Red Hat Enterprise Linux 7

7.7 Release Notes

Release Notes for Red Hat Enterprise Linux 7.7

Last Updated: 2020-09-02

Red Hat Enterprise Linux 7 7.7 Release Notes

Release Notes for Red Hat Enterprise Linux 7.7

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 7.7 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 (RHEL) minor releases are an aggregation of individual security, enhancement, and bug fix errata. The *Red Hat Enterprise Linux 7.7 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.

CHAPTER 1. OVERVIEW

- Live patching for the kernel, **kpatch**, is now available, which enables you to consume Critical and Important CVEs fixes without the need to reboot your system. For details, see Section 4.7, "Kernel".
- The IMA/EVM feature for verifying file system integrity is now supported on all architectures. See details in Section 4.7, "Kernel".
- The Image Builder is now fully supported. Cloud images can be built for Amazon Web Services, VMware vSphere, and OpenStack. See more information in Section 4.6, "Installation and Booting".
- **Python 3.6** is now available in RHEL 7. For details, see Section 4.3, "Compiler and Tools".
- The **tangd_port_t** SELinux type allows changes of the default port for Tang when deploying a Network-Bound Disc Encryption (NBDE) server. For more security enhancements, see Section 4.10, "Security".

Additional resources

- **Capabilities and limits** of Red Hat Enterprise Linux 7 as compared to other versions of the system are available in the Knowledgebase article Red Hat Enterprise Linux technology capabilities and limits.
- The Package Manifest document provides a **package listing** for RHEL 7.
- The **Red Hat Insights** service, which enables you to proactively identify, examine, and resolve known technical issues, is now available with all RHEL subscriptions. For instructions on how to install the Red Hat Insights client and register your system to the service, see the Red Hat Insights Get Started page.

In-place upgrade

An in-place upgrade offers a way of upgrading a system to a new major release of Red Hat Enterprise Linux by replacing the existing operating system. For a list of currently supported upgrade pahts, see Supported in-place upgrade paths for Red Hat Enterprise Linux .

In-place upgrade from RHEL 6 to RHEL 7

The procedure of an in-place upgrade from RHEL 6 to RHEL 7 and the usage of the **Preupgrade Assistant** and the **Red Hat Upgrade Tool** is documented in the Knowledgebase solution How do I upgrade from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7?. Further details are provided in the RHEL 7 Migration Planning Guide. Note that the **Preupgrade Assistant** and the **Red Hat Upgrade Tool** are available in the RHEL 6 Extras repository.

If you are using CentOS 6 or Oracle Linux 6, you can convert your operating system to RHEL 6 using the **convert2rhel** utility prior to upgrading to RHEL 7. For instructions, see How to convert from CentOS or Oracle Linux to RHEL.

In-place upgrade from RHEL 7 to RHEL 8

Instructions on how to perform an in-place upgrade from RHEL 7 to RHEL 8 using the **Leapp** utility are provided by the document Upgrading from RHEL 7 to RHEL 8 . Major differences between RHEL 7 and RHEL 8 are documented in Considerations in adopting RHEL 8 . The **Leapp** utility is available in the RHEL 7 Extras repository.

If you are using CentOS 7 or Oracle Linux 7, you can convert your operating system to RHEL 7 using the **convert2rhel** utility prior to upgrading to RHEL 8. For instructions, see How to convert from CentOS or Oracle Linux to RHEL.

Product life cycle

Red Hat Enterprise Linux 7 is now in the Maintenance Support 1 phase of the product life cycle. Future minor releases will focus on retaining and improving stability and reliability rather than adding new features. See the Red Hat Enterprise Linux Life Cycle document for more details.

Red Hat Customer Portal Labs

Red Hat Customer Portal Labs is a set of tools in a section of the Customer Portal. 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:

- Registration Assistant
- Kickstart Generator
- Product Life Cycle Checker
- Red Hat Product Certificates
- Red Hat Satellite Upgrade Helper
- Red Hat CVE Checker
- JVM Options Configuration Tool
- Load Balancer Configuration Tool
- Red Hat Code Browser
- Yum Repository Configuration Helper

CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 7 is available on the following architectures: [1]

- 64-bit AMD
- 64-bit Intel
- IBM POWER7+ (big endian)
- IBM POWER8 (big endian) [2]
- IBM POWER8 (little endian) [3]
- IBM POWER9 (little endian) [4][5]
- IBM Z [4][6]
- 64-bit ARM [4]

The Red Hat Enterprise Linux 7.7 is distributed with the kernel version 3.10.0-1062, which provides support for the following architectures:

- 64-bit AMD
- 64-bit Intel
- IBM POWER7+ (big endian)
- IBM POWER8 (big endian)
- IBM POWER8 (little endian)
- IBM Z (kernel version 3.10)

The following architectures remain fully supported and continue to receive z-stream security and bug fix updates in accordance with the Red Hat Enterprise Linux Life Cycle :

- IBM POWER9 (little endian)
- IBM Z - Structure A (kernel version 4.14)
- 64-bit ARM

[1] Note that the Red Hat Enterprise Linux 7 installation is supported only on 64-bit hardware. Red Hat Enterprise Linux 7 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 POWER8 (big endian) are currently supported as KVM guests on Red Hat Enterprise Linux 7 POWER8 systems that run the KVM hypervisor, and on PowerVM.

[3] Red Hat Enterprise Linux 7 POWER8 (little endian) is currently supported as a KVM guest on Red Hat Enterprise Linux 7 POWER8 systems that run the KVM hypervisor, and on PowerVM. In addition, Red Hat Enterprise Linux 7 POWER8 (little endian) guests are supported on Red Hat Enterprise Linux 7 POWER9 systems that run the KVM hypervisor in POWER8-compatibility mode on version 4.14 kernel using the **kernel-alt** package.

[4] This architecture is supported with the kernel version 4.14, provided by the **kernel-alt** packages. For details, see the Red Hat Enterprise Linux 7.5 Release Notes.

[5] Red Hat Enterprise Linux 7 POWER9 (little endian) is currently supported as a KVM guest on Red Hat Enterprise Linux 7 POWER9 systems that run the KVM hypervisor on version 4.14 kernel using the **kernel-alt** package, and on PowerVM.

[6] Red Hat Enterprise Linux 7 for IBM Z (both the 3.10 kernel version and the 4.14 kernel version) is currently supported as a KVM guest on Red Hat Enterprise Linux 7 for IBM Z hosts that run the KVM hypervisor on version 4.14 kernel using the **kernel-alt** package.

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 7.7. These changes include added or updated **proc** entries, **sysctl**, and **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

New kernel parameters

usbcore.quirks = [USB]

This parameter provides a list of quirk entries to augment the built-in usb core quirk list.
The entries are separated by commas. Each entry has the form **VendorID:ProductID:Flags**.

The **IDs** are 4-digit hex numbers and **Flags** is a set of letters. Each letter will change the built-in quirk; setting it if it is clear and clearing it if it is set. The letters have the following meanings:

- a = **USB_QUIRK_STRING_FETCH_255** (string descriptors must not be fetched using a 255-byte read);
- b = **USB_QUIRK_RESET_RESUME** (device cannot resume correctly so reset it instead);
- c = **USB_QUIRK_NO_SET_INTF** (device cannot handle Set-Interface requests);
- d = **USB_QUIRK_CONFIG_INTF_STRINGS** (device cannot handle its Configuration or Interface strings);
- e = **USB_QUIRK_RESET** (device cannot be reset (e.g morph devices), do not use reset);
- f = **USB_QUIRK_HONOR_BNUMINTERFACES** (device has more interface descriptions than the **bNumInterfaces** count, and cannot handle talking to these interfaces);
- g = **USB_QUIRK_DELAY_INIT** (device needs a pause during initialization, after we read the device descriptor);
- h = **USB_QUIRK_LINEAR_UFRAME_INTR_BINTERVAL** (For high speed and super speed interrupt endpoints, the USB 2.0 and USB 3.0 spec require the interval in microframes (1 microframe = 125 microseconds) to be calculated as interval = 2 ^ (**bInterval**-1). Devices with this quirk report their **bInterval** as the result of this calculation instead of the exponent variable used in the calculation);
- i = **USB_QUIRK_DEVICE_QUALIFIER** (device cannot handle device_qualifier descriptor requests);
- j = **USB_QUIRK_IGNORE_REMOTE_WAKEUP** (device generates spurious wakeup, ignore remote wakeup capability);
- k = **USB_QUIRK_NO_LPM** (device cannot handle Link Power Management);
- l = **USB_QUIRK_LINEAR_FRAME_INTR_BINTERVAL** (Device reports its **bInterval** as linear frames instead of the USB 2.0 calculation);
- m = **USB_QUIRK_DISCONNECT_SUSPEND** (Device needs to be disconnected before suspend to prevent spurious wakeup);
- n = **USB_QUIRK_DELAY_CTRL_MSG** (Device needs a pause after every control message);

The example entry:

```
quirks=0781:5580:bk,0a5c:5834:gij
```

ppc_tm = [PPC]

Disables Hardware Transactional Memory.
Format: {"off"}

cgroup.memory = [KNL]

Passes options to the cgroup memory controller.
Format: <string>

nokmem – This option disables kernel memory accounting.

mds = [X86,INTEL]

Controls mitigation for the Micro-architectural Data Sampling (MDS) vulnerability.
Certain CPUs are vulnerable to an exploit against CPU internal buffers which can forward information to a disclosure gadget under certain conditions.

In vulnerable processors, the speculatively forwarded data can be used in a cache side channel attack, to access data to which the attacker does not have direct access.

The options are:

- **full** - Enable MDS mitigation on vulnerable CPUs.
- **full,nosmt** - Enable MDS mitigation and disable Simultaneous multithreading (SMT) on vulnerable CPUs.
- **off** - Unconditionally disable MDS mitigation.
  Not specifying this option is equivalent to **mds=full**.

mitigations = [X86,PPC,S390]

Controls optional mitigations for CPU vulnerabilities. This is a set of curated, arch-independent options, each of which is an aggregation of existing arch-specific options.
The options are:

- **off** - Disable all optional CPU mitigations. This improves system performance, but it may also expose users to several CPU vulnerabilities.
  Equivalent to:
  - **nopti [X86,PPC]**
  - **nospectre_v1 [PPC]**
  - **nobp=0 [S390]**
  - **nospectre_v2 [X86,PPC,S390]**
  - **spec_store_bypass_disable=off [X86,PPC]**
  - **l1tf=off [X86]**

    - **mds=off [X86]**

- **auto** (default) - Mitigate all CPU vulnerabilities, but leave Simultaneous multithreading (SMT) enabled, even if it's vulnerable. This is for users who do not want to be surprised by SMT getting disabled across kernel upgrades, or who have other ways of avoiding SMT-based attacks.
  Equivalent to:

    - (default behavior)

- **auto,nosmt** - Mitigate all CPU vulnerabilities, disabling Simultaneous multithreading (SMT) if needed. This is for users who always want to be fully mitigated, even if it means losing SMT.
  Equivalent to:

    - **l1tf=flush,nosmt [X86]**

    - **mds=full,nosmt [X86]**

watchdog_thresh = [KNL]

Sets the hard lockup detector stall duration threshold in seconds.
The soft lockup detector threshold is set to twice the value.

A value of 0 disables both lockup detectors. Default is 10 seconds.

novmcoredd [KNL,KDUMP]

Disables device dump. The device dump allows drivers to append dump data to vmcore so you can collect driver specified debug info.
Drivers can append the data without any limit and this data is stored in memory, so this may cause significant memory stress.

Disabling device dump can help save memory but the driver debug data will be no longer available.

This parameter is only available when **CONFIG_PROC_VMCORE_DEVICE_DUMP** is set.

Updated kernel parameters

resource_alignment

Specifies alignment and device to reassign aligned memory resources.
Format:

- **[<order of align>@][<domain>:]<bus>:<slot>.<func>[; …]**

- **[<order of align>@]pci:<vendor>:<device>\[:<subvendor>:<subdevice>][; …]**

If **<order of align>** is not specified, PAGE_SIZE is used as alignment. PCI-PCI bridge can be specified, if resource windows need to be expanded.

irqaffinity = [SMP]

Sets the default irq affinity mask.
Format:

- **<cpu number>,…,<cpu number>**

- **<cpu number>-<cpu number>**
- drivers (must be a positive range in ascending order)
- mixture **<cpu number>,...,<cpu number>-<cpu number>**
  Drivers will use drivers' affinity masks for default interrupt assignment instead of placing them all on CPU0.

The options are:

- **auto** (default) - Mitigate all CPU vulnerabilities, but leave Simultaneous multithreading (SMT) enabled, even if it is vulnerable. This is for users who do not want to be surprised by SMT getting disabled across kernel upgrades, or who have other ways of avoiding SMT-based attacks. Equivalent to: (default behavior)
- **auto,nosmt** - Mitigate all CPU vulnerabilities, disabling Simultaneous multithreading (SMT) if needed. This is for users who always want to be fully mitigated, even if it means losing SMT. Equivalent to:
  - **l1tf=flush,nosmt [X86]**
  - **mds=full,nosmt [X86]**

New /proc/sys/net/core parameters

bpf_jit_kallsyms

If Berkeley Packet Filter Just in Time compiler is enabled, the compiled images are unknown addresses to the kernel. It means they neither show up in traces nor in the /**proc**/**kallsyms** file. This enables export of these addresses, which can be used for debugging/tracing. If the **bpf_jit_harden** parameter is enabled, this feature is disabled.
Possible values are:

0 – Disable Just in Time (JIT) **kallsyms** export (default value).

1 – Enable Just in Time (JIT) **kallsyms** export for privileged users only.

Updated /proc/sys/fs parameters

dentry-state

Dentries are dynamically allocated and deallocated.
From **linux**/**include**/**linux**/**dcache.h**:

```
struct dentry_stat_t dentry_stat {
        int nr_dentry;
        int nr_unused;
        int age_limit;          (age in seconds)
        int want_pages;         (pages requested by system)
        int nr_negative;        (# of unused negative dentries)
        int dummy;              (Reserved for future use)
};
```

The **nr_dentry** number shows the total number of dentries allocated (active + unused).

The **nr_unused** number shows the number of dentries that are not actively used, but are saved in the least recently used (LRU) list for future reuse.

The **age_limit** number is the age in seconds after which **dcache** entries can be reclaimed when memory is short and the **want_pages** number is nonzero when the **shrink_dcache_pages()** function has been called and the **dcache** is not pruned yet.

The **nr_negative** number shows the number of unused dentries that are also negative dentries which do not map to any files. Instead, they help speeding up rejection of non-existing files provided by the users.

CHAPTER 4. NEW FEATURES

This chapter documents new features and major enhancements introduced in Red Hat Enterprise Linux 7.7.

4.1. AUTHENTICATION AND INTEROPERABILITY

SSSD now fully supports sudo rules stored in AD

The System Security Services Daemon (SSSD) now fully supports **sudo** rules stored in Active Directory (AD). This feature was first introduced in Red Hat Enterprise Linux 7.0 as a Technology Preview. Note that the administrator must update the AD schema to support **sudo** rules.

(BZ#1664447)

SSSD no longer uses the fallback_homedir value from the [nss] section as fallback for AD domains

Prior to RHEL 7.7, the SSSD **fallback_homedir** parameter in an Active Directory (AD) provider had no default value. If **fallback_homedir** was not set, SSSD used instead the value from the same parameter from the **[nss]** section in the **/etc/sssd/sssd.conf** file. To increase security, SSSD in RHEL 7.7 introduced a default value for **fallback_homedir**. As a consequence, SSSD no longer falls back to the value set in the **[nss]** section. If you want to use a different value than the default for the **fallback_homedir** parameter in an AD domain, you must manually set it in the domain's section.

(BZ#1740779)

Directory Server rebased to version 1.3.9.1

The **389-ds-base** packages have been upgraded to upstream version 1.3.9.1, which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating: 1.3.9 Release Notes.

(BZ#1645359)

The Directory Server Auto Membership plug-in can now be additionally invoked by modify operations

This update enhances the Auto Membership plug-in in Directory Server to work with modify operations. Previously, the plug-in was only invoked by **ADD** operations. When an administrator changed a user entry, and that change impacted what Auto Membership groups the user belonged to, the user was not removed from the old group and only added to the new group. With the enhancement provided by this update, users can now configure that Directory Server removes the user from the old group in the mentioned scenario.

To enable the new behavior, set the **autoMemberProcessModifyOps** attribute in the **cn=Auto Membership Plugin,cn=plugins,cn=config** entry to **on**.

(BZ#1438144)

The replicaLastUpdateStatusJSON status attribute has been added to replication agreements in Directory Server

This update introduces the **replicaLastUpdateStatusJSON** status attribute to the **cn=<replication_agreement_name>,cn=replica,cn=<suffix_DN>,cn=mapping tree,cn=config** entry. The status displayed in the **replicaLastUpdateStatus** attribute was vague and unclear. The new attribute

provides a clear status message and result code and can be parsed by other applications that support the JSON format.

(BZ#1561769)

IdM now provides a utility to promote a CA to a CRL generation master

With this enhancement, administrators can promote an existing Identity Management (IdM) certificate authority (CA) to a certificate revocation list (CRL) generation master or remove this feature from a CA. Previously, multiple manual steps were required to configure an IdM CA as CRL generation master, and the procedure was error-prone. As a result, administrators can now use the **ipa-crlgen-manage enable** and **ipa-crlgen-manage disable** commands to enable and disable CRL generation on an IdM CA.

(BZ#1690037)

A command to detect and remove orphaned automember rules has been added to IdM

Automember rules in Identity Management (IdM) can refer to a hostgroup or a group that has been deleted. Previously, the **ipa automember-rebuild** command failed unexpectedly and it was difficult to diagnose the reason of the failure. This enhancement adds **ipa automember-find-orphans** to IdM to IdM to identify and remove such orphaned automember rules.

(BZ#1390757)

IdM now supports IP addresses in the SAN extension of certificates

In certain situations, administrators need to issue certificates with an IP address in the Subject Alternative Name (SAN) extension. This update adds this feature. As a result, administrators can set an IP address in the SAN extension if the address is managed in the IdM DNS service and associated with the subject host or service principal.

(BZ#1586268)

IdM now supports renewing expired system certificates when the server is offline

With this enhancement, administrators can renew expired system certificates when Identity Management (IdM) is offline. When a system certificate expires, IdM fails to start. The new **ipa-cert-fix** command replaces the workaround to manually set the date back to proceed with the renewal process. As a result, the downtime and support costs reduce in the mentioned scenario.

(BZ#1690191)

pki-core rebased to version 10.5.16

The *pki-core* packages have been upgraded to upstream version 10.5.16, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1633422)

Certificate System can now create CSRs with SKI extension for external CA signing

With this enhancement, Certificate System supports creating a certificate signing request (CSR) with the Subject Key Identifier (SKI) extension for external certificate authority (CA) signing. Certain CAs require this extension either with a particular value or derived from the CA public key. As a result, administrators can now use the **pki_req_ski** parameter in the configuration file passed to the **pkispawn** utility to create a CSR with SKI extension.

(BZ#1491453)

Uninstalling Certificate System no longer removes all log files

Previously, Certificate System removed all corresponding logs when you uninstalled subsystems. With this update, by default, the pkidestroy utility no longer removes the logs. To remove the logs when you uninstall a subsystem, pass the new --remove-logs parameter to pkidestroy. Additionally, this update adds the --force parameter to pkidestroy. Previously, an incomplete installation left some files and directories, which prevented a complete uninstallation of a Certificate System instance. Pass --force to pkidestroy to completely remove a subsystem and all corresponding files of an instance.

(BZ#1372056)

The pkispawn utility now supports using keys created in the NSS database during CA, KRA, and OCSP installations

Previously, during a Certificate System installation, the pkispawn utility only supported creating new keys and importing existing keys for system certificates. With this enhancement, pkispawn now supports using keys the administrator generates directly in the NSS database during certificate authority (CA), key recovery authority (KRA), and online certificate status protocol (OCSP) installations.

(BZ#1616134)

Certificate System now preserves the logs of previous installations when reinstalling the service

Previously, the **pkispawn** utility reported a name collision error when installing a Certificate System subsystem on a server with an existing Certificate System log directory structure. With this enhancement, Certificate System reuses the existing log directory structure to preserve logs of previous installations.

(BZ#1644769)

Certificate System now supports additional strong ciphers by default

With this update, the following additional ciphers, which are compliant with the Federal Information Processing Standard (FIPS), are enabled by default in Certificate System:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384

For a full list of enabled ciphers, enter:

```
# /usr/lib64/nss/unsupported-tools/listsuites | grep -B1 --no-group-separator "Enabled"
```

If you use a Hardware Security Module (HSM) with Certificate System, see the documentation of the HSM for supported ciphers.

(BZ#1554055)

The samba packages have been to version 4.9.1

The **samba** packages have been upgraded to upstream version 4.9.1, which provides a number of bug fixes and enhancements over the previous version. The most notable changes include:

- The Clustered Trivial Database (CTDB) configuration has been changed completely. Administrators must now specify parameters for the **ctdb** service and corresponding utilities in the **/etc/ctdb/ctdb.conf** file in a format similar to the Samba configuration. For further details, see the **ctdb.conf(5)** man page. Use the **/usr/share/doc/ctdb/examples/config_migrate.sh** script to migrate the current configuration.

- The default values of the following parameters in the **/etc/samba/smb.conf** file have been changed as follows:

  - **map readonly**: **no**
  - **store dos attributes**: **yes**
  - **ea support**: **yes**
  - **full_audit:success**: Not set
  - **full_audit:failure**: Not set

- The **net ads setspn** command has been added for managing Windows Service Principal Names (SPN) on Active Directory (AD). This command provides the same basic functionality as the **setspn.exe** utility on Windows. For example, administrators can use it to add, delete, and list Windows SPNs stored in an AD computer object.

- The **net ads keytab add** command no longer attempts to convert the service class passed to the command into a Windows SPN, which is then added to the AD computer object. By default, the command now only updates the keytab file. The new **net ads add_update_ads** command has been added to preserve the previous behavior. However, administrators should use the new **net ads setspn add** command instead.

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.

For further information about notable changes, read the upstream release notes before updating: https://www.samba.org/samba/history/samba-4.9.0.html

(BZ#1649434)

4.2. CLUSTERING

Maximum size of a supported RHEL HA cluster increased from 16 to 32 nodes

With this release, Red Hat supports cluster deployments of up to 32 full cluster nodes.

(BZ#1374857)

Improved status display of fencing actions

The output of the **pcs status** command now shows failed and pending fence actions.

(BZ#1461964)

4.3. COMPILER AND TOOLS

New packages: python3

New **python3** packages are available in RHEL 7, which provide the Python 3.6 interpreter, as well as the **pip** and **setuptools** utilities. Previously, Python 3 versions were available only as a part of Red Hat Software Collections.

When installing, invoking, or otherwise interacting with Python 3, always specify the major version of Python. For example, to install Python 3, use the **yum install python3** command. All Python-related commands should also include the version, for example, **pip3**.

Note that Python 3 is the default Python implementation in RHEL 8, so it is advisable to migrate your Python 2 code to Python 3. For more information on how to migrate large code bases to Python 3, see The Conservative Python 3 Porting Guide.

(BZ#1597718)

New packages: compat-sap-c++-8

The **compat-sap-c++-8** packages contain the **libstdc++** library named **compat-sap-c++-8.so**, which is a runtime compatibility library needed for SAP applications. The **compat-sap-c++-8** packages are based on GCC 8.

(BZ#1669683)

The elfutils packages have been rebased to version 0.176

The **elfutils** packages have been upgraded to upstream version 0.176. Notable changes include:

- Various bugs related to multiple CVEs have been fixed.
- The **libdw** library has been extended with the **dwelf_elf_begin()** function which is a variant of **elf_begin()** that handles compressed files.
- The **eu-readelf** tool now recognizes and prints out GNU Property notes and GNU Build Attribute ELF Notes with the **--notes** or **-n** options.
- A new **--reloc-debug-sections-only** option has been added to the **eu-strip** tool to resolve all trivial relocations between debug sections in place without any other stripping. This functionality is relevant only for **ET_REL** files in certain circumstances.
- A new function **dwarf_next_lines** has been added to the **libdw** library. This function reads **.debug_line** data without CU.
- The **dwarf_begin_elf** function from the **libdw** library now accepts ELF files containing only **.debug_line** or **.debug_frame** sections.

(BZ#1676504)

gcc-libraries rebased to version 8.3.1

The **gcc-libraries** packages have been updated to the upstream version 8.3.1 which brings a number of bug fixes.

(BZ#1551629)

Geolite2 Databases are now available

This update introduces Geolite2 Databases as an addition to the legacy Geolite Databases, provided by the **GeoIP** package.

Geolite2 Databases are provided by multiple packages. The **libmaxminddb** package includes the library and the **mmdblookup** command line tool, which enables manual searching of addresses. The **geoipupdate** binary from the legacy **GeoIP** package is now provided by the **geoipupdate** package, and is capable of downloading both legacy databases and the new Geolite2 databases.

The **GeoIP** package, together with the legacy database, is no longer supported in upstream, and is not distributed with RHEL 8.

(BZ#1643472, BZ#1643470, BZ#1643464)

Date formatting updates for the Japanese Reiwa era

The GNU C Library now provides correct Japanese era name formatting for the Reiwa era starting on May 1st, 2019. The time handling API data has been updated, including the data used by the **strftime** and **strptime** functions. All APIs will correctly print the Reiwa era including when **strftime** is used along with one of the era conversion specifiers such as **%EC**, **%EY**, or **%Ey**.

(BZ#1555189)

SystemTap rebased to version 4.0

The SystemTap instrumentation tool has been upgraded to upstream version 4.0. Notable improvements include:

- The extended Berkeley Packet Filter (eBPF) backend has been improved, especially for strings and functions. To use this backend, start **SystemTap** with the **--runtime=bpf** option.
- A new export network service for use with the Prometheus monitoring system has been added.
- The system call probing implementation has been improved to use the kernel tracepoints if necessary.

(BZ#1669605)

Valgrind rebased to version 3.14

The Valgrind packages have been upgraded to upstream version 3.14, which provides a number of bug fixes and enhancements over the previous version:

- Valgrind can now process integer and string vector instructions for the z13 processor of the IBM Z architecture.
- An option **--keep-debuginfo=no|yes** has been added to retain debugging information for unloaded code. This allows saved stack traces to include file and line information in more cases. For more information and known limitations, see the Valgrind user manual.

- The Helgrind tool can now be configured to compute full history stack traces as deltas with the new **--delta-stacktrace=yes|no** option. As a result, keeping full Helgrind history with the **--history-level=full** option can be up to 25% faster when **--delta-stacktrace=yes** is added.

- False positive rate in the Memcheck tool has been reduced on the AMD64 and 64-bit ARM architectures. Notably, you can use the **--expensive-definedness-checks=no|auto|yes** option to control analysis for the expensive definedness checks without loss of precision.

(BZ#1519410)

Performance Co-Pilot rebased to version 4.3.2

The Performance Co-Pilot (PCP) has been updated to upstream version 4.3.2. Notable improvements include:

- The **pcp-dstat** tool now includes historical analysis and Comma-separated Values (CSV) format output.

- The log utilities can use metric labels and help text records.

- The **pmdaperfevent** tool now reports the correct CPU numbers at the lower Simultaneous Multi Threading (SMT) levels.

- The **pmdapostgresql** tool now supports **Postgres** series 10.x.

- The **pmdaredis** tool now supports **Redis** series 5.x.

- The **pmdabcc** tool has been enhanced with dynamic process filtering and per-process syscalls, ucalls, and ustat.

- The **pmdammv** tool now exports metric labels, and the format version is increased to 3.

- The **pmdagfs2** tool supports additional glock and glock holder metrics.

- Several fixes have been made to the SELinux policy.

- The **pmcd** utility now supports PMDA suspend and resume (fencing) without configuration changes.

- Pressure-stall information metrics are now reported.

- Additional VDO metrics are now reported.

- The **pcp-atop** tool now reports statistics for pressure stall information, infiniband, perf_event, and NVIDIA GPUs.

- The **pmlogger** and **pmie** tools can now use **systemd** timers as an alternative to cron jobs.

(BZ#1647308, BZ#1641161)

ptp4l now supports team interfaces in active-backup mode

With this update, support for team interfaces in active-backup mode has been added into the **PTP Boundary/Ordinary Clock** (ptp4l).

(BZ#1650672)

linuxptp rebased to version 2.0

The **linuxptp** packages have been upgraded to upstream version 2.0, which provides a number of bug fixes and enhancements over the previous version.

The most notable features are as follows:

- Support for unicast messaging has been added
- Support for telecom G.8275.1 and G.8275.2 profiles has been added
- Support for the NetSync Monitor (NSM) protocol has been added
- Implementation of transparent clock (TC) has been added

(BZ#1623919)

The DateTime::TimeZone Perl module is now aware of recent time zone updates

The Olson time zone database has been updated to version 2018i. Previously, applications written in the Perl language that use the **DateTime::TimeZone** module mishandled time zones that changed their specifications since version 2017b due to the outdated database.

(BZ#1537984)

The trace-cmd packages have been updated to version 2.7

The updated packages provide the latest bug fixes and upstream features. As a result, the Red Hat Enterprise Linux users can now use an up-to-date **trace-cmd** command.

(BZ#1655111)

vim rebased to version 7.4.629

The **vim** packages have been upgraded to upstream version 7.4.629, which is in RHEL 6. This version provides a number of bug fixes and enhancements over the previous version.

Notable enhancements include the **breakindent** feature. For more information about the feature, see **:help breakindent** in Vim.

(BZ#1563419)

4.4. DESKTOP

cups-filters updated

The **cups-filters** packages, distributed in version 1.0.35, have been updated to provide the following enhancements:

- The **cups-browsed** daemon, which provides the functionality removed from CUPS since the version 1.5, has been rebased to version 1.13.4, excluding the support for CUPS temporary queues.
- A new backend, **implicitclass**, has been introduced to support high availability and load balancing.

(BZ#1485502)

Mutter now allows for mass-deployable homogenized display configuration

The **Mutter** window manager now makes it possible to deploy pre-set display configurations for all users on a system. As a result, **Mutter** no longer requires that the configuration for each user is copied to its own configuration directory, but it can use a system wide configuration file instead. This feature makes **Mutter** suitable for mass deployment of homogenized display configuration.

To set the configuration for a single user, create and populate the **~/.config/monitors.xml** file. For the login screen in particular, use the **~/gdm/.config/monitors.xml** file. For system-wide configurations, use the **/etc/xdg/monitors.xml** file.

(BZ#1583825)

4.5. FILE SYSTEMS

Improved quota reports

The **quota** tool in non-verbose mode now distinguishes between a file system with no limits and a file system with limits but with no used resources. Previously, **none** was printed for both use cases, which was confusing.

(BZ#1601109)

4.6. INSTALLATION AND BOOTING

The graphical installation program now detects if SMT is enabled

Previously, the RHEL 7 graphical installation program did not detect if Simultaneous Multithreading (SMT) was enabled on a system. With this update, the installation program now detects if SMT is enabled on a system. If it is enabled, a warning message is displayed in the **Status** bar, which is located at the bottom of the **Installation Summary** window.

(BZ#1678353)

New --g-libs option for the find-debuginfo.sh script

This update introduces the new **--g-libs** option for the **find-debuginfo.sh** script. This new option is an alternative to previous **-g** option, which instructed the script to remove only debugging symbols from both binary and library files. The new **--g-libs** option works the same way as **-g**, but only for library files. The binary files are stripped completely.

(BZ#1663264)

The Image Builder rebased to version 19.7.33 and fully supported

The Image Builder, provided by the **lorax-composer** package in the RHEL 7 Extras Channel, has been upgraded to version 19.7.33.

Notable changes in this version include:

- The Image Builder, previously available as Technology Preview, is now fully supported.
- Cloud images can be built for Amazon Web Services, VMware vSphere, and OpenStack.
- A Red Hat Content Delivery Network (CDN) repository mirror is no longer needed.
- You can now set a host name and create users.

- Boot loader parameters can be set, such as disabling Simultaneous Multi-Threading (SMT) with the **nosmt=force** option. This is only possible from **composer-cli** tool on command line.
- The web console UI can now edit external repositories ("sources").
- The Image Builder can now run with SElinux in enforcing mode.

To access the Image Builder functionality, use a command-line interface in the **composer-cli** utility, or a graphical user interface in the RHEL 7 web console from the **cockpit-composer** package.

(BZ#1713880, BZ#1656105, BZ#1654795, BZ#1689314, BZ#1688335)

4.7. KERNEL

Kernel version in RHEL 7.7

Red Hat Enterprise Linux 7.7 is distributed with the kernel version 3.10.0-1062.

(BZ#1801759)

Live patching for the kernel is now available

Live patching for the kernel, **kpatch**, provides a mechanism to patch a running kernel without rebooting or restarting any processes. Live kernel patches will be provided for selected minor release streams of RHEL covered under the Extended Update Support (EUS) policy to remediate Critical and Important CVEs.

To subscribe to the **kpatch** stream for the RHEL 7.7 version of kernel, install the **kpatch-patch-3_10_0-1062** package provided by the RHEA-2019:2011 advisory.

For more information, see Applying patches with kernel live patching in the Kernel Administration Guide.

(BZ#1728504)

The IMA and EVM features are now supported on all architectures

The Integrity Measurement Architecture (IMA) and Extended Verification Module (EVM) are now fully supported on all available architectures. In RHEL 7.6, they were supported only on the AMD64 and Intel 64 architecture.

IMA and EVM enable the kernel to check the integrity of files at runtime using labels attached to extended attributes. You can use IMA and EVM to monitor if files have been accidentally or maliciously altered.

The **ima-evm-utils** package provides userspace utilities to interface between user applications and the kernel features.

(BZ#1636601)

Spectre V2 mitigation default changed from IBRS to Retpoline in new installations of RHEL 7.7

The default mitigation for the Spectre V2 vulnerability (CVE-2017-5715) for systems with the 6th Generation Intel Core Processors and its close derivatives [1] has changed from Indirect Branch Restricted Speculation (IBRS) to Retpoline in new installations of RHEL 7.7. Red Hat has implemented this change as a result of Intel's recommendations to align with the defaults used in the Linux community

and to restore lost performance. However, note that using Retpoline in some cases may not fully mitigate Spectre V2. Intel's Retpoline document [2] describes any cases of exposure. This document also states that the risk of an attack is low.

For installations of RHEL 7.6 and prior, IBRS is still the default mitigation. New installations of RHEL 7.7 and later versions will have "spectre_v2=retpoline" added to the kernel command line. No change will be made for upgrades to RHEL 7.7 from earlier versions of RHEL 7.

Note that users can select which spectre_v2 mitigation will be used. To select Retpoline: a) Add the "spectre_v2=retpoline" flag to the kernel command line, and reboot. b) Alternatively, issue the following command at runtime: "echo 1 > /sys/kernel/debug/x86/retp_enabled"

To select IBRS: a) Remove the "spectre_v2=retpoline" flag from the kernel command line, and reboot. b) Alternatively, issue the following command at runtime: "echo 1 > /sys/kernel/debug/x86/ibrs_enabled"

If one or more kernel modules were not built with Retpoline support, the **/sys/devices/system/cpu/vulnerabilities/spectre_v2** file will indicate vulnerability and the **/var/log/messages** file will identify the offending modules. See How to determine which modules are responsible for spectre_v2 returning "Vulnerable: Retpoline with unsafe module(s)"? for further information.

[1] "6th generation Intel Core Processors and its close derivatives" are what the Intel's Retpoline document refers to as "Skylake-generation".

[2] Retpoline: A Branch Target Injection Mitigation - White Paper

(BZ#1653428, BZ#1659626)

PMTU discovery and route redirection is now supported with VXLAN and GENEVE tunnels

Previously, the kernel in Red Hat Enterprise Linux (RHEL) did not handle Internet Control Message Protocol (ICMP) and ICMPv6 messages for Virtual Extensible LAN (VXLAN) and Generic Network Virtualization Encapsulation (GENEVE) tunnels. As a consequence, Path MTU (PMTU) discovery and route redirection was not supported with VXLAN and GENEVE tunnels. With this update, the kernel handles ICMP "Destination Unreachable" and "Redirect Message", as well as ICMPv6 "Packet Too Big" and "Destination Unreachable" error messages by adjusting the PMTU and modifying forwarding information. As a result, PMTU discovery and route redirection are now supported with VXLAN and GENEVE tunnels.

(BZ#1511372)

A new kernel command-line option to disable hardware transactional memory on IBM POWER

RHEL 7.7 introduces the **ppc_tm=off** kernel command-line option. When the user passes **ppc_tm=off** at boot time, the kernel disables hardware transactional memory on IBM POWER systems and makes it unavailable to applications. Previously, the RHEL 7 kernel unconditionally made the hardware transactional memory feature on IBM POWER systems available to applications whenever it was supported by hardware and firmware.

(BZ#1694778)

Intel® Omni-Path Architecture (OPA) Host Software

Intel® Omni-Path Architecture (OPA) host software is fully supported in Red Hat Enterprise Linux 7.7. Intel OPA provides Host Fabric Interface (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 installing Intel Omni-Path Architecture documentation, see: https://www.intel.com/content/dam/support/us/en/documents/network-and-i-o/fabric-products/Intel_OP_Software_RHEL_7_7_RN_K65224.pdf

(BZ#1739072)

IBPB cannot be directly disabled

With this RHEL kernel source code update, it is not possible to directly disable the Indirect Branch Prediction Barrier (IBPB) control mechanism. Red Hat does not anticipate any performance issues from this setting.

(BZ#1807647)

4.8. REAL-TIME KERNEL

kernel-rt source tree now matches the latest RHEL 7 tree

The **kernel-rt** sources have been upgraded to be based on the latest Red Hat Enterprise Linux kernel source tree, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1642619)

The RHEL 7 kernel-rt timer wheel has been updated to a non-cascading timer wheel

The current timer wheel has been switched to a non-cascading wheel which improves the timer subsystem and reduces the overheads on many operations. With the backport of the non-cascading timer wheel, kernel-rt is very close to the upstream kernel in enabling the backport of future improvements.

(BZ#1593361)

4.9. NETWORKING

rpz-drop now prevents BIND for repetitive resolving of unreachable domain

The Berkeley Internet Name Domain (BIND) version distributed with RHEL 7.7 introduces the **rpz-drop** policy, which enables to mitigate DNS amplification attacks. Previously, if an attacker generated a lot of queries for an irresolvable domain, BIND was constantly trying to resolve such queries, which caused considerable load on CPU. With **rpz-drop**, BIND does not process the queries when the target domain is unreachable. This behavior significantly saves CPU capacity.

(BZ#1325789)

bind rebased to version 9.11

The **bind** packages have been upgraded to upstream version 9.11, which provides a number of bug fixes and enhancements over the previous version:

New features:

- A new method of provisioning secondary servers called **Catalog Zones** has been added.
- Domain Name System Cookies can now be sent by the **named** service and the **dig** utility.
- The **Response Rate Limiting** feature can now help with mitigation of DNS amplification attacks.

- Performance of response-policy zone (RPZ) has been improved.
- A new zone file format called **map** has been added. Zone data stored in this format can be mapped directly into memory, which enables zones to load significantly faster.
- A new tool called **delv** (domain entity lookup and validation) for sending DNS queries and validating the results has been added. The tool uses the same internal resolver and validator logic as the **named** daemon.
- A new **mdig** command is now available. This command is a version of the **dig** command that sends multiple pipelined queries and then waits for responses, instead of sending one query and waiting for the response before sending the next query.
- A new **prefetch** option, which improves the recursive resolver performance, has been added.
- A new **in-view** zone option, which allows zone data to be shared between views, has been added. When this option is used, multiple views can serve the same zones authoritatively without storing multiple copies in memory.
- A new **max-zone-ttl** option, which enforces maximum TTLs for zones, has been added. When a zone containing a higher TTL is loaded, the load fails. Dynamic DNS (DDNS) updates with higher TTLs are accepted but the TTL is truncated.
- New quotas have been added to limit queries that are sent by recursive resolvers to authoritative servers experiencing denial-of-service attacks.
- The **nslookup** utility now looks up both IPv6 and IPv4 addresses by default.
- The **named** service now checks whether other name server processes are running before starting up.
- When loading a signed zone, **named** now checks whether a Resource Record Signature's (RSIG) inception time is in the future, and if so, it regenerates the RRSIG immediately.
- Zone transfers now use smaller message sizes to improve message compression, which reduces network usage.

Feature changes:

- The version **3 XML** schema for the statistics channel, including new statistics and a flattened XML tree for faster parsing, is provided by the HTTP interface. The legacy version **2 XML** schema is still the default format.

(BZ#1640561, BZ#1578128)

ipset rebased to version 7.1

The **ipset** packages have been upgraded to upstream version 7.1, which provides a number of bug fixes and enhancements over the previous version:

- The **ipset** protocol version 7 introduces the **IPSET_CMD_GET_BYNAME** and **IPSET_CMD_GET_BYINDEX** operations. Additionally, the user space component can now detect the exact compatibility level that the kernel component supports.
- A significant number of bugs have been fixed, such as memory leaks and use-after-free bugs.

(BZ#1649080)

NetworkManager now supports VLAN filtering on bridge interfaces

With this enhancement, administrators can configure virtual LAN (VLAN) filtering on bridge interfaces in the corresponding **NetworkManager** connection profiles. This enables administrators to define VLANs directly on bridge ports.

(BZ#1652910)

NetworkManager now supports configuring policy routing rules

Previously, users must set up policy routing rules outside of **NetworkManager**, for example by using the dispatcher script provided by the **NetworkManager-dispatcher-routing-rules** package. With this update, users can now configure rules as part of a connection profile. As a result, **NetworkManager** adds the rules when the profile is activated and removes the rules when the profile is deactivated.

(BZ#1652653)

4.10. SECURITY

NSS now supports keys restricted to RSASSA-PSS

The Network Security Services (NSS) library now supports keys restricted to Rivest–Shamir–Adleman Signature Scheme with Appendix – Probabilistic Signature Scheme (RSASSA-PSS). The legacy signature scheme, Public Key Cryptography Standard #1 (PKCS#1) v1.5, permits the keys to be reused for encrypting data or keys. This makes those keys vulnerable to signature forging attacks published by Bleichenbacher. Restricting the keys to the RSASSA-PSS algorithm makes them resilient to attacks that utilize decryption.

With this update, NSS can be configured to support keys which are restricted to the RSASSA-PSS algorithm only. This enables the use of such keys included in X.509 certificates for both server and client authentication in TLS 1.2 and 1.3.

(BZ#1431241)

NSS now accepts signatures with the NULL object only when correctly included in PKCS#1 v1.5 DigestInfo

The first specification of PKCS#1 v1.5-compatible signatures used text that could be interpreted in two different ways. The encoding of parameters that are encrypted by the signer could include an encoding of a **NULL ASN.1** object or omit it. Later revisions of the standard made the requirement to include the NULL object encoding explicit.

Previous versions of Network Security Service (NSS) tried to verify signatures while allowing either encoding. With this version, NSS accepts signatures only when they correctly include the NULL object in the DigestInfo structure in the PKSC#1 v1.5 signature.

This change impacts interoperability with implementations that continue to create signatures that are not PKCS#1 v1.5-compliant.

(BZ#1552854)

OpenSC supports HID Crescendo 144K smart cards

With this enhancement, OpenSC supports HID Crescendo 144K smart cards. These tokens are not fully compatible with the Common Access Card (CAC) specification. The token also use some more advanced parts of the specification than CAC tokens issued by the government. The OpenSC driver has been enhanced to manage these tokens and special cases of the CAC specification to support HID Crescendo 144K smart cards.

(BZ#1612372)

AES-GCM ciphers are enabled in OpenSSH in FIPS mode

Previously, AES-GCM ciphers were allowed in FIPS mode only in TLS. In the current version, we clarified with NIST that these ciphers can be allowed and certified in **OpenSSH**, as well.

As a result, the AES-GCM ciphers are allowed in **OpenSSH** running in FIPS mode.

(BZ#1600869)

SCAP Security Guide supports Universal Base Image

SCAP Security Guide security policies have been enhanced to support Universal Base Image (UBI) containers and UBI images, including **ubi-minimal** images. This enables configuration compliance scanning of UBI containers and images using the **atomic scan** command. UBI containers and images can be scanned against any profile shipped in **SCAP Security Guide**. Only the rules that are relevant to secure configuration of UBI are evaluated, which prevents false positives and produces relevant results. The rules that are not applicable to UBI images and containers are skipped automatically.

(BZ#1695213)

scap-security-guide rebased to version 0.1.43

The **scap-security-guide** packages have been upgraded to upstream version 0.1.43, which provides a number of bug fixes and enhancements over the previous version, most notably:

- Minimum supported Ansible version changed to 2.5
- New RHEL7 profile: VPP - Protection Profile for Virtualization v. 1.0 for Red Hat Enterprise Linux Hypervisor (RHELH)

(BZ#1684545)

tangd_port_t allows changes of the default port for Tang

This update introduces the **tangd_port_t** SELinux type that allows the **tangd** service run as confined with SELinux enforcing mode. That change helps to simplify configuring a Tang server to listen on a user-defined port and it also preserves the security level provided by SELinux in enforcing mode.

(BZ#1650909)

A new SELinux type: boltd_t

A new SELinux type, **boltd_t**, confines **boltd**, a system daemon for managing Thunderbolt 3 devices. As a result, **boltd** now runs as a confined service in SELinux enforcing mode.

(BZ#1589086)

A new SELinux policy class: bpf

A new SELinux policy class, **bpf**, has been introduced. The **bpf** class enables users to control the Berkeley Packet Filter (BPF) flow through SElinux, and allows inspection and simple manipulation of Extended Berkeley Packet Filter (eBPF) programs and maps controlled by SELinux.

(BZ#1626115)

shadow-utils rebased to version 4.6

The **shadow-utils** packages have been upgraded to upstream version 4.6, which provides a number of bug fixes and enhancements over the previous version, most notably the **newuidmap** and **newgidmap** commands for manipulating the UID and GID namespace mapping.

(BZ#1498628)

4.11. SERVERS AND SERVICES

chrony rebased to version 3.4

The **chrony** packages have been upgraded to upstream version 3.4, which provides a number of bug fixes and enhancements over the previous version, notably:

- The support for hardware time stamping has received improvements.
- The range of supported polling intervals has been extended.
- Burst and filter options have been added to NTP sources.
- A pid file has been moved to prevent the **chronyd -q** command from breaking the system service.
- An compatibility with NTPv1 clients has been fixed.

(BZ#1636117)

GNU enscript now supports ISO-8859-15 encoding

With this update, support for ISO-8859-15 encoding has been added into the GNU enscript program.

(BZ#1573876)

ghostscript rebased to version 9.25

The **ghostscript** packages have been upgraded to upstream version 9.25, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1636115)

libssh2 package rebased to version 1.8.0

This update rebases the **libssh2** package to version 1.8.0.

This version includes the following:

- Added support for HMAC-SHA-256 and HMAC-SHA-512
- Added support for diffie-hellman-group-exchange-sha256 key exchange
- Fixed many small bugs in the code

(BZ#1592784)

ReaR updates

ReaR has been updated to a later version. Notable bug fixes and enhancements over the previous version include:

- Shared libraries provided by the system are now correctly added into the ReaR rescue system in cases where additional libraries of the same name are needed by the backup mechanism. Verification of NetBackup binaries is performed using the correct libraries, so the verification no longer fails when creating the rescue image. As a result, you can now use NetBackup as a backup mechanism with ReaR. Note that this applies only for NetBackup versions prior to NetBackup 8.0.0. Note that it is currently impossible to use NetBackup 8.0.0 and later versions due to other unresolved problems.

- Creation of a rescue image in cases with large number of multipath devices now proceeds faster. Scanning of devices has been improved in the following ways:

  - Scanning uses caching to avoid querying the multipath devices multiple times.

  - Scanning queries only device-mapper devices for device-mapper specific information.

  - Scanning avoids collecting information about FibreChannel devices.

- Several bugs in ReaR affecting complex network configurations have been fixed:

  - The Link Aggregation Control Protocol (LACP) configuration is now correctly restored in the rescue system in cases when teaming, or bonding with the **SIMPLIFY_BONDING** option, is used together with LACP.

  - ReaR now correctly restores the configuration of the interface in the rescue system in cases when a network interface is renamed from the standard name, such as **ethX**, to a custom name.

  - ReaR has been fixed to record a correct MAC address of the network interfaces in cases when bonding or teaming is used.

- ReaR has been fixed to correctly report errors when saving the rescue image. Previously, such errors resulted only in creation of unusable rescue images. As a result of the fix, ReaR now fails in such cases, so the problem can be properly investigated.

- The computation of disk layout for disks with a logical sector size different from 512 bytes has been fixed.

- ReaR now properly sets the bootlist during a restore on IBM Power Systems that use more than one bootable disk.

- ReaR now properly excludes its temporary directory from backup when an alternate temporary directory is specified using the **TMPDIR** environment variable.

- ReaR now depends on the **xorriso** packages instead of on the **genisoimage** package for ISO image generation. This makes it possible to create an image with a file larger than 4 GB, which occurs especially when creating an image with an embedded backup.

(BZ#1652828, BZ#1652853, BZ#1631183, BZ#1610638, BZ#1426341, BZ#1655956, BZ#1462189, BZ#1700807)

tuned rebased to version 2.11

The **tuned** packages have been upgraded to upstream version 2.11, which provides a number of bug fixes and enhancements over the previous version, notably:

- Support for boot loader specification (BLS) has been added. (BZ#1576435)

- The **mssql** profile has been updated. (BZ#1660178)

- The **virtual-host** profile has been updated. (BZ#1569375)
- A range feature for CPU exclusion has been added. (BZ#1533908)
- Profile configuration now automatically reloads when the **tuned** service detects the hang-up signal (SIGHUP). (BZ#1631744)

For full list of changes see the upstream git log: https://github.com/redhat-performance/tuned/commits/v2.11.0

(BZ#1643654)

New packages: xorriso

Xorriso is a program for creating and manipulating ISO 9660 images, and for writing CD-ROMs or DVD-ROMs. The program includes the **xorrisofs** command, which is a recommended replacement for the **genisoimage** utility. The **xorrisofs** command has a compatible interface with **genisoimage**, and provides multiple enhancements over **genisoimage**. For example, with **xorrisofs**, maximum file size is no longer limited to 4 GB. Xorriso is suitable for backups, and it is used by Relax-and-Recover (ReaR), a recovery and system migration utility.

(BZ#1638857)

4.12. STORAGE

Support for Data Integrity Field/Data Integrity Extension (DIF/DIX)

DIF/DIX is supported on configurations where the hardware vendor has qualified it and provides full support for the particular host bus adapter (HBA) and storage array configuration on RHEL.

DIF/DIX is not supported on the following configurations:

- It is not supported for use on the boot device.
- It is not supported on virtualized guests.
- Red Hat does not support using the Automatic Storage Management library (ASMLib) when DIF/DIX is enabled.

DIF/DIX is enabled or disabled at the storage device, which involves various layers up to (and including) the application. The method for activating the DIF on storage devices is device-dependent.

For further information on the DIF/DIX feature, see What is DIF/DIX.

(BZ#1649493)

New scan_lvs configuration setting

A new **lvm.conf** configuration file setting, **scan_lvs**, has been added and set to 0 by default. The new default behavior stops LVM from looking for PVs that may exist on top of LVs; that is, it will not scan active LVs for more PVs. The default setting also prevents LVM from creating PVs on top of LVs.

Layering PVs on top of LVs can occur by way of VM images placed on top of LVs, in which case it is not safe for the host to access the PVs. Avoiding this unsafe access is the primary reason for the new default behavior. Also, in environments with many active LVs, the amount of device scanning done by LVM can be significantly decreased.

The previous behavior can be restored by changing this setting to 1.

(BZ#1674563)

4.13. SYSTEM AND SUBSCRIPTION MANAGEMENT

The web console rebased to version 195

The web console, provided by the **cockpit** packages, has been upgraded to version 195, which provides a number of new features and bug fixes.

The **cockpit** packages distributed in the Base channel of RHEL 7 include the following features:

- You can now open individual ports for services in the firewall.
- The firewall page now enables adding and removing firewall zones and adding services to a specific zone.
- Cockpit can now help you with enabling certain security vulnerability mitigations, starting with the disabling SMT (Simultaneous Multi-Threading) option.

The **cockpit** packages distributed in the Extras channel of RHEL 7 have been updated to version 151.1, which provides the following additional features:

- You can now add an iSCSI direct target as a storage pool for your virtual machines.
- Notifications about virtual machines have been streamlined and use a common presentation now.
- You can select encryption type separately from the file system.

With this update, support for the Internet Explorer browser has been removed from the RHEL 7 web console. Attempting to open the web console in Internet Explorer now displays an error screen with a list of recommended browsers that can be used instead.

(BZ#1712833)

4.14. VIRTUALIZATION

virt-v2v can now convert SUSE Linux VMs

You can now use the **virt-v2v** utility to convert virtual machines (VMs) that use SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED) guest operating systems (OSs) from non-KVM hypervisors to KVM.

Note that the conversion is only supported for SLES or SLED guest OSs version 11 Service Pack 4 or later. In addition, SLES 11 and SLED 11 VMs that use X graphics need to be re-adjusted after the conversion for the graphics to work properly. To do so, use the **sax2** distribution tool in the guest OS after the migration is finished.

(BZ#1463620)

virt-v2v can now use vmx configuration files to convert VMware guests

The **virt-v2v** utility now includes the **vmx** input mode, which enables the user to convert a guest virtual machine from a VMware vmx configuration file. Note that to do this, you also need access to the corresponding VMware storage, for example by mounting the storage using NFS. It is also possible to

access the storage using SSH, by adding the **-it ssh** parameter.

(BZ#1441197)

virt-v2v converts VMWare guests faster and more reliably

The **virt-v2v** utility can now use the VMWare Virtual Disk Development Kit (VDDK) to convert a VMWare guest virtual machine to a KVM guest. This enables **virt-v2v** to connect directly to the VMWare ESXi hypervisor, which improves the speed and reliability of the conversion.

Note that this conversion import method requires the external **nbdkit** utility and its VDDK plug-in.

(BZ#1477912)

virt-v2v can convert UEFI guests for RHV

Using the **virt-v2v** utility, it is now possible to convert virtual machines that use the UEFI firmware to run in Red Hat Virtualization (RHV).

(BZ#1509931)

virt-v2v removes VMware Tools more reliably

This update makes it more likely that the **virt-v2v** utility automatically attempts to remove VMware Tools software from a VMware virtual machine that **virt-v2v** is converting to KVM. Notably, **virt-v2v** now attempts to remove VMWare Tools in the following scenarios:

- When converting Windows virtual machines.
- When VMMware Tools were installed on a Linux virtual machine from a tarball.
- When WMware Tools were installed as *open-vm-tools*.

(BZ#1481930)

4.15. ATOMIC HOST AND CONTAINERS

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.

4.16. 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 7 on AMD64 and Intel 64 architectures, the 64-bit ARM architecture, IBM Z, and IBM POWER, little endian. Certain components are available also for all supported releases of Red Hat Enterprise Linux 6 on AMD64 and Intel 64 architectures.

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. Red Hat Developer Toolset is included 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.

CHAPTER 5. DEVICE DRIVERS

This chapter provides a comprehensive listing of all device drivers that are new or have been updated in Red Hat Enterprise Linux 7.7.

5.1. NEW DRIVERS

Graphics Drivers and Miscellaneous Drivers

- Virtual GEM provider (vgem.ko.xz).
- Intel® Broxton SoC pinctrl/GPIO driver (pinctrl-broxton.ko.xz).
- Intel® Cedar Fork PCH pinctrl/GPIO driver (pinctrl-cedarfork.ko.xz).
- Intel® Ice Lake PCH pinctrl/GPIO driver (pinctrl-icelake.ko.xz).

Network Drivers

- Intel® Ethernet Adaptive Virtual Function Network Driver (iavf.ko.xz).
- Intel® Ethernet Connection E800 Series Linux Driver (ice.ko.xz), available as a Technology Preview.
- Intel® 2.5G Ethernet Linux Driver (igc.ko.xz), available as a Technology Preview.
- Realtek 802.11ac wireless core module (rtw88.ko.xz).
- Realtek 802.11ac wireless PCI driver (rtwpci.ko.xz).

5.2. UPDATED DRIVERS

Graphics Driver and Miscellaneous Driver Updates

- Standalone drm driver for the VMware SVGA device (vmwgfx.ko.xz) has been updated to version 2.15.0.0
- VMware Virtual Machine Communication Interface. (vmw_vmci.ko.xz) has been updated to version 1.1.6.0-k.
- Generic UIO driver for VMBus devices (uio_hv_generic.ko.xz) has been updated to version 0.02.1.
- HPE watchdog driver (hpwdt.ko.xz) has been updated to version 2.0.2.

Network Driver Updates

- Elastic Network Adapter (ENA) (ena.ko.xz) has been updated to version 2.0.3K.
- QLogic BCM57710/57711/57711E/57712/57712_MF/57800/57800_MF/57810/57810_MF/57840/57840_ Driver (bnx2x.ko.xz) has been updated to version 1.713.36-0.
- Broadcom BCM573xx network driver (bnxt_en.ko.xz) has been updated to version 1.10.0.
- Intel® Ethernet Switch Host Interface Driver (fm10k.ko.xz) has been updated to version 0.26.1-k.

- Intel® Ethernet Connection XL710 Network Driver (i40e.ko.xz) has been updated to version 2.8.10-k.
- Intel® Gigabit Ethernet Network Driver (igb.ko.xz) has been updated to version 5.6.0-k.
- Intel® 10 Gigabit PCI Express Network Driver (ixgbe.ko.xz) has been updated to version 5.1.0-k-rh7.7.
- Intel® 10 Gigabit Virtual Function Network Driver (ixgbevf.ko.xz) has been updated to version 4.1.0-k-rh7.7.
- The Netronome Flow Processor (NFP) driver. (nfp.ko.xz) has been updated to version 3.10.0-1060.el7.x86_64.
- QLogic FastLinQ 4xxxx Core Module (qed.ko.xz) has been updated to version 8.37.0.20.
- QLogic FastLinQ 4xxxx Ethernet Driver (qede.ko.xz) has been updated to version 8.37.0.20.
- VMware vmxnet3 virtual NIC driver (vmxnet3.ko.xz) has been updated to version 1.4.16.0-k.

Storage Driver Updates

- Cisco FCoE HBA Driver (fnic.ko.xz) has been updated to version 1.6.0.47.
- Driver for HP Smart Array Controller version 3.4.20-170-RH1 (hpsa.ko.xz) has been updated to version 3.4.20-170-RH1.
- Emulex LightPulse Fibre Channel SCSI driver 12.0.0.10 (lpfc.ko.xz) has been updated to version 0:12.0.0.10.
- Broadcom MegaRAID SAS Driver (megaraid_sas.ko.xz) has been updated to version 07.707.50.00-rh1.
- LSI MPT Fusion SAS 3.0 Device Driver (mpt3sas.ko.xz) has been updated to version 27.101.01.00.
- QLogic FastLinQ 4xxxx iSCSI Module (qedi.ko.xz) has been updated to version 8.33.0.21.
- QLogic Fibre Channel HBA Driver (qla2xxx.ko.xz) has been updated to version 10.00.00.12.07.7-k.
- Driver for Microsemi Smart Family Controller version 1.2.4-070 (smartpqi.ko.xz) has been updated to version 1.2.4-070.

CHAPTER 6. NOTABLE BUG FIXES

This chapter describes bugs fixed in Red Hat Enterprise Linux 7.7 that have a significant impact on users.

6.1. AUTHENTICATION AND INTEROPERABILITY

Directory Server flushes the entry cache after a back end transaction plug-in failed

Previously, if a back end transaction plug-in failed, Directory Server rolled-back the operation, but did not revert the changes in the entry cache. As a consequence, the entry cache contained incorrect entries. With this update, Directory Server flushes the entry cache after a back end transaction plug-in failed. As a result, clients retrieve the correct data when querying the database in the mentioned situation.

(BZ#1417340)

The ds-replcheck utility no longer incorrectly reports non-matching tombstone entries on replicas

Previously, if an administrator ran the **ds-replcheck** utility on different Directory Server replicas with tombstones present, **ds-replcheck** reported that one of the replicas was missing the tombstone entries. It is expected that tombstone entries do not match on each replica. With this update, **ds-replcheck** no longer searches for tombstone entries. As a result, the utility does not report missing tombstone entries as a problem.

(BZ#1629055)

Directory Server no longer crashes when shutting down the service while a cleanAllRUV task is running

Previously, stopping the Directory Server service while a **cleanAllRUV** task was running freed resources the task was using. As a consequence, the service terminated unexpectedly. With this update, Directory Server increments a reference counter that enables the task to complete before the service shutdown process proceeds. As a result, the server no longer crashes in the mentioned scenario.

(BZ#1466441)

Directory Server now correctly rejects the current password if passwordInHistory is set to 0

Previously, administrators could not set the **passwordInHistory** attribute in Directory Server to **0**. As a consequence, Users could reset their password to the same password as they currently use. With this update, users can now set **passwordInHistory** to **0** and, as a result, to check the current password.

(BZ#1563999)

Directory Server no longer truncates nsSSL3Ciphers values longer than 1023 characters

Previously, Directory Server used a fixed buffer size to store the preferred TLS ciphers set in the **nsSSL3Ciphers** parameter in the **cn=encryption,cn=config** entry. As a consequence, if the value was longer than 1024 characters, the server truncated the value and used only ciphers specified in the first 1023 characters. With this fix, Directory Server no longer uses a fixed buffer size to store the value. As a result, the setting works as expected.

(BZ#1716267)

Directory Server no longer uses the CoS attribute with a higher priority than the real attribute

Previously, Directory Server used the **operational-default** Class of Service (CoS) attribute with a higher priority than the real attribute. As a consequence, the server overwrote the attribute set in a local password with the CoS policy defined in a subtree. This update fixes the problem. As a result, CoS-defined password policies work as expected.

(BZ#1652984)

Directory Server now updates the pwdLastSet field of a user on password changes

Previously, if password synchronization was enabled and a user changed a password in Directory Server, the server did not set the **pwdLastSet** attribute. As a consequence, Active Directory (AD) still forced the user to update the password. Directory Server now updates **pwdLastSet** in the mentioned scenario. As a result. AD does not force the user to change the password again.

(BZ#1597202)

Searches with scope one no longer return incomplete results in Directory Server

Previously, when a user performed a search with a scope set to **one**, the search operation did not return all expected entries. With this update, Directory Server correctly creates the entry candidates list for one level searches. As a result, the server returns the expected entries.

(BZ#1665752)

Directory Server no longer ignores IPv6 addresses in an ACI if both IPv6 and IPv4 addresses are used

Administrators can specify both IPv4 and IPv6 addresses in Access Control Instructions (ACI) to allow or deny access. Previously, if an ACI contained both IPv4 and IPv6 addresses, Directory Server ignored the IPv6 address. As a consequence, the ACI did not work as expected. This update fixes the parsing of the **ip** keyword in ACIs. As a result, IP-based ACIs work as expected in the mentioned scenario.

(BZ#1710848)

Replicating modrdn operations to read-only Directory Server now succeeds

The conflict entry management in Directory Server requires to add tracking entries for **modrdn** operations. Previously, adding these entries failed on read-only consumers and, as a consequence, **modrdn** operations could not be replicated to such instances. This update fixes the problem. As a result, replicating **modrdn** operations to read-only consumers succeeds.

(BZ#1602001)

The time after which Directory Server deletes tasks has been changed

Previously, Directory Server deleted task entries 2 minutes after a task finished. As a consequence, applications that were monitoring the task could miss the task result. This update changes the time after which the server deletes tasks. By default, all completed tasks are now deleted after 1 hour, except import and export tasks, which are deleted 24 hours after completion.

(BZ#1663829)

Directory Server did not return the shadowWarning attribute if passwordWarning was set lower than 86400

Previously, Directory Server did not return the **shadowWarning** attribute in searches if the **passwordWarning** attribute in the **cn=config** entry was set to a value lower than **86400** seconds (1 day). This update fixes the problem. As a result, the server returns the value of the **shadowWarning** attribute in the mentioned scenario.

(BZ#1589144)

krb5 memory caches are now thread-safe

Previously, the memory caches of the Kerberos V5 login program (**krb5**) were not completely thread-safe. As a consequence, multi-threaded access terminated unexpectedly in some cases. With this update, the memory caches are cleaned up to be more thread-safe. As a result, no more crashes occur.

(BZ#1605756)

krb5 configurations prohibited by FIPS 140-2 can now work again

Previously, Red Hat Enterprise Linux 7.6 build of the Kerberos V5 (**krb5**) system increased compliance with FIPS 140-2. As a consequence, certain previously permitted configurations that were prohibited by FIPS 140-2 stopped working. With this update, the changes have been reverted, because **krb5** only requires to work in FIPS mode, not be FIPS-compliant. As a result, configurations prohibited by FIPS 140-2 can now work again.

Note that Red Hat Enterprise Linux 8 does not support these configurations at the moment.

(BZ#1645711)

Certificate System starts even if the value in the numSubordinates attribute exceeds the number of profile entries

The LDAP **numSubordinates** operational attribute defines the expected number of profile entries. Previously, Certificate System did not start until all profiles and lightweight Certificate Authorities (CA) were loaded. As a consequence, if the value in the attribute exceeds the number of profile entries the start process did not complete. With this update, a watchdog timer forces the start process to proceed after a short delay in the mentioned scenario and Certificate System logs the unexpected condition. As a result, the Certificate System starts completes even when **numSubordinates** in the profiles or lightweight CA subtrees exceeds the number of entries in the search result.

(BZ#1638379)

TLS_RSA_* ciphers are now disabled by default in Certificate System

Previously, by default, TLS_RSA_* ciphers were enabled in Certificate System. However, in environments with certain hardware security modules (HSM) in Federal Information Processing Standard (FIPS) mode, these ciphers are not supported. As a consequence, the SSL handshake failed and the connection was not established. This update disables TLS_RSA_* ciphers by default. As a result, connections work with those HSMs in FIPS mode.

(BZ#1578389)

The Certificate System REST API no longer stores clear text passwords in log files

Previously, the Certificate System REST API did not filter out plain password values. As a consequence, passwords were visible in clear text in log files. With this update, the server replaces password attribute values with "(sensitive)". As a result, clear text passwords are no longer visible in logs.

(BZ#1617894)

Client authentication can now be disabled in Certificate System

A previous version of Certificate System added a feature to enforce TLS client authentication when authenticating through CMCAuth. However, certain older applications do not support TLS client authentication and failed to connect to Certificate System. This update adds the **bypassClientAuth**

configuration parameter to the **/var/lib/pki/pki-instance_name/ca/conf/CS.cfg** file. As a result, administrators can now set this parameter to **true** to disable client authentication if not supported by certain applications.

(BZ#1628410)

Certificate System CA installations succeed when using a PKCS #12 file

Previously, the default value of the **pki_ca_signing_cert_path** parameter was set to a predefined path. Due to a recent change in the way the **pkispawn** utility validates the parameter when an administrator used a PKCS #12 file to install a certificate authority (CA), the installation failed with an **Invalid certificate path: pki_ca_signing_cert_path=/etc/pki/pki-tomcat/external_ca.cert** error. This update fixes the problem by removing the default value of **pki_ca_signing_cert_path**. As a result, the CA installation succeeds in the mentioned scenario.

(BZ#1633761)

The pki utility correctly asks for a password

Previously, if the user did not provide a password using command-line options, the **pki** utility did not prompt for a password. As a consequence, **pki** incorrectly reported **Error: Missing user password** and the operation failed. The **pki** utility has been fixed to prompt for a password under the described circumstances.

(BZ#1479559)

Certificate System automatically shuts down if signed audit logs cannot be stored due to a full file system

Previously, if audit signing was enabled and the file system on which Certificate System stored the signed audit logs was full, Certificate System continued operating but did not log further operations. To prevent missing signed audit logs, Certificate System now shuts down automatically in the mentioned scenario.

(BZ#1639710)

SSSD uses the AD LDAP server to retrieve POSIX attributes for initgroup lookups

The SSSD service uses the Active Directory (AD) global catalog (GC) for initgroup lookups, but the POSIX attributes, such as the user home directory or shell, are not replicated to the GC set by default. Consequently, when SSSD requests the POSIX attributes during SSSD lookups, SSSD incorrectly considers the attributes to be removed from the server, because they are not present in the GC, and removes them from the SSSD cache as well. With this update, initgroup lookups now switch between LDAP and GC connection as appropriate, because the AD LDAP server contains the POSIX attributes even without schema modification. As a result, POSIX attributes, such as shell or home directory, are no longer overwritten or missing.

(BZ#1194345)

Changing the shell with ypchsh no longer results in an overwritten password when NIS uses passwd.adjunct

Previously, when the NIS server was set up to support the **passwd.adjunct** map and the user changed the shell on a NIS client by using the **ypchsh** command, the **yppasswdd** daemon overwrote the user's password hash inside **passwd.adjunct** with the **##username** string. Consequently, the affected user was unable to log in due to a corrupted password hash. This bug has been fixed, and **yppasswdd** no longer overwrites the user's password hash while updating the user's shell information. As a result, the user can successfully log in the new shell after running **ypchsh**.

(BZ#1624295)

6.2. COMPILER AND TOOLS

The SystemTap Dyninst backend works without the dyninst-devel package

The **stap --dyninst** command uses the SystemTap Dyninst backend. Previously, this backend did not work when the **dyninst-devel** package was not installed. As a consequence, SystemTap terminated unexpectedly, and users had to manually install **dyninst-devel** and run the **ldconfig** tool as a workaround. This bug has been fixed and the SystemTap Dyninst backend now works without the **dyninst-devel** package.

(BZ#1498558)

GDB breakpoint default source file works for symbolic links

Previously, the GDB debugger could not locate the symbol table information for the default source file, if the file was a symbolic link. As a consequence, users could not set breakpoints by omitting the source file name and using the default, such as **break 63**. This bug has been fixed and users can now use default source files with breakpoints for files behind symbolic links.

(BZ#1639077)

The DNS stub resolver in glibc no longer rejects valid host names, such as hostname-.example.com

The DNS stub resolver in **glibc** rejected certain valid host names, such as hostname-.example.com, and accepted some invalid names. As a consequence, some host names on the Internet could not be resolved. To fix the problem, the DNS name validation functions, such as **res hnok**, have been adjusted to match user expectations and specifications more closely. As a result, host names of the form hostname-.example.com can now be resolved successfully if they exist in DNS.

(BZ#1039304)

iconv no longer hangs when converting from certain IBM character sets

Previously, the **glibc** converters for the IBM930, IBM933, IBM935, IBM937, and IBM393 character sets returned an error and failed to advance to the next input character when they encountered invalid redundant shift sequences. As a consequence, converting from these character sets using the **iconv** tool with the **-c** option to discard these characters made the tool unresponsive, because it could not progress beyond the first occurence of a redundant shift sequence. The converters have been modified to accept these sequences and continue correctly. As a result, the conversions mentioned above are now possible.

(BZ#1427734)

iconv can convert between the IBM273 and ISO-8859-1 character sets

Previously, the **glibc** implementation of the IBM273 character set was not equivalent to the ISO-8859-1 character set. It did not have a representation for the Unicode character **MACRON**, instead it used the corresponding byte to represent the **OVERLINE** Unicode character, which has the same visual representation as a **MACRON**. As a consequence, using the **iconv** tool provided by **glibc** to convert IBM273 text containing an **OVERLINE** character to ISO-8859-1 or ISO-8859-1 text containing a **MACRON** character to IBM273 resulted in an error during conversion. To fix this bug, the IBM273 character set was made equivalent to the ISO-8859-1 character set by replacing its **OVERLINE** representation with **MACRON**. As a result, both character sets now use the **MACRON** Unicode character, are equivalent, and conversion from one to the other does not lead to an error.

(BZ#1591268)

getifaddrs calls can no longer unexpectedly terminate applications

Previously, the network interface list produced by the **getifaddrs** function in the **glibc** library could lack interface names if the interfaces changed in the kernel at the same time. As a consequence, applications using **getifaddrs** could terminate unexpectedly in such situation. This has been fixed and **getifaddrs** now ensures the list is identical to kernel state. As a result, the unexpected termination mentioned above cannot happen.

(BZ#1472832)

Makefiles containing explicit targets before implicit work again

Previously, mixing implicit (pattern) and explicit targets in Makefiles was deprecated. After update to version 3.82, the **make** build tool returned errors for mixed targets. As a consequence, legacy Makefiles containing mixed targets could not be used. With this update, **make** can correctly parse situations where an explicit target is listed before an implicit target. As a result, certain legacy Makefiles can now be used again without modification. However, implicit targets before explicit targets still result in an error.

Note that mixing explicit and implicit targets in Makefiles is deprecated and should **not** be added to new Makefiles.

(BZ#1582545)

PCP now reports all process details on large systems

Previously, the Performance Co-Pilot (PCP) toolkit failed to report certain process details in some cases on very large systems. The code reading the process details files was changed so that it can read data of arbitrary length, instead of only the first 1024 bytes. As a result, the described PCP error can no longer happen.

(BZ#1600262)

strip no longer crashes with certain executable files

Previously, the **strip** tool contained untrue assumptions about executable file structure. As a consequence, attempting to strip certain executable files could unexpectedly terminate **strip**. The assumptions about structure have been changed such that this problem can no longer happen and **strip** works correctly.

(BZ#1644632)

Optimized CPU consumption by libdb

A previous update to the **libdb** database caused an excessive CPU consumption in the trickle thread. With this update, the CPU usage has been optimized.

(BZ#1608749)

passwd --stdin no longer limits the password length to 79 characters

When changing a password using the **passwd** command with the **--stdin** option, the length of the password was limited to 79 characters. Consequently, when you entered a password longer than 79 characters via standard input, only the first 79 characters were accepted, and no warning was shown. With this update, **passwd** has been fixed to align the accepted size of the password with size defined by Pluggable Authentication Module (PAM). As a result, the **passwd --stdin** command now accepts passwords longer than 79 characters, but not longer than **PAM_MAX_RESP_SIZE - 1** characters. If that limit is exceeded, **passwd** reports an error to the standard error output, and exits with exit code 1.

(BZ#1276570)

fixfiles no longer incorrectly fails

Previously, the **fixfiles** script failed if the **/etc/selinux/fixfiles_exclude_dirs** file contained at least one entry and the **/etc/selinux/targeted/contexts/files/file_contexts.local** file was not present. With this update, the requirement for existence of **/etc/selinux/targeted/contexts/files/file_contexts.local** has been removed, and fixfiles now works correctly in the described scenario.

(BZ#1647714)

6.3. DESKTOP

System no longer boots to a blank screen when Xinerama is enabled

When the Xinerama extension was enabled in **/etc/X11/xorg.conf** on a system using the nvidia or nouveau driver, the RANDR X extension got disabled. Consequently, login screen failed to start upon boot due to the RANDR X extension being disabled. This bug has been fixed and the login screen now starts properly even with Xinerama enabled.

(BZ#1579257)

Soft lock-ups fixed during boot in the kernel with i915

On a rare occasion when a GM45 system had an improper firmware configuration, an incorrect **DisplayPort** hot-plug signal could cause the **i915** driver to be overloaded on boot. Consequently, certain GM45 systems experienced very slow boot times while the video driver attempted to work around the problem. In some cases, the kernel also reported soft lock-ups. This bug has been fixed and the lock-ups no longer occur in the described scenario.

(BZ#1608704)

X.org server no longer crashes during fast user switching

Previously, the X.Org X11 **qxl** video driver did not emulate the leaving virtual terminal event on shutdown. Consequently, the X.Org display server terminated unexpectedly during fast user switching, and the current user session was terminated when switching a user. With this update, **qxl** has been fixed, and the X.org server no longer crashes during fast user switching.

(BZ#1640918)

6.4. FILE SYSTEMS

Non-root users can now access SMB shares mounted using the multiuser option

In Red Hat Enterprise Linux (RHEL) 7.5, a fix was added to handle NT LAN Manager (NTLM) authentication when no domain was specified. This change affected how the **cifs.ko** kernel module selected the domain name when using NTLM. As a consequence, when a server message block (SMB) share was mounted with the **multiuser** option, an incorrect domain name was selected and non-root users failed to access the mounted SMB share. This update reverts the fix. As a result, shares mounted with **multiuser** can now be accessed by non-root users in RHEL 7.7.

(BZ#1710421)

Setting disk quota limits over a network works again for users occupying more than 4 GB of space on the network file system

Previously, the **setquota** utility was unable to handle an occupied space greater than 4 GB when communicating with an NFS server due to an incorrect format of the used disk size. Consequently, when setting disk quota limits for a user exceeding 4 GB of used space on a NFS-mounted file system, **setquota** failed to perform the operation. This update corrects the conversion of the used disk size to an RPC protocol format, and the described problem no longer occurs.

(BZ#1697605)

6.5. INSTALLATION AND BOOTING

NVDIMM commands are added to the Kickstart script file anaconda-ks.cfg after installation

The installer creates a Kickstart script equivalent to the configuration used for system installation. This script is stored in the **/root/anaconda-ks.cfg** file. Previously, when the graphical user interface was used to install RHEL, the **nvdimm** commands used for configuring Non-Volatile Dual In-line Memory (NVDIMM) devices were not added to this file. This bug has been fixed and the Kickstart file now contains the **nvdimm** commands as expected.

(BZ#1620109)

The graphical installation program no longer permits an invalid passphrase

Previously, when installing RHEL 7 using the graphical installation program, it was possible to leave the passphrase field in the **Partitioning Disk Encryption Passphrase** dialog box empty, click the **Save Passphrase** button, and finish your partitioning tasks. As a consequence, partitioning was misconfigured and you had to cancel the disk encryption process or enter a valid passphrase. With this update, the **Save Passphrase** button is available only when you enter a valid and non-empty passphrase.

(BZ#1489713)

Using the version or inst.version kernel boot parameters no longer stops the installation program

Previously, booting the installation program from the kernel command line using the **version** or **inst.version** boot parameters printed the version, for example **anaconda 30.25.6**, and stopped the installation program.

With this update, the **version** and **inst.version** parameters are ignored when the installation program is booted from the kernel command line, and as a result, the installation program is not stopped.

(BZ#1637112)

The RHEL 7.7 graphical installation now displays supported NVDIMM device sector sizes

Previously, when configuring NVDIMM devices using the graphical user interface (GUI), it was possible to enter an unsupported sector size. No warning message was displayed, and as a consequence, a reconfiguration error occurred. With this update, the sector size dialog box contains a drop-down list that displays only the supported sector sizes of **512** and **4096**.

(BZ#1614049)

Cancelling a job initiated from cockpit-composer no longer fails

Image build process did not support cancelling an image build. As a consequence, cancelling a job initiated from **cockpit-composer** GUI using **composer-cli compose cancel** resulted in a hung compose API server, causing newly queued job builds to not start, and remain in waiting state. To fix the problem, a feature to cancel the Image build process was implemented. As a result, cancelling a job initiated from **cockpit-composer** no longer fails.

(BZ#1659129)

The rpm command now supports the --setcaps and --restore options

This update introduces the **--setcaps** and **--restore** options for the **rpm** command.

The **--setcaps** option sets capabilities of files in a required package. The syntax is as follows:

```
rpm --setcaps _PACKAGE_NAME_
```

The **--restore** option restores owner, group, permissions, and capabilities of files in a required package. The syntax is as follows:

```
rpm --restore _PACKAGE_NAME_
```

(BZ#1550745)

GRUB 2 regexp command is no longer missing

Previously, the module providing the **regexp** command for the Grand Unified Bootloader version 2 (GRUB2) was missing in the GRUB2 EFI binary. As a consequence, on UEFI systems with Secure Boot enabled, using **regexp** failed with the **error: can't find command `regexp`** message. With this update, the module providing **regexp** is included in the GRUB2 EFI binary and works correctly in the described situation.

(BZ#1630678)

6.6. KERNEL

Netfilter now supports zero-length CIDR values in certain IP set types

Previously, the kernel rejected a zero-length Classless Inter-domain Routing (CIDR) network mask value in the first and the last parameter in **hash:net,port,net** and **hash:net6,port,net6** IP set types. As a consequence, Netfilter could not match a port against all network destinations. With this update, zero-length CIDR values are allowed in the first and the last parameter of the mentioned IP set types. As a result, administrators can create firewall rules that match a port that is valid for all destinations.

(BZ#1680426)

AVC denials for NFS mounted directories mounted on the server side

NFS **crossmnt** mounts automatically create internal mounts when a process accesses a subdirectory that is used as a mount point on the server. Consequently, SELinux checks whether the process accessing an NFS mounted directory has a mount permission, which may cause Access Vector Cache (AVC) denials. In this update, SELinux permission checking is skipped for internal mounts of this type. As a result, mount permission is not needed when accessing an NFS directory that is mounted on the server side.

(BZ#1077929)

The intel_pstate driver loads on the Intel Skylake-X systems with HWP disabled

Previously, with the Intel Skylake-X systems, it was impossible to load the **intel_pstate** driver if Hardware P-States (HWP) were disabled. As a consequence, the kernel defaulted to loading the **acpi_cpufreq** driver. This update fixes the problem and **intel_pstate** now loads correctly in the described scenario.

In the event that the user wants to use **acpi_cpufreq** (not recommended), the solution is to append the **intel_pstate=disable** parameter to the kernel command line.

(BZ#1698453)

Data corruption no longer occurs on RAID 10 reshape on top of VDO

Previously, RAID 10 reshape (with both LVM and "mdadm") on top of VDO corrupted data. With this fix, the data corruption no longer occurs. However, Stacking RAID 10 (or other RAID types) on top of VDO does not take advantage of the deduplication and compression capabilities of VDO and is not recommended.

(BZ#1528466)

write-behind in RAID1 no longer triggers a kernel panic

Previously, the write-behind mode in the Redundant Array of Independent Disks Mode 1 (RAID1) virtualization technology used the upper layer bio structures. The structures were freed immediately after the bio structures written to bottom layer disks came back. As a consequence, a kernel panic was triggered and the **write-behind** function could not be used. This update fixes the problem and **write-behind** can now be used without triggering a kernel panic in the described scenario.

(BZ#1632575)

The kernel now supports destination MAC addresses in **bitmap:ipmac, hash:ipmac, and hash:mac** IP set types

Previously, the kernel implementation of the **bitmap:ipmac**, **hash:ipmac**, and **hash:mac** IP set types only allowed matching on the source MAC address, while destination MAC addresses could be specified, but were not matched against set entries. As a consequence, administrators could create **iptables** rules that used a destination MAC address in one of these IP set types, but packets matching the given specification were not actually classified. With this update, the kernel compares the destination MAC address and returns a match if the specified classification corresponds to the destination MAC address of a packet. As a result, rules that match packets against the destination MAC address now work correctly.

(BZ#1607252)

The **kdump** kernel is now able to boot after a CPU hot add or hot remove operation

When running Red Hat Enterprise Linux 7 on the little-endian variant of IBM Power Systems with **kdump** enabled, the **kdump** crash kernel failed to boot if triggered by the **kexec** system call after a CPU hot add or hot remove operation. This update fixes the bug by utilizing the CPU online and offline events. As a result, **kdump** kernel manages to boot in the described scenario.

(BZ#1549355)

6.7. NETWORKING

dnsmasq no longer uses ports lower than 1024 as a source port

Previously, the Domain Name System forwarder (**dnsmasq**) used for queries all ports below 1024. However, Berkeley Internet Name Domain (BIND) drops DNS queries incoming from some of the low ports. Consequently, the target port 464 was ignored by BIND. With this update, **dnsmasq** has been fixed to not use custom random port generator, but it now lets the operating system to assign random ports instead. As a result, **dnsmasq** no longer uses ports lower than 1024 as a source port, which prevents the described problem with BIND.

(BZ#1614331)

Dnsmasq with enabled cache no longer returns cached responses without DNSSEC records

Previously, **dnsmasq** service with enabled cache returned cached responses without **DNSSEC** records, even if query had **DNSSEC OK** bit set. As a consequence, returned replies could not pass **DNSSEC** validation by client under the **dnsmasq**. That causes clients under **dnsmasq** not able to use DNSSEC validation. To fix this, always forward requests with **DNSSEC OK** bit set and do not use cached values, unless **DNSSEC** validation is enabled locally. As a result, clients under **dnsmasq** can successfully validate all responses.

(BZ#1638703)

The ipset service can now load sets which depends on other sets

The **ipset** service saves IP sets (lists of IP addresses) in separate files. In Red Hat Enterprise Linux (RHEL) 7.6, when starting the service, each set was loaded sequentially ignoring dependencies between them. As a consequence, the service failed to load IP sets with dependencies on other sets. With this update, the **ipset** service creates first all the sets included in the saved configuration, and then adds their entries. As a result, IP sets with dependencies on other sets can now be loaded.

(BZ#1646666)

Error logging in the ipset service has been improved

Previously, the **ipset** service did not report configuration errors with a meaningful severity in the **systemd** logs. The severity level for invalid configuration entries was only **informational**, and the service did not report errors for an unusable configuration. As a consequence, it was difficult for administrators to identify and troubleshoot issues in the **ipset** service's configuration. With this update, **ipset** reports configuration issues as **warnings** in **systemd** logs and, if the service fails to start, it logs an entry with the **error** severity including further details. As a result, it is now easier to troubleshoot issues in the configuration of the **ipset** service.

(BZ#1649877)

The ipset service now ignores invalid configuration entries during startup

The **ipset** service stores configurations as sets in separate files. Previously, when the service started, it restored the configuration from all sets in a single operation, without filtering invalid entries that can be inserted by manually editing a set. As a consequence, if a single configuration entry was invalid, the service did not restore further unrelated sets. The problem has been fixed. As a result, the **ipset** service detects and removes invalid configuration entries during the restore operation, and ignores invalid configuration entries.

(BZ#1650297)

firewalld rebased to version 0.6.3

The **firewalld** packages have been upgraded to upstream version 0.6.3, which provides a number of bug fixes over the previous version:

- The **firewalld** service now only modifies **ifcfg** files for permanent configuration changes.
- Untranslated strings in the **firewall-config** utility have been fixed, which caused that rich rules could not be modified in the UI.
- The **set-log-denied** parameter now works correctly when used in combination with the **icmp-block-inversion** parameter.

- The **firewall-cmd** utility now correctly checks the return value of the **ipset** command.
- IP forwarding is no longer enabled when using port forwarding and the **toaddr** parameter is not specified.
- The shell auto-complete feature no longer constantly asks for authentication.

(BZ#1637204)

6.8. SECURITY

An SELinux policy reload no longer causes false ENOMEM

Reloading SELinux policy previously caused the internal security context lookup table to become unresponsive. Consequently, when the kernel encountered a new security context during a policy reload, the operation failed with a false "Out of memory" (ENOMEM) error. With this update, the internal Security Identifier (SID) lookup table has been redesigned and no longer freezes. As a result, the kernel no longer returns misleading ENOMEM errors during an SELinux policy reload.

(BZ#1335986)

NSS now processes X.509 certificates for use with IPsec correctly

Previously, the NSS library did not properly process X.509 certificates for use with IPsec. As a consequence, if X.509 certificates had non-empty Extended Key Usage (EKU) attributes that did not contain **serverAuth** and **clientAuth** attributes, the **Libreswan** IPsec implementation incorrectly rejected validation of the certificates. With this update, the IPsec profiles in NSS have been fixed, and Libreswan can now accept the described certificates.

(BZ#1212132)

NSS no longer accepts RSA PKCS#1 v1.5 signatures made with an RSA-PSS key

RSA-PSS keys can be used for creating RSA-PSS signatures only and signatures made with those keys that use the PKCS#1 v1.5 algorithm violate the standard. Previously, the Network Security Services (NSS) libraries did not check the type of an RSA public key used by a server when validating signatures made using a corresponding private key. Consequently, NSS accepted RSA PKCS#1 v1.5 signatures as valid, even if they were made with an RSA-PSS key.

The bug has been fixed and the NSS libraries now properly check the type of RSA public keys used by a server when validating signatures made using a corresponding private key. As a result, the signatures in this scenario are no longer accepted by NSS.

(BZ#1510156)

Accessing authorized keys no longer fails when switching users

Previously, group information cache in OpenSSH was not cleaned when changing the user for retrieving authorized keys using the **AuthorizedKeysCommand*** configuration options. Consequently, an attempt to access authorized keys failed for the new user due to incorrect group information. This bug has been fixed, and authorized keys can now be successfully accessed when the user is changed.

(BZ#1583735)

scap-security-guide now correctly skips rules that are not applicable to containers and container images

SCAP Security Guide content can be used to scan containers and container images now. Rules that are

not applicable to containers and container images have been marked with a specific CPE identifier. As a result, the evaluation of these rules is skipped automatically, and the result **not applicable** is reported when scanning containers and container images.

(BZ#1630739)

Ansible playbooks from the SCAP Security Guide no longer fail due to common errors

Ansible tasks included in the SCAP Security Guide content were previously unable to handle certain common cases, such as missing configuration files, non-existent files, or uninstalled packages. As a consequence, when using an Ansible playbook from the SCAP Security Guide or generated by the **oscap** command, the **ansible-playbook** command terminated with every error. With this update, the Ansible tasks have been updated to handle common cases, and Ansible playbooks from the SCAP Security Guide can be successfully executed even if common errors are encountered during the playbook execution.

(BZ#1647189)

SCAP Security Guide now correctly checks the dconf configuration

Prior to this update, OVAL (Open Vulnerability and Assessment Language) checks used in the **SCAP Security Guide** project did not check the **dconf** binary database directly, but it checked only the respective key files. This could lead to false positives or negatives in scanning results. With this update, **SCAP Security Guide** adds one more check component, which ensures that the **dconf** binary database is up-to-date with regards to those key files. As a result, the complex check now checks the **dconf** configuration correctly.

(BZ#1631378)

SELinux now allow gssd_t processes to access kernel keyrings of other processes

Previously, an allow rule for the **gssd_t** type was missing in the SELinux policy. As a consequence, SELinux in enforcing mode occasionally prevented processes running as **gssd_t** from accessing kernel keyrings of other processes and could block for example **sec=krb5** mounts. The rule has been added to the policy, and processes running as **gssd_t** are now able to access keyrings of other processes.

(BZ#1487350)

SELinux no longer blocks snapperd from managing all non-security directories

Prior to this update, an allow rule for the snapper daemon (**snapperd**) was missing in the SELinux policy. Consequently, snapper was not able to create a configuration file on a btrfs volume for a new snapshot with SELinux in enforcing mode. With this update, the missing rule has been added, and SELinux now allows **snapperd** to manage all non-security directories.

(BZ#1619306)

sudo I/O logging function now works also for SELinux-confined users

Prior to this update of the SELinux policy, rules that allow user domains to use generic pseudoterminal interfaces were missing. As a consequence, the I/O logging function of the **sudo** utility did not work for SELinux-confined users. The missing rules have been added to the policy, and the I/O logging function no longer fails in the described scenario.

(BZ#1564470)

sudo configured using LDAP now handles sudoRunAsGroup correctly

Previously, the **sudo** tool configured using LDAP did not correctly handle the case when the

sudoRunAsGroup attribute was defined and the **sudoRunAsUser** attribute was not. As a consequence, the **root** user was used as the target user. With this update, the handling of **sudoRunAsGroup** has been fixed to match the behavior documented in the **sudoers.ldap(5)** man page, and **sudo** now works properly in the described scenario.

(BZ#1618702)

6.9. SERVERS AND SERVICES

chronyd no longer fails to synchronize with NTP servers after reboot

Previously, when an interface was controlled by network scripts and NetworkManager was enabled at the same time, the **chrony** NetworkManager dispatcher script switched NTP sources to the offline state on boot. As a consequence, **chronyd** was prevented from synchronizing the system clock. With this update, the **chrony** dispatcher script ignores events that are not related to interfaces coming up or down. As a result, **chronyd** now synchronizes with NTP servers as expected under the described circumstances.

(BZ#1600882)

CUPS no longer denies access if SSSD running on the same server is configured with ignore_group_members = true

When System Security Services Daemon (SSSD) uses the **ignore_group_members = true** setting in the **/etc/sssd/sssd.conf** file, the **getgrnam()** function returns the group structure without group members of groups retrieved by SSSD. This is expected behavior. Previously, CUPS used only **getgrnam()** to verify if a user is a member of a group. As a consequence, if SSSD was configured with the mentioned setting on a CUPS server that used groups to allow access to the server for members of a group, CUPS denied access to users in these groups. With this update, CUPS now additionally uses the **getgrouplist()** function, which returns group members even if SSSD is configured with **ignore_group_members = true**. As a result, CUPS correctly determines access based on group memberships in the mentioned scenario.

(BZ#1570480)

Running dbus-daemon no longer fails to activate a system service

With the rebase of the D-Bus message bus daemon (**dbus-daemon**) to version 1.10.24, locations of several **dbus** tools were migrated. The **dbus-send** executable was moved from the **/bin** directory to the **/usr/bin** directory; the **dbus-daemon-launch-helper** executable was moved from the **libdir** directory to the **libexecdir** directory. Consequently, if a scriptlet in a package called the **dbus-send** command to send a message to D-Bus, and triggered a service activation, the activation could fail. With this update, the bug has been fixed by creating compatibility symlinks between the old and new locations of **dbus-daemon-launch-helper**. As a result, any running instance of **dbus-daemon** can now call the system bus and activate a system service.

(BZ#1568856)

Teaming in the rescue system works correctly again

Updates provided by the advisory RHBA-2019:0498 fixed several problems in ReaR, affecting complex network configurations. However, in case of teaming, this update introduced another problem. If the team had multiple member interfaces, the team device was not configured correctly in the rescue system. As a consequence, after applying an update provided by RHBA-2019:0498, a work around was needed to preserve the previous behavior. This update fixes the bug in ReaR, and teaming in the rescue system now works correctly.

(BZ#1685166)

Virtual machines now work correctly on RHEL 7 nodes in RHOSP 10

Previously, upgrading a Red Hat Enterprise Linux 7 (RHEL 7) node in Red Hat OpenStack Plaform 10 (RHOSP 10) to a later minor version sometimes caused virtual machines (VMs) hosted on that node to become unable to start. This update fixes how the **tuned** service configures parameters of the *kvm-intel* module, which prevents the described problem from occurring.

(BZ#1649408)

Handling of ksm and ksmtuned in Tuned has been fixed

Previously, **Tuned** sometimes failed to apply the **cpu-partitioning** profile if the **ksm** and **ksmtuned** services were enabled. With this update, handling of the **ksm** and **ksmtuned** services has been fixed. As a result, **Tuned** now applies the **cpu-partitioning** profile reliably.

(BZ#1622239)

Error messages in /var/log/tuned/tuned.log referring to non-existent sysctl settings no longer occur when a Tuned profile is loaded

Previously, the **Tuned** daemon treated non-existent sysctl settings as an error. For example **net.bridge.bridge-nf-call-ip6tables**, **net.bridge.bridge-nf-call-iptables**, or **net.bridge.bridge-nf-call-arptables**, which are unavailable on some systems, could trigger error in the **/var/log/tuned/tuned.log** file:

```
Failed to set sysctl parameter 'net.bridge.bridge-nf-call-ip6tables' to '0', the parameter does not exist
```

With this update, **Tuned** has been fixed, and the error messages no longer occur within **/var/log/tuned/tuned.log** under the described circumstances.

(BZ#1714595)

6.10. STORAGE

LVM no longer causes data corruption in the first 128kB of allocatable space of a physical volume

Previously, a bug in the I/O layer of LVM might have caused data corruption in rare cases. The bug could manifest only when the following conditions were true at the same time:

- A physical volume (PV) was created with a non-default alignment. The default is 1MB.
- An LVM command was modifying metadata at the tail end of the metadata region of the PV.
- A user or a file system was modifying the same bytes (racing).

No cases of the data corruption have been reported.

With this update, the problem has been fixed, and LVM can no longer cause data corruption under these conditions.

(BZ#1643651)

System boot is no longer delayed by ndctl

Previously, a **udev** rule installed by the **ndctl** package sometimes delayed the system boot process for several minutes on systems with Non-Volatile Dual In-line Memory Module (NVDIMM) devices. In such cases, **systemd** displayed a message similar to the following:

```
INFO: task systemd-udevd:1554 blocked for more than 120 seconds.
...
nvdimm_bus_check_dimm_count+0x31/0xa0 [libnvdimm]
...
```

With this update, **ndctl** no longer installs the **udev** rule. As a result, **ndctl** does not delay the system boot.

(BZ#1635441)

CHAPTER 7. TECHNOLOGY PREVIEWS

This chapter provides a list of all Technology Previews available in Red Hat Enterprise Linux 7.7.

For information on Red Hat scope of support for Technology Preview features, see Technology Preview Features Support Scope.

7.1. 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)

7.2. AUTHENTICATION AND INTEROPERABILITY

Containerized Identity Management server available as Technology Preview

The **rhel7/ipa-server** container image is available as a Technology Preview feature. Note that the **rhel7/sssd** container image is now fully supported.

For details, see Using Containerized Identity Management Services .

(BZ#1405325)

Setting up IdM as a hidden replica is now available as a Technology Preview

This enhancement enables administrators to set up an Identity Management (IdM) replica as a hidden replica. A hidden replica is an IdM server that has all services running and available. However, it is not advertised to other clients or masters because no **SRV** records exist for the services in DNS, and LDAP server roles are not enabled. Therefore, clients cannot use service discovery to detect hidden replicas.

Hidden replicas are primarily designed for dedicated services that can otherwise disrupt clients. For example, a full backup of IdM requires to shut down all IdM services on the master or replica. Since no clients use a hidden replica, administrators can temporarily shut down the services on this host without affecting any clients. Other use cases include high-load operations on the IdM API or the LDAP server, such as a mass import or extensive queries.

To install a new hidden replica, use the **ipa-replica-install --hidden-replica** command. To change the state of an existing replica, use the **ipa server-state** command.

(BZ#1518939)

DNSSEC available as Technology Preview in IdM

Identity Management (IdM) 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 IdM 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
- Secure Domain Name System (DNS) Deployment Guide
- DNSSEC Key Rollover Timing Considerations

Note that IdM 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 .

(BZ#1115294)

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 was 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 the related Knowlegdebase article.

(BZ#1298286)

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 available 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)

The Custodia secrets service provider is available as a Technology Preview

As a Technology Preview, you can use Custodia, a secrets service provider. Custodia stores or serves as a proxy for secrets, such as keys or passwords.

For details, see the upstream documentation at http://custodia.readthedocs.io.

Note that since Red Hat Enterprise Linux 7.6, Custodia has been deprecated.

(BZ#1403214)

7.3. CLUSTERING

Heuristics in **corosync-qdevice** available as a Technology Preview

Heuristics are a set of commands executed locally on startup, cluster membership change, successful connect to **corosync-qnetd**, and, optionally, on a periodic basis. When all commands finish successfully on time (their return error code is zero), heuristics have passed; otherwise, they have failed. The heuristics result is sent to **corosync-qnetd** where it is used in calculations to determine which partition should be quorate.

(BZ#1413573)

New fence-agents-heuristics-ping fence agent

As a Technology Preview, Pacemaker now supports the **fence_heuristics_ping** agent. This agent aims to open a class of experimental fence agents that do no actual fencing by themselves but instead exploit the behavior of fencing levels in a new way.

If the heuristics agent is configured on the same fencing level as the fence agent that does the actual fencing but is configured before that agent in sequence, fencing issues an **off** action on the heuristics agent before it attempts to do so on the agent that does the fencing. If the heuristics agent gives a negative result for the **off** action it is already clear that the fencing level is not going to succeed, causing Pacemaker fencing to skip the step of issuing the **off** action on the agent that does the fencing. A heuristics agent can exploit this behavior to prevent the agent that does the actual fencing from fencing a node under certain conditions.

A user might want to use this agent, especially in a two-node cluster, when it would not make sense for a node to fence the peer if it can know beforehand that it would not be able to take over the services properly. For example, it might not make sense for a node to take over services if it has problems reaching the networking uplink, making the services unreachable to clients, a situation which a ping to a router might detect in that case.

(BZ#1476401)

The pcs tool now manages bundle resources in Pacemaker

As a Technology Preview starting with Red Hat Enterprise Linux 7.4, Pacemaker supports a special syntax for launching a Docker container with any infrastructure it requires: the bundle. After you have created a Pacemaker bundle, you can create a Pacemaker resource that the bundle encapsulates. For information on Pacemaker support for containers, see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/high_availability_add-on_reference/.

There is one exception to this feature being Technology Preview: As of RHEL 7.4, Red Hat fully supports the usage of Pacemaker bundles for Red Hat Openstack Platform (RHOSP) deployments.

(BZ#1433016)

New LVM and LVM lock manager resource agents

As a Technology Preview, Red Hat Enterprise Linux 7.6 introduces two new resource agents: **lvmlockd** and **LVM-activate**.

The **LVM-activate** agent provides a choice from multiple methods for LVM management throughout a cluster:

- tagging: the same as tagging with the existing **lvm** resource agent
- clvmd: the same as clvmd with the existing **lvm** resource agent
- system ID: a new option for using system ID for volume group failover (an alternative to tagging).

- lvmlockd: a new option for using **lvmlockd** and **dlm** for volume group sharing (an alternative to **clvmd**).

The new **lvmlockd** resource agent is used to start the **lvmlockd** daemon when **LVM-activate** is configured to use **lvmlockd**.

For information on the lvmlockd and LVM-activate resource agent, see the PCS help screens for those agents. For information on setting up LVM for use with **lvmlockd**, see the **lvmlockd(8)** man page.

(BZ#1513957)

7.4. DESKTOP

Wayland available as a Technology Preview

The **Wayland** display server protocol is available in Red Hat Enterprise Linux as a Technology Preview with the dependent packages required to enable **Wayland** support in GNOME, which supports fractional scaling. **Wayland** uses the **libinput** library as its input driver.

The following features are currently unavailable or do not work correctly:

- Multiple GPU support is not possible at this time.
- The **NVIDIA** binary driver does not work under **Wayland**.
- The **xrandr** utility does not work under **Wayland** due to its different approach to handling, resolutions, rotations, and layout.
- Screen recording, remote desktop, and accessibility do not always work correctly under **Wayland**.
- No clipboard manager is available.
- It is currently impossible to restart **GNOME Shell** under **Wayland**.
- **Wayland** ignores keyboard grabs issued by X11 applications, such as virtual machines viewers.

(BZ#1481411)

Fractional Scaling available as a Technology Preview

Starting with Red Hat Enterprise Linux 7.5, GNOME provides, as a Technology Preview, fractional scaling to address problems with monitors whose DPI lies in the middle between lo (scale 1) and hi (scale 2).

Due to technical limitations, fractional scaling is available only on Wayland.

(BZ#1481395)

7.5. FILE SYSTEMS

File system DAX is now available for ext4 and XFS as a Technology Preview

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.

(BZ#1274459)

pNFS block layout is now available

As a Technology Preview, Red Hat Enterprise Linux clients can now mount pNFS shares with the block layout feature.

Note that Red Hat recommends using the pNFS SCSI layout instead, which is similar to block layout but easier to use.

(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. See the Linux kernel documentation for additional information.

OverlayFS remains a Technology Preview 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.

- On Red Hat Enterprise Linux 7.3 and earlier, 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 the **/etc/sysconfig/docker** file must not contain **--selinux-enabled**. Starting with Red Hat Enterprise Linux 7.4, OverlayFS supports SELinux security labels, and you can enable SELinux support for containers by specifying **--selinux-enabled** in **/etc/sysconfig/docker**.

- 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 in this release. For details, see **Non-standard behavior** in the Linux kernel documentation.

(BZ#1206277)

Btrfs file system

The B-Tree file system, **Btrfs**, is available as a Technology Preview in Red Hat Enterprise Linux 7.

Red Hat Enterprise Linux 7.4 introduced the last planned update to this feature. **Btrfs** has been deprecated, which means Red Hat will not be moving **Btrfs** to a fully supported feature and it will be removed in a future major release of Red Hat Enterprise Linux.

(BZ#1477977)

7.6. 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.

(BZ#1062759)

tss2 enables TPM 2.0 for IBM Power LE

The **tss2** package adds IBM implementation of a Trusted Computing Group Software Stack (TSS) 2.0 as a Technology Preview for the IBM Power LE architecture. This package enables users to interact with TPM 2.0 devices.

(BZ#1384452)

The ibmvnic device driver available as a Technology Preview

Since Red Hat Enterprise Linux 7.3, the IBM Virtual Network Interface Controller (vNIC) driver for IBM POWER architectures, **ibmvnic**, has been available as a Technology Preview. vNIC is a 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.

In Red Hat Enterprise Linux 7.6, the **ibmvnic** driver was upgraded to version 1.0, which provides a number of bug fixes and enhancements over the previous version. Notable changes include:

- The code that previously requested error information has been removed because no error ID is provided by the Virtual Input-Output (VIOS) Server.

- Error reporting has been updated with the cause string. As a result, during a recovery, the driver classifies the string as a warning rather than an error.
- Error recovery on a login failure has been fixed.
- The failed state that occurred after a failover while migrating Logical Partitioning (LPAR) has been fixed.
- The driver can now handle all possible login response return values.
- A driver crash that happened during a failover or Link Power Management (LPM) if the Transmit and Receive (Tx/Rx) queues have changed has been fixed.

(BZ#1519746)

Aero adapters available as a Technology Preview

The following Aero adapters are available as a Technology Preview:

- PCI ID 0x1000:0x00e2 and 0x1000:0x00e6, controlled by the **mpt3sas** driver
- PCI ID 0x1000:Ox10e5 and 0x1000:0x10e6, controlled by the **megaraid_sas** driver

(BZ#1660791, BZ#1660289)

The ice driver available as a Technology Preview

The Intel® Ethernet Connection E800 Series Linux Driver (**ice.ko.xz**) is available as a Technology Preview.

(BZ#1454916)

The igc driver available as a Technology Preview

The Intel® 2.5G Ethernet Linux Driver (**igc.ko.xz**) is available as a Technology Preview.

(BZ#1454918)

7.7. KERNEL

eBPF system call for tracing

Red Hat Enterprise Linux 7.6 introduces the Extended Berkeley Packet Filter tool (eBPF) as a Technology Preview. This tool is enabled only for the tracing subsystem. For details, see the related Red Hat Knowledgebase article.

(BZ#1559615)

Heterogeneous memory management included as a Technology Preview

Red Hat Enterprise Linux 7.3 introduced 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)

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)

kexec fast reboot as a Technology Preview

The **kexec fast reboot** feature, which was introduced in Red Hat Enterprise Linux 7.5, continues to be available as a Technology Preview. **kexec fast reboot** makes the reboot significantly faster. To use this feature, you must load the kexec kernel manually, and then reboot the operating system.

It is not possible to make **kexec fast reboot** as the default reboot action. Special case is using **kexec fast reboot** for **Anaconda**. It still does not enable to make **kexec fast reboot** default. However, when used with **Anaconda**, the operating system can automatically use **kexec fast reboot** after the installation is complete in case that user boots kernel with the anaconda option. To schedule a kexec reboot, use the **inst.kexec** command on the kernel command line, or include a **reboot --kexec** line in the Kickstart file.

(BZ#1464377)

perf cqm has been replaced by resctrl

The Intel Cache Allocation Technology (CAT) was introduced in Red Hat Enterprise Linux 7.4 as a Technology Preview. However, the **perf cqm** tool did not work correctly due to an incompatibility between perf infrastructure and Cache Quality of Service Monitoring (CQM) hardware support. Consequently, multiple problems occurred when using **perf cqm**.

These problems included most notably:

- **perf cqm** did not support the group of tasks which is allocated using **resctrl**
- **perf cqm** gave random and inaccurate data due to several problems with recycling
- **perf cqm** did not provide enough support when running different kinds of events together (the different events are, for example, tasks, system-wide, and cgroup events)
- **perf cqm** provided only partial support for cgroup events
- The partial support for cgroup events did not work in cases with a hierarchy of cgroup events, or when monitoring a task in a cgroup and the cgroup together
- Monitoring tasks for the lifetime caused **perf** overhead
- **perf cqm** reported the aggregate cache occupancy or memory bandwidth over all sockets, while in most cloud and VMM-bases use cases the individual per-socket usage is needed

In Red Hat Enterprise Linux 7.5, **perf cqm** was replaced by the approach based on the **resctrl** file system, which addressed all of the aforementioned problems.

(BZ#1457533)

TC HW offloading available as a Technology Preview

Starting with Red Hat Enterprise Linux 7.6, Traffic Control (TC) Hardware offloading has been provided as a Technology Preview.

Hardware offloading enables that the selected functions of network traffic processing, such as shaping, scheduling, policing and dropping, are executed directly in the hardware instead of waiting for software processing, which improves the performance.

(BZ#1503123)

AMD xgbe network driver available as a Technology Preview

Starting with Red Hat Enterprise Linux 7.6, the AMD **xgbe** network driver has been provided as a Technology Preview.

(BZ#1589397)

Secure Memory Encryption is available only as a Technology Preview

Currently, Secure Memory Encryption (SME) is incompatible with kdump functionality, as the kdump kernel lacks the memory key to decrypt SME-encrypted memory. Red Hat found that with SME enabled, servers under testing might fail to perform some functions and therefore the feature is unfit for use in production. Consequently, SME is changing the support level from Supported to Technology Preview. Customers are encouraged to report any issues found while testing in pre-production to Red Hat or their system vendor.

(BZ#1726642)

criu rebased to version 3.5

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.

In Red Hat Enterprise Linux 7.7, the **criu** packages were upgraded to the latest upstream version, which provides support for Podman to do a container checkpoint and restore. The newly added functionality only works without SELinux support.

(BZ#1400230)

The mlx5_core driver supports the Mellanox ConnectX-6 Dx network adapter as a Technology Preview

This enhancement adds the PCI IDs of the Mellanox ConnectX-6 Dx network adapter to the **mlx5_core** driver. On hosts that use this adapter, RHEL loads the **mlx5_core** driver automatically. Note that Red Hat provides this feature as an unsupported Technology Preview.

(BZ#1685900)

7.8. 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 available 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 available 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, available 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)

The flower classifier with off-loading support

flower is a Traffic Control (TC) classifier intended to allow users to configure matching on well-known packet fields for various protocols. It is intended to make it easier to configure rules over the **u32** classifier for complex filtering and classification tasks. **flower** also supports the ability to off-load classification and action rules to underlying hardware if the hardware supports it. The **flower** TC classifier is now provided as a Technology Preview.

(BZ#1393375)

7.9. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The postfix role of RHEL System Roles available as a Technology Preview

Red Hat Enterprise Linux System Roles provides a configuration interface for Red Hat Enterprise Linux subsystems, which makes system configuration easier through the inclusion of Ansible Roles. This interface enables managing system configurations across multiple versions of Red Hat Enterprise Linux, as well as adopting new major releases.

Since Red Hat Enterprise Linux 7.4, the **rhel-system-roles** packages have been distributed through the Extras repository.

The **postfix** role is available as a Technology Preview.

The following roles are fully supported:

- **kdump**
- **network**
- **selinux**
- **storage** - available with the RHEA-2020:0407 advisory
- **timesync**

For more information, see the Knowledgebase article about RHEL System Roles.

(BZ#1439896)

rhel-system-roles-sap available as a Technology Preview

The **rhel-system-roles-sap** package provides Red Hat Enterprise Linux (RHEL) System Roles for SAP, which can be used to automate the configuration of a RHEL system to run SAP workloads. These roles greatly reduce the time to configure a system to run SAP workloads by automatically applying the optimal settings that are based on best practices outlined in relevant SAP Notes. Access is limited to RHEL for SAP Solutions offerings. Please contact Red Hat Customer Support if you need assistance with your subscription.

With the RHEA-2019:3190 advisory, the following new roles in the **rhel-system-roles-sap** package are available as a Technology Preview:

- **sap-preconfigure**
- **sap-netweaver-preconfigure**
- **sap-hana-preconfigure**

For more information, see Red Hat Enterprise Linux System Roles for SAP .

Note: RHEL 7.7 for SAP Solutions is scheduled to be validated for use with SAP HANA on Intel 64 architecture and IBM POWER8. Other SAP applications and database products, for example, SAP NetWeaver and SAP ASE, can use RHEL 7.7 features. Please consult SAP Notes 2369910 and 2235581 for the latest information about validated releases and SAP support.

(BZ#1752544)

7.10. SECURITY

SECCOMP can be now enabled in *libreswan*

As a Technology Preview, the **seccomp=enabled|tolerant|disabled** option has been added to the **ipsec.conf** configuration file, which makes it possible to use the Secure Computing mode (SECCOMP). This improves the syscall security by whitelisting all the system calls that **Libreswan** is allowed to execute. For more information, see the **ipsec.conf(5)** man page.

(BZ#1375750)

pk12util can now import certificates signed with RSA-PSS

The **pk12util** tool now provides importing a certificate signed with the **RSA-PSS** algorithm as a Technology Preview.

Note that if the corresponding private key is imported and has the **PrivateKeyInfo.privateKeyAlgorithm** field that restricts the signing algorithm to **RSA-PSS**, it is ignored when importing the key to a browser. See https://bugzilla.mozilla.org/show_bug.cgi?id=1413596 for more information.

(BZ#1431210)

Support for certificates signed with RSA-PSS in certutil has been improved

Support for certificates signed with the **RSA-PSS** algorithm in the **certutil** tool has been improved. Notable enhancements and fixes include:

- The **--pss** option is now documented.
- The **PKCS#1 v1.5** algorithm is no longer used for self-signed signatures when a certificate is restricted to use **RSA-PSS**.
- Empty **RSA-PSS** parameters in the **subjectPublicKeyInfo** field are no longer printed as invalid when listing certificates.
- The **--pss-sign** option for creating regular RSA certificates signed with the **RSA-PSS** algorithm has been added.

Support for certificates signed with **RSA-PSS** in **certutil** is provided as a Technology Preview.

(BZ#1425514)

NSS is now able to verify RSA-PSS signatures on certificates

Since the RHEL 7.5 version of the *nss* package, the **Network Security Services** (NSS) libraries provide verifying **RSA-PSS** signatures on certificates as a Technology Preview. Prior to this update, clients using **NSS** as the **SSL** backend were not able to establish a **TLS** connection to a server that offered only certificates signed with the **RSA-PSS** algorithm.

Note that the functionality has the following limitations:

- The algorithm policy settings in the **/etc/pki/nss-legacy/rhel7.config** file do not apply to the hash algorithms used in **RSA-PSS** signatures.
- **RSA-PSS** parameters restrictions between certificate chains are ignored and only a single certificate is taken into account.

(BZ#1432142)

USBGuard enables blocking USB devices while the screen is locked as a Technology Preview

With the **USBGuard** framework, you can influence how an already running **usbguard-daemon** instance handles newly inserted USB devices by setting the value of the "InsertedDevicePolicy" runtime parameter. This functionality is provided as a Technology Preview, and the default choice is to apply the policy rules to figure out whether to authorize the device or not.

See the Blocking USB devices while the screen is locked Knowledgebase article.

(BZ#1480100)

7.11. STORAGE

NVMe/FC available as a Technology Preview in Qlogic adapters using the qla2xxx driver

The NVMe over Fibre Channel (NVMe/FC) transport type is available as a Technology Preview in Qlogic adapters using the **qla2xxx** driver.

NVMe/FC is an additional fabric transport type for the Nonvolatile Memory Express (NVMe) protocol, in addition to the Remote Direct Memory Access (RDMA) protocol that was previously introduced in Red Hat Enterprise Linux.

NVMe/FC provides a higher-performance, lower-latency I/O protocol over existing Fibre Channel infrastructure. This is especially important with solid-state storage arrays, because it allows the performance benefits of NVMe storage to be passed through the fabric transport, rather than being encapsulated in a different protocol, SCSI.

Note that since Red Hat Enterprise Linux 7.6, NVMe/FC is fully supported with Broadcom Emulex Fibre Channel 32Gbit adapters using the **lpfc** driver.

(BZ#1387768)

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.

Also note that although **blk-mq** is intended to offer improved performance, particularly for low-latency devices, it is not guaranteed to always provide better performance. Notably, in some cases, enabling *scsi-mq* can result in significantly deteriorated performance, especially on systems with many CPUs.

(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)

SCSI-MQ as a Technology Preview in the qla2xxx and lpfc drivers

The **qla2xxx** driver updated in Red Hat Enterprise Linux 7.4 can enable the use of SCSI-MQ (multiqueue) with the **ql2xmqsupport=1** module parameter. The default value is **0** (disabled).

The SCSI-MQ functionality is provided as a Technology Preview when used with the **qla2xxx** or the **lpfc** drivers.

Note that a recent performance testing at Red Hat with async IO over Fibre Channel adapters using SCSI-MQ has shown significant performance degradation under certain conditions.

(BZ#1414957)

7.12. SYSTEM AND SUBSCRIPTION MANAGEMENT

YUM 4 available as Technology Preview

YUM version 4, a next generation of the YUM package manager, is available as a Technology Preview in the Red Hat Enterprise Linux 7 Extras channel.

YUM 4 is based on the **DNF** technology and offers the following advantages over the standard **YUM 3** used on RHEL 7:

- Increased performance
- Support for modular content
- Well-designed stable API for integration with tooling

To install **YUM 4**, run the **yum install nextgen-yum4** command.

Make sure to install the **dnf-plugin-subscription-manager** package, which includes the **subscription-manager** plug-in. This plug-in is required for accessing protected repositories provided by the Red Hat Customer Portal or Red Hat Satellite 6, and for automatic updates of the **/etc/yum.repos.d/redhat.repo** file.

To manage packages, use the **yum4** command and its particular options the same way as the **yum** command.

For detailed information about differences between the new **YUM 4** tool and **YUM 3**, see Changes in DNF CLI compared to YUM.

For instructions on how to enable the Extras channel, see the Knowledgebase article How to subscribe to the Extras channel/repo.

(BZ#1461652)

7.13. VIRTUALIZATION

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.

(BZ#1103193)

Select Intel network adapters now support SR-IOV in RHEL 7 guest OS on Hyper-V

As a Technology Preview, Red Hat Enterprise Linux 7 guest operating systems running on a Hyper-V hypervisor can now use the single-root I/O virtualization (SR-IOV) feature for Intel network adapters supported by the **ixgbevf** and **i40evf** drivers. This feature 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 2019 and 2016.

(BZ#1348508)

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)

Azure M416v2 as a host for RHEL 7 guests

As a Technology Preview, the Azure M416v2 instance type can now be used as a host for virtual machines that use RHEL 7.6 and later as the guest operating systems.

(BZ#1661654)

virt-v2v can convert Debian and Ubuntu guests

As a Technology Preview, the **virt-v2v** utility can now convert Debian and Ubuntu guest virtual machines. Note that the following problems currently occur when performing this conversion:

- **virt-v2v** cannot change the default kernel in the GRUB2 configuration, and the kernel configured in the guest is not changed during the conversion, even if a more optimal version of the kernel is available on the guest.
- After converting a Debian or Ubuntu VMware guest to KVM, the name of the guest's network interface may change, and thus requires manual configuration.

(BZ#1387213)

GPU-based mediated devices now support the VNC console

As a Technology Preview, the Virtual Network Computing (VNC) console is now available for use with GPU-based mediated devices, such as the NVIDIA vGPU technology. As a result, it is now possible to use these mediated devices for real-time rendering of a virtual machine's graphical output.

(BZ#1475770)

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. However, OVMF is not bootable with virtualization components available in RHEL 7. Note that OVMF is fully supported in RHEL 8.

(BZ#653382)

CHAPTER 8. KNOWN ISSUES

This chapter documents known problems in Red Hat Enterprise Linux 7.7.

8.1. AUTHENTICATION AND INTEROPERABILITY

Inconsistent warning message when applying an ID range change

In RHEL Identity Management (IdM), you can define multiple identity ranges (ID ranges) associated with a local IdM domain or a trusted Active Directory domain. The information about ID ranges is retrieved by the SSSD daemon on all enrolled systems.

A change to ID range properties requires restart of SSSD. Previously, there was no warning about the need to restart SSSD. RHEL 7.7 adds a warning that is displayed when ID range properties are modified in a way that requires restart of SSSD.

The warning message currently uses inconsistent wording. The purpose of the warning message is to ask for a restart of SSSD on any IdM system that consumes the ID range. To learn more about ID ranges, see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/managing-unique_uid_and_gid_attributes

(BZ#1631826)

8.2. COMPILER AND TOOLS

GCC thread sanitizer included in RHEL no longer works

Due to incompatible changes in kernel memory mapping, the thread sanitizer included with the GNU C Compiler (GCC) compiler version in RHEL no longer works. Additionally, the thread sanitizer cannot be adapted to the incompatible memory layout. As a result, it is no longer possible to use the GCC thread sanitizer included with RHEL.

As a workaround, use the version of GCC included in Red Hat Developer Toolset to build code which uses the thread sanitizer.

(BZ#1569484)

Context variables in SystemTap not always accessible

The generation of debug information in the GCC compiler has some limitations. As a consequence, when analyzing the resulting executable files with the SystemTap tool, context variables listed in the form **$foo** are often inaccessible. To work around this limitation, add the **-P** option to the **$HOME/.systemtap/rc** file. This causes SystemTap to always select prologue-searching heuristics. As a result, some of the context variables can become accessible.

(BZ#1714480)

ksh with the KEYBD trap mishandles multibyte characters

The Korn Shell (KSH) is unable to correctly handle multibyte characters when the **KEYBD** trap is enabled. Consequently, when the user enters, for example, Japanese characters, **ksh** displays an incorrect string. To work around this problem, disable the **KEYBD** trap in the **/etc/kshrc** file by commenting out the following line:

```
trap keybd_trap KEYBD
```

For more details, see a related Knowledgebase solution.

(BZ#1503922)

Error while upgrading PCP from the RHEL 7.6 version

When you upgrade the **pcp** packages from the RHEL 7.6 to the RHEL 7.7 version, **yum** returns the following error message:

```
Failed to resolve allow statement at /etc/selinux/targeted/tmp/modules/400/pcpupstream/cil:83
semodule:  Failed!
```

It is safe to ignore this harmless message, which is caused by a bug in the RHEL 7.6 build of **pcp** and not by the updated package. The **PCP** functionality in RHEL 7.7 is not affected.

(BZ#1781692)

8.3. DESKTOP

Gnome Documents cannot display some documents when installed without LibreOffice

Gnome Documents uses libraries provided by the **LibreOffice** suite for rendering certain types of documents, such as OpenDocument Text or Open Office XML formats. However, the required **libreoffice-filters** libraries are missing from the dependency list of the **gnome-documents** package. Therefore, if you install **Gnome Documents** on a system that does not have **LibreOffice**, these document types cannot be rendered.

To work around this problem, install the **libreoffice-filters** package manually, even if you do not plan to use LibreOffice itself.

(BZ#1695699)

GNOME Software cannot install packages from unsigned repositories

GNOME Software cannot install packages from repositories that have the following setting in the *.repo file:

```
gpgcheck=0
```

If you attempt to install a package from such repository, **GNOME software** fails with a generic error. Currently, there is no workaround available.

(BZ#1591270)

Nautilus does not hide icons in the GNOME Classic Session

The GNOME Tweak Tool setting to show or hide icons in the GNOME session, where the icons are hidden by default, is ignored in the GNOME Classic Session. As a result, it is not possible to hide icons in the GNOME Classic Session even though the GNOME Tweak Tool displays this option.

(BZ#1474852)

8.4. INSTALLATION AND BOOTING

RHEL 7.7 and later installations add spectre_v2=retpoline to Intel Cascade Lake systems

RHEL 7.7 and later installations add the **spectre_v2=retpoline** kernel parameter to Intel Cascade Lake systems, and as a consequence, system performance is affected. To work around this problem and ensure the best performance, complete the following steps.

1. Remove the kernel boot parameter on Intel Cascade Lake systems:

```
# grubby --remove-args="spectre_v2=retpoline" --update-kernel=DEFAULT
```

2. Reboot the system:

```
# reboot
```

(BZ#1767612)

8.5. KERNEL

RHEL 7 virtual machines sometimes fail to boot on ESXi 5.5

When running Red Hat Enterprise Linux 7 guests with 12 GB RAM or above on a VMware ESXi 5.5 hypervisor, certain components currently initialize with incorrect memory type range register (MTRR) values or incorrectly reconfigure MTRR values across boots. This sometimes causes the guest kernel to panic or the guest to become unresponsive during boot.

To work around this problem, add the **disable_mtrr_trim** option to the guest's kernel command line, which enables the guest to continue booting when MTRRs are configured incorrectly. Note that with this option, the guest prints **WARNING: BIOS bug** messages during boot, which you can safely ignore.

(BZ#1429792)

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)

The i40iw module does not load automatically on boot

Some i40e NICs do not support iWarp and the **i40iw** module does not fully support suspend and resume operations. Consequently, the **i40iw** module is not automatically loaded by default to ensure suspend and resume operations work properly. To work around this problem, edit the **/lib/udev/rules.d/90-rdma-hw-modules.rules** file to enable automated load of **i40iw**.

Also note that if there is another RDMA device installed with an i40e device on the same machine, the non-i40e RDMA device triggers the **rdma** service, which loads all enabled RDMA stack modules, including the **i40iw** module.

(BZ#1622413)

The non-interleaved persistent memory configurations cannot use storage

Previously, systems with persistent memory aligned to 64 MB boundaries, prevented creating of namespaces. As a consequence, the non-interleaved persistent memory configurations in some cases

were not able to use storage. To work around this problem, use the interleaved mode for the persistent memory. As a result, most of the storage is available for use, however, with limited fault isolation.

(BZ#1691868)

System boot might fail due to persistent memory file systems

Systems with a large amount of persistent memory take a long time to boot. If the **/etc/fstab** file configures persistent memory file systems, the system might time out waiting for the devices to become available. The boot process then fails and presents the user with an emergency prompt.

To work around the problem, increase the **DefaultTimeoutStartSec** value in the **/etc/systemd/system.conf** file. Use a sufficiently large value, such as **1200s**. As a result, the system boot no longer times out.

(BZ#1666535)

radeon fails to reset hardware correctly

The **radeon** kernel driver currently does not reset hardware in the kexec context correctly. Instead, **radeon** terminates unexpectedly, which causes the rest of the **kdump** service to fail.

To work around this bug, blacklist **radeon** in **kdump** by adding the following line to the **/etc/kdump.conf** file:

```
dracut_args --omit-drivers "radeon"
```

Afterwards, restart the machine and **kdump**.

Note that in this scenario, no graphics will be available during **kdump**, but **kdump** will complete successfully.

(BZ#1509444)

Certain eBPF tools can cause the system to become unresponsive on IBM Z

Due to a bug in the JIT compiler, running certain eBPF tools contained in the **bcc-tools** package on IBM Z might cause the system to become unresponsive. To work around this problem, avoid using the **dcsnoop**, **runqlen**, and **slabratetop** tools from **bcc-tools** on IBM Z until a fix is released.

(BZ#1724027)

Concurrent SG_IO requests in /dev/sg might cause data corruption

The **/dev/sg** device driver is missing synchronization of kernel data. Concurrent requests in the driver access the same data at the same time.

As a consequence, the **ioctl** system call might sometimes erroneously use the payload of an **SG_IO** request for a different command that was sent at the same time as the correct one. This might lead to disk corruption in certain cases. Red Hat has observed this bug in Red Hat Virtualization (RHV).

To work around the problem, use either of the following solutions:

- Do not send concurrent requests to the **/dev/sg** driver. As a result, each **SG_IO** request sent to **/dev/sg** is guaranteed to use the correct data.
- Alternatively, use the **/dev/sd** or the **/dev/bsg** drivers instead of **/dev/sg**. The bug is not present in these drivers.

(BZ#1710533)

Incorrect order for inner and outer VLAN tags

The system receives the inner and outer VLAN tags in a swapped order when using QinQ (IEEE802.1Q in IEEE802.1Q standard) over representor devices when using the **mlx5** driver. That happens because the rxvlan offloading switch is not effective on this path and it causes Open vSwitch (OVS) to push this error forward. There is no known workaround.

(BZ#1701502)

kdump fails to generate vmcore on Azure instances in RHEL 7

An underlying problem with the serial console implementation on Azure instances booted through the UEFI bootloader causes that the **kdump** kernel is unable to boot. Consequently, the vmcore of the crashed kernel cannot be captured in the /**var**/**crash**/ directory. To work around this problem:

1. Add the **console=ttyS0** and **earlyprintk=ttyS0** parameters to the **KDUMP_COMMANDLINE_REMOVE** command line in the /**etc**/**sysconfig**/**kdump** directory.

2. Restart the **kdump** service.

As a result, the **kdump** kernel should correctly boot and vmcore is expected to be captured upon crash.

Make sure there is enough space in /**var**/**crash**/ to save the vmcore, which can be up to the size of system memory.

(BZ#1724993)

The kdumpctl service fails to load crash kernel if KASLR is enabled

An inappropriate setting of the **kptr_restrict** kernel tunable causes that contents of the /**proc**/**kcore** file are generated as all zeros. As a consequence, the **kdumpctl** service is not able to access /**proc**/**kcore** and to load the crash kernel if Kernel Address Space Layout Randomization (KASLR) is enabled. To work around this problem, keep **kptr_restrict** set to **1**. As a result, **kdumpctl** is able to load the crash kernel in the described scenario.

For details, refer to the /**usr**/**share**/**doc**/**kexec-tools**/**kexec-kdump-howto.txt** file.

(BZ#1600148)

Kdump fails in the second kernel

The kdump **initramfs** archive is a critical component for capturing the crash dump. However, it is strictly generated for the machine it runs on and has no generality. If you did a disk migration or installed a new machine with a disk image, kdump might fail in the second kernel.

To work around this problem, if you did a disk migration, rebuild **initramfs** manually by running the following commands:

touch /etc/kdump.conf # kdumpctl restart

If you are creating a disk image for installing new machines, it is strongly recommended not to include the kdump **initramfs** in the disk image. It helps to save space and kdump will build the **initramfs** automatically if it is missing.

(BZ#1723492)

8.6. 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)

Booting from a network device fails when the network driver is restarted

Currently, if the boot device is mounted over the network when using iSCSI or Fibre Channel over Ethernet (FCoE), Red Hat Enterprise Linux (RHEL) fails to boot when the underlying network interface driver is restarted.

For example, RHEL restarts the **bnx2x** network driver when the **libvirt** service starts its first virtual network and enables IP forwarding. To work around the problem in this specific example, enable IPv4 forwarding earlier in the boot sequence:

```
# echo 'net.ipv4.ip_forward = 1' > /etc/sysctl.d/90-forwarding.conf
# dracut -f
```

Note that this workaround works only in the mentioned scenario.

(BZ#1574536)

freeradius might fail when upgrading from RHEL 7.3

A new configuration property, **correct_escapes**, in the **/etc/raddb/radiusd.conf** file was introduced in the **freeradius** version distributed since RHEL 7.4. When an administrator sets **correct_escapes** to **true**, the new regular expression syntax for backslash escaping is expected. If **correct_escapes** is set to **false**, the old syntax is expected where backslashes are also escaped. For backward compatibility reasons, **false** is the default value.

When upgrading, configuration files in the **/etc/raddb/** directory are overwritten unless modified by the administrator, so the value of **correct_escapes** might not always correspond to which type of syntax is used in all the configuration files. As a consequence, authentication with **freeradius** might fail.

To prevent the problem from occurring, after upgrading from **freeradius** version 3.0.4 (distributed with RHEL 7.3) and earlier, make sure all configuration files in the **/etc/raddb/** directory use the new escaping syntax (no double backslash characters can be found) and that the value of **correct_escapes** in **/etc/raddb/radiusd.conf** is set to **true**.

For more information and examples, see the solution Authentication with Freeradius fails since upgrade to version >= 3.0.5.

(BZ#1489758)

RHEL 7 shows the status of an 802.3ad bond as "Churned" after a switch was unavailable for an extended period of time

Currently, when you configure an 802.3ad network bond and the switch is down for an extended period of time, Red Hat Enterprise Linux properly shows the status of the bond as "Churned", even after the connection returns to a working state. However, this is the intended behavior, as the "Churned" status aims to tell the administrator that a significant link outage occurred. To clear this status, restart the network bond or reboot the host.

(BZ#1708807)

Using client-identifier leads to IP address conflict

If the **client-identifier** option is used, certain network switches ignore the **ciaddr** field of a dynamic host configuration protocol (DHCP) request. Consequently, the same IP address is assigned to multiple clients, which leads to an IP address conflict. To work around the problem, include the following line in the **dhclient.conf** file:

```
send dhcp-client-identifier = "";
```

As a result, the IP address conflict does not occur under the described circumstances.

(BZ#1193799)

8.7. SECURITY

Libreswan does not work properly with seccomp=enabled on all configurations

The set of allowed syscalls in the **Libreswan** SECCOMP support implementation is currently not complete. Consequently, when SECCOMP is enabled in the **ipsec.conf** file, the syscall filtering rejects even syscalls needed for the proper functioning of the **pluto** daemon; the daemon is killed, and the **ipsec** service is restarted.

To work around this problem, set the **seccomp=** option back to the **disabled** state. SECCOMP support must remain disabled to run **ipsec** properly.

(BZ#1544463)

PKCS#11 devices not supporting RSA-PSS cannot be used with TLS 1.3

The TLS protocol version 1.3 requires RSA-PSS signatures, which are not supported by all PKCS#11 devices, such as hardware security modules (HSM) or smart cards. Currently, server applications using NSS do not check the PKCS#11 module capabilities before negotiating TLS 1.3. As a consequence, attempts to authenticate using PKCS#11 devices that do not support RSA-PSS fail. To work around this problem, use TLS 1.2 instead.

(BZ#1711438)

TLS 1.3 does not work in NSS in FIPS mode

TLS 1.3 is not supported on systems working in FIPS mode. As a consequence, connections that require TLS 1.3 for interoperability do not function on a system working in FIPS mode.

To enable the connections, disable the system's FIPS mode or enable support for TLS 1.2 in the peer.

(BZ#1710372)

OpenSCAP inadvertently accesses remote file systems

The **OpenSCAP** scanner cannot correctly detect whether the scanned file system is a mounted remote file system or a local file system, and the detection part contains also other bugs. Consequently, the scanner reads mounted remote file systems even if an evaluated rule applies to a local file-system only, and it might generate unwanted traffic on remote file systems.

To work around this problem, unmount remote file systems before scanning. Another option is to exclude affected rules from the evaluated profile by providing a tailoring file.

(BZ#1694962)

8.8. SERVERS AND SERVICES

Manual initialization of MariaDB using mysql_install_db fails

The **mysql_install_db** script for initializing the MariaDB database calls the **resolveip** binary from the **/usr/libexec/** directory, while the binary is located in **/usr/bin/**. Consequently, manual initialization of the database using **mysql_install_db** fails.

To work around this problem, create a symbolic link to the actual location of the **resolveip** binary:

```
ln -s /usr/bin/resolveip /usr/libexec/resolveip
```

When the symlink is created, **mysql_install_db** successfully locates **resolveip**, and the manual database initialization is successful.

Alternatively, use **mysql_install_db** with the **--rpm** option. In this case, **mysql_install_db** does not call the **resolveip** binary, and therefore does not fail.

(BZ#1731062)

mysql-connector-java does not work with MySQL 8.0

The **mysql-connector-java** database connector provided in RHEL 7 does not work with the MySQL 8.0 database server. To work around this problem, use the **rh-mariadb103-mariadb-java-client** database connector from Red Hat Software Collections.

(BZ#1646363)

Harmless error messages occur when the balanced Tuned profile is used

The **balanced Tuned** profile has been changed in the way that the **cpufreq_conservative** kernel module loads when this profile is applied. However, **cpufreq_conservative** is built-in in the kernel, and it is not available as a module. Consequently, when the **balanced** profile is used, the following error messages occasionally appear in **/var/log/tuned/tuned.log** file:

```
tuned.utils.commands: Executing modinfo error: modinfo: ERROR: Module cpufreq_conservative not found.
tuned.plugins.plugin_modules: kernel module 'cpufreq_conservative' not found, skipping it
tuned.plugins.plugin_modules: verify: failed: 'module 'cpufreq_conservative' is not loaded'
```

Such error messages are harmless, so you can safely ignore them. However, to eliminate the errors, you can override the **balanced** profile, so that **Tuned** does not attempt to load the kernel module.

For example, create the **/etc/tuned/balanced/tuned.conf** file with the following contents:

```
[main]
include=balanced

[modules]
enabled=0
```

(BZ#1719160)

The php-mysqlnd database connector does not work with MySQL 8.0

The default character set has been changed to **utf8mb4** in MySQL 8.0 but this character set is unsupported by the **php-mysqlnd** database connector. Consequently, **php-mysqlnd** fails to connect in the default configuration. To work around this problem, specify a known character set as a parameter of the MySQL server configuration. For example, modify the **/etc/opt/rh/rh-mysql80/my.cnf.d/mysql-server.cnf** file to read:

```
[mysqld]
character-set-server=utf8
```

(BZ#1646158)

8.9. STORAGE

The system halts unexpectedly when using scsi-mq with software FCoE

The host system halts unexpectedly when it is configured to use both multiqueue scheduling (**scsi-mq**) and software Fibre Channel over Ethernet (FCoE) at the same time.

To work around the problem, disable **scsi-mq** when using software FCoE. As a result, the system no longer crashes.

(BZ#1712664)

The system boot sometimes fails on large systems

During the boot process, the **udev** device manager sometimes generates too many rules on large systems. For example, the problem has manifested on a system with 32 TB of memory and 192 CPUs. As a consequence, the boot process becomes unresponsive or times out and switches to the emergency shell.

To work around the problem, add the **udev.children-max=1000** option to the kernel command line. You can experiment with different values of **udev.children-max** to see which value results in the fastest boot on your system. As a result, the system boots successfully.

(BZ#1722855)

When an image is split off from an active/active cluster mirror, the resulting new logical volume has no active component

When you split off an image from an active/active cluster mirror, the resulting new logical appears active but it has no active component. To activate the newly split-off logical volume, deactivate the volume and then activate it with the following commands:

```
lvchange -an _vg_/_newly_split_lv_
lvchange -ay _vg_/_newly_split_lv_
```

(BZ#1642162)

8.10. VIRTUALIZATION

Virtual machines sometimes enable unnecessary CPU vulnerability mitigation

Currently, the **MDS_NO** CPU flags, which indicate that the CPU is not vulnerable to the Microarchitectural Data Sampling (MDS) vulnerability, are not exposed to guest operating systems. As a consequence, the guest operating system in some cases automatically enables CPU vulnerability mitigation features that are not necessary for the current host.

If the host CPU is known not to be vulnerable to MDS and the virtual machine is not going to be migrated to hosts vulnerable to MDS, MDS vulnerability mitigation can be disabled in Linux guests by using the "mds=off" kernel command-line option. Note, however, that this option disables all MDS mitigations on the guest. Therefore, it should be used with care and should never be used if the host CPU is vulnerable to MDS.

(BZ#1708465)

Modifying a RHEL 8 virtual image on a RHEL 7 host sometimes fails

On RHEL 7 hosts, using virtual image manipulation utilities such as **guestfish**, **virt-sysprep**, or **virt-customize** in some cases fails if the utility targets a virtual image that is using a RHEL 8 file system. This is because RHEL 7 is not fully compatible with certain file-system features in RHEL 8.

To work around the problem, you can disable the problematic features when creating the guest file systems using the **mkfs** utility:

- For XFS file systems, use the "-m reflink=0" option.
- For ext4 file systems, use the "-O ^metadata_csum" option.

Alternatively, use a RHEL 8 host instead of a RHEL 7 one, where the affected utilities will work as expected.

(BZ#1667478)

Slow connection to RHEL 7 guest console on a Windows Server 2019 host

When using RHEL 7 as a guest operating system in multi-user mode on a Windows Server 2019 host, connecting to a console output of the guest currently takes significantly longer than expected. To work around this problem, connect to the guest using SSH or use Windows Server 2016 as the host.

(BZ#1706522)

SMT works only on AMD EPYC CPU models

Currently, only the **AMD EPYC** CPU models support the simultaneous multithreading (SMT) feature. As a consequence, manually enabling the **topoext** feature when configuring a virtual machine (VM) with a different CPU model causes the VM not to detect the vCPU topology correctly, and the vCPU does not

perform as configured. To work around this problem, do not enable **topoext** manually and do not use the **threads** vCPU option on AMD hosts unless the host is using the **AMD EPYC** model

(BZ#1615682)

CHAPTER 9. 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 7.7.

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.

For details regarding differences between RHEL 7 and RHEL 8, see Considerations in adopting RHEL 8 .

9.1. DEPRECATED PACKAGES

The following packages are now deprecated. For information regarding replaced packages or availability in an unsupported RHEL 8 repository (if applicable), see Considerations in adopting RHEL 8 .

- a2ps
- abrt-addon-upload-watch
- abrt-devel
- abrt-gui-devel
- abrt-retrace-client
- acpid-sysvinit
- advancecomp
- adwaita-icon-theme-devel
- adwaita-qt-common
- adwaita-qt4
- agg
- aic94xx-firmware
- akonadi
- akonadi-devel
- akonadi-mysql
- alacarte

- alsa-tools
- anaconda-widgets-devel
- ant-antunit
- ant-antunit-javadoc
- antlr-C++-doc
- antlr-python
- antlr-tool
- apache-commons-collections-javadoc
- apache-commons-collections-testframework
- apache-commons-configuration
- apache-commons-configuration-javadoc
- apache-commons-daemon
- apache-commons-daemon-javadoc
- apache-commons-daemon-jsvc
- apache-commons-dbcp
- apache-commons-dbcp-javadoc
- apache-commons-digester
- apache-commons-digester-javadoc
- apache-commons-jexl
- apache-commons-jexl-javadoc
- apache-commons-lang-javadoc
- apache-commons-pool
- apache-commons-pool-javadoc
- apache-commons-validator
- apache-commons-validator-javadoc
- apache-commons-vfs
- apache-commons-vfs-ant
- apache-commons-vfs-examples
- apache-commons-vfs-javadoc

- apache-rat
- apache-rat-core
- apache-rat-javadoc
- apache-rat-plugin
- apache-rat-tasks
- apr-util-nss
- args4j
- args4j-javadoc
- ark
- ark-libs
- asciidoc-latex
- at-spi
- at-spi-devel
- at-spi-python
- at-sysvinit
- atlas-static
- attica
- attica-devel
- audiocd-kio
- audiocd-kio-devel
- audiocd-kio-libs
- audiofile
- audiofile-devel
- audit-libs-python
- audit-libs-static
- authconfig
- authconfig-gtk
- authd
- autogen-libopts-devel

- automoc
- autotrace-devel
- avahi-dnsconfd
- avahi-glib-devel
- avahi-gobject-devel
- avahi-qt3
- avahi-qt3-devel
- avahi-qt4
- avahi-qt4-devel
- avahi-tools
- avahi-ui
- avahi-ui-devel
- avahi-ui-tools
- avalon-framework
- avalon-framework-javadoc
- avalon-logkit
- avalon-logkit-javadoc
- bacula-console-bat
- bacula-devel
- bacula-traymonitor
- baekmuk-ttf-batang-fonts
- baekmuk-ttf-dotum-fonts
- baekmuk-ttf-fonts-common
- baekmuk-ttf-fonts-ghostscript
- baekmuk-ttf-gulim-fonts
- baekmuk-ttf-hline-fonts
- base64coder
- base64coder-javadoc
- batik

- batik-demo
- batik-javadoc
- batik-rasterizer
- batik-slideshow
- batik-squiggle
- batik-svgpp
- batik-ttf2svg
- bcc-devel
- bcel
- bison-devel
- blas-static
- blas64-devel
- blas64-static
- bltk
- bluedevil
- bluedevil-autostart
- bmc-snmp-proxy
- bogofilter-bogoupgrade
- bridge-utils
- bsdcpio
- bsh-demo
- bsh-utils
- btrfs-progs
- btrfs-progs-devel
- buildnumber-maven-plugin
- buildnumber-maven-plugin-javadoc
- bwidget
- bzr
- bzr-doc

- cairo-tools
- cal10n
- caribou
- caribou-antler
- caribou-devel
- caribou-gtk2-module
- caribou-gtk3-module
- cdi-api-javadoc
- cdparanoia-static
- cdrskin
- ceph-common
- check-static
- cheese-libs-devel
- cifs-utils-devel
- cim-schema-docs
- cim-schema-docs
- cjkuni-ukai-fonts
- clutter-gst2-devel
- clutter-tests
- cmpi-bindings-pywbem
- cobertura
- cobertura-javadoc
- cockpit-machines-ovirt
- codehaus-parent
- codemodel
- codemodel-javadoc
- cogl-tests
- colord-extra-profiles
- colord-kde

- compat-cheese314
- compat-dapl
- compat-dapl-devel
- compat-dapl-static
- compat-dapl-utils
- compat-db
- compat-db-headers
- compat-db47
- compat-exiv2-023
- compat-gcc-44
- compat-gcc-44-c++
- compat-gcc-44-gfortran
- compat-glade315
- compat-glew
- compat-glibc
- compat-glibc-headers
- compat-gnome-desktop314
- compat-grilo02
- compat-libcap1
- compat-libcogl-pango12
- compat-libcogl12
- compat-libcolord1
- compat-libf2c-34
- compat-libgdata13
- compat-libgfortran-41
- compat-libgnome-bluetooth11
- compat-libgnome-desktop3-7
- compat-libgweather3
- compat-libical1

- compat-libmediaart0
- compat-libmpc
- compat-libpackagekit-glib2-16
- compat-libstdc++-33
- compat-libtiff3
- compat-libupower-glib1
- compat-libxcb
- compat-locales-sap-common
- compat-openldap
- compat-openmpi16
- compat-openmpi16-devel
- compat-opensm-libs
- compat-poppler022
- compat-poppler022-cpp
- compat-poppler022-glib
- compat-poppler022-qt
- compat-sap-c++-5
- compat-sap-c++-6
- compat-sap-c++-7
- conman
- console-setup
- coolkey
- coolkey-devel
- cpptest
- cpptest-devel
- cppunit
- cppunit-devel
- cppunit-doc
- cpuid

- cracklib-python
- crda-devel
- crit
- criu-devel
- crypto-utils
- cryptsetup-python
- cvs
- cvs-contrib
- cvs-doc
- cvs-inetd
- cvsps
- cyrus-imapd-devel
- dapl
- dapl-devel
- dapl-static
- dapl-utils
- dbus-doc
- dbus-python-devel
- dbus-tests
- dbusmenu-qt
- dbusmenu-qt-devel
- dbusmenu-qt-devel-docs
- debugmode
- dejagnu
- dejavu-lgc-sans-fonts
- dejavu-lgc-sans-mono-fonts
- dejavu-lgc-serif-fonts
- deltaiso
- dhcp-devel

- dialog-devel
- dleyna-connector-dbus-devel
- dleyna-core-devel
- dlm-devel
- dmraid
- dmraid-devel
- dmraid-events
- dmraid-events-logwatch
- docbook-simple
- docbook-slides
- docbook-style-dsssl
- docbook-utils
- docbook-utils-pdf
- docbook5-schemas
- docbook5-style-xsl
- docbook5-style-xsl-extensions
- docker-rhel-push-plugin
- dom4j
- dom4j-demo
- dom4j-javadoc
- dom4j-manual
- dovecot-pigeonhole
- dracut-fips
- dracut-fips-aesni
- dragon
- drm-utils
- drpmsync
- dtdinst
- e2fsprogs-static

- ecj
- edac-utils-devel
- efax
- efivar-devel
- egl-utils
- ekiga
- ElectricFence
- emacs-a2ps
- emacs-a2ps-el
- emacs-auctex
- emacs-auctex-doc
- emacs-git
- emacs-git-el
- emacs-gnuplot
- emacs-gnuplot-el
- emacs-php-mode
- empathy
- enchant-aspell
- enchant-voikko
- eog-devel
- epydoc
- espeak-devel
- evince-devel
- evince-dvi
- evolution-data-server-doc
- evolution-data-server-perl
- evolution-data-server-tests
- evolution-devel
- evolution-devel-docs

- evolution-tests
- expat-static
- expect-devel
- expectk
- farstream
- farstream-devel
- farstream-python
- farstream02-devel
- fedfs-utils-admin
- fedfs-utils-client
- fedfs-utils-common
- fedfs-utils-devel
- fedfs-utils-lib
- fedfs-utils-nsdbparams
- fedfs-utils-python
- fedfs-utils-server
- felix-bundlerepository
- felix-bundlerepository-javadoc
- felix-framework
- felix-framework-javadoc
- felix-osgi-obr
- felix-osgi-obr-javadoc
- felix-shell
- felix-shell-javadoc
- fence-sanlock
- festival
- festival-devel
- festival-docs
- festival-freebsoft-utils

- festival-lib
- festival-speechtools-devel
- festival-speechtools-libs
- festival-speechtools-utils
- festvox-awb-arctic-hts
- festvox-bdl-arctic-hts
- festvox-clb-arctic-hts
- festvox-jmk-arctic-hts
- festvox-kal-diphone
- festvox-ked-diphone
- festvox-rms-arctic-hts
- festvox-slt-arctic-hts
- file-static
- filebench
- filesystem-content
- finch
- finch-devel
- finger
- finger-server
- flatpak-devel
- flex-devel
- fltk-fluid
- fltk-static
- flute-javadoc
- folks
- folks-devel
- folks-tools
- fontforge-devel
- fontpackages-tools

- fonttools
- fop
- fop-javadoc
- fprintd-devel
- freeradius-python
- freetype-demos
- fros
- fros-gnome
- fros-recordmydesktop
- fwupd-devel
- fwupdate-devel
- gamin-python
- gavl-devel
- gcab
- gcc-gnat
- gcc-go
- gcc-objc
- gcc-objc++
- gcc-plugin-devel
- gconf-editor
- gd-progs
- gdk-pixbuf2-tests
- gdm-devel
- gdm-pam-extensions-devel
- gedit-devel
- gedit-plugin-bookmarks
- gedit-plugin-bracketcompletion
- gedit-plugin-charmap
- gedit-plugin-codecomment

- gedit-plugin-colorpicker
- gedit-plugin-colorschemer
- gedit-plugin-commander
- gedit-plugin-drawspaces
- gedit-plugin-findinfiles
- gedit-plugin-joinlines
- gedit-plugin-multiedit
- gedit-plugin-smartspaces
- gedit-plugin-synctex
- gedit-plugin-terminal
- gedit-plugin-textsize
- gedit-plugin-translate
- gedit-plugin-wordcompletion
- gedit-plugins
- gedit-plugins-data
- gegl-devel
- geoclue
- geoclue-devel
- geoclue-doc
- geoclue-gsmloc
- geoclue-gui
- GeoIP
- GeoIP-data
- GeoIP-devel
- GeoIP-update
- geronimo-jaspic-spec
- geronimo-jaspic-spec-javadoc
- geronimo-jaxrpc
- geronimo-jaxrpc-javadoc

- geronimo-jms
- geronimo-jta
- geronimo-jta-javadoc
- geronimo-osgi-support
- geronimo-osgi-support-javadoc
- geronimo-saaj
- geronimo-saaj-javadoc
- ghostscript-chinese
- ghostscript-chinese-zh_CN
- ghostscript-chinese-zh_TW
- ghostscript-cups
- ghostscript-devel
- ghostscript-gtk
- giflib-utils
- gimp-data-extras
- gimp-help
- gimp-help-ca
- gimp-help-da
- gimp-help-de
- gimp-help-el
- gimp-help-en_GB
- gimp-help-es
- gimp-help-fr
- gimp-help-it
- gimp-help-ja
- gimp-help-ko
- gimp-help-nl
- gimp-help-nn
- gimp-help-pt_BR

- gimp-help-ru
- gimp-help-sl
- gimp-help-sv
- gimp-help-zh_CN
- git-bzr
- git-cvs
- git-gnome-keyring
- git-hg
- git-p4
- gjs-tests
- glade
- glade3
- glade3-libgladeui
- glade3-libgladeui-devel
- glassfish-dtd-parser
- glassfish-dtd-parser-javadoc
- glassfish-jaxb-javadoc
- glassfish-jsp
- glassfish-jsp-javadoc
- glew
- glib-networking-tests
- gmp-static
- gnome-clocks
- gnome-common
- gnome-contacts
- gnome-desktop3-tests
- gnome-devel-docs
- gnome-dictionary
- gnome-doc-utils

- gnome-doc-utils-stylesheets
- gnome-documents
- gnome-documents-libs
- gnome-icon-theme
- gnome-icon-theme-devel
- gnome-icon-theme-extras
- gnome-icon-theme-legacy
- gnome-icon-theme-symbolic
- gnome-packagekit
- gnome-packagekit-common
- gnome-packagekit-installer
- gnome-packagekit-updater
- gnome-python2
- gnome-python2-bonobo
- gnome-python2-canvas
- gnome-python2-devel
- gnome-python2-gconf
- gnome-python2-gnome
- gnome-python2-gnomevfs
- gnome-settings-daemon-devel
- gnome-software-devel
- gnome-vfs2
- gnome-vfs2-devel
- gnome-vfs2-smb
- gnome-weather
- gnome-weather-tests
- gnote
- gnu-efi-utils
- gnu-getopt

- gnu-getopt-javadoc
- gnuplot-latex
- gnuplot-minimal
- gob2
- gom-devel
- google-noto-sans-korean-fonts
- google-noto-sans-simplified-chinese-fonts
- google-noto-sans-traditional-chinese-fonts
- gperftools
- gperftools-devel
- gperftools-libs
- gpm-static
- grantlee
- grantlee-apidocs
- grantlee-devel
- graphviz-graphs
- graphviz-guile
- graphviz-java
- graphviz-lua
- graphviz-ocaml
- graphviz-perl
- graphviz-php
- graphviz-python
- graphviz-ruby
- graphviz-tcl
- groff-doc
- groff-perl
- groff-x11
- groovy

- groovy-javadoc
- grub2
- grub2-ppc-modules
- grub2-ppc64-modules
- gsm-tools
- gsound-devel
- gssdp-utils
- gstreamer
- gstreamer-devel
- gstreamer-devel-docs
- gstreamer-plugins-bad-free
- gstreamer-plugins-bad-free-devel
- gstreamer-plugins-bad-free-devel-docs
- gstreamer-plugins-base
- gstreamer-plugins-base-devel
- gstreamer-plugins-base-devel-docs
- gstreamer-plugins-base-tools
- gstreamer-plugins-good
- gstreamer-plugins-good-devel-docs
- gstreamer-python
- gstreamer-python-devel
- gstreamer-tools
- gstreamer1-devel-docs
- gstreamer1-plugins-base-devel-docs
- gstreamer1-plugins-base-tools
- gstreamer1-plugins-ugly-free-devel
- gtk-vnc
- gtk-vnc-devel
- gtk-vnc-python

- gtk-vnc2-devel
- gtk3-devel-docs
- gtk3-immodules
- gtk3-tests
- gtkhtml3
- gtkhtml3-devel
- gtksourceview3-tests
- gucharmap
- gucharmap-devel
- gucharmap-libs
- gupnp-av-devel
- gupnp-av-docs
- gupnp-dlna-devel
- gupnp-dlna-docs
- gupnp-docs
- gupnp-igd-python
- gutenprint-devel
- gutenprint-extras
- gutenprint-foomatic
- gvfs-tests
- gvnc-devel
- gvnc-tools
- gvncpulse
- gvncpulse-devel
- gwenview
- gwenview-libs
- hamcrest
- hawkey-devel
- hesiod

- highcontrast-qt
- highcontrast-qt4
- highcontrast-qt5
- highlight-gui
- hispavoces-pal-diphone
- hispavoces-sfl-diphone
- hsakmt
- hsakmt-devel
- hspell-devel
- hsqldb
- hsqldb-demo
- hsqldb-javadoc
- hsqldb-manual
- htdig
- html2ps
- http-parser-devel
- httpunit
- httpunit-doc
- httpunit-javadoc
- i2c-tools-eepromer
- i2c-tools-python
- ibus-pygtk2
- ibus-qt
- ibus-qt-devel
- ibus-qt-docs
- ibus-rawcode
- ibus-table-devel
- ibutils
- ibutils-devel

- ibutils-libs
- icc-profiles-openicc
- icon-naming-utils
- im-chooser
- im-chooser-common
- ImageMagick
- ImageMagick-c++
- ImageMagick-c++-devel
- ImageMagick-devel
- ImageMagick-doc
- ImageMagick-perl
- imake
- imsettings
- imsettings-devel
- imsettings-gsettings
- imsettings-libs
- imsettings-qt
- imsettings-xim
- indent
- infinipath-psm
- infinipath-psm-devel
- iniparser
- iniparser-devel
- iok
- ipa-gothic-fonts
- ipa-mincho-fonts
- ipa-pgothic-fonts
- ipa-pmincho-fonts
- iperf3-devel

- iproute-doc
- ipset-devel
- ipsilon
- ipsilon-authform
- ipsilon-authgssapi
- ipsilon-authldap
- ipsilon-base
- ipsilon-client
- ipsilon-filesystem
- ipsilon-infosssd
- ipsilon-persona
- ipsilon-saml2
- ipsilon-saml2-base
- ipsilon-tools-ipa
- iputils-sysvinit
- iscsi-initiator-utils-devel
- isdn4k-utils
- isdn4k-utils-devel
- isdn4k-utils-doc
- isdn4k-utils-static
- isdn4k-utils-vboxgetty
- isomd5sum-devel
- isorelax
- istack-commons-javadoc
- ixpdimm_sw
- ixpdimm_sw-devel
- ixpdimm-cli
- ixpdimm-monitor
- jai-imageio-core

- jai-imageio-core-javadoc
- jakarta-commons-httpclient-demo
- jakarta-commons-httpclient-javadoc
- jakarta-commons-httpclient-manual
- jakarta-oro
- jakarta-taglibs-standard
- jakarta-taglibs-standard-javadoc
- jandex
- jandex-javadoc
- jansson-devel-doc
- jarjar
- jarjar-javadoc
- jarjar-maven-plugin
- jasper
- jasper-utils
- java-1.6.0-openjdk
- java-1.6.0-openjdk-demo
- java-1.6.0-openjdk-devel
- java-1.6.0-openjdk-javadoc
- java-1.6.0-openjdk-src
- java-1.7.0-openjdk
- java-1.7.0-openjdk-accessibility
- java-1.7.0-openjdk-demo
- java-1.7.0-openjdk-devel
- java-1.7.0-openjdk-headless
- java-1.7.0-openjdk-javadoc
- java-1.7.0-openjdk-src
- java-1.8.0-openjdk-accessibility-debug
- java-1.8.0-openjdk-debug

- java-1.8.0-openjdk-demo-debug
- java-1.8.0-openjdk-devel-debug
- java-1.8.0-openjdk-headless-debug
- java-1.8.0-openjdk-javadoc-debug
- java-1.8.0-openjdk-javadoc-zip-debug
- java-1.8.0-openjdk-src-debug
- java-11-openjdk-debug
- java-11-openjdk-demo-debug
- java-11-openjdk-devel-debug
- java-11-openjdk-headless-debug
- java-11-openjdk-javadoc-debug
- java-11-openjdk-javadoc-zip-debug
- java-11-openjdk-jmods-debug
- java-11-openjdk-src-debug
- javamail
- jaxen
- jboss-ejb-3.1-api
- jboss-ejb-3.1-api-javadoc
- jboss-el-2.2-api
- jboss-el-2.2-api-javadoc
- jboss-jaxrpc-1.1-api
- jboss-jaxrpc-1.1-api-javadoc
- jboss-servlet-2.5-api
- jboss-servlet-2.5-api-javadoc
- jboss-servlet-3.0-api
- jboss-servlet-3.0-api-javadoc
- jboss-specs-parent
- jboss-transaction-1.1-api
- jboss-transaction-1.1-api-javadoc

- jdom
- jettison
- jettison-javadoc
- jetty-annotations
- jetty-ant
- jetty-artifact-remote-resources
- jetty-assembly-descriptors
- jetty-build-support
- jetty-build-support-javadoc
- jetty-client
- jetty-continuation
- jetty-deploy
- jetty-distribution-remote-resources
- jetty-http
- jetty-io
- jetty-jaas
- jetty-jaspi
- jetty-javadoc
- jetty-jmx
- jetty-jndi
- jetty-jsp
- jetty-jspc-maven-plugin
- jetty-maven-plugin
- jetty-monitor
- jetty-parent
- jetty-plus
- jetty-project
- jetty-proxy
- jetty-rewrite

- jetty-runner
- jetty-security
- jetty-server
- jetty-servlet
- jetty-servlets
- jetty-start
- jetty-test-policy
- jetty-test-policy-javadoc
- jetty-toolchain
- jetty-util
- jetty-util-ajax
- jetty-version-maven-plugin
- jetty-version-maven-plugin-javadoc
- jetty-webapp
- jetty-websocket-api
- jetty-websocket-client
- jetty-websocket-common
- jetty-websocket-parent
- jetty-websocket-server
- jetty-websocket-servlet
- jetty-xml
- jing
- jing-javadoc
- jline-demo
- jna
- jna-contrib
- jna-javadoc
- joda-convert
- joda-convert-javadoc

- js
- js-devel
- jsch-demo
- json-glib-tests
- jsr-311
- jsr-311-javadoc
- juk
- junit
- junit-demo
- jvnet-parent
- k3b
- k3b-common
- k3b-devel
- k3b-libs
- kaccessible
- kaccessible-libs
- kactivities
- kactivities-devel
- kamera
- kate
- kate-devel
- kate-libs
- kate-part
- kcalc
- kcharselect
- kcm_colors
- kcm_touchpad
- kcm-gtk
- kcolorchooser

- kcoloredit
- kde-base-artwork
- kde-baseapps
- kde-baseapps-devel
- kde-baseapps-libs
- kde-filesystem
- kde-l10n
- kde-l10n-Arabic
- kde-l10n-Basque
- kde-l10n-Bosnian
- kde-l10n-British
- kde-l10n-Bulgarian
- kde-l10n-Catalan
- kde-l10n-Catalan-Valencian
- kde-l10n-Croatian
- kde-l10n-Czech
- kde-l10n-Danish
- kde-l10n-Dutch
- kde-l10n-Estonian
- kde-l10n-Farsi
- kde-l10n-Finnish
- kde-l10n-Galician
- kde-l10n-Greek
- kde-l10n-Hebrew
- kde-l10n-Hungarian
- kde-l10n-Icelandic
- kde-l10n-Interlingua
- kde-l10n-Irish
- kde-l10n-Kazakh

- kde-l10n-Khmer
- kde-l10n-Latvian
- kde-l10n-Lithuanian
- kde-l10n-LowSaxon
- kde-l10n-Norwegian
- kde-l10n-Norwegian-Nynorsk
- kde-l10n-Polish
- kde-l10n-Portuguese
- kde-l10n-Romanian
- kde-l10n-Serbian
- kde-l10n-Slovak
- kde-l10n-Slovenian
- kde-l10n-Swedish
- kde-l10n-Tajik
- kde-l10n-Thai
- kde-l10n-Turkish
- kde-l10n-Ukrainian
- kde-l10n-Uyghur
- kde-l10n-Vietnamese
- kde-l10n-Walloon
- kde-plasma-networkmanagement
- kde-plasma-networkmanagement-libreswan
- kde-plasma-networkmanagement-libs
- kde-plasma-networkmanagement-mobile
- kde-print-manager
- kde-runtime
- kde-runtime-devel
- kde-runtime-drkonqi
- kde-runtime-libs

- kde-settings
- kde-settings-ksplash
- kde-settings-minimal
- kde-settings-plasma
- kde-settings-pulseaudio
- kde-style-oxygen
- kde-style-phase
- kde-wallpapers
- kde-workspace
- kde-workspace-devel
- kde-workspace-ksplash-themes
- kde-workspace-libs
- kdeaccessibility
- kdeadmin
- kdeartwork
- kdeartwork-screensavers
- kdeartwork-sounds
- kdeartwork-wallpapers
- kdeclassic-cursor-theme
- kdegraphics
- kdegraphics-devel
- kdegraphics-libs
- kdegraphics-strigi-analyzer
- kdegraphics-thumbnailers
- kdelibs
- kdelibs-apidocs
- kdelibs-common
- kdelibs-devel
- kdelibs-ktexteditor

- kdemultimedia
- kdemultimedia-common
- kdemultimedia-devel
- kdemultimedia-libs
- kdenetwork
- kdenetwork-common
- kdenetwork-devel
- kdenetwork-fileshare-samba
- kdenetwork-kdnssd
- kdenetwork-kget
- kdenetwork-kget-libs
- kdenetwork-kopete
- kdenetwork-kopete-devel
- kdenetwork-kopete-libs
- kdenetwork-krdc
- kdenetwork-krdc-devel
- kdenetwork-krdc-libs
- kdenetwork-krfb
- kdenetwork-krfb-libs
- kdepim
- kdepim-devel
- kdepim-libs
- kdepim-runtime
- kdepim-runtime-libs
- kdepimlibs
- kdepimlibs-akonadi
- kdepimlibs-apidocs
- kdepimlibs-devel
- kdepimlibs-kxmlrpcclient

- kdeplasma-addons
- kdeplasma-addons-devel
- kdeplasma-addons-libs
- kdesdk
- kdesdk-cervisia
- kdesdk-common
- kdesdk-devel
- kdesdk-dolphin-plugins
- kdesdk-kapptemplate
- kdesdk-kapptemplate-template
- kdesdk-kcachegrind
- kdesdk-kioslave
- kdesdk-kmtrace
- kdesdk-kmtrace-devel
- kdesdk-kmtrace-libs
- kdesdk-kompare
- kdesdk-kompare-devel
- kdesdk-kompare-libs
- kdesdk-kpartloader
- kdesdk-kstartperf
- kdesdk-kuiviewer
- kdesdk-lokalize
- kdesdk-okteta
- kdesdk-okteta-devel
- kdesdk-okteta-libs
- kdesdk-poxml
- kdesdk-scripts
- kdesdk-strigi-analyzer
- kdesdk-thumbnailers

- kdesdk-umbrello
- kdeutils
- kdeutils-common
- kdeutils-minimal
- kdf
- kernel-rt-doc
- kernel-rt-trace
- kernel-rt-trace-devel
- kernel-rt-trace-kvm
- keytool-maven-plugin
- keytool-maven-plugin-javadoc
- kgamma
- kgpg
- kgreeter-plugins
- khotkeys
- khotkeys-libs
- kiconedit
- kinfocenter
- kio_sysinfo
- kmag
- kmenuedit
- kmix
- kmod-oracleasm
- kolourpaint
- kolourpaint-libs
- konkretcmpi
- konkretcmpi-devel
- konkretcmpi-python
- konsole

- konsole-part
- kross-interpreters
- kross-python
- kross-ruby
- kruler
- ksaneplugin
- kscreen
- ksnapshot
- ksshaskpass
- ksysguard
- ksysguard-libs
- ksysguardd
- ktimer
- kwallet
- kwin
- kwin-gles
- kwin-gles-libs
- kwin-libs
- kwrite
- kxml
- kxml-javadoc
- lapack64-devel
- lapack64-static
- lasso-devel
- latrace
- lcms2-utils
- ldns-doc
- ldns-python
- libabw-devel

- libabw-doc
- libabw-tools
- libappindicator
- libappindicator-devel
- libappindicator-docs
- libappstream-glib-builder
- libappstream-glib-builder-devel
- libart_lgpl
- libart_lgpl-devel
- libasan-static
- libavc1394-devel
- libbase-javadoc
- libblockdev-btrfs
- libblockdev-btrfs-devel
- libblockdev-crypto-devel
- libblockdev-devel
- libblockdev-dm-devel
- libblockdev-fs-devel
- libblockdev-kbd-devel
- libblockdev-loop-devel
- libblockdev-lvm-devel
- libblockdev-mdraid-devel
- libblockdev-mpath-devel
- libblockdev-nvdimm-devel
- libblockdev-part-devel
- libblockdev-swap-devel
- libblockdev-utils-devel
- libblockdev-vdo-devel
- libbluedevil

- libbluedevil-devel
- libbluray-devel
- libbonobo
- libbonobo-devel
- libbonoboui
- libbonoboui-devel
- libbytesize-devel
- libcacard-tools
- libcap-ng-python
- libcdr-devel
- libcdr-doc
- libcdr-tools
- libcgroup-devel
- libchamplain-demos
- libchewing
- libchewing-devel
- libchewing-python
- libcmis-devel
- libcmis-tools
- libcryptui
- libcryptui-devel
- libdb-devel-static
- libdb-java
- libdb-java-devel
- libdb-tcl
- libdb-tcl-devel
- libdbi
- libdbi-dbd-mysql
- libdbi-dbd-pgsql

- libdbi-dbd-sqlite
- libdbi-devel
- libdbi-drivers
- libdbusmenu-doc
- libdbusmenu-gtk2
- libdbusmenu-gtk2-devel
- libdbusmenu-gtk3-devel
- libdhash-devel
- libdmapsharing-devel
- libdmmp-devel
- libdmx-devel
- libdnet-progs
- libdnet-python
- libdnf-devel
- libdv-tools
- libdvdnav-devel
- libeasyfc-devel
- libeasyfc-gobject-devel
- libee
- libee-devel
- libee-utils
- libesmtp
- libesmtp-devel
- libestr-devel
- libetonyek-doc
- libetonyek-tools
- libevdev-utils
- libexif-doc
- libexttextcat-devel

- libexttextcat-tools
- libfastjson-devel
- libfdt
- libfonts-javadoc
- libformula-javadoc
- libfprint-devel
- libfreehand-devel
- libfreehand-doc
- libfreehand-tools
- libgcab1-devel
- libgccjit
- libgdither-devel
- libgee06
- libgee06-devel
- libgepub
- libgepub-devel
- libgfortran-static
- libgfortran4
- libgfortran5
- libgit2-devel
- libglade2
- libglade2-devel
- libGLEWmx
- libgnat
- libgnat-devel
- libgnat-static
- libgnome
- libgnome-devel
- libgnome-keyring-devel

- libgnomecanvas
- libgnomecanvas-devel
- libgnomeui
- libgnomeui-devel
- libgo
- libgo-devel
- libgo-static
- libgovirt-devel
- libgudev-devel
- libgxim
- libgxim-devel
- libgxps-tools
- libhangul-devel
- libhbaapi-devel
- libhif-devel
- libical-glib
- libical-glib-devel
- libical-glib-doc
- libid3tag
- libid3tag-devel
- libiec61883-utils
- libieee1284-python
- libimobiledevice-python
- libimobiledevice-utils
- libindicator
- libindicator-devel
- libindicator-gtk3-devel
- libindicator-tools
- libinvm-cim

- libinvm-cim-devel
- libinvm-cli
- libinvm-cli-devel
- libinvm-i18n
- libinvm-i18n-devel
- libiodbc
- libiodbc-devel
- libipa_hbac-devel
- libiptcdata-devel
- libiptcdata-python
- libitm-static
- libixpdimm-cim
- libixpdimm-core
- libjpeg-turbo-static
- libkcddb
- libkcddb-devel
- libkcompactdisc
- libkcompactdisc-devel
- libkdcraw
- libkdcraw-devel
- libkexiv2
- libkexiv2-devel
- libkipi
- libkipi-devel
- libkkc-devel
- libkkc-tools
- libksane
- libksane-devel
- libkscreen

- libkscreen-devel
- libkworkspace
- liblayout-javadoc
- libloader-javadoc
- liblognorm-devel
- liblouis-devel
- liblouis-doc
- liblouis-utils
- libmatchbox-devel
- libmbim-devel
- libmediaart-devel
- libmediaart-tests
- libmnl-static
- libmodman-devel
- libmodulemd-devel
- libmpc-devel
- libmsn
- libmsn-devel
- libmspub-devel
- libmspub-doc
- libmspub-tools
- libmtp-examples
- libmudflap
- libmudflap-devel
- libmudflap-static
- libmwaw-devel
- libmwaw-doc
- libmwaw-tools
- libmx

- libmx-devel
- libmx-docs
- libndp-devel
- libnetfilter_cthelper-devel
- libnetfilter_cttimeout-devel
- libnftnl-devel
- libnl
- libnl-devel
- libnm-gtk
- libnm-gtk-devel
- libntlm
- libntlm-devel
- libobjc
- libodfgen-doc
- libofa
- libofa-devel
- liboil
- liboil-devel
- libopenraw-pixbuf-loader
- liborcus-devel
- liborcus-doc
- liborcus-tools
- libosinfo-devel
- libosinfo-vala
- libotf-devel
- libpagemaker-devel
- libpagemaker-doc
- libpagemaker-tools
- libpinyin-devel

- libpinyin-tools
- libpipeline-devel
- libplist-python
- libpng-static
- libpng12-devel
- libproxy-kde
- libpst
- libpst-devel
- libpst-devel-doc
- libpst-doc
- libpst-python
- libpurple-perl
- libpurple-tcl
- libqmi-devel
- libquadmath-static
- LibRaw-static
- librelp-devel
- libreoffice
- libreoffice-bsh
- libreoffice-gdb-debug-support
- libreoffice-glade
- libreoffice-librelogo
- libreoffice-nlpsolver
- libreoffice-officebean
- libreoffice-officebean-common
- libreoffice-postgresql
- libreoffice-rhino
- libreofficekit-devel
- librepo-devel

- libreport-compat
- libreport-devel
- libreport-gtk-devel
- libreport-web-devel
- librepository-javadoc
- librevenge-doc
- librsvg2-tools
- libseccomp-devel
- libselinux-static
- libsemanage-devel
- libsemanage-static
- libserializer-javadoc
- libsexy
- libsexy-devel
- libsmbios-devel
- libsmi-devel
- libsndfile-utils
- libsolv-demo
- libsolv-devel
- libsolv-tools
- libspiro-devel
- libss-devel
- libssh2
- libsss_certmap-devel
- libsss_idmap-devel
- libsss_nss_idmap-devel
- libsss_simpleifp-devel
- libstaroffice-devel
- libstaroffice-doc

- libstaroffice-tools
- libstdc++-static
- libstoragemgmt-devel
- libstoragemgmt-targetd-plugin
- libtar-devel
- libteam-devel
- libtheora-devel-docs
- libtiff-static
- libtimezonemap-devel
- libtnc
- libtnc-devel
- libtranslit
- libtranslit-devel
- libtranslit-icu
- libtranslit-m17n
- libtsan-static
- libudisks2-devel
- libuninameslist-devel
- libunwind
- libunwind-devel
- libusal-devel
- libusb-static
- libusbmuxd-utils
- libuser-devel
- libvdpau-docs
- libverto-glib
- libverto-glib-devel
- libverto-libevent-devel
- libverto-tevent

- libverto-tevent-devel
- libvirt-cim
- libvirt-daemon-driver-lxc
- libvirt-daemon-lxc
- libvirt-gconfig-devel
- libvirt-glib-devel
- libvirt-gobject-devel
- libvirt-java
- libvirt-java-devel
- libvirt-java-javadoc
- libvirt-login-shell
- libvirt-snmp
- libvisio-doc
- libvisio-tools
- libvma-devel
- libvma-utils
- libvoikko-devel
- libvpx-utils
- libwebp-java
- libwebp-tools
- libwpd-tools
- libwpg-tools
- libwps-tools
- libwsman-devel
- libwvstreams
- libwvstreams-devel
- libwvstreams-static
- libxcb-doc
- libXevie

- libXevie-devel
- libXfont
- libXfont-devel
- libxml2-static
- libxslt-python
- libXvMC-devel
- libzapojit
- libzapojit-devel
- libzmf-devel
- libzmf-doc
- libzmf-tools
- lldpad-devel
- log4cxx
- log4cxx-devel
- log4j-manual
- lpsolve-devel
- lua-devel
- lua-static
- lvm2-cluster
- lvm2-python-libs
- lvm2-sysvinit
- lz4-static
- m17n-contrib
- m17n-contrib-extras
- m17n-db-devel
- m17n-db-extras
- m17n-lib-devel
- m17n-lib-tools
- m2crypto

- malaga-devel
- man-pages-cs
- man-pages-es
- man-pages-es-extra
- man-pages-fr
- man-pages-it
- man-pages-ja
- man-pages-ko
- man-pages-pl
- man-pages-ru
- man-pages-zh-CN
- mariadb-bench
- marisa-devel
- marisa-perl
- marisa-python
- marisa-ruby
- marisa-tools
- maven-changes-plugin
- maven-changes-plugin-javadoc
- maven-deploy-plugin
- maven-deploy-plugin-javadoc
- maven-doxia-module-fo
- maven-ear-plugin
- maven-ear-plugin-javadoc
- maven-ejb-plugin
- maven-ejb-plugin-javadoc
- maven-error-diagnostics
- maven-gpg-plugin
- maven-gpg-plugin-javadoc

- maven-istack-commons-plugin
- maven-jarsigner-plugin
- maven-jarsigner-plugin-javadoc
- maven-javadoc-plugin
- maven-javadoc-plugin-javadoc
- maven-jxr
- maven-jxr-javadoc
- maven-osgi
- maven-osgi-javadoc
- maven-plugin-jxr
- maven-project-info-reports-plugin
- maven-project-info-reports-plugin-javadoc
- maven-release
- maven-release-javadoc
- maven-release-manager
- maven-release-plugin
- maven-reporting-exec
- maven-repository-builder
- maven-repository-builder-javadoc
- maven-scm
- maven-scm-javadoc
- maven-scm-test
- maven-shared-jar
- maven-shared-jar-javadoc
- maven-site-plugin
- maven-site-plugin-javadoc
- maven-verifier-plugin
- maven-verifier-plugin-javadoc
- maven-wagon-provider-test

- maven-wagon-scm
- maven-war-plugin
- maven-war-plugin-javadoc
- mdds-devel
- meanwhile-devel
- meanwhile-doc
- memcached-devel
- memstomp
- mesa-demos
- mesa-libxatracker-devel
- mesa-private-llvm
- mesa-private-llvm-devel
- metacity-devel
- mgetty
- mgetty-sendfax
- mgetty-viewfax
- mgetty-voice
- migrationtools
- minizip
- minizip-devel
- mkbootdisk
- mobile-broadband-provider-info-devel
- mod_auth_kerb
- mod_auth_mellon-diagnostics
- mod_nss
- mod_revocator
- ModemManager-vala
- mono-icon-theme
- mozjs17

- mozjs17-devel
- mozjs24
- mozjs24-devel
- mpich-3.0-autoload
- mpich-3.0-doc
- mpich-3.2-autoload
- mpich-3.2-doc
- mpitests-compat-openmpi16
- msv-demo
- msv-msv
- msv-rngconv
- msv-xmlgen
- mvapich2-2.0-devel
- mvapich2-2.0-doc
- mvapich2-2.0-psm-devel
- mvapich2-2.2-devel
- mvapich2-2.2-doc
- mvapich2-2.2-psm-devel
- mvapich2-2.2-psm2-devel
- mvapich23-devel
- mvapich23-doc
- mvapich23-psm-devel
- mvapich23-psm2-devel
- nagios-plugins-bacula
- nasm
- nasm-doc
- nasm-rdoff
- ncurses-static
- nekohtml

- nekohtml-demo
- nekohtml-javadoc
- nepomuk-core
- nepomuk-core-devel
- nepomuk-core-libs
- nepomuk-widgets
- nepomuk-widgets-devel
- net-snmp-gui
- net-snmp-perl
- net-snmp-python
- net-snmp-sysvinit
- netsniff-ng
- NetworkManager-glib
- NetworkManager-glib-devel
- newt-static
- nfsometer
- nfstest
- nhn-nanum-brush-fonts
- nhn-nanum-fonts-common
- nhn-nanum-myeongjo-fonts
- nhn-nanum-pen-fonts
- nmap-frontend
- nss_compat_ossl
- nss_compat_ossl-devel
- nss-pem
- nss-pkcs11-devel
- ntp-doc
- ntp-perl
- nuvola-icon-theme

- nuxwdog
- nuxwdog-client-java
- nuxwdog-client-perl
- nuxwdog-devel
- objectweb-anttask
- objectweb-anttask-javadoc
- objectweb-asm
- ocaml-brlapi
- ocaml-calendar
- ocaml-calendar-devel
- ocaml-csv
- ocaml-csv-devel
- ocaml-curses
- ocaml-curses-devel
- ocaml-docs
- ocaml-emacs
- ocaml-fileutils
- ocaml-fileutils-devel
- ocaml-gettext
- ocaml-gettext-devel
- ocaml-libvirt
- ocaml-libvirt-devel
- ocaml-ocamlbuild-doc
- ocaml-source
- ocaml-x11
- ocaml-xml-light
- ocaml-xml-light-devel
- oci-register-machine
- okular

- okular-devel
- okular-libs
- okular-part
- opa-libopamgt-devel
- opal
- opal-devel
- open-vm-tools-devel
- open-vm-tools-test
- opencc-tools
- openchange-client
- openchange-devel
- openchange-devel-docs
- opencv-devel-docs
- opencv-python
- OpenEXR
- openhpi-devel
- openjade
- openjpeg-devel
- openjpeg-libs
- openldap-servers
- openldap-servers-sql
- openlmi
- openlmi-account
- openlmi-account-doc
- openlmi-fan
- openlmi-fan-doc
- openlmi-hardware
- openlmi-hardware-doc
- openlmi-indicationmanager-libs

- openlmi-indicationmanager-libs-devel
- openlmi-journald
- openlmi-journald-doc
- openlmi-logicalfile
- openlmi-logicalfile-doc
- openlmi-networking
- openlmi-networking-doc
- openlmi-pcp
- openlmi-powermanagement
- openlmi-powermanagement-doc
- openlmi-providers
- openlmi-providers-devel
- openlmi-python-base
- openlmi-python-providers
- openlmi-python-test
- openlmi-realmd
- openlmi-realmd-doc
- openlmi-service
- openlmi-service-doc
- openlmi-software
- openlmi-software-doc
- openlmi-storage
- openlmi-storage-doc
- openlmi-tools
- openlmi-tools-doc
- openobex
- openobex-apps
- openobex-devel
- openscap-containers

- openscap-engine-sce-devel
- openslp-devel
- openslp-server
- opensm-static
- opensp
- openssh-server-sysvinit
- openssl-static
- openssl098e
- openwsman-perl
- openwsman-ruby
- oprofile-devel
- oprofile-gui
- oprofile-jit
- optipng
- ORBit2
- ORBit2-devel
- orc-doc
- ortp
- ortp-devel
- oscilloscope
- oxygen-cursor-themes
- oxygen-gtk
- oxygen-gtk2
- oxygen-gtk3
- oxygen-icon-theme
- PackageKit-yum-plugin
- pakchois-devel
- pam_krb5
- pam_pkcs11

- pam_snapper
- pango-tests
- paps-devel
- passivetex
- pax
- pciutils-devel-static
- pcp-collector
- pcp-monitor
- pcre-tools
- pcre2-static
- pcre2-tools
- pentaho-libxml-javadoc
- pentaho-reporting-flow-engine-javadoc
- perl-AppConfig
- perl-Archive-Extract
- perl-B-Keywords
- perl-Browser-Open
- perl-Business-ISBN
- perl-Business-ISBN-Data
- perl-CGI-Session
- perl-Class-Load
- perl-Class-Load-XS
- perl-Class-Singleton
- perl-Config-Simple
- perl-Config-Tiny
- perl-Convert-ASN1
- perl-CPAN-Changes
- perl-CPANPLUS
- perl-CPANPLUS-Dist-Build

- perl-Crypt-CBC
- perl-Crypt-DES
- perl-Crypt-OpenSSL-Bignum
- perl-Crypt-OpenSSL-Random
- perl-Crypt-OpenSSL-RSA
- perl-Crypt-PasswdMD5
- perl-Crypt-SSLeay
- perl-CSS-Tiny
- perl-Data-Peek
- perl-DateTime
- perl-DateTime-Format-DateParse
- perl-DateTime-Locale
- perl-DateTime-TimeZone
- perl-DBD-Pg-tests
- perl-DBIx-Simple
- perl-Devel-Cover
- perl-Devel-Cycle
- perl-Devel-EnforceEncapsulation
- perl-Devel-Leak
- perl-Devel-Symdump
- perl-Digest-SHA1
- perl-Email-Address
- perl-FCGI
- perl-File-Find-Rule-Perl
- perl-File-Inplace
- perl-Font-AFM
- perl-Font-TTF
- perl-FreezeThaw
- perl-GD

- perl-GD-Barcode
- perl-Hook-LexWrap
- perl-HTML-Format
- perl-HTML-FormatText-WithLinks
- perl-HTML-FormatText-WithLinks-AndTables
- perl-HTML-Tree
- perl-HTTP-Daemon
- perl-Image-Base
- perl-Image-Info
- perl-Image-Xbm
- perl-Image-Xpm
- perl-Inline
- perl-Inline-Files
- perl-IO-CaptureOutput
- perl-IO-stringy
- perl-JSON-tests
- perl-LDAP
- perl-libxml-perl
- perl-List-MoreUtils
- perl-Locale-Maketext-Gettext
- perl-Locale-PO
- perl-Log-Message
- perl-Log-Message-Simple
- perl-Mail-DKIM
- perl-Mixin-Linewise
- perl-Module-Implementation
- perl-Module-Manifest
- perl-Module-Signature
- perl-Net-Daemon

- perl-Net-DNS-Nameserver
- perl-Net-DNS-Resolver-Programmable
- perl-Net-LibIDN
- perl-Net-Telnet
- perl-Newt
- perl-Object-Accessor
- perl-Object-Deadly
- perl-Package-Constants
- perl-Package-DeprecationManager
- perl-Package-Stash
- perl-Package-Stash-XS
- perl-PAR-Dist
- perl-Parallel-Iterator
- perl-Params-Validate
- perl-Parse-CPAN-Meta
- perl-Parse-RecDescent
- perl-Perl-Critic
- perl-Perl-Critic-More
- perl-Perl-MinimumVersion
- perl-Perl4-CoreLibs
- perl-PIRPC
- perl-Pod-Coverage
- perl-Pod-Coverage-TrustPod
- perl-Pod-Eventual
- perl-Pod-POM
- perl-Pod-Spell
- perl-PPI
- perl-PPI-HTML
- perl-PPIx-Regexp

- perl-PPIx-Utilities
- perl-Probe-Perl
- perl-Readonly-XS
- perl-SGMLSpm
- perl-Sort-Versions
- perl-String-Format
- perl-String-Similarity
- perl-Syntax-Highlight-Engine-Kate
- perl-Task-Weaken
- perl-Template-Toolkit
- perl-Term-UI
- perl-Test-ClassAPI
- perl-Test-CPAN-Meta
- perl-Test-DistManifest
- perl-Test-EOL
- perl-Test-HasVersion
- perl-Test-Inter
- perl-Test-Manifest
- perl-Test-Memory-Cycle
- perl-Test-MinimumVersion
- perl-Test-MockObject
- perl-Test-NoTabs
- perl-Test-Object
- perl-Test-Output
- perl-Test-Perl-Critic
- perl-Test-Perl-Critic-Policy
- perl-Test-Pod
- perl-Test-Pod-Coverage
- perl-Test-Portability-Files

- perl-Test-Script
- perl-Test-Spelling
- perl-Test-SubCalls
- perl-Test-Synopsis
- perl-Test-Tester
- perl-Test-Vars
- perl-Test-Without-Module
- perl-Text-CSV_XS
- perl-Text-Iconv
- perl-Tree-DAG_Node
- perl-Unicode-Map8
- perl-Unicode-String
- perl-UNIVERSAL-can
- perl-UNIVERSAL-isa
- perl-Version-Requirements
- perl-WWW-Curl
- perl-XML-Dumper
- perl-XML-Filter-BufferText
- perl-XML-Grove
- perl-XML-Handler-YAWriter
- perl-XML-LibXSLT
- perl-XML-SAX-Writer
- perl-XML-TreeBuilder
- perl-XML-Twig
- perl-XML-Writer
- perl-XML-XPathEngine
- perl-YAML-Tiny
- perltidy
- phonon

- phonon-backend-gstreamer
- phonon-devel
- php-pecl-memcache
- php-pspell
- pidgin-perl
- pinentry-qt
- pinentry-qt4
- pki-javadoc
- plasma-scriptengine-python
- plasma-scriptengine-ruby
- plexus-digest
- plexus-digest-javadoc
- plexus-mail-sender
- plexus-mail-sender-javadoc
- plexus-tools-pom
- plymouth-devel
- pm-utils
- pm-utils-devel
- pngcrush
- pngnq
- polkit-kde
- polkit-qt
- polkit-qt-devel
- polkit-qt-doc
- poppler-demos
- poppler-qt
- poppler-qt-devel
- popt-static
- postfix-sysvinit

- pothana2000-fonts
- powerpc-utils-python
- pprof
- pps-tools
- pptp-setup
- procps-ng-devel
- protobuf-emacs
- protobuf-emacs-el
- protobuf-java
- protobuf-javadoc
- protobuf-lite-devel
- protobuf-lite-static
- protobuf-python
- protobuf-static
- protobuf-vim
- psutils
- psutils-perl
- pth-devel
- ptlib
- ptlib-devel
- publican
- publican-common-db5-web
- publican-common-web
- publican-doc
- publican-redhat
- pulseaudio-esound-compat
- pulseaudio-module-gconf
- pulseaudio-module-zeroconf
- pulseaudio-qpaeq

- pygpgme
- pygtk2-libglade
- pykde4
- pykde4-akonadi
- pykde4-devel
- pyldb-devel
- pyliblzma
- PyOpenGL
- PyOpenGL-Tk
- pyOpenSSL-doc
- pyorbit
- pyorbit-devel
- PyPAM
- pyparsing-doc
- PyQt4
- PyQt4-devel
- pytalloc-devel
- python-appindicator
- python-beaker
- python-cffi-doc
- python-cherrypy
- python-criu
- python-debug
- python-deltarpm
- python-dtopt
- python-fpconst
- python-gpod
- python-gudev
- python-inotify-examples

- python-ipaddr
- python-IPy
- python-isodate
- python-isomd5sum
- python-kerberos
- python-kitchen
- python-kitchen-doc
- python-krbV
- python-libteam
- python-lxml-docs
- python-matplotlib
- python-matplotlib-doc
- python-matplotlib-qt4
- python-matplotlib-tk
- python-memcached
- python-mutagen
- python-paramiko
- python-paramiko-doc
- python-paste
- python-pillow-devel
- python-pillow-doc
- python-pillow-qt
- python-pillow-sane
- python-pillow-tk
- python-rados
- python-rbd
- python-reportlab-docs
- python-requests-kerberos
- python-rtslib-doc

- python-setproctitle
- python-slip-gtk
- python-smbc
- python-smbc-doc
- python-smbios
- python-sphinx-doc
- python-tempita
- python-tornado
- python-tornado-doc
- python-twisted-core
- python-twisted-core-doc
- python-twisted-web
- python-twisted-words
- python-urlgrabber
- python-volume_key
- python-webob
- python-webtest
- python-which
- python-zope-interface
- python2-caribou
- python2-futures
- python2-gexiv2
- python2-smartcols
- python2-solv
- python2-subprocess32
- qca-ossl
- qca2
- qca2-devel
- qdox

- qimageblitz
- qimageblitz-devel
- qimageblitz-examples
- qjson
- qjson-devel
- qpdf-devel
- qt
- qt-assistant
- qt-config
- qt-demos
- qt-devel
- qt-devel-private
- qt-doc
- qt-examples
- qt-mysql
- qt-odbc
- qt-postgresql
- qt-qdbusviewer
- qt-qvfb
- qt-settings
- qt-x11
- qt3
- qt3-config
- qt3-designer
- qt3-devel
- qt3-devel-docs
- qt3-MySQL
- qt3-ODBC
- qt3-PostgreSQL

- qt5-qt3d-doc
- qt5-qtbase-doc
- qt5-qtcanvas3d-doc
- qt5-qtconnectivity-doc
- qt5-qtdeclarative-doc
- qt5-qtenginio
- qt5-qtenginio-devel
- qt5-qtenginio-doc
- qt5-qtenginio-examples
- qt5-qtgraphicaleffects-doc
- qt5-qtimageformats-doc
- qt5-qtlocation-doc
- qt5-qtmultimedia-doc
- qt5-qtquickcontrols-doc
- qt5-qtquickcontrols2-doc
- qt5-qtscript-doc
- qt5-qtsensors-doc
- qt5-qtserialbus-devel
- qt5-qtserialbus-doc
- qt5-qtserialport-doc
- qt5-qtsvg-doc
- qt5-qttools-doc
- qt5-qtwayland-doc
- qt5-qtwebchannel-doc
- qt5-qtwebsockets-doc
- qt5-qtx11extras-doc
- qt5-qtxmlpatterns-doc
- quagga
- quagga-contrib

- quota-devel
- qv4l2
- rarian-devel
- rcs
- rdate
- rdist
- readline-static
- realmd-devel-docs
- Red_Hat_Enterprise_Linux-Release_Notes-7-as-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-bn-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-de-DE
- Red_Hat_Enterprise_Linux-Release_Notes-7-en-US
- Red_Hat_Enterprise_Linux-Release_Notes-7-es-ES
- Red_Hat_Enterprise_Linux-Release_Notes-7-fr-FR
- Red_Hat_Enterprise_Linux-Release_Notes-7-gu-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-hi-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-it-IT
- Red_Hat_Enterprise_Linux-Release_Notes-7-ja-JP
- Red_Hat_Enterprise_Linux-Release_Notes-7-kn-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-ko-KR
- Red_Hat_Enterprise_Linux-Release_Notes-7-ml-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-mr-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-or-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-pa-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-pt-BR
- Red_Hat_Enterprise_Linux-Release_Notes-7-ru-RU
- Red_Hat_Enterprise_Linux-Release_Notes-7-ta-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-te-IN
- Red_Hat_Enterprise_Linux-Release_Notes-7-zh-CN

- Red_Hat_Enterprise_Linux-Release_Notes-7-zh-TW
- redhat-access-plugin-ipa
- redhat-bookmarks
- redhat-lsb-supplemental
- redhat-lsb-trialuse
- redhat-upgrade-dracut
- redhat-upgrade-dracut-plymouth
- redhat-upgrade-tool
- redland-mysql
- redland-pgsql
- redland-virtuoso
- regexp
- relaxngcc
- rest-devel
- resteasy-base-jettison-provider
- resteasy-base-tjws
- rhdb-utils
- rhino
- rhino-demo
- rhino-javadoc
- rhino-manual
- rhythmbox-devel
- rngom
- rngom-javadoc
- rp-pppoe
- rrdtool-php
- rrdtool-python
- rsh
- rsh-server

- rsyslog-libdbi
- rsyslog-udpspoof
- rtcheck
- rtctl
- ruby-tcltk
- rubygem-net-http-persistent
- rubygem-net-http-persistent-doc
- rubygem-thor
- rubygem-thor-doc
- rusers
- rusers-server
- rwho
- sac-javadoc
- samba-dc
- samba-devel
- satyr-devel
- satyr-python
- saxon
- saxon-demo
- saxon-javadoc
- saxon-manual
- saxon-scripts
- sbc-devel
- sblim-cim-client2
- sblim-cim-client2-javadoc
- sblim-cim-client2-manual
- sblim-cmpi-base
- sblim-cmpi-base-devel
- sblim-cmpi-base-test

- sblim-cmpi-fsvol
- sblim-cmpi-fsvol-devel
- sblim-cmpi-fsvol-test
- sblim-cmpi-network
- sblim-cmpi-network-devel
- sblim-cmpi-network-test
- sblim-cmpi-nfsv3
- sblim-cmpi-nfsv3-test
- sblim-cmpi-nfsv4
- sblim-cmpi-nfsv4-test
- sblim-cmpi-params
- sblim-cmpi-params-test
- sblim-cmpi-sysfs
- sblim-cmpi-sysfs-test
- sblim-cmpi-syslog
- sblim-cmpi-syslog-test
- sblim-gather
- sblim-gather-devel
- sblim-gather-provider
- sblim-gather-test
- sblim-indication_helper
- sblim-indication_helper-devel
- sblim-smis-hba
- sblim-testsuite
- sblim-wbemcli
- scannotation
- scannotation-javadoc
- scpio
- screen

- SDL-static
- seahorse-nautilus
- seahorse-sharing
- sendmail-sysvinit
- setools-devel
- setools-gui
- setools-libs-tcl
- setuptool
- shared-desktop-ontologies
- shared-desktop-ontologies-devel
- shim-unsigned-ia32
- shim-unsigned-x64
- sisu
- sisu-parent
- slang-slsh
- slang-static
- smbios-utils
- smbios-utils-bin
- smbios-utils-python
- snakeyaml
- snakeyaml-javadoc
- snapper
- snapper-devel
- snapper-libs
- sntp
- SOAPpy
- soprano
- soprano-apidocs
- soprano-devel

- source-highlight-devel
- sox
- sox-devel
- speex-tools
- spice-xpi
- sqlite-tcl
- squid-migration-script
- squid-sysvinit
- sssd-libwbclient-devel
- sssd-polkit-rules
- stax2-api
- stax2-api-javadoc
- strigi
- strigi-devel
- strigi-libs
- strongimcv
- subversion-kde
- subversion-python
- subversion-ruby
- sudo-devel
- suitesparse-doc
- suitesparse-static
- supermin-helper
- svgpart
- svrcore
- svrcore-devel
- sweeper
- syslinux-devel
- syslinux-perl

- system-config-date
- system-config-date-docs
- system-config-firewall
- system-config-firewall-base
- system-config-firewall-tui
- system-config-keyboard
- system-config-keyboard-base
- system-config-language
- system-config-printer
- system-config-users-docs
- system-switch-java
- systemd-sysv
- t1lib
- t1lib-apps
- t1lib-devel
- t1lib-static
- t1utils
- taglib-doc
- talk
- talk-server
- tang-nagios
- targetd
- tcl-pgtcl
- tclx
- tclx-devel
- tcp_wrappers
- tcp_wrappers-devel
- tcp_wrappers-libs
- teamd-devel

- teckit-devel
- telepathy-farstream
- telepathy-farstream-devel
- telepathy-filesystem
- telepathy-gabble
- telepathy-glib
- telepathy-glib-devel
- telepathy-glib-vala
- telepathy-haze
- telepathy-logger
- telepathy-logger-devel
- telepathy-mission-control
- telepathy-mission-control-devel
- telepathy-salut
- tex-preview
- texinfo
- texlive-collection-documentation-base
- texlive-mh
- texlive-mh-doc
- texlive-misc
- texlive-thailatex
- texlive-thailatex-doc
- tix-doc
- tncfhh
- tncfhh-devel
- tncfhh-examples
- tncfhh-libs
- tncfhh-utils
- tog-pegasus-test

- tokyocabinet-devel-doc
- tomcat
- tomcat-admin-webapps
- tomcat-docs-webapp
- tomcat-el-2.2-api
- tomcat-javadoc
- tomcat-jsp-2.2-api
- tomcat-jsvc
- tomcat-lib
- tomcat-servlet-3.0-api
- tomcat-webapps
- totem-devel
- totem-pl-parser-devel
- tracker-devel
- tracker-docs
- tracker-needle
- tracker-preferences
- trang
- trousers-static
- txw2
- txw2-javadoc
- unique3
- unique3-devel
- unique3-docs
- uriparser
- uriparser-devel
- usbguard-devel
- usbredir-server
- ustr

- ustr-debug
- ustr-debug-static
- ustr-devel
- ustr-static
- uuid-c++
- uuid-c++-devel
- uuid-dce
- uuid-dce-devel
- uuid-perl
- uuid-php
- v4l-utils
- v4l-utils-devel-tools
- vala-doc
- valadoc
- valadoc-devel
- valgrind-openmpi
- velocity-demo
- velocity-javadoc
- velocity-manual
- vemana2000-fonts
- vigra
- vigra-devel
- virtuoso-opensource
- virtuoso-opensource-utils
- vlgothic-p-fonts
- vsftpd-sysvinit
- vte3
- vte3-devel
- wayland-doc

- webkitgtk3
- webkitgtk3-devel
- webkitgtk3-doc
- webkitgtk4-doc
- webrtc-audio-processing-devel
- weld-parent
- whois
- woodstox-core
- woodstox-core-javadoc
- wordnet
- wordnet-browser
- wordnet-devel
- wordnet-doc
- ws-commons-util
- ws-commons-util-javadoc
- ws-jaxme
- ws-jaxme-javadoc
- ws-jaxme-manual
- wsdl4j
- wsdl4j-javadoc
- wvdial
- x86info
- xchat-tcl
- xdg-desktop-portal-devel
- xerces-c
- xerces-c-devel
- xerces-c-doc
- xerces-j2-demo
- xerces-j2-javadoc

- xferstats
- xguest
- xhtml2fo-style-xsl
- xhtml2ps
- xisdnload
- xml-commons-apis-javadoc
- xml-commons-apis-manual
- xml-commons-apis12
- xml-commons-apis12-javadoc
- xml-commons-apis12-manual
- xml-commons-resolver-javadoc
- xmlgraphics-commons
- xmlgraphics-commons-javadoc
- xmlrpc-c-apps
- xmlrpc-client
- xmlrpc-common
- xmlrpc-javadoc
- xmlrpc-server
- xmlsec1-gcrypt-devel
- xmlsec1-nss-devel
- xmlto-tex
- xmlto-xhtml
- xmltoman
- xorg-x11-apps
- xorg-x11-drv-intel-devel
- xorg-x11-drv-keyboard
- xorg-x11-drv-mouse
- xorg-x11-drv-mouse-devel
- xorg-x11-drv-openchrome

- xorg-x11-drv-openchrome-devel
- xorg-x11-drv-synaptics
- xorg-x11-drv-synaptics-devel
- xorg-x11-drv-vmmouse
- xorg-x11-drv-void
- xorg-x11-server-source
- xorg-x11-xkb-extras
- xpp3
- xpp3-javadoc
- xpp3-minimal
- xsettings-kde
- xstream
- xstream-javadoc
- xulrunner
- xulrunner-devel
- xz-compat-libs
- yelp-xsl-devel
- yum-langpacks
- yum-NetworkManager-dispatcher
- yum-plugin-filter-data
- yum-plugin-fs-snapshot
- yum-plugin-keys
- yum-plugin-list-data
- yum-plugin-local
- yum-plugin-merge-conf
- yum-plugin-ovl
- yum-plugin-post-transaction-actions
- yum-plugin-pre-transaction-actions
- yum-plugin-protectbase

- yum-plugin-ps
- yum-plugin-rpm-warm-cache
- yum-plugin-show-leaves
- yum-plugin-upgrade-helper
- yum-plugin-verify
- yum-updateonboot

9.2. DEPRECATED DEVICE DRIVERS

The following device drivers continue to be supported until the end of life of Red Hat Enterprise Linux 7 but will likely not be supported in future major releases of this product and are not recommended for new deployments.

- 3w-9xxx
- 3w-sas
- aic79xx
- aoe
- arcmsr
- ata drivers:
  - acard-ahci
  - sata_mv
  - sata_nv
  - sata_promise
  - sata_qstor
  - sata_sil
  - sata_sil24
  - sata_sis
  - sata_svw
  - sata_sx4
  - sata_uli
  - sata_via
  - sata_vsc
- bfa

- cxgb3
- cxgb3i
- e1000
- floppy
- hptiop
- initio
- isci
- iw_cxgb3
- mptbase
- mptctl
- mptsas
- mptscsih
- mptspi
- mtip32xx
- mvsas
- mvumi
- OSD drivers:
  - osd
  - libosd
- osst
- pata drivers:
  - pata_acpi
  - pata_ali
  - pata_amd
  - pata_arasan_cf
  - pata_artop
  - pata_atiixp
  - pata_atp867x
  - pata_cmd64x

    - pata_cs5536
    - pata_hpt366
    - pata_hpt37x
    - pata_hpt3x2n
    - pata_hpt3x3
    - pata_it8213
    - pata_it821x
    - pata_jmicron
    - pata_marvell
    - pata_netcell
    - pata_ninja32
    - pata_oldpiix
    - pata_pdc2027x
    - pata_pdc202xx_old
    - pata_piccolo
    - pata_rdc
    - pata_sch
    - pata_serverworks
    - pata_sil680
    - pata_sis
    - pata_via
    - pdc_adma
- pm80xx(pm8001)
- pmcraid
- qla3xxx
- stex
- sx8
- tulip
- ufshcd

- wireless drivers:
  - carl9170
  - iwl4965
  - iwl3945
  - mwl8k
  - rt73usb
  - rt61pci
  - rtl8187
  - wil6210

9.3. DEPRECATED ADAPTERS

The following adapters continue to be supported until the end of life of Red Hat Enterprise Linux 7 but will likely not be supported in future major releases of this product and are not recommended for new deployments. Other adapters from the mentioned drivers that are not listed here remain unchanged.

PCI IDs are in the format of *vendor:device:subvendor:subdevice*. If the *subdevice* or *subvendor:subdevice* entry is not listed, devices with any values of such missing entries have been deprecated.

To check the PCI IDs of the hardware on your system, run the **lspci -nn** command.

- The following adapters from the **aacraid** driver have been deprecated:
  - PERC 2/Si (Iguana/PERC2Si), PCI ID 0x1028:0x0001:0x1028:0x0001
  - PERC 3/Di (Opal/PERC3Di), PCI ID 0x1028:0x0002:0x1028:0x0002
  - PERC 3/Si (SlimFast/PERC3Si), PCI ID 0x1028:0x0003:0x1028:0x0003
  - PERC 3/Di (Iguana FlipChip/PERC3DiF), PCI ID 0x1028:0x0004:0x1028:0x00d0
  - PERC 3/Di (Viper/PERC3DiV), PCI ID 0x1028:0x0002:0x1028:0x00d1
  - PERC 3/Di (Lexus/PERC3DiL), PCI ID 0x1028:0x0002:0x1028:0x00d9
  - PERC 3/Di (Jaguar/PERC3DiJ), PCI ID 0x1028:0x000a:0x1028:0x0106
  - PERC 3/Di (Dagger/PERC3DiD), PCI ID 0x1028:0x000a:0x1028:0x011b
  - PERC 3/Di (Boxster/PERC3DiB), PCI ID 0x1028:0x000a:0x1028:0x0121
  - catapult, PCI ID 0x9005:0x0283:0x9005:0x0283
  - tomcat, PCI ID 0x9005:0x0284:0x9005:0x0284
  - Adaptec 2120S (Crusader), PCI ID 0x9005:0x0285:0x9005:0x0286
  - Adaptec 2200S (Vulcan), PCI ID 0x9005:0x0285:0x9005:0x0285
  - Adaptec 2200S (Vulcan-2m), PCI ID 0x9005:0x0285:0x9005:0x0287

- Legend S220 (Legend Crusader), PCI ID 0x9005:0x0285:0x17aa:0x0286
- Legend S230 (Legend Vulcan), PCI ID 0x9005:0x0285:0x17aa:0x0287
- Adaptec 3230S (Harrier), PCI ID 0x9005:0x0285:0x9005:0x0288
- Adaptec 3240S (Tornado), PCI ID 0x9005:0x0285:0x9005:0x0289
- ASR-2020ZCR SCSI PCI-X ZCR (Skyhawk), PCI ID 0x9005:0x0285:0x9005:0x028a
- ASR-2025ZCR SCSI SO-DIMM PCI-X ZCR (Terminator), PCI ID 0x9005:0x0285:0x9005:0x028b
- ASR-2230S + ASR-2230SLP PCI-X (Lancer), PCI ID 0x9005:0x0286:0x9005:0x028c
- ASR-2130S (Lancer), PCI ID 0x9005:0x0286:0x9005:0x028d
- AAR-2820SA (Intruder), PCI ID 0x9005:0x0286:0x9005:0x029b
- AAR-2620SA (Intruder), PCI ID 0x9005:0x0286:0x9005:0x029c
- AAR-2420SA (Intruder), PCI ID 0x9005:0x0286:0x9005:0x029d
- ICP9024RO (Lancer), PCI ID 0x9005:0x0286:0x9005:0x029e
- ICP9014RO (Lancer), PCI ID 0x9005:0x0286:0x9005:0x029f
- ICP9047MA (Lancer), PCI ID 0x9005:0x0286:0x9005:0x02a0
- ICP9087MA (Lancer), PCI ID 0x9005:0x0286:0x9005:0x02a1
- ICP5445AU (Hurricane44), PCI ID 0x9005:0x0286:0x9005:0x02a3
- ICP9085LI (Marauder-X), PCI ID 0x9005:0x0285:0x9005:0x02a4
- ICP5085BR (Marauder-E), PCI ID 0x9005:0x0285:0x9005:0x02a5
- ICP9067MA (Intruder-6), PCI ID 0x9005:0x0286:0x9005:0x02a6
- Themisto Jupiter Platform, PCI ID 0x9005:0x0287:0x9005:0x0800
- Themisto Jupiter Platform, PCI ID 0x9005:0x0200:0x9005:0x0200
- Callisto Jupiter Platform, PCI ID 0x9005:0x0286:0x9005:0x0800
- ASR-2020SA SATA PCI-X ZCR (Skyhawk), PCI ID 0x9005:0x0285:0x9005:0x028e
- ASR-2025SA SATA SO-DIMM PCI-X ZCR (Terminator), PCI ID 0x9005:0x0285:0x9005:0x028f
- AAR-2410SA PCI SATA 4ch (Jaguar II), PCI ID 0x9005:0x0285:0x9005:0x0290
- CERC SATA RAID 2 PCI SATA 6ch (DellCorsair), PCI ID 0x9005:0x0285:0x9005:0x0291
- AAR-2810SA PCI SATA 8ch (Corsair-8), PCI ID 0x9005:0x0285:0x9005:0x0292
- AAR-21610SA PCI SATA 16ch (Corsair-16), PCI ID 0x9005:0x0285:0x9005:0x0293

- ESD SO-DIMM PCI-X SATA ZCR (Prowler), PCI ID 0x9005:0x0285:0x9005:0x0294
- AAR-2610SA PCI SATA 6ch, PCI ID 0x9005:0x0285:0x103C:0x3227
- ASR-2240S (SabreExpress), PCI ID 0x9005:0x0285:0x9005:0x0296
- ASR-4005, PCI ID 0x9005:0x0285:0x9005:0x0297
- IBM 8i (AvonPark), PCI ID 0x9005:0x0285:0x1014:0x02F2
- IBM 8i (AvonPark Lite), PCI ID 0x9005:0x0285:0x1014:0x0312
- IBM 8k/8k-l8 (Aurora), PCI ID 0x9005:0x0286:0x1014:0x9580
- IBM 8k/8k-l4 (Aurora Lite), PCI ID 0x9005:0x0286:0x1014:0x9540
- ASR-4000 (BlackBird), PCI ID 0x9005:0x0285:0x9005:0x0298
- ASR-4800SAS (Marauder-X), PCI ID 0x9005:0x0285:0x9005:0x0299
- ASR-4805SAS (Marauder-E), PCI ID 0x9005:0x0285:0x9005:0x029a
- ASR-3800 (Hurricane44), PCI ID 0x9005:0x0286:0x9005:0x02a2
- Perc 320/DC, PCI ID 0x9005:0x0285:0x1028:0x0287
- Adaptec 5400S (Mustang), PCI ID 0x1011:0x0046:0x9005:0x0365
- Adaptec 5400S (Mustang), PCI ID 0x1011:0x0046:0x9005:0x0364
- Dell PERC2/QC, PCI ID 0x1011:0x0046:0x9005:0x1364
- HP NetRAID-4M, PCI ID 0x1011:0x0046:0x103c:0x10c2
- Dell Catchall, PCI ID 0x9005:0x0285:0x1028
- Legend Catchall, PCI ID 0x9005:0x0285:0x17aa
- Adaptec Catch All, PCI ID 0x9005:0x0285
- Adaptec Rocket Catch All, PCI ID 0x9005:0x0286
- Adaptec NEMER/ARK Catch All, PCI ID 0x9005:0x0288

- The following adapters from the **mpt2sas** driver have been deprecated:
  - SAS2004, PCI ID 0x1000:0x0070
  - SAS2008, PCI ID 0x1000:0x0072
  - SAS2108_1, PCI ID 0x1000:0x0074
  - SAS2108_2, PCI ID 0x1000:0x0076
  - SAS2108_3, PCI ID 0x1000:0x0077
  - SAS2116_1, PCI ID 0x1000:0x0064

- SAS2116_2, PCI ID 0x1000:0x0065
- SSS6200, PCI ID 0x1000:0x007E

- The following adapters from the **megaraid_sas** driver have been deprecated:
  - Dell PERC5, PCI ID 0x1028:0x15
  - SAS1078R, PCI ID 0x1000:0x60
  - SAS1078DE, PCI ID 0x1000:0x7C
  - SAS1064R, PCI ID 0x1000:0x411
  - VERDE_ZCR, PCI ID 0x1000:0x413
  - SAS1078GEN2, PCI ID 0x1000:0x78
  - SAS0079GEN2, PCI ID 0x1000:0x79
  - SAS0073SKINNY, PCI ID 0x1000:0x73
  - SAS0071SKINNY, PCI ID 0x1000:0x71
- The following adapters from the **qla2xxx** driver have been deprecated:
  - ISP24xx, PCI ID 0x1077:0x2422
  - ISP24xx, PCI ID 0x1077:0x2432
  - ISP2422, PCI ID 0x1077:0x5422
  - QLE220, PCI ID 0x1077:0x5432
  - QLE81xx, PCI ID 0x1077:0x8001
  - QLE10000, PCI ID 0x1077:0xF000
  - QLE84xx, PCI ID 0x1077:0x8044
  - QLE8000, PCI ID 0x1077:0x8432
  - QLE82xx, PCI ID 0x1077:0x8021
- The following adapters from the **qla4xxx** driver have been deprecated:
  - QLOGIC_ISP8022, PCI ID 0x1077:0x8022
  - QLOGIC_ISP8324, PCI ID 0x1077:0x8032
  - QLOGIC_ISP8042, PCI ID 0x1077:0x8042
- The following adapters from the **be2iscsi** driver have been deprecated:
  - BladeEngine 2 (BE2) Devices
    - BladeEngine2 10Gb iSCSI Initiator (generic), PCI ID 0x19a2:0x212

        - OneConnect OCe10101, OCm10101, OCe10102, OCm10102 BE2 adapter family, PCI ID 0x19a2:0x702
        - OCe10100 BE2 adapter family, PCI ID 0x19a2:0x703
    - BladeEngine 3 (BE3) Devices
        - OneConnect TOMCAT iSCSI, PCI ID 0x19a2:0x0712
        - BladeEngine3 iSCSI, PCI ID 0x19a2:0x0222
- The following Ethernet adapters controlled by the **be2net** driver have been deprecated:
    - BladeEngine 2 (BE2) Devices
        - OneConnect TIGERSHARK NIC, PCI ID 0x19a2:0x0700
        - BladeEngine2 Network Adapter, PCI ID 0x19a2:0x0211
    - BladeEngine 3 (BE3) Devices
        - OneConnect TOMCAT NIC, PCI ID 0x19a2:0x0710
        - BladeEngine3 Network Adapter, PCI ID 0x19a2:0x0221
- The following adapters from the **lpfc** driver have been deprecated:
    - BladeEngine 2 (BE2) Devices
        - OneConnect TIGERSHARK FCoE, PCI ID 0x19a2:0x0704
    - BladeEngine 3 (BE3) Devices
        - OneConnect TOMCAT FCoE, PCI ID 0x19a2:0x0714
    - Fibre Channel (FC) Devices
        - FIREFLY, PCI ID 0x10df:0x1ae5
        - PROTEUS_VF, PCI ID 0x10df:0xe100
        - BALIUS, PCI ID 0x10df:0xe131
        - PROTEUS_PF, PCI ID 0x10df:0xe180
        - RFLY, PCI ID 0x10df:0xf095
        - PFLY, PCI ID 0x10df:0xf098
        - LP101, PCI ID 0x10df:0xf0a1
        - TFLY, PCI ID 0x10df:0xf0a5
        - BSMB, PCI ID 0x10df:0xf0d1
        - BMID, PCI ID 0x10df:0xf0d5
        - ZSMB, PCI ID 0x10df:0xf0e1
        - ZMID, PCI ID 0x10df:0xf0e5

        - NEPTUNE, PCI ID 0x10df:0xf0f5
        - NEPTUNE_SCSP, PCI ID 0x10df:0xf0f6
        - NEPTUNE_DCSP, PCI ID 0x10df:0xf0f7
        - FALCON, PCI ID 0x10df:0xf180
        - SUPERFLY, PCI ID 0x10df:0xf700
        - DRAGONFLY, PCI ID 0x10df:0xf800
        - CENTAUR, PCI ID 0x10df:0xf900
        - PEGASUS, PCI ID 0x10df:0xf980
        - THOR, PCI ID 0x10df:0xfa00
        - VIPER, PCI ID 0x10df:0xfb00
        - LP10000S, PCI ID 0x10df:0xfc00
        - LP11000S, PCI ID 0x10df:0xfc10
        - LPE11000S, PCI ID 0x10df:0xfc20
        - PROTEUS_S, PCI ID 0x10df:0xfc50
        - HELIOS, PCI ID 0x10df:0xfd00
        - HELIOS_SCSP, PCI ID 0x10df:0xfd11
        - HELIOS_DCSP, PCI ID 0x10df:0xfd12
        - ZEPHYR, PCI ID 0x10df:0xfe00
        - HORNET, PCI ID 0x10df:0xfe05
        - ZEPHYR_SCSP, PCI ID 0x10df:0xfe11
        - ZEPHYR_DCSP, PCI ID 0x10df:0xfe12
    - Lancer FCoE CNA Devices
        - OCe15104-FM, PCI ID 0x10df:0xe260
        - OCe15102-FM, PCI ID 0x10df:0xe260
        - OCm15108-F-P, PCI ID 0x10df:0xe260

9.4. OTHER DEPRECATED FUNCTIONALITY

Python 2 has been deprecated

In the next major release, RHEL 8, **Python 3.6** is the default Python implementation, and only limited support for **Python 2.7** is provided.

See the Conservative Python 3 Porting Guide for information on how to migrate large code bases to **Python 3**.

LVM libraries and LVM Python bindings have been deprecated

The **lvm2app** library and LVM Python bindings, which are provided by the **lvm2-python-libs** package, have been deprecated.

Red Hat recommends the following solutions instead:

- The LVM D-Bus API in combination with the **lvm2-dbusd** service. This requires using Python version 3.
- The LVM command-line utilities with JSON formatting. This formatting has been available since the **lvm2** package version 2.02.158.
- The **libblockdev** library for C and C++.

Mirrored mirror log has been deprecated in LVM

The mirrored mirror log feature of mirrored LVM volumes has been deprecated. A future major release of Red Hat Enterprise Linux will no longer support creating or activating LVM volumes with a mirrored mirror log.

The recommended replacements are:

- RAID1 LVM volumes. The main advantage of RAID1 volumes is their ability to work even in degraded mode and to recover after a transient failure. For information on converting mirrored volumes to RAID1, see the Converting a Mirrored LVM Device to a RAID1 Device section in the LVM Administration guide.
- Disk mirror log. To convert a mirrored mirror log to disk mirror log, use the following command: **lvconvert --mirrorlog disk *my_vg/my_lv***.

The clvmd daemon has been deprecated

The **clvmd** daemon for managing shared storage devices has been deprecated. A future major release of Red Hat Enterprise linux will instead use the **lvmlockd** daemon.

The lvmetad daemon has been deprecated

The **lvmetad** daemon for caching metadata has been deprecated. In a future major release of Red Hat Enterprise Linux, LVM will always read metadata from disk.

Previously, autoactivation of logical volumes was indirectly tied to the **use_lvmetad** setting in the **lvm.conf** configuration file. The correct way to disable autoactivation continues to be setting **auto_activation_volume_list=[]** (an empty list) in the **lvm.conf** file.

Deprecated packages related to Identity Management and security

The following packages have been deprecated and will not be included in a future major release of Red Hat Enterprise Linux:

Deprecated packages	Proposed replacement package or product
authconfig	authselect
pam_pkcs11	sssd [a]

Deprecated packages	Proposed replacement package or product
pam_krb5	**sssd** [b]
openldap-servers	Depending on the use case, migrate to Identity Management included in Red Hat Enterprise Linux; or to Red Hat Directory Server. [c]
mod_auth_kerb	**mod_auth_gssapi**
python-kerberos **python-krbV**	**python-gssapi**
python-requests-kerberos	**python-requests-gssapi**
hesiod	No replacement available.
mod_nss	**mod_ssl**
mod_revocator	No replacement available.

[a] System Security Services Daemon (SSSD) contains enhanced smart card functionality.

[b] For details on migrating from **pam_krb5** to **sssd**, see Migrating from pam_krb5 to sssd in the upstream SSSD documentation.

[c] Red Hat Directory Server requires a valid Directory Server subscription. For details, see also What is the support status of the LDAP-server shipped with Red Hat Enterprise Linux? in Red Hat Knowledgebase.

The Clevis HTTP pin has been deprecated

The **Clevis** HTTP pin has been deprecated and this feature will not be included in the next major version of Red Hat Enterprise Linux and will remain out of the distribution until a further notice.

crypto-utils has been deprecated

The **crypto-utils** packages have been deprecated, and they will not be available in a future major version of Red Hat Enterprise Linux. You can use tools provided by the **openssl**, **gnutls-utils**, and **nss-tools** packages instead.

All-numeric user and group names in shadow-utils have been deprecated

Creating user and group names consisting purely of numeric characters using the **useradd** and **groupadd** commands has been deprecated and will be removed from the system with the next major release. Such names can potentially confuse many tools that work with user and group names and user and group ids (which are numbers).

3DES is removed from the Python SSL default cipher list

The Triple Data Encryption Standard (**3DES**) algorithm has been removed from the **Python** SSL default cipher list. This enables **Python** applications using SSL to be PCI DSS-compliant.

sssd-secrets has been deprecated

The **sssd-secrets** component of the **System Security Services Daemon** (SSSD) has been deprecated

in Red Hat Enterprise Linux 7.6. This is because Custodia, a secrets service provider, available as a Technology Preview, is no longer actively developed. Use other Identity Management tools to store secrets, for example the Vaults.

Support for earlier IdM servers and for IdM replicas at domain level 0 will be limited

Red Hat does not plan to support using Identity Management (IdM) servers running Red Hat Enterprise Linux (RHEL) 7.3 and earlier with IdM clients of the next major release of RHEL. If you plan to introduce client systems running on the next major version of RHEL into a deployment that is currently managed by IdM servers running on RHEL 7.3 or earlier, be aware that you will need to upgrade the servers, moving them to RHEL 7.4 or later.

In the next major release of RHEL, only domain level 1 replicas will be supported. Before introducing IdM replicas running on the next major version of RHEL into an existing deployment, be aware that you will need to upgrade all IdM servers to RHEL 7.4 or later, and change the domain level to 1.

Consider planning the upgrade in advance if your deployment will be affected.

Bug-fix only support for the nss-pam-ldapd and NIS packages in the next major release of Red Hat Enterprise Linux

The **nss-pam-ldapd** packages and packages related to the **NIS server** will be released in the future major release of Red Hat Enterprise Linux but will receive a limited scope of support. Red Hat will accept bug reports but no new requests for enhancements. Customers are advised to migrate to the following replacement solutions:

Affected packages	Proposed replacement package or product
nss-pam-ldapd	**sssd**
ypserv **ypbind** **portmap** **yp-tools**	Identity Management in Red Hat Enterprise Linux

Use the Go Toolset instead of golang

The **golang** package, previously available in the Optional channel, will no longer receive updates in Red Hat Enterprise Linux 7. Developers are encouraged to use the **Go Toolset** instead, which is available through the Red Hat Developer program.

mesa-private-llvm will be replaced with llvm-private

The **mesa-private-llvm** package, which contains the LLVM-based runtime support for **Mesa**, will be replaced in a future minor release of Red Hat Enterprise Linux 7 with the **llvm-private** package.

libdbi and libdbi-drivers have been deprecated

The **libdbi** and **libdbi-drivers** packages will not be included in the next Red Hat Enterprise Linux (RHEL) major release.

Ansible deprecated in the Extras channel

Ansible and its dependencies will no longer be updated through the Extras channel. Instead, the Red Hat Ansible Engine product has been made available to Red Hat Enterprise Linux subscriptions and will provide access to the official Ansible Engine channel. Customers who have previously installed **Ansible**

and its dependencies from the Extras channel are advised to enable and update from the Ansible Engine channel, or uninstall the packages as future errata will not be provided from the Extras channel.

Ansible was previously provided in Extras (for AMD64 and Intel 64 architectures, and IBM POWER, little endian) as a runtime dependency of, and limited in support to, the Red Hat Enterprise Linux (RHEL) System Roles. Ansible Engine is available today for AMD64 and Intel 64 architectures, with IBM POWER, little endian availability coming soon.

Note that **Ansible** in the Extras channel was not a part of the Red Hat Enterprise Linux FIPS validation process.

The following packages have been deprecated from the Extras channel:

- **ansible(-doc)**
- **libtomcrypt**
- **libtommath(-devel)**
- **python2-crypto**
- **python2-jmespath**
- **python-httplib2**
- **python-paramiko(-doc)**
- **python-passlib**
- **sshpass**

For more information and guidance, see the Knowledgebase article at https://access.redhat.com/articles/3359651.

Note that Red Hat Enterprise Linux System Roles continue to be distributed though the Extras channel. Although Red Hat Enterprise Linux System Roles no longer depend on the **ansible** package, installing **ansible** from the Ansible Engine repository is still needed to run playbooks which use Red Hat Enterprise Linux System Roles.

signtool has been deprecated and moved to unsupported-tools

The **signtool** tool from the **nss** packages, which uses insecure signature algorithms, has been deprecated. The **signtool** executable has been moved to the **/usr/lib64/nss/unsupported-tools/** or **/usr/lib/nss/unsupported-tools/** directory, depending on the platform.

SSL 3.0 and RC4 are disabled by default in NSS

Support for the RC4 ciphers in the TLS protocols and the SSL 3.0 protocol is disabled by default in the NSS library. Applications that require RC4 ciphers or SSL 3.0 protocol for interoperability do not work in default system configuration.

It is possible to re-enable those algorithms by editing the **/etc/pki/nss-legacy/nss-rhel7.config** file. To re-enable RC4, remove the **:RC4** string from the **disallow=** list. To re-enable SSL 3.0 change the **TLS-VERSION-MIN=tls1.0** option to **ssl3.0**.

TLS compression support has been removed from nss

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

Public web CAs are no longer trusted for code signing by default

The Mozilla CA certificate trust list distributed with Red Hat Enterprise Linux 7.5 no longer trusts any public web CAs for code signing. As a consequence, any software that uses the related flags, such as **NSS** or **OpenSSL**, no longer trusts these CAs for code signing by default. The software continues to fully support code signing trust. Additionally, it is still possible to configure CA certificates as trusted for code signing using system configuration.

Sendmail has been deprecated

Sendmail has been deprecated in Red Hat Enterprise Linux 7. Customers are advised to use **Postfix**, which is configured as the default Mail Transfer Agent (MTA).

dmraid has been deprecated

Since Red Hat Enterprise Linux 7.5, the **dmraid** packages have been deprecated. It will stay available in Red Hat Enterprise Linux 7 releases but a future major release will no longer support legacy hybrid combined hardware and software RAID host bus adapter (HBA).

Automatic loading of DCCP modules through socket layer is now disabled by default

For security reasons, automatic loading of the **Datagram Congestion Control Protocol (DCCP)** kernel modules through socket layer is now disabled by default. This ensures that userspace applications can not maliciously load any modules. All **DCCP** related modules can still be loaded manually through the **modprobe** program.

The **/etc/modprobe.d/dccp-blacklist.conf** configuration file for blacklisting the **DCCP** modules is included in the kernel package. Entries included there can be cleared by editing or removing this file to restore the previous behavior.

Note that any re-installation of the same kernel package or of a different version does not override manual changes. If the file is manually edited or removed, these changes persist across package installations.

rsyslog-libdbi has been deprecated

The **rsyslog-libdbi** sub-package, which contains one of the less used **rsyslog** module, has been deprecated and will not be included in a future major release of Red Hat Enterprise Linux. Removing unused or rarely used modules helps users to conveniently find a database output to use.

The inputname option of the rsyslog imudp module has been deprecated

The **inputname** option of the **imudp** module for the **rsyslog** service has been deprecated. Use the **name** option instead.

SMBv1 is no longer installed with Microsoft Windows 10 and 2016 (updates 1709 and later)

Microsoft announced that the Server Message Block version 1 (SMBv1) protocol will no longer be installed with the latest versions of Microsoft Windows and Microsoft Windows Server. Microsoft also recommends users to disable SMBv1 on earlier versions of these products.

This update impacts Red Hat customers who operate their systems in a mixed Linux and Windows environment. Red Hat Enterprise Linux 7.1 and earlier support only the SMBv1 version of the protocol. Support for SMBv2 was introduced in Red Hat Enterprise Linux 7.2.

For details on how this change affects Red Hat customers, see SMBv1 no longer installed with latest Microsoft Windows 10 and 2016 update (version 1709) in Red Hat Knowledgebase.

The -ok option of the tc command has been deprecated

The **-ok** option of the **tc** command has been deprecated and this feature will not be included in the next major version of Red Hat Enterprise Linux.

FedFS has been deprecated

Federated File System (FedFS) has been deprecated because the upstream FedFS project is no longer being actively maintained. Red Hat recommends migrating FedFS installations to use **autofs**, which provides more flexible functionality.

Btrfs has been deprecated

The **Btrfs** file system has been in Technology Preview state since the initial release of Red Hat Enterprise Linux 6. Red Hat will not be moving **Btrfs** to a fully supported feature and it will be removed in a future major release of Red Hat Enterprise Linux.

The **Btrfs** file system did receive numerous updates from the upstream in Red Hat Enterprise Linux 7.4 and will remain available in the Red Hat Enterprise Linux 7 series. However, this is the last planned update to this feature.

tcp_wrappers deprecated

The **tcp_wrappers** package has been deprecated. **tcp_wrappers** provides a library and a small daemon program that can monitor and filter incoming requests for **audit**, **cyrus-imap**, **dovecot**, **nfs-utils**, **openssh**, **openldap**, **proftpd**, **sendmail**, **stunnel**, **syslog-ng**, **vsftpd**, and various other network services.

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 have been 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 was 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) was 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.

Several rsyslog options deprecated

The **rsyslog** utility version in Red Hat Enterprise Linux 7.4 has deprecated a large number of options. These options no longer have any effect and cause a warning to be displayed.

- The functionality previously provided by the options **-c**, **-u**, **-q**, **-x**, **-A**, **-Q**, **-4**, and **-6** can be achieved using the **rsyslog** configuration.
- There is no replacement for the functionality previously provided by the options **-l** and **-s**

Deprecated symbols from the memkind library

The following symbols from the **memkind** library have been deprecated:

- **memkind_finalize()**
- **memkind_get_num_kind()**
- **memkind_get_kind_by_partition()**
- **memkind_get_kind_by_name()**
- **memkind_partition_mmap()**
- **memkind_get_size()**
- **MEMKIND_ERROR_MEMALIGN**
- **MEMKIND_ERROR_MALLCTL**
- **MEMKIND_ERROR_GETCPU**

- **MEMKIND_ERROR_PMTT**
- **MEMKIND_ERROR_TIEDISTANCE**
- **MEMKIND_ERROR_ALIGNMENT**
- **MEMKIND_ERROR_MALLOCX**
- **MEMKIND_ERROR_REPNAME**
- **MEMKIND_ERROR_PTHREAD**
- **MEMKIND_ERROR_BADPOLICY**
- **MEMKIND_ERROR_REPPOLICY**

Options of Sockets API Extensions for SCTP (RFC 6458) deprecated

The options **SCTP_SNDRCV**, **SCTP_EXTRCV** and **SCTP_DEFAULT_SEND_PARAM** of Sockets API Extensions for the Stream Control Transmission Protocol have been deprecated per the RFC 6458 specification.

New options **SCTP_SNDINFO**, **SCTP_NXTINFO**, **SCTP_NXTINFO** and **SCTP_DEFAULT_SNDINFO** have been implemented as a replacement for the deprecated options.

Managing NetApp ONTAP using SSLv2 and SSLv3 is no longer supported by libstorageMgmt

The SSLv2 and SSLv3 connections to the NetApp ONTAP storage array are no longer supported by the **libstorageMgmt** library. Users can contact NetApp support to enable the Transport Layer Security (TLS) protocol.

dconf-dbus-1 has been deprecated and dconf-editor is now delivered separately

With this update, the **dconf-dbus-1** API has been removed. However, the **dconf-dbus-1** library has been backported to preserve binary compatibility. Red Hat recommends using the **GDBus** library instead of **dconf-dbus-1**.

The **dconf-error.h** file has been renamed to **dconf-enums.h**. In addition, the **dconf Editor** is now delivered in the separate **dconf-editor** package.

FreeRADIUS no longer accepts Auth-Type := System

The **FreeRADIUS** server no longer accepts the **Auth-Type := System** option for the **rlm_unix** authentication module. This option has been replaced by the use of the **unix** module in the **authorize** section of the configuration file.

The libcxgb3 library and the cxgb3 firmware package have been deprecated

The **libcxgb3** library provided by the **libibverbs** package and the **cxgb3** firmware package have been deprecated. They continue to be supported in Red Hat Enterprise Linux 7 but will likely not be supported in the next major releases of this product. This change corresponds with the deprecation of the **cxgb3**, **cxgb3i**, and **iw_cxgb3** drivers listed above.

SFN4XXX adapters have been deprecated

Starting with Red Hat Enterprise Linux 7.4, SFN4XXX Solarflare network adapters have been deprecated. Previously, Solarflare had a single driver **sfc** for all adapters. Recently, support of SFN4XXX was split from **sfc** and moved into a new SFN4XXX-only driver, called **sfc-falcon**. Both drivers continue to be supported at this time, but **sfc-falcon** and SFN4XXX support is scheduled for removal in a future major release.

Software-initiated-only FCoE storage technologies have been deprecated

The software-initiated-only type of the Fibre Channel over Ethernet (FCoE) storage technology has been deprecated due to limited customer adoption. The software-initiated-only storage technology will remain supported for the life of Red Hat Enterprise Linux 7. The deprecation notice indicates the intention to remove software-initiated-based FCoE support in a future major release of Red Hat Enterprise Linux.

It is important to note that the hardware support and the associated user-space tools (such as drivers, **libfc**, or **libfcoe**) are unaffected by this deprecation notice.

For details regarding changes to FCoE support in RHEL 8, see Considerations in adopting RHEL 8 .

Target mode in Software FCoE and Fibre Channel has been deprecated

- Software FCoE:
  The NIC Software FCoE target functionality has been deprecated and will remain supported for the life of Red Hat Enterprise Linux 7. The deprecation notice indicates the intention to remove the NIC Software FCoE target functionality support in a future major release of Red Hat Enterprise Linux. For more information regarding changes to FCoE support in RHEL 8, see Considerations in adopting RHEL 8 .

- Fibre Channel:
  Target mode in Fibre Channel has been deprecated and will remain supported for the life of Red Hat Enterprise Linux 7. Target mode will be disabled for the **tcm_fc** and **qla2xxx** drivers in a future major release of Red Hat Enterprise Linux.

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 .

The Perl and shell scripts for Directory Server have been deprecated

The Perl and shell scripts, which are provided by the **389-ds-base** package, have been deprecated. The scripts will be replaced by new utilities in the next major release of Red Hat Enterprise Linux.

The *Shell Scripts* and *Perl Scripts* sections in the *Red Hat Directory Server Command, Configuration, and File Reference* have been updated. The descriptions of affected scripts contain now a note that they are deprecated.

libguestfs can no longer inspect ISO installer files

The **libguestfs** library does no longer support inspecting ISO installer files, for example using the **guestfish** or **virt-inspector** utilities. Use the **osinfo-detect** command for inspecting ISO files instead. This command can be obtained from the **libosinfo** package.

Creating internal snapshots of virtual machines has been deprecated

Due to their lack of optimization and stability, internal virtual machine snapshots are now deprecated. In their stead, external snapshots are recommended for use. For more information, including instructions for creating external snapshots, see the Virtualization Deployment and Admnistration Guide.

IVSHMEM has been deprecated

The inter-VM shared memory device (IVSHMEM) feature has been deprecated. Therefore, in a future major release of RHEL, if a virtual machine (VM) is configured to share memory between multiple virtual machines in the form of a PCI device that exposes memory to guests, the VM will fail to boot.

The gnome-shell-browser-plugin subpackage has been deprecated

Since the Firefox Extended Support Release (ESR 60), Firefox no longer supports the Netscape Plugin Application Programming Interface (NPAPI) that was used by the **gnome-shell-browser-plugin** subpackage. The subpackage, which provided the functionality to install GNOME Shell Extensions, has thus been deprecated. The installation of GNOME Shell Extensions is now handled directly in the **gnome-software** package.

The VDO read cache has been deprecated

The read cache functionality in Virtual Data Optimizer (VDO) has been deprecated. The read cache is disabled by default on new VDO volumes.

In the next major Red Hat Enterprise Linux release, the read cache functionality will be removed, and you will no longer be able to enable it using the **--readCache** option of the **vdo** utility.

cpuid has been deprecated

The **cpuid** command has been deprecated. A future major release of Red Hat Enterprise Linux will no longer support using **cpuid** to dump the information about CPUID instruction for each CPU. To obtain similar information, use the **lscpu** command instead.

KDE has been deprecated

KDE Plasma Workspaces (KDE), which has been provided as an alternative to the default GNOME desktop environment has been deprecated. A future major release of Red Hat Enterprise Linux will no longer support using KDE instead of the default GNOME desktop environment.

Using virt-install with NFS locations is deprecated

With a future major version of Red Hat Enterprise Linux, the **virt-install** utility will not be able to mount NFS locations. As a consequence, attempting to install a virtual machine using **virt-install** with a NFS address as a value of the **--location** option will fail. To work around this change, mount your NFS share prior to using **virt-install**, or use a HTTP location.

The lwresd daemon has been deprecated

The **lwresd** daemon, which is a part of the **bind** package, has been deprecated. A future major release of Red Hat Enterprise Linux will no longer support providing name lookup services to clients that use the BIND 9 lightweight resolver library with **lwresd**.

The recommended replacements are:

- The **systemd-resolved** daemon and **nss-resolve** API, provided by the **systemd** package
- The **unbound** library API and daemon, provided by the **unbound** and **unbound-libs** packages
- The **getaddrinfo** and related **glibc** library calls

The /etc/sysconfig/nfs file and legacy NFS service names have been deprecated

A future major Red Hat Enterprise Linux release will move the NFS configuration from the **/etc/sysconfig/nfs** file to **/etc/nfs.conf**.

Red Hat Enterprise Linux 7 currently supports both of these files. Red Hat recommends that you use the new **/etc/nfs.conf** file to make NFS configuration in all versions of Red Hat Enterprise Linux compatible with automated configuration systems.

Additionally, the following NFS service aliases will be removed and replaced by their upstream names:

- **nfs.service**, replaced by **nfs-server.service**
- **nfs-secure.service**, replaced by **rpc-gssd.service**
- **rpcgssd.service**, replaced by **rpc-gssd.service**
- **nfs-idmap.service**, replaced by **nfs-idmapd.service**
- **rpcidmapd.service**, replaced by **nfs-idmapd.service**
- **nfs-lock.service**, replaced by **rpc-statd.service**
- **nfslock.service**, replaced by **rpc-statd.service**

The JSON export functionality has been removed from the nft utility

Previously, the **nft** utility provided an export feature, but the exported content could contain internal ruleset representation details, which was likely to change without further notice. For this reason, the deprecated export functionality has been removed from **nft** starting with RHEL 7.7. Future versions of **nft**, such as provided by RHEL 8, contain a high-level JSON API. However, this API not available in RHEL 7.7.

The openvswitch-2.0.0-7 package in the RHEL 7 Optional channel has been deprecated

RHEL 7.5 introduced the **openvswitch-2.0.0-7.el7** package in the RHEL 7 Optional channel as a dependency of the **NetworkManager-ovs** package. This dependency no longer exists and, as a result, **openvswitch-2.0.0-7.el7** is now deprecated.

Note that Red Hat does not support packages in the RHEL 7 Optional channel and that **openvswitch-2.0.0-7.el7** will not be updated in the future. For this reason, do not use this package in production environments.

Deprecated PHP extensions

The following PHP extensions have been deprecated:

- aspell
- mysql
- memcache

Deprecated Apache HTTP Server modules

The following modules of the Apache HTTP Server have been deprecated:

- mod_file_cache
- mod_nss
- mod_perl

Apache Tomcat has been deprecated

The Apache Tomcat server, a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies, has been deprecated. Red Hat recommends that users requiring a servlet container use the JBoss Web Server.

The DES algorithm is deprecated in IdM

Due to security reasons, the Data Encryption Standard (DES) algorithm is deprecated in Identity Management (IdM). The MIT Kerberos libraries provided by the **krb5-libs** package do not support using the Data Encryption Standard (DES) in new deployments. Use DES only for compatibility reasons if your environment does not support any newer algorithm.

Red Hat also recommends to avoid using RC4 ciphers over Kerberos. While DES is deprecated, the Server Message Block (SMB) protocol still uses RC4. However, the SMB protocol can also use the secure AES algorithms.

For further details, see:

- MIT Kerberos Documentation - Retiring DES
- RFC6649: Deprecate DES, RC4-HMAC-EXP, and Other Weak Cryptographic Algorithms in Kerberos

real(kind=16) type support has been removed from libquadmath library

real(kind=16) type support has been removed from the **libquadmath** library in the **compat-libgfortran-41** package in order to preserve ABI compatibility.

Deprecated glibc features

The following features of the GNU C library provided by the **glibc** packages have been deprecated:

- the **librtkaio** library
- Sun RPC and NIS interfaces

Deprecated features of the GDB debugger

The following features and capabilities of the GDB debugger have been deprecated:

- debugging Java programs built with the **gcj** compiler
- HP-UX XDB compatibility mode and the **-xdb** option
- Sun version of the **stabs** format

Development headers and static libraries from valgrind-devel have been deprecated

The **valgrind-devel** sub-package includes development files for developing custom Valgrind tools. These files do not have a guaranteed API, have to be linked statically, are unsupported, and thus have been deprecated. Red Hat recommends to use the other development files and header files for valgrind-aware programs from the **valgrind-devel** package such as **valgrind.h**, **callgrind.h**, **drd.h**, **helgrind.h**, and **memcheck.h**, which are stable and well supported.

The nosegneg libraries for 32-bit Xen have been deprecated

The **glibc** i686 packages contain an alternative **glibc** build, which avoids the use of the thread descriptor segment register with negative offsets (**nosegneg**). This alternative build is only used in the 32-bit version of the Xen Project hypervisor without hardware virtualization support, as an optimization to reduce the cost of full paravirtualization. This alternative build is deprecated.

Ada, Go, and Objective C/C++ build capability in GCC has been deprecated

Capability for building code in the Ada (GNAT), GCC Go, and Objective C/C++ languages using the GCC compiler has been deprecated.

To build Go code, use the Go Toolset instead.

Deprecated Kickstart commands and options

The following Kickstart commands and options have been deprecated:

- **upgrade**
- **btrfs**
- **part btrfs** and **partition btrfs**
- **part --fstype btrfs** and **partition --fstype btrfs**
- **logvol --fstype btrfs**
- **raid --fstype btrfs**
- **unsupported_hardware**

Where only specific options and values are listed, the base command and its other options are not deprecated.

The env option in virt-who has become deprecated

With this update, the **virt-who** utility no longer uses the **env** option for hypervisor detection. As a consequence, Red Hat discourages the use of **env** in your **virt-who** configurations, as the option will not have the intended effect.

AGP graphics card have been deprecatd

Graphics cards using the Accelerated Graphics Port (AGP) bus have been deprecated and are not supported in RHEL 8. AGP graphics cards are rarely used in 64-bit machines and the bus has been replaced by PCI-Express.

APPENDIX A. COMPONENT VERSIONS

This appendix provides a list of key components and their versions in the Red Hat Enterprise Linux 7.7 release.

Table A.1. Component Versions

Component	Version
kernel	3.10.0-1062
kernel-alt	4.14.0-115
QLogic **qla2xxx** driver	10.00.00.12.07.7-k
QLogic **qla4xxx** driver	5.04.00.00.07.02-k0
Emulex **lpfc** driver	0:12.0.0.10
iSCSI initiator utils (**iscsi-initiator-utils**)	6.2.0.874-11
DM-Multipath (**device-mapper-multipath**)	0.4.9-127
LVM (**lvm2**)	2.02.185-2
qemu-kvm[a]	1.5.3-167
qemu-kvm-ma[b]	2.12.0-18

[a] The **qemu-kvm** packages provide KVM virtualization on AMD64 and Intel 64 systems.

[b] The **qemu-kvm-ma** packages provide KVM virtualization on IBM POWER8, IBM POWER9, and IBM Z. Note that KVM virtualization on IBM POWER9 and IBM Z also requires using the **kernel-alt** packages.

APPENDIX B. LIST OF TICKETS BY COMPONENT

Component	Tickets
389-ds-base	BZ#1645359, BZ#1438144, BZ#1561769, BZ#1417340, BZ#1629055, BZ#1466441, BZ#1563999, BZ#1716267, BZ#1652984, BZ#1597202, BZ#1665752, BZ#1710848, BZ#1602001, BZ#1663829, BZ#1589144
NetworkManager	BZ#1652910, BZ#1652653
anaconda	BZ#1678353, BZ#1620109, BZ#1489713, BZ#1637112, BZ#1614049
ansible	BZ#1439896
bind	BZ#1325789, BZ#1640561
binutils	BZ#1644632
chrony	BZ#1636117, BZ#1600882
compat-sap-c++-8	BZ#1669683
corosync	BZ#1374857, BZ#1413573
criu	BZ#1400230
cups-filters	BZ#1485502
cups	BZ#1570480
custodia	BZ#1403214
dbus	BZ#1568856
desktop	BZ#1579257, BZ#1608704, BZ#1481411
dhcp	BZ#1193799
dnf	BZ#1461652
dnsmasq	BZ#1614331, BZ#1638703
dyninst	BZ#1498558
elfutils	BZ#1676504
enscript	BZ#1573876

Component	Tickets
fence-agents	BZ#1476401
filesystems	BZ#1274459, BZ#1111712, BZ#1206277, BZ#1477977, BZ#1710421
firewalld	BZ#1637204
gcc-libraries	BZ#1551629
gdb	BZ#1639077
geolite2	BZ#1643472
ghostscript	BZ#1636115
glibc	BZ#1555189, BZ#1039304, BZ#1427734, BZ#1591268, BZ#1472832
gnome-documents	BZ#1695699
gnome-shell	BZ#1481395
gnome-software	BZ#1591270
gnome-tweak-tool	BZ#1474852
grub2	BZ#1630678
hardware-enablement	BZ#1062759, BZ#1384452, BZ#1519746, BZ#1660791, BZ#1454916, BZ#1454918
identity-management	BZ#1664447, BZ#1740779, BZ#1405325
image-builder	BZ#1713880
ipa	BZ#1690037, BZ#1390757, BZ#1586268, BZ#1690191, BZ#1518939, BZ#1115294, BZ#1298286, BZ#1631826
ipset	BZ#1646666, BZ#1649080, BZ#1649877, BZ#1650297
kernel-rt	BZ#1642619, BZ#1593361

Component	Tickets
kernel	BZ#1728504, BZ#1636601, BZ#1653428, BZ#1511372, BZ#1680426, BZ#1694778, BZ#1739072, BZ#1077929, BZ#1698453, BZ#1528466, BZ#1632575, BZ#1429792, BZ#1607252, BZ#1559615, BZ#1230959, BZ#1460849, BZ#1464377, BZ#1457533, BZ#1503123, BZ#1589397, BZ#1726642, BZ#1315400, BZ#1622413, BZ#1691868, BZ#1666535, BZ#1549355, BZ#1509444, BZ#1724027, BZ#1710533, BZ#1701502, BZ#1724993
kexec-tools	BZ#1600148, BZ#1723492
krb5	BZ#1605756, BZ#1645711
ksh	BZ#1503922
libdb	BZ#1608749
libguestfs	BZ#1463620, BZ#1441197, BZ#1387213, BZ#1477912, BZ#1509931, BZ#1481930
libreswan	BZ#1375750, BZ#1544463
libssh2	BZ#1592784
libvirt	BZ#1475770
linuxptp	BZ#1650672, BZ#1623919
lorax	BZ#1659129
lvm2	BZ#1674563, BZ#1643651, BZ#1642162
make	BZ#1582545
mariadb	BZ#1731062
mutter	BZ#1583825
mysql-connector-java	BZ#1646363
ndctl	BZ#1635441
networking	BZ#916384, BZ#916382, BZ#755087, BZ#1259547, BZ#1393375, BZ#1062656, BZ#1574536, BZ#1489758, BZ#1708807
nss	BZ#1431241, BZ#1552854, BZ#1212132, BZ#1510156, BZ#1431210, BZ#1425514, BZ#1432142, BZ#1711438, BZ#1710372

Component	Tickets
opensc	BZ#1612372
openscap	BZ#1694962
openssh	BZ#1600869, BZ#1583735
ovmf	BZ#653382
pacemaker	BZ#1461964
passwd	BZ#1276570
pcp	BZ#1647308, BZ#1600262
pcs	BZ#1433016
perl-DateTime-TimeZone	BZ#1537984
php	BZ#1646158
pki-core	BZ#1633422, BZ#1491453, BZ#1372056, BZ#1616134, BZ#1644769, BZ#1554055, BZ#1638379, BZ#1578389, BZ#1617894, BZ#1628410, BZ#1633761, BZ#1479559, BZ#1639710
policycoreutils	BZ#1647714
python3	BZ#1597718
qemu-kvm-rhev	BZ#1615682
quota	BZ#1601109, BZ#1697605
rear	BZ#1652828, BZ#1685166
resource-agents	BZ#1513957
rpm	BZ#1663264, BZ#1550745
samba	BZ#1649434
scap-security-guide	BZ#1695213, BZ#1684545, BZ#1630739, BZ#1647189, BZ#1631378
security	BZ#1335986

Component	Tickets
selinux-policy	BZ#1650909, BZ#1589086, BZ#1626115, BZ#1487350, BZ#1619306, BZ#1564470
shadow-utils	BZ#1498628
sssd	BZ#1194345, BZ#1068725
storage	BZ#1649493, BZ#1387768, BZ#1109348, BZ#1119909, BZ#1414957, BZ#1712664, BZ#1722855
sudo	BZ#1618702
system-management	BZ#1712833
systemd	BZ#1284974
systemtap	BZ#1669605
tools	BZ#1569484, BZ#1714480
trace-cmd	BZ#1655111
tuned	BZ#1643654, BZ#1649408, BZ#1622239, BZ#1714595, BZ#1719160
usbguard	BZ#1480100
valgrind	BZ#1519410
vim	BZ#1563419
virtualization	BZ#1103193, BZ#1348508, BZ#1299662, BZ#1708465, BZ#1661654, BZ#1667478, BZ#1706522
xorg-x11-drv-qxl	BZ#1640918
xorriso	BZ#1638857
ypserv	BZ#1624295

APPENDIX C. REVISION HISTORY

0.1-3

Wed Sep 2 2020, Jaroslav Klech (jklech@redhat.com)

- Added a kernel enhancement that IBPB cannot be directly disabled.

0.1-2

Tue Apr 28 2020, Lenka Špačková (lspackova@redhat.com)

- Updated information about in-place upgrades.

0.1-1

Thu Mar 19 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue related to installation.

0.1-0

Thu Mar 12 2020, Lenka Špačková (lspackova@redhat.com)

- Added information about the **storage** RHEL System Role.

0.0-9

Wed Feb 12 2020, Jaroslav Klech (jklech@redhat.com)

- Provided a complete kernel version to Architectures and New Features chapters.

0.0-8

Mon Feb 03 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue about an error message when upgrading from the RHEL 7.6 version of **PCP**.

0.0-7

Tue Nov 05 2019, Lenka Špačková (lspackova@redhat.com)

- Updated Overview with the new supported in-place upgrade path from RHEL 7.6 to RHEL 8.1.
- Updated deprecated functionality.

0.0-6

Fri Oct 25 2019, Lenka Špačková (lspackova@redhat.com)

- Added a note that RHEL System Roles for SAP are now available as a Technology Preview.

0.0-5

Mon Oct 7 2019, Jiří Herrman (jherrman@redhat.com)

- Clarified a Technology Preview note related to OVMF.

0.0-4

Wed Aug 21 2019, Lenka Špačková (lspackova@redhat.com)

- Added instructions on how to enable the Extras channel to the **YUM 4** Technology Preview note (System and Subscription Management).

0.0-3

Tue Aug 20 2019, Lenka Špačková (lspackova@redhat.com)

- Added a known issue related to **kdump** (Kernel).
- Updated text of a Technology Preview description (Virtualization).

0.0-2

Thu Aug 15 2019, Lenka Špačková (lspackova@redhat.com)

- Added a Technology Preview related to Azure M416v2 as a host (Virtualization).
- Added a link to Intel® Omni-Path Architecture documentation (Kernel).
- Added an SSSD-related feature: a new default value for the **fallback_homedir** parameter (Authentication and Interoperability).
- Added a known issue related to the **bnx2x** driver (Kernel).
- Added two desktop-related bug fixes.

0.0-1

Tue Aug 06 2019, Lenka Špačková (lspackova@redhat.com)

- Release of the Red Hat Enterprise Linux 7.7 Release Notes.

0.0-0

Wed Jun 05 2019, Lenka Špačková (lspackova@redhat.com)

- Release of the Red Hat Enterprise Linux 7.7 Beta Release Notes.