Red Hat Enterprise Linux 8.4

8.4 Release Notes

Release Notes for Red Hat Enterprise Linux 8.4

Last Updated: 2024-05-23

Red Hat Enterprise Linux 8.4 8.4 Release Notes

Release Notes for Red Hat Enterprise Linux 8.4

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 8.4 and document known problems in this release, as well as notable bug fixes, Technology Previews, deprecated functionality, and other details.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE 5

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION 6

CHAPTER 1. OVERVIEW 7
1.1. MAJOR CHANGES IN RHEL 8.4 7
Security 7
Networking 7
Kernel 7
High availability and clusters 8
Dynamic programming languages, web and database servers 8
Compilers and development tools 8
OpenJDK 11 is now available 8
Identity Management 8
1.2. IN-PLACE UPGRADE AND OS CONVERSION 9
In-place upgrade from RHEL 7 to RHEL 8 9
In-place upgrade from RHEL 6 to RHEL 8 9
Conversion from a different Linux distribution to RHEL 9
1.3. RED HAT CUSTOMER PORTAL LABS 9
1.4. ADDITIONAL RESOURCES 10

CHAPTER 2. ARCHITECTURES 11

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 8 12
3.1. INSTALLATION 12
3.2. REPOSITORIES 12
3.3. APPLICATION STREAMS 13
3.4. PACKAGE MANAGEMENT WITH YUM/DNF 13

CHAPTER 4. NEW FEATURES 14
4.1. INSTALLER AND IMAGE CREATION 14
4.2. RHEL FOR EDGE 14
4.3. SOFTWARE MANAGEMENT 15
4.4. SHELLS AND COMMAND-LINE TOOLS 16
4.5. INFRASTRUCTURE SERVICES 19
4.6. SECURITY 22
4.7. NETWORKING 26
4.8. KERNEL 29
4.9. FILE SYSTEMS AND STORAGE 37
4.10. HIGH AVAILABILITY AND CLUSTERS 40
4.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 41
4.12. COMPILERS AND DEVELOPMENT TOOLS 49
4.13. IDENTITY MANAGEMENT 58
4.14. DESKTOP 63
4.15. GRAPHICS INFRASTRUCTURES 64
4.16. THE WEB CONSOLE 66
4.17. RED HAT ENTERPRISE LINUX SYSTEM ROLES 67
4.18. VIRTUALIZATION 69
4.19. RHEL IN CLOUD ENVIRONMENTS 70
4.20. SUPPORTABILITY 70
4.21. CONTAINERS 72

CHAPTER 5. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS 74

5.1. NEW KERNEL PARAMETERS 74
5.2. NEW /PROC/SYS/USER PARAMETERS 75
5.3. NEW /PROC/SYS/VM PARAMETERS 75

CHAPTER 6. DEVICE DRIVERS 77
6.1. NEW DRIVERS 77
Network drivers 77
Graphics drivers and miscellaneous drivers 77
6.2. UPDATED DRIVERS 78
Graphics and miscellaneous driver updates 78

CHAPTER 7. BUG FIXES 79
7.1. INSTALLER AND IMAGE CREATION 79
7.2. SOFTWARE MANAGEMENT 80
7.3. SHELLS AND COMMAND-LINE TOOLS 80
7.4. INFRASTRUCTURE SERVICES 81
7.5. SECURITY 81
7.6. NETWORKING 84
7.7. KERNEL 85
7.8. FILE SYSTEMS AND STORAGE 87
7.9. HIGH AVAILABILITY AND CLUSTERS 88
7.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 88
7.11. COMPILERS AND DEVELOPMENT TOOLS 88
7.12. IDENTITY MANAGEMENT 89
7.13. GRAPHICS INFRASTRUCTURES 90
7.14. RED HAT ENTERPRISE LINUX SYSTEM ROLES 91
7.15. VIRTUALIZATION 91
7.16. RHEL IN CLOUD ENVIRONMENTS 91
7.17. CONTAINERS 92

CHAPTER 8. TECHNOLOGY PREVIEWS 94
8.1. INSTALLER AND IMAGE CREATION 94
8.2. NETWORKING 94
8.3. KERNEL 97
8.4. FILE SYSTEMS AND STORAGE 98
8.5. HIGH AVAILABILITY AND CLUSTERS 100
8.6. IDENTITY MANAGEMENT 101
8.7. DESKTOP 103
8.8. GRAPHICS INFRASTRUCTURES 104
8.9. RED HAT ENTERPRISE LINUX SYSTEM ROLES 104
8.10. VIRTUALIZATION 105
8.11. CONTAINERS 106

CHAPTER 9. DEPRECATED FUNCTIONALITY 108
9.1. INSTALLER AND IMAGE CREATION 108
9.2. SOFTWARE MANAGEMENT 109
9.3. SHELLS AND COMMAND-LINE TOOLS 109
9.4. SECURITY 110
9.5. NETWORKING 111
9.6. KERNEL 112
9.7. PLATFORM ENABLEMENT 112
9.8. FILE SYSTEMS AND STORAGE 112
9.9. HIGH AVAILABILITY AND CLUSTERS 114
9.10. COMPILERS AND DEVELOPMENT TOOLS 114

9.11. IDENTITY MANAGEMENT 115
9.12. DESKTOP 117
9.13. GRAPHICS INFRASTRUCTURES 117
9.14. THE WEB CONSOLE 117
9.15. RED HAT ENTERPRISE LINUX SYSTEM ROLES 117
9.16. VIRTUALIZATION 118
9.17. CONTAINERS 119
9.18. DEPRECATED PACKAGES 119
9.19. DEPRECATED DEVICES 121

CHAPTER 10. KNOWN ISSUES 124
10.1. INSTALLER AND IMAGE CREATION 124
10.2. SUBSCRIPTION MANAGEMENT 127
10.3. INFRASTRUCTURE SERVICES 128
10.4. SECURITY 128
10.5. NETWORKING 134
10.6. KERNEL 134
10.7. HARDWARE ENABLEMENT 139
10.8. FILE SYSTEMS AND STORAGE 139
10.9. HIGH AVAILABILITY AND CLUSTERS 141
10.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 141
10.11. COMPILERS AND DEVELOPMENT TOOLS 142
10.12. IDENTITY MANAGEMENT 143
10.13. DESKTOP 145
10.14. GRAPHICS INFRASTRUCTURES 146
10.15. VIRTUALIZATION 147
10.16. RHEL IN CLOUD ENVIRONMENTS 150
10.17. SUPPORTABILITY 153

CHAPTER 11. INTERNATIONALIZATION 154
11.1. RED HAT ENTERPRISE LINUX 8 INTERNATIONAL LANGUAGES 154
11.2. NOTABLE CHANGES TO INTERNATIONALIZATION IN RHEL 8 154

APPENDIX A. LIST OF TICKETS BY COMPONENT 156

APPENDIX B. REVISION HISTORY 165

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

Submitting feedback through Jira (account required)

1. Log in to the Jira website.
2. Click **Create** in the top navigation bar.
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. Click **Create** at the bottom of the dialogue.

CHAPTER 1. OVERVIEW

1.1. MAJOR CHANGES IN RHEL 8.4

Security

IPsec VPN provided by Libreswan now supports TCP encapsulation and security labels for IKEv2.

The **scap-security-guide** packages have been rebased to version 0.1.54, and **OpenSCAP** has been rebased to version 1.3.4. These updates provide substantial improvements, including:

- Improved memory management
- Added RHEL8 ANSSI-BP-028 Minimal, Intermediary and Enhanced profiles
- Updated RHEL8 STIG profile to DISA STIG v1r1

The **fapolicyd** framework now provides **integrity checking**, and the RPM plugin now registers any system update that is handled by either the YUM package manager or the RPM Package Manager.

The **rhel8-tang** container image provides Tang-server decryption capabilities for Clevis clients that run either in OpenShift Container Platform (OCP) clusters or in separate virtual machines.

See Section 4.6, “Security” for more information.

Networking

Nmstate is a network API for hosts and fully supported in RHEL 8.4. The **nmstate** packages provide a library and the **nmstatectl** command-line utility to manage host network settings in a declarative manner.

The Multi-protocol Label Switching (MPLS) is an in-kernel data-forwarding mechanism to route traffic flow across enterprise networks. For example, you can add **tc filters** for managing packets received from specific ports or carrying specific types of traffic, in a consistent way. The MPLS support is available in this release as a Technology Preview.

The **iproute2** utility introduces three new traffic control (**tc**) actions; **mac_push**, **push_eth**, and **pop_eth** to add MPLS labels, build an Ethernet header at the beginning of the packet, and drop the outer Ethernet header respectively.

The support for **bareudp** devices is now available with the **ip link** command as a Technology Preview.

For more information about the features introduced in this release and changes in the existing functionality, see Section 4.7, “Networking”.

Kernel

The **kpatch-dnf** package provides a **DNF** plugin for subscribing a RHEL system to kernel live patch updates. The plugin enables automatic subscription for any kernel the system currently uses, and also for kernels to-be-installed in the future.

Proactive compaction regularly initiates memory compaction work **before** a request for allocation is made. Therefore, latency for specific memory allocation requests is lowered.

A new implementation of slab memory controller for the **control groups** technology is now available in RHEL 8. The slab memory controller brings improvement in slab utilization, and enables to shift the memory accounting from the page level to the object level. As a result, you can observe a significant drop in the total kernel memory footprint and positive effects on memory fragmentation.

The time namespace feature is available in RHEL 8.4. This feature is suited for changing the date and time inside Linux containers. The in-container clock adjustments after restoration from a checkpoint are also now possible.

RHEL 8 supports the Error Detection and Correction (EDAC) kernel module set in 8th and 9th generation Intel Core Processors.

For more information about the features introduced in this release and changes in the existing functionality, see Section 4.8, "Kernel".

High availability and clusters

A persistent Pacemaker resource agent that maintains state data can detect failures asynchronously and inject a failure into Pacemaker immediately without waiting for the next monitor interval. A persistent resource agent can also speed up cluster response time for services with a high state overhead, since maintaining state data can reduce the state overhead for cluster actions such as start, stop, and monitor by not invoking the state separately for each action.

For information on creating a persistent Pacemaker resource agent, you can now consult the article Creating a Persistent (Daemonized) Pacemaker Resource Agent .

Dynamic programming languages, web and database servers

Later versions of the following components are now available as new module streams:

- **Python 3.9**
- **SWIG 4.0**
- **Subversion 1.14**
- **Redis 6**
- **PostgreSQL 13**
- **MariaDB 10.5**

See Section 4.11, "Dynamic programming languages, web and database servers" for more information.

Compilers and development tools

The following compiler toolsets have been updated:

- **GCC Toolset 10**
- **LLVM Toolset 11.0.0**
- **Rust Toolset 1.49.0**
- **Go Toolset 1.15.7**

See Section 4.12, "Compilers and development tools" for more information.

OpenJDK 11 is now available

A new version of Open Java Development Kit (OpenJDK) is now available. For more information about the features introduced in this release and changes in the existing functionality, see OpenJDK documentation.

Identity Management

RHEL 8.4 provides Ansible modules for automated management of role-based access control (RBAC) in Identity Management (IdM), an Ansible role for backing up and restoring IdM servers, and an Ansible module for location management.

See Section 4.13, "Identity Management" for more information.

1.2. IN-PLACE UPGRADE AND OS CONVERSION

In-place upgrade from RHEL 7 to RHEL 8

The supported in-place upgrade paths currently are:

- From RHEL 7.9 to RHEL 8.4 on the 64-bit Intel, IBM POWER 8 (little endian), and IBM Z architectures
- From RHEL 7.6 to RHEL 8.4 on architectures that require kernel version 4.14: IBM POWER 9 (little endian) and IBM Z (Structure A)
- From RHEL 7.7 to RHEL 8.2 on systems with SAP HANA. To ensure your system with SAP HANA remains supported after upgrading to RHEL 8.2, enable the RHEL 8.2 Update Services for SAP Solutions (E4S) repositories.

For more information, see Supported in-place upgrade paths for Red Hat Enterprise Linux . For instructions on performing an in-place upgrade, see Upgrading from RHEL 7 to RHEL 8 .

With the release of RHEL 8.4, additional required data files are now downloaded automatically from cloud.redhat.com if you are using Red Hat Subscription Manager (RHSM) and have not previously downloaded older required data files without performing the upgrade.

In-place upgrade from RHEL 6 to RHEL 8

To upgrade from RHEL 6.10 to RHEL 8.4, follow instructions in Upgrading from RHEL 6 to RHEL 8 .

Conversion from a different Linux distribution to RHEL

If you are using CentOS Linux 8 or Oracle Linux 8, you can convert your operating system to RHEL 8 using the Red Hat-supported **Convert2RHEL** utility. For more information, see Converting from an RPM-based Linux distribution to RHEL.

If you are using an earlier version of CentOS Linux or Oracle Linux, namely versions 6 or 7, you can convert your operating system to RHEL and then perform an in-place upgrade to RHEL 8. Note that CentOS Linux 6 and Oracle Linux 6 conversions use the unsupported **Convert2RHEL** utility. For more information on unsupported conversions, see How to convert from CentOS Linux 6 or Oracle Linux 6 to RHEL 6.

For information regarding how Red Hat supports conversions from other Linux distributions to RHEL, see the Convert2RHEL Support Policy document .

1.3. RED HAT CUSTOMER PORTAL LABS

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

- Registration Assistant
- Product Life Cycle Checker

- Kickstart Generator
- Kickstart Converter
- 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
- Red Hat Memory Analyzer
- Kernel Oops Analyzer
- Red Hat Product Errata Advisory Checker

1.4. ADDITIONAL RESOURCES

- **Capabilities and limits** of Red Hat Enterprise Linux 8 as compared to other versions of the system are available in the Knowledgebase article Red Hat Enterprise Linux technology capabilities and limits.
- Information regarding the Red Hat Enterprise Linux **life cycle** is provided in the Red Hat Enterprise Linux Life Cycle document.
- The Package manifest document provides a **package listing** for RHEL 8.
- Major **differences between RHEL 7 and RHEL 8** are documented in Considerations in adopting RHEL 8.
- Instructions on how to perform an **in-place upgrade from RHEL 7 to RHEL 8** are provided by the document Upgrading from RHEL 7 to RHEL 8 .
- The **Red Hat Insights** service, which enables you to proactively identify, examine, and resolve known technical issues, is now available with all RHEL subscriptions. For instructions on how to install the Red Hat Insights client and register your system to the service, see the Red Hat Insights Get Started page.

CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 8.4 is distributed with the kernel version 4.18.0-305, which provides support for the following architectures:

- AMD and Intel 64-bit architectures
- The 64-bit ARM architecture
- IBM Power Systems, Little Endian
- 64-bit IBM Z

Make sure you purchase the appropriate subscription for each architecture. For more information, see Get Started with Red Hat Enterprise Linux - additional architectures . For a list of available subscriptions, see Subscription Utilization on the Customer Portal.

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 8

3.1. INSTALLATION

Red Hat Enterprise Linux 8 is installed using ISO images. Two types of ISO image are available for the AMD64, Intel 64-bit, 64-bit ARM, IBM Power Systems, and IBM Z architectures:

- Binary DVD ISO: A full installation image that contains the BaseOS and AppStream repositories and allows you to complete the installation without additional repositories.

NOTE

The Binary DVD ISO image is larger than 4.7 GB, and as a result, it might not fit on a single-layer DVD. A dual-layer DVD or USB key is recommended when using the Binary DVD ISO image to create bootable installation media. You can also use the Image Builder tool to create customized RHEL images. For more information about Image Builder, see the *Composing a customized RHEL system image* document.

- Boot ISO: A minimal boot ISO image that is used to boot into the installation program. This option requires access to the BaseOS and AppStream repositories to install software packages. The repositories are part of the Binary DVD ISO image.

See the Performing a standard RHEL 8 installation document for instructions on downloading ISO images, creating installation media, and completing a RHEL installation. For automated Kickstart installations and other advanced topics, see the Performing an advanced RHEL 8 installation document.

3.2. REPOSITORIES

Red Hat Enterprise Linux 8 is distributed through two main repositories:

- BaseOS
- AppStream

Both repositories are required for a basic RHEL installation, and are available with all RHEL subscriptions.

Content in the BaseOS repository is intended to provide the core set of the underlying OS functionality that provides the foundation for all installations. This content is available in the RPM format and is subject to support terms similar to those in previous releases of RHEL. For a list of packages distributed through BaseOS, see the Package manifest.

Content in the Application Stream repository includes additional user space applications, runtime languages, and databases in support of the varied workloads and use cases. Application Streams are available in the familiar RPM format, as an extension to the RPM format called *modules*, or as Software Collections. For a list of packages available in AppStream, see the Package manifest.

In addition, the CodeReady Linux Builder repository is available with all RHEL subscriptions. It provides additional packages for use by developers. Packages included in the CodeReady Linux Builder repository are unsupported.

For more information about RHEL 8 repositories, see the Package manifest.

3.3. APPLICATION STREAMS

Red Hat Enterprise Linux 8 introduces the concept of Application Streams. Multiple versions of user space components are now delivered and updated more frequently than the core operating system packages. This provides greater flexibility to customize Red Hat Enterprise Linux without impacting the underlying stability of the platform or specific deployments.

Components made available as Application Streams can be packaged as modules or RPM packages and are delivered through the AppStream repository in RHEL 8. Each Application Stream component has a given life cycle, either the same as RHEL 8 or shorter. For details, see Red Hat Enterprise Linux Life Cycle.

Modules are collections of packages representing a logical unit: an application, a language stack, a database, or a set of tools. These packages are built, tested, and released together.

Module streams represent versions of the Application Stream components. For example, several streams (versions) of the PostgreSQL database server are available in the **postgresql** module with the default **postgresql:10** stream. Only one module stream can be installed on the system. Different versions can be used in separate containers.

Detailed module commands are described in the Installing, managing, and removing user-space components document. For a list of modules available in AppStream, see the Package manifest.

3.4. PACKAGE MANAGEMENT WITH YUM/DNF

On Red Hat Enterprise Linux 8, installing software is ensured by the **YUM** tool, which is based on the **DNF** technology. We deliberately adhere to usage of the **yum** term for consistency with previous major versions of RHEL. However, if you type **dnf** instead of **yum**, the command works as expected because **yum** is an alias to **dnf** for compatibility.

For more details, see the following documentation:

- Installing, managing, and removing user-space components
- Considerations in adopting RHEL 8

CHAPTER 4. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 8.4.

4.1. INSTALLER AND IMAGE CREATION

Anaconda replaces the original boot device NVRAM variable list with new values

Previously, booting from NVRAM could lead to boot system failure due to the entries with the incorrect **values** in the boot device list.

With this update the problem is fixed, but the previous list of devices is cleared when updating the boot device NVRAM variable.

(BZ#1854307)

Graphical installation of KVM virtual machines on IBM Z is now available

When using the KVM hypervisor on IBM Z hardware, you can now use the graphical installation when creating virtual machines (VMs).

Now, when a user executes the installation in KVM, and QEMU provides a **virtio-gpu** driver, the installer automatically starts the graphical console. The user can switch to text or VNC mode by appending the **inst.text** or **inst.vnc** boot parameters in the VM's kernel command line.

(BZ#1609325)

Warnings for deprecated kernel boot arguments

Anaconda boot arguments without the **inst.** prefix (for example, **ks**, **stage2**, **repo** and so on) are deprecated starting RHEL7. These arguments will be removed in the next major RHEL release.

With this release, appropriate warning messages are displayed when the boot arguments are used without the **inst** prefix. The warning messages are displayed in **dracut** when booting the installation and also when the installation program is started on a terminal.

Following is a sample warning message that is displayed on a terminal:

Deprecated boot argument **%s** must be used with the **inst.** prefix. Please use **inst.%s** instead. Anaconda boot arguments without **inst.** prefix have been deprecated and will be removed in a future major release.

Following is a sample warning message that is displayed in **dracut**:

$1 has been deprecated. All usage of Anaconda boot arguments without the **inst.** prefix have been deprecated and will be removed in a future major release. Please use **$2** instead.

(BZ#1897657)

4.2. RHEL FOR EDGE

Support to specify the kernel name as customization for RHEL for Edge image types

When creating OSTree commits for **RHEL for Edge** images, only one kernel package can be installed at a time, otherwise the commit creation fails in **rpm-ostree**. This prevents RHEL for Edge from adding alternative kernels, in particular, the real-time kernel (**kernel-rt**). With this enhancement, when creating a

blueprint for RHEL for Edge image using the CLI, you can define the name of the kernel to be used in an image, by setting the **customizations.kernel.name** key. If you do not specify any kernel name, the image include the default kernel package.

(BZ#1960043)

4.3. SOFTWARE MANAGEMENT

New fill_sack_from_repos_in_cache function is now supported in DNF API

With this update, the new DNF API **fill_sack_from_repos_in_cache** function has been introduced which allows to load repositories only from the cached **solv**, **solvx** files, and the **repomd.xml** file. As a result, if the user manages **dnf** cache, it is possible to save resources without having duplicate information (**xml** and **solv**), and without processing **xml** into **solv**.

(BZ#1865803)

createrepo_c now automatically adds modular metadata to repositories

Previously, running the **createrepo_c** command on RHEL8 packages to create a new repository did not include modular repodata in this repository. Consequently, it caused various problems with repositories. With this update, **createrepo_c**:

- scans for modular metadata
- merges the found module YAML files into a single modular document **modules.yaml**
- automatically adds this document to the repository.

As a result, adding modular metadata to repositories is now automatic and no longer has to be done as a separate step using the **modifyrepo_c** command.

(BZ#1795936)

The ability to mirror a transaction between systems within DNF is now supported

With this update, the user can store and replay a transaction within DNF.

- To store a transaction from DNF history into a JSON file, run the **dnf history store** command.
- To replay the transaction later on the same machine, or on a different one, run the **dnf history replay** command.

Comps groups operations storing and replaying is supported. Module operations are not yet supported, and consequently, are not stored or replayed.

(BZ#1807446)

createrepo_c rebased to version 0.16.2

The **createrepo_c** packages have been rebased to version 0.16.2 which provides the following notable changes over the previous version:

- Added module metadata support for **createrepo_c**.
- Fixed various memory leaks

(BZ#1894361)

The protect_running_kernel configuration option is now available.

With this update, the **protect_running_kernel** configuration option for the **dnf** and **microdnf** commands has been introduced. This option controls whether the package corresponding to the running version of the kernel is protected from removal. As a result, the user can now disable protection of the running kernel.

(BZ#1698145)

4.4. SHELLS AND COMMAND-LINE TOOLS

OpenIPMI rebased to version 2.0.29

The **OpenIPMI** packages have been upgraded to version 2.0.29. Notable changes over the previous version include:

- Fixed memory leak, variable binding, and missing error messages.
- Added support for **IPMB**.
- Added support for registration of individual group extension in the **lanserv**.

(BZ#1796588)

freeipmi rebased to version 1.6.6

The **freeipmi** packages have been upgraded to version 1.6.6. Notable changes over the previous version include:

- Fixed memory leaks and typos in the source code.
- Implemented workarounds for the following known issues:
  - unexpected completion code.
  - Dell Poweredge FC830.
  - out of order packets with **lan/rmcpplus ipmb**.
- Added support for new Dell, Intel, and Gigabyte devices.
- Added support for the interpretation of system information and events.

(BZ#1861627)

opal-prd rebased to version 6.6.3

The **opal-prd** package has been rebased to version 6.6.3. Notable changes include:

- Added an offline worker process handle page for **opal-prd** daemon.
- Fixed the bug for **opal-gard** on **POWER9P** so that the system can identify the chip targets for **gard** records.
- Fixed false negatives in **wait_for_all_occ_init()** of **occ** command.
- Fixed **OCAPI_MEM BAR** values in **hw/phys-map**.

- Fixed warnings for **Inconsistent MSAREA** in **hdata/memory.c**.
- For sensors in occ:
  - Fixed sensor values zero bug.
  - Fixed the GPU detection code.
- Skipped **sysdump** retrieval in **MPIPL** boot.
- Fixed **IPMI** double-free in the **Mihawk** platform.
- Updated **non-MPIPL scenario** in **fsp/dump**.
- For hw/phb4:
  - Verified AER support before initialising AER regs.
  - Enabled error reporting.
- Added new **smp-cable-connector** VPD keyword in **hdata**.

(BZ#1844427)

opencryptoki rebased to version 3.15.1

The **opencryptoki** packages have been rebased to version 3.15.1. Notable changes include:

- Fixed segfault in **C_SetPin**.
- Fixed usage of **EVP_CipherUpdate** and **EVP_CipherFinal**.
- Added utility to migrate the token repository to **FIPS** compliant encryption.
- For **pkcstok_migrate** tool:
  - Fixed **NVTOK.DAT** conversion on Little Endian platforms.
  - Fixed private and public token object conversion on Little Endian platforms.
- Fixed storing of public token objects in the new data format.
- Fixed the parameter checking mechanism in **dh_pkcs_derive**.
- Corrected soft token model name.
- Replaced deprecated OpenSSL interfaces in **mech_ec.c** file and in **ICA**, **TPM**, and Soft tokens.
- Replaced deprecated OpenSSL AES/3DES interfaces in **sw_crypt.c** file.
- Added support for ECC mechanism in Soft token.
- Added IBM specific SHA3 HMAC and SHA512/224/256 HMAC mechanisms in the Soft token.
- Added support for key wrapping with **CKM_RSA_PKCS** in CCA.
- For EP11 crypto stack:
  - Fixed **ep11_get_keytype** to recognize **CKM_DES2_KEY_GEN**.

    - Fixed error trace in **token_specific_rng**.
    - Enabled specific FW version and API in HSM simulation.
- Fixed Endian bug in **X9.63 KDF**.
- Added an error message for handling **p11sak remove-key command**.
- Fixed compiling issues with C++.
- Fixed the problem with **C_Get/SetOperationState** and digest contexts.
- Fixed **pkcscca** migration fails with **usr/sb2**.

(BZ#1847433)

powerpc-utils rebased to version 1.3.8

The **powerpc-utils** packages have been rebased to version 1.3.8. Notable changes include:

- Commands that do not depend on **Perl** are now moved to the core subpackage.
- Added support for Linux Hybrid Network Virtualization.
- Updated safe bootlist.
- Added **vcpustat** utility.
- Added support for **cpu-hotplug** in **lparstat** command.
- Added switch to print Scaled metrics in **lparstat** command.
- Added **helper** function to calculate the delta, scaled timebase, and to derive **PURR/SPURR** values.
- For **ofpathname** utility:
    - Improved the speed for **l2of_scsi()**.
    - Fixed the **udevadm** location.
    - Added partition to support **l2od_ide()** and **l2of_scsi()**.
    - Added support for the plug ID of a **SCSI/SATA** host.
- Fixed the **segfault** condition on the unsupported connector type.
- Added tools to support migration of **SR_IOV** to a hybrid virtual network.
- Fixed the **format-overflow** warnings.
- Fixed the bash command substitution warning using the **lsdevinfo** utility.
- Fixed boot-time bonding interface cleanup.

(BZ#1853297)

New kernel cmdline option now generates network device name

The **net_id** built-in from **systemd-udevd** service gains a new kernel cmdline option **net.naming-scheme=SCHEME_VERSION**. Based on the value of the **SCHEME_VERSION**, a user can select a version of the algorithm that will generate the network device name.

For example, to use the features of **net_id** built-in in RHEL 8.4, set the value of the **SCHEME_VERSION** to **rhel-8.4**.

Similarly, you can set the value of the **SCHEME_VERSION** to any other minor release that includes the required change or fix.

(BZ#1827462)

4.5. INFRASTRUCTURE SERVICES

Difference in default postfix-3.5.8 behavior

For better RHEL-8 backward compatibility, the behavior of the **postfix-3.5.8** update differs from the default upstream **postfix-3.5.8** behavior. For the default upstream **postfix-3.5.8** behavior, run the following commands:

 # postconf info_log_address_format=external

 # postconf smtpd_discard_ehlo_keywords=

 # postconf rhel_ipv6_normalize=yes

For details, see the **/usr/share/doc/postfix/README-RedHat.txt** file. If the incompatible functionalities are not used or RHEL-8 backward compatibility is the priority, no steps are necessary.

(BZ#1688389)

BIND rebased to version 9.11.26

The **bind** packages have been updated to version 9.11.26. Notable changes include:

- Changed the default EDNS buffer size from 4096 to 1232 bytes. This change will prevent the loss of fragmented packets in some networks.
- Increased the default value of max-recursion-queries from 75 to 100. Related to CVE-2020-8616.
- Fixed the problem of reused dead nodes in **lib/dns/rbtdb.c** file in **named**.
- Fixed the crashing problem in the **named** service when cleaning the reused dead nodes in the **lib/dns/rbtdb.c** file.
- Fixed the problem of configured multiple forwarders sometimes occurring in the **named** service.
- Fixed the problem of the **named** service of assigning incorrect signed zones with no DS record at the parent as bogus.
- Fixed the missing **DNS cookie response** over **UDP**.

(BZ#1882040)

unbound configuration now provides enhanced logging output

With this enhancement, the following three options have been added to the **unbound** configuration:

- **log-servfail** enables log lines that explain the reason for the **SERVFAIL** error code to clients.
- **log-local-actions** enables logging of all local zone actions.
- **log-tag-queryreply** enables tagging of log queries and log replies in the log file.

(BZ#1850460)

Multiple vulnerabilities fixed with ghostscript-9.27

- The **ghostscript-9.27** release contains security fixes for the following vulnerabilities:
  - CVE-2020-14373
  - CVE-2020-16287
  - CVE-2020-16288
  - CVE-2020-16289
  - CVE-2020-16290
  - CVE-2020-16291
  - CVE-2020-16292
  - CVE-2020-16293
  - CVE-2020-16294
  - CVE-2020-16295
  - CVE-2020-16296
  - CVE-2020-16297
  - CVE-2020-16298
  - CVE-2020-16299
  - CVE-2020-16300
  - CVE-2020-16301
  - CVE-2020-16302
  - CVE-2020-16303
  - CVE-2020-16304
  - CVE-2020-16305
  - CVE-2020-16306
  - CVE-2020-16307
  - CVE-2020-16308

- CVE-2020-16309
- CVE-2020-16310
- CVE-2020-17538

(BZ#1874523)

Tuned rebased to version 2.15-1.

Notable changes include:

- Added **service** plugin for Linux services control.
- Improved **scheduler** plugin.

(BZ#1874052)

DNSTAP now records incoming detailed queries.

DNSTAP provides an advanced way to monitor and log details of incoming name queries. It also records sent answers from the **named** service. Classic query logging of the named service has a negative impact on the performance of the **named** service.

As a result, DNSTAP offers a way to perform continuous logging of detailed incoming queries without impacting the performance penalty. The new **dnstap-read** utility allows you to analyze the queries running on a different system.

(BZ#1854148)

SpamAssassin rebased to version 3.4.4

The **SpamAssassin** package has been upgraded to version 3.4.4. Notable changes include:

- **OLEVBMacro** plugin has been added.
- New functions **check_rbl_ns**, **check_rbl_rcvd**, **check_hashbl_bodyre**, and **check_hashbl_uris** have been added.

(BZ#1822388)

Key algorithm can be changed using the OMAPI shell

With this enhancement, users can now change the key algorithm. The key algorithm that was hardcoded as **HMAC-MD5** is not considered secure anymore. As a result, users can use the **omshell** command to change the key algorithm.

(BZ#1883999)

Sendmail now supports TLSFallbacktoClear configuration

With this enhancement, if the outgoing TLS connection fails, the sendmail client will fall back to the plaintext. This overcomes the TLS compatibility problems with the other parties. Red Hat ships sendmail with the **TLSFallbacktoClear** option disabled by default.

(BZ#1868041)

tcpdump now allows viewing RDMA capable devices

This enhancement enables support for capturing RDMA traffic with **tcpdump**. It allows users to capture and analyze offloaded RDMA traffic with the **tcpdump** tool. As a result, users can use **tcpdump** to view RDMA capable devices, capture RoCE and VMA traffic, and analyze its content.

(BZ#1743650)

4.6. SECURITY

libreswan rebased to 4.3

The **libreswan** packages have been upgraded to version 4.3. Notable changes over the previous version include:

- IKE and ESP over TCP support (RFC 8229)
- IKEv2 Labeled IPsec support
- IKEv2 leftikeport/rightikeport support
- Experimental support for Intermediate Exchange
- Extended Redirect support for loadbalancing
- Default IKE lifetime changed from 1 h to 8 h for increased interoperability
- **:RSA** sections in the **ipsec.secrets** file are no longer required
- Fixed Windows 10 rekeying
- Fixed sending certificate for ECDSA authentication
- Fixes for MOBIKE and NAT-T

(BZ#1891128)

IPsec VPN now supports TCP transport

This update of the **libreswan** packages adds support for IPsec-based VPNs over TCP encapsulation as described in RFC 8229. The addition helps establish IPsec VPNs on networks that prevent traffic using Encapsulating Security Payload (ESP) and UDP. As a result, administrators can configure VPN servers and clients to use TCP either as a fallback or as the main VPN transport protocol.

(BZ#1372050)

Libreswan now supports IKEv2 for Labeled IPsec

The Libreswan Internet Key Exchange (IKE) implementation now includes Internet Key Exchange version 2 (IKEv2) support of Security Labels for IPsec. With this update, systems that use security labels with IKEv1 can be upgraded to IKEv2.

(BZ#1025061)

libpwquality rebased to 1.4.4

The **libpwquality** package has been rebased to version 1.4.4. This release includes multiple bug fixes and translation updates. Most notably, the following setting options have been added to the **pwquality.conf** file:

- **retry**
- **enforce_for_root**
- **local_users_only**

(BZ#1537240)

p11-kit rebased to 0.23.19

The **p11-kit** packages have been upgraded from version 0.23.14 to version 0.23.19. The new version fixes several bugs and provides various enhancements, notably:

- Fixed CVE-2020-29361, CVE-2020-29362, CVE-2020-29363 security issues.
- **p11-kit** now supports building through the **meson** build system.

(BZ#1887853)

pyOpenSSL rebased to 19.0.0

The **pyOpenSSL** packages have been rebased to upstream version 19.0.0. This version provides bug fixes and enhancements, most notably:

- Improved TLS 1.3 support with **openssl** version 1.1.1.
- No longer raising an error when trying to add a duplicate certificate with **X509Store.add_cert**
- Improved handling of X509 certificates containing NUL bytes in components

(BZ#1629914)

SCAP Security Guide rebased to 0.1.54

The **scap-security-guide** packages have been rebased to upstream version 0.1.54, which provides several bug fixes and improvements. Most notably:

- The **Operating System Protection Profile** (OSPP) has been updated in accordance with the Protection Profile for General Purpose Operating Systems for Red Hat Enterprise Linux 8.4.
- The **ANSSI** family of profiles based on the ANSSI BP-028 recommendations from the French National Security Agency (ANSSI), has been introduced. The content contains profiles implementing rules of the Minimum, Intermediary and Enhanced hardening levels.
- The Security Technical Implementation Guide (**STIG**) security profile has been updated, and it implements rules from the recently-released version V1R1.

(BZ#1889344)

OpenSCAP rebased to 1.3.4

The OpenSCAP packages have been rebased to upstream version 1.3.4. Notable fixes and enhancements include:

- Fixed certain memory issues that were causing systems with large amounts of files to run out of memory.
- OpenSCAP now treats GPFS as a remote file system.

- Proper handling of OVALs with circular dependencies between definitions.
- Improved **yamlfilecontent**: updated **yaml-filter**, extended the schema and probe to be able to work with a set of values in maps.
- Fixed numerous warnings (GCC and Clang).
- Numerous memory management fixes.
- Numerous memory leak fixes.
- Platform elements in XCCDF files are now properly resolved in accordance with the XCCDF specification.
- Improved compatibility with uClibc.
- Local and remote file system detection methods improved.
- Fixed **dpkginfo** probe to use **pkgCacheFile** instead of manually opening the cache.
- OpenSCAP scan report is now a valid HTML5 document.
- Fixed unwanted recursion in the file probe.

(BZ#1887794)

The RHEL 8 STIG security profile updated to version V1R1

With the release of the RHBA-2021:1886 advisory, the **DISA STIG for Red Hat Enterprise Linux 8** profile in the SCAP Security Guide has been updated to align with the latest version **V1R1**. The profile is now also more stable and better aligns with the RHEL 8 STIG (Security Technical Implementation Guide) manual benchmark provided by the Defense Information Systems Agency (DISA). This first iteration brings approximately 60% of coverage with regards to the STIG.

You should use only the current version of this profile because the draft profile is no longer valid.

WARNING

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

(BZ#1918742)

New DISA STIG profile compatible with Server with GUI installations

A new profile, **DISA STIG with GUI**, has been added to the **SCAP Security Guide** with the release of the RHBA-2021:4098 advisory. This profile is derived from the **DISA STIG** profile and is compatible with RHEL installations that selected the **Server with GUI** package group. The previously existing **stig** profile was not compatible with **Server with GUI** because DISA STIG demands uninstalling any Graphical User Interface. However, this can be overridden if properly documented by a Security Officer during evaluation. As a result, the new profile helps when installing a RHEL system as a **Server with GUI** aligned with the DISA STIG profile.

(BZ#2005431)

Profiles for ANSSI-BP-028 Minimal, Intermediary and Enhanced levels are now available in SCAP Security Guide

With the new profiles, you can harden the system to the recommendations from the French National Security Agency (ANSSI) for GNU/Linux Systems at the Minimal, Intermediary and Enhanced hardening levels. As a result, you can configure and automate compliance of your RHEL 8 systems according to your required ANSSI hardening level by using the ANSSI Ansible Playbooks and the ANSSI SCAP profiles.

(BZ#1778188)

scap-workbench can now scan remote systems using sudo privileges

The **scap-workbench** GUI tool now supports scanning remote systems using passwordless **sudo** access. This feature reduces the security risk imposed by supplying root's credentials.

Be cautious when using **scap-workbench** with passwordless **sudo** access and the **remediate** option. Red Hat recommends dedicating a well-secured user account just for the OpenSCAP scanner.

(BZ#1877522)

rhel8-tang container image is now available

With this release, the **rhel8/rhel8-tang** container image is available in the **registry.redhat.io** catalog. The container image provides Tang-server decryption capabilities for Clevis clients that run either in OpenShift Container Platform (OCP) clusters or in separate virtual machines.

(BZ#1913310)

Clevis rebased to version 15

The **clevis** packages have been rebased to upstream version 15. This version provides many bug fixes and enhancements over the previous version, most notably:

- Clevis now produces a generic initramfs and no longer automatically adds the **rd.neednet=1** parameter to the kernel command line.
- Clevis now properly handles incorrect configurations that use the **sss** pin, and the **clevis encrypt sss** sub-command returns outputs that indicate the error cause.

(BZ#1887836)

Clevis no longer automatically adds rd.neednet=1

Clevis now correctly produces a generic **initrd** (initial ramdisk) without host-specific configuration options by default. As a result, Clevis no longer automatically adds the **rd.neednet=1** parameter to the kernel command line.

If your configuration uses the previous functionality, you can either enter the **dracut** command with the **--hostonly-cmdline** argument or create the **clevis.conf** file in the **/etc/dracut.conf.d** and add the **hostonly_cmdline=yes** option to the file. A Tang binding must be present during the **initrd** build process.

(BZ#1853651)

New package: rsyslog-udpspoof

The **rsyslog-udpspoof** subpackage has been added back to RHEL 8. This module is similar to the regular UDP forwarder, but permits relaying **syslog** between different network segments while maintaining the source IP in the **syslog** packets.

(BZ#1869874)

fapolicyd rebased to 1.0.2

The **fapolicyd** packages have been rebased to upstream version 1.0.2. This version provides many bug fixes and enhancements over the previous version, most notably:

- Added the **integrity** configuration option for enabling integrity checks through:
  - Comparing file sizes
  - Comparing SHA-256 hashes
  - Integrity Measurement Architecture (IMA) subsystem
- The **fapolicyd** RPM plugin now registers any system update that is handled by either the YUM package manager or the RPM Package Manager.
- Rules now can contain GID in subjects.
- You can now include rule numbers in debug and **syslog** messages.

(BZ#1887451)

New RPM plugin notifies fapolicyd about changes during RPM transactions

This update of the **rpm** packages introduces a new RPM plugin that integrates the **fapolicyd** framework with the RPM database. The plugin notifies **fapolicyd** about installed and changed files during an RPM transaction. As a result, **fapolicyd** now supports integrity checking.

Note that the RPM plugin replaces the YUM plugin because its functionality is not limited to YUM transactions but covers also changes by RPM.

(BZ#1923167)

4.7. NETWORKING

The PTP capabilities output format of the ethtool utility has changed

Starting with RHEL 8.4, the **ethtool** utility uses the **netlink** interface instead of the **ioctl()** system call to communicate with the kernel. Consequently, when you use the **ethtool -T *<network_controller>*** command, the format of Precision Time Protocol (PTP) values changes.

Previously, with the **ioctl()** interface, **ethtool** translated the capability bit names by using an **ethtool**-internal string table and, the **ethtool -T *<network_controller>*** command displayed, for example:

```
Time stamping parameters for <network_controller>:
Capabilities:
hardware-transmit (SOF_TIMESTAMPING_TX_HARDWARE)
software-transmit (SOF_TIMESTAMPING_TX_SOFTWARE)
...
```

With the **netlink** interface, **ethtool** receives the strings from the kernel. These strings do not include the internal **SOF_TIMESTAMPING_*** names. Therefore, **ethtool -T *<network_controller>*** now displays, for example:

```
Time stamping parameters for <network_controller>:
Capabilities:
hardware-transmit
software-transmit
...
```

If you use the PTP capabilities output of **ethtool** in scripts or applications, update them accordingly.

(JIRA:RHELDOCS-18188)

XDP is conditionally supported

Red Hat supports the eXpress Data Path (XDP) feature only if all of the following conditions apply:

- You load the XDP program on an AMD or Intel 64-bit architecture
- You use the **libxdp** library to load the program into the kernel
- The XDP program does not use the XDP hardware offloading

In RHEL 8.4, **XDP_TX** and **XDP_REDIRECT** return codes are now supported in XDP programs.

For details about unsupported XDP features, see XDP features that are available as Technology Preview

(BZ#1952421)

NetworkManager rebased to version 1.30.0

The **NetworkManager** packages have been upgraded to upstream version 1.30.0, which provides a number of enhancements and bug fixes over the previous version:

- The **ipv4.dhcp-reject-servers** connection property has been added to define from which DHCP server IDs NetworkManager should reject lease offers.
- The **ipv4.dhcp-vendor-class-identifier** connection property has been added to send a custom Vendor Class Identifier DHCP option value.
- The **active_slave** bond option has been deprecated. Instead, set the **primary** option in the controller connection.
- The **nm-initrd-generator** utility now supports MAC addresses to indicate interfaces.
- The **nm-initrd-generator** utility generator now supports creating InfiniBand connections.
- The timeout of the **NetworkManager-wait-online** service has been increased to 60 seconds.
- The **ipv4.dhcp-client-id=ipv6-duid** connection property has been added to be compliant to RFC4361.
- Additional **ethtool** offload features have been added.
- Support for the WPA3 Enterprise Suite-B 192-bit mode has been added.
- Support for virtual Ethernet (**veth**) devices has been added.

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

- NetworkManager 1.30.0
- NetworkManager 1.28.0

(BZ#1878783)

The iproute2 utility introduces traffic control actions to add MPLS headers before Ethernet header

With this enhancement, the **iproute2** utility offers three new traffic control (**tc**) actions:

- **mac_push** - The **act_mpls** module provides this action to add MPLS labels before the original Ethernet header.
- **push_eth** - The **act_vlan** module provides this action to build an Ethernet header at the beginning of the packet.
- **pop_eth** - The **act_vlan** module provides this action to drop the outer Ethernet header.

These **tc** actions help in implementing layer 2 virtual private network (L2VPN) by adding multiprotocol label switching (MPLS) labels before Ethernet headers. You can use these actions while adding **tc filters** to the network interfaces.

Red Hat provides these actions as unsupported Technology Preview, because MPLS itself is a Technology Preview feature.

For more information about these actions and their parameters, refer to the **tc-mpls(8)** and **tc-vlan(8)** man pages.

(BZ#1861261)

The nmstate API is now fully supported

Nmstate, which was previously a Technology Preview, is a network API for hosts and fully supported in RHEL 8.4. The **nmstate** packages provide a library and the **nmstatectl** command-line utility to manage host network settings in a declarative manner. The networking state is described by a predefined schema. Reporting of the current state and changes to the desired state both conform to the schema.

For further details, see the **/usr/share/doc/nmstate/README.md** file and the sections about **nmstatectl** in the Configuring and managing networking documentation.

(BZ#1674456)

New package: rshim

The **rhsim** package provides the Mellanox BlueField rshim user-space driver, which enables accessing the rshim resources on the BlueField SmartNIC target from the external host machine. The current version of the rshim user-space driver implements device files for boot image push and virtual console access. In addition, it creates a virtual network interface to connect to the BlueField target and provides a way to access internal rshim registers.

Note that in order for the virtual console or virtual network interface to be operational, the target must be running a **tmfifo** driver.

(BZ#1744737)

iptraf-ng rebased to 1.2.1

The **iptraf-ng** packages have been rebased to upstream version 1.2.1, which provides several bug fixes and improvements. Most notably:

- The **iptraf-ng** application no longer causes 100% CPU usage when showing the detailed statistics of a deleted interface.
- The unsafe handling arguments of **printf()** functions have been fixed.
- Partial support for IP over InfiniBand (IPoIB) interface has been added. Because the kernel does not provide the source address on the interface, you cannot use this feature in the LAN station monitor mode.
- Packet capturing abstraction has been added to allow **iptraf-ng** to capture packets at multi-gigabit speed.
- You can now scroll using the **Home**, **End**, **Page up**, and **Page down** keyboard keys.
- The application now shows the dropped packet count.

(BZ#1906097)

4.8. KERNEL

Kernel version in RHEL 8.4

Red Hat Enterprise Linux 8.4 is distributed with the kernel version 4.18.0-305.

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

(BZ#1839151)

Extended Berkeley Packet Filter for RHEL 8.4

The **Extended Berkeley Packet Filter (eBPF)** is an in-kernel virtual machine that allows code execution in the kernel space, in the restricted sandbox environment with access to a limited set of functions. The virtual machine executes a special assembly-like code.

The **eBPF** bytecode first loads to the kernel, followed by its verification, code translation to the native machine code with just-in-time compilation, and then the virtual machine executes the code.

Red Hat ships numerous components that utilize the **eBPF** virtual machine. Each component is in a different development phase, and thus not all components are currently fully supported. In RHEL 8.4, the following **eBPF** components are supported:

- The **BPF Compiler Collection (BCC)** tools package, which provides tools for I/O analysis, networking, and monitoring of Linux operating systems using **eBPF**.
- The **BCC** library which allows the development of tools similar to those provided in the **BCC** tools package.
- The **eBPF for Traffic Control (tc)** feature, which enables programmable packet processing inside the kernel network data path.
- The **eXpress Data Path (XDP)** feature, which provides access to received packets before the kernel networking stack processes them, is supported under specific conditions.

- The **libbpf** package, which is crucial for bpf related applications like **bpftrace** and **bpf/xdp** development.
- The **xdp-tools** package, which contains userspace support utilities for the **XDP** feature, is now supported on the AMD and Intel 64-bit architectures. This includes the **libxdp** library, the **xdp-loader** utility for loading XDP programs, the **xdp-filter** example program for packet filtering, and the **xdpdump** utility for capturing packets from a network interface with XDP enabled.

Note that all other **eBPF** components are available as Technology Preview, unless a specific component is indicated as supported.

The following notable **eBPF** components are currently available as Technology Preview:

- The **bpftrace** tracing language
- The **AF_XDP** socket for connecting the **eXpress Data Path (XDP)** path to user space

For more information regarding the Technology Preview components, see Technology Previews.

(BZ#1780124)

New package: kmod-redhat-oracleasm

This update adds the new **kmod-redhat-oracleasm** package, which provides the kernel module part of the ASMLib utility. Oracle Automated Storage Management (ASM) is a data volume manager for Oracle databases. ASMLib is an optional utility that can be used on Linux systems to manage Oracle ASM devices.

(BZ#1827015)

The xmon program changes to support Secure Boot and kernel_lock resilience against attacks

If the **Secure Boot** mechanism is disabled, you can set the **xmon** program into read-write mode (**xmon=rw**) on the kernel command-line. However, if you specify **xmon=rw** and boot into **Secure Boot** mode, the **kernel_lockdown** feature overrides **xmon=rw** and changes it to read-only mode. The additional behavior of **xmon** depending on **Secure Boot** enablement is listed below:

Secure Boot is on:

- **xmon=ro** (default)
- A stack trace is printed
- Memory read works
- Memory write is blocked

Secure Boot is off:

- Possibility to set **xmon=rw**
- A stack trace is always printed
- Memory read always works
- Memory write is permitted only if **xmon=rw**

These changes to **xmon** behavior aim to support the **Secure Boot** and **kernel_lock** resilience against attackers with root permissions.

For information how to configure kernel command-line parameters, see Configuring kernel command-line parameters on the Customer Portal.

(BZ#1952161)

Cornelis Omni-Path Architecture (OPA) Host Software

Omni-Path Architecture (OPA) host software is fully supported in Red Hat Enterprise Linux 8.4. OPA provides Host Fabric Interface (HFI) hardware with initialization and setup for high performance data transfers (high bandwidth, high message rate, low latency) between compute and I/O nodes in a clustered environment.

For instructions on installing Omni-Path Architecture, see: Cornelis Omni-Path Fabric Software Release Notes file.

(BZ#1960412)

SLAB cache merging disabled by default

The **CONFIG_SLAB_MERGE_DEFAULT** kernel configuration option has been disabled, and now SLAB caches are not merged by default. This change aims to enhance the allocator's reliability and traceability of cache usage. If the previous slab-cache merging behavior was desirable, the user can re-enable it by adding the **slub_merge** 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.

(BZ#1871214)

The ima-evm-utils package rebased to version 1.3.2

The **ima-evm-utils** package has been upgraded to version 1.3.2, which provides multiple bug fixes and enhancements. Notable changes include:

- Added support for handling the Trusted Platform Module (TPM2) multi-banks feature
- Extended the boot aggregate value to Platform Configuration Registers (PCRs) 8 and 9
- Preloaded OpenSSL engine through a CLI parameter
- Added support for Intel Task State Segment (TSS2) PCR reading
- Added support for the original Integrity Measurement Architecture (IMA) template

Both the **libimaevm.so.0** and **libimaevm.so.2** libraries are part of **ima-evm-utils**. Users of **libimaevm.so.0** will not be affected, when their more recent applications use **libimaevm.so.2**.

(BZ#1868683)

Levelling IMA and EVM features across supported CPU architectures

All CPU architectures, except ARM, have a similar level of feature support for Integrity Measurement Architecture (IMA) and Extended Verification Module (EVM) technologies. The enabled functionalities are different for each CPU architecture. The following are the most significant changes for each supported CPU architecture:

- IBM Z: IMA appraise and trusted keyring enablement.

- AMD64 and Intel 64: specific architecture policy in secure boot state.
- IBM Power System (little-endian): specific architecture policy in secure and trusted boot state.
- SHA-256 as default hash algorithm for all supported architectures.
- For all architectures, the measurement template has changed to IMA-SIG The template includes the signature bits when present. Its format is **d-ng|n-ng|sig**.

The goal of this update is to decrease the level of feature difference in IMA and EVM, so that userspace applications can behave equally across all supported CPU architectures.

(BZ#1869758)

Proactive compaction is now included in RHEL 8 as disabled-by-default

With ongoing workload activity, system memory becomes fragmented. The fragmentation can result in capacity and performance problems. In some cases, program errors are also possible. Thereby, the kernel relies on a reactive mechanism called memory compaction. The original design of the mechanism is conservative, and the compaction activity is initiated on demand of allocation request. However, reactive behavior tends to increase the allocation latency if the system memory is already heavily fragmented. **Proactive compaction** improves the design by **regularly** initiating memory compaction work **before** a request for allocation is made. This enhancement increases the chances that memory allocation requests find the physically contiguous blocks of memory without the need of memory compaction producing those on-demand. As a result, latency for specific memory allocation requests is lowered.

WARNING

Proactive compaction can result in increased compaction activity. This might have serious, system-wide impact, because memory pages that belong to different processes are moved and remapped. Therefore, enabling **proactive compaction** requires utmost care to avoid latency spikes in applications.

(BZ#1848427)

EDAC support has been added in RHEL 8

With this update, RHEL 8 supports the Error Detection and Correction (EDAC) kernel module set in 8th and 9th generation Intel Core Processors (CoffeeLake). The EDAC kernel module mainly handles Error Code Correction (ECC) memory and detect and report PCI bus parity errors.

(BZ#1847567)

A new package: kpatch-dnf

The **kpatch-dnf** package provides a **DNF** plugin, which makes it possible to subscribe a RHEL system to kernel live patch updates. The subscription will affect all kernels currently installed on the system, including kernels that will be installed in the future. For more details about **kpatch-dnf**, see the **dnf-kpatch(8)** manual page or the Managing, monitoring, and updating the kernel documentation.

(BZ#1798711)

A new cgroups controller implementation for slab memory

A new implementation of slab memory controller for the **control groups** technology is now available in RHEL 8. Currently, a single memory slab can contain objects owned by different memory **control group**. The slab memory controller brings improvement in slab utilization (up to 45%) and enables to shift the memory accounting from the page level to the object level. Also, this change eliminates each set of duplicated per-CPU and per-node slab caches for each memory control group and establishes one common set of per-CPU and per-node slab caches for all memory **control groups**. As a result, you can achieve a significant drop in the total kernel memory footprint and observe positive effects on memory fragmentation.

Note that the new and more precise memory accounting requires more CPU time. However, the difference seems to be negligible in practice.

(BZ#1877019)

Time namespace has been added in RHEL 8

The time namespace enables the system monotonic and boot-time clocks to work with per-namespace offsets on AMD64, Intel 64, and the 64-bit ARM architectures. This feature is suited for changing the date and time inside Linux containers and for in-container adjustments of clocks after restoration from a checkpoint. As a result, users can now independently set time for each individual container.

(BZ#1548297)

New feature: Free memory page returning

With this update, the RHEL 8 host kernel is able to return memory pages that are not used by its virtual machines (VMs) back to the hypervisor. This improves the stability and resource efficiency of the host. Note that for memory page returning to work, it must be configured in the VM, and the VM must also use the **virtio_balloon** device.

(BZ#1839055)

Supports changing the sorting order in perf top

With this update, **perf top** can now sort samples by arbitrary event column in case multiple events in a group are sampled, instead of sorting by the first column. As a result, pressing a number key sorts the table by the matching data column.

NOTE

The column numbering starts from **0**.

Using the **--group-sort-idx** command line option, it is possible to sort by the column number.

(BZ#1851933)

The kabi_whitelist package has been renamed to kabi_stablelist

In accordance with Red Hat commitment to replacing problematic language, we renamed the **kabi_whitelist** package to **kabi_stablelist** in the RHEL 8.4 release.

(BZ#1867910, BZ#1886901)

bpf rebased to version 5.9

The **bpf** kernel technology in RHEL 8 has been brought up-to-date with its upstream counterpart from the kernel v5.9.

The update provides multiple bug fixes and enhancements. Notable changes include:

- Added Berkeley Packet Filter (BPF) iterator for map elements and to iterate all BPF programs for efficient in-kernel inspection.
- Programs in the same control group (cgroup) can share the cgroup local storage map.
- BPF programs can run on socket lookup.
- The **SO_KEEPALIVE** and related options are available to the **bpf_setsockopt()** helper.

Note that some BPF programs may need changes to their source code.

(BZ#1874005)

The bcc package rebased to version 0.16.0

The **bcc** package has been upgraded to version 0.16.0, which provides multiple bug fixes and enhancements. Notable changes include:

- Added utilities **klockstat** and **funcinterval**
- Fixes in various parts of the **tcpconnect** manual page
- Fix to make the **tcptracer** tool output show SPORT and DPORT columns for IPv6 addresses
- Fix broken dependencies

(BZ#1879411)

bpftrace rebased to version 0.11.0

The **bpftrace** package has been upgraded to version 0.11.0, which provides multiple bug fixes and enhancements. Notable changes include:

- Added utilities **threadsnoop**, **tcpsynbl**, **tcplife**, **swapin**, **setuids**, and **naptime**
- Fixed failures to run of the **tcpdrop.bt** and **syncsnoop.bt** tools
- Fixed a failure to load the Berkeley Packet Filter (BPF) program on IBM Z architectures
- Fixed a symbol lookup error

(BZ#1879413)

libbpf rebased to version 0.2.0.1

The **libbpf** package has been upgraded to version 0.2.0.1, which provides multiple bug fixes and enhancements. Notable changes include:

- Added support for accessing Berkeley Packet Filter (BPF) map fields in the **bpf_map** struct from programs that have BPF Type Format (BTF) struct access
- Added BPF ring buffer
- Added **bpf** iterator infrastructure

- Improved **bpf_link** observability

(BZ#1919345)

perf now supports adding or removing tracepoints from a running collector without having to stop or restart perf

Previously, to add or remove tracepoints from an instance of **perf record**, the **perf** process had to be stopped. As a consequence, performance data that occurred during the time the process was stopped was not collected and, therefore, lost. With this update, you can dynamically enable and disable tracepoints being collected by **perf record** via the control pipe interface without having to stop the **perf record** process.

(BZ#1844111)

The perf tool now supports recording and displaying absolute timestamps for trace data

With this update, **perf script** can now record and display trace data with absolute timestamps.

Note: To display trace data with absolute timestamps, the data must be recorded with the clock ID specified.

To record data with absolute timestamps, specify the clock ID:

```
# perf record -k CLOCK_MONOTONIC sleep 1
```

To display trace data recorded with the specified clock ID, execute the following command:

```
# perf script -F+tod
```

(BZ#1811839)

dwarves rebased to version 1.19.1

The **dwarves** package has been upgraded to version 1.19.1, which provides multiple bug fixes and enhancements. Notably, this update introduces a new way of checking functions from the DWARF debug data with related **ftrace** entries to ensure a subset of **ftrace** functions is generated.

(BZ#1903566)

perf now supports circular buffers that use specified events to trigger snapshots

With this update, you can create custom circular buffers that write data to a **perf.data** file when an event you specify is detected. As a result, **perf record** can run continuously in the system background without generating excess overhead by continuously writing data to a **perf.data** file, and only recording data you are interested in.

To create a custom circular buffer using the **perf** tool that records event specific snapshots, use the following command:

```
# perf record --overwrite -e _events_to_be_collected_ --switch-output-event
_snapshot_trigger_event_
```

(BZ#1844086)

Kernel DRBG and Jitter entropy source are compliant to NIST SP 800-90A and NIST SP 800-90B

Kernel Deterministic Random Bit Generator (DRBG) and Jitter entropy source are now compliant to recommendation for random number generation using DRBG (NIST SP 800-90A) and recommendation for the entropy sources used for random bit generation (NIST SP 800-90B) specifications. As a result, applications in FIPS mode can use these sources as FIPS-compliant randomness and noise sources.

(BZ#1905088)

kdump now supports Virtual Local Area Network tagged team network interface

This update adds support to configure Virtual Local Area Network tagged team interface for **kdump**. As a result, this feature now enables **kdump** to use a Virtual Local Area Network tagged team interface to dump a **vmcore** file.

(BZ#1844941)

kernel-rt source tree has been updated to RHEL 8.4 tree

The **kernel-rt** source has been updated to use the latest Red Hat Enterprise Linux kernel source tree. The real-time patch set has also been updated to the latest upstream version, v5.10-rt7. Both of these updates provide a number of bug fixes and enhancements.

(BZ#1858099, BZ#1858105)

The stalld package is now added to RHEL 8.4 distribution

This update adds the **stalld** package to RHEL 8.4.0. **stalld** is a daemon that monitors threads on a system running low latency applications. It checks for job threads that have been on a run-queue without being scheduled onto a CPU for a specified threshold.

When it detects a stalled thread, **stalld** temporarily changes the scheduling policy to **SCHED_DEADLINE** and assigns the thread a slice of CPU time to make forward progress. When the time slice completes or the thread blocks, the thread goes back to its original scheduling policy.

(BZ#1875037)

Support for CPU hotplug in the hv_24x7 and hv_gpci PMUs

With this update, PMU counters correctly react to the hot-plugging of a CPU. As a result, if a **hv_gpci** event counter is running on a CPU that gets disabled, the counting redirects to another CPU.

(BZ#1844416)

Metrics for POWERPC hv_24x7 nest events are now available

Metrics for POWERPC **hv_24x7** nest events are now available for **perf**. By aggregating multiple events, these metrics provide a better understanding of the values obtained from **perf** counters and how effectively the CPU is able to process the workload.

(BZ#1780258)

hwloc rebased to version 2.2.0

The **hwloc** package has been upgraded to version 2.2.0, which provides the following change:

- The **hwloc** functionality can report details on Nonvolatile Memory Express (NVMe) drives including total disk size and sector size.

(BZ#1841354)

The igc driver is now fully supported

The **igc** Intel 2.5G Ethernet Linux wired LAN driver was introduced in RHEL 8.1 as a Technology Preview. Starting with RHEL 8.4, it is fully supported on all architectures. The **ethtool** utility also supports **igc** wired LANs.

(BZ#1495358)

4.9. FILE SYSTEMS AND STORAGE

RHEL installation now supports creating a swap partition of size 16 TiB

Previously, when installing RHEL, the installer created a swap partition of maximum 128 GB for automatic and manual partitioning.

With this update, for automatic partitioning, the installer continues to create a swap partition of maximum 128 GB, but in case of manual partitioning, you can now create a swap partition of 16 TiB.

(BZ#1656485)

Surprise removal of NVMe devices

With this enhancement, you can surprise remove NVMe devices from the Linux operating system without notifying the operating system beforehand. This will enhance the serviceability of NVMe devices because no additional steps are required to prepare the devices for orderly removal, which ensures the availability of servers by eliminating server downtime.

Note the following:

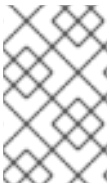
- Surprise removal of NVMe devices requires **kernel-4.18.0-193.13.2.el8_2.x86_64** version or later.
- Additional requirements from the hardware platform or the software running on the platform might be necessary for successful surprise removal of NVMe devices.
- Surprise removing an NVMe device that is critical to the system operation is not supported. For example, you cannot remove an NVMe device that contains the operating system or a swap partition.

(BZ#1634655)

Stratis filesystem symlink paths have changed

With this enhancement, Stratis filesystem symlink paths have changed from **/stratis/*<stratis-pool>*/*<filesystem-name>*** to **/dev/stratis/*<stratis-pool>*/*<filesystem-name>***. Consequently, all existing Stratis symlinks must be migrated to utilize the new symlink paths.

Use the included **stratis_migrate_symlinks.sh** migration script or reboot your system to update the symlink paths. If you manually changed the **systemd** unit files or the **/etc/fstab** file to automatically mount Stratis filesystems, you must update them with the new symlink paths.



NOTE

If you do not update your configuration with the new Stratis symlink paths, or if you temporarily disable the automatic mounts, the boot process might not complete the next time you reboot or start your system.

(BZ#1798244)

Stratis now supports binding encrypted pools to a supplementary Clevis encryption policy

With this enhancement, you can now bind encrypted Stratis pools to Network Bound Disk Encryption (NBDE) using a Tang server, or to the Trusted Platform Module (TPM) 2.0. Binding an encrypted Stratis pool to NBDE or TPM 2.0 facilitates automatic unlocking of pools. As a result, you can access your Stratis pools without having to provide the kernel keyring description after each system reboot. Note that binding a Stratis pool to a supplementary Clevis encryption policy does not remove the primary kernel keyring encryption.

(BZ#1868100)

New mount options to control when DAX is enabled on XFS and ext4 file systems

This update introduces new mount options which, when combined with the **FS_XFLAG_DAX** inode flag, provide finer-grained control of the Direct Access (DAX) mode for files on XFS and ext4 file systems. In prior releases, DAX was enabled for the entire file system using the **dax** mount option. Now, the direct access mode can be enabled on a per-file basis.

The on-disk flag, **FS_XFLAG_DAX**, is used to selectively enable or disable DAX for a particular file or directory. The **dax** mount option dictates whether or not the flag is honored:

- **-o dax=inode** - follow **FS_XFLAG_DAX**. This is the default when no dax option is specified.
- **-o dax=never** - never enable DAX, ignore **FS_XFLAG_DAX**.
- **-o dax=always** - always enable DAX, ignore **FS_XFLAG_DAX**.
- **-o dax** - is a legacy option which is an alias for "dax=always". This may be removed in the future, so "-o dax=always" is preferred.

You can set **FS_XFLAG_DAX** flag by using the **xfs_io** utility's chatter command:

```
# xfs_io -c "chattr +x" filename
```

(BZ#1838876, BZ#1838344)

SMB Direct is now supported

With this update, the SMB client now supports SMB Direct.

(BZ#1887940)

New API for mounting filesystems has been added

With this update, a new API for mounting filesystems based on an internal kernel structure called a filesystem context (**struct fs_context**) has been added into RHEL 8.4, allowing greater flexibility in communication of mount parameters between userspace, the VFS, and the file system. Along with this, there are following system calls for operating on the file system context:

- **fsopen()** - creates a blank filesystem configuration context within the kernel for the filesystem named in the **fsname** parameter, adds it into creation mode, and attaches it to a file descriptor, which it then returns.
- **fsmount()** - takes the file descriptor returned by **fsopen()** and creates a mount object for the file system root specified there.

- **fsconfig()** - supplies parameters to and issues commands against a file system configuration context as set up by the **fsopen(2)** or **fspick(2)** system calls.
- **fspick()** - creates a new file system configuration context within the kernel and attaches a pre-existing superblock to it so that it can be reconfigured.
- **move_mount()** - moves a mount from one location to another; it can also be used to attach an unattached mount created by **fsmount()** or **open_tree()** with the **OPEN_TREE_CLONE** system call.
- **open_tree()** - picks the mount object specified by the pathname and attaches it to a new file descriptor or clones it and attaches the clone to the file descriptor.

Note that the old API based on the **mount()** system call is still supported.

For additional information, see the **Documentation/filesystems/mount_api.txt** file in the kernel source tree.

(BZ#1622041)

Discrepancy in vfat file system mtime no longer occurs

With this update, the discrepancy in the **vfat** file system **mtime** between in-memory and on-disk write times is no longer present. This discrepancy was caused by a difference between in-memory and on-disk **mtime** metadata, which no longer occurs.

(BZ#1533270)

RHEL 8.4 now supports close_range() system call

With this update, the **close_range()** system call was backported to RHEL 8.4. This system call closes all file descriptors in a given range effectively, preventing timing problems which are present when closing a wide range of file descriptors sequentially if applications configure very large limits.

(BZ#1900674)

Support for user extended attributes through the NFSv4.2 protocol has been added

This update adds NFSV4.2 client-side and server-side support for user extended attributes (RFC 8276) and newly includes the following protocol extensions:

New operations:

- **- GETXATTR** - get an extended attribute of a file
- **- SETXATTR** - set an extended attribute of a file
- **- LISTXATTR** - list extended attributes of a file
- **- REMOVEXATTR** - remove an extended attribute of a file

New error codes:

- **- NFS4ERR-NOXATTR** - **xattr** does not exist
- **- NFS4ERR_XATTR2BIG** - **xattr** value is too big

New attribute:

- **- xattr_support** - per-fs read-only attribute determines whether **xattrs** are supported. When set to **True**, the object's file system supports extended attributes.

(BZ#1888214)

4.10. HIGH AVAILABILITY AND CLUSTERS

Noncritical resources in colocation constraints are now supported

With this enhancement, you can configure a colocation constraint such that if the dependent resource of the constraint reaches its migration threshold for failure, Pacemaker will leave that resource offline and keep the primary resource on its current node rather than attempting to move both resources to another node. To support this behavior, colocation constraints now have an **influence** option, which can be set to **true** or **false**, and resources have a **critical** meta-attribute, which can also be set to **true** or **false**. The value of the **critical** resource meta option determines the default value of the **influence** option for all colocation constraints involving the resource as a dependent resource.

When the **influence** colocation constraint option has a value of **true** Pacemaker will attempt to keep both the primary and dependent resource active. If the dependent resource reaches its migration threshold for failures, both resources will move to another node, if possible.

When the **influence** colocation option has a value of **false**, Pacemaker will avoid moving the primary resource as a result of the status of the dependent resource. In this case, if the dependent resource reaches its migration threshold for failures, it will stop if the primary resource is active and can remain on its current node.

By default, the value of the **critical** resource meta option is set to **true**, which in turn determines that the default value of the **influence** option is **true**. This preserves the previous behavior where Pacemaker attempted to keep both resources active.

(BZ#1371576)

New number data type supported by Pacemaker rules

PCS now supports a data type of **number**, which you can use when defining Pacemaker rules in any PCS command that accepts rules. Pacemaker rules implement **number** as a double-precision floating-point number and **integer** as a 64-bit integer.

(BZ#1869399)

Ability to specify a custom clone ID when creating a clone resource or promotable clone resource

When you create a clone resource or a promotable clone resource, the clone resource is named *resource-id* **-clone** by default. If that ID is already in use, PCS adds the suffix - *integer*, starting with an integer value of **1** and incrementing by one for each additional clone. You can now override this default by specifying a name for a clone resource ID or promotable clone resource ID with the *clone-id* option when creating a clone resource with the **pcs resource create** or the **pcs resource clone** command. For information on creating clone resources, see Creating cluster resources that are active on multiple nodes.

(BZ#1741056)

New command to display Corosync configuration

You can now print the contents of the **corosync.conf** file in several output formats with the new **pcs cluster config [show]** command. By default, the **pcs cluster config** command uses the **text** output

format, which displays the Corosync configuration in a human-readable form, with the same structure and option names as the **pcs cluster setup** and **pcs cluster config update** commands.

(BZ#1667066)

New command to modify the Corosync configuration of an existing cluster

You can now modify the parameters of the **corosync.conf** file with the new **pcs cluster config update** command. You can use this command, for example, to increase the **totem** token to avoid fencing during temporary system unresponsiveness. For information on modifying the **corosync.conf** file, see Modifying the corosync.conf file with the pcs command .

(BZ#1667061)

Enabling and disabling Corosync traffic encryption in an existing cluster

Previously, you could configure Corosync traffic encryption only when creating a new cluster. With this update:

- You can change the configuration of the Corosync crypto cipher and hash with the **pcs cluster config update** command.
- You can change the Corosync **authkey** with the **pcs cluster authkey corosync** command.

(BZ#1457314)

New crypt resource agent for shared and encrypted GFS2 file systems

RHEL HA now supports a new **crypt** resource agent, which allows you to configure a LUKS encrypted block device that can be used to provide shared and encrypted GFS2 file systems. Using the **crypt** resource is currently supported only with GFS2 file systems. For information on configuring an encrypted GFS2 file system, see Configuring an encrypted GFS2 file system in a cluster .

(BZ#1471182)

4.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new module: python39

RHEL 8.4 introduces Python 3.9, provided by the new module **python39** and the **ubi8/python-39** container image.

Notable enhancements compared to Python 3.8 include:

- The merge (|) and update (**|=**) operators have been added to the **dict** class.
- Methods to remove prefixes and suffixes have been added to strings.
- Type hinting generics have been added to certain standard types, such as **list** and **dict**.
- The IANA Time Zone Database is now available through the new zoneinfo module.

Python 3.9 and packages built for it can be installed in parallel with Python 3.8 and Python 3.6 on the same system.

To install packages from the **python39** module, use, for example:

-

```
# yum install python39
# yum install python39-pip
```

The **python39:3.9** module stream will be enabled automatically.

To run the interpreter, use, for example:

```
$ python3.9
$ python3.9 -m pip --help
```

See Installing and using Python for more information.

Note that Red Hat will continue to provide support for Python 3.6 until the end of life of RHEL 8. Similarly to Python 3.8, Python 3.9 will have a shorter life cycle; see Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1877430)

Changes in the default separator for the Python urllib parsing functions

To mitigate the Web Cache Poisoning CVE-2021-23336 in the Python **urllib** library, the default separator for the **urllib.parse.parse_qsl** and **urllib.parse.parse_qs** functions is being changed from both ampersand (**&**) and semicolon (**;**) to only an ampersand.

This change has been implemented in Python 3.6 with the release of RHEL 8.4, and will be backported to Python 3.8 and Python 2.7 in the following minor release of RHEL 8.

The change of the default separator is potentially backwards incompatible, therefore Red Hat provides a way to configure the behavior in Python packages where the default separator has been changed. In addition, the affected **urllib** parsing functions issue a warning if they detect that a customer's application has been affected by the change.

For more information, see the Mitigation of Web Cache Poisoning in the Python urllib library (CVE-2021-23336).

Python 3.9 is unaffected and already includes the new default separator (**&**), which can be changed only by passing the separator parameter when calling the **urllib.parse.parse_qsl** and **urllib.parse.parse_qs** functions in Python code.

(BZ#1935686, BZ#1928904)

A new module stream: swig:4.0

RHEL 8.4 introduces the Simplified Wrapper and Interface Generator (SWIG) version 4.0, available as a new module stream, **swig:4.0**.

Notable changes over the previously released **SWIG 3.0** include:

- The only supported **Python** versions are: 2.7 and 3.2 to 3.8.
- The **Python** module has been improved: the generated code has been simplified and most optimizations are now enabled by default.
- Support for **Ruby 2.7** has been added.
- **PHP 7** is now the only supported PHP version; support for **PHP 5** has been removed.

- Performance has been significantly improved when running **SWIG** on large interface files.
- Support for a command-line options file (also referred to as a response file) has been added.
- Support for JavaScript **Node.js** versions 2 to 10 has been added.
- Support for **Octave** versions 4.4 to 5.1 has been added.

To install the **swig:4.0** module stream, use:

```
# yum module install swig:4.0
```

If you want to upgrade from the **swig:3.0** stream, see Switching to a later stream .

For information about the length of support for the **swig** module streams, see the Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1853639)

A new module stream: subversion:1.14

RHEL 8.4 introduces a new module stream, **subversion:1.14**. **Subversion 1.14** is the most recent Long Term Support (LTS) release.

Notable changes since **Subversion 1.10** distributed in RHEL 8.0 include:

- **Subversion 1.14** includes **Python 3** bindings for automation and integration of **Subversion** into the customer's build and release infrastructure.
- A new **svnadmin rev-size** command enables users to determine the total size of a revision.
- A new **svnadmin build-repcache** command enables administrators to populate the **rep-cache** database with missing entries.
- A new experimental command has been added to provide an overview of the current working copy status.
- Various improvements to the **svn log**, **svn info**, and **svn list** commands have been implemented. For example, **svn list --human-readable** now uses human-readable units for file sizes.
- Significant improvements to **svn status** for large working copies have been made.

Compatibility information:

- **Subversion 1.10** clients and servers interoperate with **Subversion 1.14** servers and clients. However, certain features might not be available unless both client and server are upgraded to the latest version.
- Repositories created under **Subversion 1.10** can be successfully loaded in **Subversion 1.14**.
- **Subversion 1.14** distributed in RHEL 8 enables users to cache passwords in plain text on the client side. This behaviour is the same as **Subversion 1.10** but different from the upstream release of **Subversion 1.14**.

- The experimental **Shelving** feature has been significantly changed, and it is incompatible with shelves created in **Subversion 1.10**. See the upstream documentation for details and upgrade instructions.
- The interpretation of path-based authentication configurations with both global and repository-specific rules has changed in **Subversion 1.14**. See the upstream documentation for details on affected configurations.

To install the **subversion:1:14** module stream, use:

```
# yum module install subversion:1.14
```

If you want to upgrade from the **subversion:1.10** stream, see Switching to a later stream .

For information about the length of support for the **subversion** module streams, see the Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1844947)

A new module stream: redis:6

Redis 6, an advanced key-value store, is now available as a new module stream, **redis:6**.

Notable changes over **Redis 5** include:

- **Redis** now supports SSL on all channels.
- **Redis** now supports Access Control List (ACL), which defines user permissions for command calls and key pattern access.
- **Redis** now supports a new **RESP3** protocol, which returns more semantical replies.
- **Redis** can now optionally use threads to handle I/O.
- **Redis** now offers server-side support for client-side caching of key values.
- The **Redis** active expire cycle has been improved to enable faster eviction of expired keys.

Redis 6 is compatible with **Redis 5**, with the exception of this backward incompatible change:

- When a set key does not exist, the **SPOP <count>** command no longer returns null. In **Redis 6**, the command returns an empty set in this scenario, similar to a situation when it is called with a **0** argument.

To install the **redis:6** module stream, use:

```
# yum module install redis:6
```

If you want to upgrade from the **redis:5** stream, see Switching to a later stream .

For information about the length of support for the **redis** module streams, see the Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1862063)

A new module stream: postgresql:13

RHEL 8.4 introduces **PostgreSQL 13**, which provides a number of new features and enhancements over version 12. Notable changes include:

- Performance improvements resulting from de-duplication of B-tree index entries
- Improved performance for queries that use aggregates or partitioned tables
- Improved query planning when using extended statistics
- Parallelized vacuuming of indexes
- Incremental sorting

Note that support for Just-In-Time (JIT) compilation, available in upstream since **PostgreSQL 11**, is not provided by the **postgresql:13** module stream.

See also Using PostgreSQL.

To install the **postgresql:13** stream, use:

```
# yum module install postgresql:13
```

If you want to upgrade from an earlier **postgresql** stream within RHEL 8, follow the procedure described in Switching to a later stream and then migrate your **PostgreSQL** data as described in Migrating to a RHEL 8 version of PostgreSQL.

For information about the length of support for the **postgresql** module streams, see the Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1855776)

A new module stream: mariadb:10.5

MariaDB 10.5 is now available as a new module stream, **mariadb:10.5**. Notable enhancements over the previously available version 10.3 include:

- **MariaDB** now uses the **unix_socket** authentication plug-in by default. The plug-in enables users to use operating system credentials when connecting to **MariaDB** through the local Unix socket file.
- **MariaDB** supports a new **FLUSH SSL** command to reload SSL certificates without a server restart.
- **MariaDB** adds **mariadb-*** named binaries and **mysql*** symbolic links pointing to the **mariadb-*** binaires. For example, the **mysqladmin**, **mysqlaccess**, and **mysqlshow** symlinks point to the **mariadb-admin**, **mariadb-access**, and **mariadb-show** binaries, respectively.
- **MariaDB** supports a new **INET6** data type for storing IPv6 addresses.
- **MariaDB** now uses the Perl Compatible Regular Expressions (PCRE) library version 2.
- The **SUPER** privilege has been split into several privileges to better align with each user role. As a result, certain statements have changed required privileges.
- **MariaDB** adds a new global variable, **binlog_row_metadata**, as well as system variables and status variables to control the amount of metadata logged.

- The default value of the **eq_range_index_dive_limit** variable has been changed from **0** to **200**.
- A new **SHUTDOWN WAIT FOR ALL SLAVES** server command and a new **mysqladmin shutdown --wait-for-all-slaves** option have been added to instruct the server to shut down only after the last binlog event has been sent to all connected replicas.
- In parallel replication, the **slave_parallel_mode** variable now defaults to **optimistic**.

The **InnoDB** storage engine introduces the following changes:

- **InnoDB** now supports an instant **DROP COLUMN** operation and enables users to change the column order.
- Defaults of the following variables have been changed: **innodb_adaptive_hash_index** to **OFF** and **innodb_checksum_algorithm** to **full_crc32**.
- Several **InnoDB** variables have been removed or deprecated.

MariaDB Galera Cluster has been upgraded to version 4 with the following notable changes:

- **Galera** adds a new streaming replication feature, which supports replicating transactions of unlimited size. During an execution of streaming replication, a cluster replicates a transaction in small fragments.
- **Galera** now fully supports Global Transaction ID (GTID).
- The default value for the **wsrep_on** option in the **/etc/my.cnf.d/galera.cnf** file has changed from **1** to **0** to prevent end users from starting **wsrep** replication without configuring required additional options.

See also Using MariaDB.

To install the **mariadb:10.5** stream, use:

```
# yum module install mariadb:10.5
```

If you want to upgrade from the **mariadb:10.3** module stream, see Upgrading from MariaDB 10.3 to MariaDB 10.5.

For information about the length of support for the **mariadb** module streams, see the Red Hat Enterprise Linux 8 Application Streams Life Cycle.

(BZ#1855781)

MariaDB 10.5 provides the PAM plug-in version 2.0

MariaDB 10.5 adds a new version of the Pluggable Authentication Modules (PAM) plug-in. The PAM plug-in version 2.0 performs PAM authentication using a separate **setuid root** helper binary, which enables **MariaDB** to utilize additional PAM modules.

In **MariaDB 10.5**, the Pluggable Authentication Modules (PAM) plug-in and its related files have been moved to a new package, **mariadb-pam**. This package contains both PAM plug-in versions: version 2.0 is the default, and version 1.0 is available as the **auth_pam_v1** shared object library.

Note that the **mariadb-pam** package is not installed by default with the **MariaDB** server. To make the PAM authentication plug-in available in **MariaDB 10.5**, install the **mariadb-pam** package manually.

See also known issue PAM plug-in version 1.0 does not work in **MariaDB**.

(BZ#1936842)

A new package: mysql-selinux

RHEL 8.4 adds a new **mysql-selinux** package that provides an SELinux module with rules for the **MariaDB** and **MySQL** databases. The package is installed by default with the database server. The module's priority is set to **200**.

(BZ#1895021)

python-PyMySQL rebased to version 0.10.1

The **python-PyMySQL** package, which provides the pure-Python MySQL client library, has been updated to version 0.10.1. The package is included in the **python36**, **python38**, and **python39** modules.

Notable changes include:

- This update adds support for the **ed25519** and **caching_sha2_password** authentication mechanisms.
- The default character set in the **python38** and **python39** modules is **utf8mb4**, which aligns with upstream. The **python36** module preserves the default **latin1** character set to maintain compatibility with earlier versions of this module.
- In the **python36** module, the **/usr/lib/python3.6/site-packages/pymysql/tests/** directory is no longer available.

(BZ#1820628, BZ#1885641)

A new package: python3-pyodbc

This update adds the **python3-pyodbc** package to RHEL 8. The **pyodbc** Python module provides access to Open Database Connectivity (ODBC) databases. This module implements the Python DB API 2.0 specification and can be used with third-party ODBC drivers. For example, you can now use the Performance Co-Pilot (**pcp**) to monitor performance of the SQL Server.

(BZ#1881490)

A new package: micropipenv

A new **micropipenv** package is now available. It provides a lightweight wrapper for the **pip** package installer to support **Pipenv** and **Poetry** lock files.

Note that the **micropipenv** package is distributed in the AppStream repository and is provided under the Compatibility level 4. For more information, see the Red Hat Enterprise Linux 8 Application Compatibility Guide.

(BZ#1849096)

New packages: py3c-devel and py3c-docs

RHEL 8.4 introduces new **py3c-devel** and **py3c-docs** packages, which simplify porting C extensions to Python 3. These packages include a detailed guide and a set of macros for easier porting.

Note that the **py3c-devel** and **py3c-docs** packages are distributed through the unsupported CodeReady Linux Builder (CRB) repository .

(BZ#1841060)

Enhanced ProxyRemote directive for configuring httpd

The **ProxyRemote** configuration directive in the Apache HTTP Server has been enhanced to optionally take user name and password credentials. These credentials are used for authenticating to the remote proxy using HTTP **Basic** authentication. This feature has been backported from **httpd 2.5**.

(BZ#1869576)

Non-end-entity certificates can be used with the SSLProxyMachineCertificateFile and SSLProxyMachineCertificatePath httpd directives

With this update, you can use non-end-entity (non-leaf) certificates, such as a Certificate Authority (CA) or intermediate certificate, with the **SSLProxyMachineCertificateFile** and **SSLProxyMachineCertificatePath** configuration directives in the Apache HTTP Server. The Apache HTTP server now treats such certificates as trusted CAs, as if they were used with the **SSLProxyMachineCertificateChainFile** directive. Previously, if non-end-entity certificates were used with the **SSLProxyMachineCertificateFile** and **SSLProxyMachineCertificatePath** directives, **httpd** failed to start with a configuration error.

(BZ#1883648)

A new SecRemoteTimeout directive in the mod_security module

Previously, you could not modify the default timeout for retrieving remote rules in the **mod_security** module for the Apache HTTP Server. With this update, you can set a custom timeout in seconds using the new **SecRemoteTimeout** configuration directive.

When the timeout has been reached, **httpd** now fails with an error message **Timeout was reached**. Note that in this scenario, the error message also contains **Syntax error** even if the configuration file is syntactically valid. The **httpd** behavior upon timeout depends on the value of the **SecRemoteRulesFailAction** configuration directive (the default value is **Abort**).

(BZ#1824859)

The mod_fcgid module can now pass up to 1024 environment variables to an FCGI server process

With this update, the **mod_fcgid** module for the Apache HTTP Server can pass up to 1024 environment variables to a FastCGI (FCGI) server process. The previous limit of 64 environment variables could cause applications running on the FCGI server to malfunction.

(BZ#1876525)

perl-IO-String is now available in the AppStream repository

The **perl-IO-String** package, which provides the Perl **IO::String** module, is now distributed through the supported AppStream repository. In previous releases of RHEL 8, the **perl-IO-String** package was available in the unsupported CodeReady Linux Builder repository.

(BZ#1890998)

A new package: quota-devel

RHEL 8.4 introduces the **quota-devel** package, which provides header files for implementing the **quota** Remote Procedure Call (RPC) service.

Note that the **quota-devel** package is distributed through the unsupported CodeReady Linux Builder (CRB) repository.

(BZ#1868671)

4.12. COMPILERS AND DEVELOPMENT TOOLS

The glibc library now supports glibc-hwcaps subdirectories for loading optimized shared library implementations

On certain architectures, hardware upgrades sometimes caused **glibc** to load libraries with baseline optimizations, rather than optimized libraries for the previous hardware generation. Additionally, when running on AMD CPUs, optimized libraries were not loaded at all.

With this enhancement, **glibc** supports locating optimized library implementations in the **glibc-hwcaps** subdirectories. The dynamic loader checks for library files in the sub-directories based on the CPU in use and its hardware capabilities. This feature is available on following architectures: IBM Power Systems (little endian), IBM Z, 64-bit AMD and Intel.

(BZ#1817513)

The glibc dynamic loader now activates selected audit modules at run time

Previously, the **binutils** link editor **ld** supported the **--audit** option to select audit modules for activation at run time, but the **glibc** dynamic loader ignored the request. With this update, the **glib** dynamic loader no longer ignores the request, and loads the indicated audit modules. As a result, it is possible to activate audit modules for specific programs without writing wrapper scripts or using similar mechanisms.

(BZ#1871385)

glibc now provides improved performance on IBM POWER9

This update introduces new implementations of the functions **strlen**, **strcpy**, **stpcpy**, and **rawmemchr** for IBM POWER9. As a result, these functions now execute faster on IBM POWER9 hardware which leads to performance gains.

(BZ#1871387)

Optimized performance of memcpy and memset on IBM Z

With this enhancement, the core library implementation for the **memcpy** and **memset** APIs were adjusted to accelerate both small (< 64KiB) and larger data copies on IBM Z processors. As a result, applications working with in-memory data now benefit from significantly improved performance across a wide variety of workloads.

(BZ#1871395)

GCC now supports the ARMv8.1 LSE atomic instructions

With this enhancement, the GCC compiler now supports Large System Extensions (LSE), atomic instructions added with the ARMv8.1 specification. These instructions provide better performance in multi-threaded applications than the ARMv8.0 Load-Exclusive and Store-Exclusive instructions.

(BZ#1821994)

GCC now emits vector alignment hints for certain IBM Z systems

This update enables the GCC compiler to emit vector load and store alignment hints for IBM z13 processors. To use this enhancement the assembler must support such hints. As a result, users now benefit from improved performance of certain vector operations.

(BZ#1850498)

Dyninst rebased to version 10.2.1

The Dyninst binary analysis and modification tool has been updated to version 10.2.1. Notable bug fixes and enhancements include:

- Support for the elfutils **debuginfod** client library.
- Improved parallel binary code analysis.
- Improved analysis and instrumentation of large binaries.

(BZ#1892001)

elfutils rebased to version 0.182

The **elfutils** package has been updated to version 0.182. Notable bug fixes and enhancements include:

- Recognizes the **DW_CFA_AARCH64_negate_ra_state** instruction. When Pointer Authentication Code (PAC) is not enabled, you can use **DW_CFA_AARCH64_negate_ra_state** to unwind code that is compiled for PAC on the 64-bit ARM architecture.
- **elf_update** now fixes bad **sh_addralign** values in sections that have set the **SHF_COMPRESSED** flag.
- **debuginfod-client** now supports kernel ELF images compressed with ZSTD.
- **debuginfod** has a more efficient package traversal, tolerating various errors during scanning. The grooming process is more visible and interruptible, and provides more Prometheus metrics.

(BZ#1875318)

SystemTap rebased to version 4.4

The SystemTap instrumentation tool has been updated to version 4.4, which provides multiple bug fixes and enhancements. Notable changes include:

- Performance and stability improvements to user-space probing.
- Users can now access implicit thread local storage variables on these architectures: AMD64, Intel 64, IBM Z, the little-endian variant of IBM Power Systems.
- Initial support for processing of floating point values.
- Improved concurrency for scripts using global variables. The locks required to protect concurrent access to global variables have been optimized so that they span the smallest possible critical region.
- New syntax for defining aliases with both a prologue and an epilogue.
- New **@probewrite** predicate.
- **syscall** arguments are writable again.

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

(BZ#1875341)

Valgrind now supports IBM z14 instructions

With this update, the Valgrind tool suite supports instructions for the IBM z14 processor. As a result, you can now use the Valgrind tools to debug programs using the z14 vector instructions and the miscellaneous z14 instruction set.

(BZ#1504123)

CMake rebased to version 3.18.2

The CMake build system has been upgraded from version 3.11.4 to version 3.18.2. It is available in RHEL 8.4 as the **cmake-3.18.2-8.el8** package.

To use CMake on a project that requires the version 3.18.2 or less, use the command **cmake_minimum_required(version x.y.z)**.

For further information on new features and deprecated functionalities, see the CMake Release Notes .

(BZ#1816874)

libmpc rebased to version 1.1.0

The **libmpc** package has been rebased to version 1.1.0, which provides several enhancements and bug fixes over the previous version. For details, see GNU MPC 1.1.0 release notes .

(BZ#1835193)

Updated GCC Toolset 10

GCC Toolset 10 is a compiler toolset that provides recent versions of development tools. It is available as an Application Stream in the form of a Software Collection in the **AppStream** repository.

Notable changes introduced with RHEL 8.4 include:

- The GCC compiler has been updated to the upstream version, which provides multiple bug fixes.
- **elfutils** has been updated to version 0.182.
- Dyninst has been updated to version 10.2.1.
- SystemTap has been updated to version 4.4.

The following tools and versions are provided by GCC Toolset 10:

Tool	Version
GCC	10.2.1
GDB	9.2
Valgrind	3.16.0

Tool	Version
SystemTap	4.4
Dyninst	10.2.1
binutils	2.35
elfutils	0.182
dwz	0.12
make	4.2.1
strace	5.7
ltrace	0.7.91
annobin	9.29

To install GCC Toolset 10, run the following command as root:

```
# yum install gcc-toolset-10
```

To run a tool from GCC Toolset 10:

```
$ scl enable gcc-toolset-10 tool
```

To run a shell session where tool versions from GCC Toolset 10 override system versions of these tools:

```
$ scl enable gcc-toolset-10 bash
```

For more information, see Using GCC Toolset.

The GCC Toolset 10 components are available in the two container images:

- **rhel8/gcc-toolset-10-toolchain**, which includes the GCC compiler, the GDB debugger, and the **make** automation tool.
- **rhel8/gcc-toolset-10-perftools**, which includes the performance monitoring tools, such as SystemTap and Valgrind.

To pull a container image, run the following command as root:

```
# podman pull registry.redhat.io/<image_name>
```

Note that only the GCC Toolset 10 container images are now supported. Container images of earlier GCC Toolset versions are deprecated.

For details regarding the container images, see Using the GCC Toolset container images.

(BZ#1918055)

GCC Toolset 10: GCC now supports bfloat16

In GCC Toolset 10, the GCC compiler now supports the **bfloat16** extension through ACLE Intrinsics. This enhancement provides high-performance computing.

(BZ#1656139)

GCC Toolset 10: GCC now supports ENQCMD and ENQCMDS instructions on Intel Sapphire Rapids processors

In GCC Toolset 10, the GNU Compiler Collection (GCC) now supports the **ENQCMD** and **ENQCMDS** instructions, which you can use to submit work descriptors to devices automatically. To apply this enhancement, run GCC with the **-menqcmd** option.

(BZ#1891998)

GCC Toolset 10: Dyninst rebased to version 10.2.1

In GCC Toolset 10, the Dyninst binary analysis and modification tool has been updated to version 10.2.1. Notable bug fixes and enhancements include:

- Support for the elfutils **debuginfod** client library.
- Improved parallel binary code analysis.
- Improved analysis and instrumentation of large binaries.

(BZ#1892007)

GCC Toolset 10: elfutils rebased to version 0.182

In GCC Toolset 10, the **elfutils** package has been updated to version 0.182. Notable bug fixes and enhancements include:

- Recognizes the **DW_CFA_AARCH64_negate_ra_state** instruction. When Pointer Authentication Code (PAC) is not enabled, you can use **DW_CFA_AARCH64_negate_ra_state** to unwind code that is compiled for PAC on the 64-bit ARM architecture.
- **elf_update** now fixes bad **sh_addralign** values in sections that have set the **SHF_COMPRESSED** flag.
- **debuginfod-client** now supports kernel ELF images compressed with ZSTD.
- **debuginfod** has a more efficient package traversal, tolerating various errors during scanning. The grooming process is more visible and interruptible, and provides more Prometheus metrics.

(BZ#1879758)

Go Toolset rebased to version 1.15.7

Go Toolset has been upgraded to 1.15.7. Notable enhancements include:

- Linking is now faster and requires less memory due to the newly implemented object file format and increased concurrency of internal phases. With this enhancement, internal linking is now the default. To disable this setting, use the compiler flag **-ldflags=-linkmode=external**.
- Allocating small objects has been improved for high core counts, including worst-case latency.

- Treating the **CommonName** field on X.509 certificates as a host name when no **Subject Alternative Names** are specified is now disabled by default. To enable it, add the value **x509ignoreCN=0** to the **GODEBUG** environment variable.
- **GOPROXY** now supports skipping proxies that return errors.
- Go now includes the new package **time/tzdata**. It enables you to embed the timezone database into a program even if the timezone database is not available on your local system.

For more information on Go Toolset, go to Using Go Toolset.

(BZ#1870531)

Rust Toolset rebased to version 1.49.0

Rust Toolset has been updated to version 1.49.0. Notable changes include:

- You can now use the path of a rustdoc page item to link to it in rustdoc.
- The rust test framework now hides thread output. Output of failed tests still show in the terminal.
- You can now use **[T; N]: TryFrom<Vec<T>>** to turn a vector into an array of any length.
- You can now use **slice::select_nth_unstable** to perform ordered partitioning. This function is also available with the following variants:
  - **slice::select_nth_unstable_by** provides a comparator function.
  - **slice::select_nth_unstable_by_key** provides a key extraction function.
- You can now use **ManuallyDrop** as the type of a union field. It is also possible to use **impl Drop for Union** to add the Drop trait to existing unions. This makes it possible to define unions where certain fields need to be dropped manually.
- Container images for Rust Toolset have been deprecated and Rust Toolset has been added to the Universal Base Images (UBI) repositories.

For further information, see Using Rust Toolset.

(BZ#1896712)

LLVM Toolset rebased to version 11.0.0

LLVM Toolset has been upgraded to version 11.0.0. Notable changes include:

- Support for the **-fstack-clash-protection** command-line option has been added to the AMD and Intel 64-bit architectures, IBM Power Systems, Little Endian, and IBM Z. This new compiler flag protects from stack-clash attacks by automatically checking each stack page.
- The new compiler flag **ffp-exception-behavior={ignore,maytrap,strict}** enables the specification of floating-point exception behavior. The default setting is **ignore**.
- The new compiler flag **ffp-model={precise,strict,fast}** allows the simplification of single purpose floating-point options. The default setting is **precise**.

- The new compiler flag **-fno-common** is now enabled by default. With this enhancement, code written in C using tentative variable definitions in multiple translation units now triggers multiple-definition linker errors. To disable this setting, use the **-fcommon** flag.
- Container images for LLVM Toolset have been deprecated and LLVM Toolset has been added to the Universal Base Images (UBI) repositories.

For more information, see Using LLVM Toolset.

(BZ#1892716)

pcp rebased to version 5.2.5

The **pcp** package has been upgraded to version 5.2.5. Notable changes include:

- SQL Server metrics support via a secure connection.
- **eBPF**/**BCC** netproc module with per-process network metrics.
- **pmdaperfevent(1)** support for the **hv_24x7 core-level** and **hv_gpci** event metrics.
- New Linux process accounting metrics, Linux ZFS metrics, Linux XFS metric, Linux kernel socket metrics, Linux multipath TCP metrics, Linux memory and ZRAM metrics, and S.M.A.R.T. metric support for NVM Express disks.
- New **pcp-htop(1)** utility to visualize the system and process metrics.
- New pmrepconf(1) utility to generate the **pmrep**/**pcp2xxx** configurations.
- New **pmiectl(1)** utility for controlling the **pmie** services.
- New **pmlogctl(1)** utility for controlling the **pmlogger** services.
- New **pmlogpaste(1)** utility for writing log string metrics.
- New **pcp-atop(1)** utility to process accounting statistics and per-process network statistics reporting.
- New **pmseries(1)** utility to query functions, language extensions, and REST API.
- New **pmie(1)** rules for detecting OOM kills and socket connection saturation.
- Bug fixes in the **pcp-atopsar(1)**, **pcp-free(1)**, **pcp-dstat(1)**, **pmlogger(1)**, and **pmchart(1)** utilities.
- REST API and C API support for per-context derived metrics.
- Improved OpenMetrics metric metadata (units, semantics).
- Rearranged installed /**var** file system layouts extensively.

(BZ#1854035)

Accessing remote hosts through a central pmproxy for the Vector data source in grafana-pcp

In some environments, the network policy does not allow connections from the dashboard viewer's browser to the monitored hosts directly. This update makes it possible to customize the **hostspec** in order to connect to a central **pmproxy**, which forwards the requests to the individual hosts.

(BZ#1845592)

grafana rebased to version 7.3.6

The **grafana** package has been upgraded to version 7.3.6. Notable changes include:

- New panel editor and new data transformations feature
- Improved time zone support
- Default provisioning path now changed from the **/usr/share/grafana/conf/provisioning** to the **/etc/grafana/provisioning** directory. You can configure this setting in the **/etc/grafana/grafana.ini** configuration file.

For more information, see What's New in Grafana v7.0 , What's New in Grafana v7.1, What's New in Grafana v7.2, and What's New in Grafana v7.3 .

(BZ#1850471)

grafana-pcp rebased to version 3.0.2

The **grafana-pcp** package has been upgraded to version 3.0.2. Notable changes include:

- Redis:
  - Supports creating an alert in Grafana.
  - Using the **label_values(metric, label)** in a Grafana variable query is deprecated due to performance reasons. The **label_values(label)** query is still supported.
- Vector:
  - Supports derived metrics, which allows the usage of arithmetic operators and statistical functions inside a query. For more information, see the **pmRegisterDerived(3)** man page.
  - Configurable hostspec, where you can access remote Performance Metrics Collector Daemon (PMCDs) through a central **pmproxy**.
  - Automatically configures the unit of the panel.
- Dashboards:
  - Detects potential performance issues and shows possible solutions with the checklist dashboards, using the Utilization Saturation and Errors (USE) method.
  - New MS SQL server dashboard, **eBPF/BCC** dashboard, and container overview dashboard with the **CGroups v2**.
  - All dashboards are now located in the **Dashboards** tab in the **Datasource** settings pages and are not imported automatically.

Upgrade notes:

Update the Grafana configuration file:

1. Edit the **/etc/grafana/grafana.ini** Grafana configuration file and make sure that the following option is set:

```
allow_loading_unsigned_plugins = pcp-redis-datasource
```

2. Restart the Grafana server:

```
# systemctl restart grafana-server
```

(BZ#1854093)

Active Directory authentication for accessing SQL Server metrics in PCP

With this update, a system administrator can configure **pmdamssql(1)** to connect securely to the SQL Server metrics using Active Directory (AD) authentication.

(BZ#1847808)

grafana-container rebased to version 7.3.6

The **rhel8/grafana** container image provides Grafana. Grafana is an open source utility with metrics dashboard, and graphic editor for Graphite, Elasticsearch, OpenTSDB, Prometheus, InfluxDB, and Performance Co-Pilot (PCP). The **grafana-container** package has been upgraded to version 7.3.6. Notable changes include:

- The **grafana** package is now updated to version 7.3.6.
- The **grafana-pcp** package is now updated to version 3.0.2.

The rebase updates the **rhel8/grafana** image in the Red Hat Container Registry.

To pull this container image, execute the following command:

```
# podman pull registry.redhat.io/rhel8/grafana
```

(BZ#1916154)

pcp-container rebased to version 5.2.5

The **rhel8/pcp** container image provides Performance Co-Pilot, which is a system performance analysis toolkit. The **pcp-container** package has been upgraded to version 5.2.5. Notable changes include:

- The **pcp** package is now updated to version 5.2.5.
- Introduced a new **PCP_SERVICES** environment variable, which specifies a comma-separated list of PCP services to start inside the container.

The rebase updates the **rhel8/pcp** image in the Red Hat Container Registry.

To pull this container image, execute the following command:

```
# podman pull registry.redhat.io/rhel8/pcp
```

(BZ#1916155)

JDK Mission Control rebased to version 8.0.0

The JDK Mission Control (JMC) profiler for HotSpot JVMs, provided by the **jmc:rhel8** module stream, has been upgraded to version 8.0.0. Notable enhancements include:

- The **Treemap** viewer has been added to the **JOverflow** plug-in for visualizing memory usage by classes.
- The **Threads** graph has been enhanced with more filtering and zoom options.
- JDK Mission Control now provides support for opening JDK Flight Recorder recordings compressed with the LZ4 algorithm.
- New columns have been added to the **Memory** and **TLAB** views to help you identify areas of allocation pressure.
- **Graph** view has been added to improve visualization of stack traces.
- The **Percentage** column has been added to histogram tables.

JMC in RHEL 8 requires JDK version 8 or later to run. Target Java applications must run with at least OpenJDK version 8 so that JMC can access JDK Flight Recorder features.

The **jmc:rhel8** module stream has two profiles:

- The **common** profile, which installs the entire JMC application
- The **core** profile, which installs only the core Java libraries (**jmc-core**)

To install the **common** profile of the **jmc:rhel8** module stream, use:

```
# yum module install jmc:rhel8/common
```

Change the profile name to **core** to install only the **jmc-core** package.

(BZ#1919283)

4.13. IDENTITY MANAGEMENT

Making Identity Management more inclusive

Red Hat is committed to using conscious language. See details about this initiative in Making open source more inclusive.

In Identity Management, planned terminology replacements include:

- ***block list*** replaces *blacklist*
- ***allow list*** replaces *whitelist*
- ***secondary*** replaces *slave*
- The word *master* is going to be replaced with more precise language, depending on the context:
  - ***IdM server*** replaces *IdM master*
  - ***CA renewal server*** replaces *CA renewal master*
  - ***CRL publisher server*** replaces *CRL master*

- ***multi-supplier*** replaces *multi-master*

(JIRA:RHELPLAN-73418)

The dsidm utility supports renaming and moving entries

With this enhancement, you can use the **dsidm** utility to rename and move users, groups, POSIX groups, roles, and organizational units (OU) in Directory Server. For further details and examples, see the Renaming Users, Groups, POSIX Groups, and OUs section in the Directory Server Administration Guide.

(BZ#1859218)

Deleting Sub-CAs in IdM

With this enhancement, if you run the **ipa ca-del** command and have not disabled the Sub-CA, an error indicates the Sub-CA cannot be deleted and it must be disabled. First run the **ipa ca-disable** command to disable the Sub-CA and then delete it using the **ipa ca-del** command.

Note that you cannot disable or delete the IdM CA.

(JIRA:RHELPLAN-63081)

IdM now supports new Ansible management role and modules

RHEL 8.4 provides Ansible modules for automated management of role-based access control (RBAC) in Identity Management (IdM), an Ansible role for backing up and restoring IdM servers, and an Ansible module for location management:

- You can use the **ipapermission** module to create, modify, and delete permissions and permission members in IdM RBAC.
- You can use the **ipaprivilege** module to create, modify, and delete privileges and privilege members in IdM RBAC.
- You can use the **iparole** module to create, modify, and delete roles and role members in IdM RBAC.
- You can use the **ipadelegation** module to delegate permissions over users in IdM RBAC.
- You can use the **ipaselfservice** module to create, modify, and delete self-service access rules in IdM.
- You can use the **ipabackup** role to create, copy, and remove IdM server backups and restore an IdM server either locally or from the control node.
- You can use the **ipalocation** module to ensure the presence or absence of the physical locations of hosts, such as their data center racks.

(JIRA:RHELPLAN-72660)

IdM in FIPS mode now supports a cross-forest trust with AD

With this enhancement, administrators can establish a cross-forest trust between an IdM domain with FIPS mode enabled and an Active Directory (AD) domain. Note that you cannot establish a trust using a shared secret while FIPS mode is enabled in IdM, see FIPS compliance.

(JIRA:RHELPLAN-58629)

AD users can now log in to IdM with UPN suffixes subordinate to known UPN suffixes

Previously, Active Directory (AD) users could not log into Identity Management (IdM) with a Universal Principal Name (UPN) (for example, **sub1.ad-example.com**) that is a subdomain of a known UPN suffix (for example, **ad-example.com**) because internal Samba processes filtered subdomains as duplicates of any Top Level Names (TLNs). This update validates UPNs by testing if they are subordinate to the known UPN suffixes. As a result, users can now log in using subordinate UPN suffixes in the described scenario.

(BZ#1891056)

IdM now supports new password policy options

With this update, Identity Management (IdM) supports additional **libpwquality** library options:

--maxrepeat

Specifies the maximum number of the same character in sequence.

--maxsequence

Specifies the maximum length of monotonic character sequences (**abcd**).

--dictcheck

Checks if the password is a dictionary word.

--usercheck

Checks if the password contains the username.

If any of the new password policy options are set, then the minimum length of passwords is 6 characters regardless of the value of the **--minlength** option. The new password policy settings are applied only to new passwords.

In a mixed environment with RHEL 7 and RHEL 8 servers, the new password policy settings are enforced only on servers running on RHEL 8.4 and later. If a user is logged in to an IdM client and the IdM client is communicating with an IdM server running on RHEL 8.3 or earlier, then the new password policy requirements set by the system administrator will not be applied. To ensure consistent behavior, upgrade or update all servers to RHEL 8.4 and later.

(BZ#1340463)

Improved Active Directory site discovery process

The SSSD service now discovers Active Directory sites in parallel over connection-less LDAP (CLDAP) to multiple domain controllers to speed up site discovery in situations where some domain controllers are unreachable. Previously, site discovery was performed sequentially and, in situations where domain controllers were unreachable, a timeout eventually occurred and SSSD went offline.

(BZ#1819012)

The default value of nsslapd-nagle has been turned off to increase the throughput

Previously, the **nsslapd-nagle** parameter in the **cn=config** entry was enabled by default. As a consequence, Directory Server performed a high number of **setsocketopt** system calls which slowed down the server. This update changes the default value of **nsslapd-nagle** to **off**. As a result, Directory Server performs a lower number of **setsocketopt** system calls and can handle a higher number of operations per second.

(BZ#1996076)

Enabling or disabling SSSD domains within the [domain] section of the sssd.conf file

With this update, you can now enable or disable an SSSD domain by modifying its respective **[domain]** section in the **sssd.conf** file.

Previously, if your SSSD configuration contained a standalone domain, you still had to modify the **domains** option in the **[sssd]** section of the **sssd.conf** file. This update allows you to set the **enabled=** option in the domain configuration to true or false.

- Setting the **enabled** option to true enables a domain, even if it is not listed under the **domains** option in the **[sssd]** section of the **sssd.conf** file.
- Setting the **enabled** option to false disables a domain, even if it is listed under the **domains** option in the **[sssd]** section of the **sssd.conf** file.
- If the **enabled** option is not set, the configuration in the **domains** option in the **[sssd]** section of the **sssd.conf** is used.

(BZ#1884196)

Added an option to manually control the maximum offline timeout

The **offline_timeout** period determines the time incrementation between attempts by SSSD to go back online. Previously, the maximum possible value for this interval was hardcoded to 3600 seconds, which was adequate for general usage but resulted in issues in fast or slow changing environments.

This update adds the **offline_timeout_max** option to manually control the maximum length of each interval, allowing you more flexibility to track the server behavior in SSSD.

Note that you should set this value in correlation to the **offline_timeout** parameter value. A value of 0 disables the incrementing behavior.

(BZ#1884213)

Support for exclude_users and exclude_groups with scope=all in SSSD session recording configuration

Red Hat Enterprise 8.4 now provides new SSSD options for defining session recording for large lists of groups or users:

1. **exclude_users**
   A comma-separated list of users to be excluded from recording, only applicable with the **scope=all** configuration option.
2. **exclude_groups**
   A comma-separated list of groups, members of which should be excluded from recording. Only applicable with the **scope=all** configuration option.

For more information, refer to the **sssd-session-recording** man page.

(BZ#1784459)

samba rebased to version 4.13.2

The *samba* packages have been upgraded to upstream version 4.13.2, which provides a number of bug fixes and enhancements over the previous version:

- To avoid a security issue that allows unauthenticated users to take over a domain using the **netlogon** protocol, ensure that your Samba servers use the default value (**yes**) of the **server schannel** parameter. To verify, use the **testparm -v | grep 'server schannel'** command. For

further details, see CVE-2020-1472.

- The Samba "wide links" feature has been converted to a VFS module .
- Running Samba as a PDC or BDC is deprecated .
- You can now use Samba on RHEL with FIPS mode enabled. Due to the restrictions of the FIPS mode:
  - You cannot use NT LAN Manager (NTLM) authentication because the RC4 cipher is blocked.
  - By default in FIPS mode, Samba client utilities use Kerberos authentication with AES ciphers.
  - You can use Samba as a domain member only in Active Directory (AD) or Red Hat Identity Management (IdM) environments with Kerberos authentication that uses AES ciphers. Note that Red Hat continues supporting the primary domain controller (PDC) functionality IdM uses in the background.
- The following parameters for less-secure authentication methods, which are only usable over the server message block version 1 (SMB1) protocol, are now deprecated:
  - **client plaintext auth**
  - **client NTLMv2 auth**
  - **client lanman auth**
  - **client use spnego**
- An issue with the GlusterFS write-behind performance translator, when used with Samba, has been fixed to avoid data corruption.
- The minimum runtime support is now Python 3.6.
- The deprecated **ldap ssl ads** parameter has been removed.

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

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

(BZ#1878109)

New GSSAPI PAM module for passwordless sudo authentication with SSSD

With the new **pam_sss_gss.so** Pluggable Authentication Module (PAM), you can configure the System Security Services Daemon (SSSD) to authenticate users to PAM-aware services with the Generic Security Service Application Programming Interface (GSSAPI).

For example, you can use this module for passwordless **sudo** authentication with a Kerberos ticket. For additional security in an IdM environment, you can configure SSSD to grant access only to users with specific authentication indicators in their tickets, such as users that have authenticated with a smart card or a one-time password.

For additional information, see Granting sudo access to an IdM user on an IdM client .

(BZ#1893698)

Directory Server rebased to version 1.4.3.16

The **389-ds-base** packages have been upgraded to upstream version 1.4.3.16, which provides a number of bug fixes and enhancements over the previous version. For a complete list of notable changes, read the upstream release notes before updating:

- https://www.port389.org/docs/389ds/releases/release-1-4-3-16.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-15.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-14.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-13.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-12.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-11.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-10.html
- https://www.port389.org/docs/389ds/releases/release-1-4-3-9.html

(BZ#1862529)

Directory Server now logs the work and operation time in RESULT entries

With this update, Directory Server now logs two additional time values in **RESULT** entries in the **/var/log/dirsrv/slapd-<instance_name>/access** file:

- The **wtime** value indicates how long it took for an operation to move from the work queue to a worker thread.
- The **optime** value shows the time the actual operation took to be completed once a worker thread started the operation.

The new values provide additional information about how the Directory Server handles load and processes operations.

For further details, see the Access Log Reference section in the Red Hat Directory Server Configuration, Command, and File Reference.

(BZ#1850275)

Directory Server can now reject internal unindexed searches

This enhancement adds the **nsslapd-require-internalop-index** parameter to the **cn=*<database_name>*,cn=ldbm database,cn=plugins,cn=config** entry to reject internal unindexed searches. When a plug-in modifies data, it has a write lock on the database. On large databases, if a plug-in then executes an unindexed search, the plug-in sometimes uses all database locks, which corrupts the database or causes the server to become unresponsive. To avoid this problem, you can now reject internal unindexed searches by enabling the **nsslapd-require-internalop-index** parameter.

(BZ#1851975)

4.14. DESKTOP

You can configure the unresponsive application timeout in GNOME

GNOME periodically sends a signal to every application to detect if the application is unresponsive. When GNOME detects an unresponsive application, it displays a dialog over the application window that asks if you want to stop the application or wait.

Certain applications cannot respond to the signal in time. As a consequence, GNOME displays the dialog even when the application is working properly.

With this update, you can configure the time between the signals. The setting is stored in the **org.gnome.mutter.check-alive-timeout** GSettings key. To completely disable the unresponsive application detection, set the key to 0.

For details on configuring a GSettings key, see Working with GSettings keys on command line .

(BZ#1886034)

4.15. GRAPHICS INFRASTRUCTURES

Intel Tiger Lake GPUs are now supported

This release adds support for the Intel Tiger Lake CPU microarchitecture with integrated graphics. This includes Intel UHD Graphics and Intel Xe integrated GPUs found with the following CPU models:

- Intel Core i7-1160G7
- Intel Core i7-1185G7
- Intel Core i7-1165G7
- Intel Core i7-1165G7
- Intel Core i7-1185G7E
- Intel Core i7-1185GRE
- Intel Core i7-11375H
- Intel Core i7-11370H
- Intel Core i7-1180G7
- Intel Core i5-1130G7
- Intel Core i5-1135G7
- Intel Core i5-1135G7
- Intel Core i5-1145G7E
- Intel Core i5-1145GRE
- Intel Core i5-11300H
- Intel Core i5-1145G7
- Intel Core i5-1140G7

- Intel Core i3-1115G4
- Intel Core i3-1115G4
- Intel Core i3-1110G4
- Intel Core i3-1115GRE
- Intel Core i3-1115G4E
- Intel Core i3-1125G4
- Intel Core i3-1125G4
- Intel Core i3-1120G4
- Intel Pentium Gold 7505
- Intel Celeron 6305
- Intel Celeron 6305E

You no longer have to set the **i915.alpha_support=1** or **i915.force_probe=*** kernel option to enable Tiger Lake GPU support.

(BZ#1882620)

Intel GPUs that use the 11th generation Core microprocessors are now supported

This release adds support for the 11th generation Core CPU architecture (formerly known as *Rocket Lake*) with Xe gen 12 integrated graphics, which is found in the following CPU models:

- Intel Core i9-11900KF
- Intel Core i9-11900K
- Intel Core i9-11900
- Intel Core i9-11900F
- Intel Core i9-11900T
- Intel Core i7-11700K
- Intel Core i7-11700KF
- Intel Core i7-11700T
- Intel Core i7-11700
- Intel Core i7-11700F
- Intel Core i5-11500T
- Intel Core i5-11600
- Intel Core i5-11600K

- Intel Core i5-11600KF
- Intel Core i5-11500
- Intel Core i5-11600T
- Intel Core i5-11400
- Intel Core i5-11400F
- Intel Core i5-11400T

(BZ#1784246, BZ#1784247, BZ#1937558)

Nvidia Ampere is now supported

This release adds support for the Nvidia Ampere GPUs that use the GA102 or GA104 chipset. That includes the following GPU models:

- GeForce RTX 3060 Ti
- GeForce RTX 3070
- GeForce RTX 3080
- GeForce RTX 3090
- RTX A4000
- RTX A5000
- RTX A6000
- Nvidia A40

Note that the **nouveau** graphics driver does not yet support 3D acceleration with the Nvidia Ampere family.

(BZ#1916583)

Various updated graphics drivers

The following graphics drivers have been updated to the latest upstream version:

- The Matrox **mgag200** driver
- The Aspeed **ast** driver

(JIRA:RHELPLAN-72994, BZ#1854354, BZ#1854367)

4.16. THE WEB CONSOLE

Software Updates page checks for required restarts

With this update, the Software Updates page in the RHEL web console checks if it is sufficient to only restart some services or running processes for updates to become effective after installation. In these cases this avoids having to reboot the machine.

(JIRA:RHELPLAN-59941)

Graphical performance analysis in the web console

With this update the system graphs page has been replaced with a new dedicated page for analyzing the performance of a machine. To view the performance metrics, click **View details and history** from the **Overview** page. It shows current metrics and historical events based on the Utilization Saturation, and Errors (USE) method.

(JIRA:RHELPLAN-59938)

Web console assists with SSH key setup

Previously, the web console allowed logging into remote hosts with your initial login password when **Reuse my password for remote connections** was selected during login. This option has been removed, and instead of that the web console now helps with setting up SSH keys for users that want automatic and password-less login to remote hosts.

Check Managing remote systems in the web console for more details.

(JIRA:RHELPLAN-59950)

4.17. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The RELP secure transport support added to the Logging role configuration

Reliable Event Logging Protocol, RELP, is a secure, reliable protocol to forward and receive log messages among **rsyslog** servers. With this enhancement, administrators can now benefit from the RELP, which is a useful protocol with high demands from **rsyslog** users, as **rsyslog** servers are capable of forwarding and receiving log messages over the RELP protocol.

(BZ#1889484)

SSH Client RHEL System Role is now supported

Previously, there was no vendor-supported automation tooling to configure RHEL SSH in a consistent and stable manner for servers and clients. With this enhancement, you can use the RHEL System Roles to configure SSH clients in a systematic and unified way, independently of the operating system version.

(BZ#1893712)

An alternative to the traditional RHEL System Roles format: Ansible Collection

RHEL 8.4 introduces RHEL System Roles in the Collection format, available as an option to the traditional RHEL System Roles format.

This update introduces the concept of a fully qualified collection name (FQCN), that consists of a namespace and the collection name. For example, the Kernel role fully qualified name is: **redhat.rhel_system_roles.kernel_settings**

- The combination of a namespace and a collection name guarantees that the objects are unique.
- The combination of a namespace and a collection name ensures that the objects are shared across the Collections and namespaces without any conflicts.

Install the Collection using an RPM package. Ensure that you have the **python3-jmespath** installed on the host on which you execute the playbook:

```
# yum install rhel-system-roles
```

The RPM package includes the roles in both the legacy Ansible Roles format as well as the new Ansible Collection format. For example, to use the network role, perform the following steps:

Legacy format:

```
---
- hosts: all
  roles:
rhel-system-roles.network
```

Collection format:

```
---
- hosts: all
  roles:
redhat.rhel_system_roles.network
```

If you are using Automation Hub and want to install the System Roles Collection hosted in Automation Hub, enter the following command:

```
$ ansible-galaxy collection install redhat.rhel_system_roles
```

Then you can use the roles in the Collection format, as previously described. This requires configuring your system with the ansible-galaxy command to use Automation Hub instead of Ansible Galaxy. See How to configure the **ansible-galaxy** client to use Automation Hub instead of Ansible Galaxy for more details.

(BZ#1893906)

Metrics role supports configuration and enablement of metrics collection for SQL server via PCP

The **metrics** RHEL System Role now provides the ability to connect SQL Server, **mssql** with Performance Co-Pilot, **pcp**. SQL Server is a general purpose relational database from Microsoft. As it runs, SQL Server updates internal statistics about the operations it is performing. These statistics can be accessed using SQL queries but it is important for system and database administrators undertaking performance analysis tasks to be able to record, report, visualize these metrics. With this enhancement, users can use the metrics RHEL System Role to automate connecting SQL server, **mssql**, with Performance Co-Pilot, **pcp**, which provides recording, reporting, and visualization functionality for **mssql** metrics.

(BZ#1893908)

exporting-metric-data-to-elasticsearch functionality available in the Metrics RHEL System Role

Elasticsearch is a popular, powerful and scalable search engine. With this enhancement, by exporting metric values from the Metrics RHEL System Role to the Elasticsearch, users are able to access metrics via Elasticsearch interfaces, including via graphical interfaces, REST APIs, between others. As a result, users are able to use these Elasticsearch interfaces to help diagnose performance problems and assist in other performance related tasks like capacity planning, benchmarking and so on.

(BZ#1895188)

Support for SSHD RHEL System Role

Previously, there was no vendor-supported automation tooling to configure SSH RHEL System Roles in a consistent and stable manner for servers and clients. With this enhancement, you can use the RHEL System Roles to configure **sshd** servers in a systematic and unified way regardless of operating system version.

(BZ#1893696)

Crypto Policies RHEL System Role is now supported

With this enhancement, RHEL 8 introduces a new feature for system-wide cryptographic policy management. By using RHEL System Roles, you now can consistently and easily configure cryptographic policies on any number of RHEL 8 systems.

(BZ#1893699)

The Logging RHEL System Role now supports rsyslog behavior

With this enhancement, **rsyslog** receives the message from Red Hat Virtualization and forwards the message to the **elasticsearch**.

(BZ#1889893)

The networking RHEL System Role now supports the ethtool settings

With this enhancement, you can use the **networking** RHEL System Role to configure **ethtool** coalesce settings of a **NetworkManager** connection. When using the **interrupt coalescing** procedure, the system collects network packets and generates a single interrupt for multiple packets. As a result, this increases the amount of data sent to the kernel with one hardware interrupt, which reduces the interrupt load, and maximizes the throughput.

(BZ#1893961)

4.18. VIRTUALIZATION

IBM Z virtual machines can now run up to 248 CPUs

Previously, the number of CPUs that you could use in an IBM Z (s390x) virtual machine (VM), with **DIAG318** enabled, was limited to 240. Now, using the Extended-Length SCCB, IBM Z VMs can run up to 248 CPUs.

(JIRA:RHELPLAN-44450)

HMAT is now supported on RHEL KVM

With this update, ACPI Heterogeneous Memory Attribute Table (HMAT) is now supported on RHEL KVM. The ACPI HMAT optimizes memory by providing information about memory attributes, such as memory side cache attributes as well as bandwidth and latency details related to the System Physical Address (SPA) Memory Ranges.

(JIRA:RHELPLAN-37817)

Virtual machines can now use features of Intel Atom P5000 Processors

The **Snowridge** CPU model name is now available for virtual machines (VMs). On hosts with Intel Atom P5000 processors, using **Snowridge** as the CPU type in the XML configuration of the VM exposes new features of these processors to the VM.

(JIRA:RHELPLAN-37579)

virtio-gpu devices now work better on virtual machines with Windows 10 and later

This update extends the **virtio-win** drivers to also provide custom drivers for **virtio-gpu** devices on selected Windows platforms. As a result, the **virtio-gpu** devices now have improved performance on virtual machines that use Windows 10 or later as their guest systems. In addition, the devices will also benefit from future enhancements to **virtio-win**.

(BZ#1861229)

Virtualization support for 3rd generation AMD EPYC processors

With this update, virtualization on RHEL 8 adds support for the 3rd generation AMD EPYC processors, also known as EPYC Milan. As a result, virtual machines hosted on RHEL 8 can now use the **EPYC-Milan** CPU model and utilise new features that the processors provide.

(BZ#1790620)

4.19. RHEL IN CLOUD ENVIRONMENTS

Automatic registration for gold images for AWS

With this update, gold images of RHEL 8.4 and later for Amazon Web Services and Microsoft Azure can be configured by the user to automatically register to Red Hat Subscription Management (RHSM) and Red Hat Insights. This makes it faster and easier to configure a large number of virtual machines created from a gold image.

However, if you require consuming repositories provided by RHSM, ensure that the **manage_repos** option in **/etc/rhsm/rhsm.conf** is set to **1**. For more information, please refer to Red Hat KnowledgeBase.

(BZ#1905398, BZ#1932804)

cloud-init is now supported on Power Systems Virtual Server in IBM Cloud

With this update, the **cloud-init** utility can be used to configure RHEL 8 virtual machines hosted on IBM Power Systems hosts and running in the IBM Cloud Virtual Server service.

(BZ#1886430)

4.20. SUPPORTABILITY

sos rebased to version 4.0

The **sos** package has been upgraded to version 4.0. This major version release includes a number of new features and changes.

Major changes include:

- A new **sos** binary has replaced the former sosreport binary as the main entry point for the utility.
- **sos report** is now used to generate sosreport tarballs. The **sosreport** binary is maintained as a redirection point and now invokes **sos report**.
- The **/etc/sos.conf** file has been moved to **/etc/sos/sos.conf**, and its layout has changed as follows:

- The **[general]** section has been renamed to **[global]**, and may be used to specify options that are available to all **sos** commands and sub-commands.
- The **[tunables]** section has been renamed to **[plugin_options]**.
- Each **sos** component, **report**, **collect**, and **clean**, has its own dedicated section. For example, **sos report** loads options from **global** and from **report**.

- **sos** is now a Python3-only utility. Python2 is no longer supported in any capacity.

sos collect

sos collect formally brings the **sos-collector** utility into the main **sos** project, and is used to collect sosreports from multiple nodes simultaneously. The **sos-collector** binary is maintained as a redirection point and invokes **sos collect**. The standalone **sos-collector** project will no longer be independently developed. Enhancements for **sos collect** include:

- **sos collect** is now supported on all distributions that **sos** report supports, that is any distribution with a *Policy* defined.
- The **--insecure-sudo** option has been renamed to **--nopasswd-sudo**.
- The **--threads** option, used to connect simultaneously to the number of nodes, has been renamed to **--jobs**

sos clean

sos clean formally brings the functionality of the **soscleaner** utility into the main **sos** project. This subcommand performs further data obfuscation on reports, such as cleaning IP addresses, domain names, and user-provided keywords.

Note: When the **--clean** option is used with the **sos report** or **sos collect** command, **sos clean** is applied on a report being generated. Thus, it is not necessary to generate a report and only after then apply the cleaner function on it.

Key enhancements for **sos clean** include:

- Support for IPv4 address obfuscation. Note that this will attempt to preserve topological relationships between discovered addresses.
- Support for host name and domain name obfuscation.
- Support for user-provided keyword obfuscations.
- The **--clean** or **--mask** flag used with the **sos report** command obfuscates a report being generated. Alternatively, the following command obfuscates an already existing report:

```
[user@server1 ~]$ sudo sos (clean|mask) $archive
```

Using the former results in a single obfuscated report archive, while the latter results in two; an obfuscated archive and the un-obfuscated original.

For full information on the changes contained in this release, see sos-4.0.

(BZ#1966838)

4.21. CONTAINERS

Podman now supports volume plugins written for Docker

Podman now has support for Docker volume plugins. These volume plugins or drivers, written by vendors and community members, can be used by Podman to create and manage container volumes.

The **podman volume create** command now supports creation of the volume using a volume plugin with the given name. The volume plugins must be defined in the **[engine.volume_plugins]** section of the **container.conf** configuration file.

Example:

```
[engine.volume_plugins]
testvol = "/run/docker/plugins/testvol.sock"
```

where **testvol** is the name of the plugin and **/run/docker/plugins/testvol.sock** is the path to the plugin socket.

You can use the **podman volume create --driver testvol** to create a volume using a **testvol** plugin.

(BZ#1734854)

The ubi-micro container image is now available

The **registry.redhat.io/ubi8/ubi-micro** container image is the smallest base image that uses the package manager on the underlying host to install packages, typically using Buildah or multi-stage builds with Podman. Excluding package managers and all of its dependencies increases the level of security of the image.

(JIRA:RHELPLAN-56664)

Support to auto-update container images is available

With this enhancement, users can use the **podman auto-update** command to auto-update containers according to their auto-update policy. The containers have to be labeled with a specified **"io.containers.autoupdate=image"** label to check if the image has been updated. If it has, Podman pulls the new image and restarts the systemd unit executing the container. The **podman auto-update** command relies on systemd and requires a fully-specified image name to create a container.

(JIRA:RHELPLAN-56661)

Podman now supports secure short names

Short-name aliases for images can now be configured in the **registries.conf** file in the **[aliases]** table. The short-names modes are:

- Enforcing: If no matching alias is found during the image pull, Podman prompts the user to choose one of the unqualified-search registries. If the selected image is pulled successfully, Podman automatically records a new short-name alias in the users **$HOME/.config/containers/short-name-aliases.conf** file. If the user cannot be prompted (for example, stdin or stdout are not a TTY), Podman fails. Note that the **short-name-aliases.conf** file has precedence over **registries.conf** file if both specify the same alias.

- Permissive: Similar to enforcing mode but it does not fail if the user cannot be prompted. Instead, Podman searches in all unqualified-search registries in the given order. Note that no alias is recorded.

Example:

```
unqualified-search-registries=[“registry.fedoraproject.org”, “quay.io”]

[aliases]

"fedora"="registry.fedoraproject.org/fedora"
```

(JIRA:RHELPLAN-39843)

container-tools:3.0 stable stream is now available

The **container-tools:3.0** stable module stream, which contains the Podman, Buildah, Skopeo, and runc tools is now available. This update provides bug fixes and enhancements over the previous version.

For instructions how to upgrade from an earlier stream, see Switching to a later stream .

(JIRA:RHELPLAN-56782)

CHAPTER 5. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel shipped with Red Hat Enterprise Linux 8.4. These changes could include for example added or updated **proc** entries, **sysctl**, and **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

5.1. NEW KERNEL PARAMETERS

bgrt_disable = [ACPI, X86]

This parameter disables Boot Graphics Resource Table (BGRT) to avoid flickering Original Equipment Manufacturer (OEM) logo.

radix_hcall_invalidate = on [PPC/PSERIES]

This parameter disables Radix GTSE feature and use hcall for Translation Lookaside Buffer (TLB) invalidate.

disable_tlbie = [PPC]

This parameter disables Translation Look-Aside Buffer Invalidate Entry (TLBIE) instruction. Currently does not work with KVM, with hash Memory management Unit (MMU), or with coherent accelerators.

fw_devlink = [KNL]

This parameter creates device links between consumer and supplier devices by scanning the firmware to infer the consumer and supplier relationships. This feature is useful when drivers are loaded as modules as it ensures proper ordering of tasks like:

- device probing (suppliers first, then consumers)
- supplier boot state clean up (only after all consumers have probed)
- suspend, resume and runtime Power Management (PM) (consumers first, then suppliers) Format: { off | permissive | on | rpm }
- **off** - Do not create device links from firmware info.
- **permissive** - Create device links from firmware info but use it only for ordering boot state clean up (**sync_state()** calls).
- **on** - Create device links from firmware info and use it to enforce probe and suspend or resume ordering.
- **rpm** - Like **on**, but also used to order runtime PM.

The default value is **permissive**. You can check the configured value in the **/proc/cmdline** file.

init_on_alloc = [MM]

This parameter fills newly allocated pages and heap objects with zeroes.
Format: 0 | 1

Default set by the kernel **CONFIG_INIT_ON_ALLOC_DEFAULT_ON** configuration

init_on_free = [MM]

This parameter fills freed pages and heap objects with zeroes.

Format: 0 | 1

Default set by **CONFIG_INIT_ON_FREE_DEFAULT_ON**

nofsgsbase [X86]

This parameter disables FSGSBASE instructions.

nosgx [X86-64,SGX]

This parameter disables Intel Software Guard Extensions (SGX) kernel support.

rcutree.rcu_min_cached_objs = [KNL]

Minimum number of objects which are cached and maintained per one CPU. Object size is equal to **PAGE_SIZE**. The cache allows to reduce the pressure to page allocator. Also it makes the whole algorithm to behave better in low memory condition.

rcuperf.kfree_rcu_test = [KNL]

This parameter is used to measure performance of the **kfree_rcu()** function flooding.

rcuperf.kfree_nthreads = [KNL]

The number of threads running loops of **kfree_rcu()**.

rcuperf.kfree_alloc_num = [KNL]

Number of allocations and frees done in an iteration.

rcuperf.kfree_loops = [KNL]

Number of loops doing **rcuperf.kfree_alloc_num** number of allocations and frees.

rcupdate.rcu_cpu_stall_ftrace_dump = [KNL]

This parameter dumps **ftrace** buffer after reporting Read-copy-update (RCU) CPU stall warning.

nopvspin = [X86,KVM]

This parameter disables the **qspinlock** slow path using Para-virtualization (PV) optimizations. This allows the hypervisor to 'idle' the guest on lock contention.

5.2. NEW /PROC/SYS/USER PARAMETERS

max_time_namespaces

The maximum number of time namespaces that any user in the current user namespace can create.

5.3. NEW /PROC/SYS/VM PARAMETERS

compaction_proactiveness

This parameter determines how aggressively the kernel should compact memory in the background. The parameter takes a value in the range [0, 100] and the default value is 0. The motivation to disable this parameter by default was to avoid breaking the currently established and expected behavior of the system by a kthread that would be woken up every 500msec to move memory around.
Note that compaction has a non-trivial system-wide impact as pages belonging to different processes are moved around. This could also lead to latency spikes in unsuspecting applications. The kernel employs various heuristics to avoid wasting CPU cycles if it detects that proactive compaction is not being effective.

Be careful when setting this parameter to extreme values such as 100. This can cause excessive background compaction activity.

watermark_boost_factor

This parameter controls the level of reclaim when memory is being fragmented. It defines the percentage of the high watermark of a zone that will be reclaimed if pages of different mobility are being mixed within pageblocks. The intent is that compaction has less work to do in the future and to increase the success rate of future high-order allocations such as SLUB allocations, THP and hugetlbfs pages.
With respect to the **watermark_scale_factor** parameter, the unit is in fractions of 10,000. The default value of 15,000 on **!DISCONTIGMEM** configurations means that up to 150% of the high watermark is reclaimed in the event of a pageblock being mixed due to fragmentation. The level of reclaim is determined by the number of fragmentation events that occurred in the recent past. If this value is smaller than a pageblock then a pageblocks worth of pages are going to be reclaimed (e.g. 2MB on 64-bit x86). A boost factor of 0 will disable the feature.

CHAPTER 6. DEVICE DRIVERS

6.1. NEW DRIVERS

Network drivers

- Realtek 802.11ac wireless 8822b driver (rtw88_8822b.ko.xz)
- Realtek 802.11ac wireless 8822be driver (rtw88_8822be.ko.xz)
- Realtek 802.11ac wireless 8822c driver (rtw88_8822c.ko.xz)
- Realtek 802.11ac wireless 8822ce driver (rtw88_8822ce.ko.xz)
- Realtek 802.11ac wireless core module (rtw88_core.ko.xz)
- Realtek 802.11ac wireless PCI driver (rtw88_pci.ko.xz)
- Interface driver for UDP encapsulated traffic (bareudp.ko.xz)

Graphics drivers and miscellaneous drivers

- Regmap SoundWire Module (regmap-sdw.ko.xz)
- Intel® QuickAssist Technology (qat_4xxx.ko.xz)
- Intel® Data Accelerator Driver (idxd.ko.xz)
- Oracle VM VirtualBox Graphics Card (vboxvideo.ko.xz)
- HID driver for gaming keys on Logitech gaming keyboards (hid-lg-g15.ko.xz)
- Driver for AMD Energy reporting from RAPL MSR via HWMON interface (amd_energy.ko.xz)
- Elastic Fabric Adapter (EFA) (efa.ko.xz)
- AMD® PCI-E Non-Transparent Bridge Driver (ntb_hw_amd.ko.xz)
- PCIe NTB Performance Measurement Tool (ntb_perf.ko.xz)
- PCIe NTB Simple Pingpong Client (ntb_pingpong.ko.xz)
- PCIe NTB Debugging Tool (ntb_tool.ko.xz)
- Software Queue-Pair Transport over NTB (ntb_transport.ko.xz)
- Intel Elkhart Lake PCH pinctrl/GPIO driver (pinctrl-elkhartlake.ko.xz)
- Dell platform setting control interface (dell-wmi-sysman.ko.xz)
- DesignWare PWM Controller (pwm-dwc.ko.xz)
- SoundWire bus (soundwire-bus.ko.xz)
- Cadence Soundwire Library (soundwire-cadence.ko.xz)
- SoundWire Generic Bandwidth Allocation (soundwire-generic-allocation.ko.xz)

- Intel Soundwire Init Library (soundwire-intel.ko.xz)
- Fast-charge control for Apple "MFi" devices (apple-mfi-fastcharge.ko.xz)
- TI HD3SS3220 DRP Port Controller Driver (hd3ss3220.ko.xz)
- STMicroelectronics STUSB160x Type-C controller driver (stusb160x.ko.xz)
- Nitro Enclaves Driver (nitro_enclaves.ko.xz)

6.2. UPDATED DRIVERS

Graphics and miscellaneous driver updates

- Standalone drm driver for the VMware SVGA device (vmwgfx.ko.xz) has been updated to version 2.18.0.0.
- Cisco FCoE HBA Driver (fnic.ko.xz) has been updated to version 1.6.0.53.
- Driver for HP Smart Array Controller version 3.4.20-200-RH1 (hpsa.ko.xz) has been updated to version 3.4.20-200-RH1.
- Emulex LightPulse Fibre Channel SCSI driver 12.8.0.5 (lpfc.ko.xz) has been updated to version 0:12.8.0.5.
- LSI MPT Fusion SAS 3.0 Device Driver (mpt3sas.ko.xz) has been updated to version 35.101.00.00.
- QLogic Fibre Channel HBA Driver (qla2xxx.ko.xz) has been updated to version 10.02.00.104-k.
- SCSI debug adapter driver (scsi_debug.ko.xz) has been updated to version 0190.
- Driver for Microsemi Smart Family Controller version 1.2.16-012 (smartpqi.ko.xz) has been updated to version 1.2.16-012.
- hpe watchdog driver (hpwdt.ko.xz) has been updated to version 2.0.4.

CHAPTER 7. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 8.4 that have a significant impact on users.

7.1. INSTALLER AND IMAGE CREATION

Anaconda now shows a dialog for **ldl** or unformatted DASD disks in text mode

Previously, during an installation in text mode, Anaconda failed to show a dialog for Linux disk layout (**ldl**) or unformatted Direct-Access Storage Device (DASD) disks. As a result, users were unable to utilize those disks for the installation.

With this update, in text mode Anaconda recognizes **ldl** and unformatted DASD disks and shows a dialog where users can format them properly for the future utilization for the installation.

(BZ#1874394)

RHEL installer failed to start when InfiniBand network interfaces were configured using installer boot options

Previously, when you configured InfiniBand network interfaces at an early stage of RHEL installation using installer boot options (for example, downloaded installer image using PXE server), the installer failed to activate the network interfaces.

This issue occured because the RHEL NetworkManager failed to recognize the network interfaces in InfiniBand mode, and instead configured Ethernet connections for the interfaces.

As a result, connection activation failed, and if the connectivity over the InfiniBand interface was required at an early stage, RHEL installer failed to start the installation.

With this release, the installer successfully activates the InfiniBand network interfaces that you configure at an early stage of RHEL installation using installer boot options, and the installation completes successfully.

(BZ#1890009)

The automatic partitioning can be scheduled in Anaconda

Previously, during automatic partitioning on LVM type disks, the installer tried to create a partition for an LVM PV on each selected disk. If these disks already had partitioning layout, the schedule of the automatic partitioning could have failed with the error message.

With this update, the problem has been fixed. Now you can schedule the automatic partitioning in the installer.

(BZ#1642391)

Configuring a wireless network using Anaconda GUI is fixed

Previously, configuring the wireless network while using Anaconda graphical user interface (GUI) caused the installation to crash.

With this update, the problem has been fixed. You can configure the wireless network during the installation while using Anaconda GUI.

(BZ#1847681)

7.2. SOFTWARE MANAGEMENT

New -m and -M parameters are now supported for the %autopatch rpm macro

With this update, the **-m** (min) and **-M** (max) parameters have been added to the **%autopatch** macro to apply only a range of patches with given parameters.

(BZ#1834931)

popt rebased to version 1.18

The **popt** packages have been upgraded to the upstream version 1.18, which provides the following notable changes over the previous version:

- Overall codebase cleanup and modernization.
- Failing to drop privileges on the **alias exec** command has been fixed.
- Various bugs, including resource leaks, have been fixed.

(BZ#1843787)

7.3. SHELLS AND COMMAND-LINE TOOLS

snmpbulkget now provides valid output for a non-existing PID

Previously, the **snmpbulkget** command did not provide valid output for a non-existing PID. Consequently, this command would fail with the output as **no results found**.

With this update,**snmpbulkget** provides valid output for a non-existing PID.

(BZ#1817190)

The CRON command now sends an email as per the trigger conditions.

Previously, when the Relax-and-Recover (**ReaR**) utility was configured incorrectly, the **CRON** command triggered an error message that was sent to the administrator through an email. Consequently, the administrator would receive emails even if the configuration was not performed for **ReaR**.

With this update, the **CRON** command is modified and sends an email as per the trigger conditions.

(BZ#1729499)

Using NetBackup version 8.2 as the backup mechanism in ReaR now works.

Previously, when using NetBackup as a backup method, the Relax-and-Recover (**ReaR**) utility did not start the **vxpbx_exchanged** service in the rescue system. Consequently, restoring the data from the backup in the rescue system with NetBackup 8.2 failed with the following error messages logged on the NetBackup server:

Error bpbrm (pid=...) cannot execute cmd on clientInfo tar (pid=...) done. status: 25: cannot connect on socketError bpbrm (pid=...) client restore EXIT STATUS 25: cannot connect on socket

With this update, **ReaR** adds the **vxpbx_exchanged** service and related required files to the rescue system, and starts the service when the rescue system launches.

(BZ#1898080)

libvpd rebased to version 2.2.8.

Notable changes include:

- Improved performance of **vpdupdate** by making the **sqlite** operations asynchronous.

(BZ#1844429)

ReaR utility now restores system using LUKS2 encrypted partition

Previously, when at least one **LUKS2** encrypted partition was present on the system to backup with Relax-and-Recover (**Rear**) utility, the user was not informed that ReaR does not support **LUKS2** encrypted partition. Consequently, the **ReaR** utility was unable to recreate the original state of the system during the restore phase.

With this update, support of basic **LUKS2** configuration, error checking, and improved output has been added to the **ReaR** utility. The **ReaR** utility now restores systems using basic **LUKS2** encrypted partitions or notifies users in the opposite case.

(BZ#1832394)

Texlive now correctly works with Poppler

Previously, the **Poppler** utility underwent an update for API changes. Consequently, due to these API changes the **Texlive** build did not function. With this update, the **Texlive** build now functions correctly with the new **Poppler** utility.

(BZ#1889802)

7.4. INFRASTRUCTURE SERVICES

RPZ now works with wildcard characters

Previously, the **dns_rpz_find_name** function in the **lib/dns/rpz.c** file did not consider wildcard characters when a record for the same suffix was present. Consequently, some records containing wildcard characters were ignored. With this update, the **dns_rpz_find_name** function has been fixed and it now considers wildcard characters.

(BZ#1876492)

7.5. SECURITY

Improved padding for pkcs11

Previously, the **pkcs11** token label had extra padding for some smart cards. As a consequence, the wrong padding could cause issues matching cards based on the label attribute. With this update, the padding is fixed for all the cards and defined PKCS #11 URIs and matching against them in application should work as expected.

(BZ#1877973)

Fixed sealert connection issue handling

Previously, a crash of the **setroubleshoot** daemon could cause the **sealert** process to stop responding. Consequently, the GUI did not show any analysis and also became unresponsive, the command line tool did not print any output and kept running until killed. This update improves handling of connection issues

between **sealert** and **setroubleshootd**. Now **sealert** reports an error message and exits in case the **setroubleshoot** daemon crashes.

(BZ#1875290)

Optimized audit record analysis by setroubleshoot

Previously, new features introduced in **setroubleshoot-3.3.23-1** had a negative impact on performance, which led to the AVC analysis being up to 8 times slower than before. This update provides optimizations that significantly reduce the AVC analysis times.

(BZ#1794807)

Fixed SELinux policy interface parser

Previously, the policy interface parser caused syntax error messages to appear when installing a custom policy that contained an **ifndef** block in its interface file. This update improves the interface file parsing, and thus resolves this issue.

(BZ#1868717)

setfiles does not stop on labeling error

Previously, the **setfiles** utility stopped whenever it failed to relabel a file. Consequently, mislabeled files were left in the target directory. With this update, **setfiles** skips files it cannot relabel, and as a result, **setfiles** processes all files in the target directory.

(BZ#1926386)

Rebuilds of the SELinux policy store are now more resistant to power failures

Previously, SELinux-policy rebuilds were not resistant to power failures due to write caching. Consequently, the SELinux policy store may become corrupted after a power failure during a policy rebuild. With this update, the **libsemanage** library writes all pending modifications to metadata and cached file data to the file system that contains the policy store before using it. As a result, the policy store is now more resistant to power failures and other interruptions.

(BZ#1913224)

libselinux now determines the default context of SELinux users correctly

Previously, the **libselinux** library failed to determine the default context of SELinux users on some systems, due to the use of the deprecated **security_compute_user()** function. As a consequence, some system services were unavailable on systems with complex security policies. With this update, **libselinux** no longer uses **security_compute_user()** and determines the SELinux user's default context properly, regardless of policy complexity.

(BZ#1879368)

Geo-replication in rsync mode no longer fails due to SELinux

Previously, SELinux policy did not allow processes running under **rsync_t** to set the value of the **security.trusted** extended attribute. As a consequence, geo-replication in Red Hat Gluster Storage (RHGS) failed. This update includes the new SELinux boolean **rsync_sys_admin** that allows the **rsync_t** processes to set **security.trusted**. As a result, if the **rsync_sys_admin** boolean is enabled, **rsync** can set the **security.trusted** extended attribute and geo-replication no longer fails.

(BZ#1889673)

OpenSCAP can now scan systems with large numbers of files without running out of memory

Previously, when scanning systems with low RAM and large numbers of files, the OpenSCAP scanner sometimes caused the system to run out of memory. With this update, OpenSCAP scanner memory management has been improved. As a result, the scanner no longer runs out of memory on systems with low RAM when scanning large numbers of files, for example package groups **Server with GUI** and **Workstation**.

(BZ#1824152)

CIS-remediated systems with FAT no longer fail on boot

Previously, the Center for Internet Security (CIS) profile in the SCAP Security Guide (SSG) contained a rule which disabled loading of the kernel module responsible for access to FAT file systems. As a consequence, if SSG remediated this rule, the system could not access partitions formatted with FAT12, FAT16, and FAT32 file systems, including EFI System Partitions (ESP). This caused the systems to fail to boot. With this update, the rule has been removed from the profile. As a result, systems that use these file systems no longer fail to boot.

(BZ#1927019)

OVAL checks consider GPFS as remote

Previously, the OpenSCAP scanner did not identify mounted General Parallel File Systems (GPFS) as remote file systems (FS). As a consequence, OpenSCAP scanned GPFS even for OVAL checks that applied only to local systems. This sometimes caused the scanner to run out of resources and fail to complete the scan. With this update, GPFS has been included in the list of remote FS. As a result, OVAL checks correctly consider GPFS as a remote FS, and the scans are faster.

(BZ#1840579)

The fapolicyd-selinux SELinux policy now covers all file types

Previously, the **fapolicyd-selinux** SELinux policy did not cover all file types. Consequently, the **fapolicyd** service could not access files located on non-monitored locations such as **sysfs**. With this update, the **fapolicyd** service covers and analyzes all file system types.

(BZ#1940289)

fapolicyd no longer prevents RHEL updates

When an update replaces the binary of a running application, the kernel modifies the application binary path in memory by appending the **(deleted)** suffix. Previously, the **fapolicyd** file access policy daemon treated such applications as untrusted. As a consequence, **fapolicyd** prevented these applications from opening and executing any other files. With this update, **fapolicyd** ignores the suffix in the binary path so the binary can match the trust database. As a result, **fapolicyd** enforces the rules correctly and the update process can finish.

(BZ#1896875)

USBGuard rebased to 1.0.0-1

The **usbguard** packages have been rebased to the upstream version 1.0.0-1. This update provides improvements and bug fixes, most notably:

- Stable public API ensures backwards compatibility.
- Rule files inside the **rules.d** directory now load in alphanumeric order.

- Some use cases when the policy of multiple devices could not be changed by a single rule have been fixed.
- Filtering rules by their labels no longer produces errors.

(BZ#1887448)

USBGuard now can send Audit messages

As part of service hardening, the capabilities of **usbguard.service** were limited while the **CAP_AUDIT_WRITE** capability was missing. As a consequence, **usbguard** running as a system service could not send Audit events. With this update, the service configuration has been updated, and as a result, USBGuard can send Audit messages.

(BZ#1940060)

tangd now handles invalid requests correctly

Previously, the **tangd** daemon returned an error exit code for some invalid requests. As a consequence, **tangd.socket@.service** failed, which in turn might have caused problems if the number of such failed units increased. With this update, **tangd** exits with an error code only when the **tangd** server itself is facing problems. As a result, **tangd** handles invalid requests correctly.

(BZ#1828558)

7.6. NETWORKING

Migrating an iptables rule set from RHEL 7 to RHEL 8 with rules involving ipset lookups no longer fails

Previously, the **ipset** counters were updated only if all the additional constraints match while referring to an **ipset** command with enabled counters from an **iptables** rule set. Consequently, the rules involving **ipset** lookups, e.g. **-m set --match-set xxx src --bytes-gt 100** will never get chance to match, because the member's counter of **ipset** will not be added up. With this update, migrating an **iptables** rule set with rules involving **ipset** lookups works as expected.

(BZ#1806882)

The iptraf-ng no longer exposes raw memory content

Previously, when setting **%p** in a filter in **iptraf-ng**, the application displayed raw memory content in the status bar. Consequently, inessential information was getting displayed. With this update, the **iptraf-ng** processes do not show any raw memory content on the status bar at the bottom.

(BZ#1842690)

Network access is now available when using DHCP in the Anaconda ip boot option

The initial RAM disk (**initrd**) uses NetworkManager to manage networking. Previously, the **dracut** NetworkManager module provided by the RHEL 8.3 ISO file incorrectly assumed that the first field of the **ip** option in the Anaconda boot options was always set. As a consequence, if you used DHCP and set **ip=::::<host_name>::dhcp**, NetworkManager did not retrieve an IP address, and the network was not available in Anaconda. This problem has been fixed. As a result, the Anaconda **ip** boot option works as expected when you use the RHEL 8.4 ISO to install a host in the mentioned scenario.

(BZ#1900260)

Unloading XDP programs no longer fails on Netronome network cards that use the nfp driver

Previously, the **nfp** driver for Netronome network cards contained a bug. As a consequence, unloading eXpress Data Path (XDP) programs failed if you used such a card and loaded the XDP program using the **IFLA_XDP_EXPECTED_FD** feature with the **XDP_FLAGS_REPLACE** flag. For example, this affected XDP programs that were loaded using the **libxdp** library. This bug has been fixed. As a result, unloading an XDP program from Netronome network cards works as expected.

(BZ#1880268)

NetworkManager now tries to retrieve the host name using DHCP and reverse DNS lookups on all interfaces

Previously, if the host name was not set in the **/etc/hostname** file, NetworkManager tried to obtain the host name using DHCP or a reverse DNS lookup only through the interface with the default route with the lowest metric value. As a consequence, it was not possible to automatically assign a host name on networks without a default route. This update changes the behavior, and NetworkManager now first tries to retrieve the host name using the default route interface. If this process fails, NetworkManager tries other available interfaces. As a result, NetworkManager tries to retrieve the host name using DHCP and reverse DNS lookups on all interfaces if it is not set in **/etc/hostname**.

To configure that NetworkManager uses the old behavior:

1. Create the **/etc/NetworkManager/conf.d/10-hostname.conf** file with the following content:

```
[connection-hostname-only-from-default]
hostname.only-from-default=1
```

2. Reload the **NetworkManager** service:

```
# systemctl reload NetworkManager
```

(BZ#1766944)

7.7. KERNEL

The kernel no longer returns false positive warnings on IBM Z systems

Previously, IBM Z systems on RHEL 8 were missing an allowed entry for the **ZONE_DMA** memory zone to allow user access. Consequently, the kernel returned false positive warnings such as:

```
...
Bad or missing usercopy whitelist? Kernel memory exposure attempt detected from SLUB object
'dma-kmalloc-192' (offset 0, size 144)!
WARNING: CPU: 0 PID: 8519 at mm/usercopy.c:83 usercopy_warn+0xac/0xd8
...
```

The warnings appeared when accessing certain system information through the **sysfs** interface. For example, by running the **debuginfo.sh** script.

This update adds a flag in the Direct Memory Access (DMA) buffer, so that user space applications can access the buffer.

As a result, no warning messages are displayed in the described scenario.

(BZ#1660290)

RHEL systems boot as expected from the tboot GRUB entry

Previously, the **tboot** utility of version 1.9.12-2 caused some RHEL systems with Trusted Platform Module (TPM) 2.0 enabled to fail to boot in legacy mode. As a consequence, the system halted when it attempted to boot from the **tboot** Grand Unified Bootloader (GRUB) entry. With a new version of RHEL 8 and the update of the **tboot** utility, the problem has been fixed and RHEL systems boot as expected.

(BZ#1947839)

The kernel successfully reclaims memory in heavy-workload container scenarios

When a volume was constrained for I/O and memory within a container, the kernel code responsible for reclaiming memory experienced soft-lockup due to a data race condition. Data race is a phenomenon that happens if:

- At least two CPU threads try to modify the same set of data simultaneously.
- At least one of these CPU threads tries to do a write operation on the dataset.

Based on the exact timing of each thread to modify the dataset, the result can be A, B, or AB (indeterminate).

When a container was under memory pressure, the situation likely led to multiple Out of Memory (OOM) kills, causing the container locking up and becoming unresponsive. In this release, the RHEL kernel code for locking and optimization has been updated. As a result, the kernel no longer becomes unresponsive, and the data does not become subject to race conditions.

(BZ#1860031)

RHEL 8 with offline memory no longer causes kernel panics

Previously, when running RHEL 8 with memory that was initiated but marked as offline, the kernel in some cases attempted to access uninitialized memory pages. As a consequence, a kernel panic occurred. This update fixes the kernel mechanism for idle page tracking, which prevents the problem from occurring.

(BZ#1867490)

The NUMA systems no longer experience unexpected memory layout

Previously, **ARM64** and **S390** architectures experienced unexpected memory layouts on NUMA systems due to missing of the **CONFIG_NODES_SPAN_OTHER_NODES** option. As a consequence, the memory regions from different NUMA nodes intersected and the intersecting memory regions from low NUMA nodes were added into the high NUMA.

With this update, the NUMA systems no longer experience the memory layouts issue.

(BZ#1844157)

The rngd service no longer busy-waits on poll() system call

A new kernel entropy source for FIPS mode was added for kernels, starting with version 4.18.0-193.10. Consequently, the **rngd** service busy-waited on the **poll()** system call for the **/dev/random** device. This situation caused consumption of 100% of CPU time, when a system was in a FIPS mode. With this update, in FIPS mode, a **poll()** handler for the **/dev/random** device has been changed from a default one to a handler developed especially for the **/dev/random** device. As a result, the **rngd** service no longer busy-waits on **poll()** in the described scenario.

(BZ#1884857)

HRTICK support for SCHED_DEADLINE scheduler is enabled

Previously, the feature for high resolution system timers (**HRTICK**) was not armed for certain tasks configured with the **SCHED_DEADLINE** policy. Consequently, the throttling mechanism for these tasks using the **SCHED_DEADLINE** scheduler, consumed all the runtime configured for those tasks. This behavior caused an unexpected latency spike in the real-time environment.

This update enables the **HRTICK** feature, which provides high resolution preemption. **HRTICK** uses a high resolution timer, which enforces the throttling mechanism when a task completes its runtime. As a result, this problem no longer occurs in the described scenario.

(BZ#1885850)

tpm2-abrmd rebased to version 2.3.3.2

The **tpm2-abrmd** package has been upgraded to version 2.3.3.2, which provides multiple bug fixes. Notable changes include:

- Fixed the usage of transient handles
- Fixed partial reads in TPM Command Transmission Interface (TCTI)
- Refactored the access broker

(BZ#1855177)

The cxgb4 driver no longer causes crash in the kdump kernel

Previously, the **kdump** kernel would crash while trying to save information in the **vmcore** file. Consequently, the **cxgb4** driver prevented the **kdump** kernel from saving a core for later analysis. To work around this problem, add the **novmcoredd** parameter to the **kdump** kernel command line to allow saving core files.

With the release of the RHSA-2020:1769 advisory, the **kdump** kernel handles this situation properly and no longer crashes.

(BZ#1708456)

7.8. FILE SYSTEMS AND STORAGE

Accessing SMB targets no longer fail with EREMOTE error

Previously, mounting a DFS namespace on a RHEL SMB client with the **cifsacl** mount option was inaccessible and a listing failed with an **EREMOTE** error. This update fixes the kernel to account for **EREMOTE**, and thus makes the SMB share accessible.

(BZ#1871246)

Performance improvements for NFS readdir function

Previously, a process on a NFS client listing a directory could take a long time to complete the listing, with possibility to never complete. With this update, the NFS client directory listing performance is improved in the following scenarios:

- Listing of large directories with 100,000 or more files.

- Listing of directories that are being modified.

(BZ#1893882)

7.9. HIGH AVAILABILITY AND CLUSTERS

Default token timeout value in corosync.conf file increased from 1 second to 3 seconds

Previously, the TOTEM token timeout value in the **corosync.conf** file was set to 1 second. This short timeout makes the cluster react quickly but in the case of network delays it may result in premature failover. The default value is now set to 3 seconds to provide a better trade-off between quick response and broader applicability. For information on modifying the token timeout value, see How to change totem token timeout value in a RHEL 5, 6, 7, or 8 High Availability cluster?

(BZ#1870449)

7.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

An in-place upgrade is now possible when perl-Time-HiRes is installed

Previously, the **perl-Time-HiRes** package distributed in RHEL 8 was missing an epoch number that was included in the RHEL 7 version of the package. As a consequence, it was impossible to perform an in-place upgrade from RHEL 7 to RHEL 8 when **perl-Time-HiRes** was installed. The missing epoch number has been added, and the in-place upgrade no longer fails when **perl-Time-HiRes** is installed.

(BZ#1895852)

7.11. COMPILERS AND DEVELOPMENT TOOLS

The glibc DNS stub resolver correctly processes parallel queries with identical transaction IDs

Prior to this update, the DNS stub resolver in the GNU C library **glibc** did not process responses to parallel queries with identical transaction IDs correctly. Consequently, when the transaction IDs were equal, the second parallel response was never matched to a query, resulting in a timeout and retry.

With this update, the second parallel response is now recognized as valid. As a result, the **glibc** DNS stub resolver avoids excessive timeouts due to unrecognized responses.

(BZ#1868106)

Reading configuration files with fgetsgent() and fgetsgent_r() is now more robust

Specifically structured entries in the **/etc/gshadow** file, or changes in file sizes while reading, sometimes caused the **fgetsgent()** and **fgetsgent_r()** functions to return invalid pointers. Consequently, applications that used these functions to read **/etc/gshadow**, or other configuration files in **/etc/**, failed with a segmentation fault error. This update modifies **fgetsgent()** and **fgetsgent_r()** to make reading of configuration files more robust. As a result, applications are now able to read configuration files successfully.

(BZ#1871397)

The glibc string functions now avoid negative impact on system cache on AMD64 and Intel 64 processors

Previously, the **glibc** implementation of string functions incorrectly estimated the amount of last-level cache available to a thread on the 64-bit AMD and Intel processors. As a consequence, calling the **memcpy** function on large buffers either negatively impacted the overall cache performance of the system or slowed down the **memcpy** system call.

With this update, the last-level cache size is no longer scaled with the number of reported hardware threads in the system. As a result, the string functions now bypass caches for large buffers, avoiding negative impact on the rest of the system cache.

(BZ#1880670)

The glibc dynamic loader now avoids certain failures of libc.so.6

Previously, when the **libc.so.6** shared object ran as a main program (for example, to display the **glibc** version information), the **glibc** dynamic loader did not order relocation of **libc.so.6** correctly in relation to the objects loaded using the **LD_PRELOAD** environment variable. Consequently, when **LD_PRELOAD** was set, invoking **libc.so.6** sometimes caused **libc.so.6** to terminate unexpectedly with a segmentation fault. This update fixes the bug, and the dynamic loader now correctly handles the relocation of **libc.so.6**. As a result, the described problem no longer occurs.

(BZ#1882466)

The glibc dynamic linker now restricts part of the static thread-local storage space to static TLS allocations

Previously, the **glibc** dynamic linker used all available static thread-local storage (TLS) space for dynamic TLS, on a first come, first served basis. Consequently, loading additional shared objects at run time using the **dlopen** function sometimes failed, because dynamic TLS allocations had already consumed all available static TLS space. This problem occurred particularly on the 64-bit ARM architecture and IBM Power Systems.

Now, the dynamic linker restricts part of the static TLS area to static TLS allocations and does not use this space for dynamic TLS optimizations. As a result, **dlopen** calls succeed in more cases with the default setting. Applications that require more allocated static TLS than the default setting allows can use a new **glibc.rtld.optional_static_tls** tunable.

(BZ#1871396)

The glibc dynamic linker now disables lazy binding for the 64-bit ARM variant calling convention

Previously, the **glibc** dynamic linker did not disable lazy binding for functions using the 64-bit ARM (AArch64) variant calling convention. As a consequence, the dynamic linker corrupted arguments in such function calls, leading to incorrect results or process failures. With this update, the dynamic linker now disables lazy binding in the described scenario, and the function arguments are passed correctly.

(BZ#1893662)

gcc rebased to version 8.4

The GNU Compiler Collection (GCC) has been rebased to upstream version 8.4, which provides a number of bug fixes over the previous version.

(BZ#1868446)

7.12. IDENTITY MANAGEMENT

The Samba wide links feature has been converted to a VFS module

Previously, the **wide links** parameter was part of the **smbd** service's core functionality. Enabling this feature is insecure and, therefore, has been moved into a separate virtual file system (VFS) module named **widelinks**. For backward compatibility, Samba in RHEL 8.4 automatically loads this module for shares that have **wide links = yes** set in their configuration.

Important: Red Hat recommends not to use the insecure **wide links** feature. Instead, use a **bind mount** to mount a part of the file hierarchy to a directory that you shared in Samba. For details about configuring a bind mount, see the **Bind mount operation** section in the **mount(8)** man page.

To switch from a configuration that uses **wide links** to **bind mount**:

1. For every symbolic link that links outside of a share, replace the link with a **bind mount**. For details, see the **Bind mount operation** section in the **mount(8)** man page.
2. Remove all **wide links = yes** entries from the **/etc/samba/smb.conf** file.
3. Reload Samba:

```
# smbcontrol all reload-config
```

(BZ#1925192)

Network connection idle timeouts are no longer reported as resource errors

Previously, Directory Server reported a misleading error that a resource was temporarily unavailable when an idle network connection timed out. With this update, the error macro for network connection idle timeouts has been changed from **EAGAIN** to **ETIMEDOUT**, and an accurate error message describing a timeout is written to the Directory Server access logs.

(BZ#1859301)

Certificates issued by PKI ACME Responder connected to PKI CA no longer fail OCSP validation

Previously, the default ACME certificate profile provided by PKI CA contained a sample OCSP URL that did not point to an actual OCSP service. As a consequence, if PKI ACME Responder was configured to use a PKI CA issuer, the certificates issued by the responder could fail OCSP validation. This update removes hard-coded URLs in the ACME certificate profile and adds an upgrade script to fix the profile configuration file in case you did not customize it.

(BZ#1868233)

7.13. GRAPHICS INFRASTRUCTURES

Display backlight now works reliably on recent Intel laptops

Certain recent laptops with Intel CPUs require a proprietary interface to control display backlight. Previously, RHEL did not support the proprietary interface, and attempted to use the VESA interface, which was unreliable on the laptops. As a consequence, RHEL could not control display backlight on those laptops.

With this update, RHEL adds support for the proprietary backlight interface, and as a result, display control now works as expected.

(BZ#1885406)

7.14. RED HAT ENTERPRISE LINUX SYSTEM ROLES

tests_luks.yml no longer cause partition case fail with NVME disk

Previously, NVME disks used a different partition naming convention than the one used by **virtio/scsi** and the Storage role did not reflect it. As a consequence, running the Storage role with NVME disks resulted in a crash. With this fix, the Storage RHEL System Role now obtains the partition name from the **blivet** module.

(BZ#1865990)

The selinux RHEL System Role no longer uses variable named present

Previously, some tasks in the **selinux** RHEL System Role were incorrectly using a variable named **present** instead of using the string **present**. As a consequence, the **selinux** RHEL System Role returned an error informing that there is no variable named **present**. This update fixes this issue, changing those tasks to use the string **present**. As a result, the **selinux** RHEL System Role works as expected, with no error message.

(BZ#1926947)

Logging output no longer fails when the rsyslog-gnutls package is missing

A global **tls rsyslog-gnutls** package is required when the **logging** RHEL System Role is configured to provide secure remote input and secure forward output. Previously, thel **tls rsyslog-gnutls** package was changed to install unconditionally in the previous version. As a consequence, when the **tls rsyslog-gnutls** package was not available on the managed nodes, the **logging** role configuration failed, even if the secure remote input and secure forward output were not included as part of the configuration. This update fixes the issue by examining if the secure connection is configured and checking the global **tls logging_pki_files** variable. The **rsyslog-gnutls** package is installed only when the secure connection is configured. As a result, the operation to configure Red Hat Enterprise Virtualization Hypervisor to integrate **elasticsearch** as the logging output no longer fails with the missing **rsyslog-gnutls** package.

(BZ#1927943)

7.15. VIRTUALIZATION

Connecting to the RHEL 8 guest console on a Windows Server 2019 host is no longer slowed down

Previously, when using RHEL 8 as a guest operating system in multi-user mode on a Windows Server 2019 host, connecting to a console output of the guest currently took significantly longer than expected. This update improves the performance of VRAM on the Hyper-V hypervisor, which fixes the problem.

(BZ#1908893)

Displaying multiple monitors of virtual machines that use Wayland is now possible with QXL

Previously, using the **remote-viewer** utility to display more than one monitor of a virtual machine (VM) that was using the Wayland display server caused the VM to become unresponsive and the *Waiting for display* status message to be displayed indefinitely. The underlying code has been fixed, which prevents the described problem from occurring.

(BZ#1642887)

7.16. RHEL IN CLOUD ENVIRONMENTS

GPU-optimized Azure instances now work correctly after hibernation

When running RHEL 8 as a guest operating system on a Microsoft Azure instance with GPU-optmized virtual machine (VM) size, such as NV6, resuming the VM from hibernation previously caused the VM's GPU to work incorrectly. When this occurred, the kernel logged the following message:

```
hv_irq_unmask() failed: 0x5
```

With this update, the impacted VMs on Microsoft Azure handle their GPUs correctly after resuming, which prevents the problem from occurring.

(BZ#1846838)

The TX/RX packet counters increase as intended after virtual machines resume from hibernation

Previously, the **TX**/**RX** packet counters stopped increasing when a RHEL 8 virtual machine using a CX4 VF NIC resumed from hibernation on Microsoft Azure. This update resolves the issue, and the packet counters increase as intended.

(BZ#1876527)

RHEL 8 virtual machines no longer fail to resume from hibernation on Azure

Previously, the GUID of the virtual function (VF), **vmbus device**, changed when a RHEL 8 virtual machine (VM), with **SR-IOV** enabled, was hibernated and deallocated on Microsoft Azure. Consequently, when the VM was restarted, it failed to resume and terminated unexpectedly. With this update, the **vmbus device** VF no longer changes, and the VM resumes from hibernation successfully.

(BZ#1876519)

Removed a redundant error message in Hyper-V and KVM guests

Previously, when a RHEL 8 guest operating system was running in a KVM or Hyper-V virtual machine, the following error message was reported in the **/var/log/messages** file:

```
serial8250: too much work for irq4
```

This was a redundant error message and has now been removed.

For more information on the problem, see the Red Hat Knowledgebase solution .

(BZ#1919745)

7.17. CONTAINERS

podman system connection add automatically set the default connection

Previously, the **podman system connection add** command did not automatically set the first connection to be the default connection. As a consequence, you must manually run the **podman system connection default <connection_name>** command to set the default connection. With this update, the **podman system connection add** command works as expected.

(BZ#1881894)

The podman run --pid=host works in a rootless mode

Previously, running the **podman run --pid=host** command as a rootless user did not work. Consequently, an OCI permission error occurred:

```
$ podman run --rm --pid=host quay.io/libpod/testimage:20200929 cat -v /proc/self/attr/current

Error: container_linux.go:370: starting container process caused: process_linux.go:459: container init caused: readonly path /proc/bus: operation not permitted: OCI permission denied
```

With this update, the problem has been fixed.

(BZ#1940854)

CHAPTER 8. TECHNOLOGY PREVIEWS

This part provides a list of all Technology Previews available in Red Hat Enterprise Linux 8.4.

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

8.1. INSTALLER AND IMAGE CREATION

Red Hat Connector available as a Technology Preview

You can now connect to a RHEL system with a single command to consume Red Hat Insights and your subscription content. Available as a Technology Preview in Red Hat Enterprise Linux 8.4, the Red Hat connector (**rhc**) CLI unifies the registration experience and eliminates the need to separately run the **subscription-manager** and **insights-client** commands to connect to Red Hat. With Red Hat connector and a Smart Management subscription, you can also remediate issues directly from the cloud.

For more information, see the Red Hat Connector Configuration Guide .

(BZ#1957316)

8.2. NETWORKING

Introducing bareudp device support for encapsulating MPLS traffic over UDP tunnel as a Technology Preview

The support for **bareudp** devices is now available with the **ip link** command as a Technology Preview. The **bareudp** devices provide L3 encapsulation tunnelling support for routing traffic with different L3 protocols, such as unicast and multicast multi protocol label switching (MPLS) and IPv4/IPv6 inside the UDP tunnel. You can start routing MPLS packets in UDP with the help of adding **tc** filters and actions.

For example, to create a new **bareudp** device, use the following command:

```
# ip link add dev bareudp0 type bareudp dstport 6635 ethertype mpls_uc
```

To route MPLS incoming packets in UDP tunnel using the bareudp0 device, use the following command:

```
# tc qdisc add dev enp1s0 ingress
# tc filter add dev enp1s0 ingress proto mpls_uc matchall   \
> action tunnel_key set src_ip 2001:db8::22 dst_ip 2001:db8::21 id 0   \
> action mirred egress redirect dev bareudp0
```

For more information about options and parameters used while creating **bareudp** devices, refer to the **Bareudp Type Support** section in the **ip-link(8)** man page.

(BZ#1849815)

AF_XDP available as a Technology Preview

Address Family eXpress Data Path (**AF_XDP**) socket is designed for high-performance packet processing. It accompanies **XDP** and grants efficient redirection of programmatically selected packets to user space applications for further processing.

(BZ#1633143)

KTLS available as a Technology Preview

In Red Hat Enterprise Linux 8, Kernel Transport Layer Security (KTLS) is provided as a Technology Preview. KTLS handles TLS records using the symmetric encryption or decryption algorithms in the kernel for the AES-GCM cipher. KTLS also provides the interface for offloading TLS record encryption to Network Interface Controllers (NICs) that support this functionality.

(BZ#1570255)

XDP features that are available as Technology Preview

Red Hat provides the usage of the following eXpress Data Path (XDP) features as unsupported Technology Preview:

- Loading XDP programs on architectures other than AMD and Intel 64-bit. Note that the **libxdp** library is not available for architectures other than AMD and Intel 64-bit.
- The XDP hardware offloading.

(BZ#1889737)

Multi-protocol Label Switching for TC available as a Technology Preview

The Multi-protocol Label Switching (MPLS) is an in-kernel data-forwarding mechanism to route traffic flow across enterprise networks. In an MPLS network, the router that receives packets decides the further route of the packets based on the labels attached to the packet. With the usage of labels, the MPLS network has the ability to handle packets with particular characteristics. For example, you can add **tc filters** for managing packets received from specific ports or carrying specific types of traffic, in a consistent way.

After packets enter the enterprise network, MPLS routers perform multiple operations on the packets, such as **push** to add a label, **swap** to update a label, and **pop** to remove a label. MPLS allows defining actions locally based on one or multiple labels in RHEL. You can configure routers and set traffic control (**tc**) filters to take appropriate actions on the packets based on the MPLS label stack entry (**lse**) elements, such as **label**, **traffic class**, **bottom of stack**, and **time to live**.

For example, the following command adds a filter to the *enp0s1* network interface to match incoming packets having the first label *12323* and the second label *45832*. On matching packets, the following actions are taken:

- the first MPLS TTL is decremented (packet is dropped if TTL reaches 0)
- the first MPLS label is changed to *549386*
- the resulting packet is transmitted over *enp0s2*, with destination MAC address *00:00:5E:00:53:01* and source MAC address *00:00:5E:00:53:02*

```
# tc filter add dev enp0s1 ingress protocol mpls_uc flower mpls lse depth 1 label 12323 lse
depth 2 label 45832 \
action mpls dec_ttl pipe \
action mpls modify label 549386 pipe \
action pedit ex munge eth dst set 00:00:5E:00:53:01 pipe \
action pedit ex munge eth src set 00:00:5E:00:53:02 pipe \
action mirred egress redirect dev enp0s2
```

(BZ#1814836, BZ#1856415)

act_mpls module available as a Technology Preview

The **act_mpls** module is now available in the **kernel-modules-extra** rpm as a Technology Preview. The module allows the application of Multiprotocol Label Switching (MPLS) actions with Traffic Control (TC) filters, for example, push and pop MPLS label stack entries with TC filters. The module also allows the Label, Traffic Class, Bottom of Stack, and Time to Live fields to be set independently.

(BZ#1839311)

Improved Multipath TCP support is available as a Technology Preview

Multipath TCP (MPTCP) improves resource usage within the network and resilience to network failure. For example, with Multipath TCP on the RHEL server, smartphones with MPTCP v1 enabled can connect to an application running on the server and switch between Wi-Fi and cellular networks without interrupting the connection to the server.

RHEL 8.4 offers additional features, such as:

- Multiple concurrent active substreams
- Active-backup support
- Improved stream performances
- Better memory usage, with **receive** and **send** buffer auto-tuning
- SYN cookie support

Note that either the applications running on the server must natively support MPTCP or administrators must load an **eBPF** program into the kernel to dynamically change **IPPROTO_TCP** to **IPPROTO_MPTCP**.

For further details see, Getting started with Multipath TCP.

(JIRA:RHELPLAN-57712)

The systemd-resolved service is now available as a Technology Preview

The **systemd-resolved** service provides name resolution to local applications. The service implements a caching and validating DNS stub resolver, an Link-Local Multicast Name Resolution (LLMNR), and Multicast DNS resolver and responder.

Note that, even if the **systemd** package provides **systemd-resolved**, this service is an unsupported Technology Preview.

(BZ#1906489)

The nispor package is now available as a Technology Preview

The **nispor** package is now available as a Technology Preview, which is a unified interface for Linux network state querying. It provides a unified way to query all running network status through the python and C api, and rust crate. **nispor** works as the dependency in the **nmstate** tool.

You can install the **nispor** package as a dependency of **nmstate** or as an individual package.

- To install **nispor** as an individual package, enter:

```
# yum install nispor
```

- To install **nispor** as a dependency of **nmstate**, enter:

```
# yum install nmstate
```

nispor is listed as the dependency.

For more information on using **nispor**, refer to **/usr/share/doc/nispor/README.md** file.

(BZ#1848817)

8.3. KERNEL

The kexec fast reboot feature is available as Technology Preview

The **kexec fast reboot** feature continues to be available as a Technology Preview. **kexec fast reboot** significantly speeds the boot process by allowing the kernel to boot directly into the second kernel without passing through the Basic Input/Output System (BIOS) first. To use this feature:

1. Load the **kexec** kernel manually.
2. Reboot the operating system.

(BZ#1769727)

The accel-config package available as a Technology Preview

The **accel-config** package is now available on Intel **EM64T** and **AMD64** architectures for RHEL 8.4 as a Technology Preview. This package helps in controlling and configuring data-streaming accelerator (DSA) sub-system in the Linux Kernel. Also, it configures devices via **sysfs** (pseudo-filesystem), saves and loads the configuration in the **json** format.

(BZ#1843266)

SGX available as a Technology Preview

Software Guard Extensions(SGX) is an Intel® technology for protecting software code and data from disclosure and modification. This release initiates the kernel support for SGX v1 and v1.5. The version 1 enables platforms using the **Flexible Launch Control** mechanism to use the SGX technology.

(BZ#1660337)

eBPF available as a Technology Preview

Extended Berkeley Packet Filter (eBPF)is an in-kernel virtual machine that allows code execution in the kernel space, in the restricted sandbox environment with access to a limited set of functions.

The virtual machine includes a new system call **bpf()**, which supports creating various types of maps, and also allows to load programs in a special assembly-like code. The code is then loaded to the kernel and translated to the native machine code with just-in-time compilation. Note that the **bpf()** syscall can be successfully used only by a user with the **CAP_SYS_ADMIN** capability, such as the root user. See the **bpf(2)** manual page for more information.

The loaded programs can be attached onto a variety of points (sockets, tracepoints, packet reception) to receive and process data.

There are numerous components shipped by Red Hat that utilize the **eBPF** virtual machine. Each component is in a different development phase, and thus not all components are currently fully supported. All components are available as a Technology Preview, unless a specific component is indicated as supported.

The following notable **eBPF** components are currently available as a Technology Preview:

- **bpftrace**, a high-level tracing language that utilizes the **eBPF** virtual machine.
- **AF_XDP**, a socket for connecting the **eXpress Data Path (XDP)** path to user space for applications that prioritize packet processing performance.

(BZ#1559616)

The data streaming accelerator driver for kernel is available as a Technology Preview

The data streaming accelerator (DSA) driver for the kernel is currently available as a Technology Preview. DSA is an Intel CPU integrated accelerator and supports a shared work queue with process address space ID (pasid) submission and shared virtual memory (SVM).

(BZ#1837187)

Soft-RoCE available as a Technology Preview

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) is a network protocol which implements RDMA over Ethernet. Soft-RoCE is the software implementation of RoCE which supports two protocol versions, RoCE v1 and RoCE v2. The Soft-RoCE driver, **rdma_rxe**, is available as an unsupported Technology Preview in RHEL 8.

(BZ#1605216)

8.4. FILE SYSTEMS AND STORAGE

NVMe/TCP is available as a Technology Preview

Accessing and sharing Nonvolatile Memory Express (NVMe) storage over TCP/IP networks (NVMe/TCP) and its corresponding **nvme-tcp.ko** and **nvmet-tcp.ko** kernel modules have been added as a Technology Preview.

The use of NVMe/TCP as either a storage client or a target is manageable with tools provided by the **nvme-cli** and **nvmetcli** packages.

The NVMe/TCP target Technology Preview is included only for testing purposes and is not currently planned for full support.

(BZ#1696451)

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

In Red Hat Enterprise Linux 8, file system DAX is available as a Technology Preview. DAX provides 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#1627455)

OverlayFS

OverlayFS is a type of union file system. It enables you 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.

OverlayFS remains a Technology Preview under most circumstances. As such, the kernel logs warnings when this technology is activated.

Full support is available for OverlayFS when used with supported container engines (**podman**, **cri-o**, or **buildah**) under the following restrictions:

- OverlayFS is supported for use only as a container engine graph driver or other specialized use cases, such as squashed **kdump** initramfs. Its use is supported primarily for container COW content, not for persistent storage. You must place any persistent storage on non-OverlayFS volumes. You can use only the default container engine configuration: 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.

Additionally, the following rules and limitations apply to using OverlayFS:

- The OverlayFS kernel ABI and user-space behavior are not considered stable, and might change in future updates.

- OverlayFS provides a restricted set of the POSIX standards. Test your application thoroughly before deploying it with OverlayFS. The following cases are not POSIX-compliant:

  - Lower files opened with **O_RDONLY** do not receive **st_atime** updates when the files are read.

  - Lower files opened with **O_RDONLY**, then mapped with **MAP_SHARED** are inconsistent with subsequent modification.

  - Fully compliant **st_ino** or **d_ino** values are not enabled by default on RHEL 8, but you can enable full POSIX compliance for them with a module option or mount option.
    To get consistent inode numbering, use the **xino=on** mount option.

    You can also use the **redirect_dir=on** and **index=on** options to improve POSIX compliance. These two options make the format of the upper layer incompatible with an overlay without these options. That is, you might get unexpected results or errors if you create an overlay with **redirect_dir=on** or **index=on**, unmount the overlay, then mount the overlay without these options.

- To determine whether an existing XFS file system is eligible for use as an overlay, use the following command and see if the **ftype=1** option is enabled:

  ```
  # xfs_info /mount-point | grep ftype
  ```

- SELinux security labels are enabled by default in all supported container engines with OverlayFS.

- Several known issues are associated with OverlayFS in this release. For details, see *Non-standard behavior* in the Linux kernel documentation.

For more information about OverlayFS, see the Linux kernel documentation.

(BZ#1690207)

Stratis is now available as a Technology Preview

Stratis is a new local storage manager. It provides managed file systems on top of pools of storage with additional features to the user.

Stratis enables you to more easily perform storage tasks such as:

- Manage snapshots and thin provisioning
- Automatically grow file system sizes as needed
- Maintain file systems

To administer Stratis storage, use the **stratis** utility, which communicates with the **stratisd** background service.

Stratis is provided as a Technology Preview.

For more information, see the Stratis documentation: Setting up Stratis file systems.

RHEL 8.3 updated Stratis to version 2.1.0. For more information, see Stratis 2.1.0 Release Notes.

(JIRA:RHELPLAN-1212)

IdM now supports setting up a Samba server on an IdM domain member as a Technology Preview

With this update, you can now set up a Samba server on an Identity Management (IdM) domain member. The new **ipa-client-samba** utility provided by the same-named package adds a Samba-specific Kerberos service principal to IdM and prepares the IdM client. For example, the utility creates the **/etc/samba/smb.conf** with the ID mapping configuration for the **sss** ID mapping back end. As a result, administrators can now set up Samba on an IdM domain member.

Due to IdM Trust Controllers not supporting the Global Catalog Service, AD-enrolled Windows hosts cannot find IdM users and groups in Windows. Additionally, IdM Trust Controllers do not support resolving IdM groups using the Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) protocols. As a consequence, AD users can only access the Samba shares and printers from IdM clients.

For details, see Setting up Samba on an IdM domain member .

(JIRA:RHELPLAN-13195)

8.5. HIGH AVAILABILITY AND CLUSTERS

Local mode version of pcs cluster setup command available as a Technology Preview

By default, the **pcs cluster setup** command automatically synchronizes all configuration files to the cluster nodes. Since Red Hat Enterprise Linux 8.3, the **pcs cluster setup** command provides the **--corosync-conf** option as a Technology Preview. Specifying this option switches the command to **local** mode. In this mode, **pcs** creates a **corosync.conf** file and saves it to a specified file on the local node only, without communicating with any other node. This allows you to create a **corosync.conf** file in a script and handle that file by means of the script.

(BZ#1839637)

Pacemaker podman bundles available as a Technology Preview

Pacemaker container bundles now run on Podman, with the container bundle feature being available as a Technology Preview. There is one exception to this feature being Technology Preview: Red Hat fully supports the use of Pacemaker bundles for Red Hat Openstack.

(BZ#1619620)

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#1784200)

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#1775847)

8.6. IDENTITY MANAGEMENT

Identity Management JSON-RPC API available as Technology Preview

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

Previously, the IdM API was enhanced to enable multiple versions of API commands. These 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 can 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 Using the Identity Management API to Communicate with the IdM Server (TECHNOLOGY PREVIEW).

(BZ#1664719)

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: http://tools.ietf.org/html/rfc6781#section-2
- Secure Domain Name System (DNS) Deployment Guide: http://dx.doi.org/10.6028/NIST.SP.800-81-2
- DNSSEC Key Rollover Timing Considerations: http://tools.ietf.org/html/rfc7583

Note that 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.

(BZ#1664718)

ACME available as a Technology Preview

The Automated Certificate Management Environment (ACME) service is now available in Identity Management (IdM) as a Technology Preview. ACME is a protocol for automated identifier validation and certificate issuance. Its goal is to improve security by reducing certificate lifetimes and avoiding manual processes from certificate lifecycle management.

In RHEL, the ACME service uses the Red Hat Certificate System (RHCS) PKI ACME responder. The RHCS ACME subsystem is automatically deployed on every certificate authority (CA) server in the IdM deployment, but it does not service requests until the administrator enables it. RHCS uses the **acmeIPAServerCert** profile when issuing ACME certificates. The validity period of issued certificates is 90 days. Enabling or disabling the ACME service affects the entire IdM deployment.

IMPORTANT

It is recommended to enable ACME only in an IdM deployment where all servers are running RHEL 8.4 or later. Earlier RHEL versions do not include the ACME service, which can cause problems in mixed-version deployments. For example, a CA server without ACME can cause client connections to fail, because it uses a different DNS Subject Alternative Name (SAN).

WARNING

Currently, RHCS does not remove expired certificates. Because ACME certificates expire after 90 days, the expired certificates can accumulate and this can affect performance.

- To enable ACME across the whole IdM deployment, use the **ipa-acme-manage enable** command:

```
# ipa-acme-manage enable
The ipa-acme-manage command was successful
```

- To disable ACME across the whole IdM deployment, use the **ipa-acme-manage disable** command:

```
# ipa-acme-manage disable
The ipa-acme-manage command was successful
```

- To check whether the ACME service is installed and if it is enabled or disabled, use the **ipa-acme-manage status** command:

```
# ipa-acme-manage status
ACME is enabled
The ipa-acme-manage command was successful
```

(JIRA:RHELPLAN-58596)

8.7. DESKTOP

GNOME for the 64-bit ARM architecture available as a Technology Preview

The GNOME desktop environment is now available for the 64-bit ARM architecture as a Technology Preview. This enables administrators to configure and manage servers from a graphical user interface (GUI) remotely, using the VNC session.

As a consequence, new administration applications are available on the 64-bit ARM architecture. For example: **Disk Usage Analyzer** (**baobab**), **Firewall Configuration** (**firewall-config**), **Red Hat Subscription Manager** (**subscription-manager**), or the **Firefox** web browser. Using **Firefox**, administrators can connect to the local Cockpit daemon remotely.

(JIRA:RHELPLAN-27394, BZ#1667225, BZ#1667516, BZ#1724302)

GNOME desktop on IBM Z is available as a Technology Preview

The GNOME desktop, including the Firefox web browser, is now available as a Technology Preview on the IBM Z architecture. You can now connect to a remote graphical session running GNOME using VNC to configure and manage your IBM Z servers.

(JIRA:RHELPLAN-27737)

8.8. GRAPHICS INFRASTRUCTURES

VNC remote console available as a Technology Preview for the 64-bit ARM architecture

On the 64-bit ARM architecture, the Virtual Network Computing (VNC) remote console is available as a Technology Preview. Note that the rest of the graphics stack is currently unverified for the 64-bit ARM architecture.

(BZ#1698565)

Intel Tiger Lake graphics available as a Technology Preview

Intel Tiger Lake UP3 and UP4 Xe graphics are now available as a Technology Preview.

To enable hardware acceleration with Intel Tiger Lake graphics, add the following option on the kernel command line:

```
i915.force_probe=pci-id
```

In this option, replace *pci-id* with one of the following:

- The PCI ID of your Intel GPU
- The * character to enable the **i915** driver with all alpha-quality hardware

(BZ#1783396)

8.9. RED HAT ENTERPRISE LINUX SYSTEM ROLES

HA Cluster RHEL System Role available as a Technology Preview

The High Availability Cluster (HA Cluster) role is now available as a Technology Preview. Currently, the following notable configurations are available:

- Configuring clusters running no fencing and no resources
- Configuring multi-link clusters
- Configuring custom cluster names and node names
- Configuring whether clusters start automatically on boot

(BZ#1893743)

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.

The **rhel-system-roles** packages are distributed through the AppStream 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#1812552)

8.10. VIRTUALIZATION

KVM virtualization is usable in RHEL 8 Hyper-V virtual machines

As a Technology Preview, nested KVM virtualization can now be used on the Microsoft Hyper-V hypervisor. As a result, you can create virtual machines on a RHEL 8 guest system running on a Hyper-V host.

Note that currently, this feature only works on Intel systems. In addition, nested virtualization is in some cases not enabled by default on Hyper-V. To enable it, see the following Microsoft documentation:

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization

(BZ#1519039)

AMD SEV for KVM virtual machines

As a Technology Preview, RHEL 8 provides the Secure Encrypted Virtualization (SEV) feature for AMD EPYC host machines that use the KVM hypervisor. If enabled on a virtual machine (VM), SEV encrypts VM memory so that the host cannot access data on the VM. This increases the security of the VM if the host is successfully infected by malware.

Note that the number of VMs that can use this feature at a time on a single host is determined by the host hardware. Current AMD EPYC processors support up to 509 running VMs using SEV.

Also note that for VMs with SEV configured to be able to boot, you must also configure the VM with a hard memory limit. To do so, add the following to the VM's XML configuration:

```
<memtune>
<hard_limit unit='KiB'>N</hard_limit>
</memtune>
```

The recommended value for N is equal to or greater then the guest RAM + 256 MiB. For example, if the guest is assigned 2 GiB RAM, N should be 2359296 or greater.

(BZ#1501618, BZ#1501607, JIRA:RHELPLAN-7677)

Intel vGPU

As a Technology Preview, it is now possible to divide a physical Intel GPU device into multiple virtual devices referred to as **mediated devices**. These mediated devices can then be assigned to multiple virtual machines (VMs) as virtual GPUs. As a result, these VMs share the performance of a single physical Intel GPU.

Note that only selected Intel GPUs are compatible with the vGPU feature.

In addition, it is possible to enable a VNC console operated by Intel vGPU. By enabling it, users can connect to a VNC console of the VM and see the VM's desktop hosted by Intel vGPU. However, this currently only works for RHEL guest operating systems.

(BZ#1528684)

Creating nested virtual machines

Nested KVM virtualization is provided as a Technology Preview for KVM virtual machines (VMs) running on Intel, AMD64, and IBM Z systems hosts with RHEL 8. With this feature, a RHEL 7 or RHEL 8 VM that runs on a physical RHEL 8 host can act as a hypervisor, and host its own VMs.

(JIRA:RHELPLAN-14047, JIRA:RHELPLAN-24437)

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)

ESXi hypervisor and SEV-ES available as a Technology Preview for RHEL VMs

As a Technology Preview, in RHEL 8.4 and later, you can enable the AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) to secure RHEL virtual machines (VMs) on VMware's ESXi hypervisor, versions 7.0.2 and later.

(BZ#1904496)

8.11. CONTAINERS

CNI plugins are available in Podman as a Technology Preview

CNI plugins are now available to use in Podman rootless mode as a Technology Preview. To enable this feature, users are required to build their own rootless CNI infrastructure container image.

(BZ#1932083)

The crun is available as a Technology Preview

The **crun** OCI runtime is now available for the **container-tools:rhel8** module as a Technology Preview. The **crun** container runtime supports an annotation that allows the container to access the rootless user's additional groups. This is useful for volume mounting in a directory where setgid is set, or where the user only has group access. Currently, neither the **crun** or **runc** runtimes fully support **cgroupsv2**.

(BZ#1841438)

A podman container image is available as a Technology Preview

The **registry.redhat.io/rhel8/podman** container image is a containerized implementation of the **podman** package. The **podman** tool is used for managing containers and images, volumes mounted into those containers, and pods made of groups of containers.

(JIRA:RHELPLAN-56659)

The podman-machine command is unsupported

The **podman-machine** command for managing virtual machines, is available only as a Technology Preview. Instead, run Podman directly from the command line.

(JIRA:RHELDOCS-16861)

CHAPTER 9. DEPRECATED FUNCTIONALITY

This part provides an overview of functionality that has been *deprecated* in Red Hat Enterprise Linux 8.

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.

The support status of deprecated functionality remains unchanged within Red Hat Enterprise Linux 8. For information about the length of support, see Red Hat Enterprise Linux Life Cycle and Red Hat Enterprise Linux Application Streams Life Cycle.

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 information regarding functionality that is present in RHEL 7 but has been *removed* in RHEL 8, see Considerations in adopting RHEL 8 .

9.1. INSTALLER AND IMAGE CREATION

Several Kickstart commands and options have been deprecated

Using the following commands and options in RHEL 8 Kickstart files will print a warning in the logs.

- **auth** or **authconfig**
- **device**
- **deviceprobe**
- **dmraid**
- **install**
- **lilo**
- **lilocheck**
- **mouse**
- **multipath**
- **bootloader --upgrade**
- **ignoredisk --interactive**
- **partition --active**
- **reboot --kexec**

Where only specific options are listed, the base command and its other options are still available and not deprecated.

For more details and related changes in Kickstart, see the Kickstart changes section of the *Considerations in adopting RHEL 8* document.

(BZ#1642765)

The --interactive option of the ignoredisk Kickstart command has been deprecated

Using the **--interactive option** in future releases of Red Hat Enterprise Linux will result in a fatal installation error. It is recommended that you modify your Kickstart file to remove the option.

(BZ#1637872)

The Kickstart autostep command has been deprecated

The **autostep** command has been deprecated. The related section about this command has been removed from the RHEL 8 documentation.

(BZ#1904251)

lorax-composer back end for Image Builder is deprecated in RHEL 8

The previous back end **lorax-composer** for Image Builder is considered deprecated. It will only receive select fixes for the rest of the Red Hat Enterprise Linux 8 life cycle and will be omitted from future major releases. Red Hat recommends that you uninstall **lorax-composer** the and install **osbuild-composer** back end instead.

See Composing a customized RHEL system image for more details.

(BZ#1893767)

9.2. SOFTWARE MANAGEMENT

rpmbuild --sign is deprecated

With this update, the **rpmbuild --sign** command has become deprecated. Using this command in future releases of Red Hat Enterprise Linux can result in an error. It is recommended that you use the **rpmsign** command instead.

(BZ#1688849)

9.3. SHELLS AND COMMAND-LINE TOOLS

The OpenEXR component has been deprecated

The **OpenEXR** component has been deprecated. Hence, the support for the **EXR** image format has been dropped from the **imagecodecs** module.

(BZ#1886310)

Metalink support for curl has been disabled.

A flaw was found in curl functionality in the way it handles credentials and file hash mismatch for content downloaded using the Metalink. This flaw allows malicious actors controlling a hosting server to:

- Trick users into downloading malicious content

- Gain unauthorized access to provided credentials without the user's knowledge

The highest threat from this vulnerability is confidentiality and integrity. To avoid this, the Metalink support for curl has been disabled from Red Hat Enterprise Linux 8.2.0.z.

As a workaround, execute the following command, after the Metalink file is downloaded:

```
wget --trust-server-names --input-metalink`
```

For example:

```
wget --trust-server-names --input-metalink <(curl -s $URL)
```

(BZ#1999620)

9.4. SECURITY

NSS SEED ciphers are deprecated

The Mozilla Network Security Services (**NSS**) library will not support TLS cipher suites that use a SEED cipher in a future release. To ensure smooth transition of deployments that rely on SEED ciphers when NSS removes support, Red Hat recommends enabling support for other cipher suites.

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

(BZ#1817533)

TLS 1.0 and TLS 1.1 are deprecated

The TLS 1.0 and TLS 1.1 protocols are disabled in the **DEFAULT** system-wide cryptographic policy level. If your scenario, for example, a video conferencing application in the Firefox web browser, requires using the deprecated protocols, switch the system-wide cryptographic policy to the **LEGACY** level:

```
# update-crypto-policies --set LEGACY
```

For more information, see the Strong crypto defaults in RHEL 8 and deprecation of weak crypto algorithms Knowledgebase article on the Red Hat Customer Portal and the **update-crypto-policies(8)** man page.

(BZ#1660839)

DSA is deprecated in RHEL 8

The Digital Signature Algorithm (DSA) is considered deprecated in Red Hat Enterprise Linux 8. Authentication mechanisms that depend on DSA keys do not work in the default configuration. Note that **OpenSSH** clients do not accept DSA host keys even in the **LEGACY** system-wide cryptographic policy level.

(BZ#1646541)

SSL2 Client Hello has been deprecated in NSS

The Transport Layer Security (**TLS**) protocol version 1.2 and earlier allow to start a negotiation with a **Client Hello** message formatted in a way that is backward compatible with the Secure Sockets Layer (**SSL**) protocol version 2. Support for this feature in the Network Security Services (**NSS**) library has been deprecated and it is disabled by default.

Applications that require support for this feature need to use the new **SSL_ENABLE_V2_COMPATIBLE_HELLO** API to enable it. Support for this feature may be removed completely in future releases of Red Hat Enterprise Linux 8.

(BZ#1645153)

TPM 1.2 is deprecated

The Trusted Platform Module (TPM) secure cryptoprocessor standard version was updated to version 2.0 in 2016. TPM 2.0 provides many improvements over TPM 1.2, and it is not backward compatible with the previous version. TPM 1.2 is deprecated in RHEL 8, and it might be removed in the next major release.

(BZ#1657927)

Runtime disabling SELinux using /etc/selinux/config is now deprecated

Runtime disabling SELinux using the **SELINUX=disabled** option in the **/etc/selinux/config** file has been deprecated. In RHEL 9, when you disable SELinux only through **/etc/selinux/config**, the system starts with SELinux enabled but with no policy loaded.

If your scenario really requires to completely disable SELinux, Red Hat recommends disabling SELinux by adding the **selinux=0** parameter to the kernel command line as described in the Changing SELinux modes at boot time section of the Using SELinux title.

(BZ#1932222)

ipa SELinux module removed from selinux-policy

The **ipa** SELinux module has been removed from the **selinux-policy** package, because it is no longer maintained. The functionality is now included in the **ipa-selinux** subpackage. If you need to use types or interfaces from the **ipa** module in a local SELinux policy, install the **ipa-selinux** package.

(BZ#1461914)

9.5. NETWORKING

Network scripts are deprecated in RHEL 8

Network scripts are deprecated in Red Hat Enterprise Linux 8 and they are no longer provided by default. The basic installation provides a new version of the **ifup** and **ifdown** scripts which call the **NetworkManager** service through the **nmcli** tool. In Red Hat Enterprise Linux 8, to run the **ifup** and the **ifdown** scripts, NetworkManager must be running.

Note that custom commands in **/sbin/ifup-local**, **ifdown-pre-local** and **ifdown-local** scripts are not executed.

If any of these scripts are required, the installation of the deprecated network scripts in the system is still possible with the following command:

```
~]# yum install network-scripts
```

The **ifup** and **ifdown** scripts link to the installed legacy network scripts.

Calling the legacy network scripts shows a warning about their deprecation.

(BZ#1647725)

The dropwatch tool is deprecated

The **dropwatch** tool has been deprecated. The tool will not be supported in future releases. Thus the tool is not recommended for new deployments As a replacement of this package, Red Hat recommends to use the **perf** command line tool.

For more information on using the **perf** command line tool, see the Getting started with Perf section on the Red Hat customer portal or the **perf** man page.

(BZ#1929173)

The term slaves is deprecated in the nmstate API

Red Hat is committed to using conscious language. See details about this initiative in Making open source more inclusive. Therefore the **slaves** term is deprecated in the Nmstate API. Use the term **port** when you use **nmstatectl**.

(JIRA:RHELDOCS-17641)

9.6. KERNEL

Installing RHEL for Real Time 8 using diskless boot is now deprecated

Diskless booting allows multiple systems to share a root file system via the network. While convenient, diskless boot is prone to introducing network latency in realtime workloads. With a future minor update of RHEL for Real Time 8, the diskless booting feature will no longer be supported.

(BZ#1748980)

The rdma_rxe Soft-RoCE driver is deprecated

Software Remote Direct Memory Access over Converged Ethernet (Soft-RoCE), also known as RXE, is a feature that emulates Remote Direct Memory Access (RDMA). In RHEL 8, the Soft-RoCE feature is available as an unsupported Technology Preview. However, due to stability issues, this feature has been deprecated and will be removed in RHEL 9.

(BZ#1878207)

9.7. PLATFORM ENABLEMENT

The Linux firewire sub-system and its associated user-space components are deprecated in RHEL 8

The **firewire** sub-system provides interfaces to use and maintain any resources on the IEEE 1394 bus. In RHEL 9, **firewire** will no longer be supported in the **kernel** package.

Note that **firewire** contains several user-space components provided by the **libavc1394**, **libdc1394**, **libraw1394** packages. These packages are subject to the deprecation as well.

(BZ#1871863)

9.8. FILE SYSTEMS AND STORAGE

The elevator kernel command line parameter is deprecated

The **elevator** kernel command line parameter was used in earlier RHEL releases to set the disk scheduler for all devices. In RHEL 8, the parameter is deprecated.

The upstream Linux kernel has removed support for the **elevator** parameter, but it is still available in RHEL 8 for compatibility reasons.

Note that the kernel selects a default disk scheduler based on the type of device. This is typically the optimal setting. If you require a different scheduler, Red Hat recommends that you use **udev** rules or the Tuned service to configure it. Match the selected devices and switch the scheduler only for those devices.

For more information, see Setting the disk scheduler.

(BZ#1665295)

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 logical volume .

LVM **mirror** has several known issues. For details, see known issues in file systems and storage .

(BZ#1827628)

peripety is deprecated

The **peripety** package is deprecated since RHEL 8.3.

The Peripety storage event notification daemon parses system storage logs into structured storage events. It helps you investigate storage issues.

(BZ#1871953)

VDO write modes other than async are deprecated

VDO supports several write modes in RHEL 8:

- **sync**
- **async**
- **async-unsafe**
- **auto**

Starting with RHEL 8.4, the following write modes are deprecated:

sync

Devices above the VDO layer cannot recognize if VDO is synchronous, and consequently, the devices cannot take advantage of the VDO **sync** mode.

async-unsafe

VDO added this write mode as a workaround for the reduced performance of **async** mode, which complies to Atomicity, Consistency, Isolation, and Durability (ACID). Red Hat does not recommend **async-unsafe** for most use cases and is not aware of any users who rely on it.

auto

This write mode only selects one of the other write modes. It is no longer necessary when VDO supports only a single write mode.

These write modes will be removed in a future major RHEL release.

The recommended VDO write mode is now **async**.

For more information on VDO write modes, see Selecting a VDO write mode.

(JIRA:RHELPLAN-70700)

NFSv3 over UDP has been disabled

The NFS server no longer opens or listens on a User Datagram Protocol (UDP) socket by default. This change affects only NFS version 3 because version 4 requires the Transmission Control Protocol (TCP).

NFS over UDP is no longer supported in RHEL 8.

(BZ#1592011)

cramfs has been deprecated

Due to lack of users, the **cramfs** kernel module is deprecated. **squashfs** is recommended as an alternative solution.

(BZ#1794513)

9.9. HIGH AVAILABILITY AND CLUSTERS

pcs commands that support the clufter tool have been deprecated

The **pcs** commands that support the **clufter** tool for analyzing cluster configuration formats have been deprecated. These commands now print a warning that the command has been deprecated and sections related to these commands have been removed from the **pcs** help display and the **pcs(8)** man page.

(BZ#1851335)

9.10. COMPILERS AND DEVELOPMENT TOOLS

The gdb.i686 packages are deprecated

In RHEL 8.1, the 32-bit versions of the GNU Debugger (GDB), **gdb.i686**, were shipped due to a dependency problem in another package. Because RHEL 8 does not support 32-bit hardware, the **gdb.i686** packages are deprecated since RHEL 8.4. The 64-bit versions of GDB, **gdb.x86_64**, are fully capable of debugging 32-bit applications.

If you use **gdb.i686** note the following important issues:

- The **gdb.i686** packages will no longer be updated. Users must install **gdb.x86_64** instead.
- If you have **gdb.i686** installed, installing **gdb.x86_64** will cause **dnf** to report **package gdb-8.2-14.el8.x86_64 obsoletes gdb < 8.2-14.el8 provided by gdb-8.2-12.el8.i686**. This is expected.

Either uninstall **gdb.i686** or pass **dnf** the **--allowerasing** option to remove **gdb.i686** and install **gdb.x8_64**.

- Users will no longer be able to install the **gdb.i686** packages on 64-bit systems, that is, those with the **libc.so.6()(64-bit)** packages.

(BZ#1853140)

libdwarf has been deprecated

The **libdwarf** library has been deprecated in RHEL 8. The library will likely not be supported in future major releases. Instead, use the **elfutils** and **libdw** libraries for applications that wish to process ELF/DWARF files.

Alternatives for the **libdwarf-tools dwarfdump** program are the **binutils readelf** program or the **elfutils eu-readelf** program, both used by passing the **--debug-dump** flag.

(BZ#1920624)

9.11. IDENTITY MANAGEMENT

openssh-ldap has been deprecated

The **openssh-ldap** subpackage has been deprecated in Red Hat Enterprise Linux 8 and will be removed in RHEL 9. As the **openssh-ldap** subpackage is not maintained upstream, Red Hat recommends using SSSD and the **sss_ssh_authorizedkeys** helper, which integrate better with other IdM solutions and are more secure.

By default, the SSSD **ldap** and **ipa** providers read the **sshPublicKey** LDAP attribute of the user object, if available. Note that you cannot use the default SSSD configuration for the **ad** provider or IdM trusted domains to retrieve SSH public keys from Active Directory (AD), since AD does not have a default LDAP attribute to store a public key.

To allow the **sss_ssh_authorizedkeys** helper to get the key from SSSD, enable the **ssh** responder by adding **ssh** to the **services** option in the **sssd.conf** file. See the **sssd.conf(5)** man page for details.

To allow **sshd** to use **sss_ssh_authorizedkeys**, add the **AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys** and **AuthorizedKeysCommandUser nobody** options to the **/etc/ssh/sshd_config** file as described by the **sss_ssh_authorizedkeys(1)** man page.

(BZ#1871025)

DES and 3DES encryption types have been removed

Due to security reasons, the Data Encryption Standard (DES) algorithm has been deprecated and disabled by default since RHEL 7. With the recent rebase of Kerberos packages, single-DES (DES) and triple-DES (3DES) encryption types have been removed from RHEL 8.

If you have configured services or users to only use DES or 3DES encryption, you might experience service interruptions such as:

- Kerberos authentication errors
- **unknown enctype** encryption errors
- Kerberos Distribution Centers (KDCs) with DES-encrypted Database Master Keys (**K/M**) fail to start

Perform the following actions to prepare for the upgrade:

1. Check if your KDC uses DES or 3DES encryption with the **krb5check** open source Python scripts. See krb5check on GitHub.

2. If you are using DES or 3DES encryption with any Kerberos principals, re-key them with a supported encryption type, such as Advanced Encryption Standard (AES). For instructions on re-keying, see Retiring DES from MIT Kerberos Documentation.

3. Test independence from DES and 3DES by temporarily setting the following Kerberos options before upgrading:

    a. In **/var/kerberos/krb5kdc/kdc.conf** on the KDC, set **supported_enctypes** and do not include **des** or **des3**.

    b. For every host, in **/etc/krb5.conf** and any files in **/etc/krb5.conf.d**, set **allow_weak_crypto** to **false**. It is false by default.

    c. For every host, in **/etc/krb5.conf** and any files in **/etc/krb5.conf.d**, set **permitted_enctypes**, **default_tgs_enctypes**, and **default_tkt_enctypes** and do not include **des** or **des3**.

4. If you do not experience any service interruptions with the test Kerberos settings from the previous step, remove them and upgrade. You do not need those settings after upgrading to the latest Kerberos packages.

(BZ#1877991)

Standalone use of the ctdb service has been deprecated

As of RHEL 8.4, customers are advised to use the **ctdb** clustered Samba service only when both of the following conditions apply:

- The **ctdb** service is managed as a **pacemaker** resource with the resource-agent **ctdb**.
- The **ctdb** service uses storage volumes that contain either a GlusterFS file system provided by the Red Hat Gluster Storage product or a GFS2 file system.

The stand-alone use case of the **ctdb** service has been deprecated and will not be included in a next major release of Red Hat Enterprise Linux. For further information on support policies for Samba, see the Knowledgebase article Support Policies for RHEL Resilient Storage - ctdb General Policies .

(BZ#1916296)

Running Samba as a PDC or BDC is deprecated

The classic domain controller mode that enabled administrators to run Samba as an NT4-like primary domain controller (PDC) and backup domain controller (BDC) is deprecated. The code and settings to configure these modes will be removed in a future Samba release.

As long as the Samba version in RHEL 8 provides the PDC and BDC modes, Red Hat supports these modes only in existing installations with Windows versions which support NT4 domains. Red Hat recommends not setting up a new Samba NT4 domain, because Microsoft operating systems later than Windows 7 and Windows Server 2008 R2 do not support NT4 domains.

If you use the PDC to authenticate only Linux users, Red Hat suggests migrating to Red Hat Identity Management (IdM) that is included in RHEL subscriptions. However, you cannot join Windows systems to an IdM domain. Note that Red Hat continues supporting the PDC functionality IdM uses in the background.

Red Hat does not support running Samba as an AD domain controller (DC).

(BZ#1926114)

The SSSD version of libwbclient has been deprecated

The SSSD implementation of the **libwbclient** package was added to allow the Samba **smbd** service to retrieve user and group information from AD without the need to run the **winbind** service. As Samba now requires that the **winbind** service is running and handling communication with AD, the related code has been removed from **smdb** for security reasons. As this additional required functionality is not part of SSSD and the SSSD implementation of **libwbclient** cannot be used with recent versions of Samba, the SSSD implementation of **libwbclient** is being deprecated.

(BZ#1881992)

The SMB1 protocol is deprecated in Samba

Starting with Samba 4.11, the insecure Server Message Block version 1 (SMB1) protocol is deprecated and will be removed in a future release.

To improve the security, by default, SMB1 is disabled in the Samba server and client utilities.

Jira:RHELDOCS-16612

9.12. DESKTOP

The libgnome-keyring library has been deprecated

The **libgnome-keyring** library has been deprecated in favor of the **libsecret** library, as **libgnome-keyring** is not maintained upstream, and does not follow the necessary cryptographic policies for RHEL. The new **libsecret** library is the replacement that follows the necessary security standards.

(BZ#1607766)

9.13. GRAPHICS INFRASTRUCTURES

AGP graphics cards are no longer supported

Graphics cards using the Accelerated Graphics Port (AGP) bus are not supported in Red Hat Enterprise Linux 8. Use the graphics cards with PCI-Express bus as the recommended replacement.

(BZ#1569610)

9.14. THE WEB CONSOLE

The web console no longer supports incomplete translations

The RHEL web console no longer provides translations for languages that have translations available for less than 50 % of the Console's translatable strings. If the browser requests translation to such a language, the user interface will be in English instead.

(BZ#1666722)

9.15. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The geoipupdate package has been deprecated

The **geoipupdate** package requires a third-party subscription and it also downloads proprietary content. Therefore, the **geoipupdate** package has been deprecated, and will be removed in the next major RHEL version.

(BZ#1874892)

9.16. VIRTUALIZATION

virt-manager has been deprecated

The Virtual Machine Manager application, also known as **virt-manager**, has been deprecated. The RHEL 8 web console, also known as **Cockpit**, is intended to become its replacement in a subsequent release. It is, therefore, recommended that you use the web console for managing virtualization in a GUI. Note, however, that some features available in **virt-manager** may not be yet available the RHEL 8 web console.

(JIRA:RHELPLAN-10304)

Virtual machine snapshots are not properly supported in RHEL 8

The current mechanism of creating virtual machine (VM) snapshots has been deprecated, as it is not working reliably. As a consequence, it is recommended not to use VM snapshots in RHEL 8.

Note that a new VM snapshot mechanism is under development and will be fully implemented in a future minor release of RHEL 8.

(BZ#1686057)

The Cirrus VGA virtual GPU type has been deprecated

With a future major update of Red Hat Enterprise Linux, the **Cirrus VGA** GPU device will no longer be supported in KVM virtual machines. Therefore, Red Hat recommends using the **stdvga**, **virtio-vga**, or **qxl** devices instead of Cirrus VGA.

(BZ#1651994)

KVM on IBM POWER has been deprecated

Using KVM virtualization on IBM POWER hardware has become deprecated. As a result, KVM on IBM POWER is still supported in RHEL 8, but will become unsupported in a future major release of RHEL.

(JIRA:RHELPLAN-71200)

SecureBoot image verification using SHA1-based signatures is deprecated

Performing SecureBoot image verification using SHA1-based signatures on UEFI (PE/COFF) executables has become deprecated.

Instead, Red Hat recommends using signatures based on the SHA2 algorithm, or later.

(BZ#1935497)

SPICE has been deprecated

The SPICE remote display protocol has become deprecated. Note that SPICE will remain supported in RHEL 8, but Red Hat recommends using alternate solutions for remote display streaming:

- For remote console access, use the VNC protocol.

- For advanced remote display functions, use third party tools such as RDP, HP RGS, or Mechdyne TGX.

(BZ#1849563)

9.17. CONTAINERS

The Podman varlink-based API v1.0 has been removed

The Podman varlink-based API v1.0 was deprecated in a previous release of RHEL 8. Podman v2.0 introduced a new Podman v2.0 RESTful API. With the release of Podman v3.0, the varlink-based API v1.0 has been completely removed.

(JIRA:RHELPLAN-45858)

container-tools:1.0 has been deprecated

The **container-tools:1.0** module has been deprecated and will no longer receive security updates. It is recommended to use a newer supported stable module stream, such as **container-tools:2.0** or **container-tools:3.0**.

(JIRA:RHELPLAN-59825)

9.18. DEPRECATED PACKAGES

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

- 389-ds-base-legacy-tools
- authd
- custodia
- firewire
- geoipupdate
- hostname
- isl
- isl-devel
- libavc1394
- libdc1394
- libdwarf
- libdwarf-devel
- libdwarf-static
- libdwarf-tools
- libidn

- libpng12
- libraw1394
- lorax-composer
- mailman
- mailx - replaced by s-nail
- mercurial
- ncompress
- net-tools
- netcf
- netcf-libs
- network-scripts
- nss_nis
- nss-pam-ldapd
- openssh-ldap
- parfait
- peripety
- perl-prefork
- perl-Sys-Virt
- python3-nose
- python3-pymongo
- python3-pytoml - replaced by python3-toml
- python3-virtualenv - use the **venv** module in Python 3 instead
- redhat-support-lib-python
- redhat-support-tool
- scala
- sendmail
- yp-tools
- ypbind
- ypserv

- xdelta
- xinetd

9.19. DEPRECATED DEVICES

This section lists devices (drivers, adapters) that continue to be supported until the end of life of RHEL 8 but will likely not be supported in future major releases of this product and are not recommended for new deployments. Support for devices other than those listed remains 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.

Device type	Driver	Device	Device ID
PCI	bnx2		
PCI	hpsa		0x103C:0x3239:0x103C:0x21C4
PCI	hpsa		0x103C:0x3239:0x103C:0x21C9
PCI	hpsa		0x103C:0x3239:0x103C:0x21CC
PCI	hpsa		0x103C:0x3239:0x103C:0x21CD
PCI	hpsa		0x103C:0x3239:0x103C:0x21CE
PCI	hpsa		0x103C:0x323a:0x103C:0x3233
PCI	hpsa		0x103C:0x323a:0x103C:0x3241
PCI	hpsa		0x103C:0x323a:0x103C:0x3243
PCI	hpsa		0x103C:0x323a:0x103C:0x3245
PCI	hpsa		0x103C:0x323a:0x103C:0x3247
PCI	hpsa		0x103C:0x323a:0x103C:0x3249
PCI	hpsa		0x103C:0x323a:0x103C:0x324A
PCI	hpsa		0x103C:0x323a:0x103C:0x324B
PCI	hpsa		0x103C:0x323b:0x103C:0x3350
PCI	hpsa		0x103C:0x323b:0x103C:0x3351

Device type	Driver	Device	Device ID
PCI	hpsa		0x103C:0x323b:0x103C:0x3352
PCI	hpsa		0x103C:0x323b:0x103C:0x3353
PCI	hpsa		0x103C:0x323b:0x103C:0x3354
PCI	hpsa		0x103C:0x323b:0x103C:0x3355
PCI	hpsa		0x103C:0x323b:0x103C:0x3356
PCI	hpsa		0x103C:0x333f:0x103c:0x333f
PCI	hpsa		0x9005:0x0290:0x9005:0x0580
PCI	hpsa		0x9005:0x0290:0x9005:0x0581
PCI	hpsa		0x9005:0x0290:0x9005:0x0582
PCI	hpsa		0x9005:0x0290:0x9005:0x0583
PCI	hpsa		0x9005:0x0290:0x9005:0x0584
PCI	hpsa		0x9005:0x0290:0x9005:0x0585
PCI	lpfc		0x10df:0x0724
PCI	lpfc		0x10df:0xe200
PCI	lpfc		0x10df:0xe220
PCI	lpfc		0x10df:0xf011
PCI	lpfc		0x10df:0xf015
PCI	lpfc		0x10df:0xf100
PCI	lpfc		0x10df:0xfc40
PCI	megaraid_sas		0x1000:0x005b
PCI	mpt3sas		0x1000:0x006E
PCI	mpt3sas		0x1000:0x0080

Device type	Driver	Device	Device ID
PCI	mpt3sas		0x1000:0x0081
PCI	mpt3sas		0x1000:0x0082
PCI	mpt3sas		0x1000:0x0083
PCI	mpt3sas		0x1000:0x0084
PCI	mpt3sas		0x1000:0x0085
PCI	mpt3sas		0x1000:0x0086
PCI	mpt3sas		0x1000:0x0087
PCI	myri10ge		
PCI	netxen_nic		
PCI	sfc		0x1924:0x0803
PCI	sfc		0x1924:0x0813
PCI	qla2xxx		0x1077:0x2031
PCI	qla2xxx		0x1077:0x2532
PCI	qla2xxx		0x1077:0x8031

CHAPTER 10. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 8.4.

10.1. INSTALLER AND IMAGE CREATION

The auth and authconfig Kickstart commands require the AppStream repository

The **authselect-compat** package is required by the **auth** and **authconfig** Kickstart commands during installation. Without this package, the installation fails if **auth** or **authconfig** are used. However, by design, the **authselect-compat** package is only available in the AppStream repository.

To work around this problem, verify that the BaseOS and AppStream repositories are available to the installer or use the **authselect** Kickstart command during installation.

(BZ#1640697)

The reboot --kexec and inst.kexec commands do not provide a predictable system state

Performing a RHEL installation with the **reboot --kexec** Kickstart command or the **inst.kexec** kernel boot parameters do not provide the same predictable system state as a full reboot. As a consequence, switching to the installed system without rebooting can produce unpredictable results.

Note that the **kexec** feature is deprecated and will be removed in a future release of Red Hat Enterprise Linux.

(BZ#1697896)

Network access is not enabled by default in the installation program

Several installation features require network access, for example, registration of a system using the Content Delivery Network (CDN), NTP server support, and network installation sources. However, network access is not enabled by default, and as a result, these features cannot be used until network access is enabled.

To work around this problem, add **ip=dhcp** to boot options to enable network access when the installation starts. Optionally, passing a Kickstart file or a repository located on the network using boot options also resolves the problem. As a result, the network-based installation features can be used.

(BZ#1757877)

The USB CD-ROM drive is not available as an installation source in Anaconda

Installation fails when the USB CD-ROM drive is the source for it and the Kickstart **ignoredisk --only-use=** command is specified. In this case, Anaconda cannot find and use this source disk.

To work around this problem, use the **harddrive --partition=sdX --dir=**/ command to install from USB CD-ROM drive. As a result, the installation does not fail.

(BZ#1914955)

Anaconda does not show encryption for a custom partition

The **Encrypt my data** radio button is not available when you choose the **Custom** partitioning during the system installation. As a result, your data is not encrypted when installation is complete.

To workaround this problem, set encryption in the custom partitioning screen for each device you want to encrypt. Anaconda will ask for a passphrase when leaving the dialog.

(BZ#1903786)

Installation program attempts automatic partitioning when no partitioning scheme is specified in the Kickstart file

When using a Kickstart file to perform an automated installation, the installation program attempts to perform automatic partitioning even when you do not specify any partitioning commands in the Kickstart file. The installation program behaves as if the **autopart** command was used in the Kickstart file, resulting in unexpected partitions. To work around this problem, use the **reqpart** command in the Kickstart file so that you can interactively configure manual partitioning.

(BZ#1954408)

The new osbuild-composer back end does not replicate the blueprint state from lorax-composer on upgrades

Image Builder users that are upgrading from the **lorax-composer** back end to the new **osbuild-composer** back end, blueprints can disappear. As a result, once the upgrade is complete, the blueprints do not display automatically. To work around this problem, perform the following steps.

Prerequisites

- You have the **composer-cli** CLI utility installed.

Procedure

1. Run the command to load the previous **lorax-composer** based blueprints into the new **osbuild-composer** back end:

```
$ for blueprint in $(find /var/lib/lorax/composer/blueprints/git/workspace/master -name
'*.toml'); do composer-cli blueprints push "${blueprint}"; done
```

As a result, the same blueprints are now available in **osbuild-composer** back end.

Additional resources

- For more details about this Known Issue, see the Image Builder blueprints are no longer present following an update to Red Hat Enterprise Linux 8.3 article.

(BZ#1897383)

Adding the same username in both blueprint and Kickstart files causes Edge image installation to fail

To install a RHEL for Edge image, users must create a blueprint to build a **rhel-edge-container image** and also create a Kickstart file to install the RHEL for Edge image. When a user adds the same username, password, and SSH key in both the blueprint and the Kickstart file, the RHEL for Edge image installation fails. Currently, there is no workaround.

(BZ#1951964)

GUI installation might fail if an attempt to unregister using the CDN is made before the repository refresh is completed

Since RHEL 8.2, when registering your system and attaching subscriptions using the Content Delivery Network (CDN), a refresh of the repository metadata is started by the GUI installation program. The refresh process is not part of the registration and subscription process, and as a consequence, the

Unregister button is enabled in the **Connect to Red Hat** window. Depending on the network connection, the refresh process might take more than a minute to complete. If you click the **Unregister** button before the refresh process is completed, the GUI installation might fail as the unregister process removes the CDN repository files and the certificates required by the installation program to communicate with the CDN.

To work around this problem, complete the following steps in the GUI installation after you have clicked the **Register** button in the **Connect to Red Hat** window:

1. From the **Connect to Red Hat** window, click **Done** to return to the **Installation Summary** window.
2. From the **Installation Summary** window, verify that the **Installation Source** and **Software Selection** status messages in italics are not displaying any processing information.
3. When the Installation Source and Software Selection categories are ready, click **Connect to Red Hat**.
4. Click the **Unregister** button.

After performing these steps, you can safely unregister the system during the GUI installation.

(BZ#1821192)

Registration fails for user accounts that belong to multiple organizations

Currently, when you attempt to register a system with a user account that belongs to multiple organizations, the registration process fails with the error message **You must specify an organization for new units**.

To work around this problem, you can either:

- Use a different user account that does not belong to multiple organizations.
- Use the **Activation Key** authentication method available in the Connect to Red Hat feature for GUI and Kickstart installations.
- Skip the registration step in Connect to Red Hat and use Subscription Manager to register your system post-installation.

(BZ#1822880)

Red Hat Insights client fails to register the operating system when using the graphical installer

Currently, the installation fails with an error at the end, which points to the Insights client.

To work around this problem, uncheck the **Connect to Red Hat Insights** option during the **Connect to Red Hat** step before registering the systems in the installer.

As a result, you can complete the installation and register to Insights afterwards by using this command:

```
# insights-client --register
```

(BZ#1931069)

Installation with autopart utility fails with inconsistent disk sector sizes

Installing RHEL using **autopart** with multiple inconsistent disk sector sizes fails. As a workaround, use a **plain** partitioning scheme, for example **autopart --type=plain**, instead of the default **LVM** scheme. Another option is to try re-configuring sector sizes, for example by running **hdparm --set-sector-size= <SIZE> <DEVICE>**.

As a workaround for kickstart installations:

- Restrict the disks used for the partitioning by specifying **ignoredisk --drives=..** OR **--only-use=..**.
- Specify disks to be used for each created LVM Physical Volume: **partition pv.1 --ondisk=..**.

As a workaround for manual installations:

- Select only the disks with the same sector size during manual installation in graphical or text mode.
- When disks with inconsistent sector size are selected for the installation, restrict each created LVM Volume Group to use Physical Volumes with the same sector size. This can only be done in graphical mode in the Custom partitioning spoke.

(BZ#1935722)

The GRUB retries to access the disk after initial failures during boot

Sometimes, Storage Area Networks (SANs) fail to acknowledge the **open** and **read** disk calls. Previously, the GRUB tool used to enter into the **grub_rescue** prompt resulting in the boot failure. With this update, GRUB retries to access the disk up to 20 times after the initial call to open and read the disk fails. If the GRUB tool is still unable to open or read the disk after these attempts, it will enter into the **grub_rescue** mode.

(BZ#1987087)

IBM Power systems with HASH MMU mode fail to boot with memory allocation failures

IBM Power Systems with **HASH memory allocation unit (MMU)** mode support **kdump** up to a maximum of 192 cores. Consequently, the system fails to boot with memory allocation failures if **kdump** is enabled on more than 192 cores. This limitation is due to RMA memory allocations during early boot in **HASH MMU** mode. To work around this problem, use the **Radix MMU** mode with **fadump** enabled instead of using **kdump**.

(BZ#2028361)

Unable to rebuild grub.cfg by using grub2-mkconfig on rhel-guest-image-8.4 images

The **rhel-guest-image-8.4** type does not contain the entry 'GRUB_DEFAULT=saved' entry in the **/etc/default/grub** file. As a consequence, if you install a new kernel and rebuild the grub using the **grub2-mkconfig -o /boot/grub2/grub.cfg** command, after reboot, the system will not boot up with the new kernel. To work around this issue, you can append the **GRUB_DEFAULT=saved** to the **/etc/default/grub** file. As a result, the system should boot up with the new kernel.

(BZ#2227218)

10.2. SUBSCRIPTION MANAGEMENT

syspurpose addons have no effect on the subscription-manager attach --auto output.

In Red Hat Enterprise Linux 8, four attributes of the **syspurpose** command-line tool have been added:

role,**usage**, **service_level_agreement** and **addons**. Currently, only **role**, **usage** and **service_level_agreement** affect the output of running the **subscription-manager attach --auto** command. Users who attempt to set values to the **addons** argument will not observe any effect on the subscriptions that are auto-attached.

(BZ#1687900)

10.3. INFRASTRUCTURE SERVICES

Postfix TLS fingerprint algorithm in the FIPS mode needs to be changed to SHA-256

By default in RHEL 8, **postfix** uses MD5 fingerprints with the TLS for backward compatibility. But in the FIPS mode, the MD5 hashing function is not available, which may cause TLS to incorrectly function in the default postfix configuration. To workaround this problem, the hashing function needs to be changed to SHA-256 in the postfix configuration file.

For more details, see the related Knowledgebase article Fix postfix TLS in the FIPS mode by switching to SHA-256 instead of MD5.

(BZ#1711885)

10.4. SECURITY

Users can run sudo commands as locked users

In systems where **sudoers** permissions are defined with the **ALL** keyword, **sudo** users with permissions can run **sudo** commands as users whose accounts are locked. Consequently, locked and expired accounts can still be used to execute commands.

To work around this problem, enable the newly implemented **runas_check_shell** option together with proper settings of valid shells in **/etc/shells**. This prevents attackers from running commands under system accounts such as **bin**.

(BZ#1786990)

libselinux-python is available only through its module

The **libselinux-python** package contains only Python 2 bindings for developing SELinux applications and it is used for backward compatibility. For this reason, **libselinux-python** is no longer available in the default RHEL 8 repositories through the **dnf install libselinux-python** command.

To work around this problem, enable both the **libselinux-python** and **python27** modules, and install the **libselinux-python** package and its dependencies with the following commands:

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

Alternatively, install **libselinux-python** using its install profile with a single command:

```
# dnf module install libselinux-python:2.8/common
```

As a result, you can install **libselinux-python** using the respective module.

(BZ#1666328)

udica processes UBI 8 containers only when started with --env container=podman

The Red Hat Universal Base Image 8 (UBI 8) containers set the **container** environment variable to the **oci** value instead of the **podman** value. This prevents the **udica** tool from analyzing a container JavaScript Object Notation (JSON) file.

To work around this problem, start a UBI 8 container using a **podman** command with the **--env container=podman** parameter. As a result, **udica** can generate an SELinux policy for a UBI 8 container only when you use the described workaround.

(BZ#1763210)

Negative effects of the default logging setup on performance

The default logging environment setup might consume 4 GB of memory or even more and adjustments of rate-limit values are complex when **systemd-journald** is running with **rsyslog**.

See the Negative effects of the RHEL default logging setup on performance and their mitigations Knowledgebase article for more information.

(JIRA:RHELPLAN-10431)

File permissions of /etc/passwd- are not aligned with the CIS RHEL 8 Benchmark 1.0.0

Because of an issue with the CIS Benchmark, the remediation of the SCAP rule that ensures permissions on the **/etc/passwd-** backup file configures permissions to **0644**. However, the **CIS Red Hat Enterprise Linux 8 Benchmark 1.0.0** requires file permissions **0600** for that file. As a consequence, the file permissions of **/etc/passwd-** are not aligned with the benchmark after remediation.

(BZ#1858866)

SELINUX=disabled in /etc/selinux/config does not work properly

Disabling SELinux using the **SELINUX=disabled** option in the **/etc/selinux/config** results in a process in which the kernel boots with SELinux enabled and switches to disabled mode later in the boot process. This might cause memory leaks.

To work around this problem, disable SELinux by adding the **selinux=0** parameter to the kernel command line as described in the Changing SELinux modes at boot time section of the Using SELinux title if your scenario really requires to completely disable SELinux.

(JIRA:RHELPLAN-34199)

crypto-policies incorrectly allow Camellia ciphers

The RHEL 8 system-wide cryptographic policies should disable Camellia ciphers in all policy levels, as stated in the product documentation. However, the Kerberos protocol enables the ciphers by default.

To work around the problem, apply the **NO-CAMELLIA** subpolicy:

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

In the previous command, replace **DEFAULT** with the cryptographic level name if you have switched from **DEFAULT** previously.

As a result, Camellia ciphers are correctly disallowed across all applications that use system-wide crypto policies only when you disable them through the workaround.

(BZ#1919155)

Connections to servers with SHA-1 signatures do not work with GnuTLS

SHA-1 signatures in certificates are rejected by the GnuTLS secure communications library as insecure. Consequently, applications that use GnuTLS as a TLS backend cannot establish a TLS connection to peers that offer such certificates. This behavior is inconsistent with other system cryptographic libraries.

To work around this problem, upgrade the server to use certificates signed with SHA-256 or stronger hash, or switch to the LEGACY policy.

(BZ#1628553)

Libreswan ignores the leftikeport and rightikeport options

Libreswan ignores the **leftikeport** and **rightikeport** options in any host-to-host Libreswan connections. As a consequence, Libreswan uses the default ports regardless of **leftikeport** and **rightikeport** settings. No workaround is available at the moment.

(BZ#1934058)

Using multiple labeled IPsec connections with IKEv2 do not work correctly

When Libreswan uses the **IKEv2** protocol, security labels for IPsec do not work correctly for more than one connection. As a consequence, Libreswan using labeled IPsec can establish only the first connection, but cannot establish subsequent connections correctly. To use more than one connection, use the **IKEv1** protocol.

(BZ#1934859)

OpenSSL in FIPS mode accepts only specific D-H parameters

In FIPS mode, TLS clients that use OpenSSL return a **bad dh value** error and abort TLS connections to servers that use manually generated parameters. This is because OpenSSL, when configured to work in compliance with FIPS 140-2, works only with Diffie-Hellman parameters compliant to NIST SP 800-56A rev3 Appendix D (groups 14, 15, 16, 17, and 18 defined in RFC 3526 and with groups defined in RFC 7919). Also, servers that use OpenSSL ignore all other parameters and instead select known parameters of similar size. To work around this problem, use only the compliant groups.

(BZ#1810911)

Smart-card provisioning process through OpenSC pkcs15-init does not work properly

The **file_caching** option is enabled in the default OpenSC configuration, and the file caching functionality does not handle some commands from the **pkcs15-init** tool properly. Consequently, the smart-card provisioning process through OpenSC fails.

To work around the problem, add the following snippet to the **/etc/opensc.conf** file:

```
app pkcs15-init {
        framework pkcs15 {
                use_file_caching = false;
        }
}
```

The smart-card provisioning through **pkcs15-init** only works if you apply the previously described workaround.

(BZ#1947025)

systemd cannot execute commands from arbitrary paths

The **systemd** service cannot execute commands from **/home/user/bin** arbitrary paths because the SELinux policy package does not include any such rule. Consequently, the custom services that are executed on non-system paths fail and eventually log the Access Vector Cache (AVC) denial audit messages when SELinux denied access. To work around this problem, do one of the following:

- Execute the command using a **shell** script with the **-c** option. For example,

```
bash -c command
```

- Execute the command from a common path using **/bin**, **/sbin**, **/usr/sbin**, **/usr/local/bin**, and **/usr/local/sbin** common directories.

(BZ#1860443)

selinux-policy prevents IPsec from working over TCP

The **libreswan** package in RHEL 8.4 supports IPsec-based VPNs using TCP encapsulation. However, the **selinux-policy** package does not reflect this update. As a consequence, when you set Libreswan to use TCP, the **ipsec** service fails to bind to the given TCP port.

To work around the problem, use a custom SELinux policy:

1. Open a new **.cil** file in a text editor, for example:

```
# vim local_ipsec_tcp_listen.cil
```

2. Insert the following rule:

```
(allow ipsec_t ipsecnat_port_t (tcp_socket (name_bind name_connect)))
```

3. Save and close the file.
4. Install the policy module:

```
# semodule -i local_ipsec_tcp_listen.cil
```

5. Restart the **ipsec** service:

```
# systemctl restart ipsec
```

As a result, Libreswan can bind and connect to the commonly used **4500/tcp** port.

(BZ#1931848)

Installation with the Server with GUI or Workstation software selections and CIS security profile is not possible

The CIS security profile is not compatible with the **Server with GUI** and **Workstation** software selections. As a consequence, a RHEL 8 installation with the **Server with GUI** software selection and CIS profile is not possible. An attempted installation using the CIS profile and either of these software selections will generate the error message:

–

> package xorg-x11-server-common has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the installation.

To work around the problem, do not use the CIS security profile with the **Server with GUI** or **Workstation** software selections.

(BZ#1843932)

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)

(BZ#1843913)

Kickstart uses org_fedora_oscap instead of com_redhat_oscap in RHEL 8

The Kickstart references the Open Security Content Automation Protocol (OSCAP) Anaconda add-on as **org_fedora_oscap** instead of **com_redhat_oscap** which might cause confusion. That is done to preserve backward compatibility with Red Hat Enterprise Linux 7.

(BZ#1665082)

Certain sets of interdependent rules in SSG can fail

Remediation of **SCAP Security Guide** (SSG) rules in a benchmark can fail due to undefined ordering of rules and their dependencies. If two or more rules need to be executed in a particular order, for example, when one rule installs a component and another rule configures the same component, they can run in the wrong order and remediation reports an error. To work around this problem, run the remediation twice, and the second run fixes the dependent rules.

(BZ#1750755)

OSCAP Anaconda Addon does not install all packages in text mode

The **OSCAP Anaconda Addon** plugin cannot modify the list of packages selected for installation by the system installer if the installation is running in text mode. Consequently, when a security policy profile is specified using Kickstart and the installation is running in text mode, any additional packages required by the security policy are not installed during installation.

To work around this problem, either run the installation in graphical mode or specify all packages that are required by the security policy profile in the security policy in the **%packages** section in your Kickstart file.

As a result, packages that are required by the security policy profile are not installed during RHEL installation without one of the described workarounds, and the installed system is not compliant with the given security policy profile.

(BZ#1674001)

OSCAP Anaconda Addon does not correctly handle customized profiles

The **OSCAP Anaconda Addon** plugin does not properly handle security profiles with customizations in separate files. Consequently, the customized profile is not available in the RHEL graphical installation even when you properly specify it in the corresponding Kickstart section.

To work around this problem, follow the instructions in the Creating a single SCAP data stream from an original DS and a tailoring file Knowledgebase article. As a result of this workaround, you can use a customized SCAP profile in the RHEL graphical installation.

(BZ#1691305)

Remediating service-related rules during kickstart installations might fail

During a kickstart installation, the OpenSCAP utility sometimes incorrectly shows that a service **enable** or **disable** state remediation is not needed. Consequently, OpenSCAP might set the services on the installed system to a non-compliant state. As a workaround, you can scan and remediate the system after the kickstart installation. This will fix the service-related issues.

(BZ#1834716)

Certain rsyslog priority strings do not work correctly

Support for the **GnuTLS** priority string for **imtcp** that allows fine-grained control over encryption is not complete. Consequently, the following priority strings do not work properly in **rsyslog**:

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-SHA384:+COMP-ALL:+GROUP-ALL
```

To work around this problem, use only correctly working priority strings:

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-SHA1:+COMP-ALL:+GROUP-ALL
```

As a result, current configurations must be limited to the strings that work correctly.

(BZ#1679512)

Conflict in SELinux Audit rules and SELinux boolean configurations

If the Audit rule list includes an Audit rule that contains a **subj_*** or **obj_*** field, and the SELinux boolean configuration changes, setting the SELinux booleans causes a deadlock. As a consequence, the system stops responding and requires a reboot to recover. To work around this problem, disable all Audit rules containing the **subj_*** or **obj_*** field, or temporarily disable such rules before changing SELinux booleans.

With the release of the RHSA-2021:2168 advisory, the kernel handles this situation properly and no longer deadlocks.

(BZ#1924230)

10.5. NETWORKING

The nm-cloud-setup service removes manually-configured secondary IP addresses from interfaces

Based on the information received from the cloud environment, the **nm-cloud-setup** service configures network interfaces. Disable **nm-cloud-setup** to manually configure interfaces. However, in certain cases, other services on the host can configure interfaces as well. For example, these services could add secondary IP addresses. To avoid that **nm-cloud-setup** removes secondary IP addresses:

1. Stop and disable the **nm-cloud-setup** service and timer:

```
# systemctl disable --now nm-cloud-setup.service nm-cloud-setup.timer
```

2. Display the available connection profiles:

```
# nmcli connection show
```

3. Reactive the affected connection profiles:

```
# nmcli connection up "<profile_name>"
```

As a result, the service no longer removes manually-configured secondary IP addresses from interfaces.

(BZ#2132754)

IPsec network traffic fails during IPsec offloading when GRO is disabled

IPsec offloading is not expected to work when Generic Receive Offload (GRO) is disabled on the device. If IPsec offloading is configured on a network interface and GRO is disabled on that device, IPsec network traffic fails.

To work around this problem, keep GRO enabled on the device.

(BZ#1649647)

10.6. KERNEL

Certain BCC utilities display a harmless warning

Due to macro redefinitions in some compiler specific kernel headers. Some BPF Compiler Collection (BCC) utilities show the following warning:

```
warning: __no_sanitize_address' macro redefined [-Wmacro-redefined]
```

The warning is harmless, and you can ignore it.

(BZ#1907271)

A vmcore capture fails after memory hot-plug or unplug operation

After performing the memory hot-plug or hot-unplug operation, the event comes after updating the device tree which contains memory layout information. Thereby the **makedumpfile** utility tries to access a non-existent physical address. The problem appears if all of the following conditions meet:

- A little-endian variant of IBM Power System runs RHEL 8.
- The **kdump** or **fadump** service is enabled on the system.

Consequently, the capture kernel fails to save **vmcore** if a kernel crash is triggered after the memory hot-plug or hot-unplug operation.

To work around this problem, restart the **kdump** service after hot-plug or hot-unplug:

```
# systemctl restart kdump.service
```

As a result, **vmcore** is successfully saved in the described scenario.

(BZ#1793389)

kdump fails to dump vmcore on SSH or NFS dump targets

The new version of **dracut-network** drops dependency on **dhcp-client** that requires an **ipcalc**. Consequently, when NIC port is configured to a static IP and **kdump** is configured to dump on SSH or NFS dump targets, **kdump** fails with the following error message:

```
ipcalc: command not found
```

To work around this problem:

1. Install the **ipcalc** package manually.

   ```
   dnf install ipcalc
   ```

2. Rebuild the **initramfs** for **kdump**.

   ```
   kdumpctrl rebuild
   ```

3. Restart the **kdump** service.

   ```
   systemctl restart kdump
   ```

As a result, **kdump** is successful in the described scenario.

(BZ#1931266)

Debug kernel fails to boot in crash capture environment in RHEL 8

Due to memory-demanding nature of the debug kernel, a problem occurs when the debug kernel is in use and a kernel panic is triggered. As a consequence, the debug kernel is not able to boot as the capture kernel, and a stack trace is generated instead. To work around this problem, increase the crash kernel memory accordingly. As a result, the debug kernel successfully boots in the crash capture environment.

(BZ#1659609)

Memory allocation on crash kernel fails at boot time

On some Ampere Altra systems, memory allocation fails when the 32-bit region is disabled in BIOS settings. Consequently, the **kdump** service fails to start because the conventional memory is not large enough to reserve the memory allocation.

To work around this problem, enable 32-bit CPU in BIOS as follows:

1. Open the BIOS settings on your system.
2. Open the **Chipset** menu.
3. Under **Memory Configuration**, enable the **Slave 32-bit** option.

As a result, the crash kernel allocates memory within the 32-bit region and the **kdump** service works as expected.

(BZ#1940674)

Certain kernel drivers do not display their version

The behavior for module versioning of many networking kernel drivers has changed in RHEL 8.4. Consequently, those drivers now do not display their version. Alternatively, after executing the **ethtool -i** command, the drivers display the **kernel** version instead of the **driver** version. To work around this problem, users can run the following command:

```
# modinfo <AFFECTED_DRIVER> | grep rhelversion
```

As a result, users can determine versions of the affected kernel drivers in scenarios where it is necessary.

Note that the perceived amount of change in a driver version string has no actual bearing on the amount of change in the driver itself.

(BZ#1944639)

Using irqpoll causes vmcore generation failure

Due to an existing problem with the **nvme** driver on the 64-bit ARM architectures that run on the Amazon Web Services (AWS) cloud platforms, the **vmcore** generation fails when you provide the **irqpoll** kernel command line parameter to the first kernel. Consequently, no **vmcore** file is dumped in the **/var/crash/** directory after a kernel crash. To work around this problem:

1. Append **irqpoll** to **KDUMP_COMMANDLINE_REMOVE** in the **/etc/sysconfig/kdump** file.

   ```
   KDUMP_COMMANDLINE_REMOVE="hugepages hugepagesz slub_debug quiet
   log_buf_len swiotlb"
   ```

2. Remove **irqpoll** from **KDUMP_COMMANDLINE_APPEND** in the **/etc/sysconfig/kdump** file.

   ```
   KDUMP_COMMANDLINE_APPEND="irqpoll nr_cpus=1 reset_devices
   cgroup_disable=memory udev.children-max=2 panic=10 swiotlb=noforce novmcoredd"
   ```

3. Restart the **kdump** service by running the **systemctl restart kdump** command.

As a result, the first kernel boots correctly and the **vmcore** file is expected to be captured upon the kernel crash.

Note that the **kdump** service can use a significant amount of crash kernel memory to dump the **vmcore** file. Ensure that the capture kernel has sufficient memory available for the **kdump** service.

(BZ#1654962)

The HP NMI watchdog does not always generate a crash dump

In certain cases, the **hpwdt** driver for the HP NMI watchdog is not able to claim a non-maskable interrupt (NMI) generated by the HPE watchdog timer because the NMI was instead consumed by the **perfmon** driver.

The missing NMI is initiated by one of two conditions:

1. The **Generate NMI** button on the Integrated Lights-Out (iLO) server management software. This button is triggered by a user.

2. The **hpwdt** watchdog. The expiration by default sends an NMI to the server.

Both sequences typically occur when the system is unresponsive. Under normal circumstances, the NMI handler for both these situations calls the **kernel panic()** function and if configured, the **kdump** service generates a **vmcore** file.

Because of the missing NMI, however, **kernel panic()** is not called and **vmcore** is not collected.

In the first case (1.), if the system was unresponsive, it remains so. To work around this scenario, use the virtual **Power** button to reset or power cycle the server.

In the second case (2.), the missing NMI is followed 9 seconds later by a reset from the Automated System Recovery (ASR).

The HPE Gen9 Server line experiences this problem in single-digit percentages. The Gen10 at an even smaller frequency.

(BZ#1602962)

The tuned-adm profile powersave command causes the system to become unresponsive

Executing the **tuned-adm profile powersave** command leads to an unresponsive state of the Penguin Valkyrie 2000 2-socket systems with the older Thunderx (CN88xx) processors. Consequently, reboot the system to resume working. To work around this problem, avoid using the **powersave** profile if your system matches the mentioned specifications.

(BZ#1609288)

The kernel ACPI driver reports it has no access to a PCIe ECAM memory region

The Advanced Configuration and Power Interface (ACPI) table provided by firmware does not define a memory region on the PCI bus in the Current Resource Settings (_CRS) method for the PCI bus device. Consequently, the following warning message occurs during the system boot:

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

However, the kernel is still able to access the **0x30000000-0x31ffffff** memory region, and can assign that memory region to the PCI Enhanced Configuration Access Mechanism (ECAM) properly. You can verify that PCI ECAM works correctly by accessing the PCIe configuration space over the 256 byte offset with the following output:

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-
if 02 [NVM Express])
 ...
        Capabilities: [900 v1] L1 PM Substates
                L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
                        PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
                L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
                        T_CommonMode=0us LTR1.2_Threshold=0ns
                L1SubCtl2: T_PwrOn=10us
```

As a result, you can ignore the warning message.

For more information about the problem, see the "Firmware Bug: ECAM area **mem 0x30000000-0x31ffffff** not reserved in ACPI namespace" appears during system boot solution.

(BZ#1868526)

The hwloc commands with the default settings do not work on single CPU Power9 and Power10 LPARs

With the **hwloc** package of version 2.2.0, any single-node Non-Uniform Memory Access (NUMA) system that runs Power9 / Power10 CPU is considered to be "disallowed". Consequently, all **hwloc** commands do not work and the following error message is displayed:

```
Topology does not contain any NUMA node, aborting!
```

You can use either of these two options to work around this problem:

- Set the environment variable **HWLOC_ALLOW=all**
- Use the **disallowed** flag with various **hwloc** commands

As a result, the **hwloc** command does not return any errors in the described scenario.

(BZ#1917560)

The OPEN MPI library may trigger run-time failures with default PML

In OPEN Message Passing Interface (OPEN MPI) implementation 4.0.x series, Unified Communication X (UCX) is the default point-to-point communicator (PML). The later versions of OPEN MPI 4.0.x series deprecated **openib** Byte Transfer Layer (BTL).

However, OPEN MPI, when run over a **homogeneous** cluster (same hardware and software configuration), UCX still uses **openib** BTL for MPI one-sided operations. As a consequence, this may trigger execution errors. To work around this problem:

- Run the **mpirun** command using following parameters:

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

where,

- The **-mca btl openib** parameter disables **openib** BTL
- The **-mca pml ucx** parameter configures OPEN MPI to use **ucx** PML.

- The **x UCX_NET_DEVICES=** parameter restricts UCX to use the specified devices

The OPEN MPI, when run over a **heterogeneous** cluster (different hardware and software configuration), it uses UCX as the default PML. As a consequence, this may cause the OPEN MPI jobs to run with erratic performance, unresponsive behavior, or crash failures. To work around this problem, set the UCX priority as:

- Run the **mpirun** command using following parameters:

```
-mca pml_ucx_priority 5
```

As a result, the OPEN MPI library is able to choose an alternative available transport layer over UCX.

(BZ#1866402)

Connections fail when attaching a virtual function to virtual machine

Pensando network cards that use the **ionic** device driver silently accept VLAN tag configuration requests and attempt configuring network connections while attaching network virtual functions (**VF**) to a virtual machine (**VM**). Such network connections fail as this feature is not yet supported by the card's firmware.

(BZ#1930576)

10.7. HARDWARE ENABLEMENT

The default 7 4 1 7 printk value sometimes causes temporary system unresponsiveness

The default **7 4 1 7printk** value allows for better debugging of the kernel activity. However, when coupled with a serial console, this **printk** setting can cause intense I/O bursts that can lead to a RHEL system becoming temporarily unresponsive. To work around this problem, we have added a new **optimize-serial-console** TuneD profile, which reduces the default **printk** value to **4 4 1 7**. Users can instrument their system as follows:

```
# tuned-adm profile throughput-performance optimize-serial-console
```

Having a lower **printk** value persistent across a reboot reduces the likelihood of system hangs.

Note that this setting change comes at the expense of losing the extra debugging information.

(JIRA:RHELPLAN-28940)

10.8. FILE SYSTEMS AND STORAGE

The /boot file system cannot be placed on LVM

You cannot place the **/boot** file system on an LVM logical volume. This limitation exists for the following reasons:

- On EFI systems, the *EFI System Partition* conventionally serves as the **/boot** file system. The uEFI standard requires a specific GPT partition type and a specific file system type for this partition.

- RHEL 8 uses the *Boot Loader Specification* (BLS) for system boot entries. This specification requires that the **/boot** file system is readable by the platform firmware. On EFI systems, the platform firmware can read only the **/boot** configuration defined by the uEFI standard.
- The support for LVM logical volumes in the GRUB 2 boot loader is incomplete. Red Hat does not plan to improve the support because the number of use cases for the feature is decreasing due to standards such as uEFI and BLS.

Red Hat does not plan to support **/boot** on LVM. Instead, Red Hat provides tools for managing system snapshots and rollback that do not need the **/boot** file system to be placed on an LVM logical volume.

(BZ#1496229)

LVM no longer allows creating volume groups with mixed block sizes

LVM utilities such as **vgcreate** or **vgextend** no longer allow you to create volume groups (VGs) where the physical volumes (PVs) have different logical block sizes. LVM has adopted this change because file systems fail to mount if you extend the underlying logical volume (LV) with a PV of a different block size.

To re-enable creating VGs with mixed block sizes, set the **allow_mixed_block_sizes=1** option in the **lvm.conf** file.

(BZ#1768536)

Limitations of LVM writecache

The **writecache** LVM caching method has the following limitations, which are not present in the **cache** method:

- You cannot name a **writecache** logical volume when using **pvmove** commands.
- You cannot use logical volumes with **writecache** in combination with thin pools or VDO.

The following limitation also applies to the **cache** method:

- You cannot resize a logical volume while **cache** or **writecache** is attached to it.

(JIRA:RHELPLAN-27987, BZ#1798631, BZ#1808012)

LVM mirror devices that store a LUKS volume sometimes become unresponsive

Mirrored LVM devices with a segment type of **mirror** that store a LUKS volume might become unresponsive under certain conditions. The unresponsive devices reject all I/O operations.

To work around the issue, Red Hat recommends that you use LVM RAID 1 devices with a segment type of **raid1** instead of **mirror** if you need to stack LUKS volumes on top of resilient software-defined storage.

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 .

(BZ#1730502)

An NFS 4.0 patch can result in reduced performance under an open-heavy workload

Previously, a bug was fixed that, in some cases, could cause an NFS open operation to overlook the fact that a file had been removed or renamed on the server. However, the fix may cause slower performance

with workloads that require many open operations. To work around this problem, it might help to use NFS version 4.1 or higher, which have been improved to grant delegations to clients in more cases, allowing clients to perform open operations locally, quickly, and safely.

(BZ#1748451)

xfs_quota state doesn't output all grace times when multiple quota types are specified

Currently, the **xfs_quota state** command doesn't output the grace time for quotas as expected with options specifying multiple quota types. To work around this issue, specify the required quota type in command option individually, i. e. **xfs_quota state -g**, **xfs_quota state -p** or **xfs_quota state -u**.

(BZ#1949743)

10.9. HIGH AVAILABILITY AND CLUSTERS

The ocf:heartbeat:pgsql resource agent and any third-party agents that parse crm_mon output in their stop operation may fail to stop during a shutdown process in RHEL 8.4

In the RHEL 8.4 GA release, Pacemaker's **crm_mon** command-line tool was modified to display a "shutting down" message rather than the usual cluster information when Pacemaker starts to shut down. As a result, shutdown progress, such as the stopping of resources, can not be monitored, and resource agents that parse crm_mon output in their stop operation (such as the **ocf:heartbeat:pgsql** agent distributed with the resource-agents package, or some custom or third-party agents) could fail to stop, leading to cluster problems.

It is recommended that clusters that use the **ocf:heartbeat:pgsql** resource agent not be upgraded to RHEL 8.4 until the z-stream is available.

(BZ#1948620)

10.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

getpwnam() might fail when called by a 32-bit application

When a user of NIS uses a 32-bit application that calls the **getpwnam()** function, the call fails if the **nss_nis.i686** package is missing. To work around this problem, manually install the missing package by using the **yum install nss_nis.i686** command.

(BZ#1803161)

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.

Since the RHEL 8.3 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#1819607)

MariaDB 10.5 does not warn about dropping a non-existent table when the OQGraph plug-in is enabled

When the **OQGraph** storage engine plug-in is loaded to the **MariaDB 10.5** server, **MariaDB** does not warn about dropping a non-existent table. In particular, when the user attempts to drop a non-existent table using the **DROP TABLE** or **DROP TABLE IF EXISTS** SQL commands, **MariaDB** neither returns an error message nor logs a warning.

Note that the **OQGraph** plug-in is provided by the **mariadb-oqgraph-engine** package, which is not installed by default.

(BZ#1944653)

PAM plug-in version 1.0 does not work in MariaDB

MariaDB 10.3 provides the Pluggable Authentication Modules (PAM) plug-in version 1.0. **MariaDB 10.5** provides the plug-in versions 1.0 and 2.0, version 2.0 is the default.

The **MariaDB** PAM plug-in version 1.0 does not work in RHEL 8. To work around this problem, use the PAM plug-in version 2.0 provided by the **mariadb:10.5** module stream.

See also **MariaDB 10.5** provides the PAM plug-in version 2.0 .

(BZ#1942330)

pyodbc does not work with MariaDB 10.3

The **pyodbc** module currently does not work with the **MariaDB 10.3** server included in the RHEL 8.4 release. Earlier versions of the **MariaDB 10.3** server and the **MariaDB 10.5** server are not affected by this problem.

Note that the root cause is in the **mariadb-connector-odbc** package and the affected package versions are as follows:

- **pyodbc-4.0.30**
- **mariadb-server-10.3.27**
- **mariadb-connector-odbc-3.0.7**

(BZ#1944692)

10.11. COMPILERS AND DEVELOPMENT TOOLS

GCC Toolset 10: Valgrind erroneously reports IBM z15 architecture support

Valgrind does not support certain IBM z15 processors features yet, but a bug in GCC Toolset 10 Valgrind causes it to report z15 support when run on a z15-capable system. As a consequence, software that tries to use z15 features when available cannot run under Valgrind. To work around this problem, when running on a z15 processor, use the system version of Valgrind accessible via /usr/bin/valgrind. This build will not report z15 support.

(BZ#1937340)

Memory leaks in pmproxy in PCP

The **pmproxy** service experiences memory leaks in Performance Co-Pilot (PCP) versions earlier than 5.3.0. The PCP version 5.3.0 is unavailable in RHEL 8.4 and the earlier minor versions of RHEL 8. As a consequence, RHEL 8 users might experience higher memory usage than expected.

To work around this problem, limit the memory usage of **pmproxy**:

1. Create the **/etc/systemd/system/pmproxy.service.d/override.conf** file by executing the following command:

```
# systemctl edit pmproxy
```

2. Add the following content to **override.conf** and save the changes:

```
[Service]
MemoryMax=10G
```

   Replace the *10G* value as per your requirement.

3. Restart the **pmproxy** service:

```
# systemctl restart pmproxy
```

As a result, the **pmproxy** service is restarted if the memory usage of **pmproxy** reaches the given limit.

(BZ#1991659)

10.12. IDENTITY MANAGEMENT

Installing KRA fails if all KRA members are hidden replicas

The **ipa-kra-install** utility fails on a cluster where the Key Recovery Authority (KRA) is already present, if the first KRA instance is installed on a hidden replica. Consequently, you cannot add further KRA instances to the cluster.

To work around this problem, unhide the hidden replica that has the KRA role before you add new KRA instances. You can hide it again when **ipa-kra-install** completes successfully.

(BZ#1816784)

Using the cert-fix utility with the --agent-uid pkidbuser option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.

(BZ#1729215)

The /var/log/lastlog sparse file on IdM hosts can cause performance problems

During the IdM installation, a range of 200,000 UIDs from a total of 10,000 possible ranges is randomly selected and assigned. Selecting a random range in this way significantly reduces the probability of conflicting IDs in case you decide to merge two separate IdM domains in the future.

However, having high UIDs can create problems with the **/var/log/lastlog** file. For example, if a user with the UID of 1280000008 logs in to an IdM client, the local **/var/log/lastlog** file size increases to almost 400 GB. Although the actual file is sparse and does not use all that space, certain applications are not

designed to identify sparse files by default and may require a specific option to handle them. For example, if the setup is complex and a backup and copy application does not handle sparse files correctly, the file is copied as if its size was 400 GB. This behavior can cause performance problems.

To work around this problem:

- In case of a standard package, refer to its documentation to identify the option that handles sparse files.
- In case of a custom application, ensure that it is able to manage sparse files such as **/var/log/lastlog** correctly.

(JIRA:RHELPLAN-59111)

FreeRADIUS silently truncates Tunnel-Passwords longer than 249 characters

If a Tunnel-Password is longer than 249 characters, the FreeRADIUS service silently truncates it. This may lead to unexpected password incompatibilities with other systems.

To work around the problem, choose a password that is 249 characters or fewer.

(BZ#1723362)

FIPS mode does not support using a shared secret to establish a cross-forest trust

Establishing a cross-forest trust using a shared secret fails in FIPS mode because NTLMSSP authentication is not FIPS-compliant. To work around this problem, authenticate with an Active Directory (AD) administrative account when establishing a trust between an IdM domain with FIPS mode enabled and an AD domain.

(BZ#1924707)

Downgrading **authselect** after the rebase to version 1.2.2 breaks system authentication

The **authselect** package has been rebased to the latest upstream version **1.2.2**. Downgrading **authselect** is not supported and breaks system authentication for all users, including **root**.

If you downgraded the **authselect** package to **1.2.1** or earlier, perform the following steps to work around this problem:

1. At the GRUB boot screen, select **Red Hat Enterprise Linux** with the version of the kernel that you want to boot and press **e** to edit the entry.
2. Type **single** as a separate word at the end of the line that starts with **linux** and press **Ctrl+x** to start the boot process.
3. Upon booting in single-user mode, enter the root password.
4. Restore authselect configuration using the following command:

```
# authselect select sssd --force
```

(BZ#1892761)

Upgrading an IdM server from RHEL 8.3 to RHEL 8.4 fails if pki-ca package version is earlier than 10.10.5

The IdM server upgrade program, **ipa-server-upgrade**, fails if the **pki-ca** package version is earlier than 10.10.5. As the required files do not exist in these versions, the IdM server upgrade does not complete successfully both at package installation and when **ipa-server-upgrade** or **ipactl** are executed.

To resolve this issue, upgrade the **pki-*** packages to version 10.10.5 or higher and run the **ipa-server-upgrade** command again.

(BZ#1957768)

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)

10.13. DESKTOP

Disabling flatpak repositories from Software Repositories is not possible

Currently, it is not possible to disable or remove **flatpak** repositories in the Software Repositories tool in the GNOME Software utility.

(BZ#1668760)

Drag-and-drop does not work between desktop and applications

Due to a bug in the **gnome-shell-extensions** package, the drag-and-drop functionality does not currently work between desktop and applications. Support for this feature will be added back in a future release.

(BZ#1717947)

Generation 2 RHEL 8 virtual machines sometimes fail to boot on Hyper-V Server 2016 hosts

When using RHEL 8 as the guest operating system on a virtual machine (VM) running on a Microsoft Hyper-V Server 2016 host, the VM in some cases fails to boot and returns to the GRUB boot menu. In addition, the following error is logged in the Hyper-V event log:

> The guest operating system reported that it failed with the following error code: 0x1E

This error occurs due to a UEFI firmware bug on the Hyper-V host. To work around this problem, use Hyper-V Server 2019 as the host.

(BZ#1583445)

10.14. GRAPHICS INFRASTRUCTURES

radeon fails to reset hardware correctly

The **radeon** kernel driver currently does not reset hardware in the kexec context correctly. Instead, **radeon** falls over, 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"
force_rebuild 1
```

Restart the machine and **kdump**. After starting **kdump**, the **force_rebuild 1** line may be removed from the configuration file.

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

(BZ#1694705)

Multiple HDR displays on a single MST topology may not power on

On systems using NVIDIA Turing GPUs with the **nouveau** driver, using a **DisplayPort** hub (such as a laptop dock) with multiple monitors which support HDR plugged into it may result in failure to turn on. This is due to the system erroneously thinking there is not enough bandwidth on the hub to support all of the displays.

(BZ#1812577)

Unable to run graphical applications using sudo command

When trying to run graphical applications as a user with elevated privileges, the application fails to open with an error message. The failure happens because **Xwayland** is restricted by the **Xauthority** file to use regular user credentials for authentication.

To work around this problem, use the **sudo -E** command to run graphical applications as a **root** user.

(BZ#1673073)

VNC Viewer displays wrong colors with the 16-bit color depth on IBM Z

The VNC Viewer application displays wrong colors when you connect to a VNC session on an IBM Z server with the 16-bit color depth.

To work around the problem, set the 24-bit color depth on the VNC server. With the **Xvnc** server, replace the **-depth 16** option with **-depth 24** in the **Xvnc** configuration.

As a result, VNC clients display the correct colors but use more network bandwidth with the server.

(BZ#1886147)

Hardware acceleration is not supported on ARM

Built-in graphics drivers do not support hardware acceleration or the Vulkan API on the 64-bit ARM architecture.

To enable hardware acceleration or Vulkan on ARM, install the proprietary Nvidia driver.

(JIRA:RHELPLAN-57914)

GUI in ESXi might crash due to low video memory

The graphical user interface (GUI) on RHEL virtual machines (VMs) in the VMware ESXi 7.0.1 hypervisor with vCenter Server 7.0.1 requires a certain amount of video memory. If you connect multiple consoles or high-resolution monitors to the VM, the GUI requires least 16 MB of video memory. If you start the GUI with less video memory, the GUI might terminate unexpectedly.

To work around the problem, configure the hypervisor to assign at least 16 MB of video memory to the VM. As a result, the GUI on the VM no longer crashes.

(BZ#1910358)

10.15. VIRTUALIZATION

virsh iface-* commands do not work consistently

Currently, **virsh iface-*** commands, such as **virsh iface-start** and **virsh iface-destroy**, frequently fail due to configuration dependencies. Therefore, it is recommended not to use **virsh iface-*** commands for configuring and managing host network connections. Instead, use the NetworkManager program and its related management applications.

(BZ#1664592)

Virtual machines sometimes fail to start when using many virtio-blk disks

Adding a large number of virtio-blk devices to a virtual machine (VM) may exhaust the number of interrupt vectors available in the platform. If this occurs, the VM's guest OS fails to boot, and displays a **dracut-initqueue[392]: Warning: Could not boot** error.

(BZ#1719687)

Attaching LUN devices to virtual machines using virtio-blk does not work

The q35 machine type does not support transitional virtio 1.0 devices, and RHEL 8 therefore lacks support for features that were deprecated in virtio 1.0. In particular, it is not possible on a RHEL 8 host to send SCSI commands from virtio-blk devices. As a consequence, attaching a physical disk as a LUN device to a virtual machine fails when using the virtio-blk controller.

Note that physical disks can still be passed through to the guest operating system, but they should be configured with the **device='disk'** option rather than **device='lun'**.

(BZ#1777138)

Virtual machines using Cooperlake cannot boot when TSX is disabled on the host

Virtual machines (VMs) that use the **Cooperlake** CPU model currently fail to boot when the **TSX** CPU flag is diabled on the host. Instead, the host displays the following error message:

```
the CPU is incompatible with host CPU: Host CPU does not provide required features: hle, rtm
```

To make VMs with **Cooperlake** usable on such host, disable the HLE, RTM, and TAA_NO flags in the VM configuration in the VM's XML configuration:

```
<feature policy='disable' name='hle'/>
<feature policy='disable' name='rtm'/>
<feature policy='disable' name='taa-no'/>
```

(BZ#1860743)

Using perf kvm record on IBM POWER Systems can cause the VM to crash

When using a RHEL 8 host on the little-endian variant of IBM POWER hardware, using the **perf kvm record** command to collect trace event samples for a KVM virtual machine (VM) in some cases results in the VM becoming unresponsive. This situation occurs when:

- The **perf** utility is used by an unprivileged user, and the **-p** option is used to identify the VM - for example **perf kvm record -e trace_cycles -p 12345**.
- The VM was started using the **virsh** shell.

To work around this problem, use the **perf kvm** utility with the **-i** option to monitor VMs that were created using the **virsh** shell. For example:

```
# perf kvm record -e trace_imc/trace_cycles/  -p <guest pid> -i
```

Note that when using the **-i** option, child tasks do not inherit counters, and threads will therefore not be monitored.

(BZ#1924016)

Migrating a POWER9 guest from a RHEL 7-ALT host to RHEL 8 fails

Currently, migrating a POWER9 virtual machine from a RHEL 7-ALT host system to RHEL 8 becomes unresponsive with a **Migration status: active** status.

To work around this problem, disable Transparent Huge Pages (THP) on the RHEL 7-ALT host, which enables the migration to complete successfully.

(BZ#1741436)

Using virt-customize sometimes causes guestfs-firstboot to fail

After modifying a virtual machine (VM) disk image using the **virt-customize** utility, the **guestfs-firstboot** service in some cases fails due to incorrect SELinux permissions. This causes a variety of problems during VM startup, such as failing user creation or system registration.

To avoid this problem, add the **--selinux-relabel** option to the **virt-customize** command.

(BZ#1554735)

Virtual machines with iommu_platform=on fail to start on IBM POWER

RHEL 8 currently does not support the **iommu_platform=on** parameter for virtual machines (VMs) on IBM POWER system. As a consequence, starting a VM with this parameter on IBM POWER hardware results in the VM becoming unresponsive during the boot process.

(BZ#1910848)

SMT CPU topology is not detected by VMs when using host passthrough mode on AMD EPYC

When a virtual machine (VM) boots with the CPU host passthrough mode on an AMD EPYC host, the **TOPOEXT** CPU feature flag is not present. Consequently, the VM is not able to detect a virtual CPU topology with multiple threads per core. To work around this problem, boot the VM with the EPYC CPU model instead of host passthrough.

(BZ#1740002)

Windows Server 2016 virtual machines with Hyper-V enabled fail to boot when using certain CPU models

Currently, it is not possible to boot a virtual machine (VM) that uses Windows Server 2016 as the guest operating system, has the Hyper-V role enabled, and uses one of the following CPU models:

- **EPYC-IBPB**
- **EPYC**

To work around this problem, use the **EPYC-v3** CPU model, or manually enable the **xsaves** CPU flag for the VM.

(BZ#1942888)

Deleting a macvtap interface from a virtual machine resets all macvtap connections

Currently, deleting a **macvtap** interface from a running virtual machines (VM) with multiple **macvtap** devices also resets the connection settings of the other **macvtap** interfaces. As a consequence, the VM may experience network issues.

(BZ#1332758)

Hot unplugging an IBMVFC device on PowerVM fails

When using a virtual machine (VM) with a RHEL 8 guest operating system on the PowerVM hypervisor, attempting to remove an IBM Power Virtual Fibre Channel (IBMVFC) device from the running VM currently fails. Instead, it displays an **outstanding translation** error.

To work around this problem, remove the IBMVFC device when the VM is shut down.

(BZ#1959020)

IBM POWER hosts may crash when using the ibmvfc driver

When running RHEL 8 on a PowerVM logical partition (LPAR), a variety of errors may currently occur due problems with the **ibmvfc** driver. As a consequence, the host's kernel may panic under certain circumstances, such as:

- Using the Live Partition Mobility (LPM) feature
- Resetting a host adapter
- Using SCSI error handling (SCSI EH) functions

(BZ#1961722)

Mounting virtiofs directories fails in certain circumstances on RHEL 8 guests

Currently, when using the **virtiofs** feature to provide a host directory to a virtual machine (VM), mounting the directory on the VM fails with an "Operation not supported" error if the VM is using a RHEL 8.4 (or earlier) kernel but a RHEL 8.5 (or later) **selinux-policy** package.

To work around this problem, reboot the guest and boot it into the latest available kernel on the guest.

(BZ#1995558)

10.16. RHEL IN CLOUD ENVIRONMENTS

kdump sometimes does not start on Azure and Hyper-V

On RHEL 8 guest operating systems hosted on the Microsoft Azure or Hyper-V hypervisors, starting the **kdump** kernel in some cases fails when post-exec notifiers are enabled.

To work around this problem, disable crash kexec post notifiers:

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

(BZ#1865745)

Setting static IP in a RHEL 8 virtual machine on a VMWare host does not work

Currently, when using RHEL 8 as a guest operating system of a virtual machine (VM) on a VMWare host, the DatasourceOVF function does not work correctly. As a consequence, if you use the **cloud-init** utility to set the VM's network to static IP and then reboot the VM, the VM's network will be changed to DHCP.

(BZ#1750862)

Core dumping RHEL 8 virtual machines with certain NICs to a remote machine on Azure takes longer than expected

Currently, using the **kdump** utility to save the core dump file of a RHEL 8 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 dump file is saved after approximately 200 seconds, instead of immediately. In addition, the following error message is logged on the console before the dump file is saved.

```
device (eth0): linklocal6: DAD failed for an EUI-64 address
```

(BZ#1854037)

The nm-cloud-setup utility sets an incorrect default route on Microsoft Azure

On Microsoft Azure, the **nm-cloud-setup** utility fails to detect the correct gateway of the cloud environment. As a consequence, the utility sets an incorrect default route, and breaks connectivity. There is no workaround available at the moment.

(BZ#1912236)

The SCSI host address sometimes changes when booting a Hyper-V VM with multiple guest disks

Currently, when booting a RHEL 8 virtual machine (VM) on the Hyper-V hypervisor, the host portion of the *Host, Bus, Target, Lun* (HBTL) SCSI address in some cases changes. As a consequence, automated tasks set up with the HBTL SCSI identification or device node in the VM do not work consistently. This occurs if the VM has more than one disk or if the disks have different sizes.

To work around the problem, modify your kickstart files, using one of the following methods:

Method 1: Use persistent identifiers for SCSI devices.

You can use for example the following powershell script to determine the specific device identifiers:

```
# Output what the /dev/disk/by-id/<value> for the specified hyper-v virtual disk.
# Takes a single parameter which is the virtual disk file.
# Note: kickstart syntax works with and without the /dev/ prefix.
param (
    [Parameter(Mandatory=$true)][string]$virtualdisk
)

$what = Get-VHD -Path $virtualdisk
$part = $what.DiskIdentifier.ToLower().split('-')

$p = $part[0]
$s0 = $p[6] + $p[7] + $p[4] + $p[5] + $p[2] + $p[3] + $p[0] + $p[1]

$p = $part[1]
$s1 =  $p[2] + $p[3] + $p[0] + $p[1]

[string]::format("/dev/disk/by-id/wwn-0x60022480{0}{1}{2}", $s0, $s1, $part[4])
```

You can use this script on the hyper-v host, for example as follows:

```
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_8.vhdx
/dev/disk/by-id/wwn-0x60022480e00bc367d7fd902e8bf0d3b4
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_9.vhdx
/dev/disk/by-id/wwn-0x600224807270e09717645b1890f8a9a2
```

Afterwards, the disk values can be used in the kickstart file, for example as follows:

```
part / --fstype=xfs --grow --asprimary --size=8192 --ondisk=/dev/disk/by-id/wwn-
0x600224807270e09717645b1890f8a9a2
part /home --fstype="xfs" --grow --ondisk=/dev/disk/by-id/wwn-
0x60022480e00bc367d7fd902e8bf0d3b4
```

As these values are specific for each virtual disk, the configuration needs to be done for each VM instance. It may, therefore, be useful to use the **%include** syntax to place the disk information into a separate file.

Method 2: Set up device selection by size.

A kickstart file that configures disk selection based on size must include lines similar to the following:

```
...

# Disk partitioning information is supplied in a file to kick start
%include /tmp/disks

...

# Partition information is created during install using the %pre section
%pre --interpreter /bin/bash --log /tmp/ks_pre.log

 # Dump whole SCSI/IDE disks out sorted from smallest to largest ouputting
```

```
# just the name
disks=(`lsblk -n -o NAME -l -b -x SIZE -d -I 8,3`) || exit 1

# We are assuming we have 3 disks which will be used
# and we will create some variables to represent
d0=${disks[0]}
d1=${disks[1]}
d2=${disks[2]}

echo "part /home --fstype="xfs" --ondisk=$d2 --grow" >> /tmp/disks
echo "part swap --fstype="swap" --ondisk=$d0 --size=4096" >> /tmp/disks
echo "part / --fstype="xfs" --ondisk=$d1 --grow" >> /tmp/disks
echo "part /boot --fstype="xfs" --ondisk=$d1 --size=1024" >> /tmp/disks

%end
```

(BZ#1906870)

RHEL 8 virtual machines have lower network performance on AWS ARM64 instances

When using RHEL 8 as a guest operating system in a virtual machine (VM) that runs on an Amazon Web Services (AWS) ARM64 instance, the VM has lower than expected network performance when the **iommu.strict=1** kernel parameter is used or when no **iommu.strict** parameter is defined.

To work around this problem, change the parameter to **iommu.strict=0**. However, this can also decrease the security of the VM.

(BZ#1836058)

Hibernating RHEL 8 guests fails when FIPS mode is enabled

Currently, it is not possible to hibernate a virtual machine (VM) that uses RHEL 8 as its guest operating system if the VM is using FIPS mode.

(BZ#1934033, BZ#1944636)

SSH keys are not generated correctly on EC2 instanced created from a backup AMI

Currently, when creating a new Amazon EC2 instance of RHEL 8 from a backup Amazon Machine Image (AMI), **cloud-init** deletes existing SSH keys on the VM but does not create new ones. Consequently, the VM in some cases cannot connect to the host.

To work around this problem, edit the **cloud.cgf** file and change the "ssh_genkeytypes: ~" line to **ssh_genkeytypes: ['rsa', 'ecdsa', 'ed25519']**.

This makes it possible for SSH keys to be deleted and generated correctly when provisioning a RHEL 8 VM in the described circumstances.

(BZ#1957532)

SSH keys are not generated correctly on EC2 instanced created from a backup AMI

Currently, when creating a new Amazon EC2 instance of RHEL 8 from a backup Amazon Machine Image (AMI), **cloud-init** deletes existing SSH keys on the VM but does not create new ones. Consequently, the VM in some cases cannot connect to the host.

To work around this problem, edit the **cloud.cgf** file and change the "ssh_genkeytypes: ~" line to **ssh_genkeytypes: ['rsa', 'ecdsa', 'ed25519']**.

This makes it possible for SSH keys to be deleted and generated correctly when provisioning a RHEL 8 VM in the described circumstances.

(BZ#1963981)

10.17. SUPPORTABILITY

redhat-support-tool does not work with the FUTURE crypto policy

Because a cryptographic key used by a certificate on the Customer Portal API does not meet the requirements by the **FUTURE** system-wide cryptographic policy, the **redhat-support-tool** utility does not work with this policy level at the moment.

To work around this problem, use the **DEFAULT** crypto policy while connecting to the Customer Portal API.

(BZ#1802026)

CHAPTER 11. INTERNATIONALIZATION

11.1. RED HAT ENTERPRISE LINUX 8 INTERNATIONAL LANGUAGES

Red Hat Enterprise Linux 8 supports the installation of multiple languages and the changing of languages based on your requirements.

- East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese.
- European Languages - English, German, Spanish, French, Italian, Portuguese, and Russian.

The following table lists the fonts and input methods provided for various major languages.

Language	Default Font (Font Package)	Input Methods
English	dejavu-sans-fonts	
French	dejavu-sans-fonts	
German	dejavu-sans-fonts	
Italian	dejavu-sans-fonts	
Russian	dejavu-sans-fonts	
Spanish	dejavu-sans-fonts	
Portuguese	dejavu-sans-fonts	
Simplified Chinese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
Traditional Chinese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
Japanese	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
Korean	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-hangul, libhangul

11.2. NOTABLE CHANGES TO INTERNATIONALIZATION IN RHEL 8

RHEL 8 introduces the following changes to internationalization compared to RHEL 7:

- Support for the **Unicode 11** computing industry standard has been added.
- Internationalization is distributed in multiple packages, which allows for smaller footprint installations. For more information, see Using langpacks.

- A number of **glibc** locales have been synchronized with Unicode Common Locale Data Repository (CLDR).

APPENDIX A. 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#1859301, BZ#1862529, BZ#1859218, BZ#1850275, BZ#1851975
KVM Hypervisor	JIRA:RHELPLAN-44450
NetworkManager	BZ#1900260, BZ#1878783, BZ#1766944, BZ#1912236
OpenIPMI	BZ#1796588
SLOF	BZ#1910848
accel-config	BZ#1843266
anaconda	BZ#1890009, BZ#1874394, BZ#1642391, BZ#1609325, BZ#1854307, BZ#1821192, BZ#1822880, BZ#1914955, BZ#1847681, BZ#1903786, BZ#1931069, BZ#1954408, BZ#1897657
apr	BZ#1819607
authselect	BZ#1892761
bcc	BZ#1879411
bind	BZ#1876492, BZ#1882040, BZ#1854148
bpftrace	BZ#1879413
clevis	BZ#1887836, BZ#1853651
cloud-init	BZ#1886430, BZ#1750862, BZ#1957532, BZ#1963981
cmake	BZ#1816874
cockpit	BZ#1666722
corosync-qdevice	BZ#1784200
corosync	BZ#1870449
createrepo_c	BZ#1795936, BZ#1894361

Component	Tickets
crun	BZ#1841438
crypto-policies	BZ#1919155, BZ#1660839
dhcp	BZ#1883999
distribution	BZ#1877430, BZ#1855776, BZ#1855781, BZ#1657927
dnf	BZ#1865803, BZ#1807446, BZ#1698145
dwarves	BZ#1903566
dyninst	BZ#1892001, BZ#1892007
edk2	BZ#1935497
elfutils	BZ#1875318, BZ#1879758
fapolicyd	BZ#1940289, BZ#1896875, BZ#1887451
fence-agents	BZ#1775847
freeipmi	BZ#1861627
freeradius	BZ#1723362
gcc	BZ#1868446, BZ#1821994, BZ#1850498, BZ#1656139, BZ#1891998
gdb	BZ#1853140
ghostscript	BZ#1874523
glibc	BZ#1868106, BZ#1871397, BZ#1880670, BZ#1882466, BZ#1871396, BZ#1893662, BZ#1817513, BZ#1871385, BZ#1871387, BZ#1871395
gnome-shell-extensions	BZ#1717947
gnome-software	BZ#1668760
gnutls	BZ#1628553
go-toolset	BZ#1870531
grafana-container	BZ#1916154

Component	Tickets
grafana-pcp	BZ#1845592, BZ#1854093
grafana	BZ#1850471
grub2	BZ#1583445
httpd	BZ#1869576, BZ#1883648
hwloc	BZ#1841354, BZ#1917560
ima-evm-utils	BZ#1868683
ipa	BZ#1891056, BZ#1340463, BZ#1816784, BZ#1924707, BZ#1664719, BZ#1664718
iproute	BZ#1849815
iptraf-ng	BZ#1842690, BZ#1906097
jmc	BZ#1919283
kernel-rt	BZ#1858099
kernel	BZ#1806882, BZ#1846838, BZ#1884857, BZ#1876527, BZ#1660290, BZ#1885850, BZ#1649647, BZ#1838876, BZ#1871246, BZ#1893882, BZ#1876519, BZ#1860031, BZ#1844416, BZ#1780258, BZ#1851933, BZ#1885406, BZ#1867490, BZ#1908893, BZ#1919745, BZ#1867910, BZ#1887940, BZ#1874005, BZ#1871214, BZ#1622041, BZ#1533270, BZ#1900674, BZ#1869758, BZ#1861261, BZ#1848427, BZ#1847567, BZ#1844157, BZ#1844111, BZ#1811839, BZ#1877019, BZ#1548297, BZ#1844086, BZ#1839055, BZ#1905088, BZ#1882620, BZ#1784246, BZ#1916583, BZ#1924230, BZ#1793389, BZ#1944639, BZ#1694705, BZ#1748451, BZ#1654962, BZ#1708456, BZ#1812577, BZ#1666538, BZ#1602962, BZ#1609288, BZ#1730502, BZ#1865745, BZ#1868526, BZ#1910358, BZ#1924016, BZ#1906870, BZ#1940674, BZ#1930576, BZ#1907271, BZ#1942888, BZ#1836058, BZ#1934033, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1570255, BZ#1814836, BZ#1696451, BZ#1348508, BZ#1839311, BZ#1783396, JIRA:RHELPLAN-57712, BZ#1837187, BZ#1904496, BZ#1660337, BZ#1665295, BZ#1569610
kexec-tools	BZ#1844941, BZ#1931266, BZ#1854037
kmod-redhat-oracleasm	BZ#1827015
kpatch	BZ#1798711

Component	Tickets
krb5	BZ#1877991
libbpf	BZ#1919345
libgnome-keyring	BZ#1607766
libguestfs	BZ#1554735
libmpc	BZ#1835193
libpcap	BZ#1743650
libpwquality	BZ#1537240
libreswan	BZ#1891128, BZ#1372050, BZ#1025061, BZ#1934058, BZ#1934859
libselinux-python-2.8-module	BZ#1666328
libselinux	BZ#1879368
libsemanage	BZ#1913224
libvirt	BZ#1664592, BZ#1332758, BZ#1528684
libvpd	BZ#1844429
llvm-toolset	BZ#1892716
lvm2	BZ#1496229, BZ#1768536
mariadb-connector-odbc	BZ#1944692
mariadb	BZ#1936842, BZ#1944653, BZ#1942330
mesa	BZ#1886147
micropipenv	BZ#1849096
mod_fcgid	BZ#1876525
mod_security	BZ#1824859
mutter	BZ#1886034

Component	Tickets
mysql-selinux	BZ#1895021
net-snmp	BZ#1817190
nfs-utils	BZ#1592011
nispor	BZ#1848817
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1817533, BZ#1645153
opal-prd	BZ#1844427
opencryptoki	BZ#1847433
opencv	BZ#1886310
openmpi	BZ#1866402
opensc	BZ#1877973, BZ#1947025
openscap	BZ#1824152, BZ#1887794, BZ#1840579
openssl	BZ#1810911
osbuild-composer	BZ#1951964
oscap-anaconda-addon	BZ#1843932, BZ#1665082, BZ#1674001, BZ#1691305, BZ#1834716
p11-kit	BZ#1887853
pacemaker	BZ#1371576, BZ#1948620
pcp-container	BZ#1916155
pcp	BZ#1854035, BZ#1847808
pcs	BZ#1869399, BZ#1741056, BZ#1667066, BZ#1667061, BZ#1457314, BZ#1839637, BZ#1619620, BZ#1851335
perl-IO-String	BZ#1890998

Component	Tickets
perl-Time-HiRes	BZ#1895852
pki-core	BZ#1868233, BZ#1729215
podman	BZ#1734854, BZ#1881894, BZ#1932083
policycoreutils	BZ#1868717, BZ#1926386
popt	BZ#1843787
postfix	BZ#1688389, BZ#1711885
powerpc-utils	BZ#1853297
py3c	BZ#1841060
pyOpenSSL	BZ#1629914
pykickstart	BZ#1637872
pyodbc	BZ#1881490
python-PyMySQL	BZ#1820628
python-blivet	BZ#1656485
qemu-kvm	BZ#1790620, BZ#1719687, BZ#1860743, BZ#1740002, BZ#1651994
quota	BZ#1868671
rear	BZ#1729499, BZ#1898080, BZ#1832394
redhat-support-tool	BZ#1802026
redis	BZ#1862063
resource-agents	BZ#1471182
rhel-system-roles	BZ#1865990, BZ#1926947, BZ#1889484, BZ#1927943, BZ#1893712, BZ#1893743, BZ#1893906, BZ#1893908, BZ#1895188, BZ#1893696, BZ#1893699, BZ#1889893, BZ#1893961
rpm	BZ#1834931, BZ#1923167, BZ#1688849

Component	Tickets
rshim	BZ#1744737
rsyslog	BZ#1869874, JIRA:RHELPLAN-10431, BZ#1679512
rust-toolset	BZ#1896712
samba	BZ#1878109, JIRA:RHELPLAN-13195, Jira:RHELDOCS-16612
scap-security-guide	BZ#1889344, BZ#1927019, BZ#1918742, BZ#1778188, BZ#1843913, BZ#1858866, BZ#1750755
scap-workbench	BZ#1877522
selinux-policy	BZ#1889673, BZ#1860443, BZ#1931848, BZ#1461914
sendmail	BZ#1868041
setroubleshoot	BZ#1875290, BZ#1794807
skopeo	BZ#1940854
sos	BZ#1966838
spamassassin	BZ#1822388
spice	BZ#1849563
sssd	BZ#1819012, BZ#1884196, BZ#1884213, BZ#1784459, BZ#1893698, BZ#1881992
stalld	BZ#1875037
stratisd	BZ#1798244, BZ#1868100
subscription-manager	BZ#1905398
subversion	BZ#1844947
sudo	BZ#1786990
swig	BZ#1853639
systemd	BZ#1827462
systemtap	BZ#1875341

Component	Tickets
tang-container	BZ#1913310
tang	BZ#1828558
texlive	BZ#1889802
tpm2-abrmd	BZ#1855177
tuned	BZ#1874052
udica	BZ#1763210
unbound	BZ#1850460
usbguard	BZ#1887448, BZ#1940060
valgrind	BZ#1504123, BZ#1937340
virtio-win	BZ#1861229
wayland	BZ#1673073
xdp-tools	BZ#1880268
xfsprogs	BZ#1949743
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565

Component	Tickets
other	BZ#1839151, BZ#1780124, JIRA:RHELPLAN-59941, JIRA:RHELPLAN-59938, JIRA:RHELPLAN-59950, BZ#1952421, JIRA:RHELPLAN-37817, BZ#1918055, JIRA:RHELPLAN-56664, JIRA:RHELPLAN-56661, JIRA:RHELPLAN-39843, BZ#1925192, JIRA:RHELPLAN-73418, JIRA:RHELPLAN-63081, BZ#1935686, BZ#1634655, JIRA:RHELPLAN-56782, JIRA:RHELPLAN-72660, JIRA:RHELPLAN-72994, JIRA:RHELPLAN-37579, BZ#1952161, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, JIRA:RHELPLAN-59111, BZ#1757877, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1897383, BZ#1741436, BZ#1971061, JIRA:RHELPLAN-58629, BZ#1960412, BZ#1959020, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-56659, BZ#1906489, BZ#1957316, BZ#1960043, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1932222, BZ#1686057, BZ#1748980, JIRA:RHELPLAN-71200, BZ#1827628, JIRA:RHELPLAN-45858, BZ#1871025, BZ#1871953, BZ#1874892, BZ#1893767, BZ#1916296, BZ#1926114, BZ#1904251, JIRA:RHELPLAN-59825, BZ#1920624, JIRA:RHELPLAN-70700, BZ#1929173

APPENDIX B. REVISION HISTORY

0.3-6

Thu May 23 2024, Brian Angelica (bangelic@redhat.com)

- Updated Enhancements in JIRA:RHELDOCS-18188 (Networking).

0.3-5

Thu May 9 2024, Brian Angelica (bangelic@redhat.com)

- Updated Tech Preview in BZ#1690207.

0.3-4

Thu May 9 2024, Gabriela Fialova (gfialova@redhat.com)

- Updated a known issue BZ#1730502 (Storage).

0.3-3

Thu Feb 29 2024, Lucie Vařáková (lvarakova@redhat.com)

- Added a deprecated functionality JIRA:RHELDOCS-17641 (Networking).

0.3-2

Fri Nov 10 2023, Gabriela Fialová (gfialova@redhat.com)

- Updated the module on Providing Feedback on RHEL Documentation.

0.3-1

Tue Nov 7 2023, Gabriela Fialová (gfialova@redhat.com)

- Fix broken links.

0.3-0

Fri Oct 13 2023, Gabriela Fialová (gfialova@redhat.com)

- Added a Tech Preview JIRA:RHELDOCS-16861 (Containers).

0.2-9

September 8 2023, Marc Muehlfeld (mmuehlfeld@redhat.com)

- Added a deprecated functionality release note JIRA:RHELDOCS-16612 (Samba).

0.2-8

Fri Aug 11 2023, Lucie Vařáková (lvarakova@redhat.com)

- Added a known issue BZ#2227218 (Installer and image creation).

0.2-7

Thu Apr 27 2023, Gabriela Fialová (gfialova@redhat.com)

- Added a known issue JIRA:RHELPLAN-155168 (Identity Management).

0.2-6

Thu Apr 13 2023, Gabriela Fialová (gfialova@redhat.com)

- Fixed 2 broken links in DFs and KIs.

0.2-5

Thu Dec 08, 2022, Marc Muehlfeld (mmuehlfeld@redhat.com)

- Added a known issue BZ#2132754 (Networking).

0.2-4

Thu Jun 09, Lucie Vařáková (lmanasko@redhat.com)

- Added a new feature BZ#1996076 (Identity Management).

0.2-3

Fri Apr 29, Lenka Špačková (lspackova@redhat.com)

- Updated Deprecated functionality introduction.
- Fixed typo in BZ#1605216.
- Fixed broken links.

0.2-2

Thu Mar 24 2022, Jaroslav Klech (jklech@redhat.com)

- Added a bug fix BZ#1947839 (Kernel).

0.2-1

Mon Mar 21 2022, Jaroslav Klech (jklech@redhat.com)

- Removed a known issue (Kernel).

0.2-0

Fri Feb 04 2022, Jaroslav Klech (jklech@redhat.com)

- Added a deprecated functionality BZ#1871863 (Hardware enablement).
- Updated Deprecated packages.
- Added deprecated functionality BZ#1794513 (Filesystems and storage).

0.1-9

Thu Jan 20 2022, Lucie Maňásková (lmanasko@redhat.com)

- Added a known issue BZ#2028361 (Installer and image creation).

0.1-8

Thu Dec 23 2021, Lenka Špačková (lspackova@redhat.com)

- Added information about the Soft-RoCE driver, **rdma_rxe**, to Technology Previews BZ#1605216 and Deprecated Functionality BZ#1878207 (Kernel).

0.1-7

Wed Dec 22 29 2021, Lenka Špačková (lspackova@redhat.com)

- Added an enhancement BZ#2005431 (Security).
- Updated Deprecated packages.

0.1-6

Thu Oct 29 2021, Jaroslav Klech (jklech@redhat.com)

- Updated the **fw_devlink** parameter (Important changes to external kernel parameters).

0.1-5

Thu Oct 07 2021, Lenka Špačková (lspackova@redhat.com)

- Updated the known issue BZ#1942330 (Dynamic programming languages, web and database servers).

0.1-4

Tue Oct 05 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added deprecated functionality BZ#1999620 (Shells and command-line tools).

0.1-3

Fri Sep 17 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added known issue BZ#1987087 (Installer).

0.1-2

Tue Sep 07 2021, Lucie Maňásková (lmanasko@redhat.com)

- Updated the known issue BZ#1961722 (Virtualization).

0.1-1

Fri Sep 03 2021, Lenka Špačková (lspackova@redhat.com)

- Updated the known issue BZ#1995558 (Virtualization).

0.1-0

Mon Aug 30 2021, Lenka Špačková (lspackova@redhat.com)

- Added a known issue BZ#1995558 (Virtualization).
- Added a bug fix BZ#1940854 (Containers).

0.0-9

Fri Aug 20 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added the Package management with YUM/DNF to the Distribution chapter.
- Updated the text of BZ#1708456 (Kernel).
- Added new feature BZ#1888214 (File systems and storage).

- Added a known issue BZ#1991659 (Compilers and development tools).
- Added a Technology Preview feature JIRA:RHELPLAN-58596 (Identity Management).

0.0-8

Tue Aug 10 2021, Lucie Manásková (lmanasko@redhat.com)

- Updated new feature BZ#1905398 (RHEL in cloud environents).

0.0-7

Tue Aug 03 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added known issue BZ#1935722 (Installer and image creation).
- Added known issue BZ#1961722 (Virtualization).

0.0-6

Fri Jul 23 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added known issue BZ#1924230 (Security).
- Added known issue BZ#1957768 (Identity Management).

0.0-5

Fri Jul 16 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added known issue BZ#1959020 (Virtualization).
- Added known issue BZ#1963981 (RHEL in cloud environments).
- Added new feature BZ#1340463 (Identity Management).
- Removed invalid release note and its revision history entry.

0.0-4

Wed Jun 23 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added new feature BZ#1966838 (Supportability).
- Updated Deprecated devices with **sfc**.
- Other small improvements.

0.0-3

Wed Jun 16 2021, Lucie Maňásková (lmanasko@redhat.com)

- Added deprecated functionality BZ#1929173 (Networking).
- Added deprecated functionality BZ#1920624 (Compilers and development tools).
- Added new feature JIRA:RHELPLAN-63081 (Identity Management).
- Added known issue BZ#1949743 (File systems and storage).

- Added know inssue BZ#1332758 (Virtualization).
- Added known issue BZ#1957532 (RHEL in cloud environments).
- Other small improvements.

0.0-2

Fri Jun 04 2021, Lenka Špačková (lspackova@redhat.com)

- Fixed the BZ#1849815 note.
- Various formatting improvements.

0.0-1

Wed May 18 2021, Lucie Maňásková (lmanasko@redhat.com)

- Release of the Red Hat Enterprise Linux 8.4 Release Notes.

0.0-0

Wed Mar 31 2021, Lucie Maňásková (lmanasko@redhat.com)

- Release of the Red Hat Enterprise Linux 8.4 Beta Release Notes.