Red Hat Enterprise Linux 7

7.9 Release Notes

Release Notes for Red Hat Enterprise Linux 7.9

Last Updated: 2024-04-04

Red Hat Enterprise Linux 7 7.9 Release Notes

Release Notes for Red Hat Enterprise Linux 7.9

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 7.9 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 7.9 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

Product life cycle

Red Hat Enterprise Linux 7.9 is the last minor release of RHEL 7.

Red Hat Enterprise Linux 7 entered the Maintenance Support 2 phase of the product life cycle on August 6, 2020. See the Red Hat Enterprise Linux Life Cycle document for more information.

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 **Preupgrade Assistant** and **Red Hat Upgrade Tool** have been updated with the release of RHEL 7.9:

- The supported in-place upgrade path is from RHEL 6.10 to RHEL 7.9, with the exception of SAP HANA.
- In-place upgrade of UEFI-based RHEL installations is now supported
- The rollback functionality is available also for UEFI
- You can use custom repositories for an in-place upgrade

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 Upgrading from RHEL 6 to RHEL 7 guide. Significant differences between the two major releases are documented in the 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 Linux 6 or Oracle Linux 6, you can convert your operating system to RHEL 6 using the unsupported **Convert2RHEL** utility prior to upgrading to RHEL 7. For instructions, see How to convert from CentOS Linux 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 Linux 7 or Oracle Linux 7, you can convert your operating system to RHEL 7 using the Red Hat-supported **Convert2RHEL** utility prior to upgrading to RHEL 8. For instructions, see Converting from an RPM-based Linux distribution to RHEL . For information regarding how Red Hat supports conversions from other Linux distributions to RHEL, see the Convert2RHEL Support Policy document.

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 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.

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

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]
- 64-bit IBM Z [4][6]
- 64-bit ARM [4]

The Red Hat Enterprise Linux 7.9 is distributed with the kernel version 3.10.0-1160, 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)
- 64-bit IBM Z (kernel version 3.10)

NOTE

The IBM POWER9 (little endian) and 64-bit IBM Z - Structure A architectures was retired on May 31, 2021. The 64-bit ARM architecture was retired on August 6, 2020, as per the RHEL Life Cycle.

[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. NEW FEATURES

This chapter documents new features and major enhancements introduced in Red Hat Enterprise Linux 7.9.

3.1. AUTHENTICATION AND INTEROPERABILITY

The Certificate Profiles extension no longer has a maximum number of policies per certificate

Previously, administrators could not add more than 20 policies to a certificate because of a hardcoded limit within the Certificate Profiles extension. This update removes the restriction, so you can add an unlimited number of policies to a certificate. In addition, the extension requires at least one policy, otherwise the **pkiconsole** interface shows an error. If you modify the profile, the extension creates one empty policy. For example:

```
Identifier: Certificate Policies: - 2.5.29.32
        Critical: no
        Certificate Policies:
```

(BZ#1768718)

SSSD rebased to version 1.16.5

The *sssd* packages have been upgraded to upstream version 1.16.5, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1796352)

3.2. CLUSTERING

pacemaker rebased to version 1.1.23

The Pacemaker cluster resource manager has been upgraded to upstream version 1.1.23, which provides a number of bug fixes.

(BZ#1792492)

3.3. COMPILER AND TOOLS

The per-thread metrics is now available for historical analysis

Optionally, enable logging of the **per-thread** and **per-process** performance metric values in the Performance Co-Pilot (PCP) using the **pcp-zeroconf** package and **pmieconf** utility. Previously, only the **per-process** metric values were logged by **pmlogger** through the **pcp-zeroconf** package, but some analysis situation also requires **per-thread** values. As a result, the **per-thread** metrics are now available for historical analysis, after executing the following command:

```
# pmieconf -c enable zeroconf.all_threads
```

(BZ#1775373)

3.4. DESKTOP

FreeRDP has been updated to 2.1.1

This release updates the FreeRDP implementation of the Remote Desktop Protocol (RDP) from version 2.0.0 to 2.1.1. FreeRDP 2.1.1 supports new RDP options for the current Microsoft Windows terminal server version and fixes several security issues.

For detailed information about FreeRDP 2.1.1, see the upstream release notes: https://github.com/FreeRDP/FreeRDP/blob/2.1.1/ChangeLog.

(BZ#1834286)

3.5. KERNEL

Kernel version in RHEL 7.9

Red Hat Enterprise Linux 7.9 is distributed with the kernel version 3.10.0-1160.

See also Important Changes to External Kernel Parameters and Device Drivers.

(BZ#1801759)

A new kernel parameter: page_owner

The **page owner tracking** is a new functionality, which enables users to observe the kernel memory consumption at the page allocator level. Users can employ this functionality to debug the kernel memory leaks, or to discover the kernel modules that consume excessive amounts of memory. To enable the feature, add the **page_owner=on** parameter to the kernel command-line. For more information on how to set the kernel command-line parameters, see the Configuring kernel command-line parameters on Customer Portal.

WARNING

Regardless of the **page_owner** parameter setting (**on** or **off**) to the kernel command-line, usage of the page owner tracking adds approximately 2.14% additional memory requirement on RHEL 7.9 systems (impacts the kernel, VM, or **cgroup**). For further details on this topic, see the Why Kernel-3.10.0-1160.el7 consumes double amount of memory compared to kernel-3.10.0-1127.el7? Solution.

For more information about important changes to kernel parameters, see the New kernel parameters section.

(BZ#1781726)

EDAC driver support is now added to Intel ICX systems

This update adds the Error Detection and Correction (EDAC) driver to Intel ICX systems. As a result, memory errors can be detected on these systems and reported to the EDAC subsystem.

(BZ#1514705)

Intel® Omni-Path Architecture (OPA) Host Software

Intel® Omni-Path Architecture (OPA) host software is fully supported in Red Hat Enterprise Linux 7.9. 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.

(BZ#1855010)

The Mellanox ConnectX-6 Dx network adapter is now fully supported

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. This feature, previously available as a technology preview, is now fully supported in RHEL 7.9.

(BZ#1829777)

3.6. REAL-TIME KERNEL

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

The **kernel-rt** sources have been updated to use the latest RHEL kernel source tree, which provides a number of bug fixes and enhancements over the previous version.

(BZ#1790643)

3.7. NETWORKING

Configuring unbound to run inside chroot for systems without SELinux

For systems with SELinux enabled and in enforcing mode, SELinux provides significant protection and limits what the **unbound** service can access. If you cannot configure SELinux in enforcing mode, and you want to increase the protection of the **unbound** domain name server, use the **chroot** utility for jailing **unbound** into a limited **chroot** environment. Note that the protection by **chroot** is lower in comparison to SELinux enforcing mode.

For configuring **unbound** to run inside **chroot**, prepare your environment as described in the following support article Running unbound in chroot.

(BZ#2121623)

3.8. RED HAT ENTERPRISE LINUX SYSTEM ROLES

rhel-system-roles updated

The **rhel-system-roles** package has been updated to provide multiple bug fixes and enhancements. Notable changes include:

- Support for **802.1X** authentication with EAP-TLS was added for the **network** RHEL System Role when using the **NetworkManager** provider. As a result, now customers can configure their machines to use **802.1X** authentication with EAP-TLS using the **network** RHEL System Role instead of having to use the **nmcli** command-line utility.
- The **network** RHEL System Role tries to modify a link or network attributes without disrupting the connectivity, when possible.
- The logging in **network** module logs has been fixed so that informative messages are no longer printed as warnings, but as debugging information.

- The **network** RHEL System Role now uses **NetworkManagers** capability to revert changes, if an error occurs, when applying the configuration to avoid partial changes.

(BZ#1767177)

3.9. SECURITY

SCAP Security Guide now provides a profile aligned with the CIS RHEL 7 Benchmark v2.2.0

With this update, the **scap-security-guide** packages provide a profile aligned with the CIS Red Hat Enterprise Linux 7 Benchmark v2.2.0. The profile enables you to harden the configuration of the system using the guidelines by the Center for Internet Security (CIS). As a result, you can configure and automate compliance of your RHEL 7 systems with CIS by using the CIS Ansible Playbook and the CIS SCAP profile.

Note that the **rpm_verify_permissions** rule in the CIS profile does not work correctly. See the known issue description **rpm_verify_permissions** fails in the CIS profile .

(BZ#1821633)

SCAP Security Guide now correctly disables services

With this update, the **SCAP Security Guide** (SSG) profiles correctly disable and mask services that should not be started. This guarantees that disabled services are not inadvertently started as a dependency of another service. Before this change, the SSG profiles such as the U.S. Government Commercial Cloud Services (C2S) profile only disabled the service. As a result, services disabled by an SSG profile cannot be started unless you unmask them first.

(BZ#1791583)

The RHEL 7 STIG security profile updated to version V3R1

With the RHBA-2020:5451 advisory, the **DISA STIG for Red Hat Enterprise Linux 7** profile in the SCAP Security Guide has been updated to the latest version **V3R1**. This update adds more coverage and fixes reference problems. The profile is now also more stable and better aligns with the RHEL7 STIG benchmark provided by the Defense Information Systems Agency (DISA).

You should use only the current version of this profile because the older versions of this profile are no longer valid. The OVAL checks for several rules have changed, and scans using the **V3R1** version will fail for systems that were hardened using older versions of SCAP Security Guide. You can fix the rules automatically by running the remediation with the new version of SCAP Security Guide.

WARNING

Automatic remediation might render the system non-functional. Run the remediation in a test environment first.

The following rules have been changed:

CCE-80224-9

The default value of this SSHD configuration has changed from **delayed** to **yes**. You must now provide a value according to recommendations. Check the rule description for information about fixing this problem or run the remediation to fix it automatically.

CCE-80393-2

xccdf_org.ssgproject.content_rule_audit_rules_execution_chcon

CCE-80394-0

xccdf_org.ssgproject.content_rule_audit_rules_execution_restorecon

CCE-80391-6

xccdf_org.ssgproject.content_rule_audit_rules_execution_semanage

CCE-80660-4

xccdf_org.ssgproject.content_rule_audit_rules_execution_setfiles

CCE-80392-4

xccdf_org.ssgproject.content_rule_audit_rules_execution_setsebool

CCE-82362-5

xccdf_org.ssgproject.content_rule_audit_rules_execution_seunshare

CCE-80398-1

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_chage

CCE-80404-7

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_chsh

CCE-80410-4

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_crontab

CCE-80397-3

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_gpasswd

CCE-80403-9

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_newgrp

CCE-80411-2

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_pam_timestamp_check

CCE-27437-3

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands

CCE-80395-7

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_passwd

CCE-80406-2

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_postdrop

CCE-80407-0

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_postqueue

CCE-80408-8

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_ssh_keysign

CCE-80402-1

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_sudoedit

CCE-80401-3

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_sudo

CCE-80400-5

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_su

CCE-80405-4

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_umount

CCE-80396-5

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_unix_chkpwd

CCE-80399-9

xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands_userhelper

(BZ#1665233)

Profiles for DISA STIG version v3r3

The Defense Information Systems Agency (DISA) has published an updated version of the Secure Technical Implementation Guide (STIG) for RHEL 7 version 3, release 3. The update available with the RHBA-2021:2803 advisory:

- Aligns all rules within the existing **xccdf_org.ssgproject.content_profile_stig** profile with the latest STIG release.
- Adds a new profile **xccdf_org.ssgproject.content_profile_stig_gui** for systems with a graphical user interface (GUI).

(BZ#1958789, BZ#1970131)

scap-security-guide now provides an ANSSI-BP-028 High hardening level profile

With the release of the RHBA-2021:2803 advisory, the **scap-security-guide** packages provide an updated profile for ANSSI-BP-028 at the High hardening level. This addition completes the availability of profiles for all ANSSI-BP-028 v1.2 hardening levels. Using the updated profile, you can configure the system to comply with the recommendations from the French National Security Agency (ANSSI) for GNU/Linux Systems at the High hardening level.

As a result, you can configure and automate compliance of your RHEL 7 systems according to your required ANSSI hardening level by using the ANSSI Ansible Playbooks and the ANSSI SCAP profiles. The Draft ANSSI High profile provided with the previous versions has been aligned to ANSSI DAT-NT-028. Although the profile names and versions have changed, the IDs of the ANSSI profiles such as **xccdf_org.ssgproject.content_profile_anssi_nt28_high** remain the same to ensure backward compatibility.

WARNING

Automatic remediation might render the system non-functional. Red Hat recommends running the remediation in a test environment first.

(BZ#1955180)

The RHEL 8 STIG profile is now better aligned with the DISA STIG content

The DISA STIG for Red Hat Enterprise Linux 7 profile (**xccdf_org.ssgproject.content_profile_stig**) available in the **scap-security-guide** (SSG) package can be used to evaluate systems according to the Security Technical Implementation Guides (STIG) by the Defense Information Systems Agency (DISA). You can remediate your systems by using the content in SSG, but you might need to evaluate them using DISA STIG automated content. With the release of the RHBA-2022:6576 advisory, the DISA STIG RHEL 7 profile is better aligned with DISA's content. This leads to fewer findings against DISA content after SSG remediation.

Note that the evaluations of the following rules still diverge:

- SV-204511r603261_rule - CCE-80539-0 (**auditd_audispd_disk_full_action**)
- SV-204597r792834_rule - CCE-27485-2 (**file_permissions_sshd_private_key**)

Also, rule SV-204405r603261_rule from DISA's RHEL 7 STIG is not covered in the SSG RHEL 7 STIG profiles.

(BZ#1967950)

A warning message to configure Audit log buffer for large systems added to SCAP rule audit_rules_for_ospp

The SCAP rule **xccdf_org.ssgproject.content_rule_audit_rules_for_ospp** now displays a performance warning on large systems where the Audit log buffer configured by this rule might be too small, and can override the custom value. The warning also describes the process to configure a larger Audit log buffer. With the release of the RHBA-2022:6576 advisory, you can keep large systems compliant and correctly set their Audit log buffer.

(BZ#1993822)

3.10. SERVERS AND SERVICES

New package: compat-unixODBC234 for SAP

The new **compat-unixODBC234** package provides version 2.3.4 of **unixODBC**, a framework that supports accessing databases through the ODBC protocol. This new package is available in the RHEL 7 for SAP Solutions **sap-hana** repository to enable streaming backup of an SAP HANA database using the SAP **backint** interface. For more information, see Overview of the Red Hat Enterprise Linux for SAP Solutions subscription.

The **compat-unixODBC234** package conflicts with the base RHEL 7 **unixODBC** package. Therefore, uninstall **unixODBC** prior to installing **compat-unixODBC234**.

This package is also available for Red Hat Enterprise Linux 7.4 Update Services for SAP Solutions, Red Hat Enterprise Linux 7.6 Extended Update Support, and Red Hat Enterprise Linux 7.7 Extended Update Support through the RHEA-2020:2178 advisory.

See also The **compat-unixODBC234** package for SAP requires a symlink to load the **unixODBC** library.

(BZ#1790655)

MariaDB rebased to version 5.5.68

With RHEL 7.9, the **MariaDB** database server has been updated to version 5.5.68. This release provides multiple security and bug fixes from the recent upstream maintenance releases.

(BZ#1834835)

3.11. 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)

3.12. ATOMIC HOST AND CONTAINERS

Red Hat Enterprise Linux Atomic Host is a secure, lightweight, and minimal-footprint operating system optimized to run Linux containers.

IMPORTANT

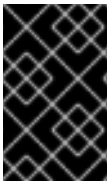
Red Hat Enterprise Linux Atomic Host is retired as of August 6, 2020 and active support is no longer provided.

3.13. RED HAT SOFTWARE COLLECTIONS

Red Hat Software Collections (RHSCL) 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, IBM Z, and IBM POWER, little endian.

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 4. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel distributed with Red Hat Enterprise Linux 7.9. These changes include added or updated **proc** entries, **sysctl**, and **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

4.1. NEW KERNEL PARAMETERS

bert_disable [ACPI]

This parameter disables Boot Error Record Table (BERT) on defective BIOSes.
BERT is one of four ACPI Platform Error Interface tables and is used for obtaining hardware error logs that occurred in the previous boot and firmware did not notify the kernel about the error at runtime, for example through a non-maskable interrupt (NMI) or a machine-check exception (MCE).

bert_enable [ACPI]

RHEL7 only. This parameter enables Boot Error Record Table (BERT). The default state is disabled.

page_owner = [KNL]

Storage of the information about who allocated each page is disabled in default. This parameter enables to store such information by using the following option:

- **on** - enable the feature

srbds = [X86,INTEL]

This parameter controls the Special Register Buffer Data Sampling (SRBDS) mitigation.
Certain CPUs are vulnerable to MDS-like (Microarchitectural Data Sampling) exploits which can leak bits from the random number generator.

By default, this issue is mitigated by microcode. However, the microcode fix can cause the **RDRAND** (read random) and **RDSEED** instructions to become much slower. Among other effects, this will result in reduced throughput from the /**dev**/**urandom** file.

The microcode mitigation can be disabled with the following option:

- **off** - Disable mitigation and remove performance impact to **RDRAND** and **RDSEED**.

4.2. NEW /PROC/SYS/KERNEL/ PARAMETERS

hyperv_record_panic_msg

This parameter controls whether the panic kernel (kmsg) data is reported to Hyper-V or not.
The values are:

- **0** - Do not report the panic kmsg data.
- **1** - Report the panic kmsg data. This is the default behavior.

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 7.9.

5.1. NEW DRIVERS

Graphics Drivers and Miscellaneous Drivers

- MC Driver for Intel 10nm server processors (i10nm_edac.ko.xz)

5.2. UPDATED DRIVERS

Network Driver Updates

- The Netronome Flow Processor (NFP) driver (nfp.ko.xz) has been updated to version 3.10.0-1150.el7.x86_64.
- VMware vmxnet3 virtual NIC driver (vmxnet3.ko.xz) has been updated to version 1.4.17.0-k.

Storage Driver Updates

- QLogic FCoE Driver (bnx2fc.ko.xz) has been updated to version 2.12.13.
- Driver for HP Smart Array Controller (hpsa.ko.xz) has been updated to version 3.4.20-170-RH5.
- Broadcom MegaRAID SAS Driver (megaraid_sas.ko.xz) has been updated to version 07.714.04.00-rh1.
- QLogic Fibre Channel HBA Driver (qla2xxx.ko.xz) has been updated to version 10.01.00.22.07.9-k.
- Driver for Microsemi Smart Family Controller version (smartpqi.ko.xz) has been updated to version 1.2.10-099.

CHAPTER 6. NOTABLE BUG FIXES

This chapter describes bugs fixed in Red Hat Enterprise Linux 7.9 that have a significant impact on users.

6.1. AUTHENTICATION AND INTEROPERABILITY

A deadlock no longer occurs when using SASL binds to Directory Server

Previously, a SASL bind to Directory Server could attempt using callbacks that were modified during the connection process. Consequently, a deadlock occurred, and Directory Server could terminated unexpectedly. With this update, the server uses a connection lock that prevents modifying IO layers and callbacks while they are in use. As a result, the deadlock no longer occurs when using SASL binds.

(BZ#1801327)

The **389-ds-base** package now sets the required permissions on directories owned by the Directory Server user

If directories in the file system owned by the Directory Server user do not have the correct permissions, Directory Server utilities adjust them accordingly. However, if these permissions were different to the ones that were set during the RPM installation, verifying the RPM using the **rpm -V 389-ds-base** command failed. This update fixes the permissions in the RPM. As a consequence, verifying the **389-ds-base** package no longer complains about incorrect permissions.

(BZ#1700987)

A memory leak has been fixed in Directory Server when using **ip** binding rules in an ACI with IPv6

The Access Control Instruction (ACI) context in Directory Server is attached to a connection and contains a structure for both the IPv4 and IPv6 protocol. Previously, when a client closed a connection, Directory Server removed the only IPv4 structure and the context. As a consequence, if an administrator configured an ACI with **ip** binding rule, Directory Server leaked memory of the IPv6 structure. With this update, the server frees both the IPv4 and IPv6 structures at the end of a connection. As a result, Directory Server no longer leaks memory in the mentioned scenario.

(BZ#1796558)

Directory Server no longer leaks memory when using ACIs with an **ip** bind rule

When a Directory Server Access Control Instruction (ACI) contains an **ip** bind rule, the server stores the value of the **ip** keyword as a reference while evaluating the ACI. Previously, when the evaluations were completed Directory Server did not free the **ip** value. As a consequence, the server leaked around 100 bytes of memory each time the server evaluated an ACI with an **ip** bind rule. With this update, Directory Server keeps track of the **ip** value in the per-connection structure and frees the structure when the connection is closed. As a consequence, Directory Server no longer leaks memory in the mentioned scenario.

(BZ#1769418)

Directory Server no longer rejects wildcards in the **rootdn-allow-ip** and **rootdn-deny-ip** parameters

Previously, when an administrator tried to set a wildcard in the **rootdn-allow-ip** or **rootdn-deny-ip** parameters in the **cn=RootDN Access Control Plugin,cn=plugins,cn=config** entry, Directory Server rejected the value. With this update, you can use wildcards when specifying allowed or denied IP addresses in the mentioned parameters.

(BZ#1807537)

Directory Server rejects update operations if retrieving the system time fails or the time difference is too large

Previously, when calling the system time() function failed or the function returned an unexpected value, Change Sequence Numbers (CSN) in Directory Server could become corrupted. As a consequence, the administrator had to re-initialize all replicas in the environment. With this update, Directory Server rejects the update operation if the time() function failed, and Directory Server no longer generates corrupt CSNs in the mentioned scenario.

Note that, if the time difference is greater than one day, the server logs a **INFO - csngen_new_csn - Detected large jump in CSN time** message in the **/var/log/dirsrv/slapd-<instance_name>/error** file. However, Directory Server still creates the CSN and does not reject the update operation.

(BZ#1837105)

Directory Server no longer hangs while updating the schema

Previously, during a mixed load of search and modify operations, the update of the Directory Server schema blocked all search and modify operations, and the server appeared to hang. This update adjusts the mutex locking during schema updates. As a result, the server does not hang while updating the schema.

(BZ#1824930)

Directory Server no longer leaks memory when using indirect COS definitions

Previously, after processing an indirect Class Of Service (COS) definition, Directory Server leaked memory for each search operation that used an indirect COS definition. With this update, Directory Server frees all internal COS structures associated with the database entry after it has been processed. As a result, the server no longer leaks memory when using indirect COS definitions.

(BZ#1827284)

Password expiration notifications sent to AD clients using SSSD

Previously, Active Directory clients (non-IdM) using SSSD were not sent password expiration notices because of a recent change in the SSSD interface for acquiring Kerberos credentials.

The Kerberos interface has been updated and expiration notices are now sent correctly.

(BZ#1733289)

KDCs now correctly enforce password lifetime policy from LDAP backends

Previously, non-IPA Kerberos Distribution Centers (KDCs) did not ensure maximum password lifetimes because the Kerberos LDAP backend incorrectly enforced password policies. With this update, the Kerberos LDAP backend has been fixed, and password lifetimes behave as expected.

(BZ#1782492)

The pkidaemon tool now reports the correct status of PKI instances when nuxwdog is enabled

Previously, the **pkidaemon status** command would not report the correct status for PKI server instances that have the **nuxwdog** watchdog enabled. With this update, **pkidaemon** detects whether **nuxwdog** is enabled and reports the correct status of the PKI server.

(BZ#1487418)

6.2. COMPILER AND TOOLS

The strptime() method of the Time::Piece Perl module now correctly parses Julian dates

The **Time::Piece** Perl module did not correctly parse a day of the year (**%j**) using the **strptime()** method. Consequently, Julian dates were parsed incorrectly. This bug has been fixed, and the **strptime()** method provided by the **Time::Piece** module now handles Julian dates properly.

(BZ#1751381)

Documentation files from perl-devel no longer have a write permission for a group

Previously, certain documentation files from the **perl-devel** package had a write permission set for a group. Consequently, users in the root group could write into these files, which represented a security risk. With this update, the write bit for a group has been removed for the affected files. As a result, no documentation file from **perl-devel** has a write permission set for a group.

(BZ#1806523)

6.3. KERNEL

Resuming from hibernation now works on the megaraid_sas driver

Previously, when the **megaraid_sas** driver resumed from hibernation, the Message Signaled Interrupts (MSIx) allocation did not work correctly. As a consequence, resuming from hibernation failed, and restarting the system was required. This bug has been fixed, and resuming from hibernation now works as expected.

(BZ#1807077)

Disabling logging in the nf-logger framework has been fixed

Previously, when an admin used the **sysctl** or **echo** commands to turn off an assigned **netfilter** logger, a **NUL**-character was not added to the end of the **NONE** string. Consequently, the **strcmp()** function failed with a **No such file or directory** error. This update fixes the problem. As a result, commands, such as **sysctl net.netfilter.nf_log.2=NONE** work as expected and turn off logging.

(BZ#1770232)

XFS now mounts correctly even if the storage device reported invalid geometry at file system creation

In RHEL 7.8, an XFS file system failed to mount with the error **SB stripe unit sanity check failed** if it was created on a block device that reported invalid stripe geometry to the **mkfs.xfs** tool.

With this update, XFS now mounts the file system even if it was created based on invalid stripe geometry.

For details, see the following solution article: https://access.redhat.com/solutions/5075561.

(BZ#1836292)

6.4. NETWORKING

The same zone file can now be included in multiple views or zones in BIND

BIND 9.11 introduced an additional check to ensure that no daemon writable zone file is used multiple times, which would result in creating errors in zone journal serialization. Consequently, configuration accepted by BIND 9.9 was no longer accepted by this daemon. With this update, the fatal error message in configuration file check is replaced by a warning, and as a result, the same zone file can now be included in multiple views or zones.

Note that using an in-view clause is recommended as a better solution.

(BZ#1744081)

A configuration parameter has been added to firewalld to disable zone drifting

Previously, the **firewalld** service contained an undocumented behavior known as "zone drifting". RHEL 7.8 removed this behavior because it could have a negative security impact. As a consequence, on hosts that used this behavior to configure a catch-all or fallback zone, **firewalld** denied connections that were previously allowed. This update re-adds the zone drifting behavior, but as a configurable feature. As a result, users can now decide to use zone drifting or disable the behavior for a more secure firewall setup.

By default, in RHEL 7.9, the new **AllowZoneDrifting** parameter in the **/etc/firewalld/firewalld.conf** file is set to **yes**. Note that, if the parameter is enabled, **firewalld** logs:

> WARNING: AllowZoneDrifting is enabled. This is considered an insecure configuration option. It will be removed in a future release. Please consider disabling it now.

(BZ#1796055)

RHEL rotates firewalld log files

Previously, RHEL did not rotate **firewalld** log files. As a consequence, the **/var/log/firewalld** log file grew indefinitely. This update adds the **/etc/logrotate.d/firewalld** log rotation configuration file for the **firewalld** service. As a result, the **/var/log/firewalld** log is rotated, and users can customize the rotation settings in the **/etc/logrotate.d/firewalld** file.

(BZ#1754117)

6.5. SECURITY

Recursive dependencies no longer cause OpenSCAP crashes

Because **systemd** units can have dependent units, OpenSCAP scans could encounter cyclical dependencies that caused the scan to terminate unexpectedly. With this update, OpenSCAP no longer analyses previously analysed units. As a result, scans now complete with a valid result even if dependencies are cyclical.

(BZ#1478285)

OpenSCAP scanner results no longer contain a lot of SELinux context error messages

Previously, the OpenSCAP scanner logged the inability to get the SELinux context on the **ERROR** level even in situations where it is not a true error. Consequently, scanner results contained a lot of SELinux context error messages and both the **oscap** command-line utility and the **SCAP Workbench** graphical utility outputs were hard to read for that reason. The **openscap** packages have been fixed, and scanner results no longer contain a lot of SELinux context error messages.

(BZ#1640522)

audit_rules_privileged_commands now works correctly for privileged commands

Remediation of the **audit_rules_privileged_commands** rule in the **scap-security-guide** packages did not account for a special case in parsing command names. Additionally, the ordering of certain rules prevented successful remediation. As a consequence, remediation of certain combinations of rules reported they were fixed although successive scans reported the rule as failing again. This update improves regular expressions in the rule and the ordering of the rules. As a result, all privileged commands are correctly audited after remediation.

(BZ#1691877)

Updated rule descriptions in the SCAP Security Guide

Because default kernel parameters cannot be reliably determined for all supported versions of RHEL, checking kernel parameter settings always requires explicit configuration. The text in the configuration guide mistakenly stated that explicit settings were not needed if the default version was compliant. With this update, the rule description in the **scap-security-guide** package correctly describes the compliance evaluation and the corresponding remediation.

(BZ#1494606)

configure_firewalld_rate_limiting now correctly rate-limits connections

The **configure_firewalld_rate_limiting** rule, which protects the system from Denial of Service (DoS) attacks, previously configured the system to accept all traffic. With this update, the system correctly rate-limits connections after remediating this rule.

(BZ#1609014)

dconf_gnome_login_banner_text no longer incorrectly fails

Remediation of the **dconf_gnome_login_banner_text** rule in the **scap-security-guide** packages previously failed after a failure to scan the configuration. As a consequence, the remediation could not properly update the login banner configuration, which was inconsistent with expected results. With this update, Bash and Ansible remediations are more reliable and align with the configuration check implemented using the OVAL standard. As a consequence, remediations now work properly and the rule passes after remediation.

(BZ#1776780)

scap-security-guide Ansible remediations no longer include the follow argument

Prior to this update, **scap-security-guide** Ansible remediations could contain the **follow** argument in the **replace** module. Because **follow** was deprecated in Ansible 2.5, and will be removed in Ansible 2.10, using such remediations caused an error. With the release of the RHBA-2021:1383 advisory, the argument has been removed. As a result, Ansible playbooks by **scap-security-guide** will work properly in Ansible 2.10.

(BZ#1890111)

Postfix-specific rules no longer fail if postfix is not installed

Previously, SCAP Security Guide (SSG) evaluated Postfix-specific rules independently of the **postfix** package installed on the system. As a result, SSG reported Postfix-specific rules as **fail** instead of **notapplicable**. With the release of the RHBA-2021:4781 advisory, SSG correctly evaluates Postfix-specific rules only if the **postfix** package is installed, and reports **notapplicable** if the **postfix** package is not installed.

(BZ#1942281)

Service Disabled rules are no longer ambiguous

Previously, rule descriptions for the Service Disabled type in the SCAP Security Guide provided options for disabling and masking a service but did not specify whether the user should disable the service, mask it, or both.

With the release of the RHBA-2021:1383 advisory, rule descriptions, remediations, and OVAL checks have been aligned and inform users that they must mask a service to disable it.

(BZ#1891435)

Fixed Ansible remediations for scap-security-guide GNOME dconf rules

Previously, Ansible remediations for some rules covering the GNOME **dconf** configuration systems were not aligned with the corresponding OVAL checks. Consequently, Ansible incorrectly remediated the following rules, marking them as **failed** in subsequent scans:

- **dconf_gnome_screensaver_idle_activation_enabled**
- **dconf_gnome_screensaver_idle_delay**
- **dconf_gnome_disable_automount_open**

With the update released in the RHBA-2021:4781 advisory, Ansible regular expressions have been fixed. As a result, these rules remediate correctly in the **dconf** configuration.

(BZ#1976123)

SELinux no longer blocks PCP from restarting unresponsive PMDAs

Previously, a rule that allows **pcp_pmie_t** processes to communicate with Performance Metric Domain Agent (PMDA) was missing in the SELinux policy. As a consequence, SELinux denied the **pmsignal** process to restart unresponsive PMDAs. With this update, the missing rule has been added to the policy, and the Performance Co-Pilot (PCP) can now restart unresponsive PMDAs.

(BZ#1770123)

SELinux no longer prevents auditd to halt or power off the system

Previously, the SELinux policy did not contain a rule that allows the Audit daemon to start a **power_unit_file_t systemd** unit. Consequently, **auditd** could not halt or power off the system even when configured to do so in cases such as no space left on a logging disk partition.

With this update, the missing rule has been added to the SELinux policy. As a result, **auditd** can now halt or power off the system.

(BZ#1780332)

The chronyd service can now execute shells in SELinux

Previously, the **chronyd** process, running under **chronyd_t**, was unable to execute the **chrony-helper** shell script, because the SELinux policy did not allow **chronyd** to execute any shell. In this update, the SELinux policy allows the **chronyd** process to run a shell that is labeled **shell_exec_t**. As a result, the **chronyd** service starts successfully under the Multi-Level Security (MLS) policy.

(BZ#1775573)

Tang reliably updates its cache

When the Tang application generates its keys, for example, at first installation, Tang updates its cache. Previously, this process was unreliable, and the application cache did not update correctly to reflect Tang keys. This caused problems with using a Tang pin in Clevis, with the client displaying the error message **Key derivation key not available**. With this update, key generation and cache update logic was moved to Tang, removing the file watching dependency. As a result, the application cache remains in a correct state after cache update.

(BZ#1703445)

6.6. SERVERS AND SERVICES

cupsd now consumes less memory during PPD caching

Previously, the CUPS daemon consumed a lot of memory when many print queues with extensive Postscript Printer Description (PPD) were created. With this update, CUPSD checks if a cached file exists and if it has newer or the same timestamp as the PPD file in **/etc/cups/ppd**, then it loads the cached file. Otherwise it creates a new cached file based on the PPD file. As a result, the memory consumption lowers by 91% in the described scenario.

(BZ#1672212)

tuned no longer hangs on SIGHUP when a non-existent profile is selected

When the **tuned** service receives the SIGHUP signal, it attempts to reload the profile. Prior to this update, **tuned** was unable to correctly handle situations when:

- The **tuned** profile was set to a non-existent profile, or
- The automatic profile selection mode was active and the recommended profile was non-existent.

As a consequence, the **tuned** service became unresponsive and had to be restarted. This bug has been fixed, and the **tuned** service no longer hangs in the described scenarios.

Note that the **tuned** behavior has changed with this update. Previously, when the user executed the **tuned-adm off** command and restarted the **tuned** service, **tuned** tried to load the recommended profile. Now, **tuned** loads no profile even if the recommended profile exists.

(BZ#1702724)

tuned no longer applies settings from sysctl.d directories when the reapply_sysctl option is set to 1

Previously, if the **reapply_sysctl** configuration option was set to **1**, the **tuned** profile applied **sysctl** settings from the **/usr/lib/sysctl.d**, **/lib/sysctl.d**, and **/usr/local/lib/sysctl.d** directories after applying **sysctl** settings from a **tuned** profile. Consequently, settings from these directories would override **sysctl** settings from the **tuned** profile. With this update, **tuned** no longer applies **sysctl** settings from the mentioned directories when the **reapply_sysctl** option is set to **1**.

Note that to re-apply **sysctl** settings you need to move them from the mentioned directories to **/etc/sysctl.d**, **/etc/sysctl.conf** or **/run/sysctl.d** directories or to a custom **tuned** profile.

(BZ#1776149)

6.7. STORAGE

LVM volumes on VDO now shut down correctly

Previously, the stacking of block layers on VDO was limited by the configuration of the VDO systemd units. As a result, the system shutdown sequence waited for 90 seconds when it tried to stop LVM volumes stored on VDO. After 90 seconds, the system uncleanly stopped the LVM and VDO volumes.

With this update, the VDO systemd units have been improved, and as a result, the system shuts down cleanly with LVM on VDO.

Additionally, the VDO startup configuration is now more flexible. You no longer have to add special mount options in the **/etc/fstab** file for most VDO configurations.

(BZ#1706154)

6.8. SYSTEM AND SUBSCRIPTION MANAGEMENT

microdnf no longer fails to retrieve GPG key for custom Satellite repository

Previously, the **librhsm** library, used internally by **microdnf**, incorrectly handled relative **gpgkey** paths, which are used in custom repositories hosted by Satellite. Consequently, when the user ran the **microdnf** command in a container to install a package signed with GNU Privacy Guard (GPG) from a custom repository through the host's Satellite subscription, **microdnf** failed with the following error:

```
GPG enabled: failed to lookup digest in keyring.
```

With this update, handling of relative **gpgkey** paths has been fixed in **librhsm**. As a result, the user can now successfully use the custom repository from Satellite inside containers.

(BZ#1708628)

YUM can now install RPM packages signed with GPG keys with revoked subkeys

Previously, the **YUM** utlity could not install RPM packages signed with GNU Privacy Guard (GPG) keys with revoked subkeys. Consequently, **YUM** failed with the following error message:

```
signature X doesn't bind subkey to key, type is subkey revocation
```

This update introduces a change in the code that checks revocation before checking binding signature. As a result, **YUM** can now install RPM packages signed with GPG keys with revoked subkeys.

(BZ#1778784)

6.9. RHEL IN CLOUD ENVIRONMENTS

Using cloud-init to create virtual machines with XFS and swap now works correctly

Previously, using the **cloud-init** utility failed when creating a virtual machine (VM) with an XFS root file system and an enabled swap partition. In addition, the following error message was logged:

kernel: swapon: swapfile has holes

This update fixes the underlying code, which prevents the problem from occurring.

(BZ#1772505)

CHAPTER 7. TECHNOLOGY PREVIEWS

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

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 a Technology Preview

An API is available for Identity Management (IdM). To view the API, IdM also provides an API browser as Technology Preview.

In RHEL 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)

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)

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 RHEL 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 the 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)

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)

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)

7.7. KERNEL

eBPF system call for tracing

Red Hat Enterprise Linux 7.6 introduced 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 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 available as a Technology Preview

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. Since Red Hat Enterprise Linux 7.8, the **criu** package provides support for Podman to do a container checkpoint and restore. The newly added functionality only works without SELinux support.

(BZ#1400230)

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 through the 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.

Note that the **qlcnic** driver has been deprecated and is not available in RHEL 8.

(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**
- **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.

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 7.8 for SAP Solutions is currently not 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 7.8 features. Please consult SAP Notes 2369910 and 2235581 for the latest information about validated releases and SAP support.

(BZ#1660838)

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 with RSA-PSS keys

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. See MZBZ#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

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 repository.

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 repository, 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)

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)

7.14. RHEL IN CLOUD ENVIRONMENTS

Select Intel network adapters now support SR-IOV in RHEL guests on Hyper-V

As a Technology Preview, Red Hat Enterprise Linux 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 **iavf** 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)

CHAPTER 8. KNOWN ISSUES

This chapter documents known problems in Red Hat Enterprise Linux 7.9.

8.1. AUTHENTICATION AND INTEROPERABILITY

Trusts with Active Directory do not work properly after upgrading ipa-server using the latest container image

After upgrading an IdM server with the latest version of the container image, existing trusts with Active Directory domains no longer work. To work around this problem, delete the existing trust and re-establish it after the upgrade.

(BZ#1819745)

Potential risk when using the default value for ldap_id_use_start_tls option

When using **ldap://** without TLS for identity lookups, it can pose a risk for an attack vector. Particularly a man-in-the-middle (MITM) attack which could allow an attacker to impersonate a user by altering, for example, the UID or GID of an object returned in an LDAP search.

Currently, the SSSD configuration option to enforce TLS, **ldap_id_use_start_tls**, defaults to **false**. Ensure that your setup operates in a trusted environment and decide if it is safe to use unencrypted communication for **id_provider = ldap**. Note **id_provider = ad** and **id_provider = ipa** are not affected as they use encrypted connections protected by SASL and GSSAPI.

If it is not safe to use unencrypted communication, enforce TLS by setting the **ldap_id_use_start_tls** option to **true** in the **/etc/sssd/sssd.conf** file. The default behavior is planned to be changed in a future release of RHEL.

(JIRA:RHELPLAN-155168)

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)

8.3. INSTALLATION AND BOOTING

Systems installed as Server with GUI with the DISA STIG profile or with the CIS profile do not start properly

The DISA STIG profile and the CIS profile require the removal of the **xorg-x11-server-common** (X Windows) package but does not require the change of the default target. As a consequence, the system is configured to run the GUI but the X Windows package is missing. As a result, the system does not start

properly. To work around this problem, do not use the DISA STIG profile and the CIS profile with the **Server with GUI** software selection or customize the profile by removing the **package_xorg-x11-server-common_removed** rule.

(BZ#1648162)

8.4. KERNEL

The radeon driver fails to reset hardware correctly when performing kdump

When booting the kernel from the currently running kernel, such as when performing the **kdump** process, the **radeon** kernel driver currently does not properly reset hardware. Instead, the **kdump** kernel terminates unexpectedly, which causes the rest of the **kdump** service to fail.

To work around this problem, disable **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#1168430)

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)

Kernel deadlocks can occur when dm_crypt is used with intel_qat

The **intel_qat** kernel module uses the **GFP_ATOMIC** memory allocations, which can fail under memory stress. Consequently, kernel deadlocks and possible data corruption can occur when the **dm_crypt** kernel module uses **intel_qat** for encryption offload. To work around this problem, you can choose either of the following:

- Update to RHEL 8
- Avoid using **intel_qat** for encryption offload (potential performance impact)
- Ensure the system does not get under excessive memory pressure

(BZ#1813394)

The vmcore file generation fails on Amazon c5a machines on RHEL 7

On Amazon c5a machines, the Advanced Programmable Interrupt Controller (APIC) fails to route the interrupts of the Local APIC (LAPIC), when configured in the **flat mode** inside the **kdump** kernel. As a consequence, the **kdump** kernel fails to boot and prevents the **kdump** kernel from saving the **vmcore** file for further analysis.

To work around the problem:

1. Increase the crash kernel size by setting the **crashkernel** argument to **256M**:

```
$ grubby-args="crashkernel=256M" --update-kernel
/boot/vmlinuz-`uname -r`
```

2. Set the **nr_cpus=9** option by editing the **/etc/sysconfig/kdump** file:

```
KDUMP_COMMANDLINE_APPEND="irqpoll" *nr_cpus=9*
reset_devices
cgroup_disable=memory mce=off numa=off udev.children-
max=2 panic=10 acpi_no_memhotplug
transparent_hugepage=never nokaslr novmcoredd
hest_disable
```

As a result, the **kdump** kernel boots with 9 CPUs and the **vmcore** file is captured upon kernel crash. Note that the **kdump** service can use a significant amount of crash kernel memory to dump the **vmcore** file since it enables 9 CPUs in the **kdump** kernel. Therefore, ensure that the crash kernel has a size reserve of 256MB available for booting the **kdump** kernel.

(BZ#1844522)

Enabling some kretprobes can trigger kernel panic

Using **kretprobes** of the following functions can cause CPU hard-lock:

- **_raw_spin_lock**
- **_raw_spin_lock_irqsave**
- **_raw_spin_unlock_irqrestore**
- **queued_spin_lock_slowpath**

As a consequence, enabling these **kprobe** events, you can experience a system response failure. This situation triggers a kernel panic. To workaround this problem, avoid configuring **kretprobes** for mentioned functions and prevent system response failure.

(BZ#1838903)

The kdump service fails on UEFI Secure Boot enabled systems

If a UEFI Secure Boot enabled system boots with a not up-to-date RHEL kernel version, the **kdump** service fails to start. In the described scenario, **kdump** reports the following error message:

```
kexec_file_load failed: Required key not available
```

This behavior displays due to either of these:

- Booting the crash kernel with a not up-to-date kernel version.
- Configuring the **KDUMP_KERNELVER** variable in **/etc/sysconfig/kdump** file to a not up-to-date kernel version.

As a consequence, **kdump** fails to start and hence no dump core is saved during the crash event.

To workaround this problem, use either of these:

- Boot the crash kernel with the latest RHEL 7 fixes.
- Configure **KDUMP_KERNELVER** in **etc/sysconfig/kdump** to use the latest kernel version.

As a result, **kdump** starts successfully in the described scenario.

(BZ#1862840)

The RHEL installer might not detect iSCSI storage

The RHEL installer might not automatically set kernel command-line options related to iSCSI for some offloading iSCSI host bus adapters (HBAs). As a consequence, the RHEL installer might not detect iSCSI storage.

To work around the problem, add the following options to the kernel command line when booting to the installer:

```
rd.iscsi.ibft=1 rd.iscsi.firmware=1
```

These options enable network configuration and iSCSI target discovery from the pre-OS firmware configuration.

The firmware configures the iSCSI storage, and as a result, the installer can discover and use the iSCSI storage.

(BZ#1871027)

Race condition in the mlx5e_rep_neigh_update work queue sometimes triggers the kernel panic

When offloading encapsulation actions over the **mlx5** device using the **switchdev** in-kernel driver model in the Single Root I/O Virtualization (SR-IOV) capability, a race condition can happen in the **mlx5e_rep_neigh_update** work queue. Consequently, the system terminates unexpectedly with the kernel panic and the following message appears:

```
Workqueue: mlx5e mlx5e_rep_neigh_update [mlx5_core]
```

Currently, a workaround or partial mitigation to this problem is not known.

(BZ#1874101)

The ice driver does not load for Intel® network adapters

The **ice** kernel driver does not load for all Intel® Ethernet network adapters E810-XXV except the following:

- **v00008086d00001593sv*sd*bc*sc*i***
- **v00008086d00001592sv*sd*bc*sc*i***
- **v00008086d00001591sv*sd*bc*sc*i***

Consequently, the network adapter remains undetected by the operating system. To work around this problem, you can use external drivers for RHEL 7 provided by Intel® or Dell.

(BZ#1933998)

kdump does not support setting nr_cpus to 2 or higher in Hyper-V virtual machines

When using RHEL 7.9 as a guest operating system on a Microsoft Hyper-V hypervisor, the kdump kernel in some cases becomes unresponsive when the **nr_cpus** parameter is set to 2 or higher. To avoid this problem from occurring, do not change the default **nr_cpus=1** parameter in the **/etc/sysconfig/kdump** file of the guest.

(BZ#1773478)

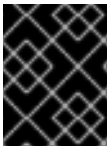
8.5. NETWORKING

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)

bind-utils DNS lookup utilities support fewer search domains than glibc

The **dig**, **host**, and **nslookup** DNS lookup utilities from the **bind-utils** package support only up to 8 search domains, while the **glibc** resolver in the system supports any number of search domains. As a consequence, the DNS lookup utilities may get different results than applications when a search in the **/etc/resolv.conf** file contains more than 8 domains.

To work around this problem, use one of the following:

- Full names ending with a dot, or
- Fewer than nine domains in the **resolv.conf** search clause.

Note that it is not recommended to use more than three domains.

(BZ#1758317)

BIND 9.11 changes log severity of query errors when query logging is enabled

With the BIND 9.11 update, the log severity for the **query-errors** changes from **debug 1** to **info** when query logging is enabled. Consequently, additional log entries describing errors now appear in the query log. To work around this problem, add the following statement into the **logging** section of the **/etc/named.conf** file:

```
category query-errors { default_debug; };
```

This will move query errors back into the debug log.

Alternatively, use the following statement to discard all query error messages:

```
category querry-errors { null; };
```

As a result, only name queries are logged in a similar way to the previous BIND 9.9.4 release.

(BZ#1853191)

named-chroot service fails to start when check-names option is not allowed in forward zone

Previously, the usage of the **check-names** option was allowed in the **forward zone** definitions.

With the rebase to **bind** 9.11, only the following **zone** types:

- **master**
- **slave**
- **stub**
- **hint**

use the **check-names** statement.

Consequently, the **check-names** option, previously allowed in the **forward zone** definitions, is no longer accepted and causes a failure on start of the **named-chroot** service. To work around this problem, remove the **check-names** option from all the **zone** types except for **master**, **slave**, **stub** or **hint**.

As a result, the **named-chroot** service starts again without errors. Note that the ignored statements will not change the provided service.

(BZ#1851836)

The NFQUEUE target overrides queue-cpu-fanout flag

iptables **NFQUEUE** target using **--queue-bypass** and **--queue-cpu-fanout** options accidentally overrides the **--queue-cpu-fanout** option if ordered after the **--queue-bypass** option. Consequently, the **--queue-cpu-fanout** option is ignored.

To work around this problem, rearrange the **--queue-bypass** option before **--queue-cpu-fanout** option.

(BZ#1851944)

8.6. SECURITY

Audit executable watches on symlinks do not work

File monitoring provided by the **-w** option cannot directly track a path. It has to resolve the path to a device and an inode to make a comparison with the executed program. A watch monitoring an executable symlink monitors the device and an inode of the symlink itself instead of the program executed in memory, which is found from the resolution of the symlink. Even if the watch resolves the symlink to get the resulting executable program, the rule triggers on any multi-call binary called from a different symlink. This results in flooding logs with false positives. Consequently, Audit executable watches on symlinks do not work.

To work around the problem, set up a watch for the resolved path of the program executable, and filter the resulting log messages using the last component listed in the **comm=** or **proctitle=** fields.

(BZ#1421794)

Executing a file while transitioning to another SELinux context requires additional permissions

Due to the backport of the fix for CVE-2019-11190 in RHEL 7.8, executing a file while transitioning to another SELinux context requires more permissions than in previous releases.

In most cases, the **domain_entry_file()** interface grants the newly required permission to the SELinux domain. However, in case the executed file is a script, then the target domain may lack the permission to execute the interpreter's binary. This lack of the newly required permission leads to AVC denials. If SELinux is running in enforcing mode, the kernel might kill the process with the SIGSEGV or SIGKILL signal in such a case.

If the problem occurs on the file from the domain which is a part of the **selinux-policy** package, file a bug against this component. In case it is part of a custom policy module, Red Hat recommends granting the missing permissions using standard SELinux interfaces:

- **corecmd_exec_shell()** for shell scripts
- **corecmd_exec_all_executables()** for interpreters labeled as **bin_t** such as Perl or Python

For more details, see the **/usr/share/selinux/devel/include/kernel/corecommands.if** file provided by the **selinux-policy-doc** package and the An exception that breaks the stability of the RHEL SELinux policy API article on the Customer Portal.

(BZ#1832194)

Scanning large numbers of files with OpenSCAP causes systems to run out of memory

The OpenSCAP scanner stores all collected results in the memory until the scan finishes. As a consequence, the system might run out of memory on systems with low RAM when scanning large numbers of files, for example, from the large package groups *Server with GUI* and *Workstation*.

To work around this problem, use smaller package groups, for example, *Server* and *Minimal Install* on systems with limited RAM. If your scenario requires large package groups, you can test whether your system has sufficient memory in a virtual or staging environment. Alternatively, you can tailor the scanning profile to deselect rules that involve recursion over the entire / filesystem:

- **rpm_verify_hashes**
- **rpm_verify_permissions**
- **rpm_verify_ownership**
- **file_permissions_unauthorized_world_writable**
- **no_files_unowned_by_user**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**

- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

This prevents the OpenSCAP scanner from causing the system to run out of memory.

(BZ#1829782)

RSA signatures with SHA-1 cannot be completely disabled in RHEL7

Because the **ssh-rsa** signature algorithm must be allowed in OpenSSH to use the new SHA2 (**rsa-sha2-512**, **rsa-sha2-256**) signatures, you cannot completely disable SHA1 algorithms in RHEL7. To work around this limitation, you can update to RHEL8 or use ECDSA/Ed25519 keys, which use only SHA2.

(BZ#1828598)

rpm_verify_permissions fails in the CIS profile

The **rpm_verify_permissions** rule compares file permissions to package default permissions. However, the Center for Internet Security (CIS) profile, which is provided by the **scap-security-guide** packages, changes some file permissions to be more strict than default. As a consequence, verification of certain files using **rpm_verify_permissions** fails. To work around this problem, manually verify that these files have the following permissions:

- **/etc/cron.d** (0700)
- **/etc/cron.hourly** (0700)
- **/etc/cron.monthly** (0700)
- **/etc/crontab** (0600)
- **/etc/cron.weekly** (0700)
- **/etc/cron.daily** (0700)

For more information about the related feature, see SCAP Security Guide now provides a profile aligned with the CIS RHEL 7 Benchmark v2.2.0.

(BZ#1838622)

OpenSCAP file ownership-related rules do not work with remote user and group back ends

The OVAL language used by the OpenSCAP suite to perform configuration checks has a limited set of capabilities. It lacks possibilities to obtain a complete list of system users, groups, and their IDs if some of them are remote. For example, if they are stored in an external database such as LDAP.

As a consequence, rules that work with user IDs or group IDs do not have access to IDs of remote users. Therefore, such IDs are identified as foreign to the system. This might result in scans to fail on compliant systems. In the **scap-security-guide** packages, the following rules are affected:

- **xccdf_org.ssgproject.content_rule_file_permissions_ungroupowned**
- **xccdf_org.ssgproject.content_rule_no_files_unowned_by_user**

To work around this problem, if a rule that deals with user or group IDs fails on a system that defines remote users, check the failed parts manually. The OpenSCAP scanner enables you to specify the **--oval-results** option together with the **--report** option. This option displays offending files and UIDs in

the HTML report and makes the manual revision process straightforward.

Additionally, in RHEL 8.3, the rules in the **scap-security-guide** packages contain a warning that only local-user back ends have been evaluated.

(BZ#1721439)

rpm_verify_permissions and rpm_verify_ownership fail in the Essential Eight profile

The **rpm_verify_permissions** rule compares file permissions to package default permissions and the **rpm_verify_ownership** rule compares file owner to package default owner. However, the Australian Cyber Security Centre (ACSC) Essential Eight profile, which is provided by the **scap-security-guide** packages, changes some file permissions and ownerships to be more strict than default. As a consequence, verification of certain files using **rpm_verify_permissions** and **rpm_verify_ownership** fails. To work around this problem, manually verify that the **/usr/libexec/abrt-action-install-debuginfo-to-abrt-cache** file is owned by **root** and that it has **suid** and **sgid** bits set.

(BZ#1778661)

8.7. SERVERS AND SERVICES

The compat-unixODBC234 package for SAP requires a symlink to load the unixODBC library

The **unixODBC** package version 2.3.1 is available in RHEL 7. In addition, the **compat-unixODBC234** package version 2.3.4 is available in the RHEL 7 for SAP Solutions **sap-hana** repository; see New package: **compat-unixODBC234** for SAP for details.

Due to minor ABI differences between **unixODBC** version 2.3.1 and 2.3.4, an application built with version 2.3.1 might not work with version 2.3.4 in certain rare cases. To prevent problems caused by this incompatibility, the **compat-unixODBC234** package uses a different SONAME for shared libraries available in this package, and the library file is available under **/usr/lib64/libodbc.so.1002.0.0** instead of **/usr/lib64/libodbc.so.2.0.0**.

As a consequence, third party applications built with **unixODBC** version 2.3.4 that load the **unixODBC** library in runtime using the **dlopen()** function fail to load the library with the following error message:

```
/usr/lib64/libodbc.so.2.0.0: cannot open shared object file: No such file or directory
```

To work around this problem, create the following symbolic link:

```
# ln -s /usr/lib64/libodbc.so.1002.0.0 /usr/lib64/libodbc.so.2.0.0
```

and similar symlinks for other libraries from the **compat-unixODBC234** package if necessary.

Note that the **compat-unixODBC234** package conflicts with the base RHEL 7 **unixODBC** package. Therefore, uninstall **unixODBC** prior to installing **compat-unixODBC234**.

(BZ#1844443)

Symbol conflicts between OpenLDAP libraries might cause crashes in httpd

When both the **libldap** and **libldap_r** libraries provided by OpenLDAP are loaded and used within a single process, symbol conflicts between these libraries might occur. Consequently, Apache **httpd** child processes using the PHP **ldap** extension might terminate unexpectedly if the **mod_security** or **mod_auth_openidc** modules are also loaded by the **httpd** configuration.

With this update to the Apache Portable Runtime (APR) library, you can work around the problem by setting the **APR_DEEPBIND** environment variable, which enables the use of the **RTLD_DEEPBIND** dynamic linker option when loading **httpd** modules. When the **APR_DEEPBIND** environment variable is enabled, crashes no longer occur in **httpd** configurations that load conflicting libraries.

(BZ#1739287)

8.8. STORAGE

RHEL 7 does not support VMD 2.0 storage

The 10th generation Intel Core and 3rd generation Intel Xeon Scalable platforms (also known as Intel Ice Lake) include hardware that utilizes version 2.0 of the Volume Management Device (VMD) technology.

RHEL 7 no longer receives updates to support new hardware. As a consequence, RHEL 7 cannot recognize Non-Volatile Memory Express (NVMe) devices that are managed by VMD 2.0.

To work around the problem, Red Hat recommends that you upgrade to a recent major RHEL release.

(BZ#1942865)

SCSI devices cannot be deleted after removing the iSCSI target

If a SCSI device is **BLOCKED** due to a transport issue, including an iSCSI session being disrupted due to a network or target side configuration change, the attached devices cannot be deleted while blocked on transport error recovery. If you attempt to remove the SCSI device using the **delete sysfs** command (**/sys/block/sd*/device/delete**) it can be blocked indefinitely.

To work around this issue, terminate the transport session with the **iscsiadm logout** commands in either session mode (specifying a session ID) or in node mode (specifying a matching target name and portal for the blocked session). Issuing an iSCSI session logout on a recovering session terminates the session and removes the SCSI devices.

(BZ#1439055)

8.9. SYSTEM AND SUBSCRIPTION MANAGEMENT

The needs-restarting command from yum-utils might fail to display the container boot time

In certain RHEL 7 container environments, the **needs-restarting** command from the **yum-utils** package might incorrectly display the host boot time instead of the container boot time. As a consequence, this command might still report a false reboot warning message after you restart the container environment. You can safely ignore this harmless warning message in such a case.

(BZ#2042313)

8.10. VIRTUALIZATION

RHEL 7.9 virtual machines on IBM POWER sometimes do not detect hot-plugged devices

RHEL7.9 virtual machines (VMs) started on an IBM POWER system on a RHEL 8.3 or later hypervisor do not detect hot-plugged PCI devices if the hot plug is performed when the VM is not fully booted yet. To work around the problem, reboot the VM.

(BZ#1854917)

8.11. RHEL IN CLOUD ENVIRONMENTS

Core dumping RHEL 7 virtual machines that use NICs with enabled accelerated networking to a remote machine on Azure fails

Currently, using the **kdump** utility to save the core dump file of a RHEL 7 virtual machine (VM) on a Microsoft Azure hypervisor to a remote machine does not work correctly when the VM is using a NIC with enabled accelerated networking. As a consequence, the **kdump** operation fails.

To prevent this problem from occurring, add the following line to the **/etc/kdump.conf** file and restart the **kdump** service.

```
extra_modules pci_hyperv
```

(BZ#1846667)

SSH with password login now impossible by default on RHEL 8 virtual machines configured using cloud-init

For security reasons, the **ssh_pwauth** option in the configuration of the **cloud-init** utility is now set to **0** by default. As a consequence, it is not possible to use a password login when connecting via SSH to RHEL 8 virtual machines (VMs) configured using **cloud-init**.

If you require using a password login for SSH connections to your RHEL 8 VMs configured using **cloud-init**, set **ssh_pwauth: 1** in the /etc/cloud/cloud.cfg file before deploying the VM.

(BZ#1685580)

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 7.9.

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
- ctdb-tests
- 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
- langtable-data
- 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-gtk2
- 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-PlRPC
- 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
- rteval-common
- 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
- webkit2gtk3-plugin-process-gtk2
- 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
- mthca
- 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
- qlcnic
- qlge
- 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 Mellanox Gen2 and ConnectX-2 adapters from the **mlx4_core** driver have been deprecated:
  - PCI ID 0x15B3:0x1002
  - PCI ID 0x15B3:0x676E
  - PCI ID 0x15B3:0x6746
  - PCI ID 0x15B3:0x6764
  - PCI ID 0x15B3:0x675A
  - PCI ID 0x15B3:0x6372
  - PCI ID 0x15B3:0x6750
  - PCI ID 0x15B3:0x6368
  - PCI ID 0x15B3:0x673C
  - PCI ID 0x15B3:0x6732
  - PCI ID 0x15B3:0x6354
  - PCI ID 0x15B3:0x634A
  - PCI ID 0x15B3:0x6340
- 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 0x1028:0x0015
  - SAS1078R, PCI ID 0x1000:0x0060
  - SAS1078DE, PCI ID 0x1000:0x007C
  - SAS1064R, PCI ID 0x1000:0x0411
  - VERDE_ZCR, PCI ID 0x1000:0x0413

- SAS1078GEN2, PCI ID 0x1000:0x0078
- SAS0079GEN2, PCI ID 0x1000:0x0079
- SAS0073SKINNY, PCI ID 0x1000:0x0073
- SAS0071SKINNY, PCI ID 0x1000:0x0071

- 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++.

LVM mirror is deprecated

The LVM **mirror** segment type is now deprecated. Support for **mirror** will be removed in a future major release of RHEL.

Red Hat recommends that you use LVM RAID 1 devices with a segment type of **raid1** instead of **mirror**. The **raid1** segment type is the default RAID configuration type and replaces **mirror** as the recommended solution.

To convert **mirror** devices to **raid1**, see Converting a Mirrored LVM Device to a RAID1 Device .

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.

The sap-hana-vmware Tuned profile has been deprecated

The **sap-hana-vmware Tuned** profile has been deprecated. For backward compatibility, this profile is still provided in the **tuned-profiles-sap-hana** package, but the profile will be removed in future major release of Red Hat Enterprise Linux. The recommended replacement is the **sap-hanaTuned** profile.

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]
pam_krb5	sssd

Deprecated packages	Proposed replacement package or product
openldap-servers	Depending on the use case, migrate to Identity Management included in Red Hat Enterprise Linux; or to Red Hat Directory Server. [b]
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] 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.

NSS SEED ciphers have been deprecated

The Mozilla Network Security Services (**NSS**) library will not support Transport Layer Security (TLS) cipher suites that use a SEED cipher in a future release. For deployments that rely on SEED ciphers, Red Hat recommends enabling support for other cipher suites. This way, you ensure smooth transitions when NSS will remove support for them.

Note that the SEED ciphers are already disabled by default in RHEL.

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 repository, 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 repository

Ansible and its dependencies will no longer be updated through the Extras repository. 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 repository 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 repository.

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 repository was not a part of the Red Hat Enterprise Linux FIPS validation process.

The following packages have been deprecated from the Extras repository:

- **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 repository. 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.

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 repository has been deprecated

RHEL 7.5 introduced the **openvswitch-2.0.0-7.el7** package in the RHEL 7 Optional repository 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 repository 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.

The copy_file_range() call has been disabled on local file systems and in NFS

The **copy_file_range()** system call on local file systems contains multiple issues that are difficult to fix. To avoid file corruptions, **copy_file_range()** support on local file systems has been disabled in RHEL 7.8. If an application uses the call in this case, **copy_file_range()** now returns an **ENOSYS** error.

For the same reason, the server-side-copy feature has been disabled in the NFS server. However, the NFS client still supports **copy_file_range()** when accessing a server that supports server-side-copy.

The ipv6, netmask, gateway, and hostname kernel parameters have been deprecated

The **ipv6**, **netmask**, **gateway**, and **hostname** parameters to set the network configuration in the kernel command line have been deprecated. RHEL 8 supports only the consolidated **ip** parameter that accepts different formats, such as the following:

```
ip=__IP_address__:__peer__:__gateway_IP_address__:__net_mask__:__host_name__:__interface_name__:__configuration_method__
```

For further details about the individual fields and other formats this parameter accepts, see the description of the **ip** parameter in the **dracut.cmdline(7)** man page.

Note that you can already use the consolidated **ip** parameter in RHEL 7.

The hidepid=n mount option is not recommended in RHEL 7

The mount option **hidepid=n**, which controls who can access information in **/proc/[pid]** directories, is not compatible with **systemd** provided in RHEL 7 and newer.

In addition, using this option might cause certain services started by **systemd** to produce SELinux AVC denial messages and prevent other operations from completing.

For more information, see the related Is mounting /proc with "hidepid=2" recommended with RHEL7 and RHEL8?.

The -s split option is no longer supported with the -f option

When providing files to **Red Hat Support** by uploading them to **Red Hat Secure FTP**, you can run the **redhat-support-tool addattachment -f** command. Due to infrastructure changes introduced in the RHBA-2022:0623 advisory, you can no longer use the **-s** option with this command for splitting big files into parts and uploading them to **Red Hat Secure FTP**.

The redhat-support-tool diagnose <file_or_directory> command has been deprecated

With the release of the RHBA-2022:0623 advisory, the **Red Hat Support Tool** no longer supports the **redhat-support-tool diagnose <file_or_directory>** command previously used for advanced diagnostic services for files or directories. The **redhat-support-tool diagnose** command continues to support the plain text analysis.

APPENDIX A. COMPONENT VERSIONS

This appendix provides a list of key components and their versions in the Red Hat Enterprise Linux 7.9 release.

Table A.1. Component Versions

Component	Version
kernel	3.10.0-1160
kernel-alt	4.14.0-115
QLogic **qla2xxx** driver	10.01.00.22.07.9-k
QLogic **qla4xxx** driver	5.04.00.00.07.02-k0
Emulex **lpfc** driver	0:12.0.0.13
iSCSI initiator utils (**iscsi-initiator-utils**)	6.2.0.874-19
DM-Multipath (**device-mapper-multipath**)	0.4.9-133
LVM (**lvm2**)	2.02.187-6
qemu-kvm[a]	1.5.3-175
qemu-kvm-ma[b]	2.12.0-33

[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

Bugzilla and JIRA IDs are listed in this document for reference. Bugzilla bugs that are publicly accessible include a link to the ticket.

Component	Tickets
389-ds-base	BZ#1801327, BZ#1700987, BZ#1796558, BZ#1769418, BZ#1807537, BZ#1837105, BZ#1824930, BZ#1827284
ansible	BZ#1767177, BZ#1439896, BZ#1660838
apr	BZ#1739287
bind	BZ#1744081, BZ#1758317, BZ#1853191, BZ#1851836
cloud-init	BZ#1772505, BZ#1685580
cloud	BZ#1846667, BZ#1348508
corosync	BZ#1413573
criu	BZ#1400230
cups	BZ#1672212
custodia	BZ#1403214
desktop	BZ#1481411
dnf	BZ#1461652
fence-agents	BZ#1476401
filesystems	BZ#1274459, BZ#1111712, BZ#1206277, BZ#1477977
firewalld	BZ#1796055, BZ#1754117
freerdp	BZ#1834286
gnome-shell	BZ#1481395
hardware-enablement	BZ#1062759, BZ#1384452, BZ#1519746, BZ#1454918, BZ#1454916
identity-management	BZ#1819745, BZ#1405325
ipa	BZ#1115294, BZ#1298286, BZ#1518939

Component	Tickets
iptables	BZ#1851944
iscsi-initiator-utils	BZ#1439055
kernel-rt	BZ#1790643
kernel	BZ#1801759, BZ#1781726, BZ#1514705, BZ#1855010, BZ#1807077, BZ#1770232, BZ#1829777, BZ#1836292, BZ#1168430, BZ#1706522, BZ#1813394, BZ#1844522, BZ#1838903, BZ#1862840, BZ#1871027, BZ#1874101, BZ#1933998, BZ#1559615, BZ#1230959, BZ#1460849, BZ#1464377, BZ#1457533, BZ#1503123, BZ#1589397, BZ#1726642
kexec-tools	BZ#1773478
krb5	BZ#1733289, BZ#1782492
libguestfs	BZ#1387213
libreswan	BZ#1375750
libvirt	BZ#1475770
mariadb	BZ#1834835
networking	BZ#1062656, BZ#916384, BZ#916382, BZ#755087, BZ#1259547, BZ#1393375
nss	BZ#1431210, BZ#1425514, BZ#1432142
openscap	BZ#1478285, BZ#1640522, BZ#1829782
openssh	BZ#1828598
oscap-anaconda-addon	BZ#1648162
ovmf	BZ#653382
pacemaker	BZ#1792492
pcp	BZ#1775373
pcs	BZ#1433016
perl	BZ#1751381, BZ#1806523

Component	Tickets
pki-core	BZ#1768718, BZ#1487418
resource-agents	BZ#1513957
scap-security-guide	BZ#1821633, BZ#1791583, BZ#1665233, BZ#1958789, BZ#1955180, BZ#1691877, BZ#1494606, BZ#1609014, BZ#1776780, BZ#1890111, BZ#1942281, BZ#1838622, BZ#1721439, BZ#1778661, BZ#1891435, BZ#1976123
security	BZ#1421794, BZ#1832194
selinux-policy	BZ#1770123, BZ#1780332, BZ#1775573
services	BZ#1790655, BZ#1844443
sssd	BZ#1796352, BZ#1068725
storage	BZ#1649493, BZ#1942865, BZ#1109348, BZ#1119909, BZ#1414957
systemd	BZ#1284974
tang	BZ#1703445
tools	BZ#1569484
tuned	BZ#1702724, BZ#1776149
unbound	BZ#2121623
usbguard	BZ#1480100
vdo	BZ#1706154
virtualization	BZ#1854917, BZ#1103193, BZ#1299662, BZ#1661654
yum-utils	BZ#2042313
yum	BZ#1708628, BZ#1778784

APPENDIX C. REVISION HISTORY

0.3-3

Fri Apr 28 2023, Lucie Vařáková (lvarakova@redhat.com)

- Added a known issue JIRA:RHELPLAN-155168 (Authentication and Interoperability).

0.3-2

Wed Oct 19 2022, Lenka Špačková (lspackova@redhat.com)

- Added information on how to configure **unbound** to run inside **chroot**, BZ#2121623 (Networking).

0.3-1

Wed Sep 21 2022, Lenka Špačková (lspackova@redhat.com)

- Added two new ehnancements, BZ#1967950 and BZ#1993822 (Security).

0.3-0

Fri Apr 22 2022, Lenka Špačková (lspackova@redhat.com)

- Added two deprecated packages to Deprecated Functionality.

0.2-9

Thu Feb 17 2022, Lenka Špačková (lspackova@redhat.com)

- Added two notes related to supportability to Deprecated Functionality.

0.2-8

Tue Feb 08 2022, Lenka Špačková (lspackova@redhat.com)

- Added information about the **hidepid=n** mount option not being recommended in RHEL 7 to Deprecated Functionality.

0.2-7

Wed Jan 26 2022, Lenka Špačková (lspackova@redhat.com)

- Added a known issue BZ#2042313 (System and Subscription Management).

0.2-6

Tue Dec 07 2021, Lenka Špačková (lspackova@redhat.com)

- Added a bug fix BZ#1942281 (Security).
- Changed a previous known issue to a bug fix BZ#1976123 (Security).

0.2-5

Tue Aug 17 2021, Lenka Špačková (lspackova@redhat.com)

- Updated the Red Hat Software Collections section.

0.2-4

Wed Jul 21 2021, Lenka Špačková (lspackova@redhat.com)

- Added enhancements BZ#1958789 and BZ#1955180 (Security).

0.2-3

Mon Jul 12 2021, Lenka Špačková (lspackova@redhat.com)

- Added a known issue BZ#1976123 (Security).

0.2-2

Thu Jun 03 2021, Lenka Špačková (lspackova@redhat.com)

- Added a known issue BZ#1933998 (Kernel).
- Added a bug fix BZ#1890111 (Security).

0.2-1

Fri May 21 2021, Lenka Špačková (lspackova@redhat.com)

- Updated information about OS conversion in Overview.

0.2-0

Wed Apr 28 2020, Lenka Špačková (lspackova@redhat.com)

- Added a bug fix BZ#1891435 (Security).

0.1-9

Mon Apr 26 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue BZ#1942865 (Storage).

0.1-8

Tue Apr 06 2021, Lenka Špačková (lspackova@redhat.com)

- Improved the list of supported architectures.

0.1-7

Wed Mar 31 2021, Lenka Špačková (lspackova@redhat.com)

- Updated information about OS conversions with the availability of the supported **Convert2RHEL** utility.

0.1-6

Tue Mar 30 2021, Lenka Špačková (lspackova@redhat.com)

- Added a known issue (Kernel).

0.1-5

Tue Mar 02 2021, Lenka Špačková (lspackova@redhat.com)

- Updated a link to Upgrading from RHEL 6 to RHEL 7 .
- Fixed CentOS Linux name.

0.1-4

Wed Feb 03 2021, Lenka Špačková (lspackova@redhat.com)

- Added a note about deprecated parameters for the network configuration in the kernel command line.

0.1-3

Tue Feb 02 2021, Lenka Špačková (lspackova@redhat.com)

- Added a retirement notice for **Red Hat Enterprise Linux Atomic Host**.

0.1-2

Thu Jan 28 2021, Lenka Špačková (lspackova@redhat.com)

- Added a note related to the new **page_owner** kernel parameter.

0.1-1

Tue Jan 19 2021, Lenka Špačková (lspackova@redhat.com)

- Updated deprecated packages.

0.1-0

Wed Dec 16 2020, Lenka Špačková (lspackova@redhat.com)

- Added **mthca** to deprecated drivers.

0.0-9

Tue Dec 15 2020, Lenka Špačková (lspackova@redhat.com)

- Added information about the STIG security profile update (Security).

0.0-8

Wed Nov 25 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue (Security).

0.0-7

Wed Nov 11 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue (RHEL in cloud environments).

0.0-6

Tue Oct 13 2020, Lenka Špačková (lspackova@redhat.com)

- Updated deprecated adapters.
- Fixed a driver name in a Technology Preview note (**iavf**).

0.0-5

Tue Sep 29 2020, Lenka Špačková (lspackova@redhat.com)

- Release of the Red Hat Enterprise Linux 7.9 Release Notes.

0.0-4

Mon Sep 7 2020, Jaroslav Klech (jklech@redhat.com)

- Provided the correct expansion of BERT in the kernel parameters section.

0.0-3

Thu Jun 25 2020, Lenka Špačková (lspackova@redhat.com)

- Added a known issue related to OpenLDAP libraries (Servers and Services).

0.0-2

Tue Jun 23 2020, Jaroslav Klech (jklech@redhat.com)

- Added and granulated the kernel parameters chapter. Added the device drivers chapter.

0.0-1

Thu Jun 18 2020, Lenka Špačková (lspackova@redhat.com)

- Various additions.

0.0-0

Wed May 20 2020, Lenka Špačková (lspackova@redhat.com)

- Release of the Red Hat Enterprise Linux 7.9 Beta Release Notes.