllers that support the feature. (BZ#1286946)

Runtime Instrumentation for IBM z Systems is now fully supported

The Runtime Instrumentation feature, previously available as a Technology Preview, is now fully supported in Red Hat Enterprise Linux 7 on IBM z Systems. Runtime Instrumentation enables advanced analysis and execution for a number of user-space applications available with the IBM zEnterprise EC12 system. (BZ#1115947)

CHAPTER 11. INSTALLATION AND BOOTING

Improved logging when network traffic is blocked during installation

This update adds improved logging when attempting to connect to a network repository during installation. Now, when there is a connection problem with a network repository during installation, logs include more detailed information about what caused the problem. (BZ#1240379)

Support for Memory Address Range Mirroring

With this update, it is possible to configure Memory Address Range Mirroring on EFI-based systems on compatible hardware, using the **`efibootmgr`** utility with the new **`--mirror-below-4G`** and **`--mirror-above-4G`** options. (BZ#1271412)

Default logging levels increased in `Yum` and `NetworkManager`

With this update, default logging levels were increased in the **`Yum`** and **`NetworkManager`** utilities. (BZ#1254368)

Driver Update Disks can now replace loaded modules

It is now possible to use a Driver Update Disk to replace a module that is already loaded, provided that the original module is not in use. (BZ#1101653)

CHAPTER 12. KERNEL

The protobuf-c packages are now available for the little-endian variant of IBM Power Systems architecture

This update adds the protobuf-c packages for the little-endian variant of IBM Power Systems architecture. The protobuf-c packages provide C bindings for Google's Protocol Buffer and are a prerequisite for the criu packages on the above mentioned architecture. The criu packages provide the Checkpoint/Restore in User space (CRIU) function, which provides the possibility to checkpoint and restore processes or groups of processes. (BZ#1289666)

The CAN protocol has been enabled in the kernel

The Controller Area Network (CAN) protocol kernel modules have been enabled, providing the device interface for CAN device drivers. CAN is a vehicle bus specification originally intended to connect the various micro-controllers in automobiles and has since extended to other areas. CAN is also used in industrial and machine controls where a high performance interface is required and other interfaces such as RS-485 are not sufficient. The functions exported from the CAN protocol modules are used by CAN device drivers to make the kernel aware of the devices and to allow applications to connect and transfer data. Enablement of CAN in the kernel allows the use of third party CAN drivers and applications to implement CAN based systems. (BZ#1311631)

Persistent memory support added to `kexec-tools`

The Linux kernel now supports E820_PRAM and E820_PMEM type for the Non-Volatile Dual In-line Memory Module (NVDIMM) memory devices. A patch has been backported from the upstream, which ensures that **`kexec-tools`** support these memory devices as well. (BZ#1282554)

`libndctl` - userspace `nvdimm` management library

The **`libndctl`** userspace library has been added. It is a collection of C interfaces to the **`ioctl`** and **`sysfs`** entry points provided by the kernel **`libnvdimm`** subsystem. The library enables higher level management software for NVDIMM-enabled platforms and also provides a command-line interface for managing NVDIMMs. (BZ#1271425)

New symbols for the kABI whitelist to support the hpvsa and hpdsa drivers

This update adds a set of symbols to the kernel Application Binary Interface (kABI) whitelist, which ensures the support for the hpvsa and hpdsa drivers.

The newly added symbols are:

- scsi_add_device
- scsi_adjust_queue_depth
- scsi_cmd_get_serial
- scsi_dma_map
- scsi_dma_unmap
- scsi_scan_host (BZ#1274471)

crash rebased to version 7.1.5

The crash packages have been upgraded to upstream version 7.1.5, which provides several bug fixes and a number of enhancements over the previous version. Notably, this rebase adds new options such as **`dis -s`**, **`dis -f`**, **`sys -i`**, **`list -l`**, new support for Quick Emulator (QEMU) generated

Executable and Linkable Format (ELF) vmcores on the 64-bit ARM architectures, and several updates required for support of recent upstream kernels. It is safer and more efficient to rebase the **crash** packages than to backport selectively the individual patches. (BZ#1292566)

New package: crash-ptdump-command

Crash-ptdump-command is a new rpm package which provides a crash extension module to add ptdump subcommand to the crash utility. The ptdump subcommand retrieves and decodes the log buffer generated by the Intel Processor Trace facility from the vmcore file and outputs to the files. This new package is designed for EM64T and AMD64 architectures. (BZ#1298172)

Ambient capabilities are now supported

Capabilities are per-thread attributes used by the Linux kernel to divide the privileges traditionally associated with superuser privileges into multiple distinct units. This update adds support for ambient capabilities to the kernel. Ambient capabilities are a set of capabilities that are preserved when a program is executed using the **execve()** system call. Only capabilities which are permitted and inheritable can be ambient. You can use the **prctl()** call to modify ambient capabilities. See the **capabilities(7)** man page for more information about kernel capabilities in general, and the **prctl(2)** man page for information about the **prctl** call. (BZ#1165316)

`cpuid` is now available

With this update, the **cpuid** utility is available in Red Hat Enterprise Linux. This utility dumps detailed information about the CPU(s) gathered from the CPUID instruction, and also determines the exact model of CPU(s). It supports Intel, AMD, and VIA CPUs. (BZ#1307043)

FC-FCoE symbols have been added to KABI white lists

With this update, a list of symbols belonging to the **libfc** and **libfcoe** kernel modules has been added to the kernel Application Binary Interface (KABI) white lists. This ensures that the Fibre Channel over Ethernet (FCoE) driver, which depends on **libfc** and **libfcoe**, can safely use the newly added symbols. (BZ#1232050)

New package: opal-prd for OpenPower systems

The new opal-prd package contains a daemon that handles hardware-specific recovery processes, and should be run as a background system process after boot. It interacts with OPAL firmware to capture hardware error causes, log events to the management processor, and handles recoverable errors where suitable. (BZ#1224121)

New package: libcxl

The new libcxl package contains the user-space library for applications in user space to access CAPI hardware via kernel **cxl** functions. It is available on IBM Power Systems and the little-endian variant of IBM Power Systems architecture. (BZ#1305080)

Kernel support for the newly added `iproute` commands

This update adds kernel support to ensure the correct functionality of newly added **iproute** commands. The provided patch set includes:

- Extension of the IPsec interface, which allows prefixed policies to be hashed.
- Inclusion of the hash prefixed policies based on preflen thresholds.
- Configuration of policy hash table thresholds by netlink. (BZ#1222936)

Backport of the `PID` cgroup controller

This update adds the new Process Identifier (PID) controller. This controller accounts for the processes per cgroup and allows a cgroup hierarchy to stop any new tasks from being forked or cloned after a certain limit is reached. (BZ#1265339)

mpt2sas and mpt3sas merged

The source codes of **mpt2sas** and **mpt3sas** drivers have been merged. Unlike in upstream, Red Hat Enterprise Linux 7 continues to maintain two binary drivers for compatibility reasons. (BZ#1262031)

Allow multiple .ko files to be specified in ksc

Previously, it was not possible to add multiple .ko files in a single run of the ksc utility. Consequently, the drivers that contain multiple kernel modules were not passed to ksc in a single run. With this update, the -k option can be specified multiple times in the same run. Thus single run of ksc can be used to query symbols used by several kernel modules. As a result, one file with symbols used by all modules is generated. (BZ#906659)

dracut update

The **dracut** initramfs generator has been updated with a number of bug fixes and enhancements over the previous version. Notably:

- **dracut** gained a new kernel command-line option **rd.emergency=[reboot|poweroff|halt]**, which specifies what action to execute in case of a critical failure. When using **rd.emergency=[reboot|poweroff|halt]**, the **rd.shell=0** option should also be specified.
- The **reboot**, **poweroff**, and **halt** commands now work in the emergency shell of **dracut**.
- **dracut** now supports multiple bond, bridge, and VLAN configurations on the kernel command line.
- The device timeout can now be specified on the kernel command line using the **rd.device.timeout=<seconds>** option.
- DNS name servers specified on the kernel command line are now used in DHCP.
- **dracut** now supports 20-byte MAC addresses.
- Maximum Transmission Unit (MTU) and MAC addresses are now set correctly for DHCP and IPv6 Stateless Address AutoConfiguration (SLAAC).
- The **ip=** kernel command line option now supports MAC addresses in brackets.
- **dracut** now supports the NFS over RDMA (NFSoRDMA) module.
- Support for **kdump** has been added to Fibre Channel over Ethernet (FCoE) devices. The configuration of FCoE devices is compiled in **kdump initramfs**. Kernel crash dumps can now be saved to FCoE devices.
- **dracut** now supports the **--install-optional <file list>** option and the **install_optional_items+= <file>[<file> ...]** configuration file directive. If you use the new option or directive, the files are installed if they exist, and no error is returned if they do not exist.
- **dracut** DHCP now recognizes the **rfc3442-classless-static-routes** option, which enables using classless network addresses. (BZ#1359144, BZ#1178497, BZ#1324454, BZ#1194604, BZ#1282679, BZ#1282680, BZ#1332412, BZ#1319270, BZ#1271656, BZ#1271656, BZ#1367374, BZ#1169672, BZ#1222529, BZ#1260955)

Support for Wacom Cintiq 27 QHD

The Wacom Cintiq 27 QHD tablets are now supported in Red Hat Enterprise Linux 7. (BZ#1342989)

Full support for Intel® Omni-Path Architecture (OPA) kernel driver

Intel® Omni-Path Architecture (OPA) kernel driver, previously available as a Technology Preview, is now fully supported. Intel® OPA provides Host Fabric Interconnect (HFI) hardware with initialization and setup for high performance data transfers (high bandwidth, high message rate, low latency) between compute and I/O nodes in a clustered environment.

For instructions on how to obtain Intel® Omni-Path Architecture documentation, see https://access.redhat.com/articles/2039623. (BZ#1374826)

Cyclitest `--smi` option available for non-root users

With this update, it is possible to use the cyclictest program with the **`--smi`** option as a non-root user, provided that the user also belongs to the **`realtime`** group. On processors that support system management interrupts (SMIs), **`--smi`** displays a report on the system's SMIs, which was previously only available for root users. (BZ#1346771)

Support added for the new Smart Array storage adapters

In Red Hat Enterprise Linux 7.2 and older versions, the new Smart Array storage adapters were not officially supported. However, these adapters were detected by the **`aacraid`** driver and the system appeared to work correctly. With this update, the new Smart Array storage adapters are properly supported by the new **`smartpqi`** driver. Note that when you update, the driver name for these adapters will change. (BZ#1273115)

The Linux kernel now supports trusted virtual function (VF) concept

The upstream code has been backported into the Linux kernel to provide support for trusted virtual function (VF) concept. As a result, the trusted VFs are now permitted to enable multicast promiscuous mode which allows them to have more than 30 IPv6 addresses assigned. The trusted VFs are also permitted to overwrite media access control (MAC) addresses. (BZ#1302101)

Seccomp mode 2 is now supported on IBM Power Systems

This update adds support for seccomp mode 2 on IBM Power Systems. Seccomp mode 2 involves the parsing of Berkeley Packet Filter (BPF) configuration files to define system call filtering. This mode provides notable security enhancements, which are essential for the adoption of containers in Linux on IBM Power Systems. (BZ#1186835)

Memory Bandwidth Monitoring has been added

This update adds Memory Bandwidth Monitoring (MBM) into the Linux kernel. MBM is a CPU feature included in the family of platform quality of service (QoS) feature that is used to track memory bandwidth usage for a specific task, or group of tasks, associated with an Resource Monitoring ID (RMID). (BZ#1084618)

`brcmfmac` now supports Broadcom wireless cards

The **`brcmfmac`** kernel driver has been updated to support Broadcom BCM4350 and BCM43602 wireless cards. (BZ#1298446)

The `autojoin` option has been added to the `ip addr` command to allow multicast group join or leave

Previously, there was no method to indicate Internet Group Management Protocol (IGMP) membership to Ethernet switches that do multicast pruning. Consequently, those switches did not replicate packets to the host's port. With this update, the **`ip addr`** command has been extended with the **`autojoin`** option, which enables a host to join or leave a multicast group. (BZ#1267398)

Open vSwitch now supports NAT

This update adds Network Address Translation (NAT) support to the Open vSwitch kernel module. (BZ#1297465)

The page tables are now initialized in parallel

Previously, the page tables were initiallized serially on Non-Uniform Memory Access (NUMA) systems, based on Intel EM64T, Intel 64, and AMD64 architectures. Consequently, large servers could perform slowly at boot time. With this update, a set of patches has been backported to ensure that memory initialization is mostly done in parallel by node-local CPUs as a part of node activation. As a result, systems with the memory of 16TB to 32TB now boot about two times faster compared to the previous version. (BZ#727269)

The Linux kernel now supports Intel MPX

This update adds the support of Intel Memory Protection Extensions (MPX) into the Linux kernel. Intel MPX is a set of extensions to the Intel 64 architectures. Intel MPX together with a compiler, runtime library and operating system support increase the robustness and security of software by checking pointer references whose compile-time normal intentions can be maliciously exploited due to buffer overflows. (BZ#1138650)

`ftrace` now prints command names as expected

When the trylock() function did not successfully acquire a lock, saving a command name in the **`ftrace`** kernel tracer failed. As a consequence, **`ftrace`** did not properly print command names in the **`/sys/kernel/debug/tracing`** file. With this update, recording of the command names has been fixed, and **`ftrace`** now prints command names as expected. Users are also now able to set the number of stored commands by setting the **`saved_cmdlines_size`** kernel configuration parameter. (BZ#1117093)

The shared memory that was swapped out is now visible in `/proc/<pid>/smaps`

Prior to this update, swapped-out shared memory appeared neither in the /proc/<pid>/status file, nor in the /proc/<pid>/smaps file. This update adds per-process accounting of swapped-out shared memory, including **`sysV shm`**, shared anonymous mapping and mapping to a **`tmpfs`** file. Swapped-out shared memory now appears in **`/proc/<pid>/smaps`**. However, swapped-out shared memory is not reflected in **`/proc/<pid>/status`**, and swapped-out **`shmem`** pages therefore remain invisible in certain tools such as **`procps`**. (BZ#838926)

Kernel UEFI support update

The Unified Extensible Firmware Interface (UEFI) support in the kernel has been updated with a set of selected patches from the upstream kernel. This set provides a number of bug fixes and enhancements over the previous version. (BZ#1310154)

Mouse controller now works on guests with Secure Boot

Red Hat Enterprise Linux now supports a mouse controller on guest virtual machines that have the Secure Boot feature enabled. This ensures mouse functionality on Red Hat Enterprise Linux guests running on hypervisors that enable secure boot by default. (BZ#1331578)

The RealTek RTS520 card reader is now supported

This update adds support for the RealTek RTS520 card reader. (BZ#1280133)

Tunnel devices now support lockless `xmit`

Previously, tunnel devices, which used the **`pfifo_fast`** queue discipline by default, required the serialization lock for the **`tx`** path. With this update, per-CPU variables are used for statistic accounting, and a serialization lock on the **`tx`** path is not required. As a result, the user space is now allowed to configure a **`noqueue`** queue discipline with no lock required on the **`xmit`** path, which significantly improves tunnel device **`xmit`** performance. (BZ#1328874)

Update of Chelsio drivers

Chelsio NIC, iWARP, vNIC and iSCSI drivers have been updated to their most recent versions, which add several bug fixes and enhancements over the previous versions.

The most notable enhancements include:

- **ethtool** support to get adapter statistics
- **ethtool** support to dump channel statistics
- **ethtool** to dump loopback port statistics
- **debugfs** entry to dump CIM MA logic analyzer logs
- **debugfs** entry to dump CIM PIF logic analyzer contents
- **debugfs** entry to dump channel rate
- **debugfs** entry to enable backdoor access
- **debugfs** support to dump meminfo
- MPS tracing support
- hardware time stamp support for RX
- device IDs for T6 adapters (BZ#1275829)

Support for 25G, 50G and 100G speed modes for Chelsio drivers

With this update, a set of patches has been backported into the Linux kernel that add definitions for 25G, 50G and 100G speed modes for Chelsio drivers. This patch set also adds the link mode mask API to the **cxgb4** and **cxgb4vf** drivers. (BZ#1365689)

mlx5 now supports NFSoRDMA

With this update, the **mlx5** driver supports export of Network File System over Remote Direct Memory Access (NFSoRDMA). As a result, customers can now mount NFS shares over RDMA and perform the following actions from the client computer:

- list files on the NFS share using the **ls** command
- use the **touch** command on new files

This feature allows some jobs to run from a shared storage, which is useful when you have large, InfiniBand-connected grids running that keep growing in size. (BZ#1262728)

I2C has been enabled on 6th Generation Intel Core Processors

Starting from this update, the I2C devices that are controlled by a kernel driver are supported on 6th Generation Intel Core Processors. (BZ#1331018)

mlx4 and mlx5 now support RoCE

This update adds the support of Remote Direct Memory Access Over Converged Ethernet (RoCE) network protocol timespanning to the **mlx4** and **mlx5** drivers. RoCE is a mechanism to provide efficient server-to-server data transfer through Remote Direct Memory Access (RDMA) with very low latencies on lossless Ethernet networks. RoCE encapsulates InfiniBand (IB) transport in one of two Ethernet packets: - RoCEv1 - dedicated ether type (0x8915) - RoCEv2 - User Datagram Protocol (UDP) and dedicated UDP port (4791).

Both RoCE versions are now supported for **mlx4** and **mlx5**. Starting from this update, **mlx4** supports RoCE Virtual function Link Aggregation protocol, which provides failover and link aggregation capabilities to **mlx4** device physical ports. Only IB port that represents the two physical ports is exposed to the

application layer. (BZ#1275423, BZ#1275187, BZ#1275209) (BZ#1275423)

Support of cross-channel synchronization

Starting from this update, the Linux kernel supports cross-channel synchronization on AMD64 and Intel 64, IBM Power Systems and 64-bit ARM architectures. Devices now have capability to synchronize or serialize execution of I/O operations on different work queues without any intervention from the host software. (BZ#1275711)

Support for SGI UV4 has been added into the Linux kernel

Starting from this update, the Linux kernel supports the SGI UV4 platform. (BZ#1276458)

Updated support of TPM 2.0.

Support of Trusted Platform Module (TPM) of the version 2.0 has been updated in the Linux kernel. (BZ#1273499)

Support of 12 TB of RAM

With this update, the kernel is certified to support 12 TB of RAM. This new feature covers the advance in memory technology and it provides the potential to meet technological requirements of future servers that will be released in the life time of Red Hat Enterprise Linux 7. This feature is available for AMD64 and Intel 64 architectures. (BZ#797488)

Full support for 10GbE RoCE Express feature for RDMA

With Red Hat Enterprise Linux 7.3, the 10GbE RDMA over Converged Ethernet (RoCE) Express feature becomes fully supported. This makes it possible to use Ethernet and Remote Direct Memory Access (RDMA), as well as the Direct Access Programming Library (DAPL) and OpenFabrics Enterprise Distribution (OFED) APIs, on IBM z Systems.

Before using this feature on an IBM z13 system, ensure that the minimum required service is applied: z/VM APAR UM34525 and HW ycode N98778.057 (bundle 14). (BZ#1289933)

zEDC compression fully supported on IBM z Systems

Red Hat Enterprise Linux 7.3 and later provide full support for the Generic Workqueue (GenWQE) engine device driver. The initial task of the driver is to perform zlib-style compression and decompression of the RFC1950, RFC1951 and RFC1952 formats, but it can be adjusted to accelerate a variety of other tasks. (BZ#1289929)

LPAR Watchdog for IBM z Systems

The enhanced watchdog driver for IBM z Systems has become fully supported. This driver supports Linux logical partitions (LPAR), as well as Linux guests in the z/VM hypervisor, and provides automatic reboot and automatic dump capabilities if a Linux system becomes unresponsive. (BZ#1278794)

CHAPTER 13. REAL-TIME KERNEL

About Red Hat Enterprise Linux for Real Time Kernel

The Red Hat Enterprise Linux for Real Time Kernel is designed to enable fine-tuning for systems with extremely high determinism requirements. The major increase in the consistency of results can, and should, be achieved by tuning the standard kernel. The real-time kernel enables gaining a small increase on top of increase achieved by tuning the standard kernel.

The real-time kernel is available in the **rhel-7-server-rt-rpms** repository. The Installation Guide contains the installation instructions and the rest of the documentation is available at Product Documentation for Red Hat Enterprise Linux for Real Time.

The can-dev module has been enabled for the real-time kernel

The **can-dev** module has been enabled for the real-time kernel, providing the device interface for Controller Area Network (CAN) device drivers. CAN is a vehicle bus specification originally intended to connect the various micro-controllers in automobiles and has since extended to other areas. CAN is also used in industrial and machine controls where a high performance interface is required and other interfaces such as RS-485 are not sufficient.

The functions exported from the **can-dev** module are used by CAN device drivers to make the kernel aware of the devices and to allow applications to connect and transfer data.

Enabling CAN in the real-time kernel allows the use of third party CAN drivers and applications to implement CAN-based systems. (BZ#1328607)

CHAPTER 14. NETWORKING

Support for latest Bluetooth, including Bluetooth LE

This update provides latest Bluetooth support, including support for connecting to Bluetooth Low Energy (LE) devices. This helps to ensure proper functionality of Internet of Things (IoT) devices. (BZ#1296707)

Open vSwitch now uses kernel lightweight tunnel support

With this update, the Open vSwitch (OVS) implementation now uses kernel lightweight tunnel support for VXLAN, GRE, and GENEVE tunnels. This allows you to eliminate duplicate functionality in the OVS **`vport`** implementation and also brings OVS benefits from feature and performance improvements in the base kernel, such as destination caching support or hardware off-loading. (BZ#1283886)

Bulking in the memory allocator subsystem is now supported

With this update, the kernel supports batching of memory allocation and memory freeing. Currently, this performance optimization is used only in the networking stack to free consecutive network packets. (BZ#1268334)

NetworkManager now supports LLDP

With this update, NetworkManager can now listen for Link Layer Discovery Protocol (LLDP) messages on given interfaces and expose information about found neighboring nodes through D-bus and nmcli. This feature is disabled by default, but you can enable it through the **`connection.lldp`** property or the **`LLDP`** variable in the **`ifcfg`** files. (BZ#1142898)

DHCP timeout in NetworkManager is configurable

The faster fallback in a Dynamic Host Configuration Protocol (DHCP) negotiation is useful in case a server is not present. With this update, the user can set the value of the **`ipv4.dhcp-timeout`** property or the **`IPV4_DHCP_TIMEOUT`** option in the **`ifcfg`** files. As a result, NetworkManager waits for a response from the DHCP server only for a given time. (BZ#1262922)

NetworkManager now detects duplicate IPv4 addresses

With this update, NetworkManager performs a check to detect duplicate IPv4 addresses when activating a new connection. If the address in LAN is already assigned, the connection activation fails. This feature is disabled by default, but you can enable it by the **`ipv4.dad-timeout`** property or the **`ARPING_WAIT`** variable in the **`ifcfg`** files. (BZ#1259063)

NetworkManager now controls the host name using `systemd-hostnamed`

With this update, NetworkManager uses the **`systemd-hostnamed`** service to read and write the static host name, which is stored in the **`/etc/hostname`** file. Due to this change, manual modifications done to the **`/etc/hostname`** file are no longer picked up automatically by NetworkManager; users should change the system host name through the **`hostnamectl`** utility. Also, the use of the **`HOSTNAME`** variable in the **`/etc/sysconfig/network`** file is now deprecated. (BZ#1367916)

`NetworkManager` now uses a randomized MAC address during wireless network scanning

During wireless network scanning, **`NetworkManager`** now uses a randomized MAC address for privacy by default. This can be explicitly disabled in configuration. (BZ#1388471)

`bridge_netfilter` rebased to version 4.4

The **`bridge_netfilter`** subsystem has been upgraded to upstream version 4.4, which provides a number of bug fixes and enhancements over the previous version. Most notably, the bridge forwarding performance is significantly improved, the bridge_netfilter hooks are now not registered by default, and functional issues in the fragments forwarding are fixed. (BZ#1265259)

libnl3 rebased to version 3.2.28

The libnl3 packages have been upgraded to version 3.2.28, which provides a number of bug fixes and enhancements. Among others:

- Library symbol versioning has been added
- Suport for new kernel features and device types has been added
- A new **libnl-xfrm-3** library is now included
- This version provides a resynchronisation with upstream (BZ#1296058)

Additional policies for the PR-SCTP extension are now supported

The Partially Reliable SCTP (PR-SCTP) extension defined in RFC3758 provides a generic method for senders to abandon user messages. With this update, three additional **PR-SCTP** policies are supported:

- Timed Reliability: This allows the sender to specify a timeout for a user message. The SCTP stack abandons the user message after the timeout expires.
- Limited Retransmission Policy: Allows limitation of the number of retransmissions.
- Priority Policy: Allows removal of lower-priority messages if space for higher-priority messages is needed in the send buffer. (BZ#965453)

Man pages for tc filter actions were added to the iproute package

With this update, man pages for the **iproute** utility's **tc** filter actions have been added. Every **tc** action has now a corresponding man page, which includes synopsis, options, and detailed functional description. (BZ#1275426)

The iproute utility can now prevent the physical interface used with MACVLAN from entering promiscuous mode by default

The new **MACVLAN_FLAG_NOPROMISC** flag allows the user to control entering physical interfaces in promiscuous mode by default after creating and setting up pass-through mode. This feature is useful in cases where all end stations' MAC addresses are known and the user wants to avoid the overhead of processing every packet the interface receives. (BZ#1013584)

New IFA_F_NOPREFIXROUTE flag to prevent automatic route creation

Previously, the user can not explicitly select the preferred interface when multiple ones belong to the same local network. With this update, the **IFA_F_NOPREFIXROUTE** netlink flag allows preventing automatic route creation when adding a new IPv4 address to a network interface. (BZ#1221311)

The ip command can now display bridge configuration

With this update, you can use the **ip** tool instead of the **brctl** tool to display network bridge configuration. (BZ#1270763)

ss now supports monitoring per connection TCP re-transmission

With this update, the **ss** command output includes the **bytes_acked**, **bytes_received**, **segs_in**, and **segs_out** fields, unless they are null. This feature improves link quality monitoring. (BZ#1269051)

iPXE packages rebased to support IPv6 on physical computers

The ipxe-bootimgs and ipxe-roms packages have been rebased to upstream commit 6366fa7a to support network booting over IPv6 on physical installations of Red Hat Enterprise Linux 7. (BZ#1298313)

New packages: libvma

libvma is a dynamically linked user space library for transparently enhancing the performance of **TCP** and **UDP** networking-heavy applications over Remote Direct Memory Access (RDMA)-capable network interface controllers. It allows standard socket API applications to run with the full network stack bypass from user space, which results in latency reduction, increased throughput, and increased packet rate.

libvma is currently limited to Mellanox ConnectX-3 Infiniband and Ethernet ports and Mellanox ConnectX-4 Ethernet ports. Mellanox ConnectX-4 Infiniband ports are not supported. (BZ#1271624)

A new `--unix-socket` option in `curl`

The **curl** utility is now able to connect through a Unix domain socket instead of using TCP/IP if the new **--unix-socket** option is specified. This feature is used by Docker REST API for monitoring. (BZ#1263318)

Kernel support for the newly added iproute commands

This updated version of Red Hat Enterprise Linux 7 adds kernel support to reach the right functionality of newly added iproute commands. The provided patchset includes: -extension of the IPsec interface which allows prefixed policies to be hashed -inclusion of the hash prefixed policies based on preflen thresholds -configuration of policy hash table thresholds by netlink (BZ#1212026)

CHAPTER 15. SECURITY

The SELinux user space packages rebased to version 2.5

The SELinux user space packages have been upgraded to upstream version 2.5, which provides a number of enhancements, bug fixes, and performance improvements over the previous version. The most important new features in the SELinux userspace 2.5 include:

- The new SELinux module store supports priorities. The priority concept provides an ability to override a system module with a module of a higher priority.
- SELinux Common Intermediate Language (CIL) provides clear and simple syntax that is easy to read, parse, and to generate by high-level compilers, analysis tools, and policy generation tools.
- Time-consuming SELinux operations, such as policy installations or loading new policy modules, are now significantly faster.

Note: The default location of the SELinux modules remains in the **`/etc/selinux/`** directory in Red Hat Enterprise Linux 7, whereas the upstream version uses **`/var/lib/selinux/`**. To change this location for migration, set the **`store-root=`** option in the **`/etc/selinux/semanage.conf`** file. (BZ#1297815)

scap-workbench rebased to version 1.1.2

The scap-workbench package has been rebased to version 1.1.2, which provides a new SCAP Security Guide integration dialog. The dialog helps the administrator choose a product that needs to be scanned instead of choosing content files. The new version also offers a number of performance and user-experience improvements, including improved rule-searching in the tailoring window, the possibility to fetch remote resources in SCAP content using the GUI, and the dry-run feature. The dry-run feature enables to user to get oscap command-line arguments to the diagnostics window instead of running the scan. (BZ#1202854)

openscap rebased to version 1.2.10

The OpenSCAP suite that enables integration of the Security Content Automation Protocol (SCAP) line of standards has been rebased to version 1.2.10, the latest upstream version. The openscap packages provide the OpenSCAP library and the **`oscap`** utility. Most notably, this update adds support for scanning containers using the **`atomic scan`** command. In addition, this update provides the following enhancements:

- **`oscap-vm`**, a tool for offline scanning of virtual machines
- **`oscap-chroot`**, a tool for offline scanning of file systems mounted at arbitrary paths
- Full support for Open Vulnerability and Assessment Language (OVAL) 5.11.1
- Native support for remote .xml.bz2 files
- Grouping HTML report results according to various criteria
- HTML report improvements
- Verbose mode for debugging OVAL evaluation (BZ#1278147)

firewalld rebased to version 0.4.3.2

The firewalld packages have been upgraded to upstream version 0.4.3.2 which provides a number of enhancements and bug fixes over the previous version. Notable changes include the following:

- Performance improvements: **`firewalld`** starts and restarts significantly faster thanks to the new transaction model which groups together rules that are applied simultaneously. This model

uses the **iptables** restore commands. Also, the **firewall-cmd**, **firewall-offline-cmd**, **firewall-config**, and **firewall-applet** tools have been improved with performance in mind.

- The improved management of connections, interfaces and sources: The user can now control zone settings for connections in **NetworkManager**. In addition, zone settings for interfaces are also controlled by **firewalld** and in the **ifcfg** file.
- Default logging option: With the new **LogDenied** setting, the user can easily debug and log denied packets.
- **ipset** support: **firewalld** now supports several IP sets as zone sources, within rich and direct rules. Note that in Red Hat Enterprise Linux 7.3, **firewalld** supports only the following **ipset** types:
  - hash:net
  - hash:ip (BZ#1302802)

audit rebased to version 2.6.5

The audit packages contain the user space utilities for storing and searching the audit records which have been generated by the audit subsystem in the Linux kernel. The audit packages have been upgraded to upstream version 2.6.5, which provides a number of enhancements and bug fixes over the previous version. Notable changes include the following:

- The **audit** daemon now includes a new flush technique called **incremental_async**, which improves its performance approximately 90 times.
- The **audit** system now has many more rules that can be composed into an **audit** policy. Some of these new rules include support for the Security Technical Implementation Guide (STIG), PCI Data Security Standard, and other capabilities such as auditing the occurrence of 32-bit syscalls, significant power usage, or module loading.
- The **auditd.conf** configuration file and the **auditctl** command now support many new options.
- The **audit** system now supports a new log format called **enriched**, which resolves UID, GID, syscall, architecture, and network addresses. This will aid in log analysis on a machine that differs from where the log was generated. (BZ#1296204)

MACsec (IEEE 802.1AE) is now supported

With this update, the Media Access Control Security (MACsec) encryption over Ethernet is supported. MACsec encrypts and authenticates all traffic in LANs with the GCM-AES-128 algorithm. (BZ#1104151)

The rsyslog RELP module now binds to a specific rule set

With this update, the rsyslog Reliable Event-Logging Protocol (RELP) module is now capable of binding to specific rule set with each input instance. The **input()** instance rule set has higher priority than the **module()** rule set. (BZ#1223566)

rsyslog imfile module now supports a wildcard file name

The rsyslog packages provide an enhanced, multi-threaded syslog daemon. With this update, the rsyslog imfile module supports using wildcards inside file names and adding the actual file name to the message's metadata. This is useful, when rsyslog needs to read logs under a directory and does not know the names of files in advance. (BZ#1303617)

Syscalls in `audit.log` are now converted to text

With this update, **auditd** converts system call numbers to their names prior to forwarding them to syslog daemon through the **audispd** event multiplexor. (BZ#1127343)

audit subsystem can now filter by process name

The user can now audit by executable name (with the **-F exe=<path-to-executable>** option), which allows expression of many new audit rules. You can use this functionality to detect events such as the bash shell opening a network connection. (BZ#1135562)

mod_security_crs rebased to version 2.2.9

The mod_security_crs package has been upgraded to upstream version 2.2.9, which provides a number of bug fixes and enhancements over the previous version. Notable changes include:

- A new PHP rule (958977) to detect PHP exploits.
- A **JS overrides** file to identify successful XSS probes.
- New XSS detection rules.
- Fixed session-hijacking rules. (BZ#1150614)

opencryptoki rebased to version 3.5

The opencryptoki packages have been upgraded to version 3.5, which provides a number of bug fixes and enhancements over the previous version.

Notable changes include:

- The **openCryptoki** service automatically creates **lock/** and **log/** directories, if not present.
- The **PKCS#11** API supports hash-based message authentication code (HMAC) with SHA hashes in all tokens.
- The **openCryptoki** library provides dynamic tracing set by the **OPENCRYPTOKI_TRACE_LEVEL** environment variable. (BZ#1185421)

gnutls now uses the central certificate store

The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic algorithms and protocols such as SSL, TLS, and DTLS. With this update, GnuTLS uses the central certificate store of Red Hat Enterprise Linux through the p11-kit packages. Certificate Authority (CA) updates, as well as certificate black lists, are now visible to applications at runtime. (BZ#1110750)

The `firewall-cmd` command can now provide additional details

With this update, firewalld shows details of a service, zone, and **ICMP** type. Additionally, the user can list the full path to the source XML file. The new options for **firewall-cmd** are:

- [--permanent] --info-zone=zone
- [--permanent] --info-service=service
- [--permanent] --info-icmptype=icmptype (BZ#1147500)

`pam_faillock` can be now configured with `unlock_time=never`

The **pam_faillock** module now allows specifying using the **unlock_time=never** option that the user authentication lock caused by multiple authentication failures should never expire. (BZ#1273373)

libica rebased to version 2.6.2

The libica packages have been updated to upstream version 2.6.2, which provides a number of bug fixes and enhancements over the previous version. Notably, this update adds support for generation of pseudo random numbers, including enhanced support for Deterministic Random Bit Generator (DRBG), according to updated security specification NIST SP 800-90A. (BZ#1274390)

New `lastlog` options

The **`lastlog`** utility now has the new **`--clear`** and **`--set`** options, which allow the system administrator to reset a user's lastlog entry to the **`never logged in`** value or to the current time. This means you can now re-enable user accounts previously locked due to inactivity. (BZ#1114081)

libreswan rebased to version 3.15

`Libreswan` is an implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) for Linux. The libreswan packages have been upgraded to upstream version 3.15, which provides a number of enhancements and bug fixes over the previous version. Notable changes include the following:

- The nonce size is increased to meet the RFC requirements when using the SHA2 algorithms.
- **`Libreswan`** now calls the **`NetworkManager`** helper in case of a connection error.
- All **`CRLdistributionpoints`** in a certificate are now processed.
- **`Libreswan`** no longer tries to delete non-existing IPsec Security Associations (SAs).
- The **`pluto`** IKE daemon now has the **`CAP_DAC_READ_SEARCH`** capability.
- **`pluto`** no longer crashes when on-demand tunnels are used.
- **`pam_acct_mgmt`** is now properly set.
- The regression was fixed so tunnels with **`keyingtries=0`** try to establish the tunnel indefinitely.
- The delay before re-establishing the deleted tunnel that is configured to remain up is now less than one second. (BZ#1389316)

The SHA-3 implementation in nettle now conforms to FIPS 202

nettle is a cryptographic library that is designed to fit easily in almost any context. With this update, the Secure Hash Algorithm 3 (SHA-3) implementation has been updated to conform the final Federal Information Processing Standard (FIPS) 202 draft. (BZ#1252936)

scap-security-guide rebased to version 0.1.30

The scap-security-guide project provides a guide for configuration of the system from the final system's security point of view. The package has been upgraded to version 0.1.30. Notable improvements include:

- The NIST Committee on National Security Systems (CNSS) Instruction No. 1253 profile is now included and updated for Red Hat Enterprise Linux 7.
- The U.S. Government Commercial Cloud Services (C2S) profile inspired by the Center for Internet Security (CIS) benchmark is now provided.
- The **`remediation`** scripts are now included in benchmarks directly, and the external shell library is no longer necessary.

- The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) profile for Red Hat Enterprise Linux 7 has been updated to be equal to the DISA STIG profile for Red Hat Enterprise Linux 6.

- The draft of the Criminal Justice Information Services (CJIS) Security Policy profile is now available for Red Hat Enterprise Linux 7. (BZ#1390661)

CHAPTER 16. SERVERS AND SERVICES

squid rebased to version 3.5.20

Squid is a fully-featured HTTP proxy, which offers a rich access control, authorization and logging environment to develop web proxy and content serving applications. The squid packages have been upgraded to version 3.5.20. The most notable changes include:

- Support for **libecap** version 1.0
- Authentication helper query extensions
- Support for named services
- Upgraded the **squidclient** utility
- Helper support for concurrency channels
- Native FTP Relay
- Receive PROXY protocol, versions 1 and 2
- SSL server certificate validator
- Note directive for annotating transactions
- TPROXY support for BSD systems
- **spoof_client_ip** directive for managing TPROXY spoofing
- Various Access Control updates
- Support for the OK, ERR, and BH response codes and the **kv-pair** options from any helper
- Improved pipeline queue configuration.
- Multicast DNS

IMPORTANT: Note that when updating squid, certain configuration directives will be changed to their more recent versions. These modifications are backward-compatible, but if you want to prevent unexpected configuration changes, you can use the squid-migration-script package to preview the results of updating your squid configuration. For further information, see https://access.redhat.com/solutions/2678941 . (BZ#1273942)

PHP cURL module now supports TLS 1.1 and TLS 1.2

Support for the TLS protocol version 1.1 and 1.2, which was previously made available in the **curl** library, has been added to the PHP **cURL** extension. (BZ#1291667)

SCTP in OpenSSL is now supported

The **SCTP** (Stream Control Transmission Protocol) support in the **OpenSSL** library is now enabled for the **OpenSSL DTLS** (Datagram Transport Layer Security) protocol implementation. (BZ#1225379)

Dovecot has tcp_wrappers support enabled

Dovecot is an **IMAP** server, primarily written with security in mind. It also contains a small **POP3** server and supports e-mail in either the **Maildir** or **Mbox** format.

In this update, Dovecot is built with tcp_wrappers support enabled. You can now limit network access to Dovecot using tcp_wrappers as an additional layer of security. (BZ#1229164)

Necessary classes added to allow `log4j` as Tomcat logging mechanism

Due to missing **`tomcat-juli.jar`** and **`tomcat-juli-adapters.jar`** files, the **`log4j`** utility could not be used as Tomcat logging mechanism. The necessary classes have been added and **`log4j`** can now be used for logging. Also, the **`symlinks`** utility has to be installed or updated to point in extras folder with the described .jar files. (BZ#1133070)

MySQL-python rebased to version 1.2.5

The MySQL-python packages have been upgraded to upstream version 1.2.5, which provides a number of bug fixes and enhancements over the previous version. Notably, a bug causing **`ResourceClosedError`** in **`neutron`** and **`cinder`** services has been fixed. (BZ#1266849)

BIND now supports GeoIP-based ACLs

With this update, the BIND DNS server is able to use GeoIP databases. The feature enables administrators to implement client access control lists (ACL), based on client's geographical location. (BZ#1220594)

The BIND server now supports CAA records

Certification Authority Authorization (CAA) support has been added to the Berkeley Internet Name Domain (BIND) server. Users can now restrict Certification Authorities by specifying the DNS record. (BZ#1306610)

The Unbound DNS validating resolver now supports ECDSA cipher for DNSSEC

This update enables the ECDSA cipher in the Unbound DNS validating resolver. As a result, the DNS resolver is now able to validate DNS responses signed using DNSSEC with ECDSA algorithm. (BZ#1245250)

tomcat rebased to version 7.0.69

The tomcat packages have been rebased to version 7.0.69. Notable changes include:

- Resolved numerous bugs and vulnerabilities
- Added the HSTS and VersionLoggerListener features
- Resolved the NoSuchElementException bug outlined in BZ#1311622 (BZ#1287928)

servicelog rebased to version 1.1.14

The servicelog packages have been upgraded to upstream version 1.1.14, which provides a number of bug fixes and enhancements over the previous version. (BZ#1182028)

CHAPTER 17. STORAGE

New kernel subsystem: `libnvdimm`

This update adds **`libnvdimm`**, a kernel subsystem responsible for the detection, configuration, and management of Non-Volatile Dual Inline Memory Modules (NVDIMMs). As a result, if NVDIMMs are present in the system, they are exposed through the **`/dev/pmem*`** device nodes and can be configured using the **`ndctl`** utility. (BZ#1269626)

Hardware with NVDIMM support

At the time of the Red Hat Enterprise Linux 7.3 release, a number of original equipment manufacturers (OEMs) are in the process of adding support for Non-Volatile Dual Inline Memory Module (NVDIMM) hardware. As these products are introduced in the market, Red Hat will work with these OEMs to test these configurations and, if possible, announce support for them on Red Hat Enterprise Linux 7.3.

Since this is a new technology, a specific support statement will be issued for each product and supported configuration. This will be done after successful Red Hat testing, and corresponding documented support by the OEM.

The currently supported NVDIMM products are:

- HPE NVDIMM on HPE ProLiant systems. For specific configurations, see Hewlett Packard Enterprise Company support statements.

NVDIMM products and configurations that are not on this list are not supported. The Red Hat Enterprise Linux 7.3 Release Notes will be updated as NVDIMM products are added to the list of supported products. (BZ#1389121)

New packages: nvml

The nvml packages contain the Non-Volatile Memory Library (NVML), a collection of libraries for using memory-mapped persistence, optimized specifically for persistent memory. (BZ#1274541)

`scsi` now supports multiple hardware queues

The **`nr_hw_queues`** field is now present in the **`Scsi_Host`** structure, which allows drivers to use the field. (BZ#1308703)

The `exclusive_pref_bit` optional argument has been added to the `multipath` ALUA prioritizer

If the **`exclusive_pref_bit`** argument is added to the **`multipath`** Asymmetric Logical Unit Access (ALUA) prioritizer, and a path has the Target Port Group Support (TPGS) **`pref`** bit set, **`multipath`** makes a path group using only that path and assigns the highest priority to the path. Users can now either allow the preferred path to be in a path group with other paths that are equally optimized, which is the default option, or in a path group by itself by adding the **`exclusive_pref_bit`** argument. (BZ#1299652)

`multipathd` now supports raw format mode in `multipathd` formatted output commands

The **`multipathd`** formatted output commands now offer **`raw`** format mode, which removes the headers and additional padding between fields. Support for additional format wildcards has been added as well. Raw format mode makes it easier to collect and parse information about multipath devices, particularly for use in scripting. (BZ#1299651)

Improved LVM locking infrastructure

`lvmlockd` is a next generation locking infrastucture for LVM. It allows LVM to safely manage shared storage from multiple hosts, using either the **`dlm`** or **`sanlock`** lock managers. **`sanlock`** allows

lvmlockd to coordinate hosts through storage-based locking, without the need for an entire cluster infrastructure. For more information, see the **lvmlockd(8)** man page.

This feature was originally introduced in Red Hat Enterprise Linux 7.2 as a Technology Preview. In Red Hat Enterprise Linux 7.3, **lvmlockd** is fully supported. (BZ#1299977)

Support for caching thinly-provisioned logical volumes with limitations

Red Hat Enterprise Linux 7.3 provides the ability to cache thinly provisioned logical volumes. This brings caching benefits to all the thin logical volumes associated with a particular thin pool. However, when thin pools are set up in this way, it is not currently possible to grow the thin pool without removing the cache layer first. This also means that thin pool auto-grow features are unavailable. Users should take care to monitor the fullness and consumption rate of their thin pools to avoid running out of space. Refer to the lvmthin(7) man page for information on thinly-provisioned logical volume and the lvmcache(7) man page for information on LVM cache volumes. (BZ#1371597)

device-mapper-persistent-data rebased to version 0.6.2

The device-mapper-persistent-data packages have been upgraded to upstream version 0.6.2, which provides a number of bug fixes and enhancements over the previous version. Notably, the **thin_ls** tool, which can provide information about thin volumes in a pool, is now available. (BZ#1315452)

Support for DIF/DIX (T10 PI) on specified hardware

SCSI T10 DIF/DIX is fully supported in Red Hat Enterprise Linux 7.3, provided that the hardware vendor has qualified it and provides full support for the particular HBA and storage array configuration. DIF/DIX is not supported on other configurations, it is not supported for use on the boot device, and it is not supported on virtualized guests.

At the current time, the following vendors are known to provide this support.

FUJITSU supports DIF and DIX on:

EMULEX 16G FC HBA:

- EMULEX LPe16000/LPe16002, 10.2.254.0 BIOS, 10.4.255.23 FW, with:
- FUJITSU ETERNUS DX100 S3, DX200 S3, DX500 S3, DX600 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3, AF250, AF650

QLOGIC 16G FC HBA:

- QLOGIC QLE2670/QLE2672, 3.28 BIOS, 8.00.00 FW, with:
- FUJITSU ETERNUS DX100 S3, DX200 S3, DX500 S3, DX600 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3

Note that T10 DIX requires database or some other software that provides generation and verification of checksums on disk blocks. No currently supported Linux file systems have this capability.

EMC supports DIF on:

EMULEX 8G FC HBA:

- LPe12000-E and LPe12002-E with firmware 2.01a10 or later, with:
- EMC VMAX3 Series with Enginuity 5977; EMC Symmetrix VMAX Series with Enginuity 5876.82.57 and later

EMULEX 16G FC HBA:

- LPe16000B-E and LPe16002B-E with firmware 10.0.803.25 or later, with:
- EMC VMAX3 Series with Enginuity 5977; EMC Symmetrix VMAX Series with Enginuity 5876.82.57 and later

QLOGIC 16G FC HBA:

- QLE2670-E-SP and QLE2672-E-SP, with:
- EMC VMAX3 Series with Enginuity 5977; EMC Symmetrix VMAX Series with Enginuity 5876.82.57 and later

Please refer to the hardware vendor's support information for the latest status.

Support for DIF/DIX remains in Technology Preview for other HBAs and storage arrays. (BZ#1379689)

iprutils rebased to version 2.4.13

The iprutils packages have been upgraded to upstream version 2.4.13, which provides a number of bug fixes and enhancements over the previous version. Notably, this update adds support for enabling an adapter write cache on 8247-22L and 8247-21L base Serial Attached SCSI (SAS) backplanes to provide significant performance improvements. (BZ#1274367)

The `multipathd` command can now display the multipath data with JSON formatting

With this release, multipathd now includes the **`show maps json`** command to display the multipath data with JSON formatting. This makes it easier for other programs to parse the **`multipathd show maps`** output. (BZ#1353357)

Default configuration added for Huawei XSG1 arrays

With this release, multipath provides a default configuration for Huawei XSG1 arrays. (BZ#1333331)

Multipath now includes support for Ceph RADOS block devices.

RDB devices need special **`uid`** handling and their own checker function with the ability to repair devices. With this release, it is now possible to run multipath on top of RADOS block devices. Note, however, that the multipath RBD support should be used only when an RBD image with the **`exclusive-lock`** feature enabled is being shared between multiple clients. (BZ#1348372)

Support added for PURE FlashArray

With this release, multipath has added built-in configuration support for the PURE FlashArray (BZ#1300415)

Default configuration added for the MSA 2040 array

With this release, multipath provides a default configuration for the MSA 2040 array. (BZ#1341748)

New `skip_kpartx` configuration option to allow skipping `kpartx` partition creation

The **`skip_kpartx`** option has been added to the defaults, devices, and multipaths sections of the **`multipath.conf`** file. When this option is set to **`yes`**, multipath devices that are configured with **`skip_kpartx`** will not have any partition devices created for them. This allows users to create a multipath device without creating partitions, even if the device has a partition table. The default value of this option is **no**. (BZ#1311659)

Multipaths `weightedpath` prioritizer now supports a `wwn` keyword

The multipaths **`weightedpath`** prioritizer now supports a **`wwn`** keyword. If this is used, the regular expression for matching the device is of the form **`host_wwnn:host_wwpn:target_wwnn:target_wwpn`**. These identifiers can either be looked up

through **sysfs** or using the following **multipathd show paths format** wildcards: **%N:%R:%n:%r**.

The **weightedpath** prioritizer previously only allowed HBTL and device nam**regex** matching. Neither of these are persistent across reboots, so the **weightedpath** prioritizer arguments needed to be changed after every boot. This feature provides a way to use the **weightedpath** prioritizer with persistent device identifiers. (BZ#1297456)

New packages: nvme-cli

The nvme-cli packages provide the Non-Volatile Memory Express (NVMe) command-line interface to manage and configure NVMe controllers. (BZ#1344730)

LVM2 now displays a warning message when autoresize is not configured

The thin pool default behavior is not to autoresize the thin pool when the space is going to be exhausted. Exhausting the space can have various negative consequences. When the user is not using autoresize and the thin pool becomes full, a new warning message notifies the user about possible problems so that they can take appropriate actions, such as resize the thin pool, or stop using the thin volume. (BZ#1189221)

dmstats now supports mapping of files to **dmstats** regions

The **--filemap** option of the **dmstats** command now allows the user to easily configure **dmstats** regions to track I/O operations to a specified file in the file system. Previously, I/O statistics were only available for a whole device, or a region of a device, which limited administrator insight into I/O performance to a per-file basis. Now, the **--filemap** option enables the user to inspect file I/O performance using the same tools used for any **device-mapper** device. (BZ#1286285)

LVM no longer applies LV polices on external volumes

Previously, LVM disruptively applied its own policy for LVM thin logical volumes (LVs) on external volumes as well, which could result in unexpected behavior. With this update, external users of thin pool can use their own management of external thin volumes, and LVM no longer applies LV polices on such volumes. (BZ#1329235)

The thin pool is now always checked for sufficient space when creating a new thin volume

Even when the user does not use autoresize with thin pool monitoring, the thin pool is now always checked for sufficient space when creating a new thin volume.

A new thin volumes now cannot be created in the following situations:

- The thin-pool has reached 100% of the data volume capacity.
- There is less than 25% of thin pool metadata free space for metadata smaller than 16 MiB.
- There is less than 4 MiB of free space in metadata. (BZ#1348336)

LVM can now set the maximum number of cache pool chunks

The new LVM allocation parameter in the allocation section of the **lvm.conf** file, **cache_pool_max_chunks**, limits the maximum number of cache pool chunks. When this parameter is undefined or set to 0, the built-in defaults are used. (BZ#1364244)

Support for ability to uncouple a cache pool from a logical volume

LVM now has the ability to uncouple a cache pool from a logical volume if a device in the cache pool has failed. Previously, this type of failure would require manual intervention and complicated alterations to LVM metadata in order to separate the cache pool from the origin logical volume.

To uncouple a logical volume from its cache-pool use the following command:

```
# lvconvert --uncache *vg*/*lv*
```

Note the following limitations:

- The cache logical volume must be inactive (may require a reboot)
- A **writeback** cache requires the **--force** option due to the possibility of abandoning data lost to failure.

(BZ#1131777)

LVM can now track and display thin snapshot logical volumes that have been removed

You can now configure your system to track thin snapshot logical volumes that have been removed by enabling the **record_lvs_history** metadata option in the **lvm.conf** configuration file. This allows you to display a full thin snapshot dependency chain that includes logical volumes that have been removed from the original dependency chain and have become historical logical volumes. The full dependency chain, including historical LVs, can be displayed with new **lv_full_ancestors** and **lv_full_descendants** reporting fields. For information on configuring and displaying historical logical volumes, see Logical Volume Administration. (BZ#1240549)

CHAPTER 18. SYSTEM AND SUBSCRIPTION MANAGEMENT

The default registration URL is now subscription.rhsm.redhat.com

Since Red Hat Enterprise Linux 7.3, the default registration URL has been changed to subscription.rhsm.redhat.com. (BZ#1396085)

`subscription-manager` displays all addresses associated with a network interface

Previously, the **`subscription-manager`** utility displayed only one address per network interface even if the network interface had more than one associated address. With this update, a new system fact with the suffix **`_list`** corresponding to each network interface is reported to the entitlement server that contains a comma-separated string of values. As a result, **`subscription-manager`** is now able to display all addresses associated with the network interface. (BZ#874735)

`rct` now enables displaying only subscription data

The **`rct`** utility now accepts the **`--no-content`** option. Passing **`--no-content`** to the **`rct cat-manifest`** command ensures that **`rct`** displays only subscription data. (BZ#1336883)

`rct cat-manifest` now displays information to determine if `virt-who` is required

The output of the **`rct cat-manifest [MANIFEST_ZIP]`** command now includes fields for **`Virt Limit`** and **`Requires Virt-who`**. These fields help determine if the **`virt-who`** component is required for the deployment. (BZ#1336880)

The `needs-restarting` utility has the new `--services` option

With this update, the **`needs-restarting`** utility has the new **`--services`** option. When the new option is specified, **`needs-restarting`** lists newline-separated service names instead of process IDs. This helps the system administrator to find out which **`systemd`** services they need to restart after running **`yum update`** to benefit from the updates. (BZ#1335587)

The `needs-restarting` utility has the new `--reboothint` option

With this update, the **`needs-restarting`** utility has the new **`--reboothint`** option. Running **`needs-restarting --reboothint`** outputs a message saying which core packages have been updated since the last boot, if any, and thus whether a reboot is recommended. This helps the system administrator to find out whether they need to reboot the system to benefit from all updates. Note that the advice is only informational and does not mean it is strictly necessary to reboot the system immediately. (BZ#1192946)

New `skip_missing_names_on_install` and `skip_missing_names_on_update` options for `yum`

The **`skip_missing_names_on_install`** and **`skip_missing_names_on_update`** options have been added to **`yum`** repository configuration. With **`skip_missing_names_on_install`** set to **`False`** in the **`/etc/yum.conf`** file, using the **`yum install`** command fails if **`yum`** cannot find one of the specified packages, groups, or RPM files. With **`skip_missing_names_on_update`** set to **`False`**, using the **`yum update`** command fails if **`yum`** cannot find one of the specified packages, groups, or RPM files, or if they are available, but not installed. (BZ#1274211)

New `compare_providers_priority` option for `yum`

This update adds the **`compare_providers_priority`** option to **`yum`** repository configuration. When set in the **`/etc/yum.conf`** file, this option enables **`yum`** to respect repository priorities when resolving dependencies, which can be used to influence what **`yum`** does when it encounters a dependency that can be satisfied by packages from multiple different repositories. (BZ#1186690)

CHAPTER 19. VIRTUALIZATION

VT-d posted interrupts

Red Hat Enterprise Linux now supports the Intel Virtualization Technology for Directed I/O (VT-d) in CPU-side posted interrupts. With the VT-d posted interrupts feature enabled, external interrupts from direct-assigned devices can be delivered to guests without the need for assistance by the Virtual Machine Manager, even when the guests are running in non-root mode. (BZ#1172351)

Hyper-V storage driver (storvsc) updated

The Hyper-V storage driver (storvsc) was updated from upstream. This provides moderate performance improvement of I/O operations when using Hyper-V storvsc driver for certain workloads. (BZ#1287040)

Hyper-V clock source changed to use the TSC page

With this update, the Time Stamp Counter (TSC) page is used as the Hyper-V clock source. The TSC page provides a more efficient way of computing the per-guest reference counter value than the previously used model-specific register (MSR). As a result, kernel operations that involve reading time stamps are now faster. (BZ#1300325)

libguestfs rebased to version 1.32.7

The libguestfs packages have been upgraded to upstream version 1.32.6, which provides a number of bug fixes and enhancements over the previous version. Notable changes include the following:

- The **`virt-get-kernel`** utility has been added, which can be used to extract the kernel and initial RAM file system (initramfs) from a disk image file. For details, see the virt-get-kernel(1) man page.
- The **`virt-dib`** utility has been added. Its capabilities include building disk image files and ramdisks. For more information, see the virt-dib(1) man page.
- Multiple options have been added for the **`virt-customize`**, **`virt-builder`**, and **`virt-systprep`** utilities. (BZ#1218766)

`virt-v2v` and `virt-p2v` add support for latest Windows releases

The **`virt-v2v`** utility now includes support for converting virtual machines that use Windows 8, 8.1 and 10, and Windows Server 2012 and 2012R2 from the VMWare hypervisor to run on KVM, Red Hat Enterprise Virtualization, and OpenStack. In addition, the **`virt-p2v`** utility now includes support for converting physical machines that use the mentioned Windows systems to virtual machines compatible with KVM, Red Hat Enterprise Virtualization, and OpenStack. (BZ#1190669)

libvirt administration API added

This update enables an administration interface for the **`libvirtd`** service. Unlike persistent **`libvirtd`** configuration, which can be adjusted using the **`libvirtd.conf`** file and requires daemon restart each time it is modified, the administration interface enables users to change the daemon settings at any time. In addition, the administration interface provides multiple means of monitoring current daemon settings.

Specifically, the operations that the API enables include the following:

- Listing all daemon servers
- Listing all client connections
- Providing detailed information about a client connection
- Closing individual client connections in a forceful manner

- Reconfiguration of the limits to number of allowed clients and active worker threads on the host.

The administration interface can be controlled using the **virt-admin** utility, which is based on the existing **virsh** client. For more information, see the virt-admin(1) man page. (BZ#735385)

virt-p2v is fully supported

The **virt-p2v** tool, introduced in Red Hat Enterprise Linux 7.2 as a Technology Preview, is now fully supported. It enables converting physical machines to virtual machines compatible with the KVM hypervisor, and was previously available as a Technology Preview.

virt-p2v is provided as an ISO image that contains a minimal Red Hat Enterprise Linux distribution and the tool itself. To convert a physical machine, burn the ISO image to a CD and use it to boot the physical machine. PXE booting and USB booting are also supported. Afterwards, follow the on-screen instructions to perform a manual conversion or activate the automated conversion.

For further information, install the virt-v2v package and see the virt-p2v(1) manual page, or refer to the following Knowledgebase article:

https://access.redhat.com/articles/2702281 (BZ#1358332)

New package: libvirt-nss

Red Hat Enterprise Linux 7.3 adds the libvirt-nss package, which enables you to use the libvirt Network Security Services (NSS) module. This module makes it easier to connect to guests with TLS, SSL, SSH, as well as other remote login services. In addition, it benefits utilities that use host name translation, such as **ping**. For more information, see the Red Hat Enterprise Linux 7 Virtualization Deployment and Administration Guide. (BZ#1325996)

Intel Xeon v5 processors supported on KVM guests

Support for Intel Xeon v5 processors has now been added to the KVM hypervisor and kernel code, and to the **libvirt** API. This enables KVM guest virtual machines to use the following features: MPX, XSAVEC, XGETBV1. (BZ#1327599)

VirtIO 1.0 full support

VirtIO 1.0 devices, introduced in Red Hat Enterprise Linux 7.2 as a Technology Preview, are now fully supported. (BZ#1227339)

libvirt iptables rules can be manually managed for a specified network

libvirt automatically generates and applies iptables rules appropriate for each type of network it creates. The rules are controlled by **forward mode** in the configuration of each network. Previously, there was no way for users to disable these automatically generated iptables rules and manually manage the iptables rules. In the current release, the **open** network **forward mode** was added. When specified for a network, **libvirt** does not generate any iptables rules for the network. As a result, iptables rules added outside the scope of **libvirt** are not disrupted and users can manually manage iptables rules. (BZ#846810)

open-vm-tools rebased to version 10.0.5

The open-vm-tools packages have been upgraded to upstream version 10.0.5, which provides a number of bug fixes and enhancements over the previous version. Notably, it introduces the guest OS customization (GOSC) and quiesce snapshot features. (BZ#1268537)

virt-who handles HTTP error 429 properly

When the Subscription Manager load is too big, it might return HTTP error code 429 to rate-limit communication with the client. Previously, virt-who did not handle this error code properly, resulting in sub-optimal behavior. With this update, virt-who now handles HTTP error code 429 properly and retries the communication with Subscription Manager later. (BZ#1286945)

Encrypted Hyper-V connections supported in virt-who

Previously, virt-who used unencrypted Hyper-V connections. All data was sent in plain text. This had security implications and needed special configuration on Hyper-V servers to be allowed. With this update, virt-who now uses Windows NT LAN Manager (NTLM) sealing and signing to protect communication with Hyper-V servers. (BZ#1278637)

New channel for registering hypervisors that are not based on Red Hat Enterprise Linux

Previously, virt-who consumed one Red Hat Enterprise Linux 6 subscription for each registered hypervisor, even when the registered hypervisor was not Red Hat Enterprise Linux-based. With this update, virt-who creates and uses a new channel named **`Hypervisor Base`** for hypervisor registration on Satellite 5. As a result, virt-who now uses the **`Hypervisor Base`** channel for newly registered hypervisors and does not consume unnecessary Red Hat Enterprise Linux 6 subscriptions. (BZ#1245035)

Full support for Diag0c on IBM z Systems

Red Hat Enterprise Linux 7.3 provides full support for the Diag0c feature on IBM z Systems. Diag0c support makes it possible to read the CPU performance metrics provided by the z/VM hypervisor, and allows obtaining the management time for each online CPU of a Linux guest where the diagnose task is executed. (BZ#1278795)

The `libvirt` API generates addresses for USB devices

With this update, **`libvirt`** generates addresses for USB devices. These devices, along with the **`libvirt`**-generated address children can be found in the domain XML file. This ensures that future start, restore, and migrate operations have a consistent address for the guests' USB devices. As a result, you can migrate virtual machines to which USB devices have been attached. (BZ#1215968)

WALinuxAgent rebased to version 2.2.0

The Windows Azure Linux Agent has been upgraded to upstream version 2.2.0, which provides a number of bug fixes and enhancements over the previous version. This agent supports the provisioning and running of Linux Virtual Machines in the Windows Azure cloud and should be installed on Linux images that are built to run in the Windows Azure environment. The WALinuxAgent package is provided in the Extras channel. (BZ#1387783)

CHAPTER 20. ATOMIC HOST AND CONTAINERS

Red Hat Enterprise Linux Atomic Host

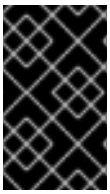
Red Hat Enterprise Linux Atomic Host is a secure, lightweight, and minimal-footprint operating system optimized to run Linux containers. See the Atomic Host and Containers Release Notes for the latest new features, known issues, and Technology Previews.

CHAPTER 21. RED HAT SOFTWARE COLLECTIONS

Red Hat Software Collections is a Red Hat content set that provides a set of dynamic programming languages, database servers, and related packages that you can install and use on all supported releases of Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 on AMD64 and Intel 64 architectures. Red Hat Developer Toolset is included as a separate Software Collection.

Red Hat Developer Toolset is designed for developers working on the Red Hat Enterprise Linux platform. It provides current versions of the GNU Compiler Collection, GNU Debugger, and other development, debugging, and performance monitoring tools. Since Red Hat Software Collections 2.3, the Eclipse development platform is provided as a separate Software Collection.

Dynamic languages, database servers, and other tools distributed with Red Hat Software Collections do not replace the default system tools provided with Red Hat Enterprise Linux, nor are they used in preference to these tools. Red Hat Software Collections uses an alternative packaging mechanism based on the **scl** utility to provide a parallel set of packages. This set enables optional use of alternative package versions on Red Hat Enterprise Linux. By using the **scl** utility, users can choose which package version they want to run at any time.



IMPORTANT

Red Hat Software Collections has a shorter life cycle and support term than Red Hat Enterprise Linux. For more information, see the Red Hat Software Collections Product Life Cycle.

See the Red Hat Software Collections documentation for the components included in the set, system requirements, known problems, usage, and specifics of individual Software Collections.

See the Red Hat Developer Toolset documentation for more information about the components included in this Software Collection, installation, usage, known problems, and more.

PART II. NOTABLE BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 7.3 that have a significant impact on users.

CHAPTER 22. GENERAL UPDATES

Shortening of long network device names

Some network devices have unacceptably long names. This is due to certain firmware reporting meaningless data, such as the device's **onboard index** value, which the kernel passes to user-space.

Previously, this resulted in problems with maximum name length, especially with VLANs. With this update, **systemd** rejects unacceptably long names and falls back to a different naming scheme. As a result, long network device names will no longer appear.

IMPORTANT: This also means that names on existing installations might change, and the affected network devices will not go online.

The change in name will happen on network cards with names **enoX** where **X** is more than 16383. This will mostly affect vmware machines, because their firmware has the described problem. (BZ#1230210)

A fix for systemd to read the device identification bytes correctly

Due to an endianness problem, the version of systemd in Red Hat Enterprise Linux 7.2 read the device identification bytes in a wrong order, causing the **dev/disk/by-id/wwn-*** symbolic links to be generated incorrectly. A patch has been applied to put the device identification bytes in the correct order and the symbolic links are now generated correctly. Any reference that depends on the value obtained from **/dev/disk/by-id/wwn-*** needs to be modified to work correctly in Red Hat Enterprise Linux 7.3 and later. (BZ#1308795)

The value of `net.unix.max_dgram_qlen` increased to 512

Previously, the default value of the **net.unix.max_dgram_qlen** kernel option was 16. As a consequence, when the network traffic was too high, certain services could terminate unexpectedly. This update sets the value to 512, thus preventing this problem. Users need to reboot the machine to apply this change. (BZ#1267707)

Links to non-root file systems in `/lib/` and `/lib64/` are removed by `ldconfig.service`

Red Hat Enterprise Linux 7.2 introduced **ldconfig.service**, which is run at an early stage of the boot process, before non-root file systems are mounted. Before this update, when **ldconfig.service** was run, links in the **/lib/** and **/lib64/** directories were removed if they pointed to file systems which were not yet mounted. In Red Hat Enterprise Linux 7.3, **ldconfig.service** has been removed, and the problem no longer occurs. (BZ#1301990)

`systemd` no longer hangs when many processes terminate in a short interval

Previously, an inefficient algorithm for reaping processes caused the **systemd** service to become unresponsive when a large number of processes terminated in a short interval. With this update, the algorithm has been improved, and **systemd** is now able to reap the processes more quickly, which prevents the described **systemd** hang from occurring. (BZ#1360160)

gnome-dictionary multilib packages conflicts no longer occur

When both the 32-bit and 64-bit packages of the gnome-dictionary multilib packages were installed, upgrading from Red Hat Enterprise Linux 7.2 to Red Hat Enterprise Linux 7.3 failed. To fix this problem, the 32-bit package has been removed from Red Hat Enterprise Linux 7.3. As a result, upgrading in this situation works as expected. (BZ#1360338)

CHAPTER 23. AUTHENTICATION AND INTEROPERABILITY

Change in keep alive entry logging level

Keep alive entries are used to prevent skipped updates from being evaluated multiple times in fractional replication. If a large number of updates is skipped, these entries can be updated very frequently. Also, each entry is tested to see if it already exists before the update, so that only unique entries are created.

This test was previously logged at the **`Fatal`** level, which caused error logs to be filled with unnecessary messages that could not be filtered out. This update changes the logging level for keep alive entries from **`Fatal`** to **`Replication debugging`** (**`8192`**), and the entries can now be filtered out. (BZ#1314557)

The `cleanAllRUV` task no longer logs false `attrlist_replace` errors

A memory corruption bug in the **`cleanAllRUV`** task was causing **`attrlist_replace`** error messages to be logged by mistake. The task has been updated to use a different function for memory copying, and it no longer writes false error messages to logs. (BZ#1288229)

Connection objects no longer deadlock

Previously, an unnecessary lock was sometimes acquired on a connection object, which could then cause a deadlock. A patch has been applied to remove the unnecessary locking, and the deadlock no longer occurs. (BZ#1278755)

Abandon requests for simple paged results searches no longer cause a crash

Prior to this update, Directory Server could receive an abandon request for a simple paged results search after the abandon check was completed but before the results were fully sent. In this case, the abandon request was processed while the results were being sent, which caused Directory Server to crash. This update adds a lock which prevents abandon requests from being processed while the results are already being sent, and the crash no longer occurs. (BZ#1278567)

Simple paged results search slots are now correctly released after a failure

Previously, if a simple paged results search failed in the back end, the simple paged results slot was not released. Consequently, multiple simple paged results slots could be accumulated in a connection object. With this update, the simple paged results slot is released correctly when a search fails, and unused simple paged results slots are no longer left in a connection object. (BZ#1290242)

`DES` to `AES` password conversion must now be done manually on suffixes other than `cn=config`

When Directory Server starts, all present passwords which are encrypted by the Data Encryption Standard (DES) algorithm are automatically converted to use the more secure Advanced Encryption Standard (AES) algorithm. **`DES`**-encrypted passwords were previously detected using an internal unindexed search, which was too slow for very large user databases, and in some cases caused the startup process to time out and prevent Directory Server from starting. With this update, only the configuration suffix **`cn=config`** is checked for **`DES`** passwords, and a new **`slapi`** task **`des2aes`** is now available, which administrators can run after starting the server to convert passwords to **`AES`** on a specific database if needed. As a result, the server starts up regardless of the size of user databases. (BZ#1342609)

Deleting a back end database no longer causes deadlocks

Transaction information was previously not passed to one of the database helper functions during back end deletion. Consequently, a deadlock occurred if a plug-in attempted to access data in the area locked by the transaction. This update ensures that transaction information is passed to all necessary database helper functions, and the deadlock no longer occurs. (BZ#1273555)

Deleting and adding the same LDAP attribute now correctly updates the equality index

Previously, when several values of the same LDAP attribute were deleted using the **ldapmodify** command, and at least one of them was added again during the same operation, the equality index was not updated. As a consequence, an exact search for the re-added attribute value did not return that entry. The logic of the index code has been modified to update the index if at least one of the values in the entry changes, and the exact search for the re-added attribute value now returns the correct entry. (BZ#1290600)

Abandon requests in simple paged results searches no longer cause deadlocks

An exclusive connection lock was previously added as part of a bug fix related to abandon requests in simple paged results searches. However, in specific circumstances, this new lock causes a self-deadlock. This update makes the lock reentrant, and self-deadlocks no longer occur during simple paged results searches. (BZ#1295947)

Simple paged results searches no longer return `0` instead of the actual results

Previously, when a simple paged results slot in a connection was discarded due to an error such as **SIZELIMIT_EXCEEDED**, the discarded slot was not cleaned up properly. Subsequent searches which reused this slot then always returned **0**. With this update, discarded simple paged results slots are cleaned up correctly, and searches return correct results even with reused slots. (BZ#1331343)

ACL plug-in no longer crashes due to missing `pblock` object

When a persistent search (psearch) was launched by a **bind** user without sufficient permissions, the access permissions object in cache failed to reset to point the initial **pblock** structure to the permanent structure. As a consequence, the access control list (ACL) plug-in could crash the server due to a missing **pblock** object. This update ensures that the initial object is reset to the permanent structure, and Directory Server no longer crashes in this situation. (BZ#1302823)

Replication changelog no longer incorrectly skips updates

A bug in the changelog iterator buffer caused it to point to an incorrect position when reloading the buffer. This caused replication to skip parts of the changelog, and consequently some changes were not replicated. This bug has been fixed, and replication data loss due to an incorrectly reloaded changelog buffer no longer occurs. (BZ#1321124)

Old schema styles can now correctly be used with single quotes

Starting with version 1.3.2, the 389-ds-base packages are compliant with the schema definition described in RFC 4512, which does not allow the schema to be used by the older versions. To ease migration from previous versions, the **nsslapd-enquote-sup-oc** parameter was introduced. However, the implementation of this parameter had a bug which prevented handling old schema styles in single quotes, such as:

```
SYNTAX oid
```

This bug is now fixed, and you can use single quotes with older schema styles.

Additionally, this update introduces the **LDAP_SCHEMA_ALLOW_QUOTES** environment variable which adds support for older style schema in the schema directory. To enable this functionality, set the following variable in the **/etc/sysconfig/dirsrv-INSTANCE** configuration file:

```
LDAP_SCHEMA_ALLOW_QUOTED=on
```

(BZ#1303641)

Password conversion from `DES` to `AES` now works properly

During the upgrade from Red Hat Enterprise Linux 7.1 to 7.2, the encryption algorithm used by the **Reversible Password Plug-in** was changed from **DES** to **AES**. Directory Server automatically

converted all passwords to the new algorithm upon upgrade. However, password conversion failed with an **error 32** if any defined back end was missing the top entry. Additionally, even if the conversion failed, 389-ds-base still disabled the **DES** plug-in, which caused existing passwords to fail to decode.

This bug has been fixed, 389-ds-base now ignores errors when searching back ends for passwords to convert, and the **DES** plug-in is now only disabled after all passwords are successfully converted to **AES**. (BZ#1320715)

Keep-alive entries no longer break replication

Previously, a keep-alive entry was being created at too many opportunities during replication, potentially causing a race condition when adding the entry to the replica changelog and resulting in operations being dropped from the replication. With this update, unnecessary keep-alive entry creation has been eliminated, and keep-alive entries no longer cause missing operations during replication. (BZ#1307151)

Failed replication updates are now retried correctly in the next session

If a replica update failed on the consumer side and was followed by another update that succeeded, the consumer's replication status was updated by the successful update, which caused the consumer to seem as if it was up to date. Consequently, the failed update was never retried, leading to data loss. With this update, a replication failure closes the connection and stops the replication session. This prevents further updates from changing the consumer's replication status, and allows the supplier to retry the failed operation in the next session, avoiding data loss. (BZ#1310848)

The `LICENSE` file now shows correct license information

Previously, the output of the **rpm -qi 389-ds-base** command displayed an incorrect License field with an earlier license, **GPLv2 with exceptions**. This problem has been fixed and the 389-ds-base package now provides the correct license information (the **GPLv3+** license) in its **LICENSE** file. (BZ#1315893)

Passwords reset by administrators are now stored in password history

When a user password was reset by an administrator, the old password was previously not stored in the user's password history. This allowed the user to reuse the same password after the reset. With this update, passwords reset manually by administrators are stored in password history, and the user must use a different password. (BZ#1332709)

Entries rejected by multiple plug-ins no longer show up in searches

Previously, when an entry was rejected by multiple back end transaction plug-ins (for example, **Auto Membership** or **Managed Entry**) at the same time, the entry cache was left in an inconsistent state. This allowed a search to return the entry even though it was not added. With this update, the entry cache which stores the Distinguished Name (DN) of the entry is properly cleaned up when an **add** operation fails, and rejected entries are no longer returned by **ldapsearch**. (BZ#1304682)

Running `db2index` with no options no longer causes replication failures

When running the **db2index** script with no options, the script failed to handle on-disk Replica Update Vector (RUV) entries because these entries have no parent entries. The existing RUV was skipped and a new one was generated instead, which subsequently caused the next replication to fail due to an ID mismatch. This update fixes handling of RUV entries in **db2index**, and running this script without specifying any options no longer causes replication failures. (BZ#1340307)

Directory Server no longer crashes when attempting to remove a busy database

Previously, attempting to remove a back end database using the console while an import was in progress caused Directory Server to crash. With this update, the removal script first checks if the back end is busy, and only proceeds if it is safe to remove. Directory Server therefore no longer crashes in this situation. (BZ#1355760)

Promoting a consumer to a master no longer fails due to duplicate ID errors

Previously, when a consumer instance was promoted to master, a new element was appended to the end of the replica update vector (RUV). However, when attempting to replicate from the newly promoted master, the remote checked the first element of the RUV instead of the last one, which caused it to abort the replication session due to a duplicate ID. With this update, the RUV is reordered when promoting a replica to a master, and replication from masters which were previously replicas no longer fails. (BZ#1278987)

`nsslapd` now correctly sets its working directory

A regression introduced in an earlier bug fix caused **`nsslapd`** to skip setting its working directory (the **`nsslapd-workingdir`** attribute) by default when it was started by **`systemd`**. This bug has been fixed and the working directory is being set during startup again. (BZ#1360447)

The IdM upgrade script now runs successfully

Previously, the Identity Management (IdM) server upgrade script failed to detect a version change. As a consequence, upgrading an IdM server failed. This bug has been fixed and the upgrade now succeeds. (BZ#1290142)

The `libkadm5*` libraries have been moved to the libkadm5 package

In Red Hat Enterprise Linux 7.3, the **`libkadm5*`** libraries have been moved from the krb5-libs to the new libkadm5 package. As a consequence, **`yum`** is not able to downgrade the krb5-libs package automatically. Before downgrading, remove the libkadm5 package manually:

```
# rpm -e --nodeps libkadm5
```

After you have manually removed the package, use the **`yum downgrade`** command to downgrade the krb5-libs package to a previous version. (BZ#1347403)

Single sign-on now works correctly in trusts with multiple AD forest root domains

Previously, if Identity Management (IdM) established a trust to two different Active Directory (AD) forests which trust each other, and IdM was set up in a DNS subdomain of one of them, the other AD forest reported a name suffix routing conflict between IdM and AD. As a consequence, single sign-on failed between IdM and the AD forest that identified the name routing conflict. A procedure now detects such conflicts when you establish the trust. If you provide the AD administrator credentials during establishing the trust, an exclusion entry is automatically created to resolve the name suffix routing conflict. As a result, single sign-on works as expected if IdM is deployed in a DNS subdomain of an AD forest. (BZ#1348560)

Upgrading from Red Hat Enterprise Linux 7.2 to 7.3 no longer fails due to certain multilib SSSD packages

The **`sssd-common`** and **`sssd-krb5-common`** packages, provided as part of the System Security Services Daemon (SSSD), no longer support multiple architectures. Previously, when the packages were installed in both 32-bit and 64-bit versions, upgrading from Red Hat Enterprise Linux 7.2 to 7.3 failed. To fix this problem, the 32-bit versions of **`sssd-common`** and **`sssd-krb5-common`** have been removed from Red Hat Enterprise Linux 7.3. This ensures that the upgrade succeeds. (BZ#1360188)

OpenLDAP now correctly sets NSS settings

Previously, the OpenLDAP server used an incorrect handling of network security settings (NSS) code. As a consequence, settings were not applied, which caused certain NSS options, such as **`olcTLSProtocolMin`**, not to work correctly. This update addresses the bug and as a result, the affected NSS options now work as expected. (BZ#1249093)

The `sudo` command now works correctly when using Kerberos with a smart card

Previously, the **`pam_krb5`** module closed to many file descriptors during fork operations. As a consequence, **`sudo`** commands for users authenticating using Kerberos and smart cards failed if the

password entry was not found within the first 4096 characters of the **/etc/passwd** file. This bug has been fixed, libraries such as nsswitch can now use the file descriptors and **sudo** works correctly. (BZ#1263745)

The Certificate System restores support for the PKCS#10 extension in CSRs

Previously, the certificate signing request (CSR) generated during the Certificate System installation with an externally signed certificate did not contain PKCS#10 extensions which are required by some external certificate authorities (CA). With this update, the Certificate System now creates a CSR with default extensions, including basic constraints and key usages extensions, and optional user-defined extensions. (BZ#1329365)

The IdM CA service now starts correctly on IPv6-only installations

Previously, on systems only configured for IPv6, the **pki-tomcat** service was incorrectly bound to the IPv4 loopback device during Identity Management (IdM) installation. As a consequence, the certificate authority (CA) service failed to start. The IdM setup now binds on systems having only the IPv6 protocol configured, to the IPv6 loopback device. As a result, the CA service starts correctly. (BZ#1082663)

The `pki` command now displays revocation details

With this update, the **pki** subcommands **cert-show** and **cert-find** now display information about revoked certificates, such as the following:

- revocation date
- revoked by (BZ#1224382)

`ipa-replica-install --setup-dns` no longer creates DNS zones for DNS names that already exist in DNS

Previously, using the **--setup-dns** option with the **ipa-replica-install** utility always created a DNS zone equal to the primary Identity Management (IdM) domain name as well as zone names for IdM servers, even if such DNS zones already existed on another DNS server. This caused certain problems on the client side if multiple DNS servers incorrectly acted as authoritative servers for a domain. To fix this problem, IdM no longer creates DNS zones if they already exist on other DNS servers. The IdM installer properly detects the conflict, and the installation fails in this situation. (BZ#1343142)

The `idmap_hash` module now works correctly when used with other modules

Previously, the **idmap_hash** module worked incorrectly when it was used together with other modules. As a consequence, user and group IDs were not mapped properly. A patch has been applied to skip already configured modules. Now, the hash module can be used as the default idmap configuration back end and IDs are resolved correctly. (BZ#1316899)

CRL now generates less messages when CA loses connection to netHSM

Previously, when a CA lost connection to Thales netHSM, the CRL generation could enter a loop caused by the unavailability of a dependent component, such as HSM or LDAP, in the middle of CRL generation. Consequently, the process generated a large amount of debug log messages until the CA got restarted. This update provides a fix to slow down the loop, significantly reducing the amount of debug messages generated in the described scenario. (BZ#1308772)

KRA no longer fails to recover keys when installed with a Gemalto Safenet LunaSA (HSM)

Previously, the Red Hat Certificate System key recovery authority (KRA) subsystem failed to recover keys if installed on a Gemalto Safenet LunaSA hardware security module (HSM). A patch was applied and now recovery works like expected, if the HSM is set to non-FIPS mode. (BZ#1331596)

Lower and more stable Directory Server's process size

Previously, Directory Server used the default memory allocator provided in the **glibc** library. This

allocator was not efficient enough to handle the Directory Server's **malloc()** and **free()** patterns. Consequently, the Directory Server's memory usage was sometimes very high, which could cause the Out of Memory (OOM) Killer to kill the **ns-slapd** process. With this update, Directory Server uses the **tcmalloc** memory allocator. As a result, the Directory Server's process size is significantly lower and more stable. (BZ#1186512)

ns-slapd now correctly prompts for a pin when the pin.txt file is not found

In previous releases, 389-ds-base did not display a prompt asking for a pin if the **pin.txt** file was not found, due to the fact that **systemd** captures standard input and output which 389-ds-base was attempting to use. With this update, 389-ds-base detects whether **systemd** is running on the system during startup, and uses the correct **systemd** API to display the password prompt if required. Directory Server can therefore be started without a **pin.txt** file, which allows administrators to keep **nssdb** passwords away from the system. (BZ#1316580)

Replication agreement update status now includes details about replication agreement failures

The replication agreement update status previously displayed only a generic message after an error occurred, which made troubleshooting the replication agreement failure difficult. Now, the update status includes a detailed error message. As a result, all replication agreement update failures are correctly and precisely logged. (BZ#1370300)

IdM now uses larger default lock table size value

Previously, the number of locks for the Identity Management (IdM) database was to low. As a consequence, updating a large number of group membership attributes could fail. The default lock table size was increased from **10000** to **100000** to address this issue. As a result, updating a large number of group membership attributes no longer fails. (BZ#1196958)

The ipa-server-certinstall command no longer fails to install an external signed certificate

Previously, using the **ipa-server-certinstall** command to install an external signed certificate

- The previous certificate was not untracked in the Certificate System.
- The new external certificate was tracked by the Certificate System.
- The first certificate found in the NSS database was used.

As a consequence, the **ipa-server-certinstall** command failed to install a new certificate for the LDAP and web server when it was signed by an external certificate authority (CA) and the services could not be started. The command has been fixed, and now only tracks certificates issued by the Identity Management (IdM) CA. As a result, the new certificate is installed correctly and the LDAP and web server no longer fail to start in the described scenario. (BZ#1294503)

sudo rules now work correctly when default_domain_suffix is set or when including a fully-qualified name

Previously, the **sudo** utility did not correctly evaluate a **sudo** rule in these situations:

- When the **default_domain_suffix** option was used in the **/etc/sssd/sssd.conf** file
- When the **sudo** rule used a fully-qualified user name

As a consequence, the **sudo** rule did not work. With this update, the System Security Services Daemon (SSSD) modifies **sudo** rules so that **sudo** evaluates them correctly in the described situation. (BZ#1300663)

The proxy configuration has been removed from the SSSD default configuration file

Previously, the System Security Services Daemon's (SSSD) **/usr/lib64/sssd/conf/sssd.conf** default configuration file used an auto-configured domain to proxy all requests to the **/etc/passwd** and **/etc/groups** files. This proxy configuration failed to integrate with other utilities like **realmd** or **ipa-client-install**. To fix the incompatibilities, the **[domain/shadowutils]** proxy configuration has been removed and SSSD now works correctly. (BZ#1369118)

Show, find, and export operations in the `sss_override` utility now work correctly

Red Hat Enterprise Linux 7.3 introduced local overrides to the System Security Services Daemon (SSSD). Due to a regression, **sss_override** commands failed if an override was created without the **-n** option. The bug has been fixed and now **sss_override** works correctly. (BZ#1373420)

`ipa` commands no longer fail when the user does not have a home directory in IdM

Previously, when Identity Management (IdM) was unable to create a cache directory at **~/.cache/ipa** in the home directory, all **ipa** commands failed. This situation occurred, for example, when the user did not have a home directory. With this update, IdM is able to continue working even when it cannot create or access the cache. Note that in such situations, **ipa** commands can take a long time to complete because all metadata must be downloaded repeatedly. (BZ#1364113)

Displaying help for the IdM command-line interface no longer takes unexpectedly long

When the user executes the **ipa** utility with the **--help** option, **ipa** gathers the required information from plug-ins and commands. Previously, the plug-ins and commands were Python modules. With this release, **ipa** generates the plug-ins and commands based on a schema downloaded from the server.

Because of this, displaying the help sometimes took significantly longer than in the previous version of Identity Management (IdM), especially if the help included lists of topics and commands. This bug has been fixed, which reduces the time required to execute **ipa** with **--help**. (BZ#1356146)

Running commands on servers with an earlier version of IdM no longer takes unexpectedly long

When a user on an Identity Management (IdM) client running IdM version 4.4 executes a command, IdM checks if the server contacted by the client supports the new command schema. Because this information is not cached, the check is performed every time the client contacts the server, which previously prolonged the time required to invoke commands on servers running an earlier version of IdM. If the user executed a new command introduced in IdM 4.4, it sometimes even seemed that the operation would not complete at all, because the server did not recognize the command. This bug has been fixed, and executing IdM commands in the described situation no longer takes unexpectedly long. (BZ#1357488)

Tree-root domains in a trusted AD forest are now marked as reachable through the forest root

When an Active Directory (AD) forest contained tree-root domains (a separate DNS domain), Identity Management (IdM) sometimes failed to correctly route authentication requests to the tree-root domain's domain controllers. Consequently, users from a tree-root domain failed to authenticate against services hosted in IdM. This update fixes the bug, and users from a tree-root domain can authenticate as expected in this situation. (BZ#1318169)

The IdM web UI shows certificates issued by sub-CAs as expected

To display the certificates issued by a certificate authority (CA), the IdM web UI uses the **ipa cert-find** command to query the CA name, and then the **ipa cert-show** command. Previously, **ipa cert-show** did not use the CA name. As a consequence, attempting to display the details page for a

certificate issued by a sub-CA failed with an error in the web UI. This bug has been fixed, and the web UI now displays the details pages for certificates as expected. (BZ#1368424)

`certmonger` no longer fails to request certificates from IdM sub-CAs

The **`certmonger`** service previously used incorrect API calls to request certificates from IdM sub-Certificate Authorities (sub-CAs). As a consequence, the sub-CA setting was ignored and the certificate was always issued by the IdM root CA. This update fixes the bug, and **`certmonger`** now requests certificates from IdM sub-CAs as expected. (BZ#1367683)

Adding an IdM OTP token with a custom key works as expected

When the user executed the **`ipa otptoken-add`** command with the **`--key`** option to add a new one-time password (OTP) token, the Identity Management (IdM) command line converted the token key provided by the user incorrectly. Consequently, the OTP token created in IdM was invalid, and attempts to authenticate using the OTP token failed. This update fixes the bug, and OTP tokens created in this situation are valid. (BZ#1368981)

Importing an Administrator Certificate into the web browser is now possible using the EE page

Previously, importing a Certificate System Administrator Certificate into the web browser using the EnrollSuccess.template failed with this error:

```
Error encountered while rendering a response.
```

With this update, you can import the certificate by following these steps:

1. Stop the **`pki-tomcatd`** service:

```
systemctl stop pki-tomcatd@pki-tomcat.service
```

2. Edit the **`/etc/pki/pki-tomcat/ca/CS.cfg`** file to include the following:

```
ca.Policy.enable=true
 cmsgateway.enableAdminEnroll=true
```

3. Start the **`pki-tomcatd`** service:

```
systemctl start pki-tomcatd@pki-tomcat.service
```

4. Create a new Firefox profile.

5. Go to the End Entity (EE) page, and select the Retrieval tab.

6. Import the CA certificate and configure it as a trusted certificate.

7. Within the new Firefox profile, go to https://pki.example.com:8443/ca/admin/ca/adminEnroll.html, and fill out the form.

8. A new Administrator Certificate source is generated. Import it into the new Firefox profile.

To verify that the certificate was imported successfully, use it to go to the Agents page. (BZ#1274419)

CHAPTER 24. CLUSTERING

Pacemaker correctly interprets systemd responses and systemd services are stopped in proper order at cluster shutdown

Previously, when a Pacemaker cluster was configured with **`systemd`** resources and the cluster was stopped, Pacemaker could mistakenly assume that a **`systemd`** service had stopped before it actually had stopped. As a consequence, services could be stopped out of order, potentially leading to stop failures. With this update, Pacemaker now correctly interprets **`systemd`** responses and **`systemd`** services are stopped in the proper order at cluster shutdown. (BZ#1286316)

Pacemaker now distinguishes transient failures from fatal failures when loading systemd units

Previously, Pacemaker treated all errors loading a **`systemd`** unit as fatal. As a consequence, Pacemaker would not start a **`systemd`** resource on a node where it could not load the **`systemd`** unit, even if the load failed due to transient conditions such as CPU load. With this update, Pacemaker now distinguishes transient failures from fatal failures when loading **`systemd`** units. Logs and cluster status now show more appropriate messages, and the resource can start on the node once the transient error clears. (BZ#1346726)

Pacemaker now removes node attributes from its memory when purging a node that has been removed from the cluster

Previously, Pacemaker's node attribute manager removed attribute values from its memory but not the attributes themselves when purging a node that had been removed from the cluster. As a result, if a new node was later added to the cluster with the same node ID, attributes that existed on the original node could not be set for the new node. With this update, Pacemaker now purges the attributes themselves when removing a node and a new node with the same ID encounters no problems with setting attributes. (BZ#1338623)

Pacemaker now correctly determines expected results for resources that are in a group or depend on a clone

Previously, when restarting a service, Pacemaker's **`crm_resource`** tool (and thus the **`pcs resource restart`** command) could fail to properly determine when affected resources successfully started. As a result, the command could fail to restart a resource that is a member of a group, or the command could hang indefinitely if the restarted resource depended on a cloned resource that moved to another node. With this update, the command now properly determines expected results for resources that are in a group or depend on a clone. The desired service is restarted, and the command returns. (BZ#1337688)

Fencing now occurs when DLM requires it, even when the cluster itself does not

Previously, DLM could require fencing due to quorum issues, even when the cluster itself did not require fencing, but would be unable to initiate it, As a consequence, DLM and DLM-based services could hang waiting for fencing that never happened. With this fix, the **`ocf:pacemaker:controld`** resource agent now checks whether DLM is in this state, and requests fencing if so. Fencing now occurs in this situation, allowing DLM to recover. (BZ#1268313)

The DLM now detects and reports connection problems

Previously, the Distributed Lock Manager (DLM) used for cluster communications expected TCP/IP packet delivery and waited for responses indefinitely. As a consequence, if a DLM connection was lost, there was no notification of the problem. With this update, the DLM detects and reports when cluster communications are lost. As a result, DLM communication problems can be identified, and cluster nodes that become unresponsive can be restarted once the problems are resolved. (BZ#1267339)

High Availability instances created by non-admin users are now evacuated when a compute instance is turned off

Previously, the **`fence_compute`** agent searched only for compute instances created by admin users.

As a consequence, instances created by non-admin users were not evacuated when a compute instance was turned off. This update makes sure that **fence_compute** searches for instances run as any user, and compute instances are evacuated to new compute nodes as expected. (BZ#1313561)

Starting the nfsserver resource no longer fails

The **nfs-idmapd** service fails to start when the **var-lib-nfs-rpc_pipefs.mount** process is active. The process is active by default. Consequently, starting the **nfsserver** resource failed. With this update, **var-lib-nfs-rpc_pipefs.mount** stops in this situation and does not prevent **nfs-idmapd** from starting. As a result, **nfsserver** starts as expected. (BZ#1325453)

lrmd logs errors as expected and no longer crashes

Previously, Pacemaker's Local Resource Management Daemon (lrmd) used an invalid format string when logging certain rare **systemd** errors. As a consequence, **lrmd** could terminate unexpectedly with a segmentation fault. A patch has been applied to fix the format string. As a result, **lrmd** no longer crashes and logs the aforementioned rare error messages as intended. (BZ#1284069)

stonithd now properly distinguishes attribute removals from device removals.

Prior to this update, if a user deleted an attribute from a fence device, Pacemaker's **stonithd** service sometimes mistakenly removed the entire device. Consequently, the cluster would no longer use the fence device. The underlying source code has been modified to fix this bug, and **stonithd** now properly distinguishes attribute removals from device removals. As a result, deleting a fence device attribute no longer removes the device itself. (BZ#1287315)

HealthCPU now correctly measures CPU usage

Previously, the **ocf:pacemaker:HealthCPU** resource parsed the output of the **top** command incorrectly on Red Hat Enterprise Linux 7. As a consequence, the **HealthCPU** resource did not work. With this update, the resource agent correctly parses the output of later versions of **top**. As a result, **HealthCPU** now correctly measures CPU usage. (BZ#1287868)

Pacemaker now checks all collected files when stripping sensitive information

Pacemaker has the ability to strip sensitive information that matches a given pattern when submitting system information with bug reports, whether directly by Pacemaker's **crm_report** tool or indirectly via **sosreport**. However, Pacemaker would only check certain collected files, not log file extracts. Because of this, sensitive information could remain in log file extracts. With this fix, Pacemaker now checks all collected files when stripping sensitive information and no sensitive information is collected. (BZ#1219188)

The corosync memory footprint no longer increases on every node rejoin

Previously, when a user rejoined a node some buffers in **corosync** were not freed so that memory consumption grew. With this fix, no memory is leaked and the memory footprint no longer increases on every node rejoin. (BZ#1306349)

Corosync starts correctly when configured to use IPv4 and DNS is set to return both IPv4 and IPv6 addresses

Previously, when a pcs-generated **corosync.conf** file used hostnames instead of IP addresses and Internet Protocol version 4 (IPv4) and the DNS server was set to return both IPV4 and IPV6 addresses, the **corosync** utility failed to start. With this fix, if Corosync is configured to use IPv4, IPv4 is really used. As a result, **corosync** starts as expected in the described circumstances. (BZ#1289169)

The corosync-cmapctl utility correctly handles errors in the print_key() function

Previously, the **corosync-cmapctl** utility did not handle corosync errors in the **print_key()** function correctly. Consequently, **corosync-cmapctl** could enter an infinite loop if the **corosync** utility was killed. The provided fix makes sure all errors returned when Corosync exits are handled correctly. As a

result, **`corosync-cmapctl`** leaves the loop and displays a relevant error message in this scenario. (BZ#1336462)

CHAPTER 25. COMPILER AND TOOLS

Support of OpenMP 4.5 for `libgomp` in GCC

This update provides support for the new version of OpenMP in GCC to allow programs in the Developer Toolset to properly link and run. (BZ#1357060)

Better stack protection in GCC

Prior to this update, GCC stack protection did not work for functions that only contained variable-length arrays and no other (or only very small) arrays. Consequently, a buffer overflow error could occur undetected. This bug has been fixed and the compiler is now able to instrument even such functions. (BZ#1289022)

`gdbserver` now supports seamless debugging of processes from containers

Prior to this update, when **GDB** was executing inside a Super-Privileged Container (SPC) and attached to a process that was running in another container on Red Hat Enterprise Linux Atomic Host, **GDB** did not locate the binary images of the main executable or any shared libraries loaded by the process to be debugged.

As a consequence, **GDB** may have displayed error messages relating to files not being present, or being present but mismatched. Also, **GDB** may have seemed to attach correctly, but subsequent commands may have failed or displayed corrupted information.

In Red Hat Enterprise Linux 7.3, **gdbserver** has been extended for seamless support of debugging processes from containers. The Red Hat Enterprise Linux 7.3 version of **gdbserver** newly supports the **qXfer:exec-file:read** and **vFile:setfs** packets. However, the Red Hat Enterprise Linux 7.3 version of **gdb** cannot use these packets. The Red Hat Developer Toolset 4.1 (or higher) version of **gdb** is recommended for use with containers and with Red Hat Enterprise Linux 7.3 **gdbserver**. The Red Hat Developer Toolset version of **gdbserver** can be used as well.

Red Hat Enterprise Linux 7.3 **gdb** can now suggest using **gdbserver** when run with the **-p** parameter (or the **attach** command) and when, at the same time, it detects that the process being attached is from a container. Red Hat Enterprise Linux 7.3 **gdb** now also suggests the explicit use of the **file** command to specify the location of the process executable in the container being debugged. The **file** command does not need to be entered when the Red Hat Developer Toolset version of **gdb** is being used instead.

With this update, Red Hat Enterprise Linux 7.3 **gdbserver** provides seamless debugging of processes from containers together with Red Hat Developer Toolset 4.1 (or higher) **gdb**. Additionally, Red Hat Enterprise Linux 7.3 **gdb** guides the user through the debugging of processes from containers when Red Hat Developer Toolset **gdb** is not available. (BZ#1186918)

`GDB` no longer kills running processes with deleted executables

Prior to this update, **GDB** attempting to attach to a running process with a deleted executable would accidentally kill the process. This bug has been fixed, and **GDB** no longer erroneously kills processes with deleted executables. (BZ#1326476)

`GDB` now generates smaller core files and respects core-dump filtering

The **gcore** command, which provides **GDB** with its own core-dumping functionality, has been updated to more closely simulate the function of the Linux kernel core-dumping code, thus generating smaller core-dump files. **GDB** now also respects the **/proc/PID/coredump_filter** file, which controls what memory segments are written to core-dump files. (BZ#1265351)

Better error message for `AArch64`

For the **AArch64** target, if a program declared a global variable as a type smaller than an integer, but

then referred to it in another file as if it were an integer, the linker could generate a confusing error message. This update fixes the error message, clearly identifying the cause and suggesting a possible reason for the error to the user. (BZ#1300543)

Large and/or high-address programs now link and execute correctly on `AArch64`

Previously, incorrect code in the linker could result in incorrect branch stubs being generated. Consequently, programs that were very big or if the programmer coded parts of the program to exist at a very high address, failed to link. The bug has been fixed and the correct kind of branch stub is now selected. (BZ#1243559)

The `opreport` and `opannote` utilities now properly analyze archive data.

Previously, when using **`oparchive`** to store data, the associated samples were not included in the archive. In addition, the **`oprofile`** utilities selected data in the current working **`oprofile_data`** directory rather than in the archive. Consequently, the **`opreport`** and **`opannote`** utilities were unable to properly analyze data in an archive generated by **`oparchive`**. This update provides a fix for storing the profiling samples in the archive and selecting them for use with archives, and **`opreport`** and **`opannote`** now work as expected. (BZ#1264443)

Events with identical numerical unit masks are now handled by their names

The 5th-generation Core i3, i5, and i7 Intel processors have some events that have multiple unit masks with the same numerical value. As a consequence, some events' default unit masks were not found and selected. This update changes the events to use a name rather than a numerical value for the default unit mask, thus fixing this bug. (BZ#1272136)

New `MACRO_INSTS_FUSED` event identifier

Previously, the **`MACRO_INSTS`** identifier was used for two different events in the 1th-generation Core i3, i5, and i7 Intel processors. As a consequence, it was impossible to clearly select either event by using **`MACRO_INSTS`**. This update renames one of the events to **`MACRO_INSTS_FUSED`**, thus fixing this bug. (BZ#1335145)

Applications no longer crash upon multiple `libpfm` initializations

Previously, when the **`libpfm`** initialization code was called multiple times (for example, in the PAPI **`fmultiplex1`** test), when run as root, the **`libpfm`** internal data structures became corrupted, causing an unexpected termination. This update ensures the counter of available events is properly reset and applications using **`libpfm`** running as root no longer crash when **`libpfm`** is reinitialized. (BZ#1276702)

Removal of purposeless warning message for physically non-existing nodes

Previously, when the numa_node_to_cpus() function was called on a node which did not have an entry in the sysfs directory, the libnuma library always printed a warning message about an invalid sysfs. Consequently, libnuma printed the confusing warning message also for physically non-existing nodes (for example, for non-contiguous node numbers) and this warning could not be overridden when the function was called using the dlsym interface. With this update, the mentioned warning message is printed just for NUMA nodes that were found during an initial scan but then did not appear in sysfs. As a result, users of libnuma no longer receive the warning message for non-contiguous node numbers. (BZ#1270734)

Selection of OpenJDK version family now remembered across updates

Prior to this update, when a user had multiple JDKs installed, **`yum update`** always updated to the newest JDK even if the user had previously selected some lower-prioritized JDK. This update introduces the **`--family`** switch for **`chkconfig`**, which makes sure that the selected JDK remains in the version **`family`** after system updates. (BZ#1296413)

RC4 is now disabled by default in OpenJDK 6 and OpenJDK 7

Earlier OpenJDK packages allowed the RC4 cryptographic algorithm to be used when making secure

connections using Transport Layer Security (TLS). This algorithm is no longer secure, and it has been disabled in this release. To retain its use, it is necessary to revert to the earlier setting of the **jdk.tls.disabledAlgorithms** of **SSLv3, DH keySize < 768**. This can be done permanently in the **<java.home>/jre/lib/security/java.security** file or by adding the following line:

```
jdk.tls.disabledAlgorithms=SSLv3, DH keySize < 768
```

to a new text file and passing the location of that file to Java on the command line using the **-Djava.security.properties=<path to file>** argument. (BZ#1302385)

zsh no longer deadlocks on malloc() execution

Previously, if the **zsh** process received a signal during the execution of a memory allocation function and the signal handler attempted to allocate or free memory, **zsh** entered a deadlock and became unresponsive. With this update, signal handlers are no longer enabled while handling the global state of **zsh** or while using the heap memory allocator. This ensures that the described deadlock no longer occurs. (BZ#1267912)

SCSI device types described using multiple words are now handled correctly

Prior to this update, the **rescan-scsi-bus.sh** tool misinterpreted SCSI device types that were described using more than one word, for example, **Medium Changer** or **Optical Device**. Consequently, when the script was run on systems that had such device types attached, the script printed multiple misleading error messages. With this update, device types described with multiple words are handled correctly, and the proper device-type description is returned to the user without any errors. (BZ#1298739)

Sphinx builds HTML documentation in FIPS mode properly

Previously, the Python Sphinx generator failed to build documentation in the HTML format on systems with FIPS mode activated. With this update,the use of the md5() function has been fixed by setting the **used_for_security** parameter to **false**. As a result, Sphinx now builds HTML documentation as expected. (BZ#966954)

Perl interpreter no longer crashes after using the PerlIO locale pragma

When a thread was spawned after using the PerlIO locale pragma, the Perl interpreter terminated unexpectedly with a segmentation fault. An upstream patch has been applied, which fixes PerlIO::encoding object duplication. As a result, threads are correctly created after setting a file handle encoding. (BZ#1344749)

Line endings are now preserved in files uploaded with the Net::FTP Perl module in text mode

Previously, when uploading a file with the Net::FTP Perl module in text mode, ends of lines in the uploaded file were incorrectly transformed. This update corrects end-of-line normalization from local to Network Virtual Terminal (NVT) encoding when uploading data to an FTP server, and the described problem no longer occurs. (BZ#1263734)

Perl interpreter no longer crashes when using glob() with a threaded program

Previously, when calling the Perl glob() function after spawning a thread, the Perl interpreter terminated unexpectedly with a segmentation fault. An upstream patch has been applied to clone glob() interpreter-wide data, and using Perl glob() with a threaded program now works as expected. (BZ#1223045)

cgroup values can now be correctly displayed for threads under a parent process by using ps -o thcgr

Previously, the **ps** command displayed only the control group (**cgroup**) of the parent process. Consequently, **cgroup** values of the threads under a parent process were identical to the **cgroup** value of the parent process. This update introduces a new option, **thcgr**, to maintain compatibility with current

cgroup listing. When the **thcgr** option is used, the correct individual **cgroup** values are displayed for threads under the parent process. (BZ#1284087)

pmap no longer reports incorrect totals

With the introduction of **VmFlags** in the kernel **smaps** interface, the **pmap** tool could no longer reliably process the content due to format differences of the **VmFlags** entry. As a consequence, **pmap** reported incorrect totals. The underlying source code has been patched, and **pmap** now works as expected. (BZ#1262864)

vmstat -d is now able to display devices with longer names

When a disk statistics report is required, only the first 15 characters of the device name were previously read from the **/proc/diskstats** file. Consequently, devices with names longer than 15 characters were not shown in the output of the **vmstat -d** command. With this update, the formatting string has been changed to read up to 31 characters, and devices with longer names are now correctly displayed by **vmstat -d**. (BZ#1169349)

A new perl-Perl4-CoreLibs subpackage contains previously removed files

The **provides** tag was incorrectly set for previously deprecated files that were no longer included in the perl package. To fix this bug, these files have been backported from the previous version of Perl and are now provided by a newly created perl-Perl4-CoreLibs subpackage. (BZ#1365991)

GSS-Proxy caches file descriptors less frequently

Previously, the **mechglue** layer of GSS-Proxy cached file descriptors for the lifetime of the process. As a consequence, daemons that often change the UID or GID, such as as **autofs**, could behave unexpectedly. A patch has been applied to close and reopen the connection to GSS-Proxy when an ID changes. As a result, GSS-Proxy caches file descriptors less frequently and daemons that change the UID or GID now work as expected. (BZ#1340259)

Fix to the PAPI_L1_TCM event computation

Previously, the PAPI presets for L1 total cache misses (PAPI_L1_TCM) was computed incorrectly on 4th-generation Core i3, i5, and i7 Intel processors. This update fixes the computation of the **PAPI_L1_TCM** event and programs using **PAPI_L1_TCM** on these processors now get more accurate measurements. (BZ#1277931)

More accurate PAPI_L1_DC* event on IBM Power7 and IBM Power8 platforms

Previously, the PAPI event presets for cache events incorrectly computed derived values for various IBM Power7 and Power8 processors. Consequently, the **PAPI_L1_DCR**, **PAPI_L1_DCW**, and **PAPI_L1_DCA** event values were incorrect. The preset computations have been fixed and the mentioned events are now more accurate. (BZ#1263666)

Improved Postfix expression parser

Previously, the **Postfix** expression parser used to calculate derived metrics from expressions in the **papi_events.csv** file did not perform proper error checking and incorrectly parsed some expressions. Consequently, the parser could potentially write outside the buffers being used to compute the value of a derived metric and cause stack smashing errors for some expressions. A fix has been provided for the parser to prevent it from overwriting memory with incorrect expressions. Now, the parser properly and robustly parses **Postfix** expressions in **papi_events.csv** and reports errors on improper expressions rather than overwriting random regions of memory. (BZ#1357587)

Undefined variable in the udp() function of the python-dns toolkit is now set

Previously, the python-dns toolkit used an undefined **response_time** variable in the **finally** section of the **udp()** function. As a consequence, an incorrect exception was displayed to the user. This bug has been fixed and the correct exception is returned. (BZ#1312770)

`zsh` parses unescaped exclamation marks correctly now

Previously, **zsh** parser state was insufficiently initialized. Consequently, **zsh** failed to parse unescaped exclamation marks in a text string. With this update, **zsh** properly initializes the parser state. As a result, **zsh** now parses unescaped exclamation marks correctly. (BZ#1338689)

`zsh` no longer hangs when receiving a signal while processing a job exit

Previously, signal handlers were enabled while processing a job exit in **zsh**. Consequently, if a signal was received while using the memory allocator and its handler attempted to allocate or free memory, the **zsh** process ended up in a deadlock and became unresponsive. With this update, signal handlers are no longer enabled while processing a job exit. Instead, signals are queued for delayed execution of the signal handlers. As a result, the deadlock no longer occurs and **zsh** no longer hangs. (BZ#1291782)

`zsh` handles the `out of memory` scenario gracefully now

The **zsh** shell allocates memory while printing the **out of memory** fatal error message. Previously, if the printing routine failed to allocate memory, it triggered an infinite recursion. Consequently, the **zsh** process terminated unexpectedly due to a stack overflow. With this update, the infinite recursion no longer appears in this scenario. As a result, after printing the fatal error message, **zsh** now terminates gracefully in case it runs out of memory. (BZ#1302229)

Syntax check in `ksh` compatibility mode now works as expected in `zsh`

Previously, while checking the syntax of a shell script in **ksh** compatibility mode, **zsh** incorrectly initialized the **$HOME** internal variable. Consequently, the **zsh** process terminated unexpectedly after it attempted to dereference a **NULL** pointer. With this update, the $HOME internal variable is properly initialized. As a result, the syntax check in **ksh** compatibility mode now works as expected in **zsh**. (BZ#1267251)

Parsing command substitutions no longer corrupts command history

Previously, commands having the **$()** command substitution construct were recorded incorrectly in the command history. This bug has been fixed and parsing command substitutions no longer corrupts command history. (BZ#1321303)

`haproxy` configuration files can now use host names longer than 32 characters correctly

Previously, when **haproxy** was configured to use peer host names, a bug caused host names longer than 32 characters to be truncated. As a consequence, the **haproxy** configuration files became invalid. This bug has now been fixed, and host names specified as peers can now safely exceed 32 characters. (BZ#1300392)

RPM verification failures no longer occur after installing psacct

When installing the psacct packages, the mode of the **/var/account/pacct** file was previously not set consistently with **logrotate** rules for **psacct**. As a consequence, the mode of **/var/account/pacct** stayed different from these rules after the installation and caused RPM verification failures. With this update, the mode of **/var/account/pacct** is set to 0600 during installation of psacct to align with **logrotate** ghost file rules. As a result, RPM verification failures no longer occur. (BZ#1249665)

The system is no longer rebooted unexpectedly due to SIGINT passed by `sadc`

Due to a race condition, the **sadc** command sometimes passed the SIGINT signal to the init process. As a consequence, the system could be unexpectedly rebooted. This update adds a verification that the SIGINT signal is not sent to the init process. As a result, the system is no longer rebooted unexpectedly. (BZ#1328490)

`pidstat` no longer outputs values above 100% for certain fields

Previously, the **pidstat** command could, under rare circumstances, run out of preallocated space for PIDs on systems with many short-lived processes. As a consequence, the **pidstat** output contained nonsensical values larger than 100%, in the **%CPU**, **%user**, and **%sys** fields. With this update, **pidstat** automatically reallocates space for PIDs, and outputs correct values for all fields. (BZ#1224882)

/usr/bin/nfsiostat provided by sysstat has been deprecated in favor of /sbin/nfsiostat provided by nfs-utils

Previously, two packages provided executables of the same name: the sysstat packages provided **/usr/bin/nfsiostat** and the nfs-utils packages provided **/sbin/nfsiostat**. As a consequence, it was not clear which binary was executed unless the full path was specified. The **nfsiostat** utility provided by sysstat has been deprecated in favor of the one provided by nfs-utils. In a transition period, the **nfsiostat** binary from the sysstat packages is renamed to **nfsiostat-sysstat**. (BZ#846699)

iostat can now print device names longer than 72 characters

Previously, device names longer than 72 characters were truncated in the **iostat** command output because the device name field was too short. The allocated space for device names has been increased to 128 characters, and **iostat** can now print longer device names in the output. (BZ#1267972)

Copying sparse files with trailing extents using cp no longer causes data corruption

When creating sparse files, the **fallocate** utility could allocate extents beyond EOF using **FALLOC_FL_KEEP_SIZE**. As a consequence, when there was a gap (hole) between the extents, and EOF was within that gap, the final hole was not reproduced, which caused silent data corruption in the copied file due to its size being too small. With this update, the **cp** command ensures that extents beyond the apparent file size are not processed, as such processing and allocating is not currently supported. As a result, silent data corruption in certain type of sparse files no longer occurs. (BZ#1284906)

NFS shares mounted by autofs no longer cause timeouts when listing local mounts using df

A bug in **df** could previously cause **NFS** shares mounted by **autofs** to be detected as local mounts. Attempts to list only local mounts using the **-l** option then timed out, because **df** was attempting to list these incorrectly detected shares. This bug has been fixed, and listing local mounts now works as expected. (BZ#1309247)

ksh now correctly displays login messages

When logging in to an interactive login shell, the contents of the **/etc/profile** script are executed in order to set up an initial environment. Messages which should have been displayed to the user upon logging in to the Korn shell (ksh) were suppressed due to an internal test to determine whether the shell is a login shell that relied upon the value of the **PS1** environment variable having already been set before **/etc/profile** was executed. However, this environment variable is set in the Korn shell only after **/etc/profile** is executed, which led to messages never being displayed to **ksh** users. This update provides an alternative test that does not rely on the **PS1** variable being set before **/etc/profile** execution, with the result that messages are properly displayed to users of the Korn shell upon login. (BZ#1321648)

New POSIX semaphore destruction semantics

Previously, the implementation of POSIX semaphores in **glibc** did not follow the current POSIX requirements for semaphores to be self-synchronizing. As a consequence, the **sem_post()** and **sem_wait()** functions could terminate unexpectedly or return the EINVAL error code because they accessed the semaphore after it has been destroyed. This update provides an implementation of the new POSIX semaphore destruction semantics which keeps track of waiters, avoiding premature destruction of the semaphore. The semaphores implemented by **glibc** are now self-synchronizing, thus fixing this bug. (BZ#1027348)

Disks are now cleanly unmounted after SELinux automatic re-label

Previously, after SELinux relabel, the **rhel-autorelabel** script started system reboot by running the **systemctl --force reboot** command. Consequently, certain steps required to cleanly unmount the **rootfs** image and deactivate the underlying Device Mapper (DM) device were skipped. To fix this bug, the **rhel-autorelabel** script has been modified to invoke the **dracut-initframs-restore** script before the reboot. As a result, disks are now cleanly unmounted in the described scenario. (BZ#1281821)

sosreport now correctly collects output of sources with non-ASCII characters

Prior to this update, the sosreport was not fully generated when the **sosreport** utility attempted to collect the output of a file or command whose name included non-ASCII characters. With this update, such files and commands are properly collected and reported in the utility. (BZ#1296813)

Configuring kdump to an NFS target destination is now possible in the Kernel Dump Configuration GUI

Previously, the input box for NFS target destination in the Kernel Dump Configuration GUI did not indicate that an export path needs to be entered. Consequently, users were not able to configure the **kdump** feature to a NFS target destination when using this GUI. With this update, the input box label has been changed to indicate that an export path is required, and users are able to configure **kdump** in the described situation. (BZ#1208191)

Correct warning message when configuring kdump to a NFS target with NFS shares unmounted

Prior to this update, users were warned with confusing error messages when trying to configure the kdump to a NFS target destination if NFS shares were not mounted. The **system-config-kdump** utility operated through the Kernel Dump Configuration GUI, did not indicate that the NFS export needs to be mounted before applying the kdump configuration. Instead, multiple confusing error messages were returned. With this update the warning message has been changed to indicate that the NFS export is currently not mounted and that it should already be mounted in the moment of kdump configuration. This warning message is less confusing and provides the user with proper information on how to successfully complete the kdump configuration. (BZ#1121590)

lparstat no longer fails due to long lines in /proc/interrupts

Prior to this update, if the SPU line in the **/proc/interrupts** file was longer than 512 characters, using the **lparstat** command failed. With this update, **lparstat** properly parses interrupt lines, and thus returns correct results in the described circumstances. (BZ#1366512)

lparstat default output mode now reports properly

Previously, when using the default output mode of the **lparstat** utility, **lparstat** incorrectly reported the value of certain parameters, for example **physc**, as **0.00**. This problem has been fixed, and the affected values are now displayed properly. (BZ#1347083)

The Socket::getnameinfo module now works correctly with tainted values

Previously, the Perl **Socket::getnameinfo** module failed to process tainted values. This update applies a patch and as a result, the module now works correctly with tainted values. (BZ#1200167)

The python-sphinx module no longer fails to build documentation

Previously, the man-page writer module of the python-sphinx package missed the **meta** and **inline** node visitors. As a consequence, building documentation could fail. A patch has been provided to add the missing node visitors and as a result, documentation now builds successfully. (BZ#1291573)

Programs no longer run out of memory when repeatedly listing available polkit actions

Previously, the **polkit** client library did not correctly free memory when listing available actions, which could cause programs to run out of memory and terminate. With this update, the library frees the memory correctly, and programs no longer crash in this scenario. (BZ#1310738)

unzip now supports non-latin and non-unicode encodings

Previously, **unzip** did not support non-latin and non-unicode encodings, so files with incorrect names could be created. With this update, **unzip** supports these encodings using the **-O** and **-I** options. For more information, run the **unzip -h** command. (BZ#1276744)

zlib now decompresses RFC1951 compliant files correctly

Previously, due to a bug in **zlib**, RFC1951 compliant files were not correctly decompressed. With this update, the bug has been fixed, and **zlib** decompresses RFC1951 compliant files correctly. (BZ#1127330)

The glibc times() function now supports NULL for the buffer

Previously, the **times()** function in glibc did not allow users to set a **NULL** value for the buffer. As a consequence, the function could cause the application using it to terminate unexpectedly. This update applies a patch and as a result, you can set a **NULL** value for the buffer and the kernel system call returns the expected results. (BZ#1308728)

iconv no longer adds a redundant shift sequence

Previously, a bug in the character conversion routines used by **iconv** for the IBM930, IBM933, IBM935, IBM937, and IBM939 character sets could result in a redundant shift sequence being included in the output of the tool. The generated non-conforming output could result in an inability to read the output data. The character conversion routines have been fixed and no longer return a redundant shift sequence. (BZ#1293916)

Core C library (glibc) enhanced to increase malloc() scalability

A defect in the implementation of the **malloc()** function could result in unnecessary serialization of memory allocation requests across threads. This update fixes the bug and substantially increases the concurrent throughput of allocation requests for applications that frequently create and destroy threads. (BZ#1276753)

Dynamic linker no longer fails when an audit module provides alternate DSO

Previously, when an audit module provided an alternate DSO (dynamic shared object) path, the **ld.so** dynamic linker terminated unexpectedly with a segmentation fault. This update fixes the bug and the dynamic linker now keeps track of the original DSO path for future reference and no longer crashes in the described scenario. (BZ#1211100)

selinux-policy now allows hypervkvpd to getattr on all filesystem types

Previously, an SELinux denial occurred during the execution of the **restorecon** command after an IP injection on the virtual machine with the **Data Exchange** option enabled. The selinux-policy packages have been updated, and an IP injection now finishes correctly both in SELinux permissive and enforcing mode. (BZ#1349356)

CHAPTER 26. DESKTOP

`Poppler` no longer renders certain characters incorrectly

Previously, the **`Poppler`** library did not map correctly to character code. As a consequence, **`Poppler`** showed the **`fi`** string instead of showing the correct glyph, or nothing, if the font did not contain necessary glyphs. With this update, the characters previously replaced with the **`fi`** string are shown correctly. (BZ#1298616)

`Poppler` no longer tries to access memory behind the array

Memory corruption due to exceeding the length of array caused the **`Poppler`** library to terminate unexpectedly. A fix has been applied to not allow **`Poppler`** to try to access memory behind the array, and **`Poppler`** no longer crashes in the described situation. (BZ#1299506)

`pdftocairo` no longer crashes when processing a PDF without group color space

Previously, the **`Poppler`** library tried to access a non-existing object when processing a PDF without group color space. As a consequence, the **`Poppler`** library terminated unexpectedly with a segmentation fault. A patch has been applied to verify if group color space exists. As a result, **`Poppler`** no longer crashes, and the **`pdftocairo`** utility works as expected in the described situation. (BZ#1299479)

`Poppler` no longer terminates unexpectedly during text extraction

Previously, a writing after the end of the lines array could cause a memory corruption. As a consequence, the **`Poppler`** library could terminate unexpectedly. A patch has been applied and array is now always relocated when an item is added. As a result, **`Poppler`** no longer crashes in the described situation. (BZ#1299481)

`Poppler` no longer terminates unexpectedly due to a missing `GfxSeparationColorSpace` class

Previously, the **`Poppler`** library tried to copy a non-existing **`GfxSeparationColorSpace`** class and as a consequence terminated unexpectedly. With this update, **`Poppler`** now checks for existence of the **`GfxSeparationColorSpace`** class, and as a result no longer crashes in the described situation. (BZ#1299490)

`pdfinfo` no longer terminates unexpectedly due to asserting broken encryption information

Previously, Poppler tried to obtain broken encryption owner information. As a consequence, the **`pdfinfo`** utility to terminate unexpectedly. A fix has been applied to fix this bug, and **`Poppler`** no longer asserts broken encryption information. As a result, **`pdfinfo`** no longer crashes in the described situation. (BZ#1299500)

`Evince` no longer crashes when viewing a PDF

Previously, screen annotation and form fields passed a NULL pointer to **`_poppler_action_new`**, and **`Poppler`** created a false **`PopplerAction`** when viewing certaing PDFs in the **`Evince`** application. As a consequence, **`Evince`** terminated unexpectedly with a segmentation fault. A patch has been applied to modify **`_poppler_annot_scren_new`** and **`poppler_form_field_get_action`** to pass **`PopplerDocument`** instead of NULL. As a result, **`Evince`** no longer crashes in the described situation. (BZ#1299503)

Virtual machines started by GNOME Boxes are no longer accessible to every user

Previously, virtual machines started by GNOME Boxes were listening on a local TCP socket. As a consequence, any user could connect to any virtual machine started by another user. A patch has been applied and GNOME Boxes no longer opens such sockets by default. As a result the virtual machines

are now accessible through SPICE only to the user who owns the virtual machine. (BZ#1043950)

GNOME boxes rebased to version 3.14.3.1

The **GNOME boxes** application has been updated to version 3.14.3.1. Most notably,a patch to one bug has been applied as a part of this rebase:

- Previously, the virtual network computing (VNC) authentication parameters in the **GNOME boxes** application were not handled correctly. As a consequence, the connections to VNC servers with authentication failed. This bug has been fixed and the connection to VNC servers with authentication now works as expected. (BZ#1015199)

FreeRDP now recognizes wildcard certificates

Previously, wildcard certificates support was not implemented in FreeRDP. As a consequence, wildcard certificates were not recognized by **FreeRDP**, and the following warning was displayed when connecting:

```
WARNING: CERTIFICATE NAME MISMATCH!
```

Missing functionality has been backported from upstream and code for comparing host names was improved. As a result, the mentioned prompt is no longer shown if a valid wildcard certificate is used. (BZ#1275241)

Important security updates now installed automatically

Previously, it was not possible to have security updates installed automatically. Even though GNOME notified the users about the available updates, they could choose to ignore the notification and not install the update. As a consequence, important updates could be left uninstalled. A gnome-shell extension is now available to enforce the installation of important updates. As a result, when new updates are available, a dialog window notifies the user that updates will be applied and they need to save their work. After a configurable amount of time, the system reboots to install the pending updates. (BZ#1302864)

Accounts' shells in accountsservice now always verified

The accountsservice package heuristics for determining disabled accounts changed between Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7. As a consequence, users with UID outside of the range 500 - 1000 would appear in the user list even if their shell was invalid. A patch has been applied to always verify the account's shell before the account is treated as a listable user account. As a result, the users with **/sbin/nologin** as a shell are now filtered out. (BZ#1341276)

New way to handle desktop in Nautilus 3

Previously, icons in Nautilus 3 on the desktop were managed by taking the biggest monitor and trying to adapt the desktop window to the minimum common shape that would fit a rectangle. As a consequence, the icons could not be placed in random areas in some of the monitors, which could cause confusion for the user. This behavior has been changed to restrict the desktop window shape to the primary monitor. Even though this change does not allow to use all available monitors as part of the desktop, it fixes the described bug. (BZ#1207646)

GLX support in Xvnc sessions

The GLX support code in Xvnc requires the use of the libGL library. If a third-party driver was installed and replaced libGL, Xvnc sessions launched with no GLX support. Consequently, 3D applications did not work under Xvnc. With this update, Xvnc has been rebuilt to require libGL, which is assumed to be installed in **/usr/lib64/**. Now, third-party drivers installed in a sub-directory no longer conflict with Xvnc, which now initializes GLX successfully. As a result, GLX functionality is available again in Xvnc sessions.

Note that client applications connecting to Xvnc need to use the same libGL version as the Xvnc server, which may require the use of the **LD_LIBRARY_PATH** environment variable. (BZ#1326867)

Flat document collections

When using the **gnome-documents** application, it was possible include one collection into another and then vice versa at the same time. Consequently, the application terminated unexpectedly. This update ensures that the collections are flat and do not allow circular chains of collections, thus fixing this bug. (BZ#958690)

control-center no longer crashes when querying with special characters

Previously, text entered by users when searching for a new printer required a specific character-set. Consequently, the **control-center** utility could terminate unexpectedly when searching for a printer name that contained a special character. With this update, the text is encoded into a valid ASCII format. As a result, **control-center** no longer crashes and correctly queries for printers. (BZ#1298952)

gnome-control-center no longer crashes because of zero-length string

Previously, the **gnome-control-center** utility worked with an empty string and an invalid pointer. As a consequence, it terminated unexpectedly. The **gnome-control-center** utility now checks whether the given application's identifier is at least 1 character long and initializes the **new_app_ids** pointer. As a result, the stated problem no longer occurs. (BZ#1298951)

The Release Notes package is now installed correctly

Previously, due to the naming of the Red Hat Enterprise Linux Release Notes packages, the packages were not installed on systems with a different language configured than English. This update provides additional parsing rules in the yum-languagepacks package. As a result, the Release Notes package is now installed correctly. (BZ#1263241)

The LibreOffice language pack is now installed correctly for pt_BR, zh_CN, and zh_TW localizations

Previously, translated libreoffice-langpack packages were not automatically installed on systems using language packs for the **pt_BR**, **zh_CN**, and **zh_TW** localizations. Parsing rules have been added to the **yum** language plug-in to address the problem. As a result, the correct LibreOffice language pack is installed. (BZ#1251388)

CHAPTER 27. FILE SYSTEMS

The `quota` RPC service is no longer unavailable

After upgrading the **`nfs-utils`** packages, the **`nfs-rquotad.service`** systemd service was previously unavailable on the system after starting the **`quota`** Remote Procedure Call (RPC) service. To fix this bug, the **`quota`** packages now include a new **`rpc-rquotad.service`** *systemd* service, which provides the **`quota`** RPC service that allows querying and setting disk quotas over a network. The service can be configured in the **`/etc/sysconfig/rpc-rquotad`** file. The **`nfs-rquotad`** service alias is also provided to ensure compatibility with earlier versions. As a result, the **`quota`** RPC service is now available on Red Hat Enterprise Linux 7 as expected in the described situation. (BZ#1207239)

`repquota` now reports quotas for users not defined in the local `passwd` database

When listing all users' quotas with **`repquota`** tool on an XFS file system when some users were defined only in the LDAP directory, quotas for users that were not defined in the local **`passwd`** database were previously not reported by **`repquota`**. Now, a new kernel interface, the **`Q_GETNEXTQUOTA`** and **`Q_XGETNEXTQUOTA`** quota **`IOCTL`** commands, is used, if available, to retrieve all quota entries stored in a file system. This new method does not require enumerating all user accounts and works even for users unknown to the local system. As a result, **`repquota`** reports quotas for all users even if a user account is retrieved from a remote LDAP server or the System Security Services Daemon (SSSD) caches the user accounts. (BZ#1305968)

`quota` now correctly reports the grace time

Previously, the integer type was misinterpreted if the **`quota`** tool displayed the grace time for an NFS-mounted file system if the soft quota limit for the current user was exceeded, and the grace quota time already expired. As a consequence, the **`quota`** command incorrectly reported a large number of days instead of the **none** value. This update fixes the misinterpretation of the integer type used to transfer grace times over the network. In addition, this update limits the range of possible values to 32-bit signed integer boundaries to ensure interoperability between NFS servers and clients with a different CPU word size. As a result, the **`quota`** tools correctly report grace time that differs from the server time in the range from -2^31+1 to 2^31 seconds. Lower values are reported as expired, and higher as a maximal possible time that stays unchanged until the difference is in the correct range. (BZ#1072858)

`cifs.idmap` now maps SIDs to UIDs

Previously, the **`cifs.idmap`** tool could not map SIDs to UIDs in Red Hat Enterprise Linux 7. As a consequence, **`cifs.idmap`** could not be used to map ownership to the user name or group name from the Active Directory (AD). The Makefile has been modified to verify that the correct build options are presented to ensure that the mapping works. As a result, the mapping in **`cifs.idmap`** now works as expected. (BZ#1289454)

`cifs-utils` rebased to version 6.2

The **`cifs-utils`** packages have been upgraded to upstream version 6.2, which provides a number of bug fixes over the previous version. The following bug fixes are included:

- Unnecessary linking of **`libwbclient`** is prevented.
- Uppercase **`orig_dev`** on 2nd try at mounting.
- **`paths.h`** is included in **`mtab.c`**
- The use of **`backupuid`** and **`backupgid`** is clarified in the manual pages.
- The **`x-*`** mount options are included. (BZ#1351618)

CHAPTER 28. HARDWARE ENABLEMENT

Primary bond interface no longer takes over active interfaces that did not fail

The primary_reselect=failure bond parameter previously worked incorrectly. The primary interface was always taking over even if others did not fail. With this update, the parameter works as expected and the primary bond interface only takes over if the current non-primary active interface fails. (BZ#1301451)

Memory corruption is prevented on a failed `updatepp` operation on the little-endian variant of IBM Power Systems

Previously, a failed **`updatepp`** operation on the little-endian variant of IBM Power Systems sometimes caused a wrong hash value to be used for the next hash insert operation in the page table. This could cause an update hash page table entry (PTE) operation or an invalidate hash PTE operation to be missed, potentially resulting in memory corruption. With this update, the hash value is always recalculated after a failed **`updatepp`** operation, which prevents the potential memory corruption. (BZ#1264920)

Removing a USB device no longer causes a race condition

Previously, removing a USB device caused a problem in synchronization, which could lead to a race condition. Consequently, the memory became corrupted, which caused the USB host controller to fail. With this update, the timer is initialized early enough, which prevents the possibility of a race condition, and the USB host controller no longer fails. (BZ#1290202)

The kernel now boots on AMD Turion II systems

Previously, because of a livelock in the tick broadcast code, AMD Turion II systems in some cases locked up and became unresponsive during boot. With this update, the livelock is fixed, and the kernel now boots more reliably on AMD Turion II systems. (BZ#1265283)

Real-time systems with many CPUs no longer have large latencies due to run-queue lock contention

Previously, on real-time systems, multiple CPUs tried to take an **`rq`** lock, which resulted in lock contention and latency. The latency was multiplied by the number of CPUs, which caused the systems with many CPUs to have large latencies. With this update, systems with more than 32 cores use the **`push`** approach rather than **`pull`**, which prevents long lists of CPUs in critical areas. As a result, real-time systems with many CPUs no longer have large latencies due to run-queue lock contention. (BZ#1209987)

The kernel no longer crashes at boot when enabling multi-queue support with NVM Express device driver

Due to a bug in the core block device code, the kernel in some cases terminated unexpectedly at boot, when enabling multi-queue support on the Nonvolatile Memory Express (NVMe) device driver. The problem was observed with the nvme driver, but other block devices were also potentially affected. With this update, this bug has been fixed, and the kernel no longer crashes in the described circumstances. (BZ#1303255)

The CPU frequency now reaches the requested value

Previously, the CPU frequency values were rounded incorrectly by the **`intel_pstate`** driver. Consequently, the CPU frequency was lower than the user requested. With this update, the rounding errors have been fixed, and the CPU frequency now reaches the requested value. (BZ#1279617)

Real-time kernel scheduling code for FCoE code has been fixed

The real-time kernel's Fibre Channel over Ethernet (FCoE) driver was changed to use the **`get_cpu_light()`** and **`put_cpu_light()`** functions, rather than the more common **`get_cpu()`** and **`put_cpu()`** functions. However, one occurrence of **`get_cpu()`** was not changed to

get_cpu_light(). Consequently, preemption was disabled, and the **BUG: scheduling while atomic** bug occured in the FCoE code. With this update, the code has been fixed and the bug no longer occurs. (BZ#1258295)

The performance of IBM Power Systems is no longer decreased by NUMA nodes not being reported for PCI adapters

Previously, due to a regression, the Non-Uniform Memory Access (NUMA) node was not reported for PCI adapters. This caused significant decrease in the performance of every IBM Power System deployed with Red Hat Enterprise Linux 7. With this update, the regression has been fixed, and the system performance is no longer decreased in this situation. (BZ#1273978)

The system no longer crashes while setting up the DMA transfer

Due to the inconsistencies in the page size of Input/Output Memory Management Unit (IOMMU), the Non-volatile Memory Express (NVMe) device, and the kernel, the **BUG_ON** signal previously occurred in the **nvme_setup_prps()** function. This could lead to an unexpected termination of the system while setting up the Direct Memory Access (DMA) transfer. With this update, the default NVMe page size is set to 4 kilobytes, and the system crash no longer occurs. (BZ#1245140)

Kernel no longer hangs during hot-unplug

Due to retry-able command errors, the NVMe driver previously leaked I/O descriptors and DMA mappings. As a consequence, the kernel could become unresponsive during the hot-unplug operation if a drive was removed. This update fixes the driver memory leak on command retries, and the kernel no longer hangs in this situation. (BZ#1271860)

Disabling the Large Receive Offload (LRO) flag now propagates correctly

Previously, disabling the Large Receive Offload (LRO) flag was not propagated downwards from above devices in vlan and bond hierarchy. Consequently, the flow of traffic broke. With this update, the problem has been fixed and disabling of LRO flags now propagates correctly. (BZ#1266578)

Switching P-states on Intel Xeon v5 platforms now succeeds

Previously, on Intel Xeon v5 platforms, the processor frequency was always tied to the highest possible frequency. As a consequence, switching P-states on these client platforms failed. This update sets the idle frequency, busy frequency, and processor frequency values by determining the range and adjusting the minimum and maximum percent limits values. As a result, switching P-states on these client platforms now succeeds. (BZ#1264990)

The cpuscaling test no longer fails

Previously, the **cpuscaling** test of the Red Hat Hardware Certification Test Suite incorrectly failed due to a number-rounding bug in the **intel-pstate** driver. This bug has been fixed and the **cpuscaling** test now passes on sufficiently powerful hardware. (BZ#1263866)

The genwqe driver can allocate memory during memory pressure

The **genwqe** device driver was previously using the **GFP_ATOMIC** flag for allocating consecutive memory pages from the kernel's atomic memory pool - even in non-atomic situations. This could lead to allocation failures during memory pressure. With this update, the **genwqe** driver's memory allocations use the **GFP_KERNEL** flag, and the driver can allocate memory even during memory pressure situations. (BZ#1270244)

The console no longer hangs when disabling CPU

Previously, when disabling a CPU using the CPU **hotplug** interface in the real-time kernel, the **hotplug** lock and the console semaphore could be acquired in an incorrect order. This could lead to a deadlock causing the system console to become unresponsive. With this update, the locks are acquired in the correct order, and console no longer hangs. (BZ#1269647)

LRO is now disabled by default in the `ixgbe` driver

Because Large Receive Offload (LRO) is incompatible with forwarding and bridging and can cause performance problems and instability, it is now disabled by default in the **ixgbe** driver.

To enable LRO:

```
# ethtool -K ethX lro on
```

Replace **ethX** with the name of the interface. (BZ#1266948)

The nx842 co-processor for IBM Power Systems no longer provides corrupted data

Previously, the nx842 co-processor for IBM Power Systems could in some circumstances provided invalid data. This was caused by a data corruption bug that occured during uncompression. With this update, all compression and uncompression calls to the nx842 co-processor contain a cyclic redundancy check (CRC) flag. This forces all compression and uncompression operations to check data integrity and prevents the co-processor from providing corrupted data. (BZ#1264905)

The system no longer crashes when calling the `mlx4_en_recover_from_oom()` function

Previously, when the **mlx4_en_recover_from_oom()** function was invoked under heavy TCP stream by the **mlx4_en** drive, the operating system terminated unexpectedly. This update fixes the bug, and the system no longer crashes in this scenario. (BZ#1258136)

`iw` displays regulatory information correctly

Previously, the **iw** utility did not correctly display the regulatory country after it was set with the **iw reg set** command. This update adjusts the **iw** code to match the Red Hat Enterprise Linux wireless code more closely. As a result, **iw** displays the regulatory country information as expected. (BZ#1324096)

`i40e` no longer issues `warn_slowpath` warnings during boot

Previously, the **i40e** driver was issuing **warn_slowpath** warnings during a ring size change because the code was cloning the **rx_ring** struct but not zeroing out the pointers before allocating new memory. With this update, the bug is fixed, and the warnings are no longer shown. (BZ#1272833)

The `netprio_cgroups` module is now mounted at boot

Previously, **systemd** mounted the **/sys/fs/cgroup/** directory as read-only, which prevented mounting of the **/sys/fs/cgroup/net_prio/** directory during the initial system setup. Consequently, the **netprio_cgroups** module was not mounted at boot. With this update, this problem has been fixed, and the **netprio_cgroups** module is now mounted at boot. (BZ#1262204)

Setting up bonding with `qlcnic` no longer fails

Prior to this update, certain bonding modes, such as **balance-tlb** or **balance-alb**, set a MAC address that was not properly stored. This MAC address was not restored when tearing down the bond, leaving a duplicate MAC in place. Consequently, re-establishing a bond failed, because the original MAC address was not present. This update improves the code to properly restore the MAC addresses when the bonding is taken down. As a result, bonding with **qlcnic** devices works as expected. (BZ#1265058)

CHAPTER 29. INSTALLATION AND BOOTING

Graphics cards using the `ast` module can now be used during installation

Due to missing dependencies for the **`ast`** module in the installation system, graphics cards that rely on this module were unable to be used during installation of Red Hat Enterprise Linux 7. These dependencies have now been added. (BZ#1272658)

Installations can now be performed on disks containing invalid or unsupported partition tables.

Previously, when attempting to install Red Hat Enterprise Linux 7 on a disk with a corrupt or unsupported partition table, the installation failed, most commonly when attempting to write to the disk. Support for the removal of invalid and unsupported partition tables has been added, and installations can now be performed on disks with such partition tables. (BZ#1266199)

Multiple `inst.dd` options are now supported to load driver disks

The job for loading driver disks based on the **`inst.dd`** option was scheduled with a unique option. When multiple **`inst.dd`** sources were specified as boot options, only the last one was actually loaded and applied. This update ensures the job is no longer called as unique. As a result, multiple **`inst.dd`** boot options can now be specified to provide drivers via multiple driver update images from different sources. (BZ#1268792)

Help for the subscription manager screen during installation

The installer's built-in help system now includes information regarding the subscription manager screen. (BZ#1260071)

The `Initial Setup` utility starts correctly

Due to a race condition between the **`initial-setup-text`** service and the **`initial-setup-graphical`** service, the interface of the **`Initial Setup`** utility sometimes started incorrectly. The two services have now been combined into a single service, **`initial-setup`**. The original services are still available for compatibility, but are not used by default. As a result, the interface now displays correctly. (BZ#1249598)

VNC installation using IPv6 works correctly

Due to an error in the processing of IPv6 addresses, IPv6 address lookup failed. Consequently, it was not possible to install through VNC using IPv6. This bug has been fixed. (BZ#1267872)

HyperPAV aliases used during installation are now available on the installed system

Previously, HyperPAV aliases activated during installation were not correctly configured on the installed system. HyperPAV handling has now been improved, and any HyperPAV aliases used during installation are now automatically configured on the installed system. (BZ#1031589)

Errors in custom partitioning are correctly detected

Previously, errors in custom partitioning were not displayed to the user properly, allowing the installation to continue with an invalid custom partition configuration, leading to unexpected behavior. This bug has been fixed and errors in custom partitioning are now correctly reported to the user so they can be adjusted before continuing the installation. (BZ#1269195)

Static routes configured during installation are now automatically configured on the installed system

Previously, static route configuration files were not copied from the installation environment to the installed system. Consequently, static route configuration during installation was lost after the installation finished. These files are now copied, and static routes configured during installation are automatically configured on the installed system. (BZ#1255801)

The `grub2-mkconfig` utility now honors certain `grubby` configuration variables

Previously, when **grubby** added some entries to the **grub** configuration file, **debug** entries in particular, **grub2-mkconfig** failed to recognize and replicate those entries when re-run. This update ensures that if **MAKEDEBUG=yes** is specified in **/etc/sysconfig/kernel**, **grub2-mkconfig** does replicate the new **grubby** configuration entries. (BZ#1226325)

`GRUB2` is now correctly configured when upgrading the kernel and redhat-release-*

Previously, if a redhat-release-* package and a kernel package were present in the same **Yum** transaction, the **GRUB2** boot loader was reconfigured incorrectly. As a consequence, **GRUB2** failed to boot the newly installed kernel. With this upate, **GRUB2** is now correctly reconfigured and can boot the new kernel in this situation. (BZ#1289314)

Kickstart files valid for Red Hat Enterprise Linux 6 are now correctly recognized by `ksvalidator`

Previously, when using the **ksvalidator** utility to validate a Kickstart file made for Red Hat Enterprise Linux 6 that uses the **logvol** command with the **--reserved-percent** option, **ksvalidator** incorrectly stated that **--reserved-percent** is not a valid option. This bug has been fixed. (BZ#1290244)

`Anaconda` no longer crashes when adding iSCSI devices

Previously, the **Anaconda** installer terminated unexpectedly when attempting to add certain iSCSI devices using the **Add a disk** button in the **Storage** screen. This bug has now been fixed. (BZ#1255280)

The `Anaconda` installer correctly allows adjustment of a problematic disk selection

Previously, if a problem occurred with the selection of disks during installation of Red Hat Enterprise Linux 7, an error was displayed after the installation started, and thus caused the installation to fail. With this update, a warning is displayed at the proper time, allowing the disk selection to be adjusted before proceeding. (BZ#1265330)

The anaconda-user-help package is now upgraded correctly

The anaconda-user-help package was not upgraded correctly when upgrading from Red Hat Enterprise Linux 7.1. This has been fixed and the package is now upgraded correctly. (BZ#1275285)

A wider variety of partitions can be used as `/boot`

Previously, the GRUB2 boot loader only supported 8-bit device node minor numbers. Consequently, boot loader installation failed on device nodes with minor numbers larger than **255**. All valid Linux device node minor numbers are now supported, and as a result a wider variety of partitions can be used as **/boot** partitions. (BZ#1279599)

Incorrect escaping of the `/` character in `systemd` no longer prevents the system from booting

Previously, **systemd** incorrectly handled the **LABEL=/** option in the initial RAM disk (initrd). As a consequence, the label was not found, and the system failed to boot when the root partition LABEL included the **/** character. With this update, **/** is escaped correctly in the described situation, and the system no longer fails to boot. Updating to a higher minor version of Red Hat Enterprise Linux updates the kernel and rebuilds the **initrd**. You can also rebuild the **initrd** by running the **dracut -f** command. (BZ#1306126)

The default size of the `/boot` partition is now 1 GB

In previous releases of Red Hat Enterprise Linux 7, the default size of the **/boot** partition was set to 500 MB. This could lead to problems on systems with multiple kernels and additional packages such as kernel-debuginfo installed. The **/boot** partition could become full or almost full in such scenario, which

then prevented the system from upgrading and required manual cleanup to free additional space.

In Red Hat Enterprise Linux 7.3, the default size of the **/boot** partition is increased to 1 GB, and these problems no longer occur on newly installed systems. Note that installations made with previous versions will not have their **/boot** partitions resized, and may still require manual cleanup in order to upgrade. (BZ#1369837)

`biosboot` and `prepboot` are now included in the Kickstart file after installation

When a Kickstart file included instructions to create **biosboot** or **prepboot** partitions, the Blivet module did not pass this information in Kickstart data. Consequently, after a Kickstart installation, the Kickstart file on the newly installed system did not include the options for creating **biosboot** and **prepboot** partitions and could not be reused successfully on other systems. With this update, the Kickstart output includes these options as expected, and the Kickstart file can be used on other systems to create the **biosboot** and **prepboot** partitions. (BZ#1242666)

`os-prober` now uses device mapper alias names in the boot loader configuration

The **os-prober** component previously used the numeric device mapper device in the boot loader configuration. After reboot, when the installer disk image was no longer mounted, the number changed, which rendered the boot entry unusable. Consequently, when two instances of Red Hat Enterprise Linux were installed on one machine, one of them failed to boot. To fix this bug, **os-prober** now uses device mapper alias names instead of the direct enumerated device mapper names. Because the alias names are more stable, the boot entry works as expected in the described situation. (BZ#1300262)

Installations on IBM z Systems now generate correct Kickstart files

Previously, the **anaconda-ks.cfg** file, which is a Kickstart file generated during system installation and which contains all selections made during the install process, was representing disk sizes as decimal numbers when installing on IBM z Systems DASDs. This bug caused the Kickstart file to be invalid because only integers are accepted when specifying disk size, and users had to manually edit the file before using it to reproduce the installation. This bug has been fixed, and Kickstart files generated during installation on IBM z Systems can now be used in subsequent installations without any editing. (BZ#1257997)

Formatting DASDs works correctly during a text-based installation

Previously, a bug prevented DASDs from being correctly formatted during a text-based installaton. As a consequence, DASDs that were unformatted or incorrectly formatted had to be manually formatted before use. This bug has been fixed, and the installer can now format DASDs when performing a text-based installation. (BZ#1259437)

Initial Setup now displays the correct window title

The Initial Setup tool, which is automatically displayed after the first post-installation reboot and which allows you to configure settings like network connections and to register your system, previously displayed an incorrect string **__main__.py** in the window title. This update fixes the bug. (BZ#1267203)

Installation no longer fails when using `%packages --nobase --nocore` in a Kickstart file

Previously, using a Kickstart file which contained the **%packages** section and specified the **--nobase** and **--nocore** options at the same time caused the installation to fail with a traceback message due to a missing yum-langpacks package. The package is now available, and the described problem no longer occurs. (BZ#1271766)

CHAPTER 30. KERNEL

A fix of PT_NOTE entries that were previously corrupted during crashdump

On some HP servers, a kernel crash could lead to the corruption of PT_NOTE entries because of a kernel code defect. As a consequence, the kernel crash dump utility failed to initialize. The provided patch aligns the allocation of PT_NOTE entries so that they are inside one physical page, and thus written and read data is identical. As a result, kernel crash dump now works as expected in the described situation. (BZ#1073651)

Removal of the `slub_debug` parameter to save memory

The **slub_debug** parameter enables debugging of the SLUB allocator, which makes each object consume extra memory. If the **slub_debug** kernel parameter was used, not enough memory was allocated to the **kdump** capture kernel by the automatic setting on 128 GB systems. Consequently, various tasks from the **kdump** init script terminated with an Out Of Memory (OOM) error message and no crash dump was saved. The provided patch removes the **slub_debug** parameter, and crash dump is now saved as expected in the aforementioned scenario. (BZ#1180246)

Removal of a race condition causing a deadlock when a new CPU was attached

Previously, when a new CPU was attached, a race condition between the CPU hotplug and the stop_two_cpus() function could occur causing a deadlock if that migration thread on the new CPU was already marked as **active** but not **enabled**. A set of patches has been applied which removes this race condition. As a result, systems with attached new CPUs now run as intended. (BZ#1252281)

Update of the kernel with hugepage migration patches from the upstream

Previously, several types of bugs including the kernel panic could occur with the hugepage migration. A set of patches from the upstream has been backported which fix these bugs. The updated kernel is now more stable and hugepage migration is automatically disabled in architectures other than AMD64 and Intel 64. (BZ#1287322)

Booting kernel with UEFI and the secure boot enabled

When the Unified Extensible Firmware Interface (UEFI) was used and the secure boot was enabled, the operating system failed to boot for all kernels since the 3.10.0-327.3.1.el7.x86_64 kernel. With the update to the 3.10.0-327.4.4.el7 kernel and newer versions the system boots up as expected. (BZ#1290441)

New microcode added into initramfs images for all installed kernels

Previously, when the microcode_ctl package was installed, the postinstall scriptlet rebuilt the initramfs file only for the running kernel and not for any other installed kernels. Consequently, when the build completed, there was an initramfs file for a kernel that was not even installed. The provided fix adds new microcode into initramfs images for all installed kernels. As a result, the superfluous initramfs file is no longer generated. (BZ#1292158)

kernel `slab` errors caused by a race condition in GFS2 no longer occur

A race condition previously occurred in the GFS2 file system in which two processes simultaneously tried to free kernel **slab** memory used for directory lookup. As a consequence, when both processes freed the same memory, a **slab** memory error occurred in the kernel. The GFS2 file system has been patched to eliminate the race condition, and a process now cannot try to free the memory that has already been freed by another process. Now, each process is forced to take turns when trying to free the memory. As a result, kernel **slab** errors no longer occur. (BZ#1276477)

GFS2 now writes data to the correct location within the file

Previously, the GFS2 file system miscalculated the starting offset when writing files opened with **O_DIRECT** (Direct I/O) at a location larger than 4 KB. As a consequence, the data was written to an incorrect location in the file. GFS2 has been patched to calculate the correct file offset for Direct I/O

writes. As a result, GFS2 now writes data to the correct location within the file. (BZ#1289630)

Dump-capture kernel memory freed when kdump mechanism fails

When crashkernel memory was allocated using the **,high** and **,low** syntax, there were cases where the reservation of the high portion succeeded but with the reservation of the low portion the kdump mechanism failed. This failure could occur especially on large systems for several reasons. The manually specified crashkernel low memory was too large and thus an adequate memblock region was not found. The kexec utility could load the dump-capture kernel successfully, but booting the dump-capture kernel failed, as there was no low memory. The provided patch set reserves low memory for the dump-capture kernel **after** the high memory portion has been allocated. As a result, the dump-capture kernel memory is freed if the kdump mechanism fails. The user thus has a chance to take measures accordingly. (BZ#1241236)

The ksc utility no longer fails to file bugs due to the unavailable kabi-whitelists component

In an earlier update, the **kabi-whitelists** component was changed to the **kabi-whitelists** sub-component of the kernel component. Consequently, the ksc utility was not able to file bugs, as the **kabi-whitelists** component value was not active, and the following error message was generated:

```
Could not create bug.<Fault 32000:"The component value 'kabi-whitelists'
is not active">
```

With this update, the correct sub-component of the kernel component is kabi-whitelisted, and ksc files bugs as expected. (BZ#1328384)

ksc now returns an error instead of crashing when running without mandatory arguments

Previously, the **ksc** tool terminated unexpectedly when running without the mandatory arguments. With this update, **ksc** returns an error message and exits gracefully in the described situation. (BZ#1272348)

ext4 file systems can now be resized as expected

Due to a bug in the ext4 code, it was previously impossible to resize ext4 file systems that had 1 kilobyte block size and were smaller than 32 megabytes. A patch has been applied to fix this bug, and the described ext4 file systems can now be resized as expected. (BZ#1172496)

Unexpected behavior when attaching a qdisc to a virtual device no longer occurs

Previously, attaching a qdisc to a virtual device could result in unexpected behavior such as packets being dropped prematurely and reduced bandwidth. With this update, virtual devices have a default **tx_queue_len** of 1000 and are represented by a device flag. Attaching a qdisc to a virtual device is now supported with default settings and any special handling of the **tx_queue_len=0** is no longer needed. (BZ#1152231)

The udev daemon is no longer stopped by dracut

Previously, a dracut script in the **initramfs** process stopped the **udev** daemon by using the **udevadm control** command, which caused the **udev** daemon to exit. However, the **systemd** service policy is to restart the daemon. Under certain circumstances, this prevented the system from booting. With this update, the code to stop the **udev** daemon has been removed from the dracut script, which avoids the described problem. (BZ#1276983)

multi-fsb buffer logging has been fixed

Previously, directory modifications on XFS filesystems with large directory block sizes could lead to a kernel panic and consequent server crash due to the problems with logging the multi-block buffers. The provided patch fixes the multi-fsb buffer logging, and the servers no longer crash in this scenario. (BZ#1356009)

Hard screen lock-up no longer occurs on laptops using integrated graphics in the 6th Generation Intel Core processors

On laptops using integrated graphics in the 6th Generation Intel Core processors, hard screen lock-up previously sometimes occurred when:

- Moving the cursor between the edges of the monitor
- Moving the cursor between multiple monitors
- Changing any aspect of the monitor configuration
- Docking or undocking the machine
- Plugging or unplugging a monitor

The bug has been fixed, and the hard lock-up of the screen no longer occurs in these situations. (BZ#1341633)

Multiple problems fixed on systems with persistent memory

Several problems sometimes occurred during boot on systems with persistent memory, either real Non-Volatile Dual In-line Memory Modules (NVDIMMs) or emulated NVDIMMs using the **`memmap=X!Y`** kernel command-line parameter.

The onlining of persistent memory caused the following messages to be displayed for every block (128 MB) of **`pmem`** devices:

```
Built 2 zonelists in Zone order, mobility grouping on.  Total pages:
8126731
Policy zone: Normal
```

The system became unresponsive.

The following **`BUG`** message was displayed:

```
BUG: unable to handle kernel paging request at ffff88007b7eef70
```

This update fixes the described bugs. (BZ#1367257)

`python` errors no longer appear when `SUDO_USER` and `USER` variables are not set

Previously, when executing in spare environments that do not have **`SUDO_USER`** or **`USER`** environment variables set, a number of **`python`** errors appeared. With this update, undefined **`SUDO_USER`** and **`USER`** variables are handled correctly, and the errors no longer appear. (BZ#1312057)

CIFS anonymous authentication no longer fails

Previously, the **`cifs`** module set values incorrectly for anonymous authentication. Changes made to the **`samba`** file server exposed this bug. As a consequence, anonymous authentication failed. This update changes the behavior of the client and sets the correct **`auth`** values for anonymous authentication. As a result, CIFS anonymous authentication now works correctly. (BZ#1361407)

CHAPTER 31. NETWORKING

`libcurl` successfully communicates with servers requiring HTTP host name to match the TLS session host name

Previously, in some cases, Network Security Services (NSS) incorrectly reused a TLS session for a server with a different host name. Consequently, HTTPS servers could respond with an HTTP error 400 (Bad Request). An upstream patch has been applied on the source code of the **`libcurl`** library to prevent NSS from reusing a TLS session in case the HTTP host name does not match the TLS session host name. As a result, **`libcurl`** can now successfully communicate with servers that require HTTP host name to match the TLS session host name. (BZ#1269855)

`curl` no longer requires a public key specified by the user

Prior to this update, the **`curl`** utility required both private and public SSH keys (paired with each other) for user authentication. Consequently, if a user provided only the private SSH key, which is a common practice with the **`scp`** utility, **`curl`** failed to authenticate the user. An upstream patch has been applied to improve the SSH user authentication, and **`curl`** now authenticates the user successfully also in case only a private SSH key is provided. (BZ#1275769)

`libcurl` no longer truncates long user names and passwords

The URL parser in the **`libcurl`** library previously did not support arbitrarily long user names and passwords. Consequently, user names and passwords longer than 255 characters were truncated. A series of upstream patches has been applied on the **`libcurl`** source code, and long user names and passwords in the URLs are now processed correctly by **`libcurl`**. (BZ#1260178)

The `pycurl.POSTFIELDS` option of `PycURL` now works correctly

Previously, the **`PycURL`** interface violated the **`libcurl`** API, which requires a string passed by the **`CURLOPT_POSTFIELDS`** option to remain valid until the transfer finishes. Consequently, if the **`pycurl.POSTFIELDS`** option was used, **`libcurl`** accessed a string beyond its lifetime, which resulted in an undefined behavior. An upstream patch has been applied on the **`PycURL`** source code to make sure that the string passed to the **`CURLOPT_POSTFIELDS`** option of **`libcurl`** remains valid long enough, and the described problem no longer occurs. (BZ#1153321)

`sctp_accept()` no longer causes a deadlock when called during a timeout event

Previously, when **`sctp_accept()`** was called by a user during a heartbeat timeout event after the 4-way handshake, a deadlock could occur. With this update, the bug has been fixed by giving the **`assoc->base.sk`** pointer to make sure **`SCTP`** correctly locks and unlocks the listening socket. (BZ#1270586)

Out of memory message no longer appears if the stack size is set to unlimited

Prior to this update, using the **`ftp`** command **`put`** when the stack size was set to unlimited caused the sysconf(_SC_ARG_MAX) function to return **`-1`**, which in turn resulted in the malloc() function being called with an argument of **`0`** and causing an **`Out of memory`** message to be displayed. With this update, the underlying source code has been improved to allocate a reasonable minimum of memory. As a result, the **`Out of memory`** message no longer appears if the stack size was previously set to unlimited. (BZ#1304064)

NetworkManager no longer provides complete FQDN (DHCP_HOSTNAME) to dhclient.

Previously, NetworkManager always sent only the host part of a machine host name in a DHCP request. As a consequence, it was not possible to force sending a Fully Qualified Domain Name (FQDN). After this update, the user can configure the FQDN to be sent in a DHCP request by using nmcli and setting ipv4.dhcp-fqdn to the desired FQDN and ensuring that ipv4.dhcp-send-hostname is enabled. In configuration files, the FQDN can be specified with the DHCP_FQDN variable. (BZ#1255507)

CHAPTER 32. SECURITY

The `ftp_home_dir` SELinux boolean has been removed

Previously, the user was able to login to the home directory despite the **`ftp_home_dir`** SELinux boolean set to **`off`**. With this update, the **`ftp_home_dir`** boolean has been removed. (BZ#1097775)

CHAPTER 33. SERVERS AND SERVICES

The `named` service now binds to all interfaces

With this update, **`BIND`** is able to react to situations when a new IP address is added to an interface. If the new address is allowed by the configuration, **`BIND`** will automatically start to listen on that interface. (BZ#1294506)

Fix for `tomcat-digest` to generate password hashes

When using the **`tomcat-digest`** utility to create an SHA hash of Tomcat passwords, the command terminated unexpectedly with the **`ClassNotFoundException`** Java exception. A patch has been provided to fix this bug and **`tomcat-digest`** now generates password hashes as expected. (BZ#1240279)

Tomcat can now use shell expansion in configuration files within the new `conf.d` directory

Previously, the **`/etc/sysconfig/tomcat`** and **`/etc/tomcat/tomcat.conf`** files were loaded without shell expansion, causing the application to terminate unexpectedly. This update provides a mechanism for using shell expansion in the Tomcat configuration files by adding a new configuration directory, **`/etc/tomcat/conf.d`**. Any files placed in the new directory may now include shell variables. (BZ#1221896)

Fix for the `tomcat-jsvc` service unit to create two independent Tomcat servers

When trying to start multiple independent Tomcat servers, the second server failed to start due to the jsvc service returning an error. This update fixes the **`jsvc`** systemd service unit as well as the handling of the TOMCAT_USER variable. (BZ#1201409)

The `dbus-daemon` service no longer becomes unresponsive due to leaking file descriptors

Previously, the **`dbus-daemon`** service incorrectly handled multiple messages containing file descriptors if they were received in a short time period. As a consequence, **`dbus-daemon`** leaked file descriptors and became unresponsive. A patch has been applied to correctly handle multiple file descriptors from different messages inside **`dbus-daemon`**. As a result, **`dbus-daemon`** closes and passes file descriptors correctly and no longer becomes unresponsive in the described situation. (BZ#1325870)

Update for marking tomcat-admin-webapps package configration files

Previously, the tomcat-admin-webapps **`web.xml`** files were not marked as the configuration files. Consequently, upgrading the tomcat-admin-webapps package overwrote the **`/usr/share/tomcat/webapps/host-manager/WEB-INF/web.xml`** and **`/usr/share/tomcat/webapps/manager/WEB-INF/web.xml`** files, causing custom user configuration to be automatically removed. This update fixes classification of these files, thus preventing this problem. (BZ#1208402)

Ghostcript no longer hangs when converting a PDF file to PNG

Previously, when converting a PDF file into a PNG file, Ghostscript could become unresponsive. This bug has been fixed, and the conversion time is now proportional to the size of the PDF file being converted. (BZ#1302121)

The `named-chroot` service now starts correctly

Due to a regression, the **`-t /var/named/chroot`** option was omitted in the **`named-chroot.service`** file. As a consequence, if the **`/etc/named.conf`** file was missing, the **`named-chroot`** service failed to start. Additionally, if different **`named.conf`** files existed in the **`/etc/`** and

/var/named/chroot/etc/ directories, the **named-checkconf** utility incorrectly checked the one in the changed-root directory when the service was started. With this update, the option in the service file has been added and the **named-chroot** service now works correctly. (BZ#1278082)

AT-SPI2 driver added to `brltty`

The Assistive Technology Service Provider Interface driver version 2 (AT-SPI2) has been added to the **brltty** daemon. AT-SPI2 enables using **brltty** with, for example, the GNOME Accessibility Toolkit. (BZ#1324672)

A new `--ignore-missing` option for `tuned-adm verify`

The **--ignore-missing** command-line option has been added to the **tuned-adm verify** command. This command verifies whether a Tuned profile has been successfully applied, and displays differences between the requested Tuned profile and the current system settings. The **--ignore-missing** parameter causes **tuned-adm verify** to silently skip features that are not supported on the system, thus preventing the described errors. (BZ#1243807)

The new `modules` Tuned plug-in

The **modules** plug-in allows Tuned to load and reload kernel modules with parameters specified in the the settings of the Tuned profiles. (BZ#1249618)

The number of `inotify` user watches increased to 65536

To allow for more pods on an Red Hat Enterprise Linux Atomic host, the number of **inotify** user watches has been increased by a factor of 8 to 65536. (BZ#1322001)

Timer migration for realtime Tuned profile has been disabled

Previously, the realtime Tuned profile that is included in the tuned-profiles-realtime package set the value of the **kernel.timer_migration** variable to 1. As a consequence, realtime applications could be negatively affected. This update disables the timer migration in the realtime profile. (BZ#1323283)

`rcu-nocbs` no longer missing from kernel boot parameters

Previously, the **rcu_nocbs** kernel parameter was not set in the **realtime-virtual-host** and **realtime-virtual-guest** tuned profiles. With this update, **rcu-nocbs** is set as expected. (BZ#1334479)

The global limit on how much time realtime scheduling may use has been removed in realtime Tuned profile

Prior to this update, the Tuned utility configuration for the **kernel.sched_rt_runtime_us** sysctl variable in the realtime profile included in the tuned-profiles-realtime package was incorrect. As a consequence, creating a virtual machine instance caused an error due to incompatible scheduling time. Now, the value of **kernel.sched_rt_runtime_us** is set to **-1** (no limit), and the described problem no longer occurs. (BZ#1346715)

`sapconf` now detects the NTP configuration properly

Previously, the **sapconf** utility did not check whether the host system was configured to use the Network Time Protocol (NTP). As a consequence, even when NTP was configured, **sapconf** displayed the following error:

```
3: NTP Service should be configured and started
```

With this update, **sapconf** properly checks for the NTP configuration, and the described problem no longer occurs. (BZ#1228550)

`sapconf` lists default packages correctly

Prior to this update, the **sapconf** utility passed an incorrect parameter to the **repoquery** utility, which caused **sapconf** not to list the default packages in package groups. The bug has been fixed, and **sapconf** now lists default packages as expected. (BZ#1235608)

The `logrotate` utility now saves status to the `/var/lib/logrotate/` directory

Previously, the **logrotate** utility saved status to the **/var/lib/logrotate.status** file. Consequently, **logrotate** did not work on systems where **/var/lib** was a read-only file system. With this update, the status file has been moved to the new **/var/lib/logrotate/** directory, which can be mounted with write permissions. As a result, **logrotate** now works on systems where **/var/lib** is a read-only file system. (BZ#1272236)

Support for printing to an SMB printer using Kerberos using cups

With this update, the cups package creates the symbolic link **/usr/lib/cups/backend/smb** referring to the **/usr/libexec/samba/cups_backend_smb** file. The symbolic link is used by the **smb_krb5_wrapper** utility to print to an server message block (SMB)-shared printer using Kerberos authentication. (BZ#1302055)

Newly installed tomcat package has a correct shell pointing to `/sbin/nologin`

Previously, the postinstall script set the Tomcat shell to **/bin/nologin**, which does not exist. Consequently, users failed to get a helpful message about the login access denial when attempting to log in as Tomcat user. This bug has been fixed, and the postinstall script now corectly sets the Tomcat shell to **/sbin/nologin**. (BZ#1277197)

CHAPTER 34. STORAGE

`/dev/disk/by-path/` now accounts for NPIV paths

Previously, if two or more virtual host bus adapters (HBAs) were created on a single physical HBA, only a single link to the device was created in the **`/dev/disk/by-path/`** directory instead of one link for each path. As a consequence, creating a **`virsh`** pool with virtual HBAs by using Fibre Channel N_Port ID Virtualization (NPIV) did not work correctly. With this update, symbolic links in **`/dev/disk/by-path/`** are created correctly and are unique. Symbolic links in **`/dev/disk/by-path/`** created by **`udev`** for logical unit numbers (LUNs) connected through a physical Fibre Channel N_Port stay the same. (BZ#1266934)

When using thin-provisioning, buffered writes are no longer lost when the thin pool reaches capacity

Previously, a resize operation, even an automated one, attempted to flush outstanding I/O to the storage device prior to the resize being performed. Since there was no room in the thin pool, the I/O operations had to be errored first to allow the grow to succeed. As a consequence, if a thin-pool was filled to capacity, some writes could be lost even if the pool was being grown at that time. With this update, buffered writes are no longer lost to the thin-pool in the described situation. (BZ#1274676)

RAID migration now works correctly on the little-endian variant of IBM Power Systems

Previously, the **`raid-migrate`** command failed on the little-endian variant of IBM Power Systems if the stripe size was not specified, as the **`iprconfig`** utility fell back on the current stripe size of the RAID and loaded it from the adapter without performing a proper endianness conversion The underlying source code has been modified to fix this bug, and RAID migration now works correctly on the little-endian variant of IBM Power Systems. (BZ#1297921)

The `multipathd` daemon no longer reinstates unusable Implicit ALUA ghost paths.

Previously, the **`multipathd`** daemon automatically reinstated Implicit ALUA devices in the GHOST state, which were not usable. Multipath would continuously retry unusable devices, if they were the only ones present, instead of failing I/O operations. With this fix, **`multipathd`** no longer reinstates unusable Implicit ALUA ghost paths. As a result, multipath no longer continually retries I/O operations when only unusuable Implicit ALU A paths are available. (BZ#1291406)

Multipath now includes 0 sized standby paths in the multipath device

Some arrays do not report their size on the standby ports, resulting in 0 sized devices. Previously, Multipath did not allow 0 sized devices to be added to a multipath device. As a result, Multipath did not add 0 sized standby paths to the multipath device. With this update, Multipath now allows the addition of 0 sized paths to a device. (BZ#1356651)

Multipath no longers modifies devices with a `dm` table type of `multipath` that were created by other programs

Previously, the multipath tools assumed that they were in charge of managing all **`dm`** devices with a multipath table. The **`multipathd`** daemon would modify the tables of devices that were not created by the multipath tools. With this update, the multipath tools now operate only on devices whose **`dm`** UUIDs start with **`mpath-`**, which is the UUID prefix that multipath uses on all the devices it creates. As a result, multipath will no longer modify devices with a **`dm`** table type of **`multipath`** that were created by other programs. (BZ#1241528)

The `multipathd` daemon now allows paths to be added to a new multipath device if it currently has no usable paths

Previously, when **`multipathd`** created a new multipath device it did not allow any more paths to be added until it saw the **`udev`** change event for the multipath device being created, even if it created the

device with no usable paths. If a multipath device was created with no usable paths, the **udev** device manager would hang trying to get information on the device, and until it timed out no active paths could be added to the device. With this fix, **multipathd** now allows paths to be added to a newly created multipath device if it currently has no usable paths. As a result, usable paths are immediately added to new devices that have none, and **udev** does not hang. (BZ#1350931, BZ#1351430)

The `multipathd` daemon no longer quits on encountering recoverable errors during startup

Perviously, **multipathd** would quit instead recovering when it hit recoverable errors during startup. With this fix, **multipathd** now continues if it hits a recoverable error during startup and no longer quits. (BZ#1368501)

The `multipathd` daemon now responds to failed removes with `fail` rather than `ok`

Previously, the **multipathd** daemon did not retain the error status when removing a path or a map failed and would respond to failed removes with **ok**. With this fix, **multipathd** now responds to failed removes with **fail**. (BZ#1272620)

Multipath no longer crashes when a uid_attribute is changed after a device is added and the device is then removed

Previously, if a path changed its WWID after being added to a multipath device, the **multipathd** daemon would create a new device. This led to the path being in both devices. As a consequence, if users changed the **uid_attribute** after multipath devices were created and then removed the devices, **multipathd** would try to access freed memory and crash. With this fix, **multipathd** no longer allows the path's WWID to be changed while it is being used in a multipath device. As a result, **multipathd** no longer crashes in this scenario. (BZ#1323429)

Multipath no longer occasionally fails while renaming devices

Previously, multipath was using an uninitialized variable in the function to rename a device. This would cause multipath to fail occasionally while renaming a device because the variable was set to an invalid value. With this fix, multipath now initializes this variable when renaming a device. (BZ#1363830)

Systemd no longer reports that the `multipath.pid` file is not readable

Previously, systemd reported that it was unable to read the **multipathd.pid** file after the **multipathd** command returned. This was because the **multipathd** command was returning as soon as it forked the daemon, and the daemon was not writing the **pid** file until after configuration was complete. With this fix, the **multipathd** command now either waits until the **multipathd** daemon has written the **pid** file or 3 seconds have passed before returning, and the daemon writes the **pid** file earlier in startup. As a result, **systemd** no longer reports that the **multipath.pid** file is not readable. (BZ#1253913)

Multipath now states that a path is `not a valid argument` for paths that do not belong to block devices

Previously, if you used a path to something that is not a valid block device, multipath would tell you that it **requires a path to check**, which is unhelpful. This is because multipath considered anything that is not a block device path or major:minor number to be a multipath alias. With this fix, multipath will not treat fully qualified paths to anything that is not a block devices as a multipath alias. As a result, multipath will state the that path is **not a valid argument** for paths that do not belong to block devices. (BZ#1319853)

All `/dev/mapper` entries for multipath devices are now symbolic links created by `udev`

Previously, some **/dev/mapper** entries for multipath devices were symbolic links (symlinks) and some were block devices since multipath was not correctly waiting for **udev** to create the **/dev/mapper/**

symlinks. With this fix, multipath now waits for **udev** after each transaction. As a result, all **/dev/mapper** entries for multipath devices are now symlinks created by **udev**. (BZ#1255885)

New devices are now claimed by multipath as soon as multipath creates a multipath device on top of them

Previously, the first time multipath saw a device, it was not claimed by multipath in the **udev** rules since multipath will not claim a device in **udev** unless the the WWID is in the **/etc/multipath/wwids** file when processing the **uevent**. With this fix, when multipath adds a new device WWID to the **wwids** file, it will issue a change event on the device so it can claim it in the **udev** rules. New devices are now claimed by multipath as soon as multipath creates a multipath device on top of them. (BZ#1299600)

Failures on some devices no longer keep multipath from creating other devices

Previously, the **multipath** command could fail to set up working devices because of failures on unrelated devices since it would quit early if it failed to get the information on any of the devices it was trying to create. With this fix, multipath no longer quits early if it fails to get information on some of the devices and failures on some devices no longer keep multipath from creating others. (BZ#1313324)

Multipath no longer misses `uevent` messages and it now adds all appropriate devices

Previously, multipath did not always adding all the path devices correctly because it was not correctly checking for the existence of a **libudev** function to compile with support for resizing the **uevent** socket. Because of this, multipath was not resizing the **uevent** socket, and it could overflow. This caused multipath to miss necessary events. With this fix, multipath now checks for the proper **libudev** function and compiles with support for resizing the **uevent** socket. As a result, multipath no longer misses **uevent** messages, and it now adds all appropriate devices. (BZ#1296979)

The `kpartx` tool no longer returns before devices are created

Previously, by default the **kpartx** tool returned without waiting for devices to be created. This was a source of confusion for users who would expect the devices to exist immediately after **kpartx** returned. With this update, **kpartx** by default now waits until the devices are created before returning. (BZ#1299648)

Multiple calls to resize a device will each attempt to resize the device, and will correctly report the result

Previously, if **multipathd** failed to resize a device, it continued to think that the device had the new size. Subsequent calls to resize the device would report success and not resize the device because **multipathd** thought that it had nothing left to do. With this fix, **multipathd** now resets the device size to the original size if the resize fails. As a result, multiple calls to resize a device will each attempt to resize the device, and will correctly report the result. (BZ#1333492)

Multipath now correctly creates partition devices for 4k block devices with DOS partitions greater than 2TB

Previously, the **kpartx** tool created the wrong size partitions for 4K block size devices with DOS partitions greater than 2TB. This was because **kpartx** stored the number of sectors and the multiplier needed to convert from the native sector size to 512B sectors in 32 bit unsigned integers. This causes a rollover if the two numbers multiplied together are larger than 2^32. with this fix, multipath now uses a 64 bit unsigned integer for the sector size multiplier variable, so the result will not roll over when the numbers are multiplied together. As a result, multipath now correctly creates the partitions. (BZ#1311463)

Multipath no longer removes partitions that are in use and restores partitions when a path is added back

Previously, if all paths to a device were lost, multipath would remove all the partitions that were not in

use and never restore them. This occured because when multipath tried to remove a device it was removing partitions even if some of them were in use, and once they were removed it was never restoring them. With this fix, multipath now checks if any partition is in use before attempting a remove, and if the remove fails, it restores the partitions when a path is added back. (BZ#1292599)

The `kpartx` tool no longer overwrites an existing partition device when a new device's name matches the existing one

Previously, when a potential new device's name matched an existing device's name, **`kpartx`** was silently overwriting the existing partition device with the new one. This would cause **`kpartx`** devices to suddenly change where they were pointing if there was a naming clash. With this fix, **`kpartx`** now checks the UUID to make sure that it is not overwriting a partition device that belongs to a different whole device. If there is a name clash, **`kpartx`** will now fail with an error message instead of changing where an existing partition device is pointing to. (BZ#1283750)

The `mpathconf --allow` command now creates a configuration file with the correct devices allowed for a node to boot

Previously, with certain setups the **`mpathconf --allow`** command created a configuration file that did not allow the node to boot. This occurred because **`mpathconf --allow`** was removing existing entries from the **`blacklist_exceptions`** section of the configuration file, which could cause some of the allowed devices to be blacklisted. It also printed duplicate WWID entries in the **`blacklist_exceptions`** section. With this fix, **`mpathconf --allow`** no longer removes the existing **`blacklist_exceptions`** entries, and prints the WWID entries only once. This command now always creates a configuration file with the correct devices allowed for a node to boot. (BZ#1288660)

Multipath devices now get correctly identified as LVM physical volumes

Previously, LVM sometimes failed to recognize multipath PVs. This was because **`multipathd`** could be reloading a device at the same time that the creation **`uevent`** for it arrived. The LVM **`udev`** rules do not allow processing a device that is currently suspended, which happens during a reload. With this fix, **`multipathd`** delays device reloads until after it has received the creation **`uevent`**. (BZ#1304687)

The `multipathd` daemon no longer prints that a path is up when it is actually down

Previously, the **`multipathd`** daemon could print that a path was up when it actually was down. If **`multipathd`** detected that the path was down before it called the path checker, it never cleared the last path checker message and would print that out. With this fix, **`multipathd`** now clears the path checker message if the path is determined to be down before the checker is run. (BZ#1280524)

`multipathd` devices no longer fail to be created if `udev` is processing a partition device at the same time

Previously, **`multipathd`** was unable to create a multipath device when **`udev`** had a lock on the path device. This was because **`multipathd`** grabbed an exclusive lock on the path devices while creating the multipath device and **`udev`** grabs a shared lock on the path devices while processing its partition devices. With this fix **`multipathd`** now grabs a shared lock as well, so that it can run at the same time as **`udev`**. (BZ#1347769)

`systemd` no longer prints warning messages about a missing dependency

Previously, **`systemd`** printed warning messages about a missing dependency when The **`multipathd`** systemd service unit file required another unit file that was not available in the **`initramfs`**. With this fix, the **`multipathd`** unit file now uses **`Wants`** instead of **`Requires`** since it is able to operate without the **`blk-availability`** unit file. (BZ#1269293)

The `kpartx` generated devices now have the same partition number as the actual partition number

Previously, the **`kpartx`** generated device partition number did not match with the actual partition

number. This was because **kpartx** was not counting sun partitions with no sectors when determining the partition number. With this fix, **kpartx** now counts sun partitions with no sectors when determining the partition number and the **kpartx** generated devices now have the same partition number as the actual partition number. (BZ#1241774)

MTX no longer fails with large tape storage arrays

On systems configured with a large tape storage drive array, the MTX tool previously failed with an error. As a consequence, it was not possible to manage the tape storage. This update improves support for larger tape storage arrays, and MTX can now manage large tape storage as expected. (BZ#1298647)

Interferences between dmraid and other device-mapper subsystems no longer occur

Previously, the dmraid packages were compiled with an incorrect testing option. As a consequence, the **dmraid** tool inadvertently scanned all devices, including any other **device-mapper** subsystems like LVM, which could interfere with those other subsystems and cause various failures while booting. With this update, testing mode is disabled in **dmraid**, and all devices are not scanned at boot. As a result, interferences between **dmraid** and other device-mapper subsystems no longer occur. (BZ#1348289)

systemd no longer warns about a missing unit for dmraid-activation.service after uninstalling dmraid

Prior to this update, the **/etc/systemd/system/sysinit.target.wants/dmraid-activation.service** symbolic link was left on the system after uninstalling the dmraid packages, which caused the **systemd** service to warn about a missing unit for the **dmraid-activation.service**. With this update, the aforementioned symbolic link is removed when uninstalling **dmraid**. (BZ#1315644)

mdadm no longer fails to stop an IMSM RAID array during a reshape

Due to a bug, attempts to stop an Intel Matrix Storage Manager (IMSM) RAID array during a reshape previously failed. The underlying source code has been modified to fix this bug, and the **mdadm** utility now stops the array correctly in the described situation. (BZ#1312837)

Using mdadm to assign a hot spare to a degraded array while running I/O operations no longer fails

Previously, assigning a hot spare to a degraded array while running I/O operations on the MD Array could fail, and the **mdadm** utility returned error messages such as:

```
mdadm: /dev/md1 has failed so using --add cannot work and might destroy
mdadm: data on /dev/sdd1. You should stop the array and re-assemble it
```

A patch has been applied to fix this bug, and adding a hot spare to a degraded array now completes as expected in the described situation. (BZ#1300579)

A degraded RAID1 array created with mdadm is no longer shown as inactive after rebooting

Previously, a degraded RAID1 array that was created using the **mdadm** utility could be shown as an inactive RAID0 array after rebooting the system. With this update, the array is started correctly after the system is rebooted. (BZ#1290494)

Trying to reshape a RAID1 array containing a bitmap to a RAID0 array no longer corrupts the RAID1 array

Reshaping a RAID1 array containing a bitmap to a RAID0 array with the **mdadm** utility is not supported. Previously, when attempting to reshape a RAID1 array containing a bitmap to a RAID0 array, the operation was denied, but the RAID1 array was corrupted. With this update the reshape is denied, but

the RAID1 array stays functional as expected. (BZ#1174622)

A race condition no longer occurs with IMSM RAID arrays running an `mdadm` reshape operation

With Intel Matrix Storage Manager (IMSM) RAID arrays running an **mdadm** reshape operation, a race condition could previously allow a second reshape to be launched on the same array before the first operation was completed, and the reshaping operation did not complete correctly. With this update, the race condition no longer occurs, and a second reshape operation cannot be started before the first operation is completed. (BZ#1347762)

`mdadm` can now assemble arrays that use device names over 15 characters long

Previously, the **mdadm** utility could terminate unexpectedly with a segmentation fault when trying to assemble an array that included a device with a device name longer than 15 characters. With this update, **mdadm** assembles arrays correctly even when the arrays use device names longer than 15 characters. (BZ#1347749)

CHAPTER 35. VIRTUALIZATION

SMEP and SMAP bits masked to enable secondary vCPUs

Previously, disabling Extended Page Table (EPT) on a host that supported Supervisor Mode Execution Protection (SMEP) or Supervisor Mode Access Protection (SMAP) resulted in guests being restricted to a single vCPU. This update masks SMEP and SMAP bits on the host side when necessary. As a result, secondary vCPUs start and can be used by the guest virtual machine. (BZ#1273807)

`Force Reset` menu entry in Japanese locale Virtual Machine Manager translated correctly

Previously, the **`Force Reset`** menu entry was translated incorrectly in the Japanese locale Virtual Machine Manager. In this update the **`Force Reset`** menu entry is translated correctly. (BZ#1282276)

Limited KSM deduplication factor

Previously, the kernel same-page merging (KSM) deduplication factor was not explicitly limited, which caused Red Hat Enterprise Linux hosts to have performance problems or become unresponsive in case of high workloads. This update limits the KSM deduplication factor, and thus eliminates the described problems with virtual memory operations related to KSM pages. (BZ#1298618)

VMDK images with streamOptimized sub-format are accepted

Previously, a Virtual Machine Disk (VMDK) image with a streamOptimized sub-format created by the qemu-img tool was rejected by Elastic Sky X (ESX) services, because the version number of the VMDK image was too low. In this update, the sub-format number of streamOptimized VMDK images are automatically increased. This results in the VMDK image being accepted by ESX services. (BZ#1299116)

Data layout of VMDK images with streamOptimized sub-format was incorrect

Previously, the data layout of a Virtual Machine Disk (VMDK) image with a streamOptimized sub-format created by the qemu-img tool was incorrect. This prevented the VMDK image from being bootable when imported to ESX servers. In this update, the image is converted to a valid VMDK streamOptimized image. This results in the VMDK image being bootable. (BZ#1299250)

`blockcopy` with `--pivot` option no longer fails

Previously, **`blockcopy`** always failed when the **`--pivot`** option was specified. With this release, the libvirt package was updated to prevent this issue. **`blockcopy`** can now be used with the **`--pivot`** option. (BZ#1197592)

Guest display problems after `virt-v2v` conversion have been fixed

Previously, the video card driver setting of a guest converted with the **`virt-v2v`** utility was ignored, causing various display problems in the guest. This update ensures that **`virt-v2v`** generates the libvirt XML file for the converted guest properly. As a result, the video card setting is preserved, and the guest can take full advantage of graphical capabilities after the conversion. (BZ#1225789)

Migrating MSR_TSC_AUX works properly

Previously, the contents of the MSR_TSC_AUX file were sometimes not migrated correctly during guest migration. As a consequence, the guest terminated unexpectedly after the migration finished. This update ensures that the contents of MSR_TSC_AUX are migrated as expected, and the described crashes no longer occur. (BZ#1265427)

Windows guest virtual machine information removed from documentation

In this update, all references to Windows guest virtual machines have been removed from the documentation. The information was moved to the following knowledgebase article: https://access.redhat.com/articles/2470791 (BZ#1262007)

Accessing guest disks on `virt-manager` works properly with SELinux and libguestfs-python

Prior to this update, when the libguestfs-python package was installed and SELinux was enabled on the host machine, accessing guest disks using the **`virt-manager`** interface caused I/O failures. Now, **`virt-manager`** and the libguestfs library share the same libvirt connection, which prevents the described failures from occurring. (BZ#1173695)

PART III. TECHNOLOGY PREVIEWS

This part provides an overview of Technology Previews introduced or updated in Red Hat Enterprise Linux 7.3.

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

CHAPTER 36. GENERAL UPDATES

The `systemd-importd` VM and container image import and export service

Latest **`systemd`** version now contains the **`systemd-importd`** daemon that was not enabled in the earlier build, which caused the **`machinectl pull-*`** commands to fail. Note, that the **`systemd-importd`** daemon is offered as a Technology Preview and should not be considered stable. (BZ#1284974)

CHAPTER 37. AUTHENTICATION AND INTEROPERABILITY

SSSD in a container now available

The System Security Services Daemon (SSSD) in a container is provided as a Technology Preview to allow Red Hat Enterprise Linux Atomic Host authentication subsystem to be connected to central identity providers like Red Hat Identity Management and Microsoft Active Directory.

To install this new image, use the **`atomic install rhel7/sssd`** command. (BZ#1200143)

Use of AD and LDAP sudo providers

The Active Directory (AD) provider is a back end used to connect to an AD server. Starting with Red Hat Enterprise Linux 7.2, using the AD sudo provider together with the LDAP provider is supported as a Technology Preview. To enable the AD sudo provider, add the **`sudo_provider=ad`** setting in the [domain] section of the **`sssd.conf`** file. (BZ#1068725)

DNSSEC available as Technology Preview in Identity Management

Identity Management servers with integrated DNS now support DNS Security Extensions (DNSSEC), a set of extensions to DNS that enhance security of the DNS protocol. DNS zones hosted on Identity Management servers can be automatically signed using DNSSEC. The cryptographic keys are automatically generated and rotated.

Users who decide to secure their DNS zones with DNSSEC are advised to read and follow these documents:

- DNSSEC Operational Practices, Version 2: http://tools.ietf.org/html/rfc6781#section-2
- Secure Domain Name System (DNS) Deployment Guide: http://dx.doi.org/10.6028/NIST.SP.800-81-2
- DNSSEC Key Rollover Timing Considerations:

http://tools.ietf.org/html/rfc7583

Note that Identity Management servers with integrated DNS use DNSSEC to validate DNS answers obtained from other DNS servers. This might affect the availability of DNS zones that are not configured in accordance with recommended naming practices described in the Red Hat Enterprise Linux Networking Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices. (BZ#1115294)

Nunc Stans event framework available for Directory Server

A new Nunc Stans event framework to handle multiple simultaneous connections has been added as Technology Preview. The framework allows supporting several thousand active connections with no performance degradation. It is disabled by default. (BZ#1206301)

Support for secrets as a service

This update adds responder **`secrets`** as a Technology Preview to the System Security Services Daemon (SSSD). This responder allows an application to communicate with SSSD over a UNIX socket using the Custodia API. This enables SSSD to store secrets in its local database or to forward them to a remote Custodia server. (BZ#1311056)

IdM web UI enables smart card login

The Identity Management (IdM) web UI enables users to log in using smart cards. Note that this feature is experimental and not supported. (BZ#1317379, BZ#1346883, BZ#1343422)

Identity Management JSON-RPC API available as Technology Preview

An API is available for Identity Management (IdM). To view the API, IdM also provides an API browser as Technology Preview.

In Red Hat Enterprise Linux 7.3, the IdM API has been enhanced to enable multiple versions of API commands. Previously, enhancements could change the behavior of a command in an incompatible way. Users are now able to continue using existing tools and scripts even if the IdM API changes. This enables:

- Administrators to use previous or later versions of IdM on the server than on the managing client.
- Developers to use a specific version of an IdM call, even if the IdM version changes on the server.

In all cases, the communication with the server is possible, regardless if one side uses, for example, a newer version that introduces new options for a feature.

For details on using the API, see https://access.redhat.com/articles/2728021 (BZ#1298286)

CHAPTER 38. CLUSTERING

`pcs` now supports managing multi-site clusters that use Booth and ticket constraints

As a Technology Preview starting with Red Hat Enterprise Linux 7.3, the **pcs** tool enables you to manage multi-site clusters that use the **Booth** cluster ticket manager by using the **pcs booth** command. You can also set ticket constraints by using the **pcs constraint ticket** command to manage resources in multi-site clusters. It is also possible to manage ticket constraints in the web UI. (BZ#1305049, BZ#1308514)

Support for quorum devices in a Pacemaker cluster

Starting with Red Hat Enterprise Linux 7.3, you can configure a separate quorum device (QDevice) which acts as a third-party arbitration device for the cluster. This functionality is provided as a Technology Preview, and its primary use is to allow a cluster to sustain more node failures than standard quorum rules allow. A quorum device is recommended for clusters with an even number of nodes and highly recommended for two-node clusters. For information on configuring a quorum device, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/. (BZ#1158805)

Support for `clufter`, a tool for transforming and analyzing cluster configuration formats

The clufter package, available as a Technology Preview in Red Hat Enterprise Linux 7, provides a tool for transforming and analyzing cluster configuration formats. It can be used to assist with migration from an older stack configuration to a newer configuration that leverages Pacemaker. For information on the capabilities of **clufter**, see the **clufter(1)** man page or the output of the **clufter -h** command. (BZ#1212909)

clufter rebased to version 0.59.5

The clufter packages, available as a Technology Preview, have been upgraded to upstream version 0.59.5, which provides a number of bug fixes, new features, and user experience enhancements over the previous version. Among the notable updates are the following:

- When converting the old cluster stack configuration into files for a Pacemaker stack or into the respective sequence of **pcs** commands with the **ccs2pcs** and **ccs2pcscmd** families of **clufter** commands, monitor action is properly propagated or added.

- When converting configuration files for the Pacemaker stack using the **corosync.conf** file, either as a byproduct of converting CMAN-based configuration or with first-class input such as the ***2pcscmd{,-needle}** families of commands, the cluster name is propagated correctly. Previously, the cluster name was mistakenly dropped, resulting in a command that confused the name of the first cluster node for the name of the cluster as in, for example, **pcs cluster setup --start --name node1 node2 node3**.

- When converting CMAN-based configuration into the parallel configuration for a Pacemaker stack with the **ccs2pcs** family of commands, accidentally broken values of attributes marked as having an ID type in the schema no longer occur.

- When converting either CMAN or Pacemaker stack specific configuration into the respective sequence of **pcs** commands with the ***2pcscmd** families of commands, the **clufter** tool no longer suggests **pcs cluster cib file --config**, which does not currently work for subsequent local-modification **pcs** commands. Instead it suggests **pcs cluster cib file**.

- The **clufter** tool outputs now may vary significantly depending on the specified distribution target since the tool now aligns the output with what the respective environment, such as the

pcs version, can support. Because of this, your distribution or setup may not be supported, and you should not expect that one sequence of **pcs** commands that the **clufter** tool produces is portable to a completely different environment.

- The **clufter** tool now supports several new features of the **pcs** tool, including quorum devices. Additionally, the **clufter** tool supports older features recently added to the **pcs** tool, including ticket constraints, and resource sets for colocation and order constraints. (BZ#1343661, BZ#1270740, BZ#1272570, BZ#1272592, BZ#1300014, BZ#1300050, BZ#1328078)

Support for Booth cluster ticket manager

Red Hat Enterprise Linux 7.3 provides support for a Booth cluster ticket manager as a technology preview. This allows you to configure multiple high availability clusters in separate sites that communicate through a distributed service to coordinate management of resources. The Booth ticket manager facilitates a consensus-based decision process for individual tickets that ensure that specified resources are run at only one site at a time, for which a ticket has been granted. For information on configuring multi-site clusters with the Booth ticket manager, see the https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/ (BZ#1302087)

CHAPTER 39. FILE SYSTEMS

The CephFS kernel client is now available

Starting with Red Hat Enterprise Linux 7.3, the Ceph File System (CephFS) kernel module enables, as a Technology Preview, Red Hat Enterprise Linux nodes to mount Ceph File Systems from Red Hat Ceph Storage clusters. The kernel client in Red Hat Enterprise Linux is a more efficient alternative to the Filesystem in Userspace (FUSE) client included with Red hat Ceph Storage. Note that the kernel client currently lacks support for CephFS quotas. For more information, see the Ceph File System Guide for Red Hat Ceph Storage 2: https://access.redhat.com/documentation/en/red-hat-ceph-storage/2/single/ceph-file-system-guide-technology-preview (BZ#1205497)

ext4 and XFS file systems now support DAX

Starting with Red Hat Enterprise Linux 7.3, Direct Access (DAX) provides, as a Technology Preview, a means for an application to directly map persistent memory into its address space. To use DAX, a system must have some form of persistent memory available, usually in the form of one or more Non-Volatile Dual In-line Memory Modules (NVDIMMs), and a file system that supports DAX must be created on the NVDIMM(s). Also, the file system must be mounted with the **`dax`** mount option. Then, an **`mmap`** of a file on the dax-mounted file system results in a direct mapping of storage into the application's address space.

For a list of supported NVDIMM products and configurations, see the **`New kernel subsystem: libnvdimm`** entry in the Storage chapter, Part I. New Features. (BZ#1274459)

pNFS Block Layout Support

As a Technology Preview, the upstream code has been backported to the Red Hat Enterprise Linux client to provide pNFS block layout support.

In addition, Red Hat Enterprise Linux 7.3 includes the Technology Preview of the pNFS SCSI layout. This feature is similar to pNFS block layout support, but limited only to SCSI devices, so it is easier to use. Therefore, Red Hat recommends the evaluation of the pNFS SCSI layout rather than the pNFS block layout for most use cases. (BZ#1111712)

OverlayFS

OverlayFS is a type of union file system. It allows the user to overlay one file system on top of another. Changes are recorded in the upper file system, while the lower file system remains unmodified. This allows multiple users to share a file-system image, such as a container or a DVD-ROM, where the base image is on read-only media. Refer to the kernel file Documentation/filesystems/overlayfs.txt for additional information.

OverlayFS remains a Technology Preview in Red Hat Enterprise Linux 7.3 under most circumstances. As such, the kernel will log warnings when this technology is activated.

Full support is available for OverlayFS when used with Docker under the following restrictions:

- OverlayFS is only supported for use as a Docker graph driver. Its use can only be supported for container COW content, not for persistent storage. Any persistent storage must be placed on non-OverlayFS volumes to be supported. Only default Docker configuration can be used; that is, one level of overlay, one lowerdir, and both lower and upper levels are on the same file system.

- Only XFS is currently supported for use as a lower layer file system.

- SELinux must be enabled and in enforcing mode on the physical machine, but must be disabled in the container when performing container separation; that is, /etc/sysconfig/docker must not contain --selinux-enabled. SELinux support for OverlayFS is being worked on upstream, and is expected in a future release.

- The OverlayFS kernel ABI and userspace behavior are not considered stable, and may see changes in future updates.
- In order to make the yum and rpm utilities work properly inside the container, the user should be using the yum-plugin-ovl packages.

Note that OverlayFS provides a restricted set of the POSIX standards. Test your application thoroughly before deploying it with OverlayFS.

Note that XFS file systems must be created with the **`-n ftype=1`** option enabled for use as an overlay. With the rootfs and any file systems created during system installation, set the **`--mkfsoptions=-n ftype=1`** parameters in the Anaconda kickstart. When creating a new file system after the installation, run the **`# mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE`** command. To determine whether an existing file system is eligible for use as an overlay, run the **`# xfs_info /PATH/TO/DEVICE | grep ftype`** command to see if the **`ftype=1`** option is enabled.

There are also several known issues associated with OverlayFS as of Red Hat Enterprise Linux 7.3 release. For details, see **`Non-standard behavior`** in the **`Documentation/filesystems/overlayfs.txt`** file. (BZ#1206277)

Support for `NFSv4` clients with flexible file layout

Support for flexible file layout on **`NFSv4`** clients was first introduced in Red Hat Enterprise Linux 7.2 as a Technology Preview. This technology enables advanced features such as non-disruptive file mobility and client-side mirroring, which provides enhanced usability in areas such as databases, big data and virtualization. This feature has been updated in Red Hat Enterprise Linux 7.3, and it is still offered as a Technology Preview.

See https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/ for detailed information about **`NFS`** flexible file layout. (BZ#1217590)

Btrfs file system

The Btrfs (B-Tree) file system is supported as a Technology Preview in Red Hat Enterprise Linux 7.3. This file system offers advanced management, reliability, and scalability features. It enables users to create snapshots, it enables compression and integrated device management. (BZ#1205873)

pNFS SCSI layouts client and server support is now provided

Client and server support for parallel NFS (pNFS) SCSI layouts is provided as a Technology Preview starting with Red Hat Enterprise Linux 7.3. Building on the work of block layouts, the pNFS layout is defined across SCSI devices and contains sequential series of fixed-size blocks as logical units that must be capable of supporting SCSI persistent reservations. The Logical Unit (LU) devices are identified by their SCSI device identification, and fencing is handled through the assignment of reservations. (BZ#1305092)

CHAPTER 40. HARDWARE ENABLEMENT

LSI Syncro CS HA-DAS adapters

Red Hat Enterprise Linux 7.1 included code in the megaraid_sas driver to enable LSI Syncro CS high-availability direct-attached storage (HA-DAS) adapters. While the megaraid_sas driver is fully supported for previously enabled adapters, the use of this driver for Syncro CS is available as a Technology Preview. Support for this adapter is provided directly by LSI, your system integrator, or system vendor. Users deploying Syncro CS on Red Hat Enterprise Linux 7.2 and later are encouraged to provide feedback to Red Hat and LSI. For more information on LSI Syncro CS solutions, please visit http://www.lsi.com/products/shared-das/pages/default.aspx. (BZ#1062759)

Intel DIMM management tools

As a Technology Preview, the following components have been added to enable the management of Intel Dual Inline Memory Modules (DIMMs).

- An API has been added for configuring DIMMs
- The libinvm-cli library, which supports storage command-line (CLI) applications
- The libinvm-cim library, which allows the use of storage common information model (CIM) providers
- The libinvm-i18n library, which provides internationalization functionality for DIMMs

These enable the user to perform basic DIMM inventory, capacity provisioning, health monitoring, and troubleshooting. (BZ#1270993, BZ#1270998, BZ#1326924, BZ#1326931)

CHAPTER 41. INSTALLATION AND BOOTING

Multi-threaded xz compression in rpm-build

Compression can take long time for highly parallel builds as it currently uses only one core. This is problematic especially for continuous integration of large projects that are built on hardware with many cores.

This feature, which is provided as a Technology Preview, enables multi-threaded **xz** compression for source and binary packages when setting the **%_source_payload** or **%_binary_payload** macros to the **wLTX.xzdio** pattern . In it, **L** represents the compression level, which is 6 by default, and **X** is the number of threads to be used (may be multiple digits), for example **w6T12.xzdio**. This can be done by editing the **/usr/lib/rpm/macros** file or by declaring the macro within the spec file or at the command line. (BZ#1278924)

CHAPTER 42. KERNEL

Heterogeneous memory management included as a Technology Preview

Red Hat Enterprise Linux 7.3 offers the heterogeneous memory management (HMM) feature as a Technology Preview. This feature has been added to the kernel as a helper layer for devices that want to mirror a process address space into their own memory management unit (MMU). Thus a non-CPU device processor is able to read system memory using the unified system address space. To enable this feature, add **`experimental_hmm=enable`** to the kernel command line. (BZ#1230959)

User namespace

This feature provides additional security to servers running Linux containers by providing better isolation between the host and the containers. Administrators of a container are no longer able to perform administrative operations on the host, which increases security. (BZ#1138782)

libocrdma RoCE support on Oce141xx cards

As a Technology Preview, the **`ocrdma`** module and the libocrdma package support the Remote Direct Memory Access over Converged Ethernet (RoCE) functionality on all network adapters in the Oce141xx family. (BZ#1334675)

No-IOMMU mode for VFIO drivers

As a Technology Preview, this update adds No-IOMMU mode for virtual function I/O (VFIO) drivers. The No-IOMMU mode provides the user with full user-space I/O (UIO) access to a direct memory access (DMA)-capable device without a I/O memory management unit (IOMMU). Note that in addition to not being supported, using this mode is not secure due to the lack of I/O management provided by IOMMU. (BZ#1299662)

criu rebased to version 2.3

Red Hat Enterprise Linux 7.2 introduced the **`criu`** tool as a Technology Preview. This tool implements **`Checkpoint/Restore in User-space (CRIU)`**, which can be used to freeze a running application and store it as a collection of files. Later, the application can be restored from its frozen state.

Note that the **`criu`** tool depends on **`Protocol Buffers`**, a language-neutral, platform-neutral extensible mechanism for serializing structured data. The protobuf and protobuf-c packages, which provide this dependency, were also introduced in Red Hat Enterprise Linux 7.2 as a Technology Preview.

With Red Hat Enterprise Linux 7.3, the criu packages have been upgraded to upstream version 2.3, which provides a number of bug fixes and enhancements over the previous version. Notably, **`criu`** is now available also on Red Hat Enterprise Linux for POWER, little endian.

Additionally, **`criu`** can now be used for following applications running in a Red Hat Enterprise Linux 7 **`runc`** container:

- vsftpd
- apache httpd
- sendmail
- postgresql
- mongodb
- mariadb
- mysql

- tomcat
- dnsmasq (BZ#1296578)

The `ibmvnic` Device Driver has been added

The **`ibmvnic`** Device Driver has been introduced as a Technology Preview in Red Hat Enterprise Linux 7.3 for IBM POWER architectures. vNIC (Virtual Network Interface Controller) is a new PowerVM virtual networking technology that delivers enterprise capabilities and simplifies network management. It is a high-performance, efficient technology that when combined with SR-IOV NIC provides bandwidth control Quality of Service (QoS) capabilities at the virtual NIC level. vNIC significantly reduces virtualization overhead, resulting in lower latencies and fewer server resources, including CPU and memory, required for network virtualization. (BZ#947163)

Kexec as a Technology Preview

The **`kexec`** system call has been provided as a Technology Preview. This system call enables loading and booting into another kernel from the currently running kernel, thus performing the function of the boot loader from within the kernel. Hardware initialization, which is normally done during a standard system boot, is not performed during a **`kexec`** boot, which significantly reduces the time required for a reboot. (BZ#1460849)

CHAPTER 43. REAL-TIME KERNEL

New scheduler class: `SCHED_DEADLINE`

This update introduces the **`SCHED_DEADLINE`** scheduler class for the real-time kernel as a Technology Preview. The new scheduler enables predictable task scheduling based on application deadlines. **`SCHED_DEADLINE`** benefits periodic workloads by reducing application timer manipulation. (BZ#1297061)

CHAPTER 44. NETWORKING

Cisco usNIC driver

Cisco Unified Communication Manager (UCM) servers have an optional feature to provide a Cisco proprietary User Space Network Interface Controller (usNIC), which allows performing Remote Direct Memory Access (RDMA)-like operations for user-space applications. The libusnic_verbs driver, which is supported as a Technology Preview, makes it possible to use usNIC devices via standard InfiniBand RDMA programming based on the Verbs API. (BZ#916384)

Cisco VIC kernel driver

The Cisco VIC Infiniband kernel driver, which is supported as a Technology Preview, allows the use of Remote Directory Memory Access (RDMA)-like semantics on proprietary Cisco architectures. (BZ#916382)

Trusted Network Connect

Trusted Network Connect, supported as a Technology Preview, is used with existing network access control (NAC) solutions, such as TLS, 802.1X, or IPsec to integrate endpoint posture assessment; that is, collecting an endpoint's system information (such as operating system configuration settings, installed packages, and others, termed as integrity measurements). Trusted Network Connect is used to verify these measurements against network access policies before allowing the endpoint to access the network. (BZ#755087)

SR-IOV functionality in the qlcnic driver

Support for Single-Root I/O virtualization (SR-IOV) has been added to the qlcnic driver as a Technology Preview. Support for this functionality will be provided directly by QLogic, and customers are encouraged to provide feedback to QLogic and Red Hat. Other functionality in the qlcnic driver remains fully supported. (BZ#1259547)

New packages: libnftnl, nftables

As a Technology Preview, this update adds the nftables and libnftl packages.

The nftables packages provide a packet-filtering tool, with numerous improvements in convenience, features, and performance over previous packet-filtering tools. It is the designated successor to the **`iptables`**, **`ip6tables`**, **`arptables`**, and **`ebtables`** utilities.

The libnftnl packages provide a library for low-level interaction with nftables Netlink's API over the **`libmnl`** library. (BZ#1332585, BZ#1332581)

CHAPTER 45. STORAGE

`LVM` RAID-level takeover is now available

RAID-level takeover, the ability to switch between RAID types, is now available as a Technology Preview. With RAID-level takeover, the user can decide based on their changing hardware characteristics what type of RAID configuration best suits their needs and make the change without having to deactivate the logical volume. For example, if a **`striped`** logical volume is created, it can be later converted to a RAID4 logical volume if an additional device is available.

Starting with Red Hat Enterprise Linux 7.3, the following conversions are available as a Technology Preview:

- striped <-> RAID4
- linear <-> RAID1
- mirror <-> RAID1 (mirror is a legacy type, but still supported) (BZ#1191630)

Multi-queue I/O scheduling for SCSI

Red Hat Enterprise Linux 7 includes a new multiple-queue I/O scheduling mechanism for block devices known as blk-mq. The scsi-mq package allows the Small Computer System Interface (SCSI) subsystem to make use of this new queuing mechanism. This functionality is provided as a Technology Preview and is not enabled by default. To enable it, add **`scsi_mod.use_blk_mq=Y`** to the kernel command line. (BZ#1109348)

Targetd plug-in from the libStorageMgmt API

Since Red Hat Enterprise Linux 7.1, storage array management with libStorageMgmt, a storage array independent API, has been fully supported. The provided API is stable, consistent, and allows developers to programmatically manage different storage arrays and utilize the hardware-accelerated features provided. System administrators can also use libStorageMgmt to manually configure storage and to automate storage management tasks with the included command-line interface.

The Targetd plug-in is not fully supported and remains a Technology Preview. (BZ#1119909)

Support for Data Integrity Field/Data Integrity Extension (DIF/DIX)

DIF/DIX is a new addition to the SCSI Standard. It is fully supported in Red Hat Enterprise Linux 7.3 for the HBAs and storage arrays specified in the Features chapter, but it remains in Technology Preview for all other HBAs and storage arrays.

DIF/DIX increases the size of the commonly used 512 byte disk block from 512 to 520 bytes, adding the Data Integrity Field (DIF). The DIF stores a checksum value for the data block that is calculated by the Host Bus Adapter (HBA) when a write occurs. The storage device then confirms the checksum on receipt, and stores both the data and the checksum. Conversely, when a read occurs, the checksum can be verified by the storage device, and by the receiving HBA. (BZ#1072107)

CHAPTER 46. VIRTUALIZATION

Nested virtualization

As a Technology Preview, Red Hat Enterprise Linux 7 offers nested virtualization. This feature enables KVM to launch guests that can act as hypervisors and create their own guests. For more information, see the Red Hat Enterprise Linux 7 Virtualization Deployment and Administration Guide. (BZ#1187762)

USB 3.0 support for KVM guests

USB 3.0 host adapter (xHCI) emulation for KVM guests remains a Technology Preview in Red Hat Enterprise Linux 7.3. (BZ#1103193)

Select Intel network adapters now support SR-IOV as a guest on Hyper-V

In this update for Red Hat Enterprise Linux guest virtual machines running on Hyper-V, a new PCI passthrough driver adds the ability to use the single-root I/O virtualization (SR-IOV) feature for Intel network adapters supported by the ixgbevf driver. This ability is enabled when the following conditions are met:

- SR-IOV support is enabled for the network interface controller (NIC)
- SR-IOV support is enabled for the virtual NIC
- SR-IOV support is enabled for the virtual switch

The virtual function (VF) from the NIC is attached to the virtual machine.

The feature is currently supported with Microsoft Windows Server 2016 Technical Preview 5. (BZ#1348508)

Driver added for devices that connect over a PCI Express bus in guest virtual machine under Hyper-V

In this update, a new driver was added that exposes a root PCI bus when a devices that connects over a PCI Express bus is passed through to a Red Hat Enterprise Linux guest virtual machine running on the Hyper-V hypervisor. The feature is currently supported with Microsoft Windows Server 2016 Technical Preview 5. (BZ#1302147)

Open Virtual Machine Firmware

The Open Virtual Machine Firmware (OVMF) is available as a Technology Preview in Red Hat Enterprise Linux 7. OVMF is a UEFI secure boot environment for AMD64 and Intel 64 guests. (BZ#653382)

PART IV. DEVICE DRIVERS

This part provides a comprehensive listing of all device drivers which were updated in Red Hat Enterprise Linux 7.3.

CHAPTER 47. NEW DRIVERS

Storage Drivers

- cxgbit
- libnvdimm
- mpt2sas
- nd_blk
- nd_btt
- nd_e820
- nd_pmem
- nvme

Network Drivers

- ath10k_core (BZ#1298484)
- ath10k_pci (BZ#1298484)
- bnxt_en (BZ#1184635)
- brcmfmac
- brcmsmac
- brcmutil
- btbcm
- btcoexist
- btintel
- btrtl
- c_can
- c_can_pci
- c_can_platform
- can-dev
- cc770
- cc770_platform
- ems_pci
- ems_usb

- esd_usb2
- fjes
- geneve
- hfi1
- i40iw
- iwl3945
- iwl4965
- iwldvm
- iwlegacy
- iwlmvm
- iwlwifi (BZ#1298113)
- kvaser_pci
- kvaser_usb
- macsec
- mwifiex
- mwifiex_pcie
- mwifiex_sdio
- mwifiex_usb
- mwl8k
- peak_pci
- peak_usb
- plx_pci
- qed
- qede
- rdmavt
- rt2800lib
- rt2800mmio
- rt2800pci
- rt2800usb

- rt2x00lib
- rt2x00mmio
- rt2x00pci
- rt2x00usb
- rt61pci
- rt73usb
- rtl_pci
- rtl_usb
- rtl8187
- rtl8188ee
- rtl8192c-common
- rtl8192ce
- rtl8192cu
- rtl8192de
- rtl8192ee
- rtl8192se
- rtl8723-common
- rtl8723ae
- rtl8723be
- rtl8821ae
- rtlwifi
- sja1000
- sja1000_platform
- slcan
- softing
- uas
- usb_8dev
- vcan

Graphics Drivers and Miscellaneous Drivers

- amdgpu

- amdkfd
- gp2ap002a00f
- gpio-ich
- gpio-viperboard
- idma64
- int3400_thermal
- leds-lt3593
- ledtrig-gpio
- nfit
- pci-hyperv
- pwm-lpss
- qat_c3xxx
- qat_c3xxxvf
- qat_c62x
- qat_c62xvf
- qat_dh895xccvf
- regmap-spi
- rotary_encoder
- rtc-rx4581
- rtsx_usb
- rtsx_usb_sdmmc
- sht15
- target_core_user
- tpm_st33zp24
- tpm_st33zp24_i2c
- virt-dma
- virtio-gpu
- zram

CHAPTER 48. UPDATED DRIVERS

Storage Driver Updates

- The 3w-9xxx driver has been updated to version 2.26.02.014.rh1.
- The aacraid driver has been updated to version 1.2-1[41066]-ms.
- The be2iscsi driver has been updated to version 11.0.0.0. (BZ#1274912)
- The bfa driver has been updated to version 3.2.25.0.
- The bnx2fc driver has been updated to version 2.10.3.
- The cxgb3i driver has been updated to version 2.0.1-ko.
- The cxgb4i driver has been updated to version 0.9.5-ko.
- The libcxgbi driver has been updated to version 0.9.1-ko.
- The fnic driver has been updated to version 1.6.0.21.
- The hpsa driver has been updated to version 3.4.14-0-RH1.
- The isci driver has been updated to version 1.2.0.
- The lpfc driver has been updated to version 0:11.1.0.2.
- The megaraid_sas driver has been updated to version 06.811.02.00-rh1.
- The mt2sas driver has been updated to version 20.102.00.00.
- The mt3sas driver has been updated to version 13.100.00.00.
- The qla2xxx driver has been updated to version 8.07.00.33.07.3-k1.
- The vmw_pvscsi driver has been updated to version 1.0.6.0-k.
- The cxgbit driver has been updated to version 1.0.0-ko.
- The nvme driver has been updated to version 1.0.
- The smartpqi driver has been updated to version 0.9.13-370.
- The mtip32xx driver has been updated to version 1.3.1. (BZ#1273618, BZ#1269525)
- The ipr driver has been updated to version 2.6.3. (BZ#1274357)
- The bnx2i driver has been updated to version 2.7.10.1. (BZ#1273086)

Network Driver Updates

- The bpa10x driver has been updated to version 0.11.
- The btbcm driver has been updated to version 0.1.
- The btintel driver has been updated to version 0.1.

- The btrtl driver has been updated to version 0.1.
- The btusb driver has been updated to version 0.8.
- The hci_uart driver has been updated to version 2.3.
- The hci_vhci driver has been updated to version 1.5.
- The hfi1 driver has been updated to version 0.9-294.
- The i40iw driver has been updated to version 0.5.123.
- The ocrdma driver has been updated to version 11.0.0.0.
- The ib_srp driver has been updated to version 2.0.
- The bnx2x driver has been updated to version 1.712.30-0.
- The bnxt_en driver has been updated to version 1.2.0.
- The cnic driver has been updated to version 2.5.22.
- The enic driver has been updated to version 2.3.0.20.
- The be2net driver has been updated to version 11.0.0.0r.
- The e1000e driver has been updated to version 3.2.6-k.
- The i40e driver has been updated to version 1.5.10-k.
- The i40evf driver has been updated to version 1.5.10-k.
- The igb driver has been updated to version 5.3.0-k.
- The ixgbe driver has been updated to version 4.4.0-k-rh7.3.
- The ixgbevf driver has been updated to version 2.12.1-k-rh7.3.
- The qed driver has been updated to version 8.7.1.20.
- The qede driver has been updated to version 8.7.1.20.
- The qlcnic driver has been updated to version 5.3.65.
- The fjes driver has been updated to version 1.1.
- The geneve driver has been updated to version 0.6.
- The vmxnet driver has been updated to version 1.4.7.0-k.
- The iwl3945 driver has been updated to version in-tree:ds.
- The iwl4965 driver has been updated to version in-tree:d.
- The iwlegacy driver has been updated to version in-tree:.
- The mwifiex driver has been updated to version 1.0.

- The mwifiex_pcie driver has been updated to version 1.0.
- The mwifiex_sdio driver has been updated to version 1.0.
- The mwifiex_usb driver has been updated to version 1.0.
- The mwl8k driver has been updated to version 0.13.
- The rt2800lib driver has been updated to version 2.3.0.
- The rt2800mmio driver has been updated to version 2.3.0.
- The rt2800pci driver has been updated to version 2.3.0.
- The rt2800usb driver has been updated to version 2.3.0.
- The rt2x00lib driver has been updated to version 2.3.0.
- The rt2x00mmio driver has been updated to version 2.3.0.
- The rt2x00pci driver has been updated to version 2.3.0.
- The rt2x00usb driver has been updated to version 2.3.0.
- The rt61pci driver has been updated to version 2.3.0.
- The rt73usb driver has been updated to version 2.3.0.
- The mlx4_core driver has been updated to version 2.2-1. (BZ#1298421)
- The mlx4_en driver has been updated to version 2.2-1. (BZ#1298422)
- The mlx4_ib driver has been updated to version 2.2-1. (BZ#1298423)
- The mlx5_core driver has been updated to version 2.2-1. (BZ#1298424)
- The mlx5_ib driver has been updated to version 3.0-1. (BZ#1298425)
- The sfc driver has been updated to the latest upstream version. (BZ#1298425)

Graphics Driver and Miscellaneous Driver Updates

- The tpm_st33zp24 driver has been updated to version 1.3.0.
- The tpm_st33zp24_i2c driver has been updated to version 1.3.0.
- The qat_c3xxx driver has been updated to version 0.6.0.
- The qat_c62x driver has been updated to version 0.6.0.
- The intel_qat driver has been updated to version 0.6.0.
- The qat_dh895xcc driver has been updated to version 0.6.0.
- The qat_dh895xccvf driver has been updated to version 0.6.0.
- The amdkfd driver has been updated to version 0.7.2.

- The qat_dh895xccvf driver has been updated to version 0.6.0.
- The vmwgfx driver has been updated to version 2.10.0.0.
- The vmw_balloon driver has been updated to version 1.4.0.0-k.
- The hpilo driver has been updated to version 1.4.1. (BZ#1274436)

CHAPTER 49. DEPRECATED FUNCTIONALITY

This chapter provides an overview of functionality that has been deprecated in all minor releases of Red Hat Enterprise Linux 7 up to Red Hat Enterprise Linux 7.3.

Deprecated functionality continues to be supported until the end of life of Red Hat Enterprise Linux 7. Deprecated functionality will likely not be supported in future major releases of this product and is not recommended for new deployments. For the most recent list of deprecated functionality within a particular major release, refer to the latest version of release documentation.

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

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

nautilus-open-terminal replaced with gnome-terminal-nautilus

Since Red Hat Enterprise Linux 7.3, the nautilus-open-terminal package has been deprecated and replaced with the gnome-terminal-nautilus package. This package provides a Nautilus extension that adds the **Open in Terminal** option to the right-click context menu in Nautilus. nautilus-open-terminal is replaced by gnome-terminal-nautilus during the system upgrade.

`sslwrap()` removed from Python

The **`sslwrap()`** function has been removed from **Python 2.7**. After the 466 Python Enhancement Proposal was implemented, using this function resulted in a segmentation fault. The removal is consistent with upstream.

Red Hat recommends using the **`ssl.SSLContext`** class and the **`ssl.SSLContext.wrap_socket()`** function instead. Most applications can simply use the **`ssl.create_default_context()`** function, which creates a context with secure default settings. The default context uses the system's default trust store, too.

Symbols from libraries linked as dependencies no longer resolved by `ld`

Previously, the **`ld`** linker resolved any symbols present in any linked library, even if some libraries were linked only implicitly as dependencies of other libraries. This allowed developers to use symbols from the implicitly linked libraries in application code and omit explicitly specifying these libraries for linking.

For security reasons, **`ld`** has been changed to not resolve references to symbols in libraries linked implicitly as dependencies.

As a result, linking with **`ld`** fails when application code attempts to use symbols from libraries not declared for linking and linked only implicitly as dependencies. To use symbols from libraries linked as dependencies, developers must explicitly link against these libraries as well.

To restore the previous behavior of **`ld`**, use the **`-copy-dt-needed-entries`** command-line option. (BZ#1292230)

Windows guest virtual machine support limited

As of Red Hat Enterprise Linux 7, Windows guest virtual machines are supported only under specific subscription programs, such as Advanced Mission Critical (AMC).

`libnetlink` is deprecated

The **libnetlink** library contained in the iproute-devel package has been deprecated. The user should use the **libnl** and **libmnl** libraries instead.

S3 and S4 power management states for KVM are deprecated

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

The Certificate Server plug-in udnPwdDirAuth is discontinued

The **udnPwdDirAuth** authentication plug-in for the Red Hat Certificate Server has been removed in Red Hat Enterprise Linux 7.3. Profiles using the plug-in are no longer supported. Certificates created with a profile using the **udnPwdDirAuth** plug-in are still valid if they have been approved.

Red Hat Access plug-in for IdM is discontinued

The Red Hat Access plug-in for Identity Management (IdM) has been removed in Red Hat Enterprise Linux 7.3. During the update, the redhat-access-plugin-ipa package is automatically uninstalled. Features previously provided by the plug-in, such as Knowledgebase access and support case engagement, are still available through the Red Hat Customer Portal. Red Hat recommends to explore alternatives, such as the **redhat-support-tool** tool.

The Ipsilon identity provider service for federated single sign-on

The ipsilon packages were introduced as Technology Preview in Red Hat Enterprise Linux 7.2. Ipsilon links authentication providers and applications or utilities to allow for single sign-on (SSO).

Red Hat does not plan to upgrade Ipsilon from Technology Preview to a fully supported feature. The ipsilon packages will be removed from Red Hat Enterprise Linux in a future minor release.

Red Hat has released Red Hat Single Sign-On as a web SSO solution based on the Keycloak community project. Red Hat Single Sign-On provides greater capabilities than Ipsilon and is designated as the standard web SSO solution across the Red Hat product portfolio. For details, see Chapter 1, *Overview*.

Deprecated Device Drivers

- 3w-9xxx
- 3w-sas
- mptbase
- mptctl
- mptsas
- mptscsih
- mptspi
- qla3xxx
- The following controllers from the **megaraid_sas** driver have been deprecated:
  - Dell PERC5, PCI ID 0x15
  - SAS1078R, PCI ID 0x60
  - SAS1078DE, PCI ID 0x7C

- SAS1064R, PCI ID 0x411
- VERDE_ZCR, PCI ID 0x413
- SAS1078GEN2, PCI ID 0x78

- The following Ethernet adapter controlled by the **`be2net`** driver has been deprecated:
  - TIGERSHARK NIC, PCI ID 0x0700
- The following controllers from the **`be2iscsi`** driver have been deprecated:
  - Emulex OneConnect 10Gb iSCSI Initiator (generic), PCI ID 0x212
  - OCe10101, OCm10101, OCe10102, OCm10102 BE2 adapter family, PCI ID 0x702
  - OCe10100 BE2 adapter family, PCI ID 0x703
- The following Emulex boards from the **`lpfc`** driver have been deprecated:

  BladeEngine 2 (BE2) Devices
  - TIGERSHARK FCOE, PCI ID 0x0704

  Fibre Channel (FC) Devices
  - FIREFLY, PCI ID 0x1ae5
  - PROTEUS_VF, PCI ID 0xe100
  - BALIUS, PCI ID 0xe131
  - PROTEUS_PF, PCI ID 0xe180
  - RFLY, PCI ID 0xf095
  - PFLY, PCI ID 0xf098
  - LP101, PCI ID 0xf0a1
  - TFLY, PCI ID 0xf0a5
  - BSMB, PCI ID 0xf0d1
  - BMID, PCI ID 0xf0d5
  - ZSMB, PCI ID 0xf0e1
  - ZMID, PCI ID 0xf0e5
  - NEPTUNE, PCI ID 0xf0f5
  - NEPTUNE_SCSP, PCI ID 0xf0f6
  - NEPTUNE_DCSP, PCI ID 0xf0f7
  - FALCON, PCI ID 0xf180

- SUPERFLY, PCI ID 0xf700
- DRAGONFLY, PCI ID 0xf800
- CENTAUR, PCI ID 0xf900
- PEGASUS, PCI ID 0xf980
- THOR, PCI ID 0xfa00
- VIPER, PCI ID 0xfb00
- LP10000S, PCI ID 0xfc00
- LP11000S, PCI ID 0xfc10
- LPE11000S, PCI ID 0xfc20
- PROTEUS_S, PCI ID 0xfc50
- HELIOS, PCI ID 0xfd00
- HELIOS_SCSP, PCI ID 0xfd11
- HELIOS_DCSP, PCI ID 0xfd12
- ZEPHYR, PCI ID 0xfe00
- HORNET, PCI ID 0xfe05
- ZEPHYR_SCSP, PCI ID 0xfe11
- ZEPHYR_DCSP, PCI ID 0xfe12

To check the PCI IDs of the hardware on your system, run the **`lspci -nn`** command.

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

Containers using the `libvirt-lxc` tooling have been deprecated

The following libvirt-lxc packages are deprecated since Red Hat Enterprise Linux 7.1:

- libvirt-daemon-driver-lxc
- libvirt-daemon-lxc
- libvirt-login-shell

Future development on the Linux containers framework is now based on the **docker** command-line interface. libvirt-lxc tooling may be removed in a future release of Red Hat Enterprise Linux (including Red Hat Enterprise Linux 7) and should not be relied upon for developing custom container management applications.

For more information, see the Red Hat KnowledgeBase article.

PART V. KNOWN ISSUES

This part documents known problems in Red Hat Enterprise Linux 7.3.

CHAPTER 50. GENERAL UPDATES

The TAB key does not expand $PWD by default

When working in CLI in Red Hat Enterprise Linux 6, pressing the TAB key expanded **`$PWD/`** to the current directory. In Red Hat Enterprise Linux 7, CLI does not have the same behavior. Users can achieve this behavior by putting the following lines into the $HOME/.bash_profile file:

```
if ((BASH_VERSINFO[0] >= 4)) && ((BASH_VERSINFO[1] >= 2)); then
    shopt -s direxpand
fi
```

(BZ#1185416)

gnome-getting-started-docs-* moved to the Optional channel

As of Red Hat Enterprise Linux 7.3, the gnome-getting-started-docs-* packages have been moved from the Base channel to the Optional channel. Consequently, upgrading from an earlier version of Red Hat Enterprise Linux 7 fails, if these packages were previously installed. To work around this problem, uninstall gnome-getting-started-docs-* prior to upgrading to Red Hat Enterprise Linux 7.3. (BZ#1350802)

The `remote-viewer` SPICE client fails to detect newly plugged-in smart card readers

The **`libcacard`** library in Red Hat Enterprise Linux 7.3 fails to handle USB hot plug events. As a consequence, while the **`remote-viewer`** SPICE client is running, the application in some cases fails to detect a USB smart card reader when it is plugged in. To work around the problem, remove the smart card from the reader and reinsert it. (BZ#1249116)

CHAPTER 51. AUTHENTICATION AND INTEROPERABILITY

Problem with importing a user certificate from CA over SSL

The **pki user-cert-add** command provides an option to import a user certificate directly from CA. Due to incorrect client library initialization, when the command is executed over an SSL port, the command fails with the following error message:

```
javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated.
```

To work around this problem, download the certificate from CA into a file using the **pki cert-show** command. Then, upload the certificate from the file using the **pki user-cert-add** command. With the workaround, the user certificate is added correctly. (BZ#1246635)

The IdM web UI displays all certificates on one page in the Certificates table

The Certificates table, available under the Authentication tab in the Identity Management (IdM) web UI, ignores the page size limit of 20 entries. When more than 20 certificates are available, the table displays all the certificates on one page, instead of only displaying 20 certificates per page. (BZ#1358836)

Security warning when using `ipa-kra-install`, `ipa-ca-install`, or `ipa-replica-install`

When using the **ipa-kra-install**, **ipa-ca-install**, and **ipa-replica-install** utilities to install an additional key recovery authority (KRA) component, certificate authority, or replica, the following warning appears:

```
SecurityWarning: Certificate has no `subjectAltName`,
falling back to check for a `commonName` for now.
This feature is being removed by major browsers and deprecated by RFC
2818.
```

The error occurs due to RFC 2818, which deprecates the practice of carrying the subject host name in the subject distinguished name (DN) common name (CN) field. However, the three utilities succeed. Therefore, you can ignore the warning message. (BZ#1358457)

`pam_pkcs11` only supports one token

The PKCS#11 modules in the opensc and coolkey packages provide support for various types of smart cards. However the **pam_pkcs11** module only supports one of them at a time. As a consequence, you cannot use PKCS#15 and CAC tokens using the same configuration. To work around the problem, install one of the following:

- the opensc package for PKCS#15 and PIV support
- the coolkey package for CAC, Coolkey, and PIV support (BZ#1367919)

Using `ipa-ca-install` on an IdM replica fails when the Directory Server is not configured with LDAPS

Installing a certificate authority (CA) using the **ipa-ca-install** utility on an Identity Management (IdM) replica fails when the Directory Server on the replica is not configured with LDAPS (using the TLS protocol over port 636). The attempt fails with this error:

```
[2/30]: configuring certificate server instance
ipa.ipaserver.install.cainstance.CAInstance: CRITICAL Failed to configure
CA
```

```
instance: Command '/usr/sbin/pkispawn -s CA -f /tmp/tmpsDHYbO' returned
non-zero exit status 1
...
```

Installing a replica in this situation is not possible. As a workaround, choose one of these options:

- Install the CA on the master server instead.
- Enable LDAPS on the replica manually before running **ipa-ca-install**.

To manually enable LDAPS on the replica:

1. Export the server certificate from the **/etc/httpd/alias** file:

```
$ pk12util -d /etc/httpd/alias -k /etc/httpd/alias/pwdfile.txt -o temp.p12
-n 'ca1/replica'
```

Replace **ca1/replica** with the nickname of your certificate.

2. Remove the trust chain from certificate, because it was already imported:

a. Extract the private key:

```
$ openssl pkcs12 -in temp.p12 -nocerts -nodes -out temp.key
```

b. Extract the public key:

```
$ openssl pkcs12 -in temp.p12 -nokeys -clcerts -out temp.pem
```

c. Create a PKCS#12 file without the CA certificate:

```
$ openssl pkcs12 -export -in temp.pem -inkey temp.key -out repl.p12 -name
'ca1/replica'
```

Replace **ca1/replica** with the nickname of your certificate.

3. Import the created certificate into the Directory Server's NSSDB database:

```
$ pk12util -d /etc/dirsrv/slapd-EXAMPLE-COM -K '' -i repl.p12
```

4. Remove the temporary certificate files:

```
$ rm -f temp.p12 temp.key temp.pem repl.p12
```

5. Create a file, **/tmp/enable_ssl.ldif**, with the following contents:

```
dn: cn=encryption,cn=config
changetype: modify
replace: nsSSL3
nsSSL3: off
-
replace: nsSSLClientAuth
nsSSLClientAuth: allowed
-
```

```
replace: nsSSL3Ciphers
nsSSL3Ciphers: default

dn: cn=config
changetype: modify
replace: nsslapd-security
nsslapd-security: on
```

6. Modify the LDAP configuration to enable SSL:

```
$ ldapmodify -H "ldap://localhost" -D "cn=directory manager" -f
/tmp/enable_ssl.ldif -w dm_password
```

Replace **dm_password** with your Directory Manager password.

7. Create a file, **/tmp/add_rsa.ldif**, with the following contents:

```
dn: cn=RSA,cn=encryption,cn=config
changetype: add
objectclass: top
objectclass: nsEncryptionModule
cn: RSA
nsSSLPersonalitySSL: ca1/replica
nsSSLToken: internal (software)
nsSSLActivation: on
```

Replace **ca1/replica** with the nickname of your certificate.

8. Add the entry to the LDAP:

```
$ ldapadd -H "ldap://localhost" -D "cn=directory manager" -f
/tmp/add_rsa.ldif -w dm_password
```

Replace **dm_password** with your Directory Manager password.

9. Remove the temporary files:

```
$ rm -f /tmp/enable_ssl.ldif /tmp/add_rsa.ldif
```

10. Restart directory server:

```
# systemctl restart dirsrv@EXAMPLE-COM.service
```

After following these steps, LDAPS is enabled, and you can successfuly run **ipa-ca-install** on the replica. (BZ#1365858)

Third-party certificate trust flags are reset after installing an external CA into IdM

The **ipa-ca-install --external-ca** command, used to install an external certificate authority (CA) into an existing Identity Management (IdM) domain, generates a certificate signing request (CSR) that the user must submit to the external CA.

When using a previously installed third-party certificate to sign the CSR, the third-party certificate trust flags in the NSS database are reset. Consequently, the certificate is no longer marked as trusted. In addition, checks performed by the **mod_nss** module fail, and the **httpd** service fails to start. The CA

installation fails with the following message in this situation:

```
CA failed to start after 300 seconds
```

As a workaround, after this message appears, reset the third-party certificate flags to their previous state and restart **httpd**. For example, if the **ca1** certificate previously had the **C,,** trust flags:

```
# certutil -d /etc/httpd/alias -n 'ca1' -M -t C,,
# systemctl restart httpd.service
```

This restores the system to the correct state. (BZ#1318616)

realmd fails to remove the computer account from AD

Red Hat Enterprise Linux uses Samba as default back end for Active Directory (AD) domain memberships. In this case, if you manually set a computer name using the **--computer-name** option with the **realm join** command, the account cannot be removed from AD when you leave the domain. To work around this problem, do not use the **--computer-name** option and instead add the computer name to the **/etc/realmd.conf** file. For example:

```
[domain.example.com]
computer-name = host_name
```

With the workaround, the host is successfully joined to the domain and the account is automatically removed if you leave the domain using the **realm leave --remove** command. (BZ#1370457)

SSSD fails to manage autofs mappings from a LDAP tree

Previously, the System Security Services Daemon (SSSD) implemented incorrect default values for autofs mappings when using the **RFC2307** LDAP schema. A patch has been applied, which fixed the defaults to match the schema. However, users connecting to LDAP servers that contain mappings with the schema SSSD previously used, are not able to load the autofs attributes. Affected users see the following error reported in the **/var/log/messages** log file:

```
Your configuration uses the autofs provider with schema set to rfc2307 and
default attribute mappings. The default map has changed in this release,
please make sure the configuration matches the server attributes.
```

To work around this problem, modify the **/etc/sssd/sssd.conf** file and set your domain to use the existing attribute mappings:

```
[domain/EXAMPLE]
...
ldap_autofs_map_object_class   = automountMap
ldap_autofs_map_name           = ou
ldap_autofs_entry_object_class = automount
ldap_autofs_entry_key          = cn
ldap_autofs_entry_value        = automountInformation
```

As a result, SSSD is able to load autofs mappings from the attributes. (BZ#1372814)

The dependency list for pkispawn does not include openssl

When the openssl package is not installed, using the **pkispawn** utility fails with this error:

```
Installation failed: [Errno 2] No such file or directory
```

This problem occurs because the openssl package is not included as a runtime dependency of the pki-server package contained within the pki-core package. As a work around, install openssl before running **pkispawn**. (BZ#1376488)

Enumerating a large number of users results in high CPU load and slows down other operations

When **enumerate=true** is set in the **etc/sssd/sssd.conf** file and a large number of users (for example, 30,000 users) are present in the LDAP server, certain performance problems occur:

- the **sssd_be** process consumes almost 99% of CPU resources
- certain operations, such as logging in as a local user or logging out, take unexpectedly long to complete
- running the **ldbsearch** operation on the **sysdb** and **timestamp** caches fails with an error reporting that the indexed and full searches both failed

Note that this is not a new known issue, as these problems occurred in previous releases of SSSD as well. (BZ#888739, BZ#1379774)

GDM fails to authenticate using a smart card

When using smart card authentication, the System Security Services Daemon's (SSSD) PAM responder does not verify if the login name is a Kerberos user principal name (UPN). As a consequence, the **gdm-password** pluggable authentication module (PAM) shows the password prompt instead of the smart card PIN prompt when using a user principal name (UPN) as login name. As a result, smart card authenticating to the GNOME display manager (GDM) fails. (BZ#1389796)

The ipa passwd command fails when using uppercase or mixed case user names

Identity Management (IdM) 4.4.0 introduced unified handling of user principals in all commands. However, some commands were not fully converted. As a consequence, the **ipa passwd** command fails when you use uppercase or mixed case letters in user names. To work around this issue, use only lower case letters in user names when using the **ipa passwd** command. (BZ#1375133)

The IdM web UI does not correctly recognize the status of a revoked certificate

The Identity Management (IdM) web UI is currently unable to determine whether a certificate has been revoked. As a consequence:

- The **Revoked** sign is not displayed when viewing the certificate from the user, service, or host details page.
- The **Revoke** action is still available from the details page. Attempting to revoke an already revoked certificate results in an error dialog.
- The **Remove Hold** button is always disabled even if the certificate has been revoked because of Certificate Hold (revocation reason 6). (BZ#1371479)

SSSD only applies values in sudoUser attributes from AD in lower case

Previously, when the System Security Services Daemon (SSSD) fetched **sudo** rules from Active Directory (AD), the **sudoUser** attribute must have match the exact case of the **samAccountName** attribute of the user the rule was assigned to. Due to a regression in Red Hat Enterprise Linux 7.3, the **sudoUser** attribute now only matches lower case values. To work around this problem, rename **sudoUser** attribute values to lower case. With the workaround, **sudo** rules are applied correctly. (BZ#1380436)

Updating the ipa-client and ipa-admintools packages can fail

During the upgrade from Red Hat Enterprise Linux 7.2 to Red Hat Enterprise Linux 7.3, updating of the ipa-client and ipa-admintools packages can fail in some cases. To work around this problem, uninstall ipa-client and ipa-admintools prior to upgrading to Red Hat Enterprise Linux 7.3, and then install the new versions of these packages. (BZ#1390565)

Upgrading SSSD sometimes causes the `sssd` process to be terminated

When the **sssd** process performs an action for an unexpectedly long time, an internal watchdog process terminates it. However, the **sssd** process does not start again. This problem usually occurs during an attempt to upgrade SSSD on a slow system if the SSSD database contains a large number of entries.

To work around this problem:

1. Make sure the central authentication server is available. This ensures that users will be able to authenticate after removing the SSSD cache in the next step.

2. Remove the SSSD cache using the **sss_cache** utility before upgrading.

A fix for this known issue will be available with the next update. (BZ#1392441)

Directory Server fails due to `bind-dyndb-ldap` schema errors

The version of the **bind-dyndb-ldap** LDAP schema included in Identity Management contains syntax errors and is missing a description of one attribute. If the user uses this version of the schema, the Directory Server component fails to start. Consequently, error messages are logged in the journal, informing the user about the incorrect syntax.

To work around this problem:

1. Obtain a corrected schema file from the upstream **git.fedorahosted.org** repository:

```
# wget https://git.fedorahosted.org/cgit/bind-dyndb-
ldap.git/plain/doc/schema.ldif?
id=17711141882aca3847a5daba2292bcbcc471ec63 -O /usr/share/doc/bind-
dyndb-ldap-10.0/schema.ldif
```

2. Copy the corrected schema file into the Directory Server's instance configuration folder.

```
# cp /usr/share/doc/bind-dyndb-ldap-10.0/schema.ldif
/etc/dirsrv/slapd-[EXAMPLE-COM]/schema/[SCHEMA_FILE_NAME].ldif
```

3. Restart Directory Server:

```
# systemctl restart dirsrv.target
```

(BZ#1413805)

CHAPTER 52. COMPILER AND TOOLS

Oprofile utilities cannot collect performance data in kernel code by default

Kernel in Red Hat Enterprise Linux 7.3 changes the default value of **/proc/sys/kernel/perf_event_paranoid** from **1** to **2**. As a consequence, collection of performance event data of code in the kernel requires root privileges. When running the **occount** or **operf** utility as a normal user, the default performance event attempts to collect data for both kernel and user code and the setup of the performance event fails because of the default **perf_event_paranoid** setting.

To work around this problem, change the value in **/proc/sys/kernel/perf_event_paranoid** to **1**. If unable to do that, instead determine the default event used on the machine by running the **ophelp -d** command, and then explicitly change the end of the event from **:1:1** to **:0:1** to disable data collection in the kernel space, for example:

```
$ operf -e CPU_CLK_UNHALTED:100000:0:0:1 true
```

As a result, changing **/proc/sys/kernel/perf_event_paranoid** or explicitly disabling monitoring of kernel events for normal users allows collection of data, thus avoiding this issue. (BZ#1349077)

The pesign key database requires manually changing permissions to enable improved access permission controls

The **pesign** key database, which is used to sign UEFI binaries, now offers a more generalized method of setting database access permissions. You can now configure permissions using system-wide key databases, and means that any user or group can now be granted access.

However, a known issue in permission settings in **pesign** currently prevents the aforementioned new feature from working. To enable the improved access control, you must change the permissions to **pesign** manually:

```
chmod 0660 /etc/pki/pesign/*
chmod 0770 /etc/pki/pesign
```

After setting these permissions, the improved access control will become available. If you do not perform these steps, **pesign** behavior will be identical to previous releases. (BZ#1141263)

CHAPTER 53. DESKTOP

Closing laptop lid breaks the GNOME multi-display configuration

When using a laptop with the GNOME graphical environment that is connected to one or more external displays, closing the lid to suspend the laptop sometimes causes windows and icons to be moved between displays and the display layout to be reset when the system is resumed. To work around this problem, open the GNOME Displays interface, which causes the display configuration to be reloaded. (BZ#1360906)

Limited support for visuals in Xorg

In the Xorg server, only TrueColor and DirectColor visuals at depth 16 or higher are supported for hardware drivers. Legacy applications that need a PseudoColor visual can be run against the Xephyr nested X server, which implements PseudoColor translation when displayed on a TrueColor screen. (BZ#1185690)

CHAPTER 54. FILE SYSTEMS

The default option specification is not overridden by the host-specific option in `/etc/exports`

When **`sec=sys`** is used in the default option section of the **`/etc/exports`** file, the options list that follows is not parsed correctly. As a consequence, the default option cannot be overridden by the host-specific option. (BZ#1359042)

CHAPTER 55. HARDWARE ENABLEMENT

Platforms relying on DDF-based RAID are not supported

Disk Data Format (DDF)-based BIOS RAID is currently not supported in Red Hat Enterprise Linux. This includes systems using the LSI BIOS, which require the **megasr** proprietary driver.

However, on certain systems, such as IBM z Systems servers with the ServeRAID adapter, it is possible to disable RAID in the BIOS. To do this, enter the **UEFI** menu and navigate through the **System Settings and Devices** and **I/O Ports** menus to the **Configure the onboard SCU** submenu. Then change the **SCU** setting from **RAID** to **nonRAID**. Save your changes and reboot the system. In this mode, the storage is configured using an open-source non-RAID LSI driver available in Red Hat Enterprise Linux, such as **mptsas**, **mpt2sas**, or **mpt3sas**.

To obtain the **megasr** driver for IBM systems refer to the IBM support page:

http://www-947.ibm.com/support/entry/portal/support

Note that the described restriction does not apply to LSI adapters that use the **megaraid** driver, as such adapters implement RAID functions in firmware. (BZ#1067292)

CHAPTER 56. INSTALLATION AND BOOTING

Dell Latitude E6430 laptops shut down unexpectedly

When booting a Dell Latitude E6430 laptop with an Nvidia graphics card and Nvidia Optimus enabled in the BIOS, as soon as the system attempts to use the Nvidia GPU, the system shuts down. The BIOS then incorrectly displays a **`system board thermal trip`** error at next boot. To work around this problem, use the **`nouveau.runpm=0`** parameter when booting. However, note that using **`nouveau.runpm=0`** can increase power consumption. (BZ#1349827)

Insufficient `/boot` partition size may prevent the system from upgrading

The **`/boot`** partition, which contains installed kernels and initial ram disks, may become full if multiple kernels and additional packages such as kernel-debug are installed. This is caused by the default size of this partition being set to 500 MB during installation, and prevents the system from being upgraded.

As a workaround, use **`yum`** to remove older kernels if you do not need them.

This known issue only affects installation made with Red Hat Enterprise Linux 7.2 and earlier. In Red Hat Enterprise Linux 7.3, the default size of the **`/boot`** partition is increased to 1 GB, which avoids this problem in future upgrades. (BZ#1270883)

Anaconda Kickstart accepts passwords that are too short

When using a Kickstart file to install Red Hat Enterprise Linux 7, the Anaconda installer immediately accepts passwords that are shorter than the minimal length defined by the **`--minlen`** Kickstart option, if the password is sufficiently strong (quality value 50 or above by default). (BZ#1383718, BZ#1356975)

The SCAP password length requirement is ignored in the kickstart installation

The interactive kickstart installation does not enforce the password length check defined by the SCAP rule and accepts shorter root passwords. To work around this problem, use the **`--strict`** option with the **`pwpolicy root`** command in the kickstart file. (BZ#1372791)

No name server is included in `/etc/resolv.conf` after an iSCSI installation with a static IP address

When connecting to the root file system on an iSCSI target from an interface with a static IP address, the name server is not configured on the installed system. To work around this problem, add the **`nameserver=<IP>`** kernel option to the boot loader configuration of the installed system. (BZ#1363831)

Generating a partition scheme based on the `Standard Partition` recipe is not possible when installing on an EAV DASD

Installing to a large enough Common Disk Layout (CDL) Direct Access Storage Device (DASD), for example Extended Address Volumes (EAVs), prompts the installer to create the **`/home`** partition in addition to **`/`**, swap, and **`/boot`**. Since CDL DASDs can only have three partitions, an error occurs. To work around this problem, create the disk layout manually. You can also use LVM with multiple logical volumes (LVs), but **`/boot`** must exist only on a separate, standard partition. (BZ#1370173)

Anaconda does not allow creating users without passwords

Currently, it is not possible to unselect the **`Require a password to use this account`** option in the Anaconda GUI during an interactive installation. As a consequence, it is impossible to create a user account that does not have a password. To work around this problem, use a Kickstart file installation with an **`--emptyok`** option in the **`pwpolicy user`** line. (BZ#1380277)

Anaconda Kickstart installation does not respect the `--changesok` option

Currently, using the **`--changesok`** option when installing Red Hat Enterprise Linux 7 from a Kickstart file does not correctly allow the Anaconda installer to change the root password. (BZ#1356966)

ISO files on hard disk drives cannot be mounted by the Anaconda TUI

ISO files on hard disk drives cannot be mounted by the Anaconda Terminal User Interface (TUI). Consequently, it is not possible to use an ISO file on a hard disk as an installation source. If you try installing from an ISO file on a hard disk, a **`No mountable devices found`** error is displayed.

It is possible to use **`inst.repo=hd:/dev/<hard disk>:/ parameter`** on the command line, but you cannot change the network configuration in the installer. Consequently, the installation source is reset, and there is no chance to access the ISO file again. (BZ#1369818)

Initial Setup does not open in a graphical interface over SSH on IBM z Systems

When connecting to an IBM z Systems machine using SSH, the Initial Setup interface after Red Hat Enterprise Linux 7 installation is opened in the text version even if X forwarding is enabled. (BZ#1378082)

PXE boot with UEFI and IPv6 displays the `grub2` shell instead of the operating system selection menu

When the **`Pre-Boot Execution Environment (PXE)`** starts on a client configured with UEFI and IPv6, the boot menu configured in the **`/boot/grub/grub.cfg`** file is not displayed Instead, the following occurs. The client obtains an IPv6 address from the expected DHCPv6 subnet, and downloads the **`.../grubx64.efi`** netboot image from the PXE server. After a timeout, the **`GRUB2`** shell is displayed instead of the configured operating system selection menu. (BZ#1154226)

FIPS mode unsupported when installing from an HTTPS kickstart source

Installation images do not support FIPS mode during installation with an HTTPS kickstart source. As a consequence, it is currently impossible to to install a system with the **`fips=1`** and **`inst.ks=https://<location>/ks.cfg`** options added to the command line. (BZ#1341280)

Extra time needed for installation when geolocation services are enabled

When installing Red Hat Enterprise Linux 7.3 with limited or no internet access, the installer pauses for a few minutes in the Installation Summary screen with the Security Policy section being **`Not ready`**. Consequently, this adds extra time before the installation proceeds to the next step.

To work around this problem, disable geolocation services by adding the **`inst.geoloc=0`** option to the boot command line. (BZ#1380224)

CHAPTER 57. KERNEL

Improved SCTP performance and better transfer rates

The Stream Control Transmission Protocol (SCTP) implementation is known to consume a large amount of CPU resources. Consequently, insufficient CPU resources often make it impossible to reach high transfer rates, such as 10Gbps on a single association. This update provides improvements that reduce CPU usage on certain SCTP handling, which improves SCTP performance and results in better transfer rates in some situations.

Note that this update does not ensure that SCTP is now able to achieve a 10Gbps transfer rate. (BZ#1058148)

Looking up transport or association can lead to kernel panic

Due to a use-after-free bug, the kernel's stream control transmission protocol (SCTP) implementation does not hold the pointer to the transport path while it is in use. As a consequence, another CPU can free the pointer, access the memory which should be unavailable, and a kernel panic occurs. Work to address this issue is being tracked in https://bugzilla.redhat.com/show_bug.cgi?id=1368884. (BZ#1368884)

`dracut` displays a harmless error message about a non-existent `/etc/hba.conf`

When **`dracut`** creates an initial RAM file system (initramfs) with Fibre Channel over Ethernet (FCoE) support, if the **`/etc/hba.conf`** file does not exist, **`dracut`** displays an error message. You can safely ignore this message. (BZ#1373129)

`kdump` does not work with legacy Type 12 persistent memory

Systems with legacy Type 12 Non-Volatile Dual In-line Memory Modules (NVDIMMs), either real dual in-line memory modules (DIMMs), or emulated using the _memmap=XG!YG kernel command line parameter, are unable to successfully capture a kernel crash dump. For systems with real NVDIMMs, attempts to capture a kernel crash dump result in data corruption in some cases. Users can work around this problem by disabling the **`kdump`** feature on such systems. (BZ#1351098)

The update of `megaraid_sas` can lead to a performance decrease

The **`megaraid_sas`** driver has been updated to version 06.811.02.00-rh1, which brings a number of performance improvements over the previous version. However, in some cases, with configurations based on Solid-state Drives (SSD) a performance decrease has been observed. To work around this problem, set the corresponding **`queue_depth`** parameter in the **`/sys/`** directory to a higher value up to 256, which brings the performance back to its original level. (BZ#1367444)

xgene-enet does not handle situations with low free memory

The **`xgene_enet`** driver currently does not handle out-of memory errors properly. When such an error occurs, the driver sometimes terminates unexpectedly and returns a kernel backtrace to the serial console and to **`dmesg`** logs. Consequently, the system becomes unable to communicate over the network and has to be restarted. (BZ#1248185)

Certain NIC firmware can become unresponsive with `bnx2x`

Due to a bug in the unload sequence of the pre-boot drivers, the firmware of some internet adapters can become unresponsive after the **`bnx2x`** driver takes over the device. The **`bnx2x`** driver detects the problem and returns the message **`storm stats were not updated for 3 times`** in the kernel log. To work around this problem, apply the latest NIC firmware updates provided by your hardware vendor. As a result, unloading of the pre-boot firmware now works as expected and the firmware no longer hangs after **`bnx2x`** takes over the device. (BZ#1315400)

Change of default settings on FCoE servers to reach the correct functionality of the kdump mechanism

Disks on Fibre Channel over Ethernet (FCoE) servers use the multipath storage system, which allows the disks to connect to system from a different interface. Several logical disks are present in the system, but they are mapped to only one real disk. Consequently, with the default settings, the FCoE servers are not able to start on a kdump kernel. To reach the correct functionality of the kdump mechanism, users are advised to specify the Universally Unique Identifier (UUID) of the FCoE disks. Users are also advised to enable the **multipath** option so that disks can be managed in a more efficient way. (BZ#1293520)

iSCSI connection produces I/O errors

Red Hat Enterprise Linux 7.3 no longer caps I/O requests for SCSI disks at a maximum of 512Kib. As a consequence, when a guest running on Red Hat Enterprise Linux 7.3 connects to an iSCSI target configured to use the **fileio** backstore and running on an older version of Red Hat Enterprise Linux, some warning messages appear in the logs, and performance is also affected negatively. To work around this problem, install a udev rule on the system to limit the I/O request size to the maximum of 4096Kib. The problem with the **fileio** backstore can also be fixed by upgrading the iSCSI target to Red Hat Enterprise Linux 7.3. (BZ#1387858)

MST displays become unresponsive when display port cable is plugged in

Previously, DEll MST displays became unresponsive when display port cable was plugged in, because unrelated dp-aux messages interrupted a sequence of dp-aux messages that implemented an I2C device read or write. This update prevents the I2C-over-dp-aux sequence from being interrupted by unrelated MST setup messages. As a result, MST displays no longer become unresponsive in the described scenario. (BZ#1274157)

On IBM Power Systems, kdump fails if fadump was used previously and both use a network target

The **kdump** kernel crash dumping mechanism will fail to save dumps to a network location if the same system was previously configured to instead use firmware-assisted dumping (fadump) and also save dumps remotely. This is because when the mechanism is switched back to **kdump**, the **kdump-** prefix is added to the configured network interface, but configuring **fadump** already added the same prefix before. The resulting interface name becomes **kdump-kdump-eth0**, and the final **0** is then truncated. This results in an invalid interface name **kdump-kdump-eth**, and **kdump** then fails to access the interface and save crash dumps to a remote target.

To work around this problem:

1. Replace the current **/boot/initramfs-$kver.img** initrd with the the **/boot /initramfs-$kver.img.default** file.

2. Run the **touch /etc/kdump.conf** command to force rebuilding the **kdump initrd** after reboot.

3. Reboot the system. (BZ#1372464)

CHAPTER 58. NETWORKING

Verification of signatures using the MD5 hash algorithm is disabled in Red Hat Enterprise Linux 7

It is impossible to connect to any Wi-Fi Protected Access (WPA) Enterprise Access Point (AP) that requires MD5 signed certificates. To work around this problem, copy the wpa_supplicant.service file from the /usr/lib/systemd/system/ directory to the /etc/systemd/system/ directory and add the following line to the Service section of the file:

```
Environment=OPENSSL_ENABLE_MD5_VERIFY=1
```

Then run the **`systemctl daemon-reload`** command as root to reload the service file.

Important: Note that MD5 certificates are highly insecure and Red Hat does not recommend using them. (BZ#1062656)

CHAPTER 59. SECURITY

scap-security-guide example kickstart files for Red Hat Enterprise Linux 6 are not recommended for use

The Red Hat Enterprise Linux 6 example kickstart files, which are included in the scap-security-guide package for Red Hat Enterprise Linux 7, install the latest version of the scap-security-guide package directly from the upstream repository, which means that this version has not been checked by the Red Hat Quality Engineering team. To work around this problem, use the corrected Red Hat Enterprise Linux 6 example kickstart files from the scap-security-guide package that is included in the current Red Hat Enterprise Linux 6 release, or alternatively, manually change the %post section in the kickstart file. Note that the Red Hat Enterprise Linux 7 example kickstart files are not affected by this problem. (BZ#1378489)

The openscap packages do not install atomic as a dependency

The OpenSCAP suite enables integration of the Security Content Automation Protocol (SCAP) line of standards. The current version adds the ability to scan containers using the **`atomic scan`** and **`oscap-docker`** commands. However, when you install only the openscap, openscap-utils, and openscap-scanner packages, the atomic package is not installed by default. As a consequence, any container scan command fails with an error message. To work around this problem, install the atomic package by running the **`yum install atomic`** command as root. (BZ#1356547)

`CIL` does not have a separate module statement

The new SELinux userspace uses SELinux Common Intermediate Language (CIL) in the module store. CIL treats files as modules and does not have a separate module statement, the module is named after the file name. As a consequence, this can cause confusion when a policy module has a name that is not the same as its base filename, and the **`semodule -l`** command does not show the module version. Additionaly, **`semodule -l`** does not show disabled modules. To work around this problem, list all modules using the **`semodule --l=full`** command. (BZ#1345825)

CHAPTER 60. SERVERS AND SERVICES

ReaR creates two ISO images instead of one

In ReaR, the **OUTPUT_URL** directive enables specifying location for the ISO image containing the rescue system. Currently, with this directive set, ReaR creates two copies of the ISO image: one in the specified directory and one in the **/var/lib/rear/output/** default directory. This requires additional space for the image. This is especially important if a full-system backup is included into the ISO image (using the **BACKUP=NETFS** and **BACKUP_URL=iso:///backup/** configuration).

To work around this behavior, delete the extra ISO image once ReaR has finished working or, to avoid having a period of time with double storage consumption, create the image in the default directory and then move it to the desired location manually.

There is a request for enhancement to change this behavior and make ReaR create only one copy of the ISO image. (BZ#1320552)

The default value of `first_valid_uid` in `dovecot` has changed

In Red Hat Enterprise Linux 7, the default configuration of **first_valid_uid** in **dovecot** was changed to **1000** to match the system wide configuration specified as **UID_MIN** in the **/etc/login.defs** file. If a system has **UID_MIN** manually changed to **500** and is relying on **dovecot** default value, **dovecot** will not serve users with IDs lower than **first_valid_uid**. As a consequence, if you have regular users with id less than **1000**, you have to update **first_valid_uid**. After you do this, **dovecot** will work as expected. (BZ#1280433)

CHAPTER 61. STORAGE

No support for thin provisioning on top of RAID in a cluster

While RAID logical volumes and thinly provisioned logical volumes can be used in a cluster when activated exclusively, there is currently no support for thin provisioning on top of RAID in a cluster. This is the case even if the combination is activated exclusively. Currently this combination is only supported in LVM's single machine non-clustered mode. (BZ#1014758)

Interaction problems with the `lvmetad` daemon when `mirror` segment type is used.

When the legacy **`mirror`** segment type is used to create mirrored logical volumes with 3 or more legs, there can be interaction problems with the **`lvmetad`** daemon. Problems observed occur only after a second device failure, when mirror fault policies are set to the non-default **`allocate`** option, when **`lvmetad`** is used, and there has been no reboot of the machine between device failure events. The simplest workaround is to disable **`lvmetad`** by setting **`use_lvmetad = 0`** in the **`lvm.conf`** file.

These issues do not arise with the **`raid1`** segment type, which is the default type for Red Hat Enterprise Linux 7. (BZ#1380521)

Important restrictions for Red Hat Enterprise Linux 7.3 upgrades on systems with RAID4 and RAID10 logical volumes

The following important restrictions apply to Red Hat Enterprise Linux 7.3 upgrades on systems with RAID4 and RAID10 logical volumes:

- Do not upgrade any systems with existing LVM RAID4 or RAID10 logical volumes to Red Hat Enterprise Linux 7.3 because these logical volumes will fail to activate. All other types are unaffected.
- If you do not have any existing RAID4 or RAID10 logical volumes and you upgrade, do not create any new RAID4 logical volumes because those may fail to activate with later releases and updates. It is safe to create RAID10 logical volumes on Red Hat Enterprise Linux 7.3.
- A z-stream fix is being worked on to allow for the activation of existing RAID4 and RAID10 logical volumes and the creation of new RAID4 logical volumes with Red Hat Enterprise Linux 7.3. (BZ#1385149)

The system sometimes becomes unresponsive if there are no working network paths to the iSCSI target

When using iSCSI targets, it is required to have a continuous multipathing from initiator to target, as it is required for **`zfcp`** attached SCSI logical unit number (LUNs). If swap is on iSCSI and the system is under memory pressure when an error recovery occurs in the network path, then the system needs some additional memory for the error recovery. As a consequence, the system can become unresponsive. To work around this problem, have at least one working network path to the iSCSI target to make obtaining memory from swap possible. (BZ#1389245)

Exit code returned from the `lvextend` command has changed

Previously, if the **`lvextend`** or **`lvresize`** commands were run in a way that would result in no change to the size of the logical volume, an attempt was still made to resize the file system. The unnecessary attempt to resize the file system is no longer made and this has caused the exit code of the command to change. LVM makes no guarantees of the consistency of exit codes beyond zero (success) and non-zero (failure). (BZ#1354396)

CHAPTER 62. VIRTUALIZATION

Migration of certain guests from Red Hat Enterprise Linux 7.2 to 7.3 hosts is not possible

Prior to this update, the PCI address of any USB controller that did not have an explicitly specified **`model`** value was ignored on IBM Power guest virtual machines. This bug has been fixed, but as a consequence of the fix, it is not possible to perform a live migration of guests that use the described USB controllers from a Red Hat Enterprise Linux 7.2 host to a Red Hat Enterprise Linux 7.3 host, due to the different PCI addresses of the USB controller.

To work around this problem, edit the guest XML file and add a **`model`** attribute with the **`pci-ohci`** value to the USB <controller> element, for example as follows:

```
<controller type='usb' model='pci-ohci' index='0'>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
function='0x0'/>
</controller>
```

Afterwards, shut down the guest and start it again for the changes to take effect. As a result, the guest can be migrated from Red Hat Enterprise Linux 7.2 to 7.3. (BZ#1357468)

numad changes QEMU memory bindings

Currently, the **`numad`** daemon cannot distinguish between memory bindings that **`numad`** sets and memory bindings set explicitly by the memory mappings of a process. As a consequence, **`numad`** changes QEMU memory bindings, even when the NUMA memory policy is specified in the QEMU command line. To work around this problem, if manual NUMA bindings are specified in the guest, disable **`numad`**. This ensures that manual bindings configured in virtual machines are not changed by **`numad`**. (BZ#1360584)

Memory usage for QEMU processes is shown without mapped hugetlbfs pages

Mapped hugetlbfs pages are not accounted for by the kernel when calculating process memory usage. As a consequence, commands such as **`top`** and **`ps`** show memory usage for QEMU processes without the mapped hugetlbfs pages when a virtual machine is configured to use huge pages. (BZ#1221443)

qemu-kvm below version 2.6.0 cannot load 2.88 MB floppy disks

When using the qemu-kvm package below version 2.6.0, KVM guests are not able to load a 2.88 MB floppy disk if it is inserted after the guest has already booted up. To work around this problem, insert the floppy disk before booting the guest, or use qemu-kvm version 2.6.0 or later. (BZ#1209707)

CHAPTER 63. ATOMIC HOST AND CONTAINERS

SELinux prevents Docker from running a container

Due to a missing label for the **`/usr/bin/docker-current`** binary file, Docker is prevented from running a container by SELinux. (BZ#1358819)

APPENDIX A. COMPONENT VERSIONS

This appendix is a list of components and their versions in the Red Hat Enterprise Linux 7.3 release.

Table A.1. Component Versions

Component	Version
Kernel	3.10.0-514
QLogic `qla2xxx` driver	8.07.00.33.07.3-k1
QLogic `qla4xxx` driver	5.04.00.00.07.02-k0
Emulex `lpfc` driver	0:11.1.0.2
iSCSI initiator utils	iscsi-initiator-utils-6.2.0.873-35
DM-Multipath	device-mapper-multipath-0.4.9-99
LVM	lvm2-2.02.166-1

APPENDIX B. LIST OF BUGZILLAS BY COMPONENT

This appendix provides a list of all components and their related Bugzillas, which are included in this book. Public Bugzilla numbers include a link to the Bugzilla details.

Table B.1. List of Bugzillas by Component

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
389-ds-base	BZ#1018944, BZ#1209094, BZ#1209128, BZ#1273549, BZ#1290111, BZ#1349571	BZ#1186512, BZ#1273555, BZ#1278567, BZ#1278755, BZ#1278987, BZ#1288229, BZ#1290242, BZ#1290600, BZ#1295947, BZ#1302823, BZ#1303641, BZ#1304682, BZ#1307151, BZ#1310848, BZ#1314557, BZ#1315893, BZ#1316580, BZ#1320715, BZ#1321124, BZ#1331343, BZ#1332709, BZ#1340307, BZ#1342609, BZ#1355760, BZ#1360447, BZ#1370300	BZ#1206301	
MySQL-python	BZ#1266849			
NetworkManager	BZ#1142898, BZ#1259063, BZ#1262922, BZ#1367916	BZ#1255507		
TPS				BZ#1274096, BZ#1379379
WALinuxAgent	BZ#1387783			
abrt	BZ#1277848, BZ#1277849, BZ#1281312			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
accountsservice		BZ#1341276		
adwaita-qt	BZ#1306307			
anaconda	BZ#1101653, BZ#1240379, BZ#1254368	BZ#1255280, BZ#1255801, BZ#1259437, BZ#1265330, BZ#1266199, BZ#1267203, BZ#1267872, BZ#1268792, BZ#1269195, BZ#1271766		BZ#1356966, BZ#1363831, BZ#1369818, BZ#1370173, BZ#1380224, BZ#1380277, BZ#1383718
anaconda-user-help		BZ#1260071, BZ#1275285		
arpwatch	BZ#1291722			
audit	BZ#1127343, BZ#1296204			
bash				BZ#1185416
bind	BZ#1220594, BZ#1306610	BZ#1278082, BZ#1294506		
bind-dyndb-ldap				BZ#1413805
binutils	BZ#1276755, BZ#1335313, BZ#1335684, BZ#1341730, BZ#1364516	BZ#1243559, BZ#1300543		
booth			BZ#1302087	
brltty		BZ#1324672		
certmonger		BZ#1367683		
chkconfig	BZ#1291340			
cifs-utils		BZ#1289454, BZ#1351618		

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
clufter			BZ#1212909, BZ#1343661	
control-center		BZ#1298951, BZ#1298952		
coreutils	BZ#1280357	BZ#1284906, BZ#1309247, BZ#1321648		
corosync		BZ#1289169, BZ#1306349, BZ#1336462		
cpuid	BZ#1307043			
crash	BZ#1292566			
crash-ptdump-command	BZ#1298172			
criu			BZ#1296578	
cups		BZ#1302055		
curl	BZ#1263318	BZ#1260178, BZ#1269855, BZ#1275769		
custodia	BZ#1206288			
dbus		BZ#1325870		

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
device-mapper-multipath	BZ#1297456, BZ#1299651, BZ#1299652, BZ#1300415, BZ#1311659, BZ#1333331, BZ#1341748, BZ#1348372, BZ#1353357	BZ#1241528, BZ#1241774, BZ#1253913, BZ#1255885, BZ#1269293, BZ#1272620, BZ#1280524, BZ#1283750, BZ#1288660, BZ#1291406, BZ#1292599, BZ#1296979, BZ#1299600, BZ#1299648, BZ#1304687, BZ#1311463, BZ#1313324, BZ#1319853, BZ#1323429, BZ#1333492, BZ#1347769, BZ#1350931, BZ#1356651, BZ#1363830, BZ#1368501		
device-mapper-persistent-data	BZ#1315452			
distribution	BZ#1272603, BZ#1297815, BZ#1374826			BZ#1062656
dmraid		BZ#1315644, BZ#1348289		
docker				BZ#1358819
dovecot	BZ#1229164			BZ#1280433
dracut	BZ#1359144	BZ#1276983		BZ#1373129
efibootmgr	BZ#1271412			
elfutils	BZ#1296313			
ethtool	BZ#1318316			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
fence-agents		BZ#1313561		
firewalld	BZ#1147500, BZ#1302802			
freerdp		BZ#1275241		
ftp		BZ#1304064		
gcc	BZ#1182152, BZ#1213268, BZ#1304449	BZ#1289022, BZ#1357060		
gcc-libraries	BZ#1265252			
gdb	BZ#1182151	BZ#1186918, BZ#1265351, BZ#1326476		
gfs2-utils	BZ#1196321, BZ#1268045, BZ#1271674			
ghostscript		BZ#1302121		
gimp	BZ#1298226			
gimp-help	BZ#1370595			
glibc	BZ#1211823, BZ#1213267, BZ#1268008, BZ#1292018, BZ#1296297, BZ#1298526, BZ#1335286	BZ#1027348, BZ#1211100, BZ#1276753, BZ#1293916, BZ#1308728		
gnome-boxes		BZ#1015199, BZ#1043950		
gnome-documents		BZ#958690		
gnome-packagekit		BZ#1290868		
gnome-shell-extensions		BZ#1302864		

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
gnome-terminal	BZ#1296110, BZ#1300826			
gnutls	BZ#1110750			
grub2		BZ#1226325, BZ#1279599		BZ#1154226
gssproxy	BZ#1092515, BZ#1292487	BZ#1340259		
haproxy		BZ#1300392		
initial-setup		BZ#1249598		BZ#1378082
initscripts		BZ#1281821		
ipa	BZ#747612, BZ#768316, BZ#825391, BZ#826790, BZ#837369, BZ#1084018, BZ#1146860, BZ#1200731, BZ#1211595, BZ#1212713, BZ#1224057, BZ#1274524, BZ#1287194, BZ#1292141, BZ#1298288, BZ#1298848, BZ#1298966, BZ#1314786, BZ#1320838, BZ#1328552	BZ#1196958, BZ#1290142, BZ#1294503, BZ#1318169, BZ#1343142, BZ#1348560, BZ#1356146, BZ#1357488, BZ#1364113, BZ#1368424, BZ#1368981	BZ#1115294, BZ#1298286, BZ#1317379	BZ#1318616, BZ#1358457, BZ#1365858, BZ#1371479, BZ#1375133
iproute	BZ#1013584, BZ#1212026, BZ#1275426			
iprutils	BZ#1274367	BZ#1297921		
iputils	BZ#1273336			
ipxe	BZ#1298313			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
iw		BZ#1324096		
iwpmd	BZ#1331651			
ixpdimm_sw			BZ#1270993	
java-1.7.0-openjdk		BZ#1296413, BZ#1302385		
java-1.8.0-openjdk	BZ#1245810			
kernel	BZ#727269, BZ#797488, BZ#838926, BZ#965453, BZ#1084618, BZ#1104151, BZ#1115947, BZ#1117093, BZ#1135562, BZ#1138650, BZ#1165316, BZ#1172351, BZ#1172819, BZ#1182021, BZ#1186835, BZ#1210350, BZ#1221311, BZ#1222936, BZ#1227339, BZ#1232050, BZ#1262031, BZ#1262728, BZ#1265259, BZ#1265339, BZ#1267398, BZ#1268334, BZ#1269051, BZ#1269281, BZ#1269626, BZ#1270763, BZ#1273115, BZ#1273499, BZ#1274471, BZ#1275423, BZ#1275711, BZ#1275829, BZ#1276458, BZ#1278794, BZ#1280133,	BZ#1073651, BZ#1152231, BZ#1172496, BZ#1241236, BZ#1245140, BZ#1252281, BZ#1257320, BZ#1258136, BZ#1262204, BZ#1263866, BZ#1264905, BZ#1264920, BZ#1264990, BZ#1265058, BZ#1265283, BZ#1266578, BZ#1266948, BZ#1267339, BZ#1270244, BZ#1270586, BZ#1271860, BZ#1272833, BZ#1273807, BZ#1273978, BZ#1276477, BZ#1279617, BZ#1287322, BZ#1289314, BZ#1289630, BZ#1290202, BZ#1290441, BZ#1298618, BZ#1301451, BZ#1341633, BZ#1361407, BZ#1367257	BZ#916382, BZ#947163, BZ#1109348, BZ#1111712, BZ#1138782, BZ#1187762, BZ#1205497, BZ#1205873, BZ#1206277, BZ#1217590, BZ#1230959, BZ#1274459, BZ#1299662, BZ#1302147, BZ#1305092, BZ#1334675, BZ#1348508	BZ#1058148, BZ#1221443, BZ#1274157, BZ#1293520, BZ#1315400, BZ#1349827, BZ#1351098, BZ#1367444, BZ#1368884, BZ#1385149, BZ#1387858

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
	BZ#1283886, BZ#1285340, BZ#1287040, BZ#1289929, BZ#1289933, BZ#1296707, BZ#1297039, BZ#1297465, BZ#1298446, BZ#1300325, BZ#1302101, BZ#1308703, BZ#1310154, BZ#1311631, BZ#1328874, BZ#1331018, BZ#1331578, BZ#1337587, BZ#1342989, BZ#1365689			
kernel-aarch64		BZ#1356009		BZ#1248185
kernel-rt	BZ#1328607	BZ#1209987, BZ#1258295, BZ#1269647, BZ#1303255	BZ#1297061	
kexec-tools	BZ#1282554	BZ#1180246		BZ#1372464
krb5	BZ#1146945, BZ#1292153	BZ#1347403		
ksc	BZ#906659	BZ#1272348, BZ#1328384		
libcacard				BZ#1249116
libcxl	BZ#1305080			
libdvdnav	BZ#1068814			
libdvdread	BZ#1326238			
libguestfs	BZ#1190669, BZ#1218766, BZ#1358332	BZ#1173695, BZ#1225789		
libgweather	BZ#1371550			
libica	BZ#1274390			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
libnftnl			BZ#1332585	
libnl3	BZ#1296058			
libosinfo	BZ#1257865, BZ#1282919			
libpfm	BZ#1321051	BZ#1276702		
libreoffice	BZ#1290148			
libreport	BZ#1258482, BZ#1289513			
libstoragemgmt			BZ#1119909	
libusnic_verbs			BZ#916384	
libvirt	BZ#735385, BZ#846810, BZ#1215968, BZ#1325996	BZ#1197592		BZ#1357468
libvma	BZ#1271624			
libvpd	BZ#1182031			
logrotate		BZ#1272236		
lorax		BZ#1272658		BZ#1341280
lvm2	BZ#1131777, BZ#1189221, BZ#1286285, BZ#1299977, BZ#1329235, BZ#1348336, BZ#1364244, BZ#1371597	BZ#1274676	BZ#1191630	BZ#1014758, BZ#1354396, BZ#1380521
mcelog	BZ#1336431			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
mdadm		BZ#1174622, BZ#1290494, BZ#1300579, BZ#1312837, BZ#1347749, BZ#1347762		BZ#1067292
memkind	BZ#1210910			
memtest86+	BZ#1280352			
mesa	BZ#1263120			
microcode_ctl		BZ#1292158		
mod_auth_openidc	BZ#1292561			
mod_security_crs	BZ#1150614			
mtx		BZ#1298647		
mutter				BZ#1360906
nautilus		BZ#1207646		
ndctl	BZ#1271425			
nettle	BZ#1252936			
nfs-utils				BZ#1359042
numactl		BZ#1270734		
numad				BZ#1360584
nvme-cli	BZ#1344730			
nvml	BZ#1274541			
opal-prd	BZ#1224121			
open-vm-tools	BZ#1268537			
opencryptoki	BZ#1185421			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
openldap	BZ#1292568	BZ#1249093		
openscap	BZ#1278147			BZ#1356547
openssl	BZ#1225379			
oprofile	BZ#1310950, BZ#1310951	BZ#1264443, BZ#1272136, BZ#1335145		BZ#1349077
os-prober		BZ#1300262		
oscap-anaconda-addon				BZ#1372791
other	BZ#1278795, BZ#1354626, BZ#1368484, BZ#1379689, BZ#1388471, BZ#1389121, BZ#1389316, BZ#1390661, BZ#1396085	BZ#1262007, BZ#1360188, BZ#1360338, BZ#1369837	BZ#1062759, BZ#1072107, BZ#1259547	BZ#1350802, BZ#1358836, BZ#1389245, BZ#1390565
OVMF			BZ#653382	
pacemaker	BZ#1288929, BZ#1303765	BZ#1219188, BZ#1268313, BZ#1284069, BZ#1286316, BZ#1287315, BZ#1287868, BZ#1337688, BZ#1338623, BZ#1346726		
pam	BZ#1273373			
pam_krb5		BZ#1263745		
pam_pkcs11				BZ#1367919
papi		BZ#1263666, BZ#1277931, BZ#1357587		
pavucontrol	BZ#1210846			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
pcp	BZ#1284307			
pcs	BZ#1164402, BZ#1315371, BZ#1315652, BZ#1327739		BZ#1158805, BZ#1305049	
perl		BZ#1223045, BZ#1263734, BZ#1344749, BZ#1365991		
perl-IO-Socket-SSL	BZ#1316377			
perl-Net-SSLeay	BZ#1316379			
perl-Socket		BZ#1200167		
pesign				BZ#1141263
php	BZ#1291667			
pidgin	BZ#1066457			
pki-core	BZ#1224365, BZ#1224642, BZ#1289323, BZ#1302136, BZ#1303175, BZ#1305622, BZ#1305992, BZ#1321491, BZ#1327683, BZ#1347466, BZ#1353005, BZ#1358439	BZ#1082663, BZ#1224382, BZ#1274419, BZ#1308772, BZ#1329365, BZ#1331596		BZ#1246635, BZ#1376488
policycoreutils				BZ#1345825
polkit		BZ#1310738		

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
poppler		BZ#1298616, BZ#1299479, BZ#1299481, BZ#1299490, BZ#1299500, BZ#1299503, BZ#1299506		
powerpc-utils		BZ#1347083, BZ#1366512		
procps-ng		BZ#1169349, BZ#1262864, BZ#1284087		
protobuf-c	BZ#1289666			
psacct		BZ#1249665		
pykickstart		BZ#1290244		
python	BZ#1289277, BZ#1315758			
python-blivet		BZ#1031589, BZ#1242666, BZ#1257997		BZ#1270883
python-dns		BZ#1312770		
python-gssapi	BZ#1292139			
python-netifaces	BZ#1303046			
python-pycurl	BZ#1260407	BZ#1153321		
python-rhsm	BZ#1104332, BZ#1346417			
python-schedutils	BZ#948381			
python-sphinx		BZ#966954, BZ#1291573		

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
qemu-kvm	BZ#1327599	BZ#1265427, BZ#1299116, BZ#1299250	BZ#1103193	BZ#1209707
quota	BZ#1155584	BZ#1072858, BZ#1207239, BZ#1305968		
realmd	BZ#1293390			BZ#1370457
rear				BZ#1320552
resource-agents		BZ#1325453		
rhythmbox	BZ#1298233			
rpm			BZ#1278924	
rsyslog	BZ#1223566, BZ#1303617			
rt-tests	BZ#1346771			
rteval		BZ#1312057		
ruby	BZ#1197720			
samba	BZ#1263322, BZ#1303076	BZ#1316899		
sapconf		BZ#1228550, BZ#1235608		
scap-security-guide				BZ#1378489
scap-workbench	BZ#1202854			
selinux-policy		BZ#1097775, BZ#1349356		
servicelog	BZ#1182028			
sg3_utils	BZ#1170719	BZ#1298739		
shadow-utils	BZ#1114081			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
sos	BZ#1187258, BZ#1246423, BZ#1293044	BZ#1296813		
squid	BZ#1273942			
sssd	BZ#789477, BZ#790113, BZ#874985, BZ#879333, BZ#988207, BZ#1007969, BZ#1031074, BZ#1059972, BZ#1140022, BZ#1287209, BZ#1290380, BZ#1310877, BZ#1325809	BZ#1300663, BZ#1369118, BZ#1373420	BZ#1068725, BZ#1311056	BZ#888739, BZ#1372814, BZ#1380436, BZ#1389796, BZ#1392441
sssd-docker			BZ#1200143	
strongimcv			BZ#755087	
subscription-manager	BZ#874735, BZ#1336880, BZ#1336883			
swig	BZ#1136487			
sysstat	BZ#1258990, BZ#1332662	BZ#846699, BZ#1224882, BZ#1267972, BZ#1328490		
system-config-kdump		BZ#1121590, BZ#1208191		
system-config-language	BZ#1328068			
system-switch-java	BZ#1283904			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
systemd	BZ#1142378, BZ#1265749, BZ#1305279	BZ#1230210, BZ#1266934, BZ#1267707, BZ#1301990, BZ#1306126, BZ#1308795, BZ#1360160	BZ#1284974	
systemtap	BZ#1289617			
tcsh	BZ#1315713			
telnet	BZ#1323094			
tftp	BZ#1311092			
tomcat	BZ#1133070, BZ#1287928	BZ#1201409, BZ#1208402, BZ#1221896, BZ#1240279, BZ#1277197		
tuned		BZ#1243807, BZ#1249618, BZ#1322001, BZ#1323283, BZ#1334479, BZ#1346715		
unbound	BZ#1245250			
unzip		BZ#1276744		
util-linux	BZ#587393, BZ#1153770, BZ#1298384			
valgrind	BZ#1271754, BZ#1296318			
vinagre	BZ#1291275			
virt-manager		BZ#1282276		
virt-who	BZ#1245035, BZ#1278637, BZ#1286945			

Component	New Features	Notable Bug Fixes	Technology Previews	Known Issues
vte	BZ#1103380			
xfsprogs	BZ#1309498			
xorg-x11-server		BZ#1326867		
xz	BZ#1160193			
yum	BZ#1186690, BZ#1274211			
yum-langpacks		BZ#1251388, BZ#1263241		
yum-utils	BZ#1192946, BZ#1335587			
zlib		BZ#1127330		
zsh		BZ#1267251, BZ#1267912, BZ#1291782, BZ#1302229, BZ#1321303, BZ#1338689		

APPENDIX C. REVISION HISTORY

Revision 0.2-6 **Tue Apr 17 2018** **Lenka Špačková**
Updated a recommendation related to the `sslwrap()` deprecation.

Revision 0.2-5 **Tue Feb 06 2018** **Lenka Špačková**
Added a missing Technology Preview - OVMF (Virtualization).
Added information regarding deprecation of containers using the `libvirt-lxc` tooling.

Revision 0.2-4 **Mon Oct 30 2017** **Lenka Špačková**
Added information on changes in the `ld` linker behavior to Deprecated Functionality.

Revision 0.2-3 **Wed Oct 11 2017** **Lenka Špačková**
Fixed workaround for the `megaraid_sas` known issue (Kernel).

Revision 0.2-2 **Wed Sep 13 2017** **Lenka Špačková**
Added information regarding limited support for visuals in the Xorg server.

Revision 0.2-1 **Fri Jul 14 2017** **Lenka Špačková**
Added `kexec` to Technology Previews (Kernel).

Revision 0.2-0 **Fri Jun 23 2017** **Lenka Špačková**
Improved an `iostat` bug fix description.

Revision 0.1-9 **Wed May 03 2017** **Lenka Špačková**
A new Pacemaker feature added to Clustering.

Revision 0.1-8 **Thu Apr 27 2017** **Lenka Špačková**
Red Hat Access Labs renamed to Red Hat Customer Portal Labs.

Revision 0.1-7 **Thu Mar 30 2017** **Lenka Špačková**
Added a new feature to Storage.

Revision 0.1-6 **Thu Mar 23 2017** **Lenka Špačková**
Updated the firewalld rebase description (Security).
Moved a SELinux-related bug fix description to the correct chapter (Security).

Revision 0.1-4 **Tue Feb 14 2017** **Lenka Špačková**
Updated the samba rebase description (Authentication and Interoperability).

Revision 0.1-2 **Fri Jan 20 2017** **Lenka Špačková**
Added a known issue related to `bind-dyndb-ldap` (Authentication and Interoperability).

Revision 0.1-1 **Fri Dec 16 2016** **Lenka Špačková**
Runtime Instrumentation for IBM z System has been moved to fully supported features (Hardware Enablement).
Added information regarding the default registration URL (System and Subscription Management).
Added a note on the WALinuxAgent rebase in the Extras channel (Virtualization).
Added a note about a configurable SSH key file for the ABRT reporter-upload tool (Compiler and Tools).

Revision 0.1-0 **Fri Nov 25 2016** **Lenka Špačková**
Added Intel DIMM management tools to Technology Previews (Hardware Enablement).
Added a known issue (Kernel).

Revision 0.0-9 **Mon Nov 21 2016** **Lenka Špačková**
Updated Known Issues (Authentication and Interoperability, Installation and Booting) and New Features (Compiler and Tools, Kernel, Storage).

Revision 0.0-8 **Thu Nov 03 2016** **Lenka Špačková**

Release of the Red Hat Enterprise Linux 7.3 Release Notes.

Revision 0.0-3 **Thu Aug 25 2016** **Lenka Špačková**

Release of the Red Hat Enterprise Linux 7.3 Beta Release Notes.