Red Hat Enterprise Linux 9

9.8 Release Notes

Release Notes for Red Hat Enterprise Linux 9.8

Last Updated: 2026-05-20

Red Hat Enterprise Linux 9 9.8 Release Notes

Release Notes for Red Hat Enterprise Linux 9.8

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 9.8 and document known problems in this release, as well as notable bug fixes, Technology Previews, deprecated functionality, and other details. For information about installing Red Hat Enterprise Linux, see Installation.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We are committed to providing high-quality documentation and value your feedback. To help us improve, you can submit suggestions or report errors through the Red Hat Jira tracking system.

Procedure

1. Log in to the Jira website.
   If you do not have an account, select the option to create one.
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 OF RED HAT ENTERPRISE LINUX 9.8

1.1. MAJOR CHANGES IN RHEL 9.8

Installer and image creation

Key highlights for RHEL image builder:

- You can use RHEL image builder to create disk images with advanced partitioning.
- You can customize your blueprint to enable injecting a Kickstart file when building ISO images.
- System images created with the RHEL image builder, such as AWS or KVM formats, do not have a separate /**boot** partition.
- RHEL image builder now supports WSL2 images.

Security

GnuTLS 3.8.10 introduces ML-KEM hybrid key exchange and ML-DSA post-quantum (PQ) algorithms.

RHEL 9.8 provides OpenSSH in version 9.9, which introduces many fixes and improvements over OpenSSH 8.7 in the previous RHEL version.

The **p11-kit** packages have been upgraded to upstream version 0.26.1, which delivers support for post-quantum cryptography (PQC) definitions in PKCS #11 headers.

The **clevis-pin-trustee** package provides a new Clevis pin trustee that enables automated encryption and decryption of LUKS-encrypted volumes by using remote attestation through the Trustee Key Broker Service (KBS).

The **fapolicyd** packages are rebased to upstream version 1.4.3, and you can now filter rules.

See New features - Security for more information.

Kernel

Review the most notable kernel updates in Red Hat Enterprise Linux 9.8.

- Extends kernel observability with additional **perf** features and new Intel **core**, **uncore**, **c-state**, and package performance events.
- Aligns **perf** and BPF tooling more closely with upstream by updating **perf** to recent upstream versions and enabling **debuginfod** support.
- Expands **uncore** and **core** performance counters for newer Intel platforms and adds AMD IBS load-latency filtering to improve CPU and memory analysis.
- Adds or updates drivers and device IDs for Intel EDAC, Intel QAT, and Intel/AMD accelerator and crypto devices to improve hardware coverage.
- Improves real-time analysis and tuning by extending **rtla** threshold-overflow actions, adding **cpupower** Python bindings, and updating **rteval**.
- Updates kernel debugging and crash analysis by rebasing **crash** and enhancing LUKS-aware **kdump** handling in both the kernel and **kdump** utilities.

Dynamic programming languages, web and database servers

Later versions of the following Application Streams are now available:

- **MariaDB 11.8**
- **Node.js 24**

See New features - Dynamic programming languages, web and database servers and Technology Previews - Dynamic programming languages, web and database servers for more information.

Compilers and development tools

Updated system toolchain

The following system toolchain components have been updated:

- **GCC 11.5**
- **glibc 2.39**
- **Annobin 12.98**
- **Binutils 2.35.2**

Updated performance tools and debuggers

The following performance tools and debuggers have been updated in RHEL 9.8:

- **GDB 16.3**
- **Valgrind 3.26.0**
- **SystemTap 5.4**
- **Dyninst 13.0.0**
- **elfutils 0.194**
- **libabigail 2.9**

Updated performance monitoring tools

The following performance monitoring tools have been updated in RHEL 9.8:

- **PCP 6.3.7**
- **Grafana 10.2.6**

Updated compiler toolsets

The following compiler toolsets have been updated in RHEL 9.8:

- **GCC Toolset 15**
  - **GCC 15.2**
  - **Binutils 2.44**
    Note that **Annobin** and **dwz** are not provided in GCC Toolset starting with version 15.
- **LLVM Toolset 21.1.8**
- **Rust Toolset 1.92.0**
- **Go Toolset 1.26.2**

For detailed changes, see New features - Compilers and development tools .

1.2. IN-PLACE UPGRADE

In-place upgrade from RHEL 8 to RHEL 9

The supported in-place upgrade paths currently are:

- From RHEL 8.10 to RHEL 9.6, and RHEL 9.8 on the following architectures:
  - AMD and Intel 64-bit architectures (x86-64-v2)
  - 64-bit ARM architecture (ARMv8.0-A)
  - IBM POWER 9 (little endian) and later
  - IBM Z architectures (IBM z14 or IBM LinuxONE II or later)
- From RHEL 8.10 to RHEL 9.6, and RHEL 9.8 on systems with SAP HANA

For instructions on performing an in-place upgrade, see Upgrading from RHEL 8 to RHEL 9 .

For instructions on performing an in-place upgrade on systems with SAP environments, see Upgrading SAP environments from RHEL 8 to RHEL 9.

For information regarding how Red Hat supports the in-place upgrade process, see the In-place upgrade Support Policy.

Notable enhancements and bug fixes include:

- New Ansible roles to automate the upgrade process. For more information, see In-place upgrade phases automation with the **analysis**, **remediate**, and **upgrade** Ansible roles .
- Modernization of the system storage initialization when booting to the upgrade environment.
- Enable upgrade with JBoss Enterprise Application Platform 7.4, 8.0, and 8.1.
- Correctly upgrade systems with configured LVM and multipath.
- Fix the upgrade on systems with Non-Volatile Memory Express over Fibre Channel (NVMe-FC).
- Fix broken DNF transaction execution when performing the system upgrade after the reboot leading to emergency mode.
- Fix the upgrade on systems with the **kernel-rt** package.

In-place upgrade from RHEL 7 to RHEL 9

It is not possible to perform an in-place upgrade directly from RHEL 7 to RHEL 9. However, you can perform an in-place upgrade from RHEL 7 to RHEL 8 and then perform a second in-place upgrade to RHEL 9. For more information, see In-place upgrades over multiple RHEL major versions by using Leapp.

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
- Kickstart Generator
- Red Hat Product Certificates
- Red Hat CVE Checker
- Kernel Oops Analyzer
- Red Hat Satellite Upgrade Helper
- Load Balancer Configuration Tool
- Ceph Placement Groups (PGs) per Pool Calculator
- Red Hat Out of Memory Analyzer
- Postfix Configuration Helper
- Red Hat IdM Upgrade Helper
- NetworkManager Command Generator

1.4. ADDITIONAL RESOURCES

Capabilities and limits of Red Hat Enterprise Linux 9 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 9, including licenses and application compatibility levels.

Application compatibility levels are explained in the Red Hat Enterprise Linux 9: Application Compatibility Guide document.

Major **differences between RHEL 8 and RHEL 9**, including removed functionality, are documented in Considerations in adopting RHEL 9 .

Instructions on how to perform an **in-place upgrade from RHEL 8 to RHEL 9** are provided by the document Upgrading from RHEL 8 to RHEL 9 .

Using **Red Hat Lightspeed** you can proactively identify, examine, and resolve known technical issues. Red Hat Lightspeed is included with all RHEL subscriptions. For instructions on how to install the client and register your system to the service, see the Red Hat Lightspeed documentation page.

NOTE

Public release notes include links to access the original tracking tickets, but private release notes are not viewable so do not include links.[1]

[1] Public release notes include links to access the original tracking tickets, but private release notes are not viewable so do not include links.

CHAPTER 2. ARCHITECTURES FOR RED HAT ENTERPRISE LINUX 9.8

Red Hat Enterprise Linux 9.8 is distributed with the kernel version 5.14.0-687.5.1, which provides support for the following architectures at the minimum required version (stated in parentheses):

- AMD and Intel 64-bit architectures (x86-64-v2)
- The 64-bit ARM architecture (ARMv8.0-A)
- IBM Power Systems, Little Endian (POWER9)
- 64-bit IBM Z (z14)

Make sure you purchase the appropriate subscription for each architecture. For more information, see Get Started with Red Hat Enterprise Linux - additional architectures .

CHAPTER 3. DISTRIBUTION OF CONTENT IN RHEL 9

3.1. INSTALLATION

Red Hat Enterprise Linux 9 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:

- Installation ISO: A full installation image that contains the BaseOS and AppStream repositories and allows you to complete the installation without additional repositories. On the Product Downloads page, the **Installation ISO** is referred to as **Binary DVD**.

NOTE

The Installation ISO image is in multiple GB size, and as a result, it might not fit on optical media formats. A USB key or USB hard drive is recommended when using the Installation 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 Installation ISO image. You can also register to Red Hat CDN or Satellite during the installation to use the latest BaseOS and AppStream content from Red Hat CDN or Satellite.

See the Interactively installing RHEL from installation media 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 Automatically installing RHEL document.

3.2. REPOSITORIES

Red Hat Enterprise Linux 9 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 operating system 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 more information, see the Scope of Coverage Details document.

Content in the AppStream repository includes additional user-space applications, runtime languages, and databases in support of the varied workloads and use cases.

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 9 repositories and the packages they provide, see the Package manifest.

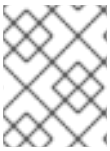
3.3. APPLICATION STREAMS

Multiple versions of user-space components are delivered as Application Streams and updated more frequently than the core operating system packages. This provides greater flexibility to customize RHEL without impacting the underlying stability of the platform or specific deployments.

Application Streams are available in the familiar RPM format, as an extension to the RPM format called modules, as Software Collections, or as Flatpaks.

Each Application Stream component has a given life cycle, either the same as RHEL 9 or shorter. For RHEL life cycle information, see Red Hat Enterprise Linux Life Cycle .

RHEL 9 improves the Application Streams experience by providing initial Application Stream versions that can be installed as RPM packages using the traditional **dnf install** command.



NOTE

Certain initial Application Streams in the RPM format have a shorter life cycle than Red Hat Enterprise Linux 9.

Some additional Application Stream versions will be distributed as modules with a shorter life cycle in future minor RHEL 9 releases. 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.

Always determine what version of an Application Stream you want to install and make sure to review the Red Hat Enterprise Linux Application Stream Lifecycle first.

Content that needs rapid updating, such as alternate compilers and container tools, is available in rolling streams that will not provide alternative versions in parallel. Rolling streams may be packaged as RPMs or modules.

For information about Application Streams available in RHEL 9 and their application compatibility level, see the Package manifest. Application compatibility levels are explained in the Red Hat Enterprise Linux 9: Application Compatibility Guide document.

3.4. PACKAGE MANAGEMENT WITH YUM/DNF

In Red Hat Enterprise Linux 9, software installation is ensured by **DNF**. Red Hat continues to support the usage of the **yum** term for consistency with previous major versions of RHEL. If you type **dnf** instead of **yum**, the command works as expected because both are aliases for compatibility.

Although RHEL 8 and RHEL 9 are based on **DNF**, they are compatible with **YUM** used in RHEL 7.

For more information, see Managing software with the DNF tool.

CHAPTER 4. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 9.8.

4.1. SECURITY

AIDE rebased to 0.19.2

The **aide** package, which provides the Advanced Intrusion Detection Environment (AIDE) utility, has been rebased to upstream version 0.19.2. This version provides important fixes and enhancements, most notably the following:

Security updates, Major library change

The **libnettle** cryptographic library replaces the previous **libmhash** cryptographic library.

Changes not compatible with earlier versions

The following options are removed and are replaced with new options:

database

Replaced with **database_in**.

summarize_changes

Replaced with **report_summarize_changes**.

grouped

Replaced with **report_grouped**.

Default configuration update

The outdated default **aide.conf** file is restructured with new attributes and rules. Review and integrate these changes.

New logging and reporting system

The previous **--verbose** and **verbose** options are removed. This version introduces more flexible **log_level** and **report_level** options and named log levels for better debugging.

New file attributes and hash sums

This version adds support for Linux capabilities and restricted rules based on file system type, implemented in the **fstype** attribute.

Improved command-line tools

This version adds the **--dry-init** command to test initial database creation without writing the file, and the **--path-check** command to test rule matching.

For more information on all detailed changes, including other bug fixes and improvements, see the installed documentation file at **/usr/share/doc/aide/NEWS**.

Jira:RHEL-83776

p11-kit-client.so separates to thep11-kit-client subpackage

The **p11-kit-client.so** module moves from the **p11-kit-server** subpackage to the new **p11-kit-client** subpackage. With the separated subpackages, you can install only the required parts and avoid redundant content on host systems or in containers.
Jira:RHEL-91952

OpenSSH provided in version 9.9

RHEL 9.8 provides OpenSSH in version 9.9, which introduces many fixes and improvements over OpenSSH 8.7, which was provided in RHEL 9.7. For the complete list of changes, see the **openssh-9.9p1/ChangeLog** file. The most important changes are as follows:

- A system for restricting forwarding and use of keys that were added to the **ssh-agent** program has been added to **ssh**, **sshd**, **ssh-add**, and **ssh-agent** programs.
- Improvements to the use of the FIDO standard:
  - The **verify-required** certificate option has been added to **ssh-keygen**.
  - Fixes to FIDO key handling reduce unnecessary PIN prompts for keys that support intrinsic user verification.
  - A check for existing matching credentials in the **ssh-keygen** program prompts the user before overwriting the credentials.
- New **EnableEscapeCommandline** option in the **ssh_config** configuration file enables the command line option in the **EscapeChar** menu for interactive sessions.
- New **ChannelTimeout** keyword specifies whether and how quickly the **sshd** daemon should close inactive channels.
- The **ssh-keygen** utility generates Ed25519 keys by default except in FIPS mode, where the default is RSA.
- The **ssh** client performs keystroke timing obfuscation by sending interactive traffic at fixed intervals, every 20 ms by default, when only a small amount of data is being sent. It also sends fake keystrokes for a random interval after the last real keystroke, defined by the **ObscureKeystrokeTiming** keyword.
- With the new **ChannelTimeout** type, **ssh** and **sshd** close all open channels if all channels lack traffic for a specified interval. This is in addition to the existing per-channel timeouts.
- The **sshd** server blocks client addresses that repeatedly fail authentication, repeatedly connect without ever completing authentication, or that crash the server.
- The **sshd** server penalizes client addresses that do not successfully complete authentication. The penalties are controlled by the new **PerSourcePenalties** keyword in **sshd_config**.
- The **sshd** server is split into a listener binary **sshd** and a per-session binary **sshd-session**. This reduces the listener binary size that does not need to support the SSH protocol. This also removes support for disabling privilege separation and disabling re-execution of **sshd**.
- In portable OpenSSH, **sshd** no longer uses **argv[0]** as the PAM service name. You can select the service name at runtime with the new **PAMServiceName** directive in the **sshd_config** file. This defaults to **sshd**.
- The **HostkeyAlgorithms** keyword allows **ssh** to disable implicit fallback from certificate host key to plain host keys.
- The components have been hardened in general and work better with the PKCS #11 standard.

Jira:RHEL-108912[1]

Valkey runs with the **redis_t** SELinux type

Before this update, Valkey processes did not use the **redis_t** SELinux type. This caused behavioral inconsistencies with Redis in RHEL 9. With this update, the SELinux policy has been enhanced to run Valkey as **redis_t**. As a result, Valkey processes align with Redis behavior, providing a consistent security context for these services in RHEL 9 environments.

Jira:RHEL-108982[1]

fapolicyd rebased to 1.4.3

The **fapolicyd** packages are rebased to upstream version 1.4.3 and provide many enhancements and bug fixes over the previous version. Most notably:

- Added the **--filter** option for the **fapolicyd-cli --file** command
- Added the **--test-filter** option for the **fapolicy-cli** command to help test filter rules
- Added the **fapolicyd-filter.conf(5)** man page
- Added the **--check-ignore_mounts** option for **fapolicyd-cli**
- Added the **--verbose** flag for the **fapolicyd-cli --check-ignore_mounts** command
- Increased the default value of the **db_max_size** parameter
- Added support for the **db_max_size = auto** option, which enables automatic database size management by the **fapolicyd** daemon
- Increased the default subject cache size
- Moved the **fapolicyd-rpm-loader** program to the **/bin** directory
- Optimized performance of the **fapolicyd** framework

Jira:RHEL-118363

CanonicalMatchUser in **sshd_config** prevents privilege escalation for capitalized AD usernames

This update of the **openssh** packages introduces the **CanonicalMatchUser** directive for the **sshd_config** configuration file. With the new directive, you can configure **Match User** blocks so that **sshd** first attempts to obtain the username from a password database instead of using an alias. As a result, Active Directory (AD) users can no longer bypass chroot restrictions when using capital letters in their usernames, which might lead to privilege escalation.

Jira:RHEL-118372[1]

GnuTLS rebased to 3.8.10

The **gnutls** package is rebased to upstream version 3.8.10. This update introduces several enhancements and bug fixes. Most notably:

Post-quantum cryptography (PQC) support

- ML-KEM and ML-DSA integration: GnuTLS supports ML-KEM hybrid key exchange algorithms and ML-DSA-44, ML-DSA-65, and ML-DSA-87 signature algorithms for TLS communications. To enable these algorithms, use the PQ system-wide cryptographic subpolicy.

- Expanded private key formats: This update adds support for all variants of ML-DSA private key formats defined in the **draft-ietf-lamps-dilithium-certificates-12** document to provide compatibility with evolving international standards.

TLS and cryptographic enhancements

- Improved OCSP verification: Before this update, when a single Online Certificate Status Protocol (OCSP) response contained multiple records, GnuTLS considered only the first record, which could cause verification failures. With this update, GnuTLS checks all records until it finds a match for the server certificate.
- Certificate compression: This update adds support for TLS certificate compression as defined in RFC 8879 to reduce handshake latency and bandwidth. Note that this feature is disabled by default.
- RSA-OAEP support: GnuTLS supports the Optimal Asymmetric Encryption Padding (RSA-OAEP) scheme as defined in RFC 8017, which provides a more secure alternative to traditional RSA padding.
- SHAKE hashing: This update adds support for the Secure Hash Algorithm Keccak (SHAKE) hashing algorithm and includes a new API to incrementally calculate SHAKE hashes of any length across multiple calls.
- Enhanced PKCS #12 security: GnuTLS can export PKCS #12 files by using Password-Based Message Authentication Code 1 (PBMAC1) as defined in RFC 9579. For interoperability with systems running in FIPS mode, use PBMAC1 explicitly.

Technology Preview

- PKCS #11 back end override: As a Technology Preview, you can use PKCS #11 modules to override the default cryptographic back end. You can test this feature by adding a **[provider]** section to the system-wide configuration to configure the module path and PIN.

Jira:RHEL-125971

crypto-policies supports hybrid ML-KEM and pure ML-DSA in GnuTLS

This update of the system-wide cryptographic policies adds support for hybrid ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) and pure ML-DSA (Module-Lattice-Based Digital Signature) post-quantum (PQ) algorithms in GnuTLS. As a result, you can use GnuTLS in RHEL 9.8 to negotiate TLS connections that use hybrid ML-KEM or pure ML-DSA as long as the other side supports them, and the PQ system-wide cryptographic subpolicy is applied.
Jira:RHEL-127829

/dev/papr-* devices have more specific SELinux labels

With this update of the **selinux-policy** packages, the following devices have more specific SELinux labels:

- **/dev/papr-indices**
- **/dev/papr-physical-attestation**
- **/dev/papr-platform-dump**

This aligns with the addition of new character device interfaces to the kernel, providing user-space application binary interface (ABI) access to the Power Architecture Platform Reference (PAPR) system parameters, in addition to the existing kernel-internal API.

As a result, the SELinux policy assigns distinct labels to these devices so that different permissions can apply to various services accessing them.

Jira:RHEL-129879

p11-kit rebased to 0.26.1

The **p11-kit** packages have been upgraded to upstream version 0.26.1. The new version provides many enhancements and bug fixes, most notably:

- PKCS #11 headers are updated to version 3.2, which supports post-quantum cryptography (PQC) definitions.
- The trust module now correctly looks up the last DN (Distinguished Name) in the **RDNSequence** attribute as defined in the RFC 4514 document.
- You can specify the server address with the new module configuration option for the Remote Procedure Call (RPC) protocol.
- Handling of an empty array attribute in RPC is fixed.
- Dependency on the **libsystemd** library for server socket activation is removed.

Jira:RHEL-139075[1]

New package: **clevis-pin-trustee**

The **clevis-pin-trustee** package provides a new Clevis pin **trustee** that enables automated encryption and decryption of LUKS-encrypted volumes by using remote attestation through the Trustee Key Broker Service (KBS). The **trustee** pin integrates with the standard Clevis framework through the **clevis-encrypt-trustee** and **clevis-decrypt-trustee** commands, and it includes a Dracut module **60clevis-pin-trustee** for automated root volume unlocking during early boot.
In scenarios such as confidential clusters for OpenShift and confidential virtual machines with OpenShift Virtualization, the Trustee server acts as the policy enforcement point, releasing the disk encryption key only when the requesting platform's attestation evidence validates against a set of reference values.

As a result, you can bind LUKS-encrypted volumes to one or more Trustee servers by using a **clevis luks bind -d *<device>* trustee '*<config>*'** command. You can also combine the **trustee** pin with other Clevis pins, such as **tang** and **tpm2**, for multi-factor or multi-policy unlock configurations.

Jira:RHEL-139790[1]

crypto-policies enables **mlkem768x25519-sha256** for OpenSSH

This update of the system-wide cryptographic policies adds support for the ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) post-quantum (PQ) key exchange **mlkem768x25519-sha256** algorithm for OpenSSH. This aligns with support for ML-KEM in OpenSSH, providing a quantum-resistant key exchange method for your SSH sessions when you use the **PQ** system-wide cryptographic policy.
Jira:RHEL-151499

OpenSCAP rebased to 1.4.3

The OpenSCAP packages have been rebased to upstream version 1.4.3. This version provides bug fixes and various enhancements. For additional information, see the OpenSCAP release notes.
Jira:RHEL-133976

SCAP Security Guide rebased to 0.1.80

For additional information, see the SCAP Security Guide release notes .
Jira:RHEL-136121

4.2. SOFTWARE MANAGEMENT

librepo rebased to 1.19.0

The **librepo** packages are rebased to upstream version 1.19.0. This version provides the following important fixes and enhancements:

- Fixed creating a directory for a **gpgme** socket when verifying a signature from a file descriptor.
- Added functions for importing keys from a file descriptor and memory.
- Added function for listing end exporting keys.
- Fixed including header files not to conflict with application's local header files.
- Removed the **/usr/include/librepo/downloader_internal.h** header file that should have been private.
- Optimized code when extended attributes are not supported by a file system.
- Improved performance when downloading multiple packages.
- Added the **LRO_USERNAME** and **LRO_PASSWORD** options to set a user name and a password separately. Use these options if you have a colon (**:**) in your user name.
- Removed the private **ensure_socket_dir_exists** ELF symbol.
- Fixed a SELinux warning if SELinux runs in a container where **/sys/fs/selinux** is not mounted.
- Fixed caching package checksums on file systems that do not support extended attribute names with uppercase characters.

Jira:RHEL-62033

4.3. SHELLS AND COMMAND-LINE TOOLS

Security and TLS improvements in**openwsman** 2.8.1

The **openwsman** package has been updated to version 2.8.1 with the following improvements:

- Improved TLS 1.3 support.
- Improved compatibility with OpenSSL 3.0.

- Improved SSL/TLS error reporting.
- Improved security by clearing passwords from memory after use and enhancing buffer safety.

Jira:RHEL-97643[1]

openCryptoki rebased to 3.26.0

The **openCryptoki** packages are updated to upstream version 3.26.0. This version provides important fixes and enhancements, most notably the following:

Post-quantum cryptography (PQC) support

ML-DSA and ML-KEM integration

Adds support for the IBM-specific Module-Lattice-Based Digital Signature Algorithm (ML-DSA) and Module-Lattice Key Encapsulation Mechanism (ML-KEM).

- EP11 token: Requires EP11 host library version 4.2 or later, and a CEX8P crypto card with firmware version 9.6 or later (on IBM z17), or version 8.39 or later (on IBM z16).
- CCA token: Requires CCA version 8.4 or later.
- Soft token: Requires OpenSSL version 3.5 or later, or a configured OQS-provider.
- The **p11sak** tool supports the IBM-specific ML-DSA and ML-KEM key types.

BLS12-381 curve support

The EP11 token supports the pairing-friendly BLS12-381 elliptic curve (EC) for signing, verification, and public key aggregation. The **p11sak** tool also supports generating BLS12-381 EC keys.

Cryptographic enhancements

Expanded RSA key sizes

- The Soft token and the **p11sak** utility support RSA keys up to 16 Kb.
- The CCA token supports RSA keys up to 8 Kb. This requires CCA version 8.4, or version 7.6 or later.

New key derivation and Hash-based Message Authentication Code (HMAC) mechanisms

- The Soft and ICA tokens support SHA512/224 and SHA512/256 key derivation mechanisms.
- The Soft, ICA, CCA, and EP11 tokens support SHA-HMAC key types and generation mechanisms.
- The **p11sak** tool supports SHA-HMAC key types and generation.

PKCS #11 version 3.0 compliance

Adds support for canceling operations by using a NULL mechanism pointer at the **C_XxxInit()** calls, which provides an alternative to the **C_SessionCancel()** calls.

Management and utility improvements

The p11sak tool enhancements

The **p11sak** utility supports key wrapping and unwrapping commands to securely export and import private and secret keys. It also provides export of non-sensitive private keys to password-protected PEM files.

HSM-protected TLS keys

The **p11kmip** tool supports using a Hardware Security Module (HSM)-protected TLS client key through a PKCS#11 provider, which increases the security of communication with Key Management Interoperability Protocol (KMIP) servers.

Jira:RHEL-100059[1]

Updated snmpcmd man page documents supported privProtocol for SNMPv3 messages

With this update, the **snmpcmd** man page documents the supported **privProtocol** for SNMPv3 messages. As a result, administrators have access to the necessary reference details to create SNMPv3 users with specific authentication and privacy protocols.

Jira:RHEL-101614[1]

Documentation updated for net-snmp-create-v3-user supported encryption algorithms

The **--help** output and manual page for the **net-snmp-create-v3-user** script have been updated to include the complete list of supported authentication and encryption algorithms. This update improves clarity when configuring authentication and encryption passwords.

Jira:RHEL-103557[1]

tog-pegasus supports post-quantum cryptography

This update enables post-quantum key exchange by default in the **tog-pegasus** packages if the peer supports it. Two new files, **/etc/pki/Pegasus/server-fallback.pem** and **/etc/pki/Pegasus/file-fallback.pem**, for **tog-pegasus** servers provide a mechanism to support a classic certificate chain and an **ML-DSA** certificate at the same time. . As a result, you can use these new files to enable the loading of a classic certificate and key when you need to use an **ML-DSA** certificate and a classic certificate chain simultaneously.

Jira:RHEL-127514[1]

The sblim-sfcb package supports post-quantum cryptography

This update enables post-quantum key exchange by default in the **sblim-sfcb** package if the peer supports it. This update also introduces two new configuration options, **sslKeyFallbackFilePath** and **sslCertificateFallbackFilePath**, in the **sblim-sfcb** server configuration file.

Before this update, there was no mechanism to support a classic certificate chain and an **ML-DSA** certificate at the same time. As a result, you can use these new options to enable the loading of a classic certificate and key when you need to use an **ML-DSA** certificate and a classic certificate chain simultaneously.

Jira:RHEL-127515[1]

Support added for post-quantum cryptography in openwsman

Previously, the package did not use post-quantum key exchange by default if the peer supports it. Also, there was no mechanism to support a classic certificate chain and the ML-DSA certificate at the same time.
With this update, two new configuration options **ssl_cert_fallback_file** and **ssl_key_fallback_file** are introduced in **openwsman** server configuration file. These options are disabled by default, but can be used to enable loading of classic certificate and key when there is a requirement to use an **ML-DSA** certificate and classic certificate chain at the same time.

As a result, the outdated SSL initialization which prevents post-quantum key exchange by default was removed from the **openwsman** server.

Jira:RHEL-127516[1]

Red Hat build of OpenJDK 25 available in RHEL 9

Red Hat build of OpenJDK 25 and the **maven-openjdk25** subpackages are available in Red Hat Enterprise Linux 9. This version provides the latest long-term support (LTS) release of the Open Java Development Kit (OpenJDK). As a result, you can leverage the latest Java features and performance improvements for your applications.

Jira:RHEL-127952[1]

4.4. INFRASTRUCTURE SERVICES

chrony rebased to version 4.8

The **chrony** packages are rebased to upstream version 4.8, which includes the following notable enhancements and bug fixes:

- The **maxunreach** option is added to limit the selection of unreachable sources.
- The **-u** option is added to the **chronyc** command to drop root privileges.
- The **opencommands** directive is added to select remote monitoring commands.
- The **waitsynced** and **waitunsynced** options are added to the **local** directive.
- The RTC **refclock** driver is added.
- You can specify the PHC **refclock** driver with a network interface name.
- Detection of clock interference from other processes is added.
- The **chronyc** socket is hidden to mitigate unsafe permissions changes.
- The **refclock** samples are validated for reachability updates.

Jira:RHEL-112598

valgrind rebased to upstream version 3.26.0

The upgrade to the upstream version 3.26.0 provides the following notable enhancements:

- valgrind recognizes the following Linux kernel system calls: **cachestat**, **futex_waitv**, **listmount**, **mount_setattr**, **mseal**, **quotactl_fd**, **remap_file_pages**, **setdomainname**, **statmount**, **swapoff**, **swapon**, **sysfs**, and **ustat**.
- A new option, **--modify-fds=yes**, has been added. This option behaves like **--modify-fds=high**, returning the highest available file descriptor first. However, if file descriptors **0**, **1**, or **2** (**stdin**, **stdout**, **stderr**) are available, they are returned before higher-numbered file descriptors.
- When **--xml=yes** is used, log output protocol version 6 is always enabled. Protocol version 6 includes error summaries in the XML output.
- A new value, **bad**, has been added for the **--track-fds** option. When **--track-fds=bad** is specified, valgrind reports only invalid file descriptor usage, such as double close or use of an invalid file descriptor. It does not report unclosed file descriptors at program exit.
- DWARF inlined subroutine handling has been rewritten to work across compilation units. This update removes backtraces that previously displayed **UnknownInlinedFun** in warnings or error messages.
- A new utility script, **vgstack**, has been added. Use **vgstack <PID>** to attach to a running valgrind process and display backtraces of the target executable. The script provides the following options:
  - **-h** - Displays minimal help.
  - **-v** - Displays version information.

Jira:RHEL-120965

SystemTap is rebased to version 5.4

SystemTap is rebased to version 5.4. The notable changes in this update include:

- **Implicit Header Discovery**: The **@cast()** operator now automatically searches the Linux Userspace API (UAPI) **<vmlinux.h>** header for type declarations. This reduces the requirement for manual header file inclusion in many common tracing scenarios.
- **Enhanced Type Validation**: Improvements to type checking and autocast processing provide more rigorous analysis during the translation phase, identifying potential type mismatches earlier in the development cycle.

Jira:RHEL-121662

elfutils rebased to 0.194

The upgrade to the upstream version 0.194 provides the following notable enhancements:

- **debuginfod-find**: Fixed a caching issue that prevented re-downloading files after a user-cancelled download.
- **elfclassify**: Added the following new options:
  - **--has-debug-sections**
  - **--any-ar-member**

- **elflint**: Vendor and application-specific ELF note types no longer trigger compliance errors.
- **libdwfl_stacktrace**: Added a new function, **dwflst_sample_getframes**.
- **libelf**: Added manual pages for many library functions.
- **readelf**: Improved performance by up to 13% when using the **-N** option.

Jira:RHEL-121664

sscg rebased to version 4.0.3

The **sscg** packages are rebased to upstream version 4.0.3. This version provides important fixes and enhancements, most notably the following:

- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) key generation is supported to provide post-quantum cryptography capabilities.
- Elliptic Curve Digital Signature Algorithm (ECDSA) key generation is supported.
- The command-line interface help output is reorganized into logical groups.

Jira:RHEL-124447

Apache's **ErrorLogFormat** supports millisecond timestamps

With this update, Apache's **ErrorLogFormat** supports millisecond timestamps. Millisecond-level timestamps in error logs improve log filtering, troubleshooting efficiency, and cross-system traceability. You can configure this, for example, by using the **%{m}t** format specifier. As a result, you can correlate and filter logs across systems with millisecond precision.

Jira:RHEL-129692[1]

4.5. NETWORKING

iproute rebased to version 6.17.0

The **iproute** package has been updated to upstream version 6.17.0.
Notable enhancements:

- The **tc** utility supports 64-bit hardware packet counters.
- The **ip** utility displays the **netns-immutable** property.
- The **ip** utility supports the **IFLA_VXLAN_MC_ROUTE** configuration attribute.
- The **ip neigh** command supports the **extern_valid** flag.
- The **ip rule** command supports port and Differentiated Services Code Point (DSCP) mask.
- The **ip stats** command supports bridge VLAN statistics.
- The **bridge fdb** command supports the forward database (FDB) activity notification control.
- The **bridge mdb** command supports the offload failed flag.

- The color output handling was improved.

Jira:RHEL-98272

HSR RedBox support for non-HSR device integration

With this enhancement, you can configure High-availability Seamless Redundancy (HSR) interfaces as a Redundancy Box (RedBox). This mode provides a communication path between standard Ethernet devices and an HSR ring. By designating an interlink port on the HSR interface, external devices connected to the interlink port reside within the same layer-2 domain as the ring participants. The interlink port operates in High-availability Seamless Redundancy to Singly Attached Node (HSR-SAN) mode, which handles the insertion and removal of HSR tags as traffic passes between the redundant network and the connected devices.

Jira:RHEL-100940[1]

The PRP and HSR protocols are fully supported

The **hsr** kernel module provides the following protocols:

- Parallel Redundancy Protocol (PRP)
- High-availability Seamless Redundancy (HSR)
  The IEC 62439-3 standard defines these protocols, and you can use this feature to configure redundancy with zero-time recovery in Ethernet networks.

  The protocols were previously available as a Technology Preview. Starting with RHEL 9.8, Red Hat fully supports this module.

Jira:RHEL-100941[1]

Nmstate can set alternative names on network interfaces

With this enhancement, you can use the Nmstate API to set alternative names on network interfaces to simplify configuration management and support processes. For example, to assign **LAN** as an alternative name to **enp1s0** and remove the name **internal-LAN**, use:

```
interfaces:
  - name: enp1s0
    alt-names:
      - name: LAN
      - name: internal-LAN
        state: absent
```

Jira:RHEL-110781[1]

NetworkManager and Nmstate support configuring IPv4 forwarding per interface

With this enhancement, NetworkManager can enable and disable IPv4 forwarding per network interface. This enables granular control directly in NetworkManager connection profiles, and updating **sysctl** kernel settings is no longer required. If you enable the **ipv4.forwarding** parameter in a profile, the corresponding interface acts as a router and forwards IPv4 packets. With the default value **auto**, NetworkManager enables IPv4 forwarding if any shared connection is active and, in other cases, it uses the kernel default value.
This feature is also available in Nmstate.

Jira:RHEL-110793[1]

The kernel supports setting a lower TCP maximum retransmission timeout value

With this enhancement, you can set a lower maximum TCP retransmission timeout value than the default **120000** ms to reduce network latency. Note that changing this setting can require tuning other kernel settings as well.
You can configure this limit either through the **tcp_rto_max_ms** kernel **sysctl** setting or the **TCP_RTO_MAX_MS** socket option. If you set both, the socket option has a higher priority.

Jira:RHEL-115191[1]

Setting the DHCP client ID is now possible through a kernel argument

With this update, users can now set the DHCP client ID as a kernel argument. Certain DHCP servers require this ID to identify a client correctly. By setting the **rd.net.dhcp.client-id** kernel argument, the client ID is already available during early boot operations.

Jira:RHEL-122166[1]

NetworkManager supports specifying an HSR interlink interface

With this update, RHEL users can configure an interlink interface for High-availability Seamless Redundancy (HSR) connections. Users can now use the **hsr.interlink** property to specify the interlink interface name. As a result, you can configure RHEL as a Redundancy Box (RedBox).

Jira:RHEL-122175[1]

The NetworkManager Libreswan plugin supports using a single tunnel for multiple subnets

This update enhances the NetworkManager Libreswan client plugin to configure multiple subnets in IPsec policies. This corresponds to the use of multiple subnets in the **leftsubnets** and **rightsubnets** parameters in the Libreswan configuration. As a result, users can connect to multiple subnets by using a single IPsec tunnel.

Jira:RHEL-124258[1]

FRRouting 10 package introduced in RHEL 9 AppStream repository

A new package, **frr10**, is available in the RHEL 9 AppStream repository. This package provides FRRouting (FRR) version 10 alongside the existing **frr** version 8 package. You can now access newer routing features without replacing the earlier version. By introducing **frr10** as a separate package, this update enables flexible adoption and testing of the latest FRR capabilities while maintaining compatibility with existing deployments.
Jira:RHEL-125957

RHEL can now generate unique interface names for onboard E8xx devices

On certain hardware platforms with onboard Intel E8xx network controllers, the BIOS lists all ports of the network controllers as the same device because they have the same **Type Instance** value in the desktop management interface (DMI) tables. Consequently, the **udev** service fails to rename the interfaces when RHEL boots. On these platforms, the **phys_port_name sysfs** attribute is the only attribute to distinguish the ports from each other.
With this enhancement, the **ice** and **i40e** drivers can make the **phys_port_name sysfs** attribute available to **udev**. By default, this behavior is disabled on RHEL 9 to not break existing

configurations. To enable the feature, add **ice.rh_phys_port_name=1 i40e.rh_phys_port_name=1** to the kernel command line. As a result, the drivers make the **phys_port_name** attribute available, and **udev** correctly renames the interfaces. The interfaces have the **np_<number_>** suffix.

Jira:RHEL-126034[1]

VLAN segmentation support for HSR and PRP interfaces

With this enhancement, you can create VLAN interfaces on top of High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) interfaces to enable network traffic segmentation. When configured, the kernel adds a VLAN tag to all packets transmitted through the VLAN interface. This provides greater control over traffic isolation. Note that supervision frames remain unaffected by this configuration and are always transmitted without a VLAN tag.

Jira:RHEL-130476[1]

The dpll utility can manage and monitor DPLL devices

With this update, the **iproute** package includes the **dpll** utility which you can use to manage and monitor digital phase-locked loop (DPLL) devices. The utility uses **libmnl** to communicate with the kernel through the **netlink** interface, providing a configuration tool for DPLL devices and pins.

Jira:RHEL-131661

Unbound rebased to version 1.24.2

The Unbound packages have been rebased to version 1.24.2. This update provides several enhancements and a security fix:

- Resolved a possible domain hijacking attack (CVE-2025-11411).
- Added the **unbound-control cache_lookup <domains>** command to query the cache for specific domains.
- Added **zone status** support for Unbound authoritative zones (**auth-zones**).
- Added **resolver.arpa** and **service.arpa** to the default list of locally served zones.
- Added configuration options for DNS Error Reporting (RFC 9567) and support for the **RESINFO** resource record (RR) type.

Jira:RHEL-132717[1]

The K1 power state flag can be disabled one1000e NICs

The K1 state reduces power consumption on ICH-family network interface controllers (NIC) during idle periods. However, on Intel Meteor Lake and later platforms, enabling K1 state on NICs that use the **e1000e** driver can cause packet loss due to firmware misconfiguration, interoperability with certain link partners, and other conditions.
Default:

- The K1 state is disabled on Intel Meteor Lake and later platforms.
- The K1 state is enabled on platforms earlier than Intel Meteor Lake.
  If you experience problems related to the K1 power state, disable K1 for the affected device:

1. Display the current status:

```
# ethtool --show-priv-flags <device>
...
disable-k1: off
```

2. Disable the K1 state:

```
# ethtool --set-priv-flags <device> disable-k1 on
```

Jira:RHEL-134986[1]

The FOU and GUE protocols added to the kernel

This update adds the **fou** and **fou6** modules to the **kernel-modules-extra** package. With these modules, you can configure connections that use the following protocols:

- Foo-over-UDP (FOU), which encapsulates IP protocols directly within UDP packages, without adding extra headers. For example, you can use this protocol for tunneling protocols, such as Generic Routing Encapsulation (GRE) or IP-in-IP (IPIP).
- Generic UDP Encapsulation (GUE), which adds a small header inside the UDP payload to carry metadata, such as the inner protocol. With GUE, you can use multiple protocols on the same UDP port, which makes GUE more flexible than FOU.
  Red Hat does not support the **fou** and **fou6** kernel modules.

Jira:RHEL-138741[1]

Qualcomm wireless cards work correctly if passed through to a VM

Due to missing upstream support for passing Qualcomm wireless cards to VMs by using the PCI pass through feature, these cards do not work correctly in VMs. With this update, the **ath11k** and **ath12k** drivers use certain kernel parameters to work around the problem. As a result, Qualcomm wireless cards that use these drivers work if you pass the devices to VMs. Note that the solution is only an unsupported workaround.

Jira:RHEL-141399[1]

Nmstate can configure Libreswan and use its default values

By default, the NMstate API uses NetworkManager to send configurations to Libreswan service. In this case, NetworkManager defines default values, which are different from Libreswan's defaults. With this enhancement, you can set **nm-auto-defaults: false** in the YAML file and Nmstate does not inject any extra settings. In this case, Libreswan uses this configuration and also its own default values.
For backward compatibility, the default value of **nm-auto-defaults** is **true**.

Jira:RHEL-141605[1]

4.6. KERNEL

Red Hat Enterprise Linux 9.8 is distributed with the kernel version 5.14.0-687.5.1.

BPF trampoline support on IBM PowerPC (ppc64le)

Before this update, BPF trampoline and associated functionality, including BPF **STRUCT_OPS** features such as **sched_ext**, were not available on the IBM PowerPC (**ppc64le**) architecture in Red Hat Enterprise Linux 9.
With this update, Red Hat Enterprise Linux 9.8 running on **ppc64le** can use BPF trampoline and BPF **STRUCT_OPS**-based features, such as **sched_ext**, for advanced tracing and scheduling use cases.

Jira:RHEL-14156[1]

PerfMon support added for Clearwater Forest on CentOS Stream kernel

With this update, PerfMon support is added for Clearwater Forest, a hardware or software platform, on the CentOS Stream kernel. This enhancement enables performance monitoring for the Clearwater Forest platform, improving overall system efficiency and stability.

Jira:RHEL-45067[1]

EDAC driver adds Intel Clearwater Forest server support

The EDAC driver is updated to add platform support for Intel Clearwater Forest (CWF) servers, enhancing RAS capabilities for this hardware. This change improves error detection and correction functionality specific to the Intel platform.

Jira:RHEL-45085[1]

Uncore events counters support enabled on the Panther Lake platform

With this update, you can use uncore events counters on the Panther Lake platform to monitor system performance.

Jira:RHEL-47456[1]

Full perf support for Intel Core Ultra Series 2 and 3 processors

The **perf** tool now provides full support for Intel Core Ultra Series 2 and Intel Core Ultra Series 3 processors. This update enables the complete range of **perf** functionality, including performance counters and C-state events. As a result, you can perform comprehensive hardware profiling, power-management analysis, and performance tuning on these Intel platforms.

Jira:RHEL-74193[1]

Intel QAT GEN6 device driver support

The Intel QAT crypto device driver is updated to support QAT GEN6 devices through the new **qat_6xxx** driver. GEN6 devices enable concurrent use of symmetric encryption, asymmetric encryption, and data compression. This was not available in earlier generations.

Jira:RHEL-94929[1]

tpm2-tools rebased for TPM 2.0 improvements

The **tpm2-tools** package is updated to ensure compatibility with modern TPM 2.0 hardware and improve security tooling support. This update enables enhanced TPM-based operations and aligns with upstream security and feature developments.

Jira:RHEL-94933[1]

Device IDs are added for the In-memory Analytics Accelerator (IAA) on the Wildcat Lake platform

With this update, the IAA is now moved from a Technology Preview to the supported state and the device IDs are added for In-memory Analytics Accelerator (IAA). As a result, devices on the Wildcat Lake platform are now supported.

Jira:RHEL-95629[1]

Perfmon drivers now support Wildcat Lake CPU platform

With this update, Perfmon drivers now support the Wildcat Lake CPU platform, enhancing performance monitoring on compatible hardware.

Jira:RHEL-95671[1]

Uncore events counter support for Intel Wildcat Lake platform

With this update, you can use uncore events counter for the Intel Wildcat Lake platform to monitor system performance. As a result, you can analyze performance on Intel-based systems.

Jira:RHEL-95673[1]

View CVEs patched by live kernel updates

kpatch reports which kernel CVEs are patched by live patches for the currently running base kernel. With this update, administrators can verify that specific CVEs are remediated, even if the on-disk kernel version appears vulnerable.
By listing CVEs that are patched only by **kpatch**, this enhancement improves security reporting and supports compliance workflows and external scanners that must account for live-patched vulnerabilities.

Jira:RHEL-103845[1]

LUKS volume keyfor secure **vmcore** data saving on RHEL systems

With this update, you can pass the LUKS volume key to the **kdump** kernel, to save **vmcore** data to a LUKS-encrypted disk volume. This enhancement secures **vmcore** data on RHEL systems, as sensitive data remains protected in the event of system crashes. To activate this optional feature, you must use the **kdumpctl setup-crypttab** command. This update is available for the x86_64 architecture in RHEL 9.8.

Jira:RHEL-104939[1]

The **perf** tool now supports AMD Turin LdLat filtering for IBS on RHEL

With this update, the Perf tool now supports Load Latency (LdLat) filtering for 5th Generation AMD EPYC processors (also known as Turin). This enhances Instruction-Based Sampling (IBS) capabilities of **perf**. This improvement aims to provide more accurate and efficient performance analysis on AMD systems.

Jira:RHEL-106898[1]

Updating **kernel** CCP crypto driver support for Venice PCI device

This update adds support for the AMD Venice CCP crypto device with PCI device ID 0x17D8 (PCIID 1002:17D8) in the kernel CCP driver. With this change, systems equipped with Venice CCP hardware can use the device's enhanced cryptographic offload capabilities.

Jira:RHEL-106910[1]

Userspace action triggers for rtla

With this update, the rtla tool now supports triggering userspace actions either when a latency threshold is reached or when tracing concludes. This allows you to execute diagnostic commands immediately or extract trace data before the instance is removed, regardless of whether a threshold violation occurred.

Jira:RHEL-113482[1]

crash rebased to 9.0.1

The **crash** package, which provides a kernel analysis utility for live systems and various types of dump files, is rebased to upstream version 9.0.1. This version provides a number of fixes and enhancements, most notably the following:

- Internal **gdb** is updated to version 16.2.
- Added **gdb multi-stack** unwind support on 64-bit architectures (x86-64-v3), aarch64, and ppc64.
- Added Rust support.

Jira:RHEL-114658

You can select **cyclictest** or **timerlat** as the measurement modules in **rteval**

With this update, you can select the measurement module for the **rteval** utility. This overrides the default setting in the **rteval.conf** file. This new feature, 'measurement-module', provides greater flexibility and control over performance testing, which enhances the precision and customization.

Jira:RHEL-114928[1]

Advanced performance analysis enabled with **perf** utility and **debuginfod** client support

With this update, advanced performance analysis is enabled using the **perf** utility with **debuginfod** client support in RHEL-9. This enhancement enables debugging and probing performance issues. The feature introduces new runtime dependencies and is currently limited to probing.

Jira:RHEL-124984[1]

4.7. FILE SYSTEMS AND STORAGE

cryptsetup rebased to version 2.8.0

The **cryptsetup** package has been upgraded to version 2.8.0. This update provides the following feature enhancements:

- Added support for inline mode on NVMe drives, eliminating double writes caused by journaling in the **dm-integrity** target. This improves performance for both **cryptsetup** encryption and decryption when using authenticated encryption modes as well as for **integritysetup** in standalone integrity device protection.
- Extended the **cryptsetup reencrypt** command to support LUKS2 tokens, enabling reencryption of existing LUKS2 devices, including token-bound devices.
- Optimized LUKS2 metadata writes, improving reencryption for configurations with metadata larger than 12 KiB, particularly for configurations sized in megabytes.

Jira:RHEL-100089[1]

io_uring interface added for asynchronous I/O

The **io_uring** interface supports asynchronous I/O operations. With this update, applications use this interface to submit multiple I/O requests without blocking the calling process. **io_uring** uses shared ring buffers between user space and kernel space to reduce system call overhead and avoid buffer copying. This interface is more efficient and supports more asynchronous system calls than Linux AIO.

Jira:RHEL-120699[1]

snapm rebased to 0.7.0

The **snapm** package has been rebased to upstream version 0.7.0. This version provides important fixes and enhancements, most notably the following:

- The new Mount Manager mounts and unmounts entire snapshots. You can run commands or interactive shells inside mounted snapshot sets by using the **snapset {mount, umount, exec, shell}** subcommands.
- The Difference Engine was added to compare snapshot sets or to compare against the running system. You can specify output formats, such as **paths**, **full**, **short**, **json**, **diff**, **summary**, and **tree**.
- The performance of the Stratis plugin was improved. With this update, the plugin queries the D-Bus every 5 seconds and caches the results internally. This improvement significantly reduces the time to discover Stratis snapshots.

Jira:RHEL-137377[1]

Multipath automatically removes unmapped LUNs

Before this update, multipath devices remained in the system if you did not remove SCSI devices before disconnecting a LUN. This sometimes resulted in queued I/O or incorrect writes if the LUN was repurposed.
With this update, the **purge_disconnected** option is available in the **defaults**, **devices**, and **multipaths** sections of the **multipath.conf** file. When you set this option to **yes**, the **multipathd** daemon automatically removes disconnected SCSI devices from the system.

Jira:RHEL-141291

4.8. HIGH AVAILABILITY AND CLUSTERS

HAProxy rebased to 2.8

The HAProxy package has been rebased to the upstream Long-Term Support (LTS) version 2.8. The notable changes in this update include:

- Security updates and critical fixes for RHEL 9 after the previous 2.4 LTS release reaches its End-of-Life (EOL) date in Q2 2026.
- Numerous upstream stability, performance, and functional improvements accumulated between versions 2.4 and 2.8.

For a complete list of changes, see the HAProxy webpage.

Jira:RHEL-74039[1]

4.9. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new module stream: postgresql:18

RHEL 9.8 introduces PostgreSQL 18 as the **postgresql:18** module stream.
Notable changes:

- The new Asynchronous I/O (AIO) subsystem provides up to three times faster data reads. You can enable this subsystem by setting the **io_method** variable.
- The MD5 authentication method is deprecated and will be removed in a future major PostgreSQL release.
- By default, data page checksums are enabled in PostgreSQL 18. If you upgrade from a previous version with data page checksums disabled, you must either enable the feature before the update or disable it during the upgrade. For further details, see Upgrading from a RHEL 9 version of PostgreSQL 16 to PostgreSQL 18.
- PostgreSQL 18 supports native OAUth 2.0 single sign-on authentication.
- The database service supports Federal Information Processing Standards (FIPS) mode validation for regulated environments.
- The **pg_upgrade** utility preserves statistics during major release upgrades and significantly faster reaches full performance after an upgrade.

Jira:RHEL-90852[1]

A new module stream: mariadb:11.8

MariaDB 11.8 is available as a new module stream, **mariadb:11.8**.
Notable changes over the previously available version 10.11 include:

- By default, MariaDB 11.8 uses the **utf8mb4** character set instead of **latin1** and legacy **utf8** to ensure full Unicode support.
- Vector support was added to support machine learning. This includes the **VECTOR(N)** data type and the following functions:
  - **VEC_DISTANCE()**
  - **VEC_DISTANCE_EUCLIDEAN()**
  - **VEC_DISTANCE_COSINE()**
  - **Vec_FromText(*json_array*)**
  - **Vec_ToText(*vector_column*)**

- The **mariadb-dump** and **mariadb-import** utilities natively support parallel operations. Specify the **--dir** and **--parallel** options to dump or load multiple databases simultaneously.
- The upper limit of the **TIMESTAMP** data type was increased from **2038-01-19** to **2106-02-07** while still using 4 bytes of storage.
- The **UUID_v4()** and **UUID_v7()** functions were added.
- The JSON handling was improved. This includes new functions, such as **JSON_SCHEMA_VALID()**.
- The following system variables were added to define the maximum storage for temporary tables and other internally created temporary files:
  - **max_tmp_session_space_usage** limits the disk space used per session
  - **max_tmp_total_space_usage** limits the total disk space used by the MariaDB server instance
- The **des_encrypt** and **des_decrypt** configuration file parameters are deprecated and will be removed in a future MariaDB release.

Notable breaking differences:

- The following utilities were renamed but symbolic links were created for backward compatibility:
  - **mysql** > **mariadb**
  - **mysqldump** > **mariadb-dump**
  - **mysqladmin** > **mariadb-admin**

  If you still use the previous names of these utilities, they display deprecation warnings.
- The **innodb_defragment** configuration parameter is no longer supported. Remove it from your configuration files.

For more information about MariaDB, see Using MariaDB.

To install the **mariadb:11.8** stream, enter:

```
# dnf module install mariadb:11.8
```

If you want to upgrade from MariaDB 10.11, see Upgrading from a RHEL 9 version of MariaDB 10.11 to MariaDB 11.8.

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

Jira:RHEL-96956[1]

New ruby:4.0 runtime module stream with database connectors

The **ruby** module provides a new Ruby 4.0 runtime, including database connector support. As a result, Red Hat Enterprise Linux 9.8 users can use Ruby 4.0 alongside existing Ruby streams to develop and run Ruby applications with supported database connectivity.

Jira:RHEL-142278[1]

The **mysql:8.4** module now includes the **perl-DBD-MySQL** package

This update adds the **perl-DBD-MySQL** package to the **mysql:8.4** module. Starting with Red Hat Enterprise Linux (RHEL) 9.7, the **perl-DBD-MySQL** package is linked against **libmysqlclient** instead of **libmariadb**. To ensure compatibility, **perl-DBD-MySQL** is included within **mysql:8.4**. As a result, the **perl-DBD-MySQL** package is fully compatible with the **mysql:8.4** module, which resolves dependency conflicts and installation failures.

Jira:RHEL-144470

New Python 3.14 stack is available

Red Hat Enterprise Linux 9.8 now includes the **python3.14** stack. This new alternative stack provides Python 3.14 for developing and running applications.

Jira:RHEL-120823[1]

4.10. COMPILERS AND DEVELOPMENT TOOLS

Optimized **glibc** math routines on x86-64-v3 hardware

On x86-64 systems that support the x86-64-v3 microarchitecture level, the **glibc** math library now provides additional IFUNC-optimized implementations of selected functions. The functions **atanh**, **expm1**, **log1p**, **log2**, **sincos**, **sinh**, and **tanh** now have optimized variants that use x86-64-v3 instructions, improving execution efficiency for workloads that rely on these operations.
As a result, the execution time for workloads that perform large volumes of these mathematical computations might be reduced.

Jira:RHEL-1063

Documented **glibc** memstream behavior with **SEEK_END**

The **glibc** memstream documentation describes the implementation behavior of **open_memstream** when you use **SEEK_END** to change the file position. This clarification aligns the documentation with the new requirement to document **glibc** behavior, introduced in **POSIX.1-2024**, and helps you understand how seeking affects the current position and buffer contents.

Jira:RHEL-61087

Enhanced **gcov** function coverage summaries in **gcc**

Before this update, **gcov** function summaries only reported the number of lines executed and did not include details about branch or call coverage within the function.
With this enhancement, requesting function summaries using the **-f** option now includes data on branches taken and function calls made within the profiled function. This provides a more comprehensive view of function-level test coverage.

Jira:RHEL-105416[1]

glibc adds **GLIBC_ABI_DT_X86_64_PLT** symbol support on x86_64 systems

This enhancement adds the **GLIBC_ABI_DT_X86_64_PLT** symbol version to **glibc** on x86_64 systems, so programs that require this symbol at startup no longer fail to start and instead run as expected.

Jira:RHEL-109622[1]

Rust Toolset is rebased to version 1.92.0

In RHEL 9.8, **rust-toolset** is rebased to version 1.92.0 from version 1.88.0. This update delivers multiple improvements to debugging, systems programming features, memory safety diagnostics, and Rust workflow tooling for RHEL developers.
Notable enhancements include:

- More reliable debugging on Linux because unwind tables are now emitted by default even when compiling with **-Cpanic=abort**, which ensures that backtraces work correctly for debugging.
- Improved systems programming support with full i128 and u128 support in extern "C" functions and the ability to create raw pointers to union fields using &raw in safe Rust code.
- Enhanced safety diagnostics through the new **dangling_pointers_from_locals** lint, which warns against returning dangling raw pointers derived from local variables.
- Clearer lifetime relationships with the new **mismatched_lifetime_syntaxes** lint, which warns when lifetime elision rules hide potentially confusing relationships between input and output lifetimes.
- Workflow improvements in Cargo, including native support for workspace publishing with **cargo publish --workspace**, which automatically handles dependency ordering for multi-crate projects.
  Rust Toolset is delivered as a rolling Application Stream, and only the latest **rust-toolset** version is supported. For more information about Rust Toolset life cycle and support, see the Red Hat Enterprise Linux Application Streams Life Cycle .

Jira:RHEL-111847

The Red Hat Build of OpenJDK 25 integrates with the **crypto-policies** package for secure system property handling

With this update, the Red Hat Build of OpenJDK 25 for RHEL integrates with the RHEL **crypto-policies** package. This enhancement ensures secure system property handling and improves the security of Java applications running on RHEL by loading additional configuration files based on Red Hat system properties. This change also adds FIPS support using NSS.

Jira:RHEL-128412[1]

glibc locale for Bulgaria now uses the euro currency symbol

The **glibc** package now uses the euro currency symbol for the **bg_BG** locale, reflecting Bulgaria's adoption of the euro as of 2026-01-01.
As a result, applications using the **bg_BG** locale display currency values with the updated euro symbol, ensuring consistency with the current official currency.

Jira:RHEL-137186

Rebase **llvm** toolset to version 21

The **llvm** toolset has been rebased to version 21 in RHEL 9.8. This rebase provides updated compiler and tooling features for building and optimizing applications that depend on **llvm**.
As part of this change, dependent packages in RHEL 9 have been rebuilt against **llvm** 21 to ensure compatibility with the updated toolset.

The notable changes are:

- The **nocapture** function attribute is replaced by the more expressive **captures(none)** attribute in LLVM IR, clarifying pointer capture semantics.
- Constant expression forms of several arithmetic instructions, including **mul**, are removed in favor of using regular instructions, simplifying IR and optimizations.
- Inline assembly calls no longer accept **label** operands. The **callbr** instruction must be used instead, which clarifies semantics for indirect labels.
- New **fmaximum** and **fminimum** operations are supported in the **atomicrmw** instruction, aligning atomic floating-point operations with **llvm.maximum.*** and **llvm.minimum.*** behavior.
- Multiple back ends, including AArch64, AMDGPU, RISC-V, PowerPC, and others, receive code generation improvements, new ISA extensions, and bug fixes that can result in better performance and broader hardware support.

Jira:RHEL-100898

Improved **trylock** performance in **glibc** for heavily contended multi-core workloads

With this enhancement, the **glibc** package optimizes the **trylock** implementation for workloads with high thread counts on multi-core systems, improving **trylock** throughput under heavy contention.
Jira:RHEL-141072

LD_DEBUG, **TLS**, and **TCB** tracing support in **glibc**

With this enhancement, **glibc** adds tracing support for Thread-Local Storage (**TLS**) and Thread Control Block (**TCB**) operations through the **tls** category of the **LD_DEBUG** environment variable. You can use **LD_DEBUG=tls** to track **TLS** and **TCB** related events in the dynamic linker and improve analysis of complex runtime issues.
LD_DEBUG also supports excluding specific debug categories by prefixing the category name with a dash, for example, **LD_DEBUG=all**, **-tls**, so that you can refine the debug output.

Jira:RHEL-49785[1]

Croatia locale uses the euro currency symbol in **glibc**

The **glibc** package now uses the euro currency symbol for the **hr_HR** locale in RHEL. This change aligns Croatian locale data with the country's current official currency.
As a result, applications that rely on **glibc** locale information for the **hr_HR** locale now display the up-to-date euro currency symbol instead of the former Croatian kuna.

Jira:RHEL-140105[1]

glibc adds RTLD_DI_ORIGIN_PATH to prevent buffer overflows

The **RTLD_DI_ORIGIN_PATH dlinfo** request type in **glibc** accepts the size of the destination buffer when retrieving the shared object origin path. This request type helps avoid buffer overflows when obtaining the shared object origin path.
The behavior of the existing **RTLD_DI_ORIGIN** request type remains unchanged.

Jira:RHEL-54450

4.11. IDENTITY MANAGEMENT

IdM password policies support libpwquality character credit options

Identity Management (IdM) password policies support four new options (**--dcredit**, **--ucredit**, **--lcredit**, and **--ocredit**) based on the **libpwquality** credit system. A negative value sets the minimum number of characters of that type required in a password; a positive value provides a credit toward the minimum password length. These options are mutually exclusive with **--minclasses** and offer a more granular way to enforce per-class character requirements. As a result, administrators can configure specific character type minimums in IdM password policies, for example, to satisfy DISA STIG compliance requirements.
For more information, see Additional password policy options in IdM .

Jira:RHEL-73399[1]

samba rebased to 4.23.0

The **samba** packages, which provide file and print services using the SMB protocol, have been rebased to upstream version 4.23.0. This version provides important fixes and enhancements, most notably the following:

- SMB3 UNIX Extensions are enabled by default to provide support for POSIX semantics, such as proper POSIX permissions and symlink handling, for UNIX and Linux clients.
- Experimental support for SMB3 connections over Quick UDP Internet Connections (QUIC) is introduced. Configurable through **client smb transports** and **server smb transports**, this allows for secure SMB traffic over UDP port 443, which is ideal for remote access.
- The new **smb_prometheus_endpoint** utility exports Samba server metrics in a Prometheus-compatible format to facilitate performance and status monitoring.
- The **samba-tool domain backup --no-secrets** command explicitly removes confidential attributes, such as BitLocker recovery data and KDS root keys, from backups.
  For a complete list of changes, see Samba 4.23.0 Available for Download.

Jira:RHEL-114548

ipa rebased to 4.13.0

The **ipa** packages have been rebased to upstream version 4.13.0. This version provides important fixes and enhancements, most notably the following:

- A new responsive and intuitive beta interface is available as a Technology Preview. You can experiment with it and provide feedback.

- You can use the **ipa-idrange-fix** tool to identify users and groups outside current ID ranges and propose new ranges to include them.
- The requirement for unique Certificate Authority (CA) subject names is relaxed, which enables duplicates under specific trust and nickname conditions.
- The platform supports the full 32-bit ID range space.
- This release resolves over 170 bugs and improves overall system performance and stability.

Jira:RHEL-120954

cepces rebased to 0.3.12

The **cepces** package, which provides a certificate enrollment client for Microsoft Active Directory Certificate Services (AD CS), has been rebased to upstream version 0.3.12. This version provides important fixes and enhancements, most notably the following:

- Support for GSSAPI channel bindings to bind Kerberos authentication to the TLS (HTTPS) tunnel is available. This is required for compatibility with Windows Server 2025, which enforces stricter security requirements for SOAP-based certificate enrollment web services (CEP/CES) by default.
- Authentication handshake failures when connecting to modern Windows environments that have TLS channel binding and Kerberos security policies enabled are fixed.
- Updates to the **cepces-submit** helper ensure smoother communication with the **certmonger** service during automated certificate renewal cycles.

Jira:RHEL-121787[1]

dsctl dbverify provides clearer output when a specified backend does not exist

The **dsctl dbverify** command, used to verify the integrity of a Directory Server database, provides explicit feedback depending on the database backend type. For Berkeley Database (BDB) backends, the command now returns an error when the specified backend does not exist, instead of incorrectly reporting a successful verification. For LMDB backends, the command displays a warning that the verification is always reported as successful because LMDB has built-in integrity protection. As a result, administrators can distinguish between a missing backend and a genuinely successful verification when running **dsctl dbverify**.

Jira:RHEL-123893[1]

You can configure external password reset agents in IdM

When integrating Identity Management (IdM) with a third-party application that does not support Kerberos authentication, you can define a dedicated system account for the application to securely reset user passwords. Notably, these resets do not trigger the "password change required" flag, ensuring a seamless login experience for the end user. The system account authenticates by using LDAP.
As a result, organizations can integrate their own secure password management solutions directly with IdM.

Jira:RHEL-126515[1]

Support for generating LWCA certificates and private keys on an HSM

For installations using a hardware security module (HSM), Lightweight CA (LWCA) certificates and private keys are now generated on the HSM. This provides the same hardware-level security for the private keys as the root CA private key. The LWCA private key is generated on the HSM with the HSM token name as the prefix, for example **mytoken:lwca**.

Jira:RHEL-128238[1]

pki rebased to 11.7.1

The **pki** packages have been rebased to upstream version 11.7.1. This version provides important fixes and enhancements, most notably the following:

- A race condition that caused **ipa ca-add** to fail with a "500 Internal Server Error" when adding multiple Sub-CAs in rapid succession is resolved. With this update, the CA engine correctly synchronizes authority initialization with signing certificate availability, which prevents API timeouts during high-volume operations.
- A regression where enabling the **nuxwdog** watchdog prevented the PKI service from starting is fixed. The **pki-server-nuxwdog** utility correctly interfaces with **systemd-ask-password**, enabling users to provide required credentials at startup when a password file is missing.
- An issue where the PKI server failed to issue certificates when a Sub-CA was specified is resolved. This fix ensures the certificate request pipeline correctly identifies and utilizes Sub-CA signing keys, which restores full functionality to multi-tier CA environments.

Jira:RHEL-129092

Automated services no longer reset account lockout counters

This update ensures that automated services like **crond** and **systemd-user** are prevented from unlocking accounts locked by **faillock**. Previously, these services would automatically clear the "failed login" counter when they ran, which could allow a malicious actor to keep guessing passwords without being permanently locked out. With this release, once an account is locked by a security policy, it remains locked until the timeout expires or an administrator intervenes, regardless of any background system activity.
Jira:RHEL-130875

ansible-freeipa rebased to 1.16.0

The **ansible-freeipa** packages, which provide Ansible modules and roles for Identity Management (IdM), have been rebased to upstream version 1.16.0. This version provides important fixes and enhancements, most notably the following:
The **sysaccount** module (**ipasysaccount**) creates and manages system accounts in IdM. The **role** module (**iparole**) supports system accounts as role members, so you can assign privileges such as user password management to those accounts in playbooks. You can, for example, use system accounts to integrate IdM with an external password reset management solution. For more information, refer to the **sysaccount** and **role** module READMEs.

The **ipapasskeyconfig** module is available in the **ansible-freeipa** collection. You can use this module to configure whether passkey authentication in IdM requires user verification, such as a PIN, when users authenticate with a passkey device. Additionally, the **ipauser** module supports **passkey** as a user authentication type, and the **ipaservice** and **ipahost** modules support **passkey** as an authentication indicator.

Jira:RHEL-139144

ansible-freeipa adds support for thepasskey authentication type in management modules

With this update, the **ipaconfig**, **ipahost**, **ipaservice**, and **ipauser** modules support the **passkey** authentication type for IdM resources. This enables you to manage Passkey device authentication directly through your Ansible playbooks by setting the authentication type to **passkey**.
Jira:RHEL-139257

389-ds-base rebased to 2.8.0

The **389-ds-base** package, which provides an enterprise-class LDAP server, has been rebased to upstream version 2.8.0.
Jira:RHEL-139825

You can specify an IdM server from which to update the local CA trust store

With this update, the **ipa-certupdate** tool includes a new **--force-server *<server_fqdn>*** option. Before this update, an Identity Management (IdM) client only connected to its default IdM server, specified in the **/etc/ipa/default.conf** file, when updating the local CA trust store. If this default server was down or unreachable, the **ipa-certupdate** command failed. As a result, administrators can ensure successful trust store updates and maintain service continuity, even if the primary server is unavailable.
Jira:RHEL-141446[1]

4.12. SSSD

sudo rebased to sudo-1.9.17p2

The **sudo** packages have been rebased to upstream version 1.9.17p2, which includes the following notable bug fixes and enhancements:

- The **sudoers** file supports regular expressions.
- The **log_subcmds** and **intercept** options are supported.
- The **json_compact** logging is supported.
- Privilege listing is enhanced.
- Added the **cmddenial_message sudoers** option.
- The **sudoers** LDAP schema now allows **sudoUser**, **sudoRunasUser**, and **sudoRunasGroup** to include UTF-8 characters.
- Added a new **-N** (no-update) command-line option to **sudo**.
- The following **sudoers** settings can be used to support more fine-grained I/O logging:
  - **log_stdin**
  - **log_stdout**
  - **log_stderr**

- **log_ttyin**
- **log_ttyout**

Jira:RHEL-128623

Recursive deletion for computer objects added to **adcli**

The **adcli delete-computer** command supports the **--recursive** option to delete computer objects from Active Directory, including their child objects. Previously, attempting to delete a computer object that contained child objects, such as metadata for BitLocker drive recovery, failed with a **CANT_ON_NON_LEAF** error in AD. With this update, users can cleanly delete computer objects that contain child objects using **adcli**.

Jira:RHEL-134951[1]

4.13. THE WEB CONSOLE

cockpit rebased to version 356

The **cockpit** packages have been rebased to version 356, which provides many improvements and fixes compared to version 344 in RHEL 9.7, most notably:

- Timers created by the RHEL web console are executed directly by the **/bin/sh** system shell, and you can edit them.
- The health dashboard shows a warning if the last shutdown or reboot was unclean.
- You can override the RHEL web console branding with a custom configuration in the **/etc/cockpit/branding.css** file.
- Support for the **pam_cockpit_cert** PAM module in the **/etc/pam.d/cockpit** file, which is redundant since version 248, is removed. If you still use the module in your configuration, you must remove it manually.
- The web console lists additional ports in a firewall zone, each in its own row, and you can delete them individually.
- Support for TLS is removed from the **cockpit-ws** subpackage. Instead, containers run the **cockpit-tls** program and directly connect to the **cockpit-ws** server.
- You can detach the VNC console viewer of a virtual machine into its own window.
- The web console no longer adds both SPICE and VNC graphics when creating new virtual machines, but only VNC.
- You can shut down and restart virtual machines with a single action from the web console.
- The **cockpit-podman** plug-in supports the quadlet lifecycle and shows inactive quadlets.
- You can create empty files in the web console file manager.

Jira:RHEL-112866

4.14. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Disk partition management available to the storage role

With this update, you can manage disk partitions by using the storage role, streamlining storage management. With this unified approach you can add, remove, resize, and format partitions, ensuring consistent and repeatable results.

Jira:RHEL-112772[1]

Support for bootable snapshots with **snapm**

With this update, you can create bootable snapshot sets on platforms that support **snapm**, such as RHEL 9.6 and Fedora 41 or later. You can now set a **bootable** flag when requesting snapshots and boot the system directly from a snapshot.

Jira:RHEL-120325[1]

The postgresql RHEL system role now supports PostgreSQL 18

The postgresql RHEL system role, which installs, configures, manages, and starts the PostgreSQL server, now supports PostgreSQL 18.

For more information about this system role, see Installing and configuring PostgreSQL by using the postgresql RHEL system role.

Jira:RHEL-122958[1]

The **firewall** RHEL system role supports IPv6 addresses within the **ipset_entries**

With this enhancement, you can now use IPv6 addresses within the **ipset_entries** variable when utilizing **hash:ip** or **hash:net** types in playbooks that use the **firewall** RHEL system role. You can also specify additional **<key>:<value>** pairs of options for **ipset** by using the **ipset_options** variable. pairs

Due to a limitation of the underlying **firewalld** implementation, you cannot mix IPv4, IPv6, and MAC addresses in the same **ipset_entries** list.

Jira:RHEL-123040[1]

The **ha_cluster** RHEL System Role now exports additional cluster configuration variables

Previously, the **ha_cluster** RHEL System Role provided limited visibility into the current cluster configuration.

With this update, the **ha_cluster** role has been expanded to include cluster properties and resource defaults.

As a result, the following variables are now exported, allowing for easier auditing and configuration mirroring:

- **ha_cluster_cluster_properties**
- **ha_cluster_resource_defaults**
- **ha_cluster_resource_operation_defaults**

Jira:RHEL-123041[1]

The **sshd** system role supports the **CanonicalMatchUser** option

To provide more granular control over conditional configurations, the **sshd** system role supports the **sshd_CanonicalMatchUser** variable. You can specify whether to evaluate OpenSSH **Match** blocks against a user's initial login name or their final canonical username after the server rewrites it.
As a result, you can consistently apply security policies in environments where external identity providers or local configuration rules modify usernames. This ensures that **Match** blocks accurately reflect the user's identity once the server determines the final canonical username.

Jira:RHEL-127973[1]

The **ha_cluster** RHEL System Role now exports cluster constraint variables

Previously, the **ha_cluster** RHEL System Role did not include detailed constraint information in its exported data.
With this enhancement, the **ha_cluster** role now includes variables for location, colocation, order, and ticket constraints.

As a result, the following variables are now available in the module output, facilitating better configuration management and role-based automation:

- **ha_cluster_constraints_location**
- **ha_cluster_constraints_colocation**
- **ha_cluster_constraints_order**
- **ha_cluster_constraints_ticket**

Jira:RHEL-128436[1]

Support added for the **fencing-watchdog-timeout** cluster property

Before this update, the high-availability stack primarily supported the **stonith-watchdog-timeout** property for managing watchdog-based fencing. However, future Pacemaker versions replace this property with **fencing-watchdog-timeout**.
With this update, the role handles both the legacy and new property names consistently.

As a result, the role supports future Pacemaker versions and ensures that watchdog-related cluster properties remain functional regardless of which property name you use. The role preserves both **stonith-watchdog-timeout** and **fencing-watchdog-timeout** when creating or pushing CIB configurations.

Jira:RHEL-136599[1]

The **VersionAddendum** option is available in SSH configuration

With this update, you can configure the **VersionAddendum** option in SSH settings for match blocks, host blocks, and global client configurations. This enhancement ensures compatibility with the latest OpenSSH versions and provides granular control over your SSH connections.

Jira:RHEL-138279[1]

The **sshd** system role supports **GSSAPIDelegateCredentials**

The new **GSSAPIDelegateCredentials** parameter provides Generic Security Services Application Programming Interface (GSSAPI) credential delegation in Kerberos environments and enables a seamless single sign-on experience.
As a result, you can automate the configuration of GSSAPI credential delegation to simplify network authentication.

Jira:RHEL-144496[1]

The **metrics** RHEL system role supports configuring TLS-encrypted connections

With this enhancement, you can use the **metrics** RHEL system role to configure TLS-encrypted connections to Grafana. To use this feature, specify the following variables in your playbook:

- **metrics_grafana_certificates** to use the **certificate** RHEL system role to generate new certificates on the managed nodes
- **metrics_grafana_cert** and **metrics_grafana_private_key** to specify the path to an existing certificate and private key on the managed nodes
- **metrics_grafana_cert_src** and **metrics_grafana_private_key_src** to copy an existing certificate and private key from the control node to the managed nodes

Jira:RHEL-144592[1]

SELinux supports the DCCP and SCTP protocols

With this update, you can manage SELinux port types for Datagram Congestion Control Protocol (DCCP) and Stream Control Transmission Protocol (SCTP). By configuring SELinux port labels for these protocols, you can apply granular access controls and improve system security.

Jira:RHEL-145215[1]

RHEL System Roles support for immutable systems (**ostree**)

You can use RHEL system roles to build and manage immutable operating systems. This provides a consistent management interface across different backend technologies, including **ostree**.
As a result, you can deploy and configure immutable systems using the same roles used for traditional systems, ensuring environment consistency. Note: This feature is currently not compatible with the **nbde_client** role.

Jira:RHELDOCS-21216

In-place upgrade phases automation with the **analysis**, **remediate**, and **upgrade** Ansible roles

With this release, you can use the **analysis**, **remediate**, and **upgrade** Ansible roles to automate the pre-upgrade and upgrade phases of the in-place upgrade. By using these Ansible roles, you can quickly and efficiently upgrade large numbers of systems, saving you time.
For more information, see Upgrading large deployments by using Ansible roles .

Jira:RHEL-117252

4.15. VIRTUALIZATION

Encryption for libvirt secrets

This update introduces the **virt-secrets-init-encryption** service, which encrypts **libvirt** secrets, such as keys for the virtual Trusted Platform Module (vTPM). By default, this encryption uses **systemd** credentials sealing. However, you can use the new **/etc/libvirt/secret.conf** file to specify a custom key for encrypting secrets, as well as to disable automatic encryption of secrets. As a result, critical vTPM metadata is protected from unauthorized access on the host file system. This also hardens the overall security of the virtualization environment.

Jira:RHEL-7125[1]

Faster updates for cryptographic coprocessors on IBM Z

After using the **virsh nodedev-update** command to update a cryptograpic coprocessor (**vfio-ap**) device on an IBM Z host, the new configuration now takes effect significantly faster.

Jira:RHEL-73001[1]

CPI for virtual machines on IBM Z

Virtual machines (VMs) on RHEL 9 hosts that use IBM Z hardware can now use the control program identification (CPI) feature. By using CPI, you can obtain system information about VMs without accessing them. For more information about CPI, see IBM documentation.
Note that on VMs that use IBM Secure Execution, CPI is disabled by default to ensure confidentiality, and must be enabled manually. For instructions, see Setting up IBM Secure Execution on IBM Z.

Jira:RHEL-73009[1]

Live migration can switch from **multifd** precopy to postcopy without restarting

With this update, you can enable both **multifd** (multiple file descriptor) precopy and postcopy virtual machine live migration strategies. **multifd** uses multiple parallel TCP channels during the precopy phase to maximize network bandwidth usage and reduce migration time. As a result, you can configure both migration strategies and switch from precopy to postcopy live migration without disruption. Note that, postcopy migration does not use **multifd**.

Jira:RHEL-97465[1]

New **s390-ccw-virtio-rhel9.8.0** machine type available for IBM Z VMs

The updated **qemu-kvm** package provides a new **s390-ccw-virtio-rhel9.8.0** machine type for IBM Z virtual machines (VMs). This machine type enables Control Program Identification (CPI) and performance-enhanced PCI translation for passthrough PCI devices by default. As a result, IBM Z VMs that use the **s390-ccw-virtio-rhel9.8.0** machine type benefit from improved performance with passthrough PCI devices and CPI without additional configuration.

Jira:RHEL-104005[1]

libvirt introduces a **host-model** mode for Hyper-V Enlightenments

The **libvirt** package provides a new **host-model** mode for Hyper-V Enlightenments, which automatically enables all Hyper-V enlightenments supported on the host. This mode eliminates the need for separate configuration templates for Intel and AMD hosts. As a result, you can configure **<hyperv mode='host-model'/>** in the XML definition of a virtual machine to automatically apply all host-supported Hyper-V Enlightenments without maintaining separate configurations for each vendor.
Jira:RHEL-114003

Native FUA support for QEMU

With this update, the QEMU emulator no longer needs to emulate the Forced Unit Access (FUA) I/O method, and instead can use FUA natively. This can improve the overall performance of virtual storage, particularly in database workloads.
Jira:RHEL-118197

PCCS for Intel TDX

This update introduces the Provisioning Caching Certification Service (PCCS) for Intel Trust Domain Extensions (TDX). This provides the local caching required to use Intel hosted Provisioning Certification Services (PCS) at scale, and also makes it possible to perform TDX attestation on host systems that are isolated from the public internet.
Jira:RHEL-127046

SCSI passthrough support for virtual machines

With this update, RHEL now supports SCSI passthrough for virtual machines (VMs). With this feature, VMs can directly access host SCSI devices, such as tape drives and Storage Area Network (SAN) Logical Unit Numbers (LUNs).
As a result, you can configure VMs to use specialized storage devices that require direct SCSI access, including support for both single-path and multipathed vDisks.

Note that for SCSI passthrough to work, the host must use a supported RHEL and kernel version. For details, see: Required RHEL versions for SGIO support in Virtual Machines

Jira:RHELDOCS-21410[1]

SCSI3 Persistent Reservation support for virtual machines

With this update, RHEL supports SCSI3 Persistent Reservation (S3-PR) for virtual machines (VMs). This feature makes it possible for multiple VMs to coordinate access to shared storage devices, which is essential for Linux clustering solutions, such as Pacemaker, and for Windows Server Failover Clustering.
As a result, VMs can register and manage persistent reservations on storage devices, which prevent conflicts when multiple VMs access the same storage. S3-PR support is available for both single-path and multipathed vDisks.

Note that for S3-PR to work, the host must use a supported RHEL and kernel version. For details, see: Required RHEL versions for SGIO support in Virtual Machines

Jira:RHELDOCS-21467

4.16. SUPPORTABILITY

Improved AAP plugins for more useful diagnostics

Before this update, the **sos** report was collected on **AAP**. With this update, the notable enhancements to the following AAP plugins are:

- **aap_containerized**: Resolved an issue that incorrectly enabled **aap_containerized** on the RPM-based Private Automation Hub servers.
- **aap_controller**: Expanded the set of gathered command outputs and conditionally collect **run_wsbroadcast** or **run_wsrelay** depending on the AWX release version.

- **aap_eda**: Collected service output details based on the installed EDA version. Starting from AAP 2.5, specific commands are used to obtain service status information.
- **aap_gateway**: Added additional command outputs for improved troubleshooting on Gateway servers.
- **aap_hub**: Centralized the collection of service information for PAH servers under a single location within the plugin directory.

Jira:RHEL-121524

SSL certificate control in SOS clean process is available

With this update, you can manage SSL/TLS certificates that contain sensitive data during the SOS clean process. The new **--treat-certificates** option provides the option to remove, obfuscate, or maintain the original binary format of these certificates ensuring that no sensitive data persists. As a result, you can enhance data security and privacy by selecting the treatment for SSL/TLS certificates during the SOS clean process.

Jira:RHEL-142619

Automatic user detection for AAP container runners in SOS reports

With this update, the **sos** utility automatically detects the user running containers for Ansible Application Platform (AAP) deployments. This eliminates the need for manual specification, ensuring the collection of all necessary AAP data.
Jira:RHEL-140738

4.17. CONTAINERS

The **log-location** option is available in the podman configuration

You can specify a custom **log-location** option in the **containers.conf** file for per-user configurations using **podman-kube systemd**. Previously, logs were restricted to a default location and could not be customized. With this release, you can define custom log paths directly in the configuration file, reducing the need to specify them manually in the **podman run** command.

Jira:RHEL-3114[1]

Enhanced **aardvark-dns** functionality rereads**resolv.conf** file without requiring a full process restart

With this update, the Aardvark-DNS process now dynamically reloads DNS configurations in the Podman 5.x stack on Red Hat Enterprise Linux (RHEL). This eliminates the need to stop and restart the entire process when changes are made to the DNS configuration file, resulting in improved efficiency and reduced downtime for end users.

Jira:RHEL-85839[1]

container-selinux rebased to version 2.244.0-1

The **container-selinux** package, which provides necessary SELinux policies, types, and rules to confine and secure container runtimes, has been rebased to version 2.244.0-1. This version provides important enhancements, most notably, it streamlines the process, enhances data protection, and

ensures confidentiality in deployments, while reducing potential security risks associated with public storage endpoints.
Jira:RHEL-112187

runc rebased to 1.3.3

The **runc** package, which serves as the low-level, CLI tool for spawning and running containers, is rebased to upstream version 1.3.3. This version provides important fixes and enhancements, most notably the following:

- You can create and manage their own private container registries on a dedicated Azure Kubernetes Service (AKS) cluster. This enhancement streamlines container workflows, enhances security, and boosts efficiency by providing a private space for storing and distributing container images, reducing the risk of unauthorized access.
- Automates routine tasks, saves time and effort, and improves the user interface. It enables seamless integration of third-party applications, expanding the platform's functionality and versatility for users.

Jira:RHEL-124800

Unified Configuration available for Rootless Podman

With this update, a unified system-wide configuration file is introduced for rootless Podman, enabling centralized policy management, a consistent security baseline, and operational standardization across all users.
As a result, you can inherit sensible defaults without manual configuration, while still maintaining the flexibility to override system settings through personal configuration files. Additionally, this update ensures backward compatibility, meaning existing user workflows and configurations remain unchanged.

Jira:RHEL-126643

The Container Tools packages have been updated

The updated Container Tools RPM meta-package, which includes the Podman, Buildah, Skopeo, **crun**, and **runc** tools, is available. The Buildah package has been updated to version 1.43.1, and Skopeo has been updated to version 1.22.2. Podman release 5.8.2 contains the following notable bug fixes and enhancements over the previous version:

- The **podman machine init --image** command can run **PowerShell-escaped** commands from the user-specified image path in a PowerShell session on the host when you use it on Windows with the Hyper-V backend (CVE-2026-33414).
- Automatic migration from BoltDB to SQLite after a reboot no longer performs a partial migration, leaving some containers in SQLite and others in BoltDB, when Quadlets are in use.
- The **podman quadlet install** command installs files that contain multiple separate Quadlet files. You must separate the files with a **--- delimiter** on a new line and begin each section with a **# FileName=<name>** line to name the new Quadlet.
- The **Quadlet .container** files include the **AppArmor** key to configure a container's AppArmor profile.
- Podman automatically attempts to migrate earlier BoltDB databases to SQLite when the system reboots. This is necessary because the Podman 6.0 release removes support for

BoltDB. If automatic migration is not possible, you can manually force a migration with the new **podman system migrate --migrate-db** option.

- Podman loads the path from the VM's filesystem when you run the **podman artifact add** command against a Podman machine VM. This improves performance if you share the path you load or build into the VM instead of streaming the data through the REST API.
- The **podman update** command has a new option, **--ulimit**, to update container ulimits.
- You can use the new **--no-session** option with the **podman exec** command to disable tracking of the exec session, which improves performance and startup time.
- Containers with the **unless-stopped** restart policy restart after a reboot when you enable the **podman-restart.service** service.
- In the **Quadlet.container** file:
  - You can set **Entrypoint=""** to clear the container's entrypoint.
  - A **HealthCmd** supports commands with double-quotes and ensures a functional health check.
  - The **RequiresMountsFor** field correctly handles bind-mount paths that contain spaces.
- Inspecting containers in host network mode no longer causes FreeBSD systems to panic.
- The Libpod System Check endpoint no longer performs operations with bad data after it returns a 400 error.
- The remote attach API for containers (Libpod & Compat) no longer panics due to a rare race condition.
- The system no longer improperly adds options from the default driver, which previously prevented the Secret Create API from creating functional secrets using the shell driver. You can enter the secret directly at the terminal with the **podman secret create** command instead of providing it through a pipe.
- Added new APIs for interacting with Quadlets:
  - **GET /libpod/quadlets/{name}/file**: Print the contents of a Quadlet file.
  - **GET /libpod/quadlets/{name}/exists**: Check if the given Quadlet exists.
  - **POST /libpod/quadlets**: Install one or more Quadlets.
  - **DELETE /libpod/quadlets**: Remove one or more Quadlets.
  - **DELETE /libpod/quadlets/{name}**: Remove a single Quadlet.
- Containers created by the **podman play kube** command no longer run health checks before the **initialDelaySeconds** option expires, and the **podman kube play** command now correctly handles precedence between environment variables set by both the **envFrom** and **env** fields.
- The **podman build** command's **--pull=newer** option now functions correctly.

- The **podman artifact push** and **podman artifact pull** commands no longer ignore authentication credentials given by the **--authfile** option.
- The **podman run --pod-id-file** option is now properly validated, preventing the creation of containers in pods with improper user namespace configuration.
  For more information about notable changes, see Upstream release notes.

Jira:RHEL-127908

Support for updates in air-gapped and disconnected environments

This update introduces air-gapped and disconnected updates for RHEL deployments, enabling edge deployments to perform updates without internet connectivity. As a result, you can benefit from greater flexibility and reliability for offline updates, improving deployment management in remote or secure environments.

Jira:RHELDOCS-20708[1]

New container images are available

The **rhel9/ruby-40**, **rhel9/postgresql-18**, **rhel9/python-314-minimal**, **rhel9/mariadb-118** and **rhel9/python-314** container images are now available in the Red Hat Container Registry. The notable enhancements for each image are:

- **rhel9/ruby-40**: You use the Ruby 4.0 container as your base platform to build and run diverse Ruby 4.0 applications and frameworks. This container image includes the npm utility, so you can install JavaScript modules for your web applications.
- **rhel9/postgresql-18**: You can use this container image to package the PostgreSQL **postgres** daemon and client application in a container. The **postgres** server daemon accepts your connections from clients and provides you access to content from PostgreSQL databases.
- **rhel9/python-314-minimal**: You use the full container image as a universal base image to build your containerized applications. However, this universal nature means that the resulting containers consume a lot of disk space. This happens mainly because the image contains npm, compilers, header files, and other packages you might need to install and deploy your applications.
- **rhel9/mariadb-118**: You use this container image to package the MariaDB **mysqld** daemon and client application into a container. The **mysqld** server daemon accepts your client connections and provides you with access to content from MySQL databases.
- **rhel9/python-314**: You can use the Python 3.14 container as your base platform to build and run your Python 3.14 applications and frameworks. This container image includes the npm utility, so you can install JavaScript modules for your web applications. Currently, Red Hat does not support a specific npm or nodejs version in the image.

Jira:RHELDOCS-22067[1]

4.18. RHEL LIGHTSPEED

Color support for the command-line assistant

With this update, the command-line assistant supports color output by default, aligning its appearance with other RHEL command-line tools. This update improves output readability through increased visual contrast.
You can disable color output by using the **--plain** option or by setting the **NO_COLOR=1** environment variable.

Jira:RHELDOCS-21814[1]

SAP Solutions documentation added to RHEL Lightspeed

With this enhancement, RHEL Lightspeed includes the Red Hat Enterprise Linux for SAP Solutions documentation set in its knowledge base. You can now ask RHEL Lightspeed technical questions specific to SAP deployments on RHEL. This update provides more accurate and context-aware responses for SAP-related administrative and configuration tasks.

Jira:RHELDOCS-21815[1]

CHAPTER 5. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel distributed with Red Hat Enterprise Linux 9.8. 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.

New kernel parameters

arm64.nompam=

[ARM64]

Disable Memory Partitioning and Monitoring (MPAM) support on systems that support MPAM but do not enable it in firmware.

cgroup_v1_proc=

[KNL]

Show missing controllers in /**proc**/**cgroups**.

Format: **{ "true" | "false" }**

By default, /**proc**/**cgroups** lists only cgroup v1 controllers. This compatibility option also lists v2 controllers (whose v1 code is not compiled) so that semi-legacy software can use this file to decide whether to use v2 controllers.

initramfs_options=

[KNL]

Specify mount options for the initramfs mount.

nvme.quirks=

[NVME]

Extend the built-in NVMe quirk list.

Format: **VendorID:ProductID:quirk_names[-VendorID:ProductID:quirk_names…]**

The IDs are 4-digit hexadecimal numbers. The **quirk_names** field is a comma-separated list of quirk names. Prefix a quirk name with **^** to disable the specified quirk.

For example:

nvme.quirks=7710:2267:bogus_nid,^identify_cns-9900:7711:broken_msi

rh_waived=

[KNL]

Control waived items in Red Hat Enterprise Linux.

Some features or security mitigations can be waived and toggled on or off on demand. Waive these items only when necessary, because this can make the system insecure or out of support scope.

Format: **<item-1>,<item-2>…<item-n>**

Use **rh_waived** to enable all waived features that **Documentation/admin-guide/rh-waived-features.rst** lists.

vmscape=

[X86]

Control mitigation for VMscape attacks.

VMscape attacks can leak information from a user space hypervisor to a guest by using speculative side channels.

Possible values:

off

Disable the mitigation.

ibpb

Use the Indirect Branch Prediction Barrier (IBPB) mitigation (default).

force

Force vulnerability detection even on processors that are not otherwise affected.

Changed kernel parameters

microcode=

[X86]

Control the behavior of the microcode loader.

You can specify the following options as a comma-separated list:

base_rev=X

Set the base microcode revision of each thread in debug mode, where **<X>** is a 32-bit unsigned integer.

dis_ucode_ldr

Disable the microcode loader.

force_minrev

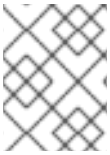
Control minimal microcode revision enforcement for the runtime microcode loader.

mitigations=

[X86,PPC,S390,ARM64]

Control optional mitigations for CPU vulnerabilities.

This kernel parameter is a set of curated, architecture-independent options. Each option aggregates architecture-specific parameters.



NOTE

The **mitigations** parameter is available only if the kernel is built with **CPU_MITIGATIONS=y**.

Possible values:

off

Disable all optional CPU mitigations. This setting can improve system performance but can expose users to several CPU vulnerabilities. This setting is equivalent to the following:
If **nokaslr** is set:

- **kpti=0** on ARM64

The following settings always apply:

- **gather_data_sampling=off** on x86
- **indirect_target_selection=off** on x86
- **kvm.nx_huge_pages=off** on x86
- **l1tf=off** on x86
- **mds=off** on x86
- **mmio_stale_data=off** on x86
- **no_entry_flush** on PowerPC
- **no_uaccess_flush** on PowerPC
- **nobp=0** on IBM Z
- **nopti** on x86 and PowerPC
- **nospectre_bhb** on ARM64
- **nospectre_v1** on x86 and PowerPC
- **nospectre_v2** on x86, PowerPC, IBM Z, and ARM64
- **reg_file_data_sampling=off** on x86
- **retbleed=off** on x86
- **spec_rstack_overflow=off** on x86
- **spec_store_bypass_disable=off** on x86 and PowerPC
- **spectre_bhi=off** on x86
- **spectre_v2_user=off** on x86
- **srbds=off** on x86 and Intel

- **ssbd=force-off** on ARM64
- **tsx_async_abort=off** on x86
- **vmscape=off** on x86

Exceptions

This setting does not affect **kvm.nx_huge_pages** when **kvm.nx_huge_pages=force**.

auto (default)

Mitigate all CPU vulnerabilities and keep simultaneous multithreading (SMT) enabled, even if it is vulnerable. Use this option if you do not want SMT to be disabled across kernel updates or you rely on other methods to avoid attacks that target SMT. This setting is the default behavior.

auto,nosmt

Mitigate all CPU vulnerabilities and disable SMT if needed. Use this option if you always want full mitigation, even if this requires disabling SMT. On x86, this setting is equivalent to the following:

- **l1tf=flush,nosmt**
- **mds=full,nosmt**
- **tsx_async_abort=full,nosmt**
- **mmio_stale_data=full,nosmt**
- **retbleed=auto,nosmt**

On x86, after you specify one of the preceding options, you can also use attack-vector-based controls as described in **Documentation/admin-guide/hw-vuln/attack_vector_controls.rst**.

CHAPTER 6. DEVICE DRIVERS

6.1. NEW DRIVERS

Table 6.1. Character device drivers

Description	Name	Limited to architectures
TPM CRB FFA driver	tpm_crb_ffa	64-bit ARM architecture

Table 6.2. Crypto drivers

Description	Name	Limited to architectures
Intel® QuickAssist Technology for GEN6 Devices	qat_6xxx	AMD and Intel 64-bit architectures

Table 6.3. Clock (DPLL) drivers

Description	Name	Limited to architectures
Microchip ZL3073x core driver	zl3073x	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Microchip ZL3073x I2C driver	zl3073x_i2c	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Microchip ZL3073x SPI driver	zl3073x_spi	64-bit ARM architecture, AMD and Intel 64-bit architectures

Table 6.4. Firmware control drivers

Description	Name	Limited to architectures
ARM FF-A bus	ffa-core	64-bit ARM architecture

Table 6.5. Graphics drivers and miscellaneous drivers

Description	Name	Limited to architectures
DRM GPU scheduler	gpu-sched	IBM Z
DRM GPUSVM	drm_gpusvm_helper	AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
Helpers for DRM sysfb drivers	drm_sysfb_helper	

Table 6.6. I2C drivers

Description	Name	Limited to architectures
PCA954x I2C mux and switch driver	i2c-mux-pca954x	AMD and Intel 64-bit architectures

Table 6.7. Network drivers

Description	Name	Limited to architectures
Aeonsemi AS21xxx PHY driver	as21xxx	
Airoha EN8811H PHY drivers	air_en8811h	IBM Z
Aquantia PHY driver	aquantia	IBM Z
Asix PHY driver	ax88796b	IBM Z
Broadcom BCM7xxx internal PHY driver	bcm7xxx	IBM Z
Broadcom PHY library	bcm-phy-lib	IBM Z
Cortina EDC CDR 10G Ethernet PHY driver	cortina	IBM Z
Intel® Ethernet common library	libie_fwlog	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Intel® Ethernet common library admin queue helpers	libie_adminq	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Intel XWAY PHY driver	intel-xway	IBM Z
Marvell 88Q2XXX 100/1000BASE-T1 automotive Ethernet PHY driver	marvell-88q2xxx	IBM Z
Marvell Alaska X/M multi-gigabit Ethernet PHY driver	marvell10g	IBM Z
MaxLinear Ethernet GPY driver	mxl-gpy	IBM Z

Description	Name	Limited to architectures
MaxLinear MXL86110 and MXL86111 PHY driver	mxl-86110	
Microchip LAN87XX, LAN937x, and LAN887x T1 PHY driver	microchip_t1	IBM Z
Microchip LAN88XX and LAN937X TX PHY driver	microchip	IBM Z
Microsemi VSC85xx PHY driver	mscc	IBM Z
PHY package support	phy_package	
Qualcomm Atheros QCA808X PHY driver	qca808x	IBM Z
Qualcomm Atheros QCA83XX PHY driver	qca83xx	IBM Z
Qualcomm PHY driver common functions	qcom-phy-lib	IBM Z
Realtek PHY driver	realtek	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Renesas uPD60620 PHY driver	uPD60620	IBM Z
Rockchip Ethernet PHY driver	rockchip	IBM Z
Teranetics PHY driver	teranetics	IBM Z
Texas Instruments DP83822 PHY driver	dp83822	IBM Z
Texas Instruments DP83848 PHY driver	dp83848	IBM Z
Texas Instruments DP83867 PHY driver	dp83867	IBM Z
Texas Instruments DP83TC811 PHY driver	dp83tc811	IBM Z
Texas Instruments DP83TG720S PHY driver	dp83tg720	IBM Z
Xilinx GMII2RGMII converter driver	xilinx_gmii2rgmii	IBM Z

Table 6.8. Platform drivers

Description	Name	Limited to architectures

Description	Name	Limited to architectures
AMD HSMP common driver	hsmp_common	AMD and Intel 64-bit architectures
AMD HSMP platform interface driver	amd_hsmp	AMD and Intel 64-bit architectures
AMD HSMP platform interface driver (ACPI)	hsmp_acpi	AMD and Intel 64-bit architectures
Intel PMC SSRAM telemetry driver	intel_pmc_ssram_telemetry	AMD and Intel 64-bit architectures
Intel PMT discovery driver	pmt_discovery	AMD and Intel 64-bit architectures

Table 6.9. Thermal drivers

Description	Name	Limited to architectures
Processor thermal PTC interface	platform_temperature_control	AMD and Intel 64-bit architectures

6.2. UPDATED DRIVERS

Table 6.10. Accelerator driver updates

Description	Name	Current version	Limited to architectures
Driver for Intel NPU (Neural Processing Unit)	intel_vpu	1.0.0 (5.14.0-687.5.1.el9_8.x86_64)	AMD and Intel 64-bit architectures

Table 6.11. Graphics driver updates

Description	Name	Current version	Limited to architectures
Standalone DRM driver for the VMware SVGA device	vmwgfx	2.21.0.0	64-bit ARM architecture, AMD and Intel 64-bit architectures

Table 6.12. Storage driver updates

Description	Name	Current version	Limited to architectures
Driver for Microchip Smart Family Controller	smartpqi	2.1.36-026	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Emulex LightPulse Fibre Channel SCSI driver	lpfc	0:14.4.0.12	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
LSI MPT Fusion SAS 3.0 device driver	mpt3sas	54.100.00.00	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures

CHAPTER 7. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 9.8 that have a significant impact on users.

7.1. INSTALLER AND IMAGE CREATION

The driver disk menu now correctly displays user input on the console

Before this release, when starting a RHEL installation with the **inst.dd** kernel command-line option, the console failed to render characters typed by the user. As a consequence, the lack of visual feedback made the application appear unresponsive, even though the input was still being processed in the background. With this update, this display issue has been resolved, and user input is now visible as expected during the driver disk selection process.
Jira:RHEL-4737

Installer falls back to English in text mode for unsupported languages

Before this release, the installer did not set the display mode (text, graphical, or non-interactive) early enough during startup. As a result, the check to determine whether a selected language is supported in text mode did not run. In text mode installations, languages that are not supported in the text user interface, such as Japanese, could be used, resulting in unreadable output.
With this fix, the installer correctly detects languages that are not supported in the text mode. If an unsupported language is selected, the text user interface falls back to English. The installed system is still configured to use the originally selected language.

Jira:RHEL-144834

7.2. SECURITY

AIDE no longer terminates when a monitored file is changed

Before this update, AIDE terminated with an error if a file was truncated or removed while AIDE was computing its hash. With this update, AIDE detects when a file is truncated or deleted during hash calculation and handles the condition safely. As a result, AIDE successfully completes integrity checks even if a monitored file change size or is removed during processing.
Jira:RHEL-1569

Updated URL in **cracklib** and **cracklib-dicts**

Before this update, the CrackLib website URL in the **cracklib** and **cracklib-dicts** packages was outdated. As a consequence, an incorrect download of **cracklib-dicts** occurred. With this release, the URL in the **cracklib** and **cracklib-dicts** RPMs is updated to the new website URL. As a result, the package information is accurate.
Jira:RHEL-5215

clevis-pin-tpm2 no longer silently ignores invalid JSON

Before this update, the **clevis-pin-tpm2** command did not validate JSON field names during encryption with TPM2 and silently ignored typos and invalid fields, for example, **pcrs_ids** instead of **pcr_ids**. Consequently, users could inadvertently create LUKS bindings with incorrect TPM2 configurations due to typos. This could lead to unlock failures when TPM state changes, potentially making systems unbootable.

This update adds JSON schema validation to reject unknown fields in the TPM2 configuration during encryption. As a result, invalid field names in TPM2 JSON configuration are properly rejected with clear error messages to prevent silent misconfigurations that could cause unlock failures.

Jira:RHEL-68417

fapolicyd-cli --check-trustdb no longer reports files without size or checksum information

Some files, for example, **/usr/lib/rpm/redhat/redhat-annobin-cc1** or **/etc/selinux/targeted/policy/policy.33**, owned by an RPM package, are expected to be changed during and after the installation, but they are still owned by the corresponding package. Consequently, **fapolicyd** cannot verify such files. With this release, the **fapolicyd** framework no longer adds files that do not have size or checksum information in the RPM database to the trust database. As a result, the **fapolicyd-cli --check-trustdb** command does not report the **miscompares: size sha256** error message for such files.
Jira:RHEL-94661

Keylime registrar no longer corrupts EK certificates

Before this update, the Keylime registrar performed an unnecessary data conversion of malformed Endorsement Key (EK) certificates. This process corrupted the certificates and invalidated their signatures. Consequently, it prevented the use of the **ek_check_script** workaround for Trusted Platform Module (TPM) devices with non-standard certificates.
With this update, the database stores EK certificates without data corruption. As a result, you can validate TPM devices with malformed certificates by using the Keylime registrar and custom verification scripts.

Jira:RHEL-111167[1]

Keylime agents correctly generate TPM quotes by using ECC keys

Before this update, when generating signed Trusted Platform Module (TPM) quotes, the **keylime-agent-rust** component did not properly support Elliptic Curve Cryptography (ECC) key algorithms. This prevented the agent from generating TPM quote evidence and caused enrollment failures for the ECC key types. With this update, the **keylime-agent-rust** component correctly handles ECC key algorithms during TPM quote generation. As a result, agents can successfully generate TPM quotes and enroll with verifiers to provide full attestation functionality with ECC keys generated by the TPM.
Jira:RHEL-118148

Keylime verifier correctly validates TPM quotes signed with ECC keys

Before this update, when verifying signed Trusted Platform Module (TPM) quotes from agents, the Keylime verifier component did not properly support Elliptic Curve Cryptography (ECC) key algorithms. This caused attestation failures when agents used the ECC key types **ecc521**, **ecc384**, **ecc256**, **ecc224**, or **ecc192**. With this update, the verifier correctly handles and verifies TPM quotes signed with ECC keys. As a result, Keylime provides full attestation functionality for these algorithms.
Jira:RHEL-118150

The **scp** utility correctly handles relative paths containing**..**

Before this update, the **scp** utility did not expand the **..** parent directory indicator in a path to the directory name. Consequently, **scp** incorrectly handled relative paths containing **..**. This update adds special handling for parent directory indicators. As a result, **scp** now processes paths containing **..** correctly.

Jira:RHEL-119515

SELinux confined users can use smart cards with ssh-agent

Before this update, the **ssh-pkcs11-helper** binary lacked a specific SELinux security context, which prevented confined users from sending a request to the **ssh-agent** program. Consequently, confined users, such as **user_u** or **staff_u**, were unable to add smart-card-based keys to **ssh-agent**. With this update, **ssh-pkcs11-helper** is labeled with the **ssh_agent_exec_t** type, and additional rules are added to cache results. As a result, confined users can successfully use smart cards with **ssh-agent**, allowing the agent to correctly access PKCS #11 keys and cache the results in the user's home cache.
Jira:RHEL-121165

NSS database password updates no longer corrupt ML-DSA seeds

Before this update, when you changed the database password, a bug in how NSS handled database re-encryption prevented the ML-DSA seed attribute from updating. As a result, the seed value was permanently lost, even if you knew the previous password.
With this update, password changes correctly update the ML-DSA seed attribute and no longer cause the permanent loss of seed values. Note that you still cannot recover the seeds lost before this update.

Jira:RHEL-127671[1]

Clevis handles migrations to image mode correctly

Before this update, user and group membership updates from package installations were not properly applied when migrating from package mode to image mode. Consequently, the **clevis** user was not added to the **tss** security group, preventing Clevis from accessing a trusted platform module (TPM) device and retrieving encryption keys during system boot. With this update, the Clevis package installation process is updated to ensure that the **clevis** user is properly added to the **tss** group during image mode updates, even when existing configuration files are preserved. As a result, Clevis can properly access the TPM device and successfully retrieve an encryption key on systems in image mode.
Jira:RHEL-132187

The SELinux policy no longer disables assistive technologies for confined users

Before this update, the SELinux policy restricted confined users from using the Assistive Technology Service Provider Interface (AT-SPI) services. As a consequence, these services failed to operate in graphical desktop environments. This update adds the required execution and directory access permissions to the SELinux policy.
As a result, assistive technologies, such as the Orca screen reader and on-screen keyboards, function correctly for confined users in SELinux enforcing mode.

Jira:RHEL-133898[1]

/usr/share/*/bin/* binaries work with fapolicyd

Before this update, the **fapolicyd** service did not add binaries from **/usr/share/*/bin/** directories to the trust database. For example, the **/usr/share/Modules/bin/mkroot** binary was not added. Consequently, users could not run these binaries when using the **trust=1** option in **fapolicyd** rules.

With this fix, the **fapolicyd-filter.conf** file contains ***/bin/***. As a result, you can run binaries from **/usr/share/*/bin/** with the **fapolicyd** service active.
Jira:RHEL-141670

7.3. SOFTWARE MANAGEMENT

DNF no longer attempts to automatically remove protected packages installed as dependencies

Before this update, if you installed a protected package as a dependency required by only one other package and had the **clean_requirements_on_remove** configuration option enabled, DNF failed to perform any transaction that tried to remove the protected package if this package became an unused dependency. This prevented the removal of the package that depended on it, because DNF would automatically attempt to remove the protected dependency as well. With this update, DNF treats all protected packages as explicitly installed by the user. As a result, DNF no longer attempts to automatically remove protected packages, allowing the removal of the package that depends on it.
Jira:RHEL-76112

DNF correctly performs comparison of**epoch-version-release** for upgrade transactions

Before this update, DNF incorrectly performed comparison of the **epoch-version-release** (**EVR**) RPM package information. As a consequence, if you performed two subsequent upgrade transactions for a package that had the same **epoch-version** but different **release**, DNF identified the overall transaction as a downgrade. This update fixes the **EVR** comparison. As a result, DNF identifies two subsequent package upgrades with different release versions as an upgrade.
Jira:RHEL-81779

dnf-automatic can send emails to multiple recipients with default**/usr/bin/mail**

Before this update, if the **dnf-automatic** utility used the **command_email** emitter to send emails to multiple recipients and also used the **/usr/bin/mail** utility installed with the **s-nail** package, **/usr/bin/mail** failed to send an email. With this update, the **dnf-automatic** utility expands the **email_to** keyword in the **command_format** formatting string from a single argument to multiple arguments. As a result, **dnf-automatic** sends emails to multiple recipients with the default **/usr/bin/mail** utility.
Jira:RHEL-94321

DNF transactions that use advisory filters to update packages with multiple architectures no longer fail with a logic error

Before this update, using DNF advisory filters, such as **--security**, to update certain packages with multiple architectures triggered a logic error in the **libsolv** dependency solver. As a consequence, updating packages by using advisory filters would sometimes result in a transaction that could not be resolved. This issue affected the **libldb** and **libsmbclient** packages. This update fixes the logic error in **libsolv**. As a result, update transactions involving multiple architectures and the **forcebest** and **implicitobsoleteusescolors** solver options resolve.
Jira:RHEL-103995

pqrpm no longer fails to verify a package with multiple signatures when the package has some **NOTTRUSTED** signatures

Before this update, when you verified a package with multiple signatures, **pqrpm**, the minimal variant

of RPM with post quantum cryptography (PQC) support, did not correctly determine the overall verification result when the **/usr/lib/pqrpm/bin/rpmkeys** utility reported some of the package signatures as **NOTTRUSTED**. A signature can become **NOTTRUSTED** if, for example, its certificate is expired or revoked, or if its algorithm is disabled by system-wide cryptographic policies. As a consequence, **pqrpm** failed to verify the package even if the package had at least one valid and trusted signature.
This update fixes the verification logic in **pqrpm** to correctly handle packages with **NOTTRUSTED** signatures. This update also improves error reporting around this functionality.

As a result, **pqrpm** ignores **NOTTRUSTED** package signatures and successfully verifies a package with multiple signatures if the package has at least one valid signature and no invalid signatures. Error messages are also clearer and more accurate when verification actually fails.

Jira:RHEL-112700

multisig no longer fails to install packages that use both supported and unsupported RPMv6 signing algorithms

Before this update, you could not install packages with signatures that used both supported and unsupported RPMv6 package signing algorithms. As a consequence, DNF rejected such packages when verifying their signatures because of the unsupported algorithms. With this update, the DNF **multisig** plugin ignores signatures classified as **NOTTRUSTED** in the **rpmkeys** command output. As a result, **multisig** can install packages that use both supported and unsupported signing algorithms.
Jira:RHEL-145372

7.4. SHELLS AND COMMAND-LINE TOOLS

volume_key successfully retrieves backup passphrases in FIPS mode

Before this update, the **volume_key** utility used functions that were incompatible with Federal Information Processing Standards (FIPS) when retrieving a backup passphrase from an escrow packet. Consequently, **volume_key** failed and reported an error on systems with FIPS mode enabled. This update ensures that the backup passphrase retrieval function is FIPS-compliant. As a result, you can successfully retrieve backup passphrases on FIPS-enabled systems.
Jira:RHEL-113757[1]

7.5. NETWORKING

RHEL disables LRO on VLAN port devices by default

Before this update, RHEL did not automatically disable large receive offload (LRO) on port if you created a VLAN device. As a consequence, this could affect VLAN packet receiving because LRO merges small packets to big ones and ignores the VLAN flag. With this update, RHEL enforces disabling LRO on the port device when you add a VLAN on it. As a result, VLAN packet receiving works correctly.
Jira:RHEL-80409[1]

The NetworkManager sriov.vfs property supports thereapply operation

Before this update, NetworkManager could not dynamically apply changes if a user changed the **sriov.vfs** property. As a consequence, NetworkManager connections with Single Root I/O Virtualization (SR-IOV) settings required a restart after modifications. With this release, **sriov.vfs**

now supports the **reapply** operation if the total number of virtual functions (VFs) does not change. As a result, restarting a connection after modifying SR-IOV settings is no longer required in the mentioned scenario.

Jira:RHEL-113954[1]

NetworkManager clients can set a global-level DNS search domain without defining a DNS server

Before this update, if a client, such as the Nmstate API or the GNOME control center application, used the D-Bus API for changes on a global level, it was not possible to set DNS search domains without defining a DNS server. This update fixes the problem, and clients can define only a global-level DNS search domain.

Jira:RHEL-115973[1]

The **xdp-trafficgen** utility works correctly on ARM systems

Before this update, the **xdp-trafficgen** utility failed on ARM systems with a **Missing required option '--interface'** error even if you specified the **-i <interface>** option. As a consequence, it was not possible to probe eXpress Data Path (XDP) support on a specific interface. This update fixes the problem, and the **-i <interface>** option works correctly on ARM systems.

Jira:RHEL-119860

The **conntrack** utility can delete connection tracking entries managed by **nftables** flowtables

When you use **nftables** flowtables, connection tracking entries handled by a flowtable can be marked with an **OFFLOAD** status to accelerate packet processing. In previous releases, a kernel safeguard prevented the **conntrack** utility from deleting any entry after it was marked as offloaded. As a consequence, deleting stale entries was not possible. With this update, the kernel was modified to allow the deletion of connection tracking entries regardless of their offload status. As a result, you can use the **conntrack** utility to remove entries that are handled by an **nftables** flowtable.

Jira:RHEL-138511[1]

7.6. FILE SYSTEMS AND STORAGE

GFS2 now handles large writes more efficiently

Before this update, multi-page write operations to GFS2 files sometimes degenerated into page-size (typically 4 KiB) chunks. This happened after an initial multi-page segment was written, particularly when using **write(2)** with a large buffer that was not resident in memory. This led to reduced write efficiency for large files.
With this release, GFS2 kernel code has been updated to fix the issue. As a result, some large write workloads may see a small improvement in write efficiency.

Jira:RHEL-7971[1]

Multipath persistent reservation handling is now more robust and consistent

Before this update, the **libmpathpersist** library, which is used by the **mpathpersist** command, had several issues and corner cases that affected persistent reservation handling for multipath devices. This caused the following problems:

- Numerous **mpathpersist** operations failed on a multipath device.

- Persistent reservations sometimes ended up in an inconsistent state. As a consequence, the multipath device denied write access when it was supposed to be allowed, and allowed write access when it was supposed to be prohibited.

With this release, multiple areas of **libmpathpersist** have been redesigned and fixed to ensure correct and consistent behavior. As a result, **mpathpersist** commands on multipath devices now work the same as the equivalent **sg_persist** commands on SCSI devices. I/O access to multipath devices also consistently reflects the device's persistent reservation state.

Jira:RHEL-118515

The Anaconda installer can now use iSCSI LUNs with ID 256 or higher

Before this update, starting an operating system installation on a system that used iSCSI storage could cause the Anaconda installer to crash. This occurred when the iSCSI Logical Unit Number (LUN) ID was 256 or higher.
This update includes a fix to the LUN ID parsing logic in the **blivet** library. As a result, installations on systems that use iSCSI targets with LUN IDs of 256 or greater can now proceed.

Jira:RHEL-122858

The output of **df** and **du** now remains consistent after file deletion in GFS2 file system

Before this update, when a large number of files were deleted on a GFS2 file system, the space occupied by those files remained claimed. As a consequence, the **df** utility reported much higher disk usage than the **du** utility, which made the file system appear to have run out of space.
With this release, the logic that manages and updates free disk space counters has been corrected. As a result, disk usage information reported by **df** and **du** now remains accurate and consistent, even after mass file deletion operations.

Jira:RHEL-129403[1]

multipathd logs offline path warnings for uninitialized paths

Before this update, if **multipathd** started or reconfigured while a path was offline, the daemon did not print regular offline warnings for that path. This made it difficult to identify issues with uninitialized paths.
With this update, **multipathd** prints offline messages for uninitialized paths. As a result, you can monitor path status consistently.

Jira:RHEL-133814[1]

Fixed delayed uevent processing in **multipathd**

Before this update, when a large number of uevents occurred, **multipathd** delayed processing the events for up to 30 seconds. During this time, **multipathd show status** incorrectly reported that there was no outstanding work. As a consequence, **multipathd** did not always react promptly when path devices were added or removed. This could lead to temporary hangs or I/O errors if no active paths were available.
With this update, **multipathd** processes uevents without delay and reports its status correctly. As a result, multipath devices no longer hang or return I/O errors after a usable path is added.

Jira:RHEL-135904[1]

Fixed NVMe **subsystem reset** recovery on PowerPC

Before this update, issuing the **nvme subsystem-reset** command on the PowerPC platform caused the Non-volatile Memory Express (NVMe) device to enter the **resetting** state and it failed to recover. As a consequence, the device hung and required a system reboot to recover.
With this release, the NVMe device recovers correctly after a **subsystem reset**. It is temporarily inaccessible while transitioning from the **resetting** state to the **live** state.

Jira:RHEL-137435[1]

7.7. HIGH AVAILABILITY AND CLUSTERS

Resource and stonith agent descriptions retain original formatting

Before this update, **pcs** automatically wrapped resource and stonith agent descriptions to fit within the terminal window. Consequently, any formatting done by the agents' authors-such as new lines, paragraphs, lists, or tables-was removed, often making the descriptions difficult to read.
With this update, **pcs** no longer reformats the description text.

As a result, **pcs** displays resource and stonith agent descriptions exactly as the agents' authors intended, preserving the original structure and improving readability.

Jira:RHEL-113763

The **db2** resource agent handles reintegration correctly

Before this update, the **db2** resource agent could encounter a race condition when a node was reintegrating into the cluster. Consequently, the reintegrating node could incorrectly attempt to start as a "Primary" instance.
With this update, a "reintegration" attribute has been added to the agent. This allows the agent to correctly identify whether it is expected to join as a "Primary" or not, avoiding the race condition.

As a result, reintegration works correctly. Note that in order to prevent issues during the upgrade, you must disable all **db2** resources before applying the update and re-enable them only after the update is complete on all nodes.

Jira:RHEL-118624[1]

7.8. COMPILERS AND DEVELOPMENT TOOLS

ANSI_X3.110-1983 codec moved to**glibc-gconv-extra**

Before this update, the ANSI_X3.110-1983 character set codec was accidentally shipped in the main **glibc** package. As a consequence, minimal installations and container images were slightly larger, and applications could be exposed to vulnerabilities in the ANSI_X3.110-1983 conversion code even when the **glibc-gconv-extra** package was not installed.
With this release, the ANSI_X3.110-1983 codec is moved from the main **glibc** package to the **glibc-gconv-extra** package. As a result, the amount of conversion code present in minimal installations is reduced, and customers who require ANSI_X3.110-1983 support can obtain it explicitly by installing the **glibc-gconv-extra** package.

Jira:RHEL-41205

Fixed missing gzip dependency for compressed locale character maps in glibc-locale-source

Before this update, the **glibc-locale-source** package provided character maps in **gzip** compressed format but did not declare a dependency on the **gzip** package. As a consequence, using **localedef** with a character map provided by **glibc-locale-source** could fail if **gzip** was not installed on the system because the compressed archive could not be uncompressed.
With this release, **glibc-locale-source** now depends on the **gzip** package to ensure that the required compression utility is installed with the character map data. As a result, using **localedef** with character maps provided by **glibc-locale-source** now works as expected even on systems where **gzip** was previously missing.

Jira:RHEL-111005[1]

glibc now returns complete group membership results when NSS group merges fail with ERANGE

Before this update, on systems where Name Service Switch (NSS) merged groups from more than two sources, if merging two groups failed because the internal buffer was too small, **glibc** skipped that merge result instead of retrying with a larger buffer.
As a consequence, on such systems, running commands like **getent group** sometimes returned incomplete or empty group lists.

With this update, **glibc** no longer skips merge failures that are caused by an insufficient internal buffer and instead retries the merge with a larger buffer as intended.

As a result, group membership lookups on systems with multiple group database sources now return complete and correct group membership data.

Jira:RHEL-112149

Boost.JSON integer parsing endian-aware on big-endian systems

Before this update, integer deserialization in Boost.JSON was not endian-aware on big-endian systems, and integer fields were interpreted with the wrong byte order. As a consequence, applications that used Boost.JSON to deserialize integer values on big-endian architectures obtained incorrect integer results and could behave unexpectedly.
With this release, the **boost** package updates Boost.JSON to handle integer deserialization in an endian-aware manner on big-endian systems. As a result, the library returns correct integer values on big-endian systems, ensuring predictable application behavior

Jira:RHEL-116553[1]

glibc NSS database lookup stability improvement

Before this update, missing checks in the **__nss_database_get** function in the **glibc** package could cause null pointer dereferences and assertion failures during Name Service Switch (NSS) database lookups. As a consequence, applications relying on NSS could terminate unexpectedly, or the C library could crash under specific lookup conditions.
With this release, additional validation checks are added to the NSS database lookup path in **glibc** to handle invalid or unexpected internal states safely. As a result, NSS database lookups are more robust, and system stability is improved.

Jira:RHEL-150269

Duplicate DNS queries fixed when the search path is set to

Before this update, when the Domain Name System (DNS) search path in **/etc/resolv.conf** file contained a single **.** entry, the **glibc** DNS stub resolver queried both the original domain name and the same domain name with a trailing dot.
As a consequence, DNS queries for non-existent domains were duplicated, increasing the load on DNS servers.

After this update, the **glibc** DNS stub resolver no longer appends a trailing dot to domain names when the search path contains only a single **.** entry.

As a result, DNS queries are no longer duplicated in this configuration, reducing unnecessary DNS traffic and server load.

Jira:RHEL-153056

7.9. IDENTITY MANAGEMENT

dsconf replication get-ruv no longer returns an error

Before this update, one of the replication functions did not call a required function. As a result, when you ran **dsconf <instance_name> replication get-ruv --suffix dc=example,dc=com**, an error was displayed. With this update, the command returns a Replica Update Vector (RUV) value as expected.

Jira:RHEL-112727[1]

Directory Server correctly displays the number of child entries under a specific node

Before this update, the **numSubordinates** and **numTombstoneSubordinates** attributes were wrongly computed during import. Consequently, when you compared the number of child entries under a specific node, the wrong values were displayed.
With this update, Directory Server computes **numSubordinates** and **numTombstoneSubordinates** correctly.

Jira:RHEL-117748[1]

Directory Server ignores **memberOfDeferredUpdate** setting on instances with LMDB

Before this update, the **memberOfDeferredUpdate** configuration attribute, which is only effective for a Berkeley DB (BDB) backend, was not ignored on instances with a Lightning Memory-Mapped Database Manager (LMDB) backend. As a consequence, if **memberOfDeferredUpdate** was enabled on an LMDB instance, the Directory Server could become unresponsive during MemberOf plugin processing of large or complex groups.
With this update, Directory Server ignores the **memberOfDeferredUpdate** setting on instances with LMDB. As a result, processing large or complex groups no longer causes the server to become unresponsive.

Jira:RHEL-117782[1]

Directory Server tools consistently accept unit suffixes when configuring the LMDB database maximum size

Before this update, **dscreate** and **dsconf** used different functions to parse and display the LMDB database maximum size (**nsslapd-mdb-max-size**). As a consequence, **dscreate create-template** displayed the value as a raw floating-point number in bytes, while **dsconf backend config set --**

mdb-max-size accepted values in bytes only, making it difficult to configure consistent values across the two tools.
With this update, both tools use the same parsing functions and accept values with unit suffixes (**k**, **m**, **g**, **t**), automatically aligning the result to the nearest page boundary. As a result, administrators can use human-readable size values consistently across **dscreate** and **dsconf** when setting the LMDB database maximum size.

Jira:RHEL-121170[1]

New **notes=N** and **notes=B** search indicators to identify asynchronous operations in the Directory Server access log

Before this update, asynchronous requests that exceeded the maximum number of threads per connection caused server unresponsiveness without identification in the Directory Server access logs. As a consequence, it was difficult to diagnose server unresponsiveness.
With this release, Directory Server uses the new search indicators in the access logs to identify such requests: **notes=N** defines that the operation is not synchronous. **notes=B** defines that the operation blocks other new incoming operations: pending operations, not the read operations, are delayed.

In both cases, you might need to increase the **nsslapd-maxthreadsperconn** attribute value to allow a connection to use more threads.

Jira:RHEL-123231[1]

The MemberOf fixup task completion message correctly displays the membership attribute name

Before this update, when the MemberOf plugin completed a global fixup task, the plugin freed its configuration structure before logging the completion message. As a consequence, the completion log message displayed (**null**) instead of the membership attribute name.
With this update, the MemberOf plugin logs the fixup task completion message before freeing its configuration structure, ensuring the attribute name is available when the message is written. As a result, the completion log message displays the correct membership attribute name, making it easier for administrators to verify fixup operations and troubleshoot issues.

Jira:RHEL-123258[1]

The Directory Server web console no longer fails with an error when enabling replication on a consumer

Before this update, when enabling replication on a consumer, the **dsconf** utility printed a warning about changelogs to the **stdout** stream instead of **stderr**. As a consequence, the textual warning broke JSON parsing in the Directory Server web console, which expects pure JSON on **stdout**.
With this update, **dsconf** utility was updated so that the warning about changelogs on consumer replicas is written to **stderr**. As a result, the Directory Server web console successfully loads the **Replication** tab after enabling replication on a consumer or changing a role to consumer.

Jira:RHEL-123897[1]

LDAP searches with spaces in DN filter values no longer return incorrect results

Before this update, a regression in the handling of filters containing distinguished name (DN) caused LDAP searches with spaces inside DN values in the filter, such as **(member=uid=user,**

ou=people,dc=example,dc=com), to be evaluated incorrectly. As a consequence, applications received incomplete group membership and search results.
With this update, Directory Server normalizes and correctly compares DN values in the filter, accepting filters both with and without spaces in DN components. As a result, LDAP searches that include spaces in DN values return the same, complete results as in earlier RHDS versions, restoring expected application behavior.

Jira:RHEL-126552[1]

Online initialization of a Directory Server consumer no longer fails with an LDAP_BUSY error

Before this update, the replication agreement could send entries faster than the consumer was able to import during online initialization. In that situation, the consumer responded with an **LDAP_BUSY** error. As a consequence, the replication agreement did not handle this error and terminated the online initialization.
With this update, the replication agreement handles received **LDAP_BUSY** responses by retrying the operation after a delay. As a result, online initialization completes successfully even when the consumer temporarily cannot keep up with the rate of incoming entries.

Jira:RHEL-129559[1]

Resolved DNS record creation failure when reverse zone is missing

Before this update, the **ipadnsrecord** module in **ansible-freeipa** ignored the **create_reverse** parameter. As a consequence, when users attempted to add **A** or **AAAA** records, the module incorrectly always required an existing reverse DNS zone and the task failed with a "DNS zone not found" error.
With this release, the module logic verifies the status of the **create_reverse** flag before attempting to validate or locate a reverse zone and skips the check entirely if it is set to **false**. As a result, the **ipadnsrecord** module successfully adds **A** and **AAAA** records to IdM-managed zones without requiring an existing reverse zone when **create_reverse** is set to **false**.

Jira:RHEL-140607

Online initialization of large databases progresses as expected

Before this update, when initializing replication with very large databases, especially after major subtree moves, the initialization could appear stalled after sending the initial suffix entry, because it spent excessive time building and checking large internal ID lists. As a consequence, the server experienced long CPU spikes, initialization was delayed or incomplete, and replicas remained outdated for an extended period.
With this update, the internal ID list lookup logic used during online initialization was optimized, making it scalable even with very large datasets. As a result, replication online initialization progresses as expected on large databases.

Jira:RHEL-142980[1]

Directory Server deletes access logs as expected

Before this update, when access log compression was enabled, the log rotation logic failed to correctly recognize **.gz**-suffixed rotated access log filenames while rebuilding the internal rotation information, so compressed logs were not associated with their corresponding rotation entries. As a consequence, the **nsslapd-accesslog-list** did not contain the actual files on disk, and access logs accumulated until manual cleanup was required to prevent disks from filling.

With this update, the log rotation logic was updated to correctly parse and match rotated access log filenames regardless of whether they are compressed (with a **.gz** suffix) or uncompressed, ensuring compressed logs are included when rebuilding rotation information and validating previous log files. As a result, compressed rotated access logs are properly tracked and removed according to the configured rotation settings.

Jira:RHEL-147212[1]

Directory Server no longer fails under heavy operations involving the NDN cache

Before this update, a defect in the concread dependency used by the Named Data Networking (NDN) cache caused LinCowCell chain drops to incorrectly free shared links when multiple references existed to the same chain. As a consequence, under heavy operations involving the NDN cache, the server could hit a use-after-free condition and fail with a segmentation fault in **atomic_compare_exchange()**, leading to erratic downtime.

With this update, the **389-ds-base** package uses concread version 0.5.10, which correctly stops freeing data when a shared cache link is detected. As a result, NDN cache operations are handled safely, preventing the segmentation fault.

Jira:RHEL-152338[1]

7.10. SSSD

User creation fails with invalid**sAMAccountName** input

Before this update, user creation with, for example, a User Principal Name (UPN) format that includes the @ character instead of a **sAMAccountName** attribute, caused **adcli** to create user objects with a **sAMAccountName** which contained invalid characters. As a consequence, Active Directory (AD) operations involving that user could break. With this release, **adcli** validates the input string for user creation against a list of illegal characters before attempting to create the entry. As a result, **adcli** terminates user creation if the input is not a valid **sAMAccountName** value. This prevents the creation of malformed user objects and ensures smoother AD operation.

Jira:RHEL-134945[1]

adcli correctly identifies machine account principals in multi-realm keytabs

Before this update, when connecting to a domain to update a password, **adcli** always used the Kerberos realm of the first entry in the keytab file. As a consequence, on systems where the keytab contained multiple realms, the renewal process failed with a "no suitable keys" error if the required realm was not listed first. With this release, **adcli** searches the keytab for a principal that matches the target domain. As a result, machine account password renewals now succeed regardless of the order of entries in the keytab.

Jira:RHEL-134948[1]

adcli testjoin correctly identifies the joined domain in multi-principal keytabs

Before this update, the **adcli testjoin** command unconditionally used the domain or realm from the first entry found in the keytab file to perform its diagnostic test. As a consequence, on systems where the keytab contained principals from multiple domains, **adcli testjoin** would often attempt to connect to an incorrect domain and fail with a "Realm not local to KDC" error.

With this release, **adcli** uses the realm from the keytab as the domain name when the domain is not explicitly specified. As a result, users can reliably verify domain connectivity without encountering false authentication failures.

Jira:RHEL-134950[1]

7.11. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The **nbde_client** role correctly maintains idempotence after failed binding operations

Before this update, when the **nbde_client** system role failed to add a required binding to a LUKS-encrypted volume, the rollback mechanism did not always function correctly. This led to idempotence issues, where subsequent attempts to run the role would fail or produce unexpected results because the system was left in a partially modified state.
With this update, the role performs a backup of the LUKS header before initiating any binding operations. If an operation fails, the role uses this backup to restore the header to its original state. As a result, the role correctly maintains idempotence and ensures the system remains in a consistent state even if a binding fails to be added.

Jira:RHEL-84891

The **network** RHEL system role no longer fails to look up routing tables by name

The **/usr/share/iproute2/rt_tables** file contains certain built-in routing table names, such as **main**. Before this update, if an administrator used the **network** RHEL system role to modify the routing table and specified a routing table by its name in a playbook, the role failed with the following error:

```
cannot find route table main in /etc/iproute2/rt_tables or /etc/iproute2/rt_tables.d/
```

With this update, the **network** RHEL system role no longer fails to look up routing tables by name in **/etc/iproute2/rt_tables** and files in the **/etc/iproute2/rt_tables.d/** directory.

Jira:RHEL-112805[1]

External configuration files correctly override all the **sshd_config** options

Before this update, external configuration files were not loaded first, which prevented overrides of all options in the **sshd_config** file. Consequently, users experienced incorrect OpenSSH daemon configuration. With this update, external configuration files take priority. As a result, users can override all options in the **sshd_config** file.

Jira:RHEL-123018[1]

The **network** RHEL system role no longer reports an incorrect state when removing profiles

Before this release, when you used the **network** RHEL system role with the **persistent_state: absent** setting to remove undefined profiles, the role attempted to delete the loopback interface profile. Because the system automatically recreates this profile immediately, Ansible incorrectly reported a **changed** state. This bug fix adds the loopback device to the role-internal **black_list_names** variable. As a result, the **network** RHEL system role ignores the loopback interface. This prevents unnecessary changes and the role reports an **ok** state.

Jira:RHEL-123028[1]

Storage role no longer fails when **/etc/fstab** is missing

Before this update, the storage role crashed on systems where **/etc/fstab** was absent. As a consequence, systems without a file system table configuration experienced failures.

With this update, the storage role checks whether **/etc/fstab** exists before attempting to parse it. As a result, systems without this file no longer experience a crash when using the storage role.

Jira:RHEL-123044[1]

The **aide** system role supports dynamic database configuration for multiple AIDE versions

Before this update, the **aide** system role used the deprecated **database** variable in its templates. On systems running Advanced Intrusion Detection Environment (AIDE) version 0.17 or later, including RHEL 10.2, RHEL 9.8, and CentOS Stream 9, this caused the AIDE service to fail during configuration parsing.
With this update, the role introduces the **database_in** and **aide_version** variables to dynamically detect the installed AIDE version and apply the appropriate configuration syntax automatically.

As a result, the **aide** system role provides consistent file integrity monitoring across different releases without requiring manual configuration changes.

Jira:RHEL-129416[1]

Improved error handling for empty disk lists in **blivet**

Before this update, the code failed to check if the disks list was empty before accessing **disks[0]** in the **blivet** module. As a consequence, an unhandled **IndexError** caused playbook failures, leading to poor performance.
With this update, the module checks whether the disk list is empty before accessing it. If no disks are available, a clear error message is displayed instead of triggering an exception.

Jira:RHEL-138058[1]

vpn role generates valid **ipsec.conf** file for unmanaged hosts

Before this update, when you tried to generate an **ipsec.conf** file for VPN connection between managed and unmanaged hosts, a logic error in the Ansible Playbook caused the task to fail. With this update, the Ansible Playbook references the host and subnet information correctly.
As a result, the **vpn** system role generates a valid **ipsec.conf** file for this scenario.

Jira:RHEL-145220[1]

The **selinux** system role supports static imports even when some variables are undefined

Before this update, undefined variables, such as module paths, caused the **selinux** system role to fail during template expansion if the **import_role** directive was used. This occurred because Ansible attempts to resolve variables in task **name** fields immediately, even if those tasks are within a block with a **when** condition that evaluates to false.
With this update, task names use the **default**, or **d**, filter to provide a fallback value for potentially undefined variables. This ensures that static imports succeed without error, and dynamic usage with the **include_role** module still provides detailed task information when variables are present.

As a result, the **selinux** role functions correctly in playbooks that use the **import_role** directive even when no specific module path is defined.

Jira:RHEL-145248[1]

Fixed ZeroDivisionError when creating LVM volumes without a specified size

Before this update, creating an LVM volume without specifying a size could cause a ZeroDivisionError. This occurred because the **blivet** module treated a volume with no specified size as zero.
With this release, if you do not specify size, the volume uses all available space in the pool. As a result, LVM volumes are created successfully even when a size is omitted.

Jira:RHEL-147823[1]

The **firewall** RHEL system role installs NetworkManager on managed nodes in order for PCI interface ID lookups to work correctly

Previously, if you wanted to look up the interface name by specifying the PCI id for the interface by using the **interface_pci_id** parameter, and NetworkManager was not installed, the **firewall** RHEL system role was unable to look up the interface by PCI ID and displayed a warning. As a consequence, the role failed to configure the **firewalld** service by using the specified **interface_pci_id** variable.
With this update, the role ensures that NetworkManager is installed, and the **firewall** RHEL system role works as expected.

Jira:RHEL-150782[1]

Resolved task name expansion issues in Ansible roles

Before this update, if you used **import_role** with modules that had no path set, the role issued undefined variable errors. This occurred because Ansible attempted to expand templates in task names within a **block** regardless of the **when** conditions.
With this update, the **d** filter provides a default value for these variables. As a result, the role no longer errors with **import_role** and modules without a defined path, and continues to provide additional context in task names when used with **include_role**.

Jira:RHEL-150789[1]

Loop mount errors on RHEL 7 are resolved

Before this update, the **blivet** module called an undefined function during loop mounts on Red Hat Enterprise Linux 7 because the **libblockdev-loop** package was missing. As a consequence, the role failed with the "The function 'bd_loop_get_backing_file' called, but not implemented" error.
With this update, the **libblockdev-loop** package is installed, which prevents **blivet** errors during loop mounts on RHEL 7.

Jira:RHEL-151438[1]

7.12. VIRTUALIZATION

VMs with large memory can now boot correctly on SEV-SNP host with AMD Genoa CPUs

Previously, virtual machines (VMs) could not boot on hosts that used a 4th Generation AMD EPYC processor (also known as Genoa) and had the AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) feature enabled. Instead of booting, a kernel panic occurred in the VM. This issue has now been fixed.

Jira:RHEL-32892[1]

Post-copy migration no longer causes connection issues on IBM Z

After migrating a virtual machine (VM) between IBM Z hosts by using post-copy migration, the VM previously in some cases lost network connection and required resetting its network interface to reconnect. With this update, the kernel handles post-copy initiation properly, and the problem no longer occurs.

Jira:RHEL-43214[1]

VM migration no longer fails when using vTPM on shared storage

Before this update, when a virtual Trusted Platform Module (vTPM) data directory was stored on a shared file system, such as NFS, the system failed to create the directory on the destination host during migration, even if it did not exist. This caused virtual machine (VM) migrations to fail. With this update, the system correctly identifies missing vTPM data directories on the destination host and creates them as needed. As a result, virtual machines with a vTPM on shared storage now migrate successfully.

Jira:RHEL-108915

VMs with large memory can now boot correctly on SEV-SNP host with AMD Genoa CPUs

Previously, virtual machines (VMs) could not boot on hosts that used a 4th Generation AMD EPYC processor (also known as Genoa) and had the AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) feature enabled. Instead of booting, a kernel panic occurred in the VM. This issue has now been fixed.

Jira:RHEL-121983[1]

TDX attestation no longer requires rebooting the host

Previously, after you installed the **linux-sgx** packages on your host, Intel Trust Domain Extensions (TDX) attestation on your virtual machines (VMs) only worked after you rebooted the host. Now, the **/dev/sgx_provision** device has correct correct ownership configured after installing **linux-sgx**, and you can proceed with TDX attestation without rebooting the host.

Jira:RHEL-129059[1]

Live VM memory dumps and VM snapshots now work correctly on IBM Z

Previously, attempting to create a memory dump of a running VM by using the **virsh dump --live** command on an IBM Z host sometimes caused the VM to become unresponsive. In rare cases, creating a snapshot of a running VM can also caused the VM to become unresponsive. With this update, this issue has been fixed, and VMs on IBM Z work as expected in the described scenarios.

Jira:RHELDOCS-21707[1]

7.13. SUPPORTABILITY

Scrub non-alphanumeric passwords are available in the installer logs

Before this update, password detection was strict for obfuscating non-alphanumeric characters. With this release, password scrubbing now accepts non-alphanumeric characters. As a result, password detection no longer rejects non-alphanumeric characters, improving password input flexibility.

Jira:RHEL-121515

Improved IPv6 obfuscation for data privacy

Before this update, the netmask portion of IPv6 addresses remained visible during the data cleaning process. With this release, both the address and the netmask are properly obfuscated, preventing the accidental exposure of network topology.
Jira:RHEL-121517

The **obfuscate_file** function correctly scrubs file content

Before this update, the **obfuscate_file** function overwrote the file content with the filename, causing issues with the main archive population in the cleaner. Consequently, incorrectly overwritten file content in **sos** caused user data corruption. This update introduces the following notable enhancements:

- The **obfuscate_file** function cleans the file content instead of the filename.
- The cleaner's **main_archive** is populated by the parsers first to ensure data integrity.
- The **obfuscate_file** function does not require **short_name**. It uses an implicit value that the cleaner automatically processes.

Jira:RHEL-121531

Enhanced post processing obfuscation in OpenStack Nova

Before this update, the passwords were never scrubbed. With this update, the obfuscation is applied only to the **/var/lib/openstack/config/nova** directory and obfuscating passwords from transport URLs, not the entire URL.
Jira:RHEL-121534

Improper scrubbing fixed in **aap_containerized** to secure passwords

Before this update, the unscrubbed passwords were collected from containerized AAP deployments because of the improper scrubbing in the **aap_containerized** plugin. As a consequence, a password leak occurred in these deployments.
With this release, secret obfuscation has been added to the plugin. As a result, sensitive data is properly obfuscated in the containerized AAP deployments, reducing the risk of password leaks.

Jira:RHEL-142618

The **rhsm.service** service is running after the **sos** report execution

Before this update, the **sos** report inadvertently started **rhsm.service** service even when it was stopped. This caused the service to run in scenarios where there was no internet connection, generating error messages.
With this fix, the **sos** report no longer starts **rhsm.service** service when it is disabled, improving system stability in offline environments.

Jira:RHEL-112563

7.14. CONTAINERS

Container restart policy is applied correctly at RHEL boot with the **podman-restart.service**

In Podman version 5.8, the container restart policy was not enforced during RHEL system reboot due to an issue in Podman v5.6 and earlier.

With this fix, the issue regarding container restart with **-restart=unless-stopped** and **Podman-restart.service** has been addressed. As a result, containers with these settings can start at boot in RHEL 9.8 and later versions.

Jira:RHEL-157746[1]

Buildah and Podman no longer request multiple tokens per operation

Previously, the Buildah and Podman utilities repeatedly requested tokens during each operation. This sometimes caused a race condition in the hosted repository manager.
This update fixes the issue, which improves the performance and stability of the hosted repository manager.

Jira:RHEL-95964

7.15. RHEL LIGHTSPEED

The **lightspeed** keyword is added to**dnf** search metadata for the CLA package

Before this update, the **lightspeed** keyword was missing from the command-line assistant (CLA) package summary. As a consequence, users could not easily find the package when performing a **dnf** search. With this update, the keyword is added to the package metadata. As a result, users can now find the package by searching for **lightspeed**, which makes the CLA easier to install.
Jira:RHEL-129825

CHAPTER 8. TECHNOLOGY PREVIEWS

This part provides a list of all Technology Previews available in Red Hat Enterprise Linux 9.

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

8.1. IDENTITY MANAGEMENT

The IdM Modern Web UI is available (Technology Preview)

With this update, Identity Management (IdM) provides the Modern Web UI as a Technology Preview. This new interface features updated design and is available at the **/ipa/modern-ui** endpoint. You can access the new interface through a link on the IdM Web UI login screen.
As a Technology Preview, the Modern Web UI is under active development and intended for experimentation in non-production environments. Provide feedback at the FreeIPA Web UI community project to help improve the interface.

Jira:RHEL-134542[1]

8.2. VIRTUALIZATION

Live migration for S3-PR (Technology Preview)

As a Technology Preview, you can now live migrate a virtual machine (VM) with enabled SCSI3-Persistent Reservation (S3-PR), with the reservation state being preserved after the migration. To do this, you must use the following XML configuration for the VM:

```
<reservations managed="no" migration="yes">
```

Note, however, that migrating a VM with S3-PR and this configuration to a host that uses a previous version of QEMU fails.

Jira:RHEL-140614[1]

8.3. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.7

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.7.

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

8.3.1. Installer and image creation

Container-based deployments on s390x is now available as a Technology Preview

The RHEL installation program now supports deploying bootable containers in Image Mode on the **s390x** architectures by using the **ostreecontainer** Kickstart command as a Technology Preview. This enhancement removes previous limitations and ensures consistent deployment options across supported architectures. Users can now automate installations on **s390x** systems by using container-based workflows.
Jira:RHEL-63237

8.3.2. Security

New package: fips-provider-next (Technology Preview)

As a Technology Preview, this update adds a new FIPS provider that showcases future code before it obtains FIPS certification.

Jira:RHEL-96056[1]

8.3.3. Shells and command-line tools

RHEL 9.7 provides ReaR on aarch64 (Technology Preview)

RHEL 9.7 introduces the Relax and Recover (ReaR) package for the 64-bit ARM architecture (**aarch64**) as a Technology Preview. ReaR is a disaster recovery tool that produces a bootable image that you can use to restore the system from a backup. You can currently use the following output methods with ReaR on **aarch64**: ISO, USB, and PXE.

For more information about ReaR, see the article What is Relax and Recover(ReaR) and how to use it for disaster recovery?.

Jira:RHEL-56045[1]

8.3.4. Kernel

Boot from NVMe/TCP is available as a Technology Preview

On systems that boot from SAN over NVMe-TCP, you can use **kdump** to write crash dumps to an NVMe namespace. This update fixes failures that occurred when **kdump** attempted to dump to the NVMe namespace. As a result, panic dumps succeed on these systems, improving recovery and reducing downtime in SAN-based environments.

Jira:RHEL-33413[1]

8.3.5. File systems and storage

xfs_scrub utility is available as a Technology Preview

You can check all the metadata on a mounted XFS file system by using the **xfs_scrub** utility as a Technology Preview. It functions similarly to the **xfs_repair -n** command for an unmounted XFS filesystem. For details, see the **xfs_scrub(8)** man page on your system. Note that currently only the scrub feature is available in RHEL 10 kernels and online repair is not enabled.

Jira:RHELDOCS-21350[1]

8.3.6. Dynamic programming languages, web and database servers

A new nodejs:24 module stream is available as a Technology Preview

A new **nodejs:24** module stream is available as a Technology Preview in Red Hat Enterprise Linux 9.7. This update introduces Node.js 24, which provides new features, bug fixes, security updates, and performance improvements compared to Node.js 22 included in RHEL 9.6.
To install the **nodejs:24** module, enter:

```
# dnf module install nodejs:24
```

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

Jira:RHEL-90821

8.3.7. Identity Management

Encrypted DNS with DoT is now available in ansible-freeipa installations of IdM as a Technology Preview

You can now use Ansible to ensure that all DNS queries and responses between DNS clients and Identity Management (IdM) DNS servers are encrypted. Encrypted DNS using DNS over TLS (DoT) has been available as a Technology Preview in IdM deployments since RHEL 10. In RHEL 10.1, the functionality is available as a Technology Preview in the **freeipa.ansible_freeipa** collection.
To enable DoT during a deployment of IdM by using **ansible-freeipa** use the following options:

- **ipaserver_dns_over_tls** with the **freeipa.ansible_freeipa.ipaserver** role for a new server.
- **ipareplica_dns_over_tls** with the **freeipa.ansible_freeipa.ipareplica** role for a replica.
- **dot_forwarder** to specify an upstream DoT-enabled DNS server.
- **dns_over_tls_key** and **dns_over_tls_cert** to configure DoT certificates.

Additionally, you can set the **dns_policy** variable to enforce DoT-only communication, overriding the default behavior that allows fallback to unencrypted DNS.

Jira:RHELDOCS-20258[1]

8.3.8. Virtualization

TDX is available on RHEL hosts as a Technology Preview

As a Technology Preview, you can enable Trust Domain Extensions (TDX) on RHEL hosts. TDX is a hardware-based security feature that provides strong memory encryption and integrity protection for virtual machines, isolating them from the hypervisor and other system software.
TDX is available only with Intel CPUs.

Jira:RHEL-111840[1]

SEV-SNP is available on RHEL hosts as a Technology Preview

As a Technology Preview, you can enable Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) on RHEL hosts. SEV-SNP is a hardware-based security feature that provides strong memory encryption and integrity protection for virtual machines, isolating them from the hypervisor and other system software.
SEV-SNP is available only with AMD CPUs, and you must use the **snphost** package to configure the feature on the host.

Jira:RHELDOCS-19756[1]

8.3.9. Containers

Podman compatibility with Docker API is available as a Technology Preview

Podman supports the following Docker API versions as a Technology Preview:

- Docker API 1.41
- Docker API 1.43

Jira:RHEL-88121

8.4. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.6

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.6.

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

8.4.1. Security

Encrypted DNS in RHEL is available (Technology Preview)

You can enable encrypted DNS to secure DNS communication that uses DNS-over-TLS (DoT). Encrypted DNS (eDNS) encrypts all DNS traffic end-to-end, with no fallback to insecure protocols, and aligns with zero trust architecture (ZTA) principles.
To perform a new installation with eDNS, specify the DoT-enabled DNS server by using the kernel command line. This ensures encrypted DNS is active during the installation process, boot time, and on the installed system. If you require a custom CA certificate bundle, you can install it only by using the **%certificate** section in the Kickstart file. Currently, the custom CA bundle can be installed only through Kickstart installation.

On an existing system, configure NetworkManager to use a new DNS plugin, **dnsconfd**, which manages the local DNS resolver (unbound) for eDNS. Add kernel arguments to configure eDNS for the early boot process, and optionally install a custom CA bundle.

Additionally, Identity Management (IdM) deployments can also use encrypted DNS, with the integrated DNS server supporting DoT.

See Securing system DNS traffic with encrypted DNS for more details.

Jira:RHELDOCS-20059[1], Jira:RHEL-67913

8.4.2. Networking

kTLS was updated to version 6.12

The kernel Transport Layer Security (KTLS) functionality is a Technology Preview. In RHEL 9.6, kTLS was updated to the 6.12 upstream version.

Jira:RHELPLAN-153754[1]

8.4.3. Kernel

The Red Hat Enterprise Linux for Real Time on ARM64 is now available as a Technology Preview

With this Technology Preview, the Red Hat Enterprise Linux for Real Time is now enabled for ARM64. The ARM64 is enabled on ARM (AARCH64), for both 4k and 64k ARM kernels.

Jira:RHELDOCS-19635[1]

The Neural Processing Unit (NPU) kernel for the RHEL Kernel is available as a Technology Preview on Intel Arrow Lake-based systems

In RHEL 9.6, the kernel introduces the Neural Processing Unit (NPU) as a Technology Preview. NPUs are special chips used for artificial intelligence (AI) and machine learning (ML) tasks on the systems. The kernel in RHEL 9.6 includes the initial driver for Intel NPUs and support infrastructure required to use the NPUs for AI/ML tasks.

Jira:RHEL-38583[1]

8.4.4. File systems and storage

NVMe/TCP Boot with NBFT is available as a Technology Preview

NVMe/TCP Boot by using the NVM Express Boot Specification (NBFT) is available on select server platforms as a Technology Preview. Consult your server manufacturer for platform-specific details and compatibility information.

Jira:RHELDOCS-21587[1]

NVMe/TCP using TLS is available (Technology Preview)

Encrypting Non-volatile Memory Express (NVMe) over TCP (NVMe/TCP) network traffic using TLS configured with Pre-Shared Keys (PSK) has been added as a Technology Preview in RHEL 9.6. For instructions, see Configuring an NVMe/TCP host using TLS with Pre-Shared-Keys .

Jira:RHEL-9301[1]

8.4.5. Compilers and development tools

eu-stacktrace available as a Technology Preview

The **eu-stacktrace** utility, which has been distributed through the **elfutils** package since version 0.192, is available as a Technology Preview feature. **eu-stacktrace** is a prototype utility that uses the **elfutils** toolkit's unwinding libraries to support a sampling profiler to unwind frame pointer-less stack sample data.

Jira:RHELDOCS-19072[1]

8.4.6. Identity Management

DNS over TLS (DoT) in IdM deployments is available as a Technology Preview

Encrypted DNS using DNS over TLS (DoT) is now available as a Technology Preview in Identity Management (IdM) deployments. You can now encrypt all DNS queries and responses between DNS clients and IdM DNS servers.

To start using this functionality, install the **ipa-server-encrypted-dns** package for IdM servers and replicas, and the **ipa-client-encrypted-dns** package for IdM clients. Administrators can enable DoT during the installation using the **--dns-over-tls** option.

IdM configures Unbound as a local caching resolver and BIND to receive DoT requests. This functionality is available through the command-line interface (CLI) and non-interactive installations of IdM.

To configure DoT, new options were added to installation utilities for IdM servers, replicas, clients, and the integrated DNS service:

- **--dot-forwarder** to specify an upstream DoT-enabled DNS server.
- **--dns-over-tls-key** and **--dns-over-tls-cert** to configure DoT certificates.
- **--dns-policy** to set a DNS security policy to either allow fallback to unencrypted DNS or enforce strict DoT usage.

By default, IdM uses **relaxed** DNS policy, which allows fallback to unencrypted DNS. You can enforce encrypted-only communication using the new **--dns-policy** option with the **enforced** setting.

You can also enable DoT on an existing IdM deployment by reconfiguring the integrated DNS service using **ipa-dns-install** with the new DoT options.

See Securing DNS with DoT in IdM for more details.

Jira:RHEL-67913[1], Jira:RHELDOCS-20059

8.4.7. Virtualization

New package: trustee-guest-components (Technology Preview)

As a Technology Preview, this update adds the **trustee-guest-components** package. This makes it possible for confidential virtual machines to attest themselves and get confidential resources from a Trustee server.

Jira:RHEL-68141[1]

8.4.8. Containers

The podman artifact command is available as a Technology Preview

The **podman artifact** command, which you can use to work with OCI artifacts at the command-line level, is available as a Technology Preview. For further information, reference the man page.
Jira:RHEL-70217

8.5. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.5

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.5.

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

8.5.1. Security

OpenSSL clients can use the QUIC protocol (Technology Preview)

OpenSSL can use the QUIC transport layer network protocol on the client side with the rebase to OpenSSL version 3.2.2 as a Technology Preview.

Jira:RHELDOCS-18935[1]

8.5.2. Networking

UDP encapsulation in packet offload mode is now available as a Technology Preview

With IPsec packet offload, the kernel can offload the entire IPsec encapsulation process to a NIC to reduce the workload. With this update, the packet offload has been improved by supporting User Datagram Protocol (UDP) encapsulation of **ipsec** tunnels when in packet offload mode.

Jira:RHEL-30141[1]

8.5.3. Dynamic programming languages, web and database servers

A new nodejs:22 module stream is available as a Technology Preview

A new module stream, **nodejs:22**, is now available as a Technology Preview. A future update will provide a Long Term Support (LTS) version of **Node.js 22**, which will be fully supported. **Node.js 22** included in RHEL 9.5 provides numerous new features, bug fixes, security fixes, and performance improvements over **Node.js 20** available since RHEL 9.3.

Notable changes include:

- The **V8** JavaScript engine has been upgraded to version 12.4.
- The **V8 Maglev** compiler is now enabled by default on architectures where it is available (AMD and Intel 64-bit architectures and the 64-bit ARM architecture).
- **Maglev** improves performance for short-lived CLI programs.
- The **npm** package manager has been upgraded to version 10.8.1.
- The **node --watch** mode is now considered stable. In **watch** mode, changes in watched files cause the **Node.js** process to restart.
- The browser-compatible implementation of **WebSocket** is now considered stable and enabled by default. As a result, a WebSocket client to Node.js is available without external dependencies.
- **Node.js** now includes an experimental feature for execution of scripts from **package.json**. To use this feature, run the **node --run <script-in-package.json>** command.

To install the **nodejs:22** module stream, enter:

```
# dnf module install nodejs:22
```

If you want to upgrade from the **nodejs20** stream, see Switching to a later stream .

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

Jira:RHEL-35990

8.5.4. Containers

Partial pulls for zstd:chunked are available as a Technology Preview

You can pull only the changed parts of the container images compressed with the **zstd:chunked** format, reducing network traffic and necessary storage. You can enable partial pulls by adding the **enable_partial_images = "true"** setting to the **/etc/containers/storage.conf** file. This functionality is available as a Technology Preview.
Jira:RHEL-32267

8.6. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.4

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.4.

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

8.6.1. Installer and image creation

Boot loader installation and configuration through bootupd / bootupctl in Anaconda is now available as a Technology Preview

As the **ostreecontainer** Kickstart command is now available in Anaconda as a Technology Preview, you can use it to install the operating system from an OSTree commit encapsulated in an OCI image. Anaconda automatically arranges a boot loader installation and configuration through the **bootupd**/**bootupctl** tool contained within the container image, even without an explicit boot loader configuration in Kickstart.
Jira:RHEL-17205[1]

Installation of bootable OSTree native containers is now available as a Technology Preview

The **ostreecontainer** Kickstart command is now available in Anaconda as a Technology Preview. You can use this command to install the operating system from an OSTree commit encapsulated in an OCI image. When performing Kickstart installations, the following commands are available together with **ostreecontainer**:

- graphical, text, or cmdline
- ostreecontainer
- clearpart, zerombr
- autopart
- part
- logvol, volgroup
- reboot and shutdown
- lang
- rootpw

- sshkey
- bootloader - Available only with the **--append** optional parameter.
- user

When you specify a group within the user command, the user account can be assigned only to a group that already exists in the container image. Kickstart commands not listed here are allowed to be used with **ostreecontainer** command, however, they are not guaranteed to work as expected with package-based installations.

However, the following Kickstart commands are unsupported together with **ostreecontainer**:

- %packages (any necessary packages must be already available in the container image)
- url (if there is a need to fetch a **stage2** image for installation, for example, PXE installations, use **inst.stage2=** on the kernel instead of providing a url for **stage2** inside the Kickstart file)
- liveimg
- vnc
- authconfig and authselect (provide relevant configuration in the container image instead)
- module
- repo
- zipl
- zfcp

Installation of bootable OSTree native containers is not supported in interactive installations that use partial Kickstart files.

Note: When customizing a mount point, you must define the mount point in the **/mnt** directory and ensure that the mount point directory exists inside **/var/mnt** in the container image.

Jira:RHEL-2250[1]

NVMe over TCP for RHEL installation is now available as a Technology Preview

With this Technology Preview, you can now use NVMe over TCP volumes to install RHEL after configuring the firmware. While adding disks from the Installation Destination screen, you can select the NVMe namespaces under the NVMe Fabrics Devices section.

Jira:RHEL-10216[1]

8.6.2. Security

The io_uring interface is available (Technology Preview)

io_uring is a new and effective asynchronous I/O interface, which is now available as a Technology Preview. By default, this feature is disabled. You can enable this interface by setting the **kernel.io_uring_disabled** sysctl variable to any one of the following values:

0

All processes can create **io_uring** instances as usual.

1

io_uring creation is disabled for unprivileged processes. The **io_uring_setup** fails with the **-EPERM** error unless the calling process is privileged by the **CAP_SYS_ADMIN** capability. Existing **io_uring** instances can still be used.

2

io_uring creation is disabled for all processes. The **io_uring_setup** always fails with **-EPERM**. Existing **io_uring** instances can still be used. This is the default setting.

An updated version of the SELinux policy to enable the **mmap** system call on anonymous inodes is also required to use this feature.

By using the **io_uring** command pass-through, an application can issue commands directly to the underlying hardware, such as **nvme**.

Jira:RHEL-11792[1]

8.6.3. RHEL for Edge

FDO now provides storing and querying Ownership Vouchers from an SQL backend (Technology Preview)

With this Technology Preview, FDO Manufacturing, Owner, and Rendezvous servers are available for storing and querying Ownership Vouchers from an SQL backend (SQLite or PostgreSQL). As a result, you can select an SQL datastore in the FDO server's options, along with credentials and other parameters, to store the Ownership Vouchers.

Jira:RHELDOCS-17752[1]

8.6.4. Infrastructure services

libabigail: Flexible array conversion warning-suppression available as a Technology Preview

As a Technology Preview, when comparing binaries, you can suppress warnings related to fake flexible arrays that were converted to true flexible arrays by using the following suppression specification:

```
[suppress_type]
    type_kind = struct
    has_size_change = true
    has_strict_flexible_array_data_member_conversion = true
```

Jira:RHEL-16629[1]

8.6.5. Networking

NetworkManager and the Nmstate API support MACsec hardware offload (Technology Preview)

You can use both NetworkManager and the Nmstate API to enable MACsec hardware offload if the hardware supports this feature. As a result, you can offload MACsec operations, such as encryption, from the CPU to the network interface controller.

Note that this feature is an unsupported Technology Preview.

Jira:RHEL-24337

NetworkManager enables configuring HSR and PRP interfaces

High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) are network protocols that provide seamless failover against failure of any single network component. Both protocols are transparent to the application layer, meaning that users do not experience any disruption in communication or any loss of data, because a switch between the main path and the redundant path happens very quickly and without awareness of the user. Now it is possible to enable and configure HSR and PRP interfaces using the **NetworkManager** service through the **nmcli** utility and the DBus message system.
Jira:RHEL-5852

8.6.6. Kernel

The IAA crypto driver is now available as a Technology Preview

The Intel® In-Memory Analytics Accelerator (Intel® IAA) is a hardware accelerator that provides very high throughput compression and decompression combined with primitive analytic functions.
The **iaa_crypto** driver, which offloads compression and decompression operations from the CPU, has been introduced in RHEL 9.4 as a Technology Preview. It supports compression and decompression compatible with the DEFLATE compression standard described in RFC 1951. The **iaa_crypto** driver is designed to work as a layer underneath higher-level compression devices such as **zswap**.

For details about the IAA crypto driver, see:

- Intel® In-Memory Analytics Accelerator (Intel® IAA) User Guide
- IAA Compression Accelerator Crypto Driver

Jira:RHEL-20145[1]

python-drgn available as a Technology Preview

The **python-drgn** package brings an advanced debugging utility, which adds emphasis on programmability. You can use its Python command-line interface to debug both the live kernels and the kernel dumps. Additionally, **python-drgn** offers scripting capabilities for you to automate debugging tasks and conduct intricate analysis of the Linux kernel.

Jira:RHEL-6973[1]

8.6.7. File systems and storage

NVMe/TCP Boot is available as a Technology Preview

The Non-volatile Memory Express (NVMe) over TCP (NVMe/TCP) Boot support is available as a Technology Preview. For more information on how to boot from SAN with NVMe/TCP, consult your Storage manufacturer's UEFI firmware configuration documentation.

Jira:RHEL-10414[1]

8.6.8. The web console

The RHEL web console can now manage WireGuard connections (Technology Preview)

Starting with RHEL 9.4, you can use the RHEL web console to create and manage WireGuard VPN connections. Note that, both the WireGuard technology and its web console integration are unsupported Technology Previews.

Jira:RHELDOCS-17520[1]

8.6.9. Virtualization

CPU clusters on 64-bit ARM (Technology Preview)

As a Technology Preview, you can now create KVM virtual machines that use multiple 64-bit ARM CPU clusters in their CPU topology.

Jira:RHEL-7043[1]

8.7. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.3

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.3.

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

8.7.1. Networking

Segment Routing over IPv6 (SRv6) is available as a Technology Preview

The RHEL kernel provides Segment Routing over IPv6 (SRv6) as a Technology Preview. You can use this functionality to optimize traffic flows in edge computing or to improve network programmability in data centers. However, the most significant use case is the end-to-end (E2E) network slicing in 5G deployment scenarios. In that area, the SRv6 protocol provides you with the programmable custom network slices and resource reservations to address network requirements for specific applications or services. At the same time, the solution can be deployed on a single-purpose appliance, and it satisfies the need for a smaller computational footprint.

Jira:RHELPLAN-154595[1]

8.8. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.2

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.2.

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

8.8.1. Networking

rvu_af, rvu_nicpf, and rvu_nicvf available as Technology Preview

The following kernel modules are available as Technology Preview for Marvell OCTEON TX2 Infrastructure Processor family:

rvu_af

Marvell OcteonTX2 RVU Admin Function driver

rvu_nicpf

Marvell OcteonTX2 NIC Physical Function driver

rvu_nicvf

Marvell OcteonTX2 NIC Virtual Function driver

Jira:RHELPLAN-108169[1]

Socket API for TuneD available as a Technology Preview

The socket API for controlling TuneD through a UNIX domain socket is now available as a Technology Preview. The socket API maps one-to-one with the D-Bus API and provides an alternative communication method for cases where D-Bus is not available. By using the socket API, you can control the TuneD daemon to optimize the performance, and change the values of various tuning parameters. The socket API is disabled by default, you can enable it in the **tuned-main.conf** file.

Jira:RHELPLAN-129881[1]

8.9. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.1

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.1.

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

8.9.1. Security

gnutls now uses kTLS (Technology Preview)

The updated **gnutls** packages can use kernel TLS (kTLS) for accelerating data transfer on encrypted channels as a Technology Preview. To enable kTLS, add the **tls.ko** kernel module using the **modprobe** command, and create a new configuration file **/etc/crypto-policies/local.d/gnutls-ktls.txt** for the system-wide cryptographic policies with the following content:

```
[global]
ktls = true
```

Note that the current version does not support updating traffic keys through TLS **KeyUpdate** messages, which impacts the security of AES-GCM ciphersuites. See the RFC 7841 - TLS 1.3 document for more information.

Jira:RHELPLAN-128129[1]

8.9.2. File systems and storage

nvme-stas package is available as a Technology Preview

The **nvme-stas** package, which is a Central Discovery Controller (CDC) client for Linux, is now available as a Technology Preview. It handles Asynchronous Event Notifications (AEN), Automated NVMe subsystem connection controls, Error handling and reporting, and Automatic (**zeroconf**) and Manual configuration.

This package consists of two daemons, Storage Appliance Finder (**stafd**) and Storage Appliance Connector (**stacd**).

Jira:RHELPLAN-58357[1]

8.10. TECHNOLOGY PREVIEWS IDENTIFIED IN RHEL 9.0

This part provides a list of all Technology Preview features that were introduced in Red Hat Enterprise Linux 9.0.

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

8.10.1. Networking

Offloading IPsec encapsulation to a NIC (Technology Preview)

This update adds the IPsec packet offloading capabilities to the kernel. Previously, it was possible to only offload the encryption to a network interface controller (NIC). With this enhancement, the kernel can now offload the entire IPsec encapsulation process to a NIC to reduce the workload. Note that offloading the IPsec encapsulation process to a NIC also reduces the ability of the kernel to monitor and filter such packets.

Jira:RHEL-88552[1]

The **systemd-resolved** service (Technology Preview)

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

Jira:RHEL-88550

The Soft-iWARP driver is available as a Technology Preview

Soft-iWARP (siw) is a software, Internet Wide-area RDMA Protocol (iWARP), kernel driver for Linux. Soft-iWARP implements the iWARP protocol suite over the Internet Protocol (TCP/IP) network stack. This protocol suite is fully implemented in software and does not require a specific Remote Direct Memory Access (RDMA) hardware. Soft-iWARP enables a system with a standard Ethernet adapter to connect to an iWARP adapter or to another system with already installed Soft-iWARP.

Jira:RHELPLAN-102815[1]

8.10.2. File systems and storage

NVMe-oF Discovery Service available as a Technology Preview

The NVMe-oF Discovery Service features, defined in the NVMexpress.org Technical Proposals (TP) 8013 and 8014, are available as a Technology Preview. To preview these features, use the **nvme-cli 2.0** package and attach the host to an NVMe-oF target device that implements TP-8013 or TP-8014. For more information about TP-8013 and TP-8014, see the NVM Express 2.0 Ratified TPs from the https://nvmexpress.org/specifications/ website.

Jira:RHELPLAN-102321[1]

8.10.3. Dynamic programming languages, web and database servers

jmc-core and owasp-java-encoder available as a Technology Preview

RHEL 9 is distributed with the **jmc-core** and **owasp-java-encoder** packages as Technology Preview features for the AMD and Intel 64-bit architectures.
jmc-core is a library providing core APIs for Java Development Kit (JDK) Mission Control, including libraries for parsing and writing JDK Flight Recording files, and libraries for Java Virtual Machine (JVM) discovery through Java Discovery Protocol (JDP).

The **owasp-java-encoder** package provides a collection of high-performance low-overhead contextual encoders for Java.

Note that since RHEL 9.2, **jmc-core** and **owasp-java-encoder** are available in the CodeReady Linux Builder (CRB) repository, which you must explicitly enable. See How to enable and make use of content within CodeReady Linux Builder for more information.

Jira:RHELPLAN-88788[1]

8.10.4. Identity Management

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-121754[1]

DNSSEC available as Technology Preview in IdM

Identity Management (IdM) servers with integrated DNS now implement DNS Security Extensions (DNSSEC), a set of extensions to DNS that enhance security of the DNS protocol. DNS zones hosted on IdM servers can be automatically signed using DNSSEC. The cryptographic keys are automatically generated and rotated.
Users who decide to secure their DNS zones with DNSSEC are advised to read and follow these documents:

- DNSSEC Operational Practices, Version 2
- Secure Domain Name System (DNS) Deployment Guide
- DNSSEC Key Rollover Timing Considerations

Note that IdM servers with integrated DNS use DNSSEC to validate DNS answers obtained from other DNS servers. This might affect the availability of DNS zones that are not configured in accordance with recommended naming practices.

Jira:RHELPLAN-121751[1]

8.10.5. Desktop

GNOME for the IBM Z architecture available as a Technology Preview

The GNOME desktop environment is available for the IBM Z architecture as a Technology Preview. You can now connect to the desktop session on an IBM Z server using RDP. As a result, you can manage the server using graphical applications.

A limited set of graphical applications is available on IBM Z. For example:

- The Mozilla Firefox web browser
- Red Hat Subscription Manager (**subscription-manager-cockpit**)
- Firewall Configuration (**firewall-config**)

- Disk Usage Analyzer (**baobab**)

Using Mozilla Firefox, you can connect to the Cockpit service on the server.

Jira:RHELPLAN-27737[1]

8.10.6. Virtualization

Creating nested virtual machines (Technology Preview)

Nested KVM virtualization is provided as a Technology Preview for KVM virtual machines (VMs) running on Intel, AMD64, and IBM Z hosts with RHEL 9. With this feature, a RHEL 7, RHEL 8, or RHEL 9 VM that runs on a physical RHEL 9 host can act as a hypervisor, and host its own VMs.

Jira:RHELDOCS-17040[1]

8.10.7. Containers

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[1]

8.11. TECHNOLOGY PREVIEWS IDENTIFIED IN PREVIOUS RELEASES

This part provides a list of all Technology Preview features that were introduced in earlier Red Hat Enterprise Linux versions.

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

8.11.1. Networking

KTLS (Technology Preview)

In RHEL, 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 includes the interface for offloading TLS record encryption to Network Interface Controllers (NICs) that provides this functionality.
Note that specific uses cases of kernel TLS offload might have a higher support status.

Jira:RHEL-88551[1]

8.11.2. Desktop

GNOME for the 64-bit ARM architecture available as a Technology Preview

The GNOME desktop environment is available for the 64-bit ARM architecture as a Technology Preview.
You can now connect to the desktop session on a 64-bit ARM server using RDP. As a result, you can manage the server using graphical applications.

A limited set of graphical applications is available on 64-bit ARM. For example:

- The Mozilla Firefox web browser
- Red Hat Subscription Manager (**subscription-manager-cockpit**)
- Firewall Configuration (**firewall-config**)
- Disk Usage Analyzer (**baobab**)

Using Mozilla Firefox, you can connect to the Cockpit service on the server.

Jira:RHELPLAN-27394[1]

CHAPTER 9. DEVELOPER PREVIEW FEATURES

Review Developer Preview features that are available in Red Hat Enterprise Linux 9.8.

For information about Red Hat scope of support for Developer Preview features, see Developer Preview - Scope of Support.

9.1. RHEL LIGHTSPEED

The **linux-mcp-server** for Red Hat Enterprise Linux is available (Developer Preview)

This Developer Preview introduces the **linux-mcp-server** for Red Hat Enterprise Linux (RHEL), which is designed to bridge the gap between RHEL systems and large language models (LLMs). By using this Model Context Protocol (MCP) server, you can enable AI applications to perform context-aware troubleshooting on RHEL systems, including log and performance analysis. For more details, see Using the MCP server for RHEL to enable AI assistants to run, discover, and troubleshoot complex issues.

Jira:RHELDOCS-21153[1]

CHAPTER 10. DEPRECATED FUNCTIONALITIES

Deprecated devices are fully supported, which means that they are tested and maintained, and their support status remains unchanged within Red Hat Enterprise Linux 9. However, these devices will likely not be supported in the next major version release, and are not recommended for new deployments on the current or future major versions of RHEL.

For the most recent list of deprecated functionality within a particular major release, see the latest version of release documentation. For information about the length of support, see Red Hat Enterprise Linux Life Cycle and Red Hat Enterprise Linux Application Streams Life Cycle .

A package can be deprecated and not recommended for further use. Under certain circumstances, a package can be removed from the 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 8 but has been *removed* in RHEL 9, see Considerations in adopting RHEL 9 .

10.1. HIGH AVAILABILITY AND CLUSTERS

SCTP transport for knet is now deprecated in Corosync

Previously, the **knet** transport protocol in Corosync allowed the selection of Stream Control Transmission Protocol (SCTP), although this specific transport was not officially supported in RHEL. With this update, using SCTP for **knet** transport is officially deprecated. The option to use SCTP might be removed in a future release.

As a result, users are advised to transition to supported transport protocols. The **pcs cluster setup**, **pcs cluster link add**, and **pcs cluster link update** commands now display a warning if SCTP is specified for **knet** transport.

Jira:RHEL-126842

10.2. CONTAINERS

MySQL80, Python 3.11, Node.js 20 and `Nodejs 20 Minimal ` container images are deprecated

The **MySQL80**, **Python 3.11**, **Node.js 20** and **Nodejs 20 Minimal** container images are now deprecated and will no longer receive feature updates. To maintain support and receive new features, migrate to the **MySQL84** and **Python 3.12**. Migrate to **Node.js22** to stay on a maintained and secure version. Alternatively, migrate to **Node.js24** to receive new features for the container images.

Jira:RHELDOCS-22087[1]

10.3. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.7

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.7.

10.3.1. Security

X25519-MLKEM768 deprecated and aliased to MLKEM768-X25519 in crypto-policies

The **X25519-MLKEM768** value in system-wide cryptographic policies is deprecated and aliased to the **MLKEM768-X25519** value. This unifies the concatenation order, allowing both variants to work.
Jira:RHEL-103793

10.3.2. Networking

The BIND **auto-dnssec** parameter is deprecated

Starting with RHEL 9.7, the BIND **auto-dnssec** parameter is deprecated and will be removed in a future release. As a replacement, use the **dnssec-policy** parameter to specify a complete Key and Signing Policy (KASP) that groups all related configurations into a single, intuitive block.
For further details and information about migrating to **dnssec-policy**, see DNSSEC Key and Signing Policy in the BIND 9 upstream documentation.

Jira:RHELDOCS-21505[1]

10.3.3. Identity Management

nsslapd-subtree-rename-switch is deprecated in **389-ds-base**

Before this update, you could configure Directory Server to prevent moving entries between sub-trees in a database. Because of the stability issues, this feature is deprecated and will be removed in a future major RHEL release.
Do not use the **nsslapd-subtree-rename-switch** parameter to deactivate moving entries between sub-trees. As an alternative, you can deactivate moving the entries by creating an access control instruction (ACI).

Jira:RHELDOCS-20337[1]

10.3.4. Virtualization

Specific IBM z16 CPU features have been deprecated

With this update, the **te** and **cte** CPU features have been deprecated for IBM z16 KVM VMs. Note, however, that migrating a virtual machine with CPU model **host-model** from an IBM z16 host to an IBM z17 host does not require any adjustments to CPU feature settings.
Jira:RHEL-89415[1]

Live VM dumps have been deprecated

The **--live** option for the **virsh dump** command has become deprecated, and will be removed in a future release of RHEL. After the removal, if you attempt to create a virtual machine dump by using **virsh dump** with the **--live** option, the command will fail.
Jira:RHEL-57677

10.3.5. Containers

The nginx 1.22 container image is deprecated

Starting with RHEL 9.7, the nginx 1.22 container image is deprecated and will no longer receive feature updates.
Jira:RHELDOCS-21687

10.4. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.6

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.6.

10.4.1. Security

Keylime policy management scripts are deprecated and replaced with **keylime-policy**

In RHEL 9.6, Keylime is provided with the **keylime-policy** tool, which replaces the following policy management scripts:

- **keylime_convert_runtime_policy**
- **keylime_create_policy**
- **keylime_sign_runtime_policy**
- **create_mb_refstate**
- **create_allowlist.sh**

These scripts have been deprecated and will be removed in a future major version of RHEL.

Jira:RHELDOCS-19815[1]

10.4.2. RHEL for Edge

Ignition has been deprecated for image mode for RHEL for Edge images

The Ignition tool, used to inject the user configuration into the Simplified Installer, AMI, and VMDK RHEL for Edge images types at an early stage of the boot process, has been deprecated in RHEL 9 and might be removed in a future major release.

Jira:RHELDOCS-19754[1]

10.4.3. Subscription management

Several options of the **subscription-manager list** module are deprecated

Because Red Hat subscription services have transitioned to account-level subscription management with Simple Content Access, the following options of the **list** module are deprecated and might be removed in a future major release:

- **--afterdate**
- **--all**
- **--available**
- **--consumed**
- **--match-installed**
- **--no-overlap**
- **--ondate**

- **--pool-only**
- **--servicelevel**

For more information about these transitions, see the Transition of Red Hat's subscription services to the Red Hat Hybrid Cloud Console article.

Jira:RHEL-66122

10.4.4. Software management

The numberless %patch syntax has been deprecated

Using the **%patch** directive without a number specified as a shorthand for **%patch 0** to apply the **zero-th** patch has been deprecated. Therefore, if you want to use **%patch**, a warning message suggests you to use the explicit syntax, for example, **%patch 0** or **%patch -P 0** to apply the **zero-th** patch.

Jira:RHELDOCS-19810[1]

10.4.5. Networking

ipset has been deprecated

In RHEL 9, the **ipset** utility is deprecated and is planned to be removed in a future major release. Red Hat will provide bug fixes and support for this feature during the current release lifecycle, but this feature will no longer receive enhancements. As an alternative to **ipset**, you can use the **nftables** sets functionality instead.

Jira:RHELDOCS-20146[1]

10.4.6. File systems and storage

Support for the block translation table driver has been deprecated

Support for the block translation table driver (btt.ko) has been deprecated and will be removed in the future major RHEL release. Red Hat will provide bug fixes and support for configuring Non-Volatile Dual In-line Memory Modules (NVDIMM) namespaces by using sector mode during the current release lifecycle. However, this feature will no longer receive enhancements and will be removed.

Jira:RHELDOCS-19716[1]

The nvme_core.multipath parameter is deprecated

In RHEL 9.6, the **nvme_core.multipath** parameter is deprecated and is planned to be removed in a future release. Red Hat will provide bug fixes and support for this feature during the current release lifecycle, but this feature will no longer receive enhancements and will be removed in a future major release.

Jira:RHELDOCS-19809[1]

10.4.7. SSSD

The ad_allow_remote_domain_local_groups option has been deprecated

The **ad_allow_remote_domain_local_groups** option in **sssd.conf** has been deprecated in Red Hat Enterprise Linux (RHEL) 9.6. The **ad_allow_remote_domain_local_groups** option might be removed from a future release of RHEL.

Jira:RHELDOCS-19455[1]

10.4.8. Desktop

Firefox and Thunderbird Flatpak images have been deprecated

The **rhel9/firefox-flatpak** and **rhel9/thunderbird-flatpak** Flatpak images, which are available in RHEL 9 as Technology Previews, have been deprecated and will be replaced by their RHEL 10 versions.

Jira:RHEL-91106[1]

Evince has been deprecated

Evince, a document viewer for the GNOME desktop, has been deprecated and will be removed in a future major release.

Jira:RHELDOCS-19889[1]

power-profile-daemon is deprecated

The **power-profile-daemon** package has been deprecated and is replaced by the **tuned-ppd** package. In new installations of RHEL 9.6, the **tuned-ppd** package is installed by default.

For systems updated to RHEL 9.6 from earlier versions, **power-profile-daemon** remains installed. If your scenario requires the use of **tuned-ppd** on an updated RHEL 9.6 version, install it manually:

```
# dnf install tuned-ppd
```

To verify that the package is installed, enter the following command:

```
# rpm -q tuned-ppd
tuned-ppd-2.25.1-1.el9.noarch
```

Jira:RHEL-68152

10.4.9. Red Hat Enterprise Linux System Roles

The mssql_accept_microsoft_odbc_driver_17_for_sql_server_eula variable has been deprecated

With a future major update of RHEL, the **mssql_accept_microsoft_odbc_driver_17_for_sql_server_eula** variable will no longer be supported in the **mssql** system role because the role can now install the **odbc** driver for **mssql_tools** version 17 and 18. Therefore, you must use the **mssql_accept_microsoft_odbc_driver_for_sql_server_eula** variable without the version number instead.

Important: If you use the deprecated variable with the version number **mssql_accept_microsoft_odbc_driver_17_for_sql_server_eula**, the role notifies you to use the new variable **mssql_accept_microsoft_odbc_driver_for_sql_server_eula**. However, the deprecated variable continues to work.

Jira:RHEL-69311

10.4.10. Containers

The **rsyslog** container image has been deprecated

The **rsyslog** container image has been deprecated and will be removed in a future major release.

Jira:RHELDOCS-19523[1]

The runc container runtime has been deprecated

The **runc** is deprecated and will be removed in RHEL 10.0. The default container runtime in RHEL 9 is crun. The crun is a fast and low-memory footprint OCI container runtime written in C. The crun binary is up to 50 times smaller and up to twice as fast as the runc binary. Using crun, you can also set a minimal number of processes when running your container. The crun runtime also supports OCI hooks.

Jira:RHEL-69742

The **podman-tests** package has been deprecated

The **podman-tests** package has been deprecated.

Jira:RHEL-67859

nodejs-18 and **nodejs-18-minimal** are deprecated

The **nodejs-18** and **nodejs-18-minimal** container images are now deprecated and will no longer receive feature updates. Use **nodejs-22** and **nodejs-22-minimal** instead.

Jira:RHELDOCS-20283[1]

The **ruby-31** container image is deprecated

The **ruby-31** container image is deprecated and will no longer receive feature updates. Use the **ruby-33** container image instead.

Jira:RHELDOCS-20519[1]

php-81 container image is deprecated

The **php-81** container image is now deprecated and will no longer receive feature updates. Use **php-83** instead.

Jira:RHELDOCS-20718[1]

10.5. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.5

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.5.

10.5.1. Security

OVAL deprecated in vulnerability scanning applications

The Open Vulnerability Assessment Language (OVAL) data format, which provides declarative security data processed by the OpenSCAP suite, is deprecated and will be removed in a future major release. Red Hat continues to provide declarative security data in the Common Security Advisory Framework (CSAF) format, which is the successor of OVAL.

For more information, see the OVAL v2 Announcement.

Alternatively, you can us Red Hat Lightspeed for RHEL vulnerability service, for more information, follow Assessing and Monitoring Security Vulnerabilities on RHEL Systems .

Jira:RHELDOCS-17532[1]

libgcrypt is deprecated

The Libgcrypt cryptographic library provided by the **libgcrypt** package is deprecated and may be removed in a future major release. Instead, use the libraries listed in the RHEL core cryptographic components article (Red Hat Knowledgebase).

Jira:RHELDOCS-17508[1]

fips-mode-setup is deprecated

The **fips-mode-setup** tool, which switches the system to FIPS mode, is deprecated in RHEL 9. You can still use the **fips-mode-setup** command to check whether FIPS mode is enabled.

To operate a system compliant with FIPS 140, install a system in FIPS mode in one of the following ways:

- Add the **fips=1** option to the kernel command line during the RHEL installation. See the Customizing boot options chapter in the Interactively installing RHEL from installation media document for more information.
- Create a FIPS-enabled image with RHEL image builder by adding the **fips=yes** directive to the **[customizations]** section of its blueprint.
- Create a disk image with the **bootc-image-builder** tool or install the system by using the **bootc install-to-disk** tool with a Containerfile that follows the example in the *Using image mode for RHEL* document to add the **fips=1** kernel command line flag and switch the system-wide cryptographic policy to **FIPS**.

The **fips-mode-setup** tool will be removed in the next major release.

Jira:RHELDOCS-19284

Using **update-ca-trust** without arguments is deprecated

Previously, the command **update-ca-trust** updated the system certificate authority (CA) store regardless of the arguments entered. This update introduces the **extract** subcommand for updating the CA store. You can also specify the location to which the CA certificates are extracted by using the **--output** argument. For compatibility with earlier versions of RHEL, entering **update-ca-trust** to update the CA store with any argument other than **-o** or **--help**, and even without any argument, is still supported for the duration of RHEL 9, but will be removed by the next major release. Update your calls to **update-ca-trust extract**.

Jira:RHEL-54695[1]

CAfile pointing to trusted root certificate files in Stunnel clients is deprecated

If Stunnel is configured in client mode, the **CAfile** directive can point to a file that contains trusted root certificates in the **BEGIN TRUSTED CERTIFICATE** format. This method is deprecated and might be removed in a future major version. In a future version, **stunnel** will pass the value of the

CAfile directive to a function that does not support the **BEGIN TRUSTED CERTIFICATE** format. As a consequence, if you use **CAfile = /etc/pki/tls/certs/ca-bundle.trust.crt**, change the location to **CAfile = /etc/pki/tls/certs/ca-bundle.crt**.

Jira:RHEL-52317[1]

DSA and SEED algorithms have been deprecated in NSS

The Digital Signature Algorithm (DSA), which was created by the National Institute of Standards and Technology (NIST) and is now completely deprecated by NIST, is deprecated in the Network Security Services (NSS) cryptographic library. You can instead use algorithms such as RSA, ECDSA, and EdDSA.
The SEED algorithm, which was created by the Korea Information Security Agency (KISA) and has been previously disabled upstream, is deprecated in the NSS cryptographic library.

Jira:RHELDOCS-19004[1]

pam_ssh_agent_auth is deprecated

The **pam_ssh_agent_auth** package is deprecated and might be removed in a future major release.

Jira:RHELDOCS-18312[1]

compat-openssl11 is deprecated

The compatibility library for OpenSSL 1.1, **compat-openssl11**, is now deprecated, and it might be removed in a future major release. OpenSSL 1.1 is no longer maintained upstream and applications that use the OpenSSL TLS toolkit should be migrated to version 3.x.

Jira:RHELDOCS-18480[1]

SHA-1 is deprecated at **SECLEVEL=2** in OpenSSL

The use of the SHA-1 algorithm at **SECLEVEL=2** is deprecated in OpenSSL and might be removed in a future major release.

Jira:RHELDOCS-18701[1]

OpenSSL Engines API is deprecated in Stunnel

The use of the OpenSSL Engines API in Stunnel is deprecated and will be removed in a future major release. The most common use is to access hardware security tokens that use PKCS#11 through the **openssl-pkcs11** package. As a replacement, you can use **pkcs11-provider**, which uses the new OpenSSL Providers API.

Jira:RHELDOCS-18702[1]

OpenSSL Engines are deprecated

OpenSSL Engines are deprecated and will be removed in the near future. Instead of using engines, you can use the **pkcs11-provider** as a replacement.

Jira:RHELDOCS-18703[1]

DSA is deprecated in GnuTLS

The Digital Signature Algorithm (DSA) is deprecated in the GnuTLS secure communications library and will be removed in a future major version of RHEL. DSA was previously deprecated by the

National Institute of Standards and Technology (NIST), and is not considered secure. You can use ECDSA instead to ensure compatibility with future versions.

Jira:RHELDOCS-19224[1]

scap-workbench is deprecated

The **scap-workbench** package is deprecated. The **scap-workbench** graphical utility was designed to perform configuration and vulnerability scans on a single local or remote system. As an alternative, you can scan local systems for configuration compliance by using the **oscap** command and remote systems by using the **oscap-ssh** command. For more information, see Configuration compliance scanning.

Jira:RHELDOCS-19028[1]

oscap-anaconda-addon is deprecated

The **oscap-anaconda-addon**, which provided means to deploy baseline-compliant RHEL systems by using the graphical installation, is deprecated. As an alternative, you can build RHEL images that comply with a specific standard by Creating pre-hardened images with RHEL image builder OpenSCAP integration.

Jira:RHELDOCS-19029[1]

10.5.2. Subscription management

Several **subscription-manager** modules have been deprecated

Because of a simplified customer experience in Red Hat subscription services, which have transitioned to the Red Hat Hybrid Cloud Console and to account level subscription management with Simple Content Access, the following modules have been deprecated and will be removed in a future major release:

- **addons**
- **attach**
- **auto-attach**
- **import**
- **remove**
- **redeem**
- **role**
- **service-level**
- **syspurpose addons**
- **usage** For more information about these transitions, see the Transition of Red Hat's subscription services to the Red Hat Hybrid Cloud Console article.

Jira:RHEL-29178

10.5.3. Software management

The DNF **debug** plug-in has been deprecated

The DNF **debug** plug-in, which includes the **dnf debug-dump** and **dnf debug-restore** commands, has been deprecated and will be removed from the **dnf-plugins-core** package in the next major RHEL release.

Jira:RHELDOCS-18592[1]

The support for **libreport** has been deprecated

The support for the **libreport** library has been deprecated and will be removed from DNF in the next major RHEL release.

Jira:RHELDOCS-18593[1]

10.5.4. Infrastructure services

Various packages are now deprecated in infrastructure services

The following packages are deprecated in RHEL 9 and will not be distributed in later major versions of RHEL:

- **sendmail**
- **libotr**
- **mod_security**
- **spamassassin**
- **redis**
- **dhcp**
- **xsane**

Jira:RHEL-22385[1]

10.5.5. Networking

The Soft-iWARP driver is deprecated

RHEL 9 provides the Soft-iWARP driver as an unsupported Technology Preview. Starting with RHEL 9.5, this driver is deprecated and will be removed in RHEL 10.

Jira:RHELDOCS-18699[1]

The **dhcp-client** package is deprecated

Previously, you could configure NetworkManager in RHEL 9 to use a DHCP client from the **dhcp-client** package. However, the option to use the **dhclient** utility is now deprecated and results in a warning being displayed at the NetworkManager startup. To configure NetworkManager as described above, switch to the internal DHCP library. In RHEL 10, the **dhcp-client** package is no longer available and the applications configured to use the **dhclient** utility use the internal DHCP library instead.

Jira:RHEL-24622

The perl(Mail::Sender) module is now deprecated

The **perl(Mail::Sender)** module is now deprecated and will be removed from the next major release without any replacement. As a result, the **checkbandwidth** script from **net-snmp-perl** package does not support email alerts when bandwidth high/low levels for a host or interface are reached.

Jira:RHELDOCS-18959[1]

10.5.6. File systems and storage

Support for NVMe devices has been deprecated from the lsscsi package

Support for Non-volatile Memory Express (NVMe) devices has been deprecated and will be removed from the **lsscsi** package in the future major RHEL release. Use native tools such as **nvme-cli**, **lsblk**, and **blkid** instead.

Jira:RHELDOCS-19068[1]

Support for NVMe devices has been deprecated from the sg3_utils package

Support for Non-volatile Memory Express (NVMe) devices has been deprecated and will be removed from the **sg3_utils** package in the future major RHEL release. You can use native tools (**nvme-cli**) instead.

Jira:RHELDOCS-19069[1]

10.5.7. High availability and clusters

Deprecated high availability features

The following features were deprecated as of Red Hat Enterprise Linux 9.5 and will be removed in the next major release. The **pcs** command-line interface produces a warning when you attempt to configure a system with these features.

- Configuring a **score** parameter in order constraints
- Use of the **rkt** container engine in bundles
- Support for **upstart** and **nagios** resources
- The **monthdays**, **weekdays**, **weekyears**, **yearsdays** and **moon** date specification options for configuring Pacemaker rules
- The **yearsdays** and **moon** duration options for configuring Pacemaker rules

Jira:RHEL-34781

Resilient Storage Add-On has been deprecated

The Red Hat Enterprise Linux (RHEL) Resilient Storage Add-On has been deprecated as of RHEL 9. The Resilient Storage Add-On will no longer be supported starting with Red Hat Enterprise Linux 10 and any subsequent releases after RHEL 10. The RHEL Resilient Storage Add-On will continue to be supported with earlier versions of RHEL (7, 8, 9) and throughout their respective maintenance support lifecycles.

Jira:RHELDOCS-19022[1]

10.5.8. Compilers and development tools

Redis will be replaced withValkey in Grafana, PCP, andgrafana-pcp

The **Redis** key-value store has been deprecated and will be replaced with **Valkey** in the next major version of RHEL. As a result, **Grafana**, PCP, and the **grafana-pcp** plug-in will use **Valkey** to store data instead of **Redis** in RHEL 10.

Jira:RHELDOCS-18207[1]

HTML content of**llvm-doc** is deprecated

The HTML content of the **llvm-doc** package will be removed in a future RHEL release and replaced with a single HTML file pointing to online documentation at llvm.org. Users of **llvm-doc** that do not have network access will need an alternative way to access LLVM documentation.

Jira:RHELDOCS-19013[1]

10.5.9. Identity Management

The **pam_console** module is deprecated

In RHEL 9.5, the **pam_console** module is deprecated and is planned to be removed in a future release. The **pam_console** module grants file permissions and authentication capabilities to users logged in at the physical console or terminals, and adjusts these privileges based on console login status and user presence. As an alternative to **pam_console**, you can use the **systemd-logind** system service instead. For configuration details, see the **logind.conf(5)** man page.

Jira:RHELDOCS-18158[1]

10.5.10. SSSD

The **sss_ssh_knownhostsproxy** tool has been deprecated

The **sss_ssh_knownhostsproxy** has been deprecated and will be replaced by a more efficient tool in RHEL 10. **sss_ssh_knownhostsproxy** will be kept for backwards compatibility in RHEL 9 and will be removed in RHEL 10. Support for the ssh **KnownHostsCommand** option will be added in a future release.

Jira:RHELDOCS-19115[1]

10.5.11. Desktop

Totem media player has been deprecated

The Totem media player has been deprecated in RHEL 9.5 and will be removed in a future major release.

Jira:RHELDOCS-19050[1]

power-profiles-daemon has been deprecated

The **power-profiles-daemon** package that provides the power mode configuration in GNOME has been deprecated and will be removed in a future major release.
You can use Tuned as a replacement for power mode configuration in GNOME. You can use the **tuned-ppd** API translation daemon as a drop-in replacement for **power-profiles-dameon**.

Jira:RHELDOCS-19093[1]

gedit is deprecated

gedit, the default graphical text editor in Red Hat Enterprise Linux, has been deprecated and will be removed in a future major release. Instead, use GNOME Text Editor.

Jira:RHELDOCS-19149[1]

Qt 5 libraries have been deprecated

Qt 5 libraries have been deprecated and will be removed in a future major release. Qt 5 libraries are replaced with Qt 6 libraries, with new functionality and better support.
For more information, see Porting to Qt 6.

Jira:RHELDOCS-19133[1]

WebKitGTK has been deprecated

The WebKitGTK web browser engine has been deprecated and will be removed in a future major release.
As a consequence, you will no longer be able to build applications that depend on WebKitGTK. Desktop applications other than Mozilla Firefox can no longer display web content. There is no alternative web browser engine provided in RHEL 10.

Jira:RHELDOCS-19171[1]

Evolution has been deprecated

Evolution is a GNOME application that provides integrated email, calendar, contact management, and communications functionality. The application and its plugins has been deprecated and will be removed in a future major version. You can find an alternative in a third party source, for example on Flathub.

Jira:RHELDOCS-19147[1]

Festival has been deprecated

The Festival speech synthesizer has been deprecated and will be removed in a future major version. As an alternative, you can use the Espeak NG speech synthesizer.

Jira:RHELDOCS-19139[1]

The Eye of GNOME has been deprecated

The Eye of GNOME (**eog**) image viewer application has been deprecated in RHEL 9.
As an alternative, you can use the Loupe application.

Jira:RHELDOCS-19135[1]

Cheese has been deprecated

The Cheese camera application has been deprecated and will be removed in a future major version. As an alternative, you can use the Snapshot application.

Jira:RHELDOCS-19137[1]

Devhelp has been deprecated

Devhelp, a graphical developer tool for browsing and searching API documentation, has been deprecated and will be removed in a future major version. You can now find API documentation online in specific upstream projects.

Jira:RHELDOCS-19154[1]

gtkmm based on GTK 3 has been deprecated

gtkmm is a C++ interface for the GTK graphical toolkit. The **gtkmm** version that was based on GTK 3 has been deprecated with all its dependencies and will be removed in a future major version. To access **gtkmm** in RHEL 10, migrate to the **gtkmm** version based on GTK 4.

Jira:RHELDOCS-19143[1]

Inkscape has been deprecated

The Inkscape vector graphics editor has been deprecated and will be removed in a future major version.

Jira:RHELDOCS-19151[1]

10.5.12. Graphics infrastructures

The PulseAudio daemon is deprecated

The PulseAudio daemon, and its packages **pulseaudio** and **alsa-plugins-pulseaudio**, have been deprecated and will be removed in a future major release.
Note that the PulseAudio client libraries and tools are not deprecated, this change only impacts the audio daemon that runs on the system.

You can use the PipeWire audio system as a replacement, which has also been the default audio daemon since RHEL 9.0. PipeWire also provides an implementation of the PulseAudio APIs.

Jira:RHELDOCS-19080[1]

10.5.13. Red Hat Enterprise Linux System Roles

Deprecated variables in the **podman** RHEL system role: **container_image_user** and **container_image_password**

The **container_image_user** and **container_image_password** variables are deprecated. In a future major release of RHEL, these variables will be removed. You can use the **podman_registry_username** and **podman_registry_password** variables instead.
For more details, see the resources in the **/usr/share/doc/rhel-system-roles/podman/** directory.

Jira:RHELDOCS-18803[1]

10.5.14. Virtualization

NIC device drivers related to iPXE are deprecated in RHEL 9

Internet Preboot eXecution Environment (iPXE) firmware provides a range of boot options over a network often used in environments, where machines need to boot remotely. Among others, it contains a large number of device drivers. The following have been marked as deprecated and will be removed in the RHEL 10 release:

- The complete **ipxe-roms** sub-RPM package
- Binary files containing device drivers from **ipxe-bootimgs-x86** sub-RPM package:
  - **/usr/share/ipxe/ipxe-i386.efi**
  - **/usr/share/ipxe/ipxe-x86_64.efi**
  - **/usr/share/ipxe/ipxe.dsk**
  - **/usr/share/ipxe/ipxe.iso**
  - **/usr/share/ipxe/ipxe.lkrn**
  - **/usr/share/ipxe/ipxe.usb**

Instead, iPXE now depends on the platform firmware to provide a NIC driver for the network boot. The **/usr/share/ipxe/ipxe-snponly-x86_64.efi** and **/usr/share/ipxe/undionly.kpxe** iPXE binary files are the part of the **ipxe-bootimgs** package and use the NIC driver provided by the platform firmware.

Jira:RHELDOCS-18531

Converting Xen virtual machines from RHEL 5 by using**virt-v2v** has been deprecated.

Using the **virt-v2v** tool to convert virtual machines from a RHEL 5 Xen host to KVM has become deprecated, and will be removed in a future major release of RHEL. For details, see the Red Hat Knowledge Base.

Jira:RHELDOCS-19193[1]

10.5.15. Containers

The Podman v5.0 deprecations

In RHEL 9.5, the following is deprecated in Podman v5.0:

- The system connections and farm information stored in the **containers.conf** file are now read-only. The system connections and farm information will now be stored in the **podman.connections.json** file, managed only by Podman. Podman continues to support the old configuration options such as **[engine.service_destinations]** and the **[farms]** section. You can still add connections or farms manually if needed; however, it is not possible to delete a connection from the **containers.conf** file with the **podman system connection rm** command.
- The **slirp4netns** network mode is deprecated and will be removed in a future major release of RHEL. The **pasta** network mode is the default network mode for rootless containers.

- The cgroups v1 for rootless containers is deprecated and will be removed in a future major release of RHEL.

Jira:RHELDOCS-19021[1]

The **runc** container runtime has been deprecated

The **runc** container runtime is deprecated and will be removed in a future major release of RHEL. The default container runtime is **crun**.

Jira:RHELDOCS-19012[1]

10.6. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.4

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.4.

10.6.1. Installer and image creation

Anaconda built-in help has been deprecated

The built-in documentation from spokes and hubs of all Anaconda user interfaces, which is available during Anaconda installation, has been deprecated. As a replacement, the Anaconda user interfaces will be self-descriptive and users can refer to the official RHEL documentation in future major RHEL releases.

Jira:RHELDOCS-17309[1]

Support for NVDIMM devices has been deprecated

Previously, the installation program allowed reconfiguring NVDIMM devices during installation. This support for NVDIMM devices during the Kickstart and GUI installation has been deprecated, and will be removed in the next major RHEL release. The NVDIMM devices in the sector mode will still be visible and usable in the installation program.
Jira:RHELDOCS-17702

10.6.2. Security

OpenSSL deprecates the Engines API

The OpenSSL 3.0 TLS toolkit deprecated the Engines API. The Engines interface is superseded by the Providers API. The migration of applications and existing engines to Providers is underway. The deprecated Engines API may be removed in a future major release.

Jira:RHELDOCS-17958[1]

openssl-pkcs11 is now deprecated

As a part of the ongoing migration of deprecated OpenSSL engines to the Providers API, the **pkcs11-provider** package replaces the **openssl-pkcs11** package (**engine_pkcs11**). The **openssl-pkcs11** package is now deprecated. The **openssl-pkcs11** package may be removed in a future major release.

Jira:RHELDOCS-16716[1]

RHEL 8 and 9 OpenSSL certificate and signing containers are now deprecated

The OpenSSL portable certificate and signing containers available in the **ubi8/openssl** and **ubi9/openssl** repositories in the Red Hat Ecosystem Catalog are now deprecated due to low demand.

Jira:RHELDOCS-17974[1]

10.6.3. Shells and command-line tools

The %vmeff metric from the sysstat package has been deprecated

The **%vmeff** metric from the **sysstat** package to measure the page reclaim efficiency will no longer be supported in a future major version of RHEL. The values of the **%vmeff** column returned by the **sar -B** command are incorrect because **sysstat** does not parse all relevant **/proc/vmstat** values provided by later kernel versions.
You can calculate the **%vmeff** value manually from the **/proc/vmstat** file. For details, see Why the **sar(1)** tool reports **%vmeff** values beyond 100 % in RHEL 8 and RHEL 9?

Jira:RHELDOCS-17015[1]

cgroupsv1 is now deprecated in RHEL 9

The **cgroups** is a kernel subsystem used for process tracking, system resource allocation and partitioning. Systemd service manager supports booting in the cgroups **v1** mode as well as in cgroups **v2** mode. In Red Hat Enterprise Linux 9, the default mode is **v2**. In Red Hat Enterprise Linux 10, systemd will not support booting in the cgroups **v1** mode and only cgroups **v2** mode will be available.

Jira:RHELDOCS-17545[1]

10.6.4. Networking

The firewalld lockdown feature is deprecated.

The lockdown feature in **firewalld** is deprecated because it cannot prevent processes that are running as **root** from adding themselves to the allow list. The lockdown feature may be removed in a future major RHEL release.
Jira:RHEL-17708

The connection.master, connection.slave-type, and connection.autoconnect-slaves properties are deprecated

Red Hat is committed to using conscious language. Therefore, the **connection.master**, **connection.slave-type**, and **connection.autoconnect-slaves** properties were renamed. To ensure backward compatibility, aliases have been created that map the old property names to the new ones:

- **connection.master** is an alias for **connection.controller**
- **connection.slave-type** is an alias for **connection.port-type**
- **connection.autoconnect-slaves** is an alias for **connection.autoconnect-ports**

Note that the **connection.master**, **connection.slave-type**, and **connection.autoconnect-slaves** aliases are deprecated and will be removed in a future RHEL version.

Jira:RHEL-17619[1]

Client-side and server-side DHCP packages are deprecated

Internet Systems Consortium (ISC) has announced the end of maintenance for ISC DHCP as of the end of 2022. As a result, Red Hat has decided to deprecate the use of client-side and server-side DHCP packages in RHEL 9 and not to distribute them in later major versions of RHEL. Customers must prepare for the transition to available alternatives, such as **dhcpcd** and **ISC Kea**.

Jira:RHELDOCS-17135[1]

10.6.5. File systems and storage

The **md-linear**, **md-faulty**, and **md-multipath** modules have been deprecated

The following MD RAID kernel modules have been deprecated and will be removed in a future major RHEL release:

- **CONFIG_MD_LINEAR** or **md-linear** to concatenate multiple drives so that when a single member disk becomes full, data are written to the next disk until all disks are full.
- **CONFIG_MD_FAULTY** or **md-faulty** to test a block device that occasionally returns read or write errors.
- **CONFIG_MD_MULTIPATH** or **md-multipath** to take advantage of hardware supporting more than one I/O path to individual LUNs (disk drives). **md-multipath** allows the data availability in case of a hardware failure or individual path saturation.

Jira:RHEL-30730[1]

The VDO **sysfs** parameters have been deprecated

The Virtual Data Optimizer (VDO) **sysfs** parameters have been deprecated and will be removed in a future major RHEL release. Except for **log_level**, all module-level **sysfs** parameters for the **kvdo** module will be removed. For individual **dm-vdo** targets, all **sysfs** parameters specific to VDO will also be removed. There is no change for the parameters that are common to all DM targets.
Configuration values for **dm-vdo** targets, which are currently set by updating the removed module-level parameters, can no longer be changed.
Statistics and configuration values for **dm-vdo** targets will no longer be accessible through **sysfs**. But these values are still accessible by using **dmsetup message stats**, **dmsetup status**, and **dmsetup table** dmsetup commands

Jira:RHEL-30525

10.6.6. Compilers and development tools

32-bit packages are deprecated

Linking against 32-bit multilib packages is deprecated. The ***.i686** packages will remain supported for the life cycle of Red Hat Enterprise Linux 9, but will be removed in the next major version of RHEL.

Jira:RHELDOCS-17917[1]

10.6.7. SSSD

The **enumeration** feature has been deprecated for AD and IdM

The **enumeration** feature enables you to list all users or groups by using **getent passwd** or **getent group** commands without arguments for Active Directory (AD), Identity Management (IdM), and LDAP providers. Support for the **enumeration** feature has been deprecated for AD and IdM in Red Hat Enterprise Linux (RHEL) 9. The **enumeration** feature will be removed for AD and IdM in RHEL 10.

Jira:RHELDOCS-22204[1]

The libsss_simpleifp subpackage has been deprecated

The **libsss_simpleifp** subpackage that provides the **libsss_simpleifp.so** library has been deprecated in Red Hat Enterprise Linux (RHEL) 9. The **libsss_simpleifp** subpackage might be removed from a future release of RHEL.

Jira:RHELDOCS-22205[1]

10.6.8. Desktop

TigerVNC is deprecated

The TigerVNC remote desktop solution is now deprecated. It will be removed in a future major RHEL release and replaced by a different remote desktop solution.
TigerVNC provides the server and client implementation of the Virtual Network Computing (VNC) protocol in RHEL 9.

The following packages are deprecated:

- **tigervnc**
- **tigervnc-icons**
- **tigervnc-license**
- **tigervnc-selinux**
- **tigervnc-server**
- **tigervnc-server-minimal**
- **tigervnc-server-module**

The **Connections** application (**gnome-connections**) continues to be supported as an alternative VNC client, but it does not provide a VNC server.

Jira:RHELDOCS-17782[1]

10.6.9. Virtualization

Using Windows Server 2012 or Windows 8 as a guest operating system is not supported

Because Microsoft ended support for the following versions of Windows, Red Hat has also removed support for using these versions as a guest operating system.

- Windows 8
- Windows 8.1

- Windows Server 2012
- Windows Server 2012 R2

Jira:RHEL-11810

Internal snapshots for VMs have been deprecated

Creating and reverting to a virtual machine (VM) snapshot has become deprecated for snapshots that use the *internal* snapshot mechanism, and will be removed in a future major release of RHEL. Instead, use snapshots with the *external* mechanism.
For more information, see Support limitations for virtual machine snapshots .

Jira:RHELDOCS-20135[1]

pmem device passthrough has become deprecated

With this update, the non-volatile memory library (**nvml**) packages have become deprecated, and will be removed in a future major version of RHEL. As a consequence, when the package removal occurs, it will no longer be possible to pass persistent memory (**pmem**) devices to the virtual machines (VMs). Note that emulated NVDIMM devices backed by volatile memory or files will still be available, but will not be possible to configure as persistent.
Jira:RHELDOCS-17989

10.6.10. Containers

pasta as a network name has been deprecated

The support for **pasta** as a network name value is deprecated and will not be accepted in the next major release of Podman, version 5.0. You can use the **pasta** network name value to create a unique network mode within Podman by employing the **podman run --network** and **podman create --network** commands.

Jira:RHELDOCS-17038[1]

The BoltDB database backend has been deprecated

The BoltDB database backend is deprecated as of RHEL 9.4. In a future version of RHEL, the BoltDB database backend will be removed and will no longer be available to Podman. For Podman, use the SQLite database backend, which is now the default as of RHEL 9.4.

Jira:RHELDOCS-17495[1]

The Podman v5.0 upcoming deprecations

The following will be deprecated in the upcoming Podman v5.0, which will be released in RHEL 9.5 and RHEL 10.0 Beta:

- The BoltDB database backend will be deprecated. The new SQLite database backend is available.
- The **containers.conf** file will be read-only. The system connections and farm information will be stored in the **podman.connections.json** file, managed only by Podman. Podman continues to support the old configuration options such as **[engine.service_destinations]**

and the **[farms]** section. You can still add connections or farms manually if needed, however, it is not possible to delete a connection from the **containers.conf** file with the **podman system connection rm** command.

The following changes are planned for RHEL 10.0 Beta:

- The **pasta** network mode will be the default network mode for rootless containers. The **slirp4netns** network mode will be deprecated.
- The cgroupv1 will be deprecated.
- The CNI network stack will be deprecated.

Jira:RHELDOCS-17462[1]

The **rhel9/openssl** has been deprecated

The **rhel9/openssl** container image has been deprecated.

Jira:RHELDOCS-18106[1]

10.7. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.3

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.3.

10.7.1. Installer and image creation

The **initial-setup** package now has been deprecated

The **initial-setup** package has been deprecated in Red Hat Enterprise Linux 9.3 and will be removed in the next major RHEL release. As a replacement, use **gnome-initial-setup** for the graphical user interface.

Jira:RHELDOCS-16393[1]

The **provider_hostip** and **provider_fedora_geoip** values of the **inst.geoloc** boot option are deprecated

The **provider_hostip** and **provider_fedora_geoip** values that specified the GeoIP API for the **inst.geoloc=** boot option are deprecated. As a replacement, you can use the **geolocation_provider=URL** option to set the required geolocation in the installation program configuration file. You can still use the **inst.geoloc=0** option to disable the geolocation.

Jira:RHELPLAN-168262[1]

10.7.2. Networking

The **PF_KEYv2** kernel API is deprecated

Applications can configure the kernel's IPsec implementation by using the **PV_KEYv2** and the newer **netlink** API. **PV_KEYv2** is not actively maintained upstream and misses important security features, such as modern ciphers, offload, and extended sequence number support. As a result, starting with RHEL 9.3, the **PV_KEYv2** API is deprecated and will be removed in the next major RHEL release. If you use this kernel API in your application, migrate it to use the modern **netlink** API as an alternative.

Jira:RHEL-1015[1]

10.7.3. File systems and storage

Persistent Memory Development Kit (pmdk) and support library have been deprecated in RHEL 9

pmdk is a collection of libraries and tools for System Administrators and Application Developers to simplify managing and accessing persistent memory devices. **pmdk** and support library have been deprecated in RHEL 9. This also includes the **-debuginfo** packages.
The following list of binary packages produced by **pmdk**, including the **nvml** source package have been deprecated:

- **libpmem**
- **libpmem-devel**
- **libpmem-debug**
- **libpmem2**
- **libpmem2-devel**
- **libpmem2-debug**
- **libpmemblk**
- **libpmemblk-devel**
- **libpmemblk-debug**
- **libpmemlog**
- **libpmemlog-devel**
- **libpmemlog-debug**
- **libpmemobj**
- **libpmemobj-devel**
- **libpmemobj-debug**
- **libpmempool**
- **libpmempool-devel**
- **libpmempool-debug**
- **pmempool**
- **daxio**
- **pmreorder**
- **pmdk-convert**

- **libpmemobj++**
- **libpmemobj++-devel**
- **libpmemobj++-doc**

Jira:RHELDOCS-16432[1]

10.7.4. Desktop

The Inkscape and LibreOffice Flatpak images are deprecated

The **rhel9/inkscape-flatpak** and **rhel9/libreoffice-flatpak** Flatpak images, which are available as Technology Previews, have been deprecated.
Red Hat recommends the following alternatives to these images:

- To replace **rhel9/inkscape-flatpak**, use the **inkscape** RPM package.
- To replace **rhel9/libreoffice-flatpak**, see the LibreOffice deprecation release note.

Jira:RHELDOCS-17102[1]

10.7.5. Graphics infrastructures

The Intel vGPU feature has been removed

Previously, as a Technology Preview, it was possible to divide a physical Intel GPU device into multiple virtual devices referred to as **mediated devices**. These mediated devices could then be assigned to multiple virtual machines (VMs) as virtual GPUs. As a result, these VMs shared the performance of a single physical Intel GPU, however only selected Intel GPUs were compatible with this feature.
Since RHEL 9.3, the Intel vGPU feature has been removed entirely.

Jira:RHELPLAN-157294[1]

10.8. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.2

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.2.

10.8.1. Security

OpenSSL requires padding for RSA encryption in FIPS mode

OpenSSL no longer supports RSA encryption without padding in FIPS mode. RSA encryption without padding is uncommon and is rarely used. Note that key encapsulation with RSA (RSASVE) does not use padding but is still supported.

Jira:RHELPLAN-148207[1]

OpenSSL rejects RSA signatures with X9.31 padding in FIPS mode

Because X9.31 RSA signatures were removed from the FIPS 186-5 standard, OpenSSL no longer supports signing or signature verification with RSA keys with X9.31 padding in FIPS mode.

Jira:RHELPLAN-139207[1]

10.8.2. Shells and command-line tools

The **dump** utility from the **dump** package has been deprecated

The **dump** utility used for backup of file systems has been deprecated and will not be available in RHEL 9.
In RHEL 9, Red Hat recommends using the **tar**, **dd**, or **bacula**, backup utility, based on type of usage, which provides full and safe backups on ext2, ext3, and ext4 file systems.

Note that the **restore** utility from the **dump** package remains available and supported in RHEL 9 and is available as the **restore** package.

Jira:RHELPLAN-94704[1]

The SQLite database backend in Bacula has been deprecated

The Bacula backup system supported multiple database backends: PostgreSQL, MySQL, and SQLite. The SQLite backend has been deprecated and will become unsupported in a later release of RHEL. As a replacement, migrate to one of the other backends (PostgreSQL or MySQL) and do not use the SQLite backend in new deployments.
Jira:RHEL-6856

10.8.3. Kernel

The **kexec_load** system call for **kexec-tools** has been deprecated

The **kexec_load** system call, which loads the second kernel, will not be supported in future RHEL releases. The **kexec_file_load** system call replaces **kexec_load** and is now the default system call on all architectures.
For more information, see Is kexec_load supported in RHEL9? .

Jira:RHELPLAN-129876[1]

The deprecated **--token** option of **subscription-manager register** will stop working at the end of November 2024

The deprecated **--token=<TOKEN>** option of the **subscription-manager register** command will no longer be a supported authentication method from the end of November 2024. The default entitlement server, **subscription.rhsm.redhat.com**, will no longer be allowing token-based authentication. As a consequence, if you use **subscription-manager register --token=<TOKEN>**, the registration will fail with the following error message:

> Token authentication not supported by the entitlement server

To register your system, use other supported authorization methods, such as including paired options **--username** / **--password** OR **--org** / **--activationkey** with the **subscription-manager register** command.

Jira:RHELPLAN-146101[1]

10.8.4. SSSD

The SSSD **files** provider has been deprecated

The SSSD **files** provider has been deprecated in Red Hat Enterprise Linux (RHEL) 9. The **files** provider might be removed from a future release of RHEL.

Jira:RHELPLAN-139805[1]

10.8.5. Desktop

LibreOffice is deprecated

The LibreOffice RPM packages are now deprecated and will be removed in a future major RHEL release. LibreOffice continues to be fully supported through the entire life cycle of RHEL 7, 8, and 9. As a replacement for the RPM packages, Red Hat recommends that you install LibreOffice from either of the following sources provided by The Document Foundation:

- The official Flatpak package in the Flathub repository: https://flathub.org/apps/org.libreoffice.LibreOffice.
- The official RPM packages: https://www.libreoffice.org/download/download-libreoffice/.

Jira:RHELDOCS-16300[1]

10.8.6. Virtualization

RDMA-based live migration is deprecated

With this update, migrating running virtual machines using Remote Direct Memory Access (RDMA) has become deprecated. As a result, it is still possible to use the **rdma** migration URI to request migration over RDMA, but this feature will become unsupported in a future major release of RHEL.

Jira:RHELPLAN-153267[1]

10.8.7. Containers

The CNI network stack has been deprecated

The Container Network Interface (CNI) network stack is deprecated and will be removed from Podman in a future minor release of RHEL. Previously, containers connected to the single Container Network Interface (CNI) plugin only by using DNS. Podman v.4.0 introduced a new Netavark network stack. You can use the Netavark network stack with Podman and other Open Container Initiative (OCI) container management applications. The Netavark network stack for Podman is also compatible with advanced Docker functionalities. Containers in multiple networks can access containers on any of those networks.

For more information, see Switching the network stack from CNI to Netavark .

Jira:RHELDOCS-16756[1]

The CNI network stack has been deprecated

The Container Network Interface (CNI) network stack is deprecated and will be removed in a future release. Use the Netavark network stack instead. For more information, see Switching the network stack from CNI to Netavark.

Jira:RHELDOCS-17518[1]

10.9. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.1

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.1.

10.9.1. Security

OpenSSL does not accept explicit curve parameters in FIPS mode

Elliptic curve cryptography parameters, private keys, public keys, and certificates that specified explicit curve parameters no longer work in FIPS mode. Specifying the curve parameters using ASN.1 object identifiers, which use one of the FIPS-approved curves, still works in FIPS mode.

Jira:RHELPLAN-113856[1]

10.9.2. Compilers and development tools

Smaller size of keys than 2048 are deprecated by openssl 3.0 in Go's FIPS mode

Key sizes smaller than 2048 bits are deprecated by **openssl** 3.0 and no longer work in Go's FIPS mode.

Jira:RHELPLAN-129104[1]

Some PKCS1 v1.5 modes are now deprecated in Go's FIPS mode

Some **PKCS1** v1.5 modes are not approved in **FIPS-140-3** for encryption and are disabled. They will no longer work in Go's FIPS mode.

Jira:RHELPLAN-123778[1]

10.9.3. Desktop

GTK 2 is now deprecated

The legacy GTK 2 toolkit and the following, related packages have been deprecated:

- **adwaita-gtk2-theme**
- **gnome-common**
- **gtk2**
- **gtk2-immodules**
- **hexchat**

Several other packages currently depend on GTK 2. These have been modified so that they no longer depend on the deprecated packages in a future major RHEL release.

If you maintain an application that uses GTK 2, Red Hat recommends that you port the application to GTK 4.

Jira:RHELPLAN-131882[1]

10.9.4. Virtualization

Legacy CPU models are now deprecated

A significant number of CPU models have become deprecated and will become unsupported for use in virtual machines (VMs) in a future major release of RHEL. The deprecated models are as follows:

- For Intel: models before Intel Xeon 55xx and 75xx Processor families (also known as Nehalem)
- For AMD: models before AMD Opteron G4
- For IBM Z: models before IBM z14

To check whether your VM is using a deprecated CPU model, use the **virsh dominfo** utility, and look for a line similar to the following in the **Messages** section:

```
tainted: use of deprecated configuration settings
deprecated configuration: CPU model 'i486'
```

Jira:RHELPLAN-114513[1]

10.10. DEPRECATED FUNCTIONALITIES IDENTIFIED IN RHEL 9.0

Review functionalities that are deprecated in Red Hat Enterprise Linux 9.0.

10.10.1. Installer and image creation

Deprecated Kickstart commands

The following Kickstart commands have been deprecated:

- **timezone --ntpservers**
- **timezone --nontp**
- **logging --level**
- **%packages --excludeWeakdeps**
- **%packages --instLangs**
- **%anaconda**
- **pwpolicy**
- **nvdimm**

Note that where only specific options are listed, the base command and its other options are still available and not deprecated. Using the deprecated commands in Kickstart files prints a warning in the logs. You can turn the deprecated command warnings into errors with the **inst.ksstrict** boot option.

Jira:RHELPLAN-60153[1]

10.10.2. Security

SHA-1 is deprecated for cryptographic purposes

The usage of the SHA-1 message digest for cryptographic purposes has been deprecated in RHEL 9. The digest produced by SHA-1 is not considered secure because of many documented successful attacks based on finding hash collisions. The RHEL core crypto components no longer create signatures using SHA-1 by default. Applications in RHEL 9 have been updated to avoid using SHA-1 in security-relevant use cases.
Among the exceptions, the HMAC-SHA1 message authentication code and the Universal Unique Identifier (UUID) values can still be created using SHA-1 because these use cases do not currently pose security risks. SHA-1 also can be used in limited cases connected with important interoperability and compatibility concerns, such as Kerberos and WPA-2. See the List of RHEL applications using cryptography that is not compliant with FIPS 140-3 section in the RHEL 9 Security hardening document for more details.

If your scenario requires the use of SHA-1 for verifying existing or third-party cryptographic signatures, you can enable it by entering the following command:

```
# update-crypto-policies --set DEFAULT:SHA1
```

Alternatively, you can switch the system-wide crypto policies to the **LEGACY** policy. Note that **LEGACY** also enables many other algorithms that are not secure.

Jira:RHELPLAN-110763[1]

fapolicyd.rules is deprecated

The **/etc/fapolicyd/rules.d/** directory for files containing allow and deny execution rules replaces the **/etc/fapolicyd/fapolicyd.rules** file. The **fagenrules** script now merges all component rule files in this directory to the **/etc/fapolicyd/compiled.rules** file. Rules in **/etc/fapolicyd/fapolicyd.trust** are still processed by the **fapolicyd** framework but only for ensuring backward compatibility.

Jira:RHELPLAN-112355[1]

SCP is deprecated in RHEL 9

The secure copy protocol (SCP) is deprecated because it has known security vulnerabilities. The SCP API remains available for the RHEL 9 lifecycle but using it reduces system security.

- In the **scp** utility, SCP is replaced by the SSH File Transfer Protocol (SFTP) by default.
- The OpenSSH suite does not use SCP in RHEL 9.
- SCP is deprecated in the **libssh** library.

Jira:RHELPLAN-99136[1]

Digest-MD5 in SASL is deprecated

The Digest-MD5 authentication mechanism in the Simple Authentication Security Layer (SASL) framework is deprecated, and it might be removed from the **cyrus-sasl** packages in a future major release.

Jira:RHELPLAN-94096[1]

/etc/system-fips is now deprecated

Support for indicating FIPS mode through the **/etc/system-fips** file has been removed, and the file will not be included in future versions of RHEL. To install RHEL in FIPS mode, add the **fips=1** parameter to the kernel command line during the system installation. You can check whether RHEL operates in FIPS mode by displaying the **/proc/sys/crypto/fips_enabled** file.

Jira:RHELPLAN-103232[1]

libcrypt.so.1 is now deprecated

The **libcrypt.so.1** library is now deprecated, and it might be removed in a future version of RHEL.

Jira:RHELPLAN-106338[1]

10.10.3. Networking

libdb has been deprecated

RHEL 9 currently provide Berkeley DB (**libdb**) version 5.3.28, which is distributed under the LGPLv2 license. The upstream Berkeley DB version 6 is available under the AGPLv3 license, which is more restrictive.
The **libdb** package is deprecated as of RHEL 9 and might not be available in future major RHEL releases.

In addition, cryptographic algorithms have been removed from **libdb** in RHEL 9 and multiple **libdb** dependencies have been removed from RHEL 9.

Users of **libdb** are advised to migrate to a different key-value database. For more information, see the following Red Hat Knowledgebase articles:

- How to migrate from libdb to a different key-value database
- Available replacements for the deprecated Berkeley DB (libdb) in RHEL

Jira:RHELPLAN-67314[1]

Network teams are deprecated in RHEL 9

The **teamd** service and the **libteam** library are deprecated in Red Hat Enterprise Linux 9 and will be removed in the next major release. As a replacement, configure a bond instead of a network team. Red Hat focuses its efforts on kernel-based bonding to avoid maintaining two features, bonds and teams, that have similar functions. The bonding code has a high customer adoption, is robust, and has an active community development. As a result, the bonding code receives enhancements and updates.

For details about how to migrate a team to a bond, see Migrating a network team configuration to network bond.

Jira:RHELPLAN-69554[1]

NetworkManager connection profiles in ifcfg format are deprecated

In RHEL 9.0 and later, connection profiles in **ifcfg** format are deprecated. The next major RHEL release will remove the support for this format. However, in RHEL 9, NetworkManager still processes and updates existing profiles in this format if you modify them.

By default, NetworkManager now stores connection profiles in keyfile format in the **/etc/NetworkManager/system-connections/** directory. Unlike the **ifcfg** format, the keyfile format supports all connection settings that NetworkManager provides. For further details about the keyfile format and how to migrate profiles, see NetworkManager connection profiles in keyfile format .

Jira:RHELPLAN-58745[1]

The **iptables** back end in**firewalld** is deprecated

In RHEL 9, the **iptables** framework is deprecated. As a consequence, the **iptables** back end and the **direct interface** in **firewalld** are also deprecated. Instead of the **direct interface** you can use the native features in **firewalld** to configure the required rules.

Jira:RHELPLAN-122745[1]

ATM encapsulation is deprecated in RHEL 9

Asynchronous Transfer Mode (ATM) encapsulation enables Layer-2 (Point-to-Point Protocol, Ethernet) or Layer-3 (IP) connectivity for the ATM Adaptation Layer 5 (AAL-5). Red Hat has not been providing support for ATM NIC drivers since RHEL 7. The support for ATM implementation is being dropped in RHEL 9. These protocols are currently used only in chipsets, which support the ADSL technology and are being phased out by manufacturers. Therefore, ATM encapsulation is deprecated in Red Hat Enterprise Linux 9.
For more information, see PPP Over AAL5, Multiprotocol Encapsulation over ATM Adaptation Layer 5, and Classical IP and ARP over ATM .

Jira:RHELPLAN-113659[1]

10.10.4. File systems and storage

lvm2-activation-generator and its generated services removed in RHEL 9.0

The **lvm2-activation-generator** program and its generated services **lvm2-activation**, **lvm2-activation-early**, and **lvm2-activation-net** are removed in RHEL 9.0. The **lvm.conf event_activation** setting, used to activate the services, is no longer functional. The only method for auto activating volume groups is event based activation.

Jira:RHELPLAN-107107[1]

10.10.5. Identity Management

SHA-1 in OpenDNSSec is now deprecated

OpenDNSSec supports exporting Digital Signatures and authentication records using the **SHA-1** algorithm. The use of the **SHA-1** algorithm is no longer supported. With the RHEL 9 release, **SHA-1** in OpenDNSSec is deprecated and it might be removed in a future minor release. Additionally, OpenDNSSec support is limited to its integration with Red Hat Identity Management. OpenDNSSec is not supported standalone.

Jira:RHELPLAN-88246[1]

The **dnssec-enable: no;** option has been deprecated

The **dnssec-enable: no;** option in the **/etc/named/ipa-options-ext.conf** file has been deprecated and will be removed in a future major version of RHEL. DNS Security Extensions (DNSSEC) are

enabled by default and disabling them will not be possible. The **dnssec-validation: no;** option still continues to be available.

Jira:RHELDOCS-20464[1]

10.10.6. SSSD

The SSSD implicit files provider domain is disabled by default

The SSSD implicit **files** provider domain, which retrieves user information from local files such as **/etc/shadow** and group information from **/etc/groups**, is now disabled by default.

To retrieve user and group information from local files with SSSD:

1. Configure SSSD. Choose one of the following options:
   a. Explicitly configure a local domain with the **id_provider=files** option in the **sssd.conf** configuration file.

```
[domain/local]
id_provider=files
...
```

   b. Enable the **files** provider by setting **enable_files_domain=true** in the **sssd.conf** configuration file.

```
[sssd]
enable_files_domain = true
```

2. Configure the name services switch.

```
# authselect enable-feature with-files-provider
```

3. To restore caching and synchronization of user information, enable the integration between **shadow-utils** and **sssd_cache** by creating a symbolic link:

```
# ln -s /usr/sbin/sss_cache /usr/sbin/sss_cache_shadow_utils
```

Jira:RHELPLAN-100639[1], Jira:RHEL-56352

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[1]

10.10.7. Graphics infrastructures

Motif has been deprecated

The Motif widget toolkit has been deprecated in RHEL, because development in the upstream Motif community is inactive.

The following Motif packages have been deprecated, including their development and debugging variants:

- **motif**
- **openmotif**
- **openmotif21**
- **openmotif22**

Additionally, the **motif-static** package has been removed.

Red Hat recommends using the GTK toolkit as a replacement. GTK is more maintainable and provides new features compared to Motif.

Jira:RHELPLAN-98983[1]

10.10.8. Red Hat Enterprise Linux System Roles

The **network** System Role displays a deprecation warning when configuring teams on RHEL 9 nodes

The network teaming capabilities have been deprecated in RHEL 9. As a result, using the **network** RHEL System Role on a RHEL 8 control node to configure a network team on RHEL 9 nodes, shows a warning about the deprecation.

Jira:RHELPLAN-95747[1]

10.10.9. Virtualization

libvirtd has become deprecated

The monolithic **libvirt** daemon, **libvirtd**, has been deprecated in RHEL 9, and will be removed in a future major release of RHEL. Note that you can still use **libvirtd** for managing virtualization on your hypervisor, but Red Hat recommends switching to the newly introduced modular **libvirt** daemons. For instructions and details, see the RHEL 9 Configuring and Managing Virtualization document.

Jira:RHELPLAN-113995[1]

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 SHA-2 algorithm, or later.

Jira:RHELPLAN-69533[1]

The virtual floppy driver has become deprecated

The **isa-fdc** driver, which controls virtual floppy disk devices, is now deprecated, and will become unsupported in a future release of RHEL. Therefore, to ensure forward compatibility with migrated virtual machines (VMs), Red Hat discourages using floppy disk devices in VMs hosted on RHEL 9.8.

Jira:RHELPLAN-81033[1]

qcow2-v2 image format is deprecated

With RHEL 9.8, the qcow2-v2 format for virtual disk images has become deprecated, and will become unsupported in a future major release of RHEL. In addition, the RHEL 9.8 Image Builder cannot create disk images in the qcow2-v2 format.
Instead of qcow2-v2, Red Hat strongly recommends using qcow2-v3. To convert a qcow2-v2 image to a later format version, use the **qemu-img amend** command.

Jira:RHELPLAN-75969[1]

10.10.10. Containers

Running RHEL 9 containers on a RHEL 7 host is not supported

Running RHEL 9 containers on a RHEL 7 host is not supported. It might work, but it is not guaranteed. For more information, see Red Hat Enterprise Linux Container Compatibility Matrix .

Jira:RHELPLAN-100087[1]

SHA1 hash algorithm within Podman has been deprecated

The SHA1 algorithm used to generate the filename of the rootless network namespace is no longer supported in Podman. Therefore, rootless containers started before updating to Podman 4.1.1 or later have to be restarted if they are joined to a network (and not just using **slirp4netns**) to ensure they can connect to containers started after the upgrade.

Jira:RHELPLAN-117005[1]

rhel9/pause has been deprecated

The **rhel9/pause** container image has been deprecated.

Jira:RHELPLAN-127619[1]

10.11. DEPRECATED FUNCTIONALITIES IDENTIFIED IN PREVIOUS RELEASES

Review functionalities that were deprecated in earlier Red Hat Enterprise Linux versions.

10.11.1. Shells and command-line tools

Setting the **TMPDIR** variable in the ReaR configuration file is deprecated

Setting the **TMPDIR** environment variable in the **/etc/rear/local.conf** or **/etc/rear/site.conf** ReaR configuration file), by using a statement such as **export TMPDIR=...**, is deprecated.
To specify a custom directory for ReaR temporary files, export the variable in the shell environment before executing ReaR. For example, execute the **export TMPDIR=...** statement and then execute the **rear** command in the same shell session or script.

Jira:RHELDOCS-18049[1]

10.11.2. Virtualization

virt-manager has been deprecated

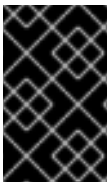
The Virtual Machine Manager application, also known as **virt-manager**, has been deprecated. The RHEL web console, also known as **Cockpit**, is intended to become its replacement in a subsequent release. It is, therefore, recommended that you use the web console for managing virtualization in a GUI. Note, however, that some features available in **virt-manager** might not be yet available in the RHEL web console.

Jira:RHELPLAN-10304[1]

10.12. DEPRECATED PACKAGES

This section lists packages that have been deprecated and will probably not be included in a future major release of Red Hat Enterprise Linux.

For changes to packages between RHEL 8 and RHEL 9, see Changes to packages in the *Considerations in adopting RHEL 9* document.



IMPORTANT

The support status of deprecated packages remains unchanged within RHEL 9. For more information about the length of support, see Red Hat Enterprise Linux Life Cycle and Red Hat Enterprise Linux Application Streams Life Cycle .

The following packages have been deprecated in RHEL 9:

- aacraid
- adwaita-gtk2-theme
- af_key
- anaconda-user-help
- aajohan-comfortaa-fonts
- adwaita-gtk2-theme
- adwaita-qt5
- anaconda-user-help
- ansible-collection-redhat-rhel_mgmt
- ant-javamail
- apr-util-bdb
- aspnetcore-runtime-7.0
- aspnetcore-targeting-pack-6.0
- aspnetcore-targeting-pack-7.0
- atkmm
- atlas

- atlas-devel
- atlas-z14
- atlas-z15
- authselect-compat
- autoconf-latest
- autoconf271
- autocorr-af
- autocorr-bg
- autocorr-ca
- autocorr-cs
- autocorr-da
- autocorr-de
- autocorr-dsb
- autocorr-el
- autocorr-en
- autocorr-es
- autocorr-fa
- autocorr-fi
- autocorr-fr
- autocorr-ga
- autocorr-hr
- autocorr-hsb
- autocorr-hu
- autocorr-is
- autocorr-it
- autocorr-ja
- autocorr-ko
- autocorr-lb
- autocorr-lt

- autocorr-mn
- autocorr-nl
- autocorr-pl
- autocorr-pt
- autocorr-ro
- autocorr-ru
- autocorr-sk
- autocorr-sl
- autocorr-sr
- autocorr-sv
- autocorr-tr
- autocorr-vi
- autocorr-vro
- autocorr-zh
- avahi-autoipd
- babl
- bacula-client
- bacula-common
- bacula-console
- bacula-director
- bacula-libs
- bacula-libs-sql
- bacula-logwatch
- bacula-storage
- bind9.18-libs
- bitmap-fangsongti-fonts
- bnx2
- bnx2fc
- bnx2i

- bogofilter
- Box2D
- brasero-nautilus
- cairomm
- cheese
- cheese-libs
- clucene-contribs-lib
- clucene-core
- clutter
- clutter-gst3
- clutter-gtk
- cnic
- cockpit-composer
- cogl
- compat-hesiod
- compat-locales-sap
- compat-locales-sap-common
- compat-openssl11
- compat-paratype-pt-sans-fonts-f33-f34
- compat-sap-c++-12
- compat-sap-c++-13
- console-setup
- containernetworking-plugins
- containers-common-extra
- culmus-aharoni-clm-fonts
- culmus-caladings-clm-fonts
- culmus-david-clm-fonts
- culmus-drugulin-clm-fonts
- culmus-ellinia-clm-fonts

- culmus-fonts-common
- culmus-frank-ruehl-clm-fonts
- culmus-hadasim-clm-fonts
- culmus-miriam-clm-fonts
- culmus-miriam-mono-clm-fonts
- culmus-nachlieli-clm-fonts
- culmus-simple-clm-fonts
- culmus-stamashkenaz-clm-fonts
- culmus-stamsefarad-clm-fonts
- culmus-yehuda-clm-fonts
- curl-minimal
- daxio
- dbus-glib
- dbus-glib-devel
- devhelp
- devhelp-libs
- dhcp-client
- dhcp-common
- dhcp-relay
- dhcp-server
- dotnet-apphost-pack-6.0
- dotnet-apphost-pack-7.0
- dotnet-hostfxr-6.0
- dotnet-hostfxr-7.0
- dotnet-runtime-6.0
- dotnet-runtime-7.0
- dotnet-sdk-6.0
- dotnet-sdk-7.0
- dotnet-targeting-pack-6.0

- dotnet-targeting-pack-7.0
- dotnet-templates-6.0
- dotnet-templates-7.0
- double-conversion
- efs-utils
- enchant
- enchant-devel
- eog
- evince
- evince-libs
- evince-nautilus
- evince-previewer
- evince-thumbnailer
- evolution
- evolution-bogofilter
- evolution-data-server-ui
- evolution-data-server-ui-devel
- evolution-devel
- evolution-ews
- evolution-ews-langpacks
- evolution-help
- evolution-langpacks
- evolution-mapi
- evolution-mapi-langpacks
- evolution-pst
- evolution-spamassassin
- festival
- festival-data
- festvox-slt-arctic-hts

- firefox
- firefox
- firefox-x11
- flite
- flite-devel
- fltk
- flute
- firewire-core
- fontawesome-fonts
- gc
- gcr-base
- gdisk
- gedit
- gedit-plugin-bookmarks
- gedit-plugin-bracketcompletion
- gedit-plugin-codecomment
- gedit-plugin-colorpicker
- gedit-plugin-colorschemer
- gedit-plugin-commander
- gedit-plugin-drawspaces
- gedit-plugin-findinfiles
- gedit-plugin-joinlines
- gedit-plugin-multiedit
- gedit-plugin-sessionsaver
- gedit-plugin-smartspaces
- gedit-plugin-synctex
- gedit-plugin-terminal
- gedit-plugin-textsize
- gedit-plugin-translate

- gedit-plugin-wordcompletion
- gedit-plugins
- gedit-plugins-data
- gegl04
- gegl04-devel-docs
- gegl04-tools
- ghc-srpm-macros
- ghostscript-x11
- git-p4
- gl-manpages
- glade
- glade-libs
- glibmm24
- gnome-backgrounds
- gnome-backgrounds-extras
- gnome-common
- gnome-logs
- gnome-photos
- gnome-photos-tests
- gnome-screenshot
- gnome-session-xsession
- gnome-shell-extension-panel-favorites
- gnome-shell-extension-updates-dialog
- gnome-terminal
- gnome-terminal-nautilus
- gnome-themes-extra
- gnome-tweaks
- gnome-video-effects
- google-noto-cjk-fonts-common

- google-noto-sans-cjk-ttc-fonts
- google-noto-sans-khmer-ui-fonts
- google-noto-sans-lao-ui-fonts
- google-noto-sans-thai-ui-fonts
- gpm
- gpm-devel
- gpm-libs
- gsl
- gsl-devel
- gspell
- gtksourceview4
- gtk2
- gtk2-devel
- gtk2-devel-docs
- gtk2-immodule-xim
- gtk2-immodules
- gtkmm30
- gtksourceview4
- gubbi-fonts
- gvfs-devel
- ha-openstack-support
- hexchat
- hesiod
- highcontrast-icon-theme
- http-parser
- ibus-gtk2
- initial-setup
- initial-setup-gui
- inkscape

- inkscape-docs
- inkscape-view
- iptables-devel
- iptables-libs
- iptables-nft
- iptables-nft-services
- iptables-utils
- iputils-ninfod
- ipxe-roms
- jakarta-activation2
- java-1.8.0-openjdk
- java-1.8.0-openjdk-demo
- java-1.8.0-openjdk-devel
- java-1.8.0-openjdk-headless
- java-1.8.0-openjdk-javadoc
- java-1.8.0-openjdk-javadoc-zip
- java-1.8.0-openjdk-src
- java-11-openjdk
- java-11-openjdk-demo
- java-11-openjdk-devel
- java-11-openjdk-headless
- java-11-openjdk-javadoc
- java-11-openjdk-javadoc-zip
- java-11-openjdk-jmods
- java-11-openjdk-src
- java-11-openjdk-static-libs
- java-17-openjdk
- java-17-openjdk-demo
- java-17-openjdk-devel

- java-17-openjdk-headless
- java-17-openjdk-javadoc
- java-17-openjdk-javadoc-zip
- java-17-openjdk-jmods
- java-17-openjdk-src
- java-17-openjdk-static-libs
- jboss-jaxrs-2.0-api
- jboss-logging
- jboss-logging-tools
- jdeparser
- jigawatts
- jigawatts-javadoc
- julietaula-montserrat-fonts
- kacst-art-fonts
- kacst-book-fonts
- kacst-decorative-fonts
- kacst-digital-fonts
- kacst-farsi-fonts
- kacst-fonts-common
- kacst-letter-fonts
- kacst-naskh-fonts
- kacst-office-fonts
- kacst-one-fonts
- kacst-pen-fonts
- kacst-poster-fonts
- kacst-qurn-fonts
- kacst-screen-fonts
- kacst-title-fonts
- kacst-titlel-fonts

- khmer-os-battambang-fonts
- khmer-os-bokor-fonts
- khmer-os-content-fonts
- khmer-os-fasthand-fonts
- khmer-os-freehand-fonts
- khmer-os-handwritten-fonts
- khmer-os-metal-chrieng-fonts
- khmer-os-muol-fonts
- khmer-os-muol-fonts-all
- khmer-os-muol-pali-fonts
- khmer-os-siemreap-fonts
- kmod-kvdo
- lasso
- libabw
- libadwaita-qt5
- libbase
- libblockdev-kbd
- libcanberra-gtk2
- libcdio-paranoia
- libcdio-paranoia-devel
- libcdr
- libcmis
- libdazzle
- libdb
- libdb-devel
- libdb-utils
- libdmx
- libepubgen
- libetonyek

- libexttextcat
- libfonts
- libformula
- libfreehand
- libgdata
- libgdata-devel
- libgnomekbd
- libiscsi
- libiscsi-utils
- liblangtag
- liblangtag-data
- liblayout
- libloader
- libmatchbox
- libmspub
- libmwaw
- libmypaint
- libnsl2
- libnumbertext
- libodfgen
- liborcus
- libotr
- libpagemaker
- libpmem
- libpmem-debug
- libpmem-devel
- libpmem2
- libpmem2-debug
- libpmem2-devel

- libpmemblk
- libpmemblk-debug
- libpmemblk-devel
- libpmemlog
- libpmemlog-debug
- libpmemlog-devel
- libpmemobj
- libpmemobj++-devel
- libpmemobj++-doc
- libpmemobj-debug
- libpmemobj-devel
- libpmempool
- libpmempool-debug
- libpmempool-devel
- libpng15
- libpst-libs
- libqxp
- LibRaw
- libreoffice
- libreoffice-base
- libreoffice-calc
- libreoffice-core
- libreoffice-data
- libreoffice-draw
- libreoffice-emailmerge
- libreoffice-filters
- libreoffice-gdb-debug-support
- libreoffice-graphicfilter
- libreoffice-gtk3

- libreoffice-help-ar
- libreoffice-help-bg
- libreoffice-help-bn
- libreoffice-help-ca
- libreoffice-help-cs
- libreoffice-help-da
- libreoffice-help-de
- libreoffice-help-dz
- libreoffice-help-el
- libreoffice-help-en
- libreoffice-help-eo
- libreoffice-help-es
- libreoffice-help-et
- libreoffice-help-eu
- libreoffice-help-fi
- libreoffice-help-fr
- libreoffice-help-gl
- libreoffice-help-gu
- libreoffice-help-he
- libreoffice-help-hi
- libreoffice-help-hr
- libreoffice-help-hu
- libreoffice-help-id
- libreoffice-help-it
- libreoffice-help-ja
- libreoffice-help-ko
- libreoffice-help-lt
- libreoffice-help-lv
- libreoffice-help-nb

- libreoffice-help-nl
- libreoffice-help-nn
- libreoffice-help-pl
- libreoffice-help-pt-BR
- libreoffice-help-pt-PT
- libreoffice-help-ro
- libreoffice-help-ru
- libreoffice-help-si
- libreoffice-help-sk
- libreoffice-help-sl
- libreoffice-help-sv
- libreoffice-help-ta
- libreoffice-help-tr
- libreoffice-help-uk
- libreoffice-help-zh-Hans
- libreoffice-help-zh-Hant
- libreoffice-impress
- libreoffice-langpack-af
- libreoffice-langpack-ar
- libreoffice-langpack-as
- libreoffice-langpack-bg
- libreoffice-langpack-bn
- libreoffice-langpack-br
- libreoffice-langpack-ca
- libreoffice-langpack-cs
- libreoffice-langpack-cy
- libreoffice-langpack-da
- libreoffice-langpack-de
- libreoffice-langpack-dz

- libreoffice-langpack-el
- libreoffice-langpack-en
- libreoffice-langpack-eo
- libreoffice-langpack-es
- libreoffice-langpack-et
- libreoffice-langpack-eu
- libreoffice-langpack-fa
- libreoffice-langpack-fi
- libreoffice-langpack-fr
- libreoffice-langpack-fy
- libreoffice-langpack-ga
- libreoffice-langpack-gl
- libreoffice-langpack-gu
- libreoffice-langpack-he
- libreoffice-langpack-hi
- libreoffice-langpack-hr
- libreoffice-langpack-hu
- libreoffice-langpack-id
- libreoffice-langpack-it
- libreoffice-langpack-ja
- libreoffice-langpack-kk
- libreoffice-langpack-kn
- libreoffice-langpack-ko
- libreoffice-langpack-lt
- libreoffice-langpack-lv
- libreoffice-langpack-mai
- libreoffice-langpack-ml
- libreoffice-langpack-mr
- libreoffice-langpack-nb

- libreoffice-langpack-nl
- libreoffice-langpack-nn
- libreoffice-langpack-nr
- libreoffice-langpack-nso
- libreoffice-langpack-or
- libreoffice-langpack-pa
- libreoffice-langpack-pl
- libreoffice-langpack-pt-BR
- libreoffice-langpack-pt-PT
- libreoffice-langpack-ro
- libreoffice-langpack-ru
- libreoffice-langpack-si
- libreoffice-langpack-sk
- libreoffice-langpack-sl
- libreoffice-langpack-sr
- libreoffice-langpack-ss
- libreoffice-langpack-st
- libreoffice-langpack-sv
- libreoffice-langpack-ta
- libreoffice-langpack-te
- libreoffice-langpack-th
- libreoffice-langpack-tn
- libreoffice-langpack-tr
- libreoffice-langpack-ts
- libreoffice-langpack-uk
- libreoffice-langpack-ve
- libreoffice-langpack-xh
- libreoffice-langpack-zh-Hans
- libreoffice-langpack-zh-Hant

- libreoffice-langpack-zu
- libreoffice-math
- libreoffice-ogltrans
- libreoffice-opensymbol-fonts
- libreoffice-pdfimport
- libreoffice-pyuno
- libreoffice-sdk
- libreoffice-sdk-doc
- libreoffice-ure
- libreoffice-ure-common
- libreoffice-voikko
- libreoffice-wiki-publisher
- libreoffice-writer
- libreoffice-x11
- libreoffice-xsltfilter
- libreofficekit
- libreport
- libreport-anaconda
- libreport-cli
- libreport-filesystem
- libreport-gtk
- libreport-plugin-bugzilla
- libreport-plugin-reportuploader
- libreport-rhel-anaconda-bugzilla
- libreport-web
- librepository
- librevenge
- librevenge-gdb
- libserializer

- libsigc++20
- libsigsegv
- libsmbios
- libsoup
- libsoup-devel
- libstaroffice
- libstemmer
- libstoragemgmt-smis-plugin
- libteam
- libuser
- libuser-devel
- libvisio
- libvisual
- libwmf
- libwmf-lite
- libwpd
- libwpe
- libwpe-devel
- libwpg
- libwps
- libxcrypt-compat
- libxklavier
- libXp
- libXp-devel
- libXScrnSaver
- libXScrnSaver-devel
- libXxf86dga
- libXxf86dga-devel
- libzmf

- lklug-fonts
- lohit-gurmukhi-fonts
- lpsolve
- man-pages-overrides
- mcpp
- memkind
- mesa-libGLw
- mesa-libGLw-devel
- mlocate
- mod_auth_mellon
- mod_jk
- mod_security
- mod_security-mlogc
- mod_security_crs
- motif
- motif-devel
- mypaint-brushes
- mythes
- mythes-bg
- mythes-ca
- mythes-cs
- mythes-da
- mythes-de
- mythes-el
- mythes-en
- mythes-eo
- mythes-es
- mythes-fr
- mythes-ga

- mythes-hu
- mythes-it
- mythes-lv
- mythes-nb
- mythes-nl
- mythes-nn
- mythes-pl
- mythes-pt
- mythes-ro
- mythes-ru
- mythes-sk
- mythes-sl
- mythes-sv
- mythes-uk
- navilu-fonts
- nbdkit-gzip-filter
- neon
- NetworkManager-initscripts-updown
- nginx
- nginx-all-modules
- nginx-core
- nginx-filesystem
- nginx-mod-devel
- nginx-mod-http-image-filter
- nginx-mod-http-perl
- nginx-mod-http-xslt-filter
- nginx-mod-mail
- nginx-mod-stream
- nispor

- nscd
- nvme-stas
- opal-firmware
- opal-prd
- opal-prd
- opal-utils
- openal-soft
- openchange
- openscap-devel
- openscap-python3
- openslp-server
- openwsman-perl
- openwsman-winrs
- overpass-fonts
- paktype-naqsh-fonts
- paktype-tehreer-fonts
- pam_ssh_agent_auth
- pangomm
- pentaho-libxml
- pentaho-reporting-flow-engine
- perl-AnyEvent
- perl-B-Hooks-EndOfScope
- perl-Class-Accessor
- perl-Class-Data-Inheritable
- perl-Class-Singleton
- perl-Class-Tiny
- perl-Crypt-OpenSSL-Bignum
- perl-Crypt-OpenSSL-Random
- perl-Crypt-OpenSSL-RSA

- perl-Date-ISO8601
- perl-DateTime
- perl-DateTime-Format-Builder
- perl-DateTime-Format-ISO8601
- perl-DateTime-Format-Strptime
- perl-DateTime-Locale
- perl-DateTime-TimeZone
- perl-DateTime-TimeZone-SystemV
- perl-DateTime-TimeZone-Tzfile
- perl-DB_File
- perl-Devel-CallChecker
- perl-Devel-Caller
- perl-Devel-LexAlias
- perl-Digest-SHA1
- perl-Dist-CheckConflicts
- perl-DynaLoader-Functions
- perl-Encode-Detect
- perl-Eval-Closure
- perl-Exception-Class
- perl-File-chdir
- perl-File-Copy-Recursive
- perl-File-Find-Object
- perl-File-Find-Rule
- perl-HTML-Tree
- perl-Importer
- perl-Mail-AuthenticationResults
- perl-Mail-DKIM
- perl-Mail-Sender
- perl-Mail-SPF

- perl-MIME-Types
- perl-Module-Implementation
- perl-Module-Pluggable
- perl-namespace-autoclean
- perl-namespace-clean
- perl-Net-CIDR-Lite
- perl-Net-DNS
- perl-NetAddr-IP
- perl-Number-Compare
- perl-Package-Stash
- perl-Package-Stash-XS
- perl-PadWalker
- perl-Params-Classify
- perl-Params-Validate
- perl-Params-ValidationCompiler
- perl-Perl-Destruct-Level
- perl-Ref-Util
- perl-Ref-Util-XS
- perl-Scope-Guard
- perl-Specio
- perl-Sub-Identify
- perl-Sub-Info
- perl-Sub-Name
- perl-Switch
- perl-Sys-CPU
- perl-Sys-MemInfo
- perl-Test-LongString
- perl-Test-Taint
- perl-Variable-Magic

- perl-XML-DOM
- perl-XML-RegExp
- perl-XML-Twig
- pinfo
- pki-jackson-annotations
- pki-jackson-core
- pki-jackson-databind
- pki-jackson-jaxrs-json-provider
- pki-jackson-jaxrs-providers
- pki-jackson-module-jaxb-annotations
- pki-resteasy-client
- pki-resteasy-core
- pki-resteasy-jackson2-provider
- pki-resteasy-servlet-initializer
- plymouth-theme-charge
- pmdk-convert
- pmempool
- podman-plugins
- poppler-qt5
- postgresql-test-rpm-macros
- power-profiles-daemon
- pulseaudio-module-x11
- python-botocore
- python-gflags
- python-netifaces
- python-pyroute2
- python-qt5-rpm-macros
- python3-bind
- python3-chardet

- python3-lasso
- python3-libproxy
- python3-libreport
- python3-netifaces
- python3-nispor
- python3-py
- python3-pycdlib
- python3-pycurl
- python3-pyghmi
- python3-pyqt5-sip
- python3-pyrsistent
- python3-pysocks
- python3-pytz
- python3-pywbem
- python3-qt5
- python3-qt5-base
- python3-requests+security
- python3-requests+socks
- python3-scour
- python3-toml
- python3-tomli
- python3-tracer
- python3-wx-siplib
- python3.11
- python3.11-cffi
- python3.11-charset-normalizer
- python3.11-cryptography
- python3.11-devel
- python3.11-idna

- python3.11-libs
- python3.11-lxml
- python3.11-mod_wsgi
- python3.11-numpy
- python3.11-numpy-f2py
- python3.11-pip
- python3.11-pip-wheel
- python3.11-ply
- python3.11-psycopg2
- python3.11-pycparser
- python3.11-PyMySQL
- python3.11-PyMySQL+rsa
- python3.11-pysocks
- python3.11-pyyaml
- python3.11-requests
- python3.11-requests+security
- python3.11-requests+socks
- python3.11-scipy
- python3.11-setuptools
- python3.11-setuptools-wheel
- python3.11-six
- python3.11-tkinter
- python3.11-urllib3
- python3.11-wheel
- python3.12-PyMySQL+rsa
- qgnomeplatform
- qla4xxx
- qt5
- qt5-assistant

- qt5-designer
- qt5-devel
- qt5-doctools
- qt5-linguist
- qt5-qdbusviewer
- qt5-qt3d
- qt5-qt3d-devel
- qt5-qt3d-doc
- qt5-qt3d-examples
- qt5-qtbase
- qt5-qtbase-common
- qt5-qtbase-devel
- qt5-qtbase-doc
- qt5-qtbase-examples
- qt5-qtbase-gui
- qt5-qtbase-mysql
- qt5-qtbase-odbc
- qt5-qtbase-postgresql
- qt5-qtbase-private-devel
- qt5-qtbase-static
- qt5-qtconnectivity
- qt5-qtconnectivity-devel
- qt5-qtconnectivity-doc
- qt5-qtconnectivity-examples
- qt5-qtdeclarative
- qt5-qtdeclarative-devel
- qt5-qtdeclarative-doc
- qt5-qtdeclarative-examples
- qt5-qtdeclarative-static

- qt5-qtdoc
- qt5-qtgraphicaleffects
- qt5-qtgraphicaleffects-doc
- qt5-qtimageformats
- qt5-qtimageformats-doc
- qt5-qtlocation
- qt5-qtlocation-devel
- qt5-qtlocation-doc
- qt5-qtlocation-examples
- qt5-qtmultimedia
- qt5-qtmultimedia-devel
- qt5-qtmultimedia-doc
- qt5-qtmultimedia-examples
- qt5-qtquickcontrols
- qt5-qtquickcontrols-doc
- qt5-qtquickcontrols-examples
- qt5-qtquickcontrols2
- qt5-qtquickcontrols2-devel
- qt5-qtquickcontrols2-doc
- qt5-qtquickcontrols2-examples
- qt5-qtscript
- qt5-qtscript-devel
- qt5-qtscript-doc
- qt5-qtscript-examples
- qt5-qtsensors
- qt5-qtsensors-devel
- qt5-qtsensors-doc
- qt5-qtsensors-examples
- qt5-qtserialbus

- qt5-qtserialbus-devel
- qt5-qtserialbus-doc
- qt5-qtserialbus-examples
- qt5-qtserialport
- qt5-qtserialport-devel
- qt5-qtserialport-doc
- qt5-qtserialport-examples
- qt5-qtsvg
- qt5-qtsvg-devel
- qt5-qtsvg-doc
- qt5-qtsvg-examples
- qt5-qttools
- qt5-qttools-common
- qt5-qttools-devel
- qt5-qttools-doc
- qt5-qttools-examples
- qt5-qttools-libs-designer
- qt5-qttools-libs-designercomponents
- qt5-qttools-libs-help
- qt5-qttools-static
- qt5-qttranslations
- qt5-qtwayland
- qt5-qtwayland-devel
- qt5-qtwayland-doc
- qt5-qtwayland-examples
- qt5-qtwebchannel
- qt5-qtwebchannel-devel
- qt5-qtwebchannel-doc
- qt5-qtwebchannel-examples

- qt5-qtwebsockets
- qt5-qtwebsockets-devel
- qt5-qtwebsockets-doc
- qt5-qtwebsockets-examples
- qt5-qtx11extras
- qt5-qtx11extras-devel
- qt5-qtx11extras-doc
- qt5-qtxmlpatterns
- qt5-qtxmlpatterns-devel
- qt5-qtxmlpatterns-doc
- qt5-qtxmlpatterns-examples
- qt5-rpm-macros
- qt5-srpm-macros
- raptor2
- rasqal
- redis
- redis-devel
- redis-doc
- redland
- rpmlint
- rubygem-openwsman
- runc
- saab-fonts
- sac
- satyr
- scap-workbench
- SDL2
- sendmail
- sendmail-cf

- sendmail-doc
- setxkbmap
- sgabios
- sgabios-bin
- sil-scheherazade-fonts
- spamassassin
- speech-tools-libs
- suitesparse
- sushi
- team
- teamd
- texlive-xdvi
- thai-scalable-fonts-common
- thai-scalable-garuda-fonts
- thai-scalable-kinnari-fonts
- thai-scalable-loma-fonts
- thai-scalable-norasi-fonts
- thai-scalable-purisa-fonts
- thai-scalable-sawasdee-fonts
- thai-scalable-tlwgmono-fonts
- thai-scalable-tlwgtypewriter-fonts
- thai-scalable-tlwgtypist-fonts
- thai-scalable-tlwgtypo-fonts
- thai-scalable-umpush-fonts
- thunderbird
- tigervnc
- tigervnc-icons
- tigervnc-license
- tigervnc-selinux

- tigervnc-server
- tigervnc-server-minimal
- tigervnc-server-module
- totem-pl-parser
- tracer-common
- ucs-miscfixed-fonts
- udftools
- usb_modeswitch
- usb_modeswitch-data
- usbredir-server
- usermode-gtk
- webkit2gtk3
- webkit2gtk3-devel
- webkit2gtk3-jsc
- webkit2gtk3-jsc-devel
- wpebackend-fdo
- wpebackend-fdo-devel
- xmlrpc-c
- xmlsec1-gcrypt
- xmlsec1-gcrypt-devel
- xmlsec1-gnutls
- xmlsec1-gnutls-devel
- xorg-x11-drivers
- xorg-x11-drv-dummy
- xorg-x11-drv-evdev
- xorg-x11-drv-fbdev
- xorg-x11-drv-libinput
- xorg-x11-drv-v4l
- xorg-x11-drv-vmware

- xorg-x11-drv-wacom
- xorg-x11-drv-wacom-serial-support
- xorg-x11-server-common
- xorg-x11-server-utils
- xorg-x11-server-Xdmx
- xorg-x11-server-Xephyr
- xorg-x11-server-Xnest
- xorg-x11-server-Xorg
- xorg-x11-server-Xvfb
- xorg-x11-utils
- xorg-x11-xbitmaps
- xorg-x11-xinit
- xorg-x11-xinit-session
- xsane
- xsane-common
- xxhash
- xxhash-libs
- yajl
- yelp
- yelp-libs
- yp-tools
- ypbind
- ypserv
- zhongyi-song-fonts

CHAPTER 11. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 9.8.

11.1. SECURITY

kdump fails to start with UKI

When you install the **kernel-uki-virt** and **kernel-modules-core** packages to enable Unified Kernel Image (UKI) on a confidential VM in Azure, the **kdump** service fails to start. Consequently, **kdump** does not work on the VM.
Workaround: Disable the SELinux policy and reboot the VM. As a result, the **kdump** service is running.

Jira:RHEL-66119[1]

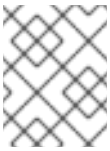
11.2. SOFTWARE MANAGEMENT

DNF installs a package from a local file when the package version is excluded in versionlock

When you exclude a package version in the **versionlock** DNF plugin configuration, DNF still installs the specified package version from a package local file.
To work around this problem, complete the following steps:

1. Turn a directory with local packages into a local repository by using the **createrepo_c** tool.
2. Enable the local repository in the DNF configuration.
3. Install all packages by their names.

As a result, the **versionlock** plugin applies to packages from the local repository and has no effect on directory with local package files.



NOTE

Consider not installing packages by a local file path if you do not want certain package versions to be installed.

For more information, see the **dnf-versionlock(8)** man page on your system.

Jira:RHEL-94014

11.3. NETWORKING

RHEL does not contain closed-source modem unlocking tools

Federal Communications Commission (FCC) regulations require that modems in the United States must be enabled by using an unlocking tool from the modem manufacturer. RHEL does not provide these tools if they are closed-source software according to FCC regulations. However, they might be available in an unsupported third-party repository, such as RPM Fusion.
For further details, see Installing the FCC unlocking tool for modems from third-party repositories .

Jira:RHEL-100057[1]

The **maddress** option of the **ip monitor** command fails

A previous update added the **ip monitor maddress** command to the **iproute2** package. Due to a bug, the **ip monitor** command now fails with the following error:

```
Failed to add ipv4 mcaddr group to list
```

To work around the problem, use a specific **ip monitor** subcommand, and avoid the **maddress** option.

Jira:RHEL-102012

Preventing non-root users from creating system-wide NetworkManager connection profiles

You can set certain properties in NetworkManager connection profiles, such as **802-1x.client-cert**, to a path to a certificate file. Because the **NetworkManager** service runs as the **root** user, the service can access those files independent of their file permissions. This can lead to security problems in the following scenarios:

- A user creates a private connection profile and specifies a path to another user's certificate file.
  With NetworkManager in RHEL 9.8 and later, referring to other users' certificates in private profiles is no longer possible.

- A user creates a system-wide connection profile and specifies a path to another user's certificate.
  On RHEL, users can only create system-wide profiles if they are logged in locally to the console and not remotely, such as over SSH. To not change this behavior of NetworkManager during the RHEL 9 release cycle, users can still create system-wide profiles.

  To mitigate the risk, you can prevent normal users from creating system-wide connection profiles. For example, create the **/etc/polkit-1/rules.d/20-nm-non-root.rules** file with the following content:

  ```
  polkit.addRule(function(action, subject) {
      if (action.id == "org.freedesktop.NetworkManager.settings.modify.system" &&
          !subject.isInGroup("wheel")) {
          return polkit.Result.AUTH_ADMIN_KEEP;
      }
  });
  ```

  The setting takes effect immediately.

Jira:RHELDOCS-21742[1]

11.4. IDENTITY MANAGEMENT

ipa-migrate does not migrate SSH public keys

When migrating an Identity Management (IdM) deployment using the **ipa-migrate** tool, SSH public keys assigned to user accounts and ID overrides are not transferred to the destination server. As a consequence, users cannot authenticate using SSH public key authentication after migration.

To work around this problem, retrieve the SSH public keys from the source server using the **ipa user-find --all** or **ldapsearch** commands, and then re-add them on the destination server using the **ipa user-mod --sshpubkey** command.

RHEL-151560

Jira:RHEL-151560[1]

11.5. VIRTUALIZATION

Stop errors in Windows guests

Currently, in virtual machines that use Windows guest operating systems on RHEL hosts, a variety of stop errors (also known as BSOD) might occur. For details of the known errors, see List of known Windows BSOD issues on OpenShift Virtualization and RHEL KVM on Red Hat Knowledge Base. For instructions on troubleshooting the errors, see Recommendations when investigating Windows BSOD issues.

Jira:RHELDOCS-22157[1]

drm_client_lib module dependency can prevent older NVIDIA vGPU driver from loading on RHEL 9.7

On RHEL 9.7, the **drm_client_lib** functionality was split from the **drm** module into a separate loadable kernel module. As a result, systems using certain older NVIDIA vGPU guest driver versions might fail to load the driver with a **Module drm_client_lib not found** error if the **drm_client_lib** module is not loaded in advance.
This issue occurs when installing or loading older NVIDIA vGPU guest drivers that do not load the required **drm_client_lib** module automatically. Updated NVIDIA drivers include a fix for this behavior.

To work around this issue, use one of the following approaches:

- Manually load the required module before loading the NVIDIA driver by running **modprobe drm_client_lib**.
- Update to a newer NVIDIA vGPU guest driver version that includes the fix.

Jira:RHEL-124779[1]

High-memory Windows guests might fail to validate with SVVP

Currently, when using the Server Virtualization Validation Program (SVVP) software to validate a Windows virtual machine (VM) with a large amount of assigned memory, the validation might fail with a **GetPhysicallyInstalledSystemMemory failed** error message. As a consequence, the VM cannot be validated for SVVP support.
Jira:RHEL-81999

11.6. KNOWN ISSUES IDENTIFIED IN RHEL 9.7

This part describes known issues identified in Red Hat Enterprise Linux 9.7.

11.6.1. Security

Containers fail to start when **fapolicyd** is running

The **fapolicyd** framework does not fully support namespaces and containers. As a consequence, containers fail to start when **fapolicyd** is running.
To work around this problem, create the **/etc/fapolicyd/rules.d/25-runc.rules** file with the following content:

```
allow perm=any pattern=ld_so exe=/usr/bin/runc : all
allow perm=any uid=0 pattern=ld_so exe=/runc : trust=1
```

Save the file, run the **fagenrules** script, and enter the **fapolicyd-cli --reload-rules** command to apply the changes. Alternatively, you can remove the **tmpfs** value from the **watch_fs** option in the **/etc/fapolicyd/fapolicyd.conf** file and restart the **fapolicyd** service by using the **systemctl restart fapolicyd** command, but this lowers the system security.

As a result, you can use **fapolicyd** on systems running containers after you apply the previously described workaround. This preserves the enhanced security provided by **fapolicyd** and helps comply with configuration standards such as the Security Technical Implementation Guide (STIG) from the Defense Information Systems Agency (DISA).

Jira:RHEL-114562

RPM packages signed with MLDSA-87 fail to install in FIPS mode

The post-quantum cryptography (PQC) algorithms are not FIPS-validated and are not available in the FIPS provider. This causes the import of MLDSA-87 PQC keys into the RPM database and PQC signature verification to fail in FIPS mode.
To work around this problem, do not enable the DNF plugin to support PQC signatures in FIPS mode. As a result, the system verifies packages in FIPS mode through classical signatures.

Jira:RHEL-111478[1]

PQC for **rpm-sequoia** is always enabled in **crypto-policies**

The **rpm-sequoia** library fails to verify dual-signed RPM packages if one of the algorithms used for signing is disabled in system-wide cryptographic policies. This problem is common on systems that have post-quantum (PQ) algorithms disabled and cannot install packages signed with both classic and PQ cryptography.
To prevent breaking the system, the enablement of PQ algorithms for **rpm-sequoia** is hardcoded on the **crypto-policies** level. As a result, PQ algorithms for **rpm-sequoia** are enabled regardless of any settings in **crypto-policies**.

Jira:RHEL-112697

11.6.2. Shells and command-line tools

Hot-plugged memory is not available to VMs running on IBM Z by default

RHEL provides default udev rules that automatically configure memory onlining when you hot plug memory to virtual machines (VMs) with **virtio-mem**. However, current udev rules do not include VMs running on IBM Z. As a consequence, after hot-plugging memory to VMs running on IBM Z with **virtio-mem**, the memory is not immediately available in the VM.
To work around this problem, set the **memhp_default_state=online** kernel parameter in the VM and reboot it. For example:

```
# grubby --update-kernel=ALL --args=memhp_default_state=online
```

As a result, the hot-plugged memory is available in the VM.

Jira:RHEL-92781

11.6.3. Networking

Inbound IPsec cryptographic offload can fail in SR-IOV **switchdev** mode with SMFS

If you configure IPsec cryptographic offload on a Mellanox ConnectX network interface controller (NIC) in Single-Root I/O Virtualization (SR-IOV) **switchdev** mode with the flow steering mode set to Software Managed Flow Steering (SMFS), the hardware offload for inbound IPsec Security Associations (SAs) fails. In this case, the **ip xfrm state dir in show** command returns the following error:

```
Error: mlx5_core: Device failed to offload this state.
```

To work around this problem, switch to Device-Managed Flow Steering (DMFS) before switching the device to **switchdev** mode. By using DMFS, the inbound IPsec state can successfully be offloaded to the hardware.

Jira:RHEL-114873[1]

11.6.4. File systems and storage

kdump does not support NVMe/TCP connected namespaces

kdump does not support using NVMe over TCP (NVMe/TCP) connected namespaces as dump devices. If you configure an NVMe/TCP namespace for **kdump**, the crash dump process fails and no dump is collected. Consequently, the system cannot save the **vmcore** file during a kernel crash.

Jira:RHEL-109510[1]

11.6.5. Dynamic programming languages, web and database servers

MariaDB 10.5 and MySQL do not work with RHEL in image mode

The MariaDB 10.5 and MySQL database management systems do not use the **sysusers.d** directories to populate users and working directories. MariaDB 10.5 and MySQL also do not use the **tmpfiles.d** directory. As a consequence, the database user can be missing and the database systems are not able to initialize because their working directory is missing. There is currently no workaround for this issue.

Jira:RHELDOCS-21366[1]

11.6.6. Virtualization

VMs with 5-level page merging and a lot of memory sometimes fail to start

VMs with the following configuration fail to boot if you set the **host-phys-bits-limit** parameter to **49** or more:

- The VM has more than 1 TB of assigned memory

- The VM uses the 5-level page merging feature
- The host uses System Management Mode (SMM) in its firmware

Instead, attempting to boot the VM fails with **ERROR: Out of aligned pages**.

Workaround: Set the **host-phys-bits-limit** parameter to 48 or less.

Jira:RHEL-82759

11.6.7. Containers

UBI images are not reproducible

The **podman build** and **buildah build** commands avoid introducing inconsistencies between builds that use the same set of inputs when you invoke them with the following arguments:

- **--rewrite-timestamp**
- **--source-date-epoch**, an equivalent build argument or environment value that you set when starting the build.

To work around this problem, invoke the **podman build** or **buildah build** commands with the **--rewrite-timestamp** and **--source-date-epoch** arguments to minimize build inconsistencies. Additionally, update tools invoked in **RUN** instructions to avoid producing nondeterministic output when the **$SOURCE_DATE_EPOCH** environment variable is set.

Some tools or tool versions might still produce nondeterministic output, and you might not be able to build specific images reproducibly.

Jira:RHEL-62749

11.6.8. RHEL Lightspeed

The command-line assistant cannot verify the Satellite server certificate

The command-line assistant does not recognize the Satellite certificate authority (CA) certificate for the Red Hat Satellite server. The Satellite CA certificate is used to issue and sign certificates for hosts that register with and are managed by Satellite. As a consequence, the command-line assistant cannot establish secure connections to the Satellite server, which prevents it from functioning correctly.
Work around: copy the Satellite CA certificate to the system trust store and update the CA trust database:

```
$ sudo cp /etc/rhsm/ca/katello* /etc/pki/ca-trust/source/anchors/
$ sudo update-ca-trust
```

Jira:RHELDOCS-21325[1]

11.7. KNOWN ISSUES IDENTIFIED IN RHEL 9.6

This part describes known issues identified in Red Hat Enterprise Linux 9.6.

11.7.1. Installer and image creation

Images built with the**stig** profile remediation fail to boot with FIPS error

FIPS mode is not supported by RHEL image builder. When using RHEL image builder customized with the **xccdf_org.ssgproject.content_profile_stig** profile remediation, the system fails to boot with the following error:

```
Warning: /boot//.vmlinuz-<kernel version>.x86_64.hmac does not exist
FATAL: FIPS integrity test failed
Refusing to continue
```

Enabling the FIPS policy manually after the system image installation with the **fips-mode-setup --enable** command does not work, because the **/boot** directory is on a different partition. System boots successfully if FIPS is disabled. Currently, there is no workaround available.

NOTE

You can manually enable FIPS after installing the image by using the **fips-mode-setup --enable** command.

Jira:RHEL-4649

RHEL images on Azure marked as LVM require default layout resizing

When using **system-reinstall-bootc** or **bootc install** on Azure, RHEL images marked as LVM will require resizing the default layout.
Workaround: Use RHEL images labeled as RAW. This does not require resizing the default layout.

Jira:RHELDOCS-19945[1]

Hostname resolution fails with encrypted DNS and custom CA in boot options

While using the **inst.repo=** or **inst.stage2=** boot options in the kernel command line along with a remote installation URL, an encrypted DNS, and a custom CA certificate in the Kickstart file, the installation program attempts to download the **install.img** stage2 image before processing the Kickstart file. Consequently, the hostname resolution fails, leading to display of some errors before successfully fetching the stage2 image.
Workaround: Define the installation source in the Kickstart file instead of the kernel command line.

Jira:RHEL-80867

Bonding device with LACP takes longer to become operational, causing subscription failures

When configuring a bonding device with LACP by using both kernel command-line boot options and a Kickstart file, the connection is created during the **initramfs** stage but reactivated in Anaconda. As a consequence, it causes a temporary disruption that leads to system subscription failure through the **rhsm** Kickstart command.
Workaround: Add **--no-activate** to the Kickstart network configuration to keep the network operational. As a result, the system subscription completes successfully.

Jira:RHELDOCS-19852[1]

Insufficient disk space can cause deployment failure

Deploying a bootc container image on a package mode system without enough free disk space can result in installation errors and prevent the system from booting. Ensure adequate disk space is available for the image to install and adjust the provision logical volume before deployment.

Jira:RHELDOCS-19948[1]

Anaconda might not work correctly on **s390x** and **ppc64le** architectures

Image mode for RHEL supports **pp64le** and **s390x** architectures besides the already supported **x86_64** and ARM architectures. However, Anaconda might not function correctly on s390x and ppc64le architectures.

Jira:RHELDOCS-19496[1]

11.7.2. Software management

A security DNF upgrade fails for packages that change their architecture through the upgrade

The patch for BZ#2108969, released with the RHBA-2022:8295 advisory, introduced the following regression: The DNF upgrade using security filters fails for packages that change their architecture from or to **noarch** through the upgrade. Consequently, it can leave the system in a vulnerable state. To work around this problem, perform the regular upgrade without security filters.

Jira:RHELPLAN-128381[1]

11.7.3. Infrastructure services

Using the incorrect Perl database driver for MariaDB and MySQL can lead to unexpected results

The MariaDB database is a fork of MySQL. Over time, these services developed independently and are no longer fully compatible. These differences also affect the Perl database drivers. Consequently, if you use the **DBD::mysql** driver in a Perl application to connect to a MariaDB database, or the **DBD::MariaDB** driver to connect to a MySQL database, operations can lead to unexpected results. For example, the driver can return incorrect data from read operations. To avoid such problems, use the Perl driver in your application that matches the database service.
Red Hat only supports the following scenarios:

- The Perl **DBD::MariaDB** driver with a MariaDB database
- The Perl **DBD::mysql** driver with a MySQL database

Note that RHEL 8 contained only the **DBD::mysql** driver. If you plan to upgrade to RHEL 9 and then to RHEL 10 and your application uses a MariaDB database, install the **perl-DBD-MariaDB** package after the upgrade and modify your application to use the **DBD::MariaDB** driver.

For further details, see the Red Hat Knowledgebase solution Support of MariaDB/MySQL cross-database connection from Perl db drivers.

Jira:RHELDOCS-19728[1]

11.7.4. Networking

Issues in DPLL stability during PF resets

The Digital Phase-Locked Loop (DPLL) system experienced several issues, including uninitialized mutex usage and incorrect handling of pin phase adjustments, particularly during Physical Function (PF) resets. These issues led to unstable management of DPLL and pin configurations, causing inconsistent data states and connection mismanagement.
Workaround: To resolve this, mutexes were properly initialized, and mechanisms for updating pin phase adjustments, DPLL data, and connection states during PF resets were corrected. As a result, the DPLL system now performs reliably during resets, with accurate phase adjustments and consistent connection states, improving the overall stability of clock synchronization.

Jira:RHEL-36283[1]

11.7.5. Kernel

Kernel panic is encountered on IBM Power systems (**ppc64le**) when **io_uring** is enabled

In some cases,**ppc64le** systems encounter a kernel panic when using the **io_uring** kernel parameter due to intensive input-output operations. As a consequence, **ppc64le** stops working and requires a system restart. The data might get lost during the crash.
Workaround: Disable the **io_uring** feature by adding the following kernel parameter at boot time:

module.builtin=io_uring=0

Jira:RHEL-28702[1]

11.7.6. Virtualization

Windows VM with VBS and IOMMU device fails to boot

When you boot a Windows VM with Virtualization Based Security (VBS) enabled and an Input-Output Memory Management Unit (IOMMU) device by using the **qemu-kvm** utility, the booting sequence only shows the boot screen, resulting in an incomplete booting process.
Workaround: Ensure the VM domain XML is configured as below:

```
<features>
  <ioapic driver='qemu'/>
</features>
<devices>
<iommu model='intel'>
   <driver intremap='on' eim='off' aw_bits='48'/>
   <alias name='iommu0'/>
</iommu>
<memballoon model='virtio'>
   <alias name='balloon0'/>
   <address type='pci' domain='0x0000' bus='0x03' slot='0x00' function='0x0'/>
   <driver iommu='on' ats='on'/>
</memballoon>
</devices>
```

Otherwise, the Windows VM cannot boot.

Jira:RHEL-45585[1]

A virtual machine with a large amount of bootable data disks might fail to start

If you attempt to start a virtual machine (VM) with a large amount of bootable data disks, the VM might fail to boot with this error: **Something has gone seriously wrong: import_mok_state() failed: Volume Full**

Workaround: Decrease the number of bootable data disks and use one system disk. To ensure the system disk is first in the boot order, add **boot order=1** to the device definition of the system disk in the XML configuration. For example:

```
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/path/to/disk.qcow2'/>
  <target dev='vda' bus='virtio'/>
  <boot order='1'/>
</disk>
```

Set boot order only for the system disk.

Jira:RHEL-68418

Windows 2025 VM slows down if assigned with a large number of vCPU

When assigned with 32 or more vCPUs, Windows Server 2025 virtual machines (VMs) slow down on a Red Hat Enterprise Linux host. Consequently, a Windows VM may boot slowly or be stuck during boot when the VM is configured with a large number of vCPUs.

Workaround: You can use the workaround at your own risk. Boot VM with small number of vCPUs to disable plaformclock on Windows Server. In command prompt with administrator privileges, run:

```
bcdedit /set useplatformclock no
```

Then, shut down the VM and reconfigure it with the desired large number of vCPUs. Also make sure that the **hv-time** option is enabled before starting the large VM again.

Jira:RHEL-62742[1]

Installing the VirtIO-Win bundle cannot be canceled

Currently, if you start the installation of **virtio-win** drivers from the VirtIO-Win installer bundle in a Windows guest operating system, clicking the **Cancel** button during the installation does not correctly stop it. The installer wizard interface displays a "Setup Failed" screen, but the drivers are installed and the IP address of the guest is reset.

Jira:RHEL-53962, Jira:RHEL-53965

Hot-plugging vCPUs and memory to Windows guests with VBS does not work

Currently, Windows Virtualization-based Security (VBS) is not compatible with hot-plugging CPU and memory resources. As a consequence, attempting to attach memory or vCPUs to a running Windows virtual machine (VM) with VBS enabled only adds the resources to the VM after the guest system is restarted.

Jira:RHEL-66229, Jira:RHELDOCS-19066

NetworkManager-wait-online.service fails to start on Azure VMs with Accelerated Networking

When you launch a Red Hat Enterprise Linux VM of Azure platform with the Accelerated Networking

feature, also known as Single Root Input Output Virtualization (SR-IOV), multiple network interface cards may have the same MAC address. Consequently, the VM may fail to acquire an IP address from a DHCP server and **NetworkManager-wait-online.service** may fail to start at boot time.

Workaround: Do not install the **initscripts-rename-device** package so that existing devices will not rename to existing device names.

Jira:RHEL-79783[1]

11.7.7. RHEL in cloud environments

Memory hot-plug possible on VMware when the memory size does not align with memory block size

Currently, it is possible to attempt hot-plugging memory to a RHEL 9 guest on VMware hypervisor even if the memory size of the attached memory dpes not align with the size of the individual memory blocks. However, attaching memory in this manner always fails with a **Block size unaligned hotplug range** error.

Workaround: Only hot-plug memory that is divisible by the configured memory block size on the guest. To obtain the memory block size, use the **lsmem** command. For further information, see The Red Hat KnowledgeBase.

Jira:RHEL-81748[1]

BIOS or UEFI supported Hyper-V Windows Server 2016 VM fails to boot if a host uses the AMD EPYC CPU processor

With the Hyper-V enabled setting, Hyper-V Windows Server 2016 VM fails to boot on the AMD EPYC CPU host.

Workaround: Check for the following log message:

```
kvm: Booting SMP Windows KVM VM with !XSAVES && XSAVEC.
If it fails to boot try disabling XSAVEC in the VM config.
```

And try adding **xsavec=off** to **-cpu cmdline** to boot Hyper-V Windows Server 2016 VM.

Jira:RHEL-38957[1]

kdump fails to complete on the Azure Confidential VMs

When you experience a kernel crash on a Red Hat Enterprise Linux VM on the Azure Confidential VM instances, in this case DCv5 and ECv5 series, the **kdump** process may not complete and the VM becomes unresponsive. As a result, after a forced reboot, there is a **vmcore-incomplete** file.

Jira:RHEL-70228[1]

11.7.8. Containers

FIPS bootc image creation fails on FIPS enabled host

Building a disk image on a host by using Podman with enabled the FIPS mode fails with the exit code 3 because of the update-crypto-policies package:

```
# Enable the FIPS crypto policy
# crypto-policies-scripts is not installed by default in RHEL-10
RUN dnf install -y crypto-policies-scripts && update-crypto-policies --no-reload --set FIPS
```

Workaround: Build the bootc image with FIPS mode disabled.

Jira:RHELDOCS-19539

11.7.9. RHEL Lightspeed

Command-line assistant configuration file changes are not applied immediately

When making changes in the **etc/xdg/command-line-assistant/config.toml** configuration file, it takes around 30 to 60 seconds for the command-line assistant daemon to recognize the changes, instead of applying the changes immediately. The command-line assistant is also missing the **reload** functionality.
Workaround: Follow the steps:

1. Make the changes that you need to the **config.toml** configuration file.
2. Run the following command:

```
# systemctl restart clad
```

Jira:RHELDOCS-19734[1]

11.8. KNOWN ISSUES IDENTIFIED IN RHEL 9.5

This part describes known issues identified in Red Hat Enterprise Linux 9.5.

11.8.1. Installer and image creation

Unable to build ISOs from a signed container

Trying to build an ISO disk image from a GPG or a simple signed container results in an error, similar to the following:

```
manifest - failed
Failed
Error: cannot run osbuild: running osbuild failed: exit status 1
2024/04/23 10:56:48 error: cannot run osbuild: running osbuild failed: exit status 1
```

This happens because the system fails to get the image source signatures.

Workaround: You can either remove the signature from the container image or build a derived container image. For example, to remove the signature, you can run the following command:

```
$ sudo skopeo copy --remove-signatures containers-storage:registry.redhat.io/rhel9/rhel-bootc:9.4
containers-storage:registry.redhat.io/rhel9/rhel-bootc:9.4
$ sudo podman run \
    --rm \
    -it \
    --privileged \
```

```
--pull=newer \
--security-opt label=type:unconfined_t \
-v /var/lib/containers/storage:/var/lib/containers/storage \
-v ~/images/iso:/output \
quay.io/centos-bootc/bootc-image-builder \
--type iso --local \
registry.redhat.io/rhel9/rhel-bootc:9.4
```

To build a derived container image, and avoid adding a simple GPG signatures to it, see the Signing container images product documentation.

Jira:RHEL-34807

SELinux autorelabel in the Rescue Mode might cause reboot loop

Accessing a file system in the **rescue** mode triggers SELinux to autorelabel the file system on the next boot, which continues until SELinux runs in the **permissive** mode. Consequently, the system might go into an infinite loop of reboots after exiting the **rescue** mode as it cannot delete the **/.autorelabel** file.

Workaround: Switch to the **permissive** mode by adding **enforcing=0** to the kernel command line on the next boot. The system displays a warning message as a preventive measure that informs about the possibility of this issue when accessing the file system in the **rescue** mode.

Jira:RHEL-14005

11.8.2. Security

OpenSSL no longer creates X.509 v1 certificates

With the OpenSSL TLS toolkit 3.2.1 introduced in RHEL 9.5, you can no longer create certificates in the X.509 version 1 format using the **openssl** CA tool. The X.509 v1 format does not meet current web requirements.

Jira:RHEL-40605

11.8.3. High availability and clusters

Removing duplicate route entries for IPv6 addresses in an IPsrcaddr resource

In Red Hat Enterprise Linux 9.4 and earlier, when you specified an IPv6 address for an **IPsrcaddr** resource, the **IPsrcaddr** resource agent created a duplicate route with a different metric when the metric was used for the subnet. For example, this happened when NetworkManager created another IP address on the IPv6 subnet. In this situation, the **IPsrcaddr** resource failed to start because there was more than one match for the IP address. As of Red Hat Enterprise Linux 9.5, the **IPsrcaddr** resource agent specifies the metric of an existing route when it is available and a second route is not created. If, however, you created an **IPaddr2** IPv6 resource that uses an IPv6 address before this upgrade, you must reboot your system to remove the duplicate route entry.

Jira:RHEL-32265[1]

11.8.4. Virtualization

SeaBIOS cannot boot from a disk with 4096 bytes sector size

When using SeaBIOS to boot a virtual machine (VM) from a disk that uses logical or physical sector size of 4096 bytes, the boot disk is not displayed as available, and booting the VM fails. To boot a VM from such a disk, use UEFI instead of SeaBIOS.
Jira:RHEL-7110

Enabling Hyper-V enlightenments in some cases does not improve CPU optimization

On virtual machines (VM) that use a Windows guest operating system, enabling Hyper-V enlightenments in some cases does not result in the expected improvement in the CPU usage of the VM. There is currently no workaround for this issue.

Jira:RHEL-17331[1]

Windows Server 2019 virtual machines crash on boot if using more than 128 cores per CPU

Virtual machines (VMs) that use a Windows Server 2019 guest operating system currently fail to boot when they are configured to use more than 128 cores for a single virtual CPU (vCPU). Instead of booting, the VM displays a stop error on a blue screen.
Workaround: Use fewer than 128 core per vCPU.

Jira:RHELDOCS-18863[1]

11.9. KNOWN ISSUES IDENTIFIED IN RHEL 9.4

This part describes known issues identified in Red Hat Enterprise Linux 9.4.

11.9.1. Installer and image creation

Kickstart installation fails due to missing packages with `systemd` service files in `%packages` section

If the Kickstart file uses the **`services --enabled=...`** directive to enable **`systemd`** services and packages containing the specified service file are not included in the **`%packages`** section, the RHEL installation process fails with the following error:

```
Error enabling service <name_of_the_service>
```

Workaround: Include the respective package with the service file in Kickstart's **`%packages`** section. As a result, RHEL installation completes, enabling expected services during installation.

Jira:RHEL-9633[1]

11.9.2. Security

Missing files in `trustdb` cause denials for `fapolicyd`

When **`fapolicyd`** is installed with the Ansible DISA STIG profile, a race condition causes the **`trustdb`** database to be out of sync with the **`rpmdb`** database. As a consequence, missing files in **`trustdb`** cause denials on the system.
Workaround: Restart **`fapolicyd`** or run the Ansible DISA STIG profile again.

Jira:RHEL-24345[1]

OpenSSH no longer logs timeout before authentication

OpenSSH does not record a timeout before authentication for **$IP port $PORT** to the log. This might be important because the Fail2Ban intrusion prevention daemon and similar systems use these log records in its **mdre-ddos** regular expression and no longer ban the IPs of clients that attempt this type of attack. There is currently no known workaround for this problem.
Jira:RHEL-45727

Interoperability of FIPS:OSPP hosts impacted due to CNSA 1.0

The **OSPP** subpolicy has been aligned with Commercial National Security Algorithm (CNSA) 1.0. This affects the interoperability of hosts that use the **FIPS:OSPP** policy-subpolicy combination, with the following major aspects:

- Minimum RSA key size is mandated at 3072 bits.
- Algorithm negotiations no longer support AES-128 ciphers, the secp256r1 elliptic curve, and the FFDHE-2048 group.

Jira:RHEL-2735[1]

11.9.3. Shells and command-line tools

The ReaR rescue image on UEFI systems with Secure Boot enabled fails to boot with the default settings

ReaR image creation by using the **rear mkrescue** or **rear mkbackup** command fails with the following message:

```
grub2-mkstandalone may fail to make a bootable EFI image of GRUB2 (no /usr/*/grub*/x86_64-efi/moddep.lst file)
(...)
grub2-mkstandalone: error: /usr/lib/grub/x86_64-efi/modinfo.sh doesn't exist. Please specify --target or --directory.
```

The missing files are part of the **grub2-efi-x64-modules** package. If you install this package, the rescue image is created successfully without any errors. When the **UEFI** Secure Boot is enabled, the rescue image is not bootable because it uses a boot loader that is not signed.

Workaround: Add the following variables to the **/etc/rear/local.conf** or **/etc/rear/site.conf** ReaR configuration file:

```
UEFI_BOOTLOADER=/boot/efi/EFI/redhat/grubx64.efi
SECURE_BOOT_BOOTLOADER=/boot/efi/EFI/redhat/shimx64.efi
```

With the suggested workaround, the image can be produced successfully even on systems without the **grub2-efi-x64-modules** package, and it is bootable on systems with Secure Boot enabled. In addition, during the system recovery, the bootloader of the recovered system is set to the **EFI** shim bootloader.

For more information about **UEFI**, **Secure Boot**, and **shim bootloader**, see the UEFI: what happens when booting the system Knowledge Base article.

Jira:RHELDOCS-18064[1]

The %util column produced by sar and iostat utilities is invalid

When you collect system usage statistics by using the **sar** or **iostat** utilities, the **%util** column produced by **sar** or **iostat** might contain invalid data.

Jira:RHEL-26275[1]

The lsb-release binary is not available in RHEL 9

The information in **/etc/os-release** was previously available by calling the **lsb-release** binary. This binary was included in the **redhat-lsb package**, which was removed in RHEL 9. Now, you can display information about the operating system, such as the distribution, version, code name, and associated metadata, by reading the **/etc/os-release** file. This file is provided by Red Hat and any changes to it will be overwritten with each update of the **redhat-release** package. The format of the file is **KEY=VALUE**, and you can safely source the data for a shell script.

Jira:RHELDOCS-16427[1]

11.9.4. File systems and storage

lldpad is auto enabled even for qedf adapters

When using a QLogic Corp. FastLinQ QL45000 Series 10/25/40/50GbE, FCOE Controller automatically enables the **lldpad** daemon on systems running RHV. As a consequence, I/O operations are stopped with an error, for example, **[qedf_eh_abort:xxxx]:1: Aborting io_req=ff5d85a9dcf3xxxx**.
Workaround: DisableLink Layer Discovery Protocol (LLDP) and then enable it for interfaces that can be set on the **vdsm** configuration level. For more information, https://access.redhat.com/solutions/6963195.

Jira:RHEL-8104[1]

System fails to boot when iommu is enabled

By enabling the Input-Output Memory Management Unit (IOMMU) on AMD platforms when the BNX2I adapter is in use, a system fails to boot with the Direct Memory Access Remapping (DMAR) timeout errors.
Workaround: Disable the IOMMU before booting by using the kernel command-line option, **iommu=off**. As a result, the system boots without any errors.

Jira:RHEL-25730[1]

11.9.5. Dynamic programming languages, web and database servers

Git fails to clone or fetch from repositories with potentially unsafe ownership

To prevent remote code execution and mitigate CVE-2024-32004, stricter ownership checks have been introduced in **Git** for cloning local repositories. With this update, **Git** treats local repositories with potentially unsafe ownership as dubious.
As a consequence, if you attempt to clone from a repository locally hosted through **git-daemon** and you are not the owner of the repository, **Git** returns a security alert about dubious ownership and fails to clone or fetch from the repository.

Workaround: Explicitly mark the repository as safe by executing the following command:

-

```
git config --global --add safe.directory /path/to/repository
```

Jira:RHELDOCS-18435[1]

11.9.6. Identity Management

The online backup and the online automembership rebuild tasks can acquire two locks resulting in a deadlock

If the online backup and the online automembership rebuild tasks attempt to acquire the same two locks in the opposite order, it can lead to an unrecoverable deadlock that requires you to stop and restart the server. To work around this problem, do not launch the online backup and the online automembership rebuild tasks in parallel.

Jira:RHELDOCS-18065[1]

11.9.7. The web console

VNC console in the RHEL web console does not work correctly on ARM64

Currently, when you import a virtual machine (VM) in the RHEL web console on ARM64 architecture and then you try to interact with it in the VNC console, the console does not react to your input. Additionally, when you create a VM in the web console on ARM64 architecture, the VNC console does not display the last lines of your input.

Jira:RHEL-31993[1]

11.9.8. Red Hat Enterprise Linux System Roles

Running Microsoft SQL Server 2022 in high-availability mode as an SELinux-confined application does not work

Microsoft SQL Server 2022 on RHEL 9.4 and later supports running as an SELinux-confined application. However, due to a limitation in Microsoft SQL Server, running the service as an SELinux-confined application does not work in high-availability mode.
Workaround: You can run Microsoft SQL Server as an unconfined application if you require the service to be high available.

Note that this limitation also impacts installing Microsoft SQL Server when you use the **mssql** RHEL System Role to install this service.

Jira:RHELDOCS-17719[1]

11.9.9. Virtualization

TX queue size cannot be changed in VMs that use vhost-kernel

Currently, you cannot set up TX queue size on KVM virtual machines (VMs) that use **vhost-kernel** as a back end for the **virtio** network driver. As a consequence, you can use only the default value of 256 for the TX queue, which might prevent you from optimizing your VM network throughput. There is currently no workaround for this issue.

Jira:RHEL-1138[1]

VMs incorrectly report the **vulnerable** status for **spec_rstack_overflow** parameter on the AMD EPYC model

When you boot a host, it does not detect any vulnerabilities in the **spec_rstack_overflow** parameter. After querying the parameter for logs, it displays the message:

```
# cat /sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow
Mitigation: Safe RET
```

After booting a VM on the same host, the VM detects a vulnerability in the **spec_rstack_overflow** parameter. And when you query the parameter for logs, it displays the message:

```
# cat /sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow
Vulnerable: Safe RET, no microcode
```

However, this is a false warning message, and you can ignore the status of the **/sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow** file inside the VM.

Jira:RHEL-17614[1]

Link status shows **up** on VM, even when status is **down** of **e1000e** or **igb** model interface

Before booting the VM, set the status of Ethernet link **down** for the **e1000** or **igb** model network interface. Despite this, after the VM boots, the network interface keeps the **up** status, because when you set the status of Ethernet link **down** and then stop and re-start the VM, it is automatically set back to **up**. Consequently, the correct state of network interface is not maintained.
Workaround: Set the network interface status to **down** inside the VM by using command:

```
# ip link set dev eth0 down
```

Alternatively, you can try to remove and add this network interface again while the VM is running.

Jira:RHEL-21867

11.10. KNOWN ISSUES IDENTIFIED IN RHEL 9.3

This part describes known issues identified in Red Hat Enterprise Linux 9.3.

11.10.1. Security

Keylime refuses runtime policies whose digests start with a backslash

The current script for generating runtime policies, **create_runtime_policy.sh**, uses SHA checksum functions, for example, **sha256sum**, to compute the file digest. However, when the input file name contains a backslash or **\n**, the checksum function adds a backslash before the digest in its output. In such cases, the generated policy file is malformed. When provided with the malformed policy file, the Keylime tenant produces the following or similar error message: **me.tenant - ERROR - Response code 400: Runtime policy is malformatted**.
Workaround: Remove the backslash from the malformed policy file manually by entering the following command: **sed -i 's/^\\//g' <malformed_file_name>**.

Jira:RHEL-11867[1]

Keylime agent rejects requests from the verifier after update

When the API version number of the Keylime agent (**keylime-agent-rust**) has been updated, the agent rejects requests that use a different version. As a consequence, if a Keylime agent is added to a verifier and then updated, the verifier tries to contact the agent using the old API version. The agent rejects this request and fails the attestation.
Workaround: Update the verifier (**keylime-verifier**) before updating the agent (**keylime-agent-rust**). As a result, when the agents are updated, the verifier detects the API change and updates its stored data accordingly.

Jira:RHEL-1518[1]

The **fapolicyd** utility incorrectly allows executing changed files

Correctly, the IMA hash of a file should update after any change to the file, and **fapolicyd** should prevent execution of the changed file. However, this does not happen due to differences in IMA policy setup and in file hashing by the **evctml** utility. As a result, the IMA hash is not updated in the extended attribute of a changed file. Consequently, **fapolicyd** incorrectly allows the execution of the changed file.
Jira:RHEL-520[1]

11.10.2. Software management

Running **createrepo_c** on local repositories generates duplicate **repodata** files

When you run the **createrepo_c** command on local repositories, it generates duplicate copies of **repodata** files, one of the copies is compressed and one is not.
Workaround: There is no workaround available, however, you can safely ignore the duplicate files. The **createrepo_c** command generates duplicate copies because of requirements and differences in other tools relying on repositories created by using **createrepo_c**.

Jira:RHELPLAN-112860[1]

11.10.3. Kernel

Upgrading to the latest real-time kernel with **dnf** does not install multiple kernel versions in parallel

Installing the latest real-time kernel with the **dnf** package manager requires resolving package dependencies to retain the new and current kernel versions simultaneously. By default, **dnf** removes the older **kernel-rt** package during the upgrade.
Workaround: Add the current **kernel-rt** package to the **installonlypkgs** option in the **/etc/yum.conf** configuration file, for example, **installonlypkgs=kernel-rt**.

The **installonlypkgs** option appends **kernel-rt** to the default list used by **dnf**. Packages listed in **installonlypkgs** directive are not removed automatically and therefore support multiple kernel versions to install simultaneously.

Note that having multiple kernels installed is a way to have a fallback option when working with a new kernel version.

Jira:RHELPLAN-153123[1]

The **kdump** mechanism fails to capture the **vmcore** file on LUKS-encrypted targets on non-x86_64 architectures

For non-x86_64 architectures, when running **kdump** on systems with Linux Unified Key Setup (LUKS) encrypted partitions, systems require a certain amount of available memory. When the available memory is less than the required amount of memory, the **systemd-cryptsetup** service fails to mount the partition. Consequently, the second kernel fails to capture the crash dump file on the LUKS-encrypted targets.
Workaround: Query the **Recommended crashkernel value** and gradually increase the memory size to an appropriate value. The **Recommended crashkernel value** can serve as a reference to set the required memory size.

1. Print the estimated crash kernel value.

```
# kdumpctl estimate
```

2. Configure the amount of required memory by increasing the **crashkernel** value.

```
# grubby --args=crashkernel=652M --update-kernel=ALL
```

3. Reboot the system for changes to take effect.

```
# reboot
```

As a result, **kdump** works correctly on systems with LUKS-encrypted partitions.

Jira:RHEL-11196[1]

The Intel® **i40e** adapter permanently fails on IBM Power10

When the **i40e** adapter encounters an I/O error on IBM Power10 systems, the Enhanced I/O Error Handling (EEH) kernel services trigger the network driver's reset and recovery. However, EEH repeatedly reports I/O errors until the **i40e** driver reaches the predefined maximum of EEH freezes. As a consequence, EEH causes the device to fail permanently.

Jira:RHEL-15404[1]

11.10.4. File systems and storage

NVMe/FC devices cannot be reliably used in a Kickstart file

NVMe/FC devices can be unavailable during parsing or execution of pre-scripts of the Kickstart file, which can cause the Kickstart installation to fail.
Workaround: Update the boot argument to **inst.wait_for_disks=30**. This option causes a delay of 30 seconds, and should provide enough time for the NVMe/FC device to connect. With this workaround along with the NVMe/FC devices connecting in time, the Kickstart installation proceeds without issues.

Jira:RHEL-8164[1]

ARM-based systems fail to update with a 64k page size kernel when **vdo** is installed

While installing the **vdo** package, RHEL installs the **kmod-kvdo** package and a kernel with **4k** page size as dependencies. As a consequence, updates from RHEL 9.3 to 9.x fail because **kmod-kvdo** conflicts with the 64k kernel.
Workaround: Remove the **vdo** package and its dependencies before attempting to update.

Jira:RHEL-8354

11.10.5. Desktop

WebKitGTK fails to display web pages on IBM Z

The WebKitGTK web browser engine fails when trying to display web pages on the IBM Z architecture. The web page remains blank and the WebKitGTK process ends unexpectedly.
As a consequence, you cannot use certain features of applications that use WebKitGTK to display web pages, such as the following:

- The Evolution mail client
- The GNOME Online Accounts settings
- The GNOME Help application

Jira:RHEL-4157

11.10.6. Virtualization

Starting a VM with an NVIDIA A16 GPU sometimes causes the host GPU to stop working

Currently, if you start a VM that uses an NVIDIA A16 GPU passthrough device, the NVIDIA A16 GPU physical device on the host system in some cases stops working.
To work around the problem, reboot the hypervisor and set the **reset_method** for the GPU device to **bus**:

```
# echo bus > /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
# cat /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
bus
```

For details, see the Red Hat Knowledgebase .

Jira:RHEL-7212[1]

Windows VMs might become unresponsive due to storage errors

On virtual machines (VMs) that use Windows guest operating systems, the system in some cases becomes unresponsive when under high I/O load. When this happens, the system logs a **viostor Reset to device, \Device\RaidPort3, was issued** error. There is currently no workaround for this issue.

Jira:RHEL-1609[1]

Windows 10 VMs with certain PCI devices might become unresponsive on boot

Currently, a virtual machine (VM) that uses a Windows 10 guest operating system might become unresponsive during boot if a **virtio-win-scsi** PCI device with a local disk back end is attached to the VM.
Workaround: Boot the VM with the **multi_queue** option enabled.

Jira:RHEL-1084[1]

The virtio balloon driver sometimes does not work on Windows 10 and Windows 11 VMs

Under certain circumstances, the **virtio-balloon** driver does not work correctly on virtual machines (VMs) that use a Windows 10 or Windows 11 guest operating system. As a consequence, such VMs might not use their assigned memory efficiently.
Jira:RHEL-12118

The virtio file system has suboptimal performance in Windows VMs

Currently, when a virtio file system (virtiofs) is configured on a virtual machine (VM) that uses a Windows guest operating system, the performance of virtiofs in the VM is significantly worse than in VMs that use Linux guests. There is currently no workaround for this issue.

Jira:RHEL-1212[1]

Hot-unplugging a storage device on Windows VMs might fail

On virtual machines (VMs) that use a Windows guest operating system, removing a storage device when the VM is running (also known as a device hot-unplug) in some cases fails. As a consequence, the storage device remains attached to the VM and the disk manager service might become unresponsive. There is currently no workaround for this issue.
Jira:RHEL-869

Hot plugging CPUs to a Windows VM might cause a system failure

When hot plugging the maximum number of CPUs to a Windows virtual machine (VM) with huge pages enabled, the guest operating system might crash with the following *Stop error*:

```
PROCESSOR_START_TIMEOUT
```

There is currently no workaround for this issue.

Jira:RHEL-1220

Updating **virtio** drivers on Windows VMs might fail

When updating the KVM paravirtualized (**virtio**) drivers on a Windows virtual machine (VM), the update might cause the mouse to stop working and the newly installed drivers might not be signed. This problem occurs when updating the **virtio** drivers by installing from the **virtio-win-guest-tools** package, which is a part of the **virtio-win.iso** file.
Workaround: Update the **virtio** drivers by using Windows Device Manager.

Jira:RHEL-574[1]

11.10.7. RHEL in cloud environments

Large VMs might fail to boot into the debug kernel when the kmemleak option is enabled

When attempting to boot a RHEL 9 virtual machine (VM) into the debug kernel, the booting might fail with the following error if the machine kernel is using the **kmemleak=on** argument.

```
Cannot open access to console, the root account is locked.
See sulogin(8) man page for more details.

Press Enter to continue.
```

This problem affects mainly large VMs because they spend more time in the boot sequence.

Workaround: Edit the **/etc/fstab** file on the machine and add extra timeout options to the **/boot** and **/boot/efi** mount points. For example:

```
UUID=e43ead51-b364-419e-92fc-b1f363f19e49 /boot xfs defaults,x-systemd.device-timeout=600,x-systemd.mount-timeout=600 0 0

UUID=7B77-95E7 /boot/efi vfat defaults,uid=0,gid=0,umask=077,shortname=winnt,x-systemd.device-timeout=600,x-systemd.mount-timeout=600 0 2
```

Jira:RHELDOCS-16979[1]

11.11. KNOWN ISSUES IDENTIFIED IN RHEL 9.2

This part describes known issues identified in Red Hat Enterprise Linux 9.2.

11.11.1. Installer and image creation

Unable to load an updated driver from the driver update disc in the installation environment

A new version of a driver from the driver update disc might not load if the same driver from the installation initial ramdisk has already been loaded. As a consequence, an updated version of the driver cannot be applied to the installation environment.
Workaround: Use the **modprobe.blacklist=** kernel command line option together with the **inst.dd** option. For example, to ensure that an updated version of the **virtio_blk** driver from a driver update disc is loaded, use **modprobe.blacklist=virtio_blk** and then continue with the usual procedure to apply drivers from the driver update disk. As a result, the system can load an updated version of the driver and use it in the installation environment.

Jira:RHEL-4762

Kickstart installations fail to configure the network connection

Anaconda performs the Kickstart network configuration only through the NetworkManager API. Anaconda processes the network configuration after the **%pre** Kickstart section. As a consequence, some tasks from the Kickstart **%pre** section are blocked. For example, downloading packages from the **%pre** section fails due to unavailability of the network configuration.
Workaround:

- Configure the network, for example using the **nmcli** tool, as a part of the **%pre** script.
- Use the installation program boot options to configure the network for the **%pre** script.

As a result, it is possible to use the network for tasks in the **%pre** section and the Kickstart installation process completes.

Jira:RHELPLAN-150080[1]

11.11.2. Security

The OSCAP Anaconda add-on does not fetch tailored profiles in the graphical installation

The OSCAP Anaconda add-on does not provide an option to select or deselect tailoring of security profiles in the RHEL graphical installation. Starting from RHEL 8.8, the add-on does not take tailoring into account by default when installing from archives or RPM packages. Consequently, the installation displays the following error message instead of fetching an OSCAP tailored profile:

> There was an unexpected problem with the supplied content.

Workaround: You must specify paths in the **%addon org_fedora_oscap** section of your Kickstart file, for example:

```
xccdf-path = /usr/share/xml/scap/sc_tailoring/ds-combined.xml
tailoring-path = /usr/share/xml/scap/sc_tailoring/tailoring-xccdf.xml
```

As a result, you can use the graphical installation for OSCAP tailored profiles only with the corresponding Kickstart specifications.

Jira:RHEL-1824

Keylime does not accept concatenated PEM certificates

When Keylime receives a certificate chain as multiple certificates in the PEM format concatenated in a single file, the **keylime-agent-rust** Keylime component does not correctly use all the provided certificates during signature verification, resulting in a TLS handshake failure. As a consequence, the client components (**keylime_verifier** and **keylime_tenant**) cannot connect to the Keylime agent. Workaround: Use just one certificate instead of multiple certificates.

Jira:RHELPLAN-157225[1]

OpenSCAP memory-consumption problems

On systems with limited memory, the OpenSCAP scanner might stop prematurely or it might not generate the results files. To work around this problem, you can customize the scanning profile to deselect rules that involve recursion over the entire / file system:

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

- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

Workaround: See the related Knowledgebase article.

Jira:RHELPLAN-145263[1]

11.11.3. Shells and command-line tools

The %vmeff metric from thesysstat package displays incorrect values

The **sysstat** package provides the **%vmeff** metric to measure the page reclaim efficiency. The values of the **%vmeff** column returned by the **sar -B** command are incorrect because **sysstat** does not parse all relevant /**proc**/**vmstat** values provided by later kernel versions.
Workaround: You can calculate the **%vmeff** value manually from the /**proc**/**vmstat** file. For details, see Why the **sar(1)** tool reports **%vmeff** values beyond 100 % in RHEL 8 and RHEL 9?

Jira:RHEL-12009

The Service Location Protocol (SLP) is vulnerable to an attack through UDP

The OpenSLP provides a dynamic configuration mechanism for applications in local area networks, such as printers and file servers. However, SLP is vulnerable to a reflective denial of service amplification attack through UDP on systems connected to the internet. SLP allows an unauthenticated attacker to register new services without limits set by the SLP implementation. By using UDP and spoofing the source address, an attacker can request the service list, creating a Denial of Service on the spoofed address.
To prevent external attackers from accessing the SLP service, disable SLP on all systems running on untrusted networks, such as those directly connected to the internet.

Workaround: Configure firewalls to block or filter traffic on UDP and TCP port 427.

Jira:RHEL-6995[1]

11.11.4. Infrastructure services

libotr is not compliant with FIPS

The **libotr** library and toolkit for off-the-record (OTR) messaging provides end-to-end encryption for instant messaging conversations. However, the **libotr** library does not conform to the Federal Information Processing Standards (FIPS) due to its use of the **gcry_pk_sign()** and **gcry_pk_verify()** functions. As a result, you cannot use the **libotr** library in FIPS mode.

Jira:RHELPLAN-122108[1]

11.11.5. Kernel

Customer applications with dependencies on kernel page size might need updating when moving from 4k to 64k page size kernel

RHEL is compatible with both 4k and 64k page size kernels. Customer applications with dependencies on a 4k kernel page size might require updating when moving from 4k to 64k page size kernels. Known instances of this include **jemalloc** and dependent applications.

The **jemalloc** memory allocator library is sensitive to the page size used in the system's runtime environment. The library can be built to be compatible with 4k and 64k page size kernels, for example, when configured with **--with-lg-page=16** or **env JEMALLOC_SYS_WITH_LG_PAGE=16** (for **jemallocator** Rust crate). Consequently, a mismatch can occur between the page size of the runtime environment and the page size that was present when compiling binaries that depend on **jemalloc**. As a result, using a **jemalloc**-based application triggers the following error:

```
<jemalloc>: Unsupported system page size
```

Workaround: To avoid this problem, use one of the following approaches:

- Use the appropriate build configuration or environment options to create 4k and 64k page size compatible binaries.
- Build any user space packages that use **jemalloc** after booting into the final 64k kernel and runtime environment.

For example, you can build the **fd-find** tool, which also uses **jemalloc**, with the **cargo** Rust package manager. In the final 64k environment, trigger a new build of all dependencies to resolve the mismatch in the page size by entering the **cargo** command:

```
# cargo install fd-find --force
```

Jira:RHELPLAN-147783[1]

Hardware certification of the real-time kernel on systems with large core-counts might require passing the skew-tick=1 boot parameter

Large or moderate sized systems with numerous sockets and large core-counts can experience latency spikes due to lock contentions on **xtime_lock**, which is used in the timekeeping system. As a consequence, latency spikes and delays in hardware certifications might occur on multiprocessing systems.

Workaround: You can offset the timer tick per CPU to start at a different time by adding the **skew_tick=1** boot parameter.

To avoid lock conflicts, enable **skew_tick=1**:

1. Enable the **skew_tick=1** parameter with **grubby**.

   ```
   # grubby --update-kernel=ALL --args="skew_tick=1"
   ```

2. Reboot for changes to take effect.

3. Verify the new settings by displaying the kernel parameters you pass during boot.

   ```
   cat /proc/cmdline
   ```

Note that enabling **skew_tick=1** causes a significant increase in power consumption and, therefore, it must be enabled only if you are running latency sensitive real-time workloads.

Jira:RHEL-9318[1]

11.11.6. File systems and storage

Disabling quota accounting is no longer possible for an XFS filesystem mounted with quotas enabled

Starting with RHEL 9.2, it is no longer possible to disable quota accounting on an XFS filesystem which has been mounted with quotas enabled.
Workaround: Disable quota accounting by remounting the filesystem, with the quota option removed.

Jira:RHELPLAN-145001[1]

udev rule change for NVMe devices

There is a udev rule change for NVMe devices that adds **OPTIONS="string_escape=replace"** parameter. This leads to a disk by-id naming change for some vendors, if the serial number of your device has leading whitespace.

Jira:RHELPLAN-154195[1]

11.11.7. Dynamic programming languages, web and database servers

python3.11-lxml does not provide the**lxml.isoschematron** submodule

The **python3.11-lxml** package is distributed without the **lxml.isoschematron** submodule because it is not under an open source license. The submodule implements ISO Schematron support. As an alternative, pre-ISO-Schematron validation is available in the **lxml.etree.Schematron** class. The remaining content of the **python3.11-lxml** package is unaffected.

Jira:RHELPLAN-143480[1]

11.11.8. Identity Management

Adding a RHEL 9 replica in FIPS mode to an IdM deployment in FIPS mode that was initialized with RHEL 8.6 or earlier fails

The default RHEL 9 FIPS cryptographic policy aiming to comply with FIPS 140-3 does not allow the use of the AES HMAC-SHA1 encryption types' key derivation function as defined by RFC3961, section 5.1.
This constraint is a blocker when adding a RHEL 9 Identity Management (IdM) replica in FIPS mode to a RHEL 8 IdM environment in FIPS mode in which the first server was installed on a RHEL 8.6 system or earlier. This is because there are no common encryption types between RHEL 9 and the previous RHEL versions, which commonly use the AES HMAC-SHA1 encryption types but do not use the AES HMAC-SHA2 encryption types.

You can view the encryption type of your IdM master key by entering the following command on the server:

```
# kadmin.local getprinc K/M | grep -E '^Key:'
```

For more information, see the AD Domain Users unable to login in to the FIPS-compliant environment KCS solution.

Jira:RHEL-4888

Installing a RHEL 7 IdM client with a RHEL 9.2 and later IdM server in FIPS mode fails due to EMS enforcement

The TLS **Extended Master Secret** (EMS) extension (RFC 7627) is now mandatory for TLS 1.2 connections on FIPS-enabled RHEL 9.2 and later systems. This is in accordance with FIPS-140-3 requirements. However, the **openssl** version available in RHEL 7.9 and lower does not support EMS. In consequence, installing a RHEL 7 Identity Management (IdM) client with a FIPS-enabled IdM server running on RHEL 9.2 and later fails.
Workaround: If upgrading the host to RHEL 8 before installing an IdM client on it is not an option, remove the requirement for EMS usage on the RHEL 9 server by applying a NO-ENFORCE-EMS subpolicy on top of the FIPS crypto policy:

```
# update-crypto-policies --set FIPS:NO-ENFORCE-EMS
```

Note that this removal goes against the FIPS 140-3 requirements. As a result, you can establish and accept TLS 1.2 connections that do not use EMS, and the installation of a RHEL 7 IdM client succeeds.

Jira:RHEL-4955

11.11.9. Red Hat Enterprise Linux System Roles

If **firewalld.service** is masked, using the **firewall** RHEL System Role fails

If **firewalld.service** is masked on a RHEL system, the **firewall** RHEL System Role fails.
Workaround: Unmask the **firewalld.service**:

```
systemctl unmask firewalld.service
```

Jira:RHELPLAN-133165[1]

Unable to register systems with environment names

The **rhc** system role fails to register the system when specifying environment names in **rhc_environment**.
Workaround: Use environment IDs instead of environment names while registering.

Jira:RHEL-1172

11.11.10. Virtualization

Windows Server 2016 VMs sometimes stops working after hot-plugging a vCPU

Currently, assigning a vCPU to a running virtual machine (VM) with a Windows Server 2016 guest operating system might cause a variety of problems, such as the VM terminating unexpectedly, becoming unresponsive, or rebooting. There is currently no workaround for this issue.

Jira:RHELPLAN-63771[1]

Redundant error messages on VMs with NVIDIA passthrough devices

When using an Intel host machine with a RHEL 9.2 and later operating system, virtual machines (VMs) with a passed through NVDIA GPU device frequently log the following error message:

```
Spurious APIC interrupt (vector 0xFF) on CPU#2, should never happen.
```

However, this error message does not impact the functionality of the VM and can be ignored. For details, see the Red Hat KnoweldgeBase .

Jira:RHELPLAN-141042[1]

Restarting the OVS service on a host might block network connectivity on its running VMs

When the Open vSwitch (OVS) service restarts or crashes on a host, virtual machines (VMs) that are running on this host cannot recover the state of the networking device. As a consequence, VMs might be completely unable to receive packets.
This problem only affects systems that use the packed virtqueue format in their **virtio** networking stack.

Workaround: Use the **packed=off** parameter in the **virtio** networking device definition to disable packed virtqueue. With packed virtqueue disabled, the state of the networking device can, in some situations, be recovered from RAM.

Jira:RHEL-333

Recovering an interrupted post-copy VM migration might fail

If a post-copy migration of a virtual machine (VM) is interrupted and then immediately resumed on the same incoming port, the migration might fail with the following error: **Address already in use**
Workaround: Wait at least 10 seconds before resuming the post-copy migration or switch to another port for migration recovery.

Jira:RHEL-7096

NUMA node mapping not working correctly on AMD EPYC CPUs

QEMU does not handle NUMA node mapping on AMD EPYC CPUs correctly. As a result, the performance of virtual machines (VMs) with these CPUs might be negatively impacted if using a NUMA node configuration. In addition, the VMs display a warning similar to the following during boot.

```
sched: CPU #4's llc-sibling CPU #3 is not on the same node! [node: 1 != 0]. Ignoring dependency.
WARNING: CPU: 4 PID: 0 at arch/x86/kernel/smpboot.c:415 topology_sane.isra.0+0x6b/0x80
```

Workaround: Do not use AMD EPYC CPUs for NUMA node configurations.

Jira:RHELPLAN-150884[1]

virsh blkiotune --weight command fails to set the correct cgroup I/O controller value

Currently, using the **virsh blkiotune --weight** command to set the VM weight does not work as expected. The command fails to set the correct **io.bfq.weight** value in the cgroup I/O controller interface file. There is no workaround at this time.

Jira:RHELPLAN-83423[1]

The **Extended Master Secret** TLS Extension is now enforced on FIPS-enabled systems

With the release of the RHSA-2023:3722 advisory, the TLS **Extended Master Secret** (EMS) extension (RFC 7627) is mandatory for TLS 1.2 connections on FIPS-enabled RHEL 9 systems. This is in accordance with FIPS-140-3 requirements. TLS 1.3 is not affected.
Legacy clients that do not support EMS or TLS 1.3 now cannot connect to FIPS servers running on RHEL 9 and 10. Similarly, RHEL 9 and 10 clients in FIPS mode cannot connect to servers that only support TLS 1.2 without EMS. This in practice means that these clients cannot connect to servers on RHEL 6, RHEL 7 and non-RHEL legacy operating systems. This is because the legacy 1.0.x versions of OpenSSL do not support EMS or TLS 1.3.

In addition, connecting from a FIPS-enabled RHEL client to a hypervisor such as VMWare ESX now fails with a **Provider routines::ems not enabled** error if the hypervisor uses TLS 1.2 without EMS. To work around this problem, update the hypervisor to support TLS 1.3 or TLS 1.2 with the EMS extension. For VMWare vSphere, this means version 8.0 or later.

For more information, see TLS Extension "Extended Master Secret" enforced with Red Hat Enterprise Linux 9.2 and later.

Jira:RHEL-13340[1]

11.12. KNOWN ISSUES IDENTIFIED IN RHEL 9.1

This part describes known issues identified in Red Hat Enterprise Linux 9.1.

11.12.1. Installer and image creation

RHEL for Edge installer image fails to create mount points when installing an **rpm-ostree** payload

When deploying **rpm-ostree** payloads, used for example in a RHEL for Edge installer image, the installation program does not properly create some mount points for custom partitions. As a consequence, the installation stops with the following error:

```
The command 'mount --bind /mnt/sysimage/data /mnt/sysroot/data' exited with the code 32.
```

Workaround:

- Use an automatic partitioning scheme and do not add any mount points manually.
- Manually assign mount points inside the **/var** directory (for example, **/var/*my-mount-point***) or to the following standard directories: /, **/boot**, **/var**.

As a result, the installation process finishes successfully.

Jira:RHEL-4741

NetworkManager fails to start after the installation when connected to a network but without DHCP or a static IP address configured

Starting with RHEL 9.0, Anaconda activates network devices automatically when there is no specific **ip=** or Kickstart network configuration set. Anaconda creates a default persistent configuration file for each Ethernet device. The connection profile has the **ONBOOT** and **autoconnect** value set to **true**. As a consequence, during the start of the installed system, RHEL activates the network devices, and the **networkManager-wait-online** service fails.

Workaround: Do one of the following:

- Delete all connections using the **nmcli** utility except one connection you want to use. For example:
  a. List all connection profiles:

```
# nmcli connection show
```

  b. Delete the connection profiles that you do not require:

```
# nmcli connection delete <connection_name>
```

  Replace <connection_name> with the name of the connection you want to delete.

- Disable the auto connect network feature in Anaconda if no specific **ip=** or Kickstart network configuration is set.
  a. In the Anaconda GUI, navigate to **Network & Host Name**
  b. Select a network device to disable.
  c. Click **Configure**.
  d. On the **General** tab, clear the **Connect automatically with priority** checkbox.
  e. Click **Save**.

Jira:RHELPLAN-130370[1]

11.12.2. Security

With a specific syntax, scp empties files copied to themselves

The **scp** utility changed from the Secure copy protocol (SCP) to the more secure SSH file transfer protocol (SFTP). Consequently, copying a file from a location to the same location erases the file content. The problem affects the following syntax:
scp localhost:/myfile localhost:/myfile

Workaround: Do not copy files to a destination that is the same as the source location using this syntax.

The problem has been fixed for the following syntaxes:

- **scp /myfile localhost:/myfile**
- **scp localhost:~/myfile ~/myfile**

Jira:RHELPLAN-113842[1]

11.12.3. Networking

The iwl7260-firmware causes Wi-Fi issues on Intel Wi-Fi 6 AX200, AX210, and Lenovo ThinkPad P1 Gen 4

If you update the **iwl7260-firmware** or **iwl7260-wifi** driver to the version provided with RHEL 9.1 or later, the hardware might enter in an incorrect state and report its status incorrectly. Consequently, Intel Wi-Fi 6 cards might fail to function properly and display the following error message:

```
kernel: iwlwifi 0000:09:00.0: Failed to start RT ucode: -110
kernel: iwlwifi 0000:09:00.0: WRT: Collecting data: ini trigger 13 fired (delay=0ms)
kernel: iwlwifi 0000:09:00.0: Failed to run INIT ucode: -110
```

Workaround: An unconfirmed workaround is to power off the system completely and then power it back on. Do not perform a reboot.

Jira:RHELPLAN-134771[1]

11.12.4. Kernel

The Delay Accounting functionality does not display the SWAPIN and IO% statistics columns by default

The **Delayed Accounting** functionality, unlike early versions, is disabled by default. Consequently, the **iotop** application does not show the **SWAPIN** and **IO%** statistics columns and displays the following warning:

```
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN and IO%
```

The **Delay Accounting** functionality, using the **taskstats** interface, provides the delay statistics for all tasks or threads that belong to a thread group. Delays in task execution occur when they wait for a kernel resource to become available, for example, a task waiting for a free CPU to run on. The statistics help in setting a task's CPU priority, I/O priority, and **rss** limit values appropriately.

Workaround: You can enable the **delayacct** boot option either at run time or boot.

- To enable **delayacct** at run time, enter:

  ```
  echo 1 > /proc/sys/kernel/task_delayacct
  ```

  Note that this command enables the feature system wide, but only for the tasks that you start after running this command.

- To enable **delayacct** permanently at boot, use one of the following procedures:
  - Edit the **/etc/sysctl.conf** file to override the default parameters:
    a. Add the following entry to the **/etc/sysctl.conf** file:

    ```
    kernel.task_delayacct = 1
    ```

    For more information, see How to set sysctl variables on Red Hat Enterprise Linux .

    b. Reboot the system for changes to take effect.
  - Add the **delayacct** option to the kernel command line.
    For more information, see Configuring kernel command-line parameters.

As a result, the **iotop** application displays the **SWAPIN** and **IO%** statistics columns.

Jira:RHELPLAN-135779[1]

The **kdump** service fails to build the **initrd** file on IBM Z systems

On the 64-bit IBM Z systems, the **kdump** service fails to load the initial RAM disk (**initrd**) when **znet** related configuration information such as **s390-subchannels** reside in an inactive **NetworkManager** connection profile. Consequently, the **kdump** mechanism fails with the following error:

```
dracut: Failed to set up znet
kdump: mkdumprd: failed to make kdump initrd
```

As a workaround, use one of the following solutions:

- Configure a network bond or bridge by re-using the connection profile that has the **znet** configuration information:

```
$ nmcli connection modify enc600 master bond0 slave-type bond
```

- Copy the **znet** configuration information from the inactive connection profile to the active connection profile:

  a. Run the **nmcli** command to query the **NetworkManager** connection profiles:

```
# nmcli connection show

NAME                    UUID              TYPE   Device

bridge-br0          ed391a43-bdea-4170-b8a2 bridge   br0
bridge-slave-enc600  caf7f770-1e55-4126-a2f4 ethernet enc600
enc600              bc293b8d-ef1e-45f6-bad1 ethernet --
```

  b. Update the active profile with configuration information from the inactive connection:

```
#!/bin/bash
 inactive_connection=enc600
 active_connection=bridge-slave-enc600
 for name in nettype subchannels options; do
 field=802-3-ethernet.s390-$name
 val=$(nmcli --get-values "$field"connection show "$inactive_connection")
 nmcli connection modify "$active_connection" "$field" $val"
 done
```

  c. Restart the **kdump** service for changes to take effect:

```
# kdumpctl restart
```

Jira:RHELPLAN-115732[1]

weak-modules from **kmod** fails to work with module inter-dependencies

The **weak-modules** script provided by the **kmod** package determines which modules are kABI-compatible with installed kernels. However, while checking modules' kernel compatibility, **weak-modules** processes modules symbol dependencies from higher to lower release of the kernel for

which they were built. As a consequence, modules with inter-dependencies built against different kernel releases might be interpreted as non-compatible, and therefore the **weak-modules** script fails to work in this scenario.
Workaround: Build or put the extra modules against the latest stock kernel before you install the new kernel.

Jira:RHELPLAN-126922[1]

11.12.5. Identity Management

IdM in FIPS mode does not support using the NTLMSSP protocol to establish a two-way cross-forest trust

Establishing a two-way cross-forest trust between Active Directory (AD) and Identity Management (IdM) with FIPS mode enabled fails because the New Technology LAN Manager Security Support Provider (NTLMSSP) authentication is not FIPS-compliant. IdM in FIPS mode does not accept the RC4 NTLM hash that the AD domain controller uses when attempting to authenticate.

Jira:RHEL-12154[1]

Heimdal client fails to authenticate a user using PKINIT against RHEL 9 KDC

By default, a Heimdal Kerberos client initiates the PKINIT authentication of an IdM user by using Modular Exponential (MODP) Diffie-Hellman Group 2 for Internet Key Exchange (IKE). However, the MIT Kerberos Distribution Center (KDC) on RHEL 9 only supports MODP Group 14 and 16. Consequently, the pre-autentication request fails with the **krb5_get_init_creds: PREAUTH_FAILED** error on the Heimdal client and **Key parameters not accepted** on the RHEL MIT KDC.

Workaround: Ensure that the Heimdal client uses MODP Group 14. Set the **pkinit_dh_min_bits** parameter in the **libdefaults** section of the client configuration file to 1759:

```
[libdefaults]
pkinit_dh_min_bits = 1759
```

As a result, the Heimdal client completes the PKINIT pre-authentication against the RHEL MIT KDC.

Jira:RHELDOCS-19846[1]

11.12.6. Desktop

User Creation screen is unresponsive

When installing RHEL using a graphical user interface, the User Creation screen is unresponsive. As a consequence, creating users during installation is more difficult.
Workaround: Use one of the following solutions to create users:

- Run the installation in VNC mode and resize the VNC window.
- Create users after completing the installation process.

Jira:RHEL-11924[1]

11.12.7. Virtualization

Host network cannot ping VMs with VFs during live migration

When live migrating a virtual machine (VM) with a configured virtual function (VF), such as a VMs that uses virtual SR-IOV software, the network of the VM is not visible to other devices and the VM cannot be reached by commands such as **ping**. After the migration is finished, however, the problem no longer occurs.
Jira:RHEL-7336

Migrated IdM users might be unable to log in due to mismatching domain SIDs

If you have used the **ipa migrate-ds** script to migrate users from one IdM deployment to another, those users might have problems using IdM services because their previously existing Security Identifiers (SIDs) do not have the domain SID of the current IdM environment. For example, those users can retrieve a Kerberos ticket with the **kinit** utility, but they cannot log in.
Workaround: See the following Knowledgebase article: Migrated IdM users unable to log in due to mismatching domain SIDs.

Jira:RHELPLAN-109613[1]

Windows VM fails to get IP address after network interface reset

Sometimes, Windows virtual machines fail to get an IP address after an automatic network interface reset. As a consequence, the VM fails to connect to the network.
Workaround: Disable and re-enable the network adapter driver in the Windows Device Manager.

Jira:RHEL-11366

PCIe ATS devices do not work on Windows VMs

When you configure a PCIe Address Translation Services (ATS) device in the XML configuration of virtual machine (VM) with a Windows guest operating system, the guest does not enable the ATS device after booting the VM. This is because Windows currently does not support ATS on **virtio** devices.
For more information, see the Red Hat KnowledgeBase .

Jira:RHELPLAN-118495[1]

11.12.8. RHEL in cloud environments

RHEL instances on Azure fail to boot if provisioned by cloud-init and configured with an NFSv3 mount entry

Currently, booting a RHEL virtual machine (VM) on the Microsoft Azure cloud platform fails if the VM was provisioned by the **cloud-init** tool and the guest operating system of the VM has an NFSv3 mount entry in the **/etc/fstab** file. There is currently no workaround for this issue.

Jira:RHELPLAN-120807[1]

11.13. KNOWN ISSUES IDENTIFIED IN RHEL 9.0

This part describes known issues identified in Red Hat Enterprise Linux 9.0.

11.13.1. Installer and image creation

Local Media installation source is not detected when booting the installation from a USB that is created using a third party tool

When booting the RHEL installation from a USB that is created using a third party tool, the installation program fails to detect the **Local Media** installation source (only *Red Hat CDN* is detected).
This issue occurs because the default boot option **int.stage2=** attempts to search for **iso9660** image format. However, a third party tool might create an ISO image with a different format.

Workaround: Use either of the following solution:

- When booting the installation, click the **Tab** key to edit the kernel command line, and change the boot option **inst.stage2=** to **inst.repo=**.
- To create a bootable USB device on Windows, use Fedora Media Writer.
- When using a third party tool such as Rufus to create a bootable USB device, first regenerate the RHEL ISO image on a Linux system, and then use the third party tool to create a bootable USB device.

For more information on the steps involved in performing any of the specified workaround, see, Installation media is not auto-detected during the installation of RHEL 8.3 .

Jira:RHELPLAN-53644[1]

Anaconda fails to verify existence of an administrator user account

While installing RHEL using a graphical user interface, Anaconda fails to verify if the administrator account has been created. As a consequence, users might install a system without any administrator user account.
Workaround: Ensure you configure an administrator user account or the root password is set and the root account is unlocked. As a result, users can perform administrative tasks on the installed system.

Jira:RHELPLAN-110191[1]

New XFS features prevent booting of PowerNV IBM POWER systems with firmware older than version 5.10

PowerNV IBM POWER systems use a Linux kernel for firmware, and use Petitboot as a replacement for GRUB. This results in the firmware kernel mounting **/boot** and Petitboot reading the GRUB config and booting RHEL.
The RHEL 9 kernel introduces **bigtime=1** and **inobtcount=1** features to the XFS filesystem, which kernels with firmware older than version 5.10 do not understand.

Workaround: You can use another filesystem for **/boot**, for example ext4.

Jira:RHELPLAN-94811[1]

The Installation process sometimes becomes unresponsive

When you install RHEL, the installation process sometimes becomes unresponsive. The **/tmp/packaging.log** file displays the following message at the end:

```
10:20:56,416 DDEBUG dnf: RPM transaction over.
```

Workaround: Restart the installation process.

Jira:RHELPLAN-118420[1]

The **services** Kickstart command fails to disable the **firewalld** service

A bug in Anaconda prevents the **services --disabled=firewalld** command from disabling the **firewalld** service in Kickstart.
Workaround: Use the **firewall --disabled** command instead. As a result, the **firewalld** service is disabled properly.

Jira:RHEL-82566

Kickstart installation fails with an unknown disk error when **ignoredisk** command precedes **iscsi** command

Installing RHEL by using the kickstart method fails if the **ignoredisk** command is placed before the **iscsi** command. This issue occurs because the **iscsi** command attaches the specified iSCSI device during command parsing, while the **ignoredisk** command resolves device specifications simultaneously. If the **ignoredisk** command references an iSCSI device name before it is attached by the **iscsi** command, the installation fails with an "unknown disk" error.
Workaround: Ensure that the **iscsi** command is placed before the **ignoredisk** command in the Kickstart file to reference the iSCSI disk and enable successful installation.

Jira:RHEL-13837

11.13.2. Security

OpenSSL does not detect if a PKCS #11 token supports the creation of raw RSA or RSA-PSS signatures

The TLS 1.3 protocol requires support for RSA-PSS signatures. If a PKCS #11 token does not support raw RSA or RSA-PSS signatures, server applications that use the OpenSSL library fail to work with an RSA key if the key is held by the PKCS #11 token. As a result, TLS communication fails in the described scenario.
Workaround: Configure servers and clients to use TLS version 1.2 as the highest TLS protocol version available.

Jira:RHELPLAN-50959[1]

OpenSSL incorrectly handles PKCS #11 tokens that does not support raw RSA or RSA-PSS signatures

The **OpenSSL** library does not detect key-related capabilities of PKCS #11 tokens. Consequently, establishing a TLS connection fails when a signature is created with a token that does not support raw RSA or RSA-PSS signatures.
Workaround: Add the following lines after the **.include** line at the end of the **crypto_policy** section in the **/etc/pki/tls/openssl.cnf** file:

```
SignatureAlgorithms =
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384
```

```
MaxProtocol = TLSv1.2
```

As a result, a TLS connection can be established in the described scenario.

Jira:RHELPLAN-48241[1]

Ansible remediations require additional collections

With the replacement of Ansible Engine by the **ansible-core** package, the list of Ansible modules provided with the RHEL subscription is reduced. As a consequence, running remediations that use Ansible content included within the **scap-security-guide** package requires collections from the **rhc-worker-playbook** package.
For an Ansible remediation, perform the following steps:

1. Install the required packages:

```
# dnf install -y ansible-core scap-security-guide rhc-worker-playbook
```

2. Navigate to the **/usr/share/scap-security-guide/ansible** directory:

```
# cd /usr/share/scap-security-guide/ansible
```

3. Run the relevant Ansible playbook using environment variables that define the path to the additional Ansible collections:

```
# ANSIBLE_COLLECTIONS_PATH=/usr/share/rhc-worker-playbook/ansible/collections/ansible_collections/ ansible-playbook -c local -i localhost, rhel9-playbook-cis_server_l1.yml
```

Replace ***cis_server_l1*** with the ID of the profile against which you want to remediate the system.

As a result, the Ansible content is processed correctly.

NOTE

Support of the collections provided in **rhc-worker-playbook** is limited to enabling the Ansible content sourced in **scap-security-guide**.

Jira:RHEL-1800

Default SELinux policy allows unconfined executables to make their stack executable

The default state of the **selinuxuser_execstack** boolean in the SELinux policy is on, which means that unconfined executables can make their stack executable. Executables should not use this option, and it might indicate poorly coded executables or a possible attack. However, due to compatibility with other tools, packages, and third-party products, Red Hat cannot change the value of the boolean in the default policy. If your scenario does not depend on such compatibility aspects, you can turn the boolean off in your local policy by entering the command **setsebool -P selinuxuser_execstack off**.

Jira:RHELPLAN-115609[1]

SSH timeout rules in STIG profiles configure incorrect options

An update of OpenSSH affected the rules in the following Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) profiles:

- DISA STIG for RHEL 9 (**xccdf_org.ssgproject.content_profile_stig**)
- DISA STIG with GUI for RHEL 9 (**xccdf_org.ssgproject.content_profile_stig_gui**)

In each of these profiles, the following two rules are affected:

```
Title: Set SSH Client Alive Count Max to zero
CCE Identifier: CCE-90271-8
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0

Title: Set SSH Idle Timeout Interval
CCE Identifier: CCE-90811-1
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout
```

When applied to SSH servers, each of these rules configures an option (**ClientAliveCountMax** and **ClientAliveInterval**) that no longer behaves as previously. As a consequence, OpenSSH no longer disconnects idle SSH users when it reaches the timeout configured by these rules.

Workaround: These rules have been temporarily removed from the DISA STIG for RHEL 9 and DISA STIG with GUI for RHEL 9 profiles until a solution is developed.

Jira:RHELPLAN-107318[1]

GnuPG incorrectly allows using SHA-1 signatures even if disallowed by crypto-policies

The GNU Privacy Guard (GnuPG) cryptographic software can create and verify signatures that use the SHA-1 algorithm regardless of the settings defined by the system-wide cryptographic policies. Consequently, you can use SHA-1 for cryptographic purposes in the **DEFAULT** cryptographic policy, which is not consistent with the system-wide deprecation of this insecure algorithm for signatures. Workaround: Do not use GnuPG options that involve SHA-1. As a result, you will prevent GnuPG from lowering the default system security by using the insecure SHA-1 signatures.

Jira:RHELPLAN-117566[1]

11.13.3. Shells and command-line tools

Setting the console keymap requires the libxkbcommon library on your minimal install

In RHEL 9, certain **systemd** library dependencies have been converted from dynamic linking to dynamic loading, so that your system opens and uses the libraries at runtime when they are available. With this change, a functionality that depends on such libraries is not available unless you install the necessary library. This also affects setting the keyboard layout on systems with a minimal install. As a result, the **localectl --no-convert set-x11-keymap gb** command fails.
Workaround: Install the **libxkbcommon** library:

```
# dnf install libxkbcommon
```

Jira:RHEL-6105

11.13.4. Networking

Network teams might not contain port-specific metadata

A earlier update to NetworkManager changed the handling of team ports to resolve potential race conditions. As a result, when you defined a port configuration within the team controller's connection profile, NetworkManager might ignore it. Consequently, utilities such as **teamdctl** might fail to display port-specific metadata, such as priority or sticky status, when you defined these settings in the team controller's connection profile.

To work around this problem, manually copy the team port configuration from the controller to each individual port connection. For example, to migrate the configuration from the **team0** profile to the **enp1s0** and **enp2s0** port profiles, enter:

```
for port in enp1s0 enp2s0; do
    # Copy the port configuration to port connections
    nmcli connection modify $port team-port.config "$(nmcli --escape no --get team.config
connection show team0 | jq .ports.${port})"
done

# Delete the port configuration from the team connection
nmcli connection modify team0 team.config "$(nmcli --escape no --get team.config connection
show team0 | jq 'del(.ports)')"
```

As a result, NetworkManager correctly applies the port-specific settings and management utilities display them correctly.

Jira:RHEL-87994

kTLS does not support offloading of TLS 1.3 to NICs

Kernel Transport Layer Security (kTLS) does not support offloading of TLS 1.3 to NICs. Consequently, software encryption is used with TLS 1.3 even when the NICs support TLS offload.

Workaround: Disable TLS 1.3 if offload is required. As a result, you can offload only TLS 1.2. When TLS 1.3 is in use, there is lower performance, since TLS 1.3 cannot be offloaded.

Jira:RHELPLAN-96004[1]

Failure to update the session key causes the connection to break

Kernel Transport Layer Security (kTLS) protocol does not support updating the session key, which is used by the symmetric cipher. Consequently, the user cannot update the key, which causes a connection break.

Workaround: Disable kTLS. As a result, with the workaround, it is possible to successfully update the session key.

Jira:RHELPLAN-99859[1]

Renaming network interfaces using ifcfg files fails

On RHEL 9, the **initscripts** package is not installed by default. Consequently, renaming network interfaces using **ifcfg** files fails.

Workaround: To solve this problem, Red Hat recommends that you use **udev** rules or link files to rename interfaces. For further details, see Consistent network interface device naming and the **systemd.link(5)** man page.

If you cannot use one of the recommended solutions, install the **initscripts** package.

Jira:RHELPLAN-100926[1]

The **initscripts** package is not installed by default

By default, the **initscripts** package is not installed. As a consequence, the **ifup** and **ifdown** utilities are not available.
Workaround: As an alternative, use the **nmcli connection up** and **nmcli connection down** commands to enable and disable connections. If the suggested alternative does not work for you, report the problem and install the **NetworkManager-initscripts-updown** package, which provides a NetworkManager solution for the **ifup** and **ifdown** utilities.

Jira:RHELPLAN-121205[1]

11.13.5. Kernel

dkms provides an incorrect warning on program failure with correctly compiled drivers on 64-bit ARM CPUs

The Dynamic Kernel Module Support (**dkms**) utility does not recognize that the kernel headers for 64-bit ARM CPUs work for both the kernels with 4 kilobytes and 64 kilobytes page sizes. As a result, when the kernel update is performed and the **kernel-64k-devel** package is not installed, **dkms** provides an incorrect warning on why the program failed on correctly compiled drivers.
Workaround: Install the **kernel-headers** package, which contains header files for both types of ARM CPU architectures and is not specific to **dkms** and its requirements.

Jira:RHEL-25967[1]

11.13.6. File systems and storage

Device Mapper Multipath is not supported with NVMe/TCP

Using Device Mapper Multipath with the **nvme-tcp** driver can result in the Call Trace warnings and system instability. To work around this problem, NVMe/TCP users must enable native NVMe multipathing and not use the **device-mapper-multipath** tools with NVMe.
By default, Native NVMe multipathing is enabled in RHEL 9. For more information, see Enabling multipathing on NVMe devices.

Jira:RHELPLAN-105944[1]

11.13.7. Dynamic programming languages, web and database servers

The **chkconfig** package is not installed by default in RHEL 9

The **chkconfig** package, which updates and queries runlevel information for system services, is not installed by default in RHEL 9.
To manage services, use the **systemctl** commands or install the **chkconfig** package manually.

For more information about **systemd**, see Introduction to systemd. For instructions on how to use the **systemctl** utility, see Managing system services with systemctl.

Jira:RHELPLAN-112043[1]

The --ssl-fips-mode option in MySQL and MariaDB does not change FIPS mode

The **--ssl-fips-mode** option in **MySQL** and **MariaDB** in RHEL works differently than in upstream. In RHEL 9, if you use **--ssl-fips-mode** as an argument for the **mysqld** or **mariadbd** daemon, or if you use **ssl-fips-mode** in the **MySQL** or **MariaDB** server configuration files, **--ssl-fips-mode** does not change FIPS mode for these database servers.

Instead:

- If you set **--ssl-fips-mode** to **ON**, the **mysqld** or **mariadbd** server daemon does not start.
- If you set **--ssl-fips-mode** to **OFF** on a FIPS-enabled system, the **mysqld** or **mariadbd** server daemons still run in FIPS mode.

This is expected because FIPS mode should be enabled or disabled for the whole RHEL system, not for specific components.

Therefore, do not use the **--ssl-fips-mode** option in **MySQL** or **MariaDB** in RHEL. Instead, ensure FIPS mode is enabled on the whole RHEL system:

- Preferably, install RHEL with FIPS mode enabled. Enabling FIPS mode during the installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place. For information about installing RHEL in FIPS mode, see Switching RHEL to FIPS mode.
- Alternatively, you can switch FIPS mode for the entire RHEL system by following the procedure in Switching the system to FIPS mode .

Jira:RHELPLAN-92864[1]

11.13.8. Compilers and development tools

Both bind and unbound disable validation of SHA-1-based signatures

The **bind** and **unbound** components disable validation support of all RSA/SHA1 (algorithm number 5) and RSASHA1-NSEC3-SHA1 (algorithm number 7) signatures, and the SHA-1 usage for signatures is restricted in the DEFAULT system-wide cryptographic policy.
As a result, certain DNSSEC records signed with the SHA-1, RSA/SHA1, and RSASHA1-NSEC3-SHA1 digest algorithms fail to verify in Red Hat Enterprise Linux 9 and the affected domain names become vulnerable.

To work around this problem, upgrade to a different signature algorithm, such as RSA/SHA-256 or elliptic curve keys.

For more information and a list of top-level domains that are affected and vulnerable, see the DNSSEC records signed with RSASHA1 fail to verify solution.

Jira:RHELPLAN-117492[1]

named fails to start if the same writable zone file is used in multiple zones

BIND does not allow the same writable zone file in multiple zones. Consequently, if a configuration includes multiple zones which share a path to a file that can be modified by the **named** service, **named** fails to start.
Workaround: Use the **in-view** clause to share one zone between multiple views and make sure to use different paths for different zones. For example, include the view names in the path.

Note that writable zone files are typically used in zones with allowed dynamic updates, secondary zones, or zones maintained by DNSSEC.

Jira:RHELPLAN-90604[1]

11.13.9. Identity Management

The DEFAULT:SHA1 subpolicy has to be set on RHEL 9 clients for PKINIT to work against AD KDCs

The SHA-1 digest algorithm has been deprecated in RHEL 9, and CMS messages for Public Key Cryptography for initial authentication (PKINIT) are now signed with the stronger SHA-256 algorithm.
However, the Active Directory (AD) Kerberos Distribution Center (KDC) still uses the SHA-1 digest algorithm to sign CMS messages. As a result, RHEL 9 Kerberos clients fail to authenticate users by using PKINIT against an AD KDC.

Workaround: Enable support for the SHA-1 algorithm on your RHEL 9 systems with the following command:

```
# update-crypto-policies --set DEFAULT:SHA1
```

Jira:RHELPLAN-114497[1]

The PKINIT authentication of a user fails if a RHEL 9 Kerberos agent communicates with a non-RHEL-9, non-AD Kerberos agent

If a RHEL 9 Kerberos agent, either a client or Kerberos Distribution Center (KDC), interacts with a non-RHEL-9 Kerberos agent that is not an Active Directory (AD) agent, the PKINIT authentication of the user fails.
Workaround: Perform one of the following actions:

- Set the RHEL 9 agent's crypto-policy to **DEFAULT:SHA1** to allow the verification of SHA-1 signatures:

  ```
  # update-crypto-policies --set DEFAULT:SHA1
  ```

- Update the non-RHEL-9 and non-AD agent to ensure it does not sign CMS data using the SHA-1 algorithm. For this, update your Kerberos client or KDC packages to the versions that use SHA-256 instead of SHA-1:
  - CentOS 9 Stream: krb5-1.19.1-15
  - RHEL 8.7: krb5-1.18.2-17
  - RHEL 7.9: krb5-1.15.1-53
  - Fedora Rawhide/36: krb5-1.19.2-7
  - Fedora 35/34: krb5-1.19.2-3

As a result, the PKINIT authentication of the user works correctly.

Note that for other operating systems, it is the krb5-1.20 release that ensures that the agent signs CMS data with SHA-256 instead of SHA-1.

See also ???TITLE???.

Jira:RHEL-4875

FIPS support for AD trust requires the AD-SUPPORT crypto subpolicy

Active Directory (AD) uses AES SHA-1 HMAC encryption types, which are not allowed in FIPS mode on RHEL 9 by default. If you want to use RHEL 9 IdM hosts with an AD trust, enable support for AES SHA-1 HMAC encryption types before installing IdM software.
Since FIPS compliance is a process that involves both technical and organizational agreements, consult your FIPS auditor before enabling the **AD-SUPPORT** subpolicy to allow technical measures to support AES SHA-1 HMAC encryption types, and then install RHEL IdM:

```
# update-crypto-policies --set FIPS:AD-SUPPORT
```

Jira:RHELPLAN-113281[1]

11.13.10. Desktop

VNC is not running after upgrading to RHEL 9

After upgrading from RHEL 8 to RHEL 9, the VNC server fails to start, even if it was previously enabled.
Workaround: Manually enable the **vncserver** service after the system upgrade:

```
# systemctl enable --now vncserver@:port-number
```

As a result, VNC is now enabled and starts after every system boot as expected.

Jira:RHELPLAN-114314[1]

xorg -configure fails to create an Xorg configuration file on a virtual machine

Running **xorg -configure** to create the Xorg configuration file on virtual machines fails due to the lack of devices to configure. This issue leads to a configuration failure. To work around this issue, construct the **xorg.conf** file manually according to the guidelines stated in Xorg documentation, or use alternative mechanisms such as an Extended Display Identification Data (EDID) override to tweak display resolutions. With this workaround, the Xorg server functions with the correct configuration.
Jira:RHELDOCS-20196[1]

11.13.11. Graphics infrastructures

NVIDIA drivers might revert to X.org

Under certain conditions, the proprietary NVIDIA drivers disable the Wayland display protocol and revert to the X.org display server:

- If the version of the NVIDIA driver is lower than 470.

- If the system is a laptop that uses hybrid graphics.
- If you have not enabled the required NVIDIA driver options.

Additionally, Wayland is enabled but the desktop session uses X.org by default if the version of the NVIDIA driver is lower than 510.

Jira:RHELPLAN-119001[1]

Night Light is not available on Wayland with NVIDIA

When the proprietary NVIDIA drivers are enabled on your system, the **Night Light** feature of GNOME is not available in Wayland sessions. The NVIDIA drivers do not currently support **Night Light**.

Jira:RHELPLAN-119852[1]

X.org configuration utilities do not work under Wayland

X.org utilities for manipulating the screen do not work in the Wayland session. Notably, the **xrandr** utility does not work under Wayland due to its different approach to handling, resolutions, rotations, and layout.

Jira:RHELPLAN-121049[1]

11.13.12. Virtualization

Installing a virtual machine over https or ssh in some cases fails

Currently, the **virt-install** utility fails when attempting to install a guest operating system (OS) from an ISO source over a https or ssh connection – for example using **virt-install --cdrom https://example/path/to/image.iso**. Instead of creating a virtual machine (VM), the described operation ends unexpectedly with an **internal error: process exited while connecting to monitor** message.
Similarly, using the RHEL 9 web console to install a guest operating system fails and displays an **Unknown driver 'https'** error if you use an https or ssh URL, or the **Download OS** function.

Workaround: Install **qemu-kvm-block-curl** and **qemu-kvm-block-ssh** on the host to enable https and ssh protocol support. Alternatively, use a different connection protocol or a different installation source.

Jira:RHELPLAN-99854[1]

Using NVIDIA drivers in virtual machines disables Wayland

Currently, NVIDIA drivers are not compatible with the Wayland graphical session. As a consequence, RHEL guest operating systems that use NVIDIA drivers automatically disable Wayland and load an Xorg session instead. This primarily occurs in the following scenarios:

- When you pass through an NVIDIA GPU device to a RHEL virtual machine (VM)
- When you assign an NVIDIA vGPU mediated device to a RHEL VM

There is currently no workaround for this issue.

Jira:RHELPLAN-117234[1]

Cloning or restoring RHEL 9 virtual machines that use LVM on Nutanix AHV causes non-root partitions to disappear

When running a RHEL 9 guest operating system on a virtual machine (VM) hosted on the Nutanix AHV hypervisor, restoring the VM from a snapshot or cloning the VM currently causes non-root partitions in the VM to disappear if the guest is using Logical Volume Management (LVM). As a consequence, the following problems occur:

- After restoring the VM from a snapshot, the VM cannot boot, and instead enters emergency mode.
- A VM created by cloning cannot boot, and instead enters emergency mode.

To work around these problems, do the following in emergency mode of the VM:

1. Remove the LVM system devices file:

```
# rm /etc/lvm/devices/system.devices
```

2. Re-create LVM device settings:

```
# vgimportdevices -a
```

3. Reboot the VM

This makes it possible for the cloned or restored VM to boot up correctly.

Alternatively, to prevent the issue from occurring, do the following before cloning a VM or creating a VM snapshot:

1. Uncomment the **use_devicesfile = 0** line in the **/etc/lvm/lvm.conf** file.
2. Regenerate initramfs. To do so, use the following steps in the VM and replace ***<kernelVersion>*** with the full version of the kernel that you want to rebuild.
   a. Back up the current **initramfs** configuration:

```
# cp /boot/initramfs-<kernelVersion>.img /boot/initramfs-<kernelVersion>.img.bak
```

   b. Build **initramfs**:

```
# dracut -f /boot/initramfs-<kernelVersion>.img  <kernelVersion>
```

3. Reboot the VM to verify successful boot.

Jira:RHELPLAN-114103[1]

The Milan VM CPU type is sometimes not available on AMD Milan systems

On certain AMD Milan systems, the Enhanced REP MOVSB (**erms**) and Fast Short REP MOVSB (**fsrm**) feature flags are disabled in the BIOS by default. Consequently, the **Milan** CPU type might not be available on these systems. In addition, VM live migration between Milan hosts with different feature flag settings might fail.
Workaround: Manually turn on **erms** and **fsrm** in the BIOS of your host.

Jira:RHELPLAN-119655[1]

A **hostdev** interface with failover settings cannot be hot-plugged after being hot-unplugged

After removing a **hostdev** network interface with failover configuration from a running virtual machine (VM), the interface currently cannot be re-attached to the same running VM. There is currently no workaround for this issue.
Jira:RHEL-7337

Live post-copy migration of VMs with failover VFs fails

Currently, attempting to post-copy migrate a running virtual machine (VM) fails if the VM uses a device with the virtual function (VF) failover capability enabled.
Workaround: Use the standard migration type, rather than post-copy migration.

Jira:RHEL-7335

Disabling AVX causes VMs to become unbootable

On a host machine that uses a CPU with Advanced Vector Extensions (AVX) support, attempting to boot a VM with AVX explicitly disabled currently fails, and instead triggers a kernel panic in the VM. There is currently no workaround for this issue.

Jira:RHELPLAN-97394[1]

11.14. KNOWN ISSUES IDENTIFIED IN PREVIOUS RELEASES

This part describes known issues identified in earlier Red Hat Enterprise Linux versions.

11.14.1. 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.
Workaround: Verify that the BaseOS and AppStream repositories are available to the installation program or use the **authselect** Kickstart command during installation.

Jira:RHELPLAN-10061[1]

Unexpected SELinux policies on systems where Anaconda is running as an application

When Anaconda is running as an application on an already installed system (for example to perform another installation to an image file using the **-image** anaconda option), the system is not prohibited to modify the SELinux types and attributes during installation. As a consequence, certain elements of SELinux policy might change on the system where Anaconda is running.
Workaround: Do not run Anaconda on the production system. Instead, run Anaconda in a temporary virtual machine to keep the SELinux policy unchanged on a production system. Running anaconda as part of the system installation process such as installing from **boot.iso** or **dvd.iso** is not affected by this issue.

Jira:RHELPLAN-110940[1]

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.
Workaround: Use the **harddrive --partition=sdX --dir=**/ command to install from USB CD-ROM drive. As a result, the installation does not fail.

Jira:RHEL-4707

Hard drive partitioned installations with iso9660 filesystem fails

You cannot install RHEL on systems where the hard drive is partitioned with the **iso9660** filesystem. This is due to the updated installation code that is set to ignore any hard disk containing a **iso9660** file system partition. This happens even when RHEL is installed without using a DVD.
Workaround: Add the following script in the Kickstart file to format the disc before the installation starts.

Note: Before performing the workaround, backup the data available on the disk. The **wipefs** command formats all the existing data from the disk.

```
%pre
wipefs -a /dev/sda
%end
```

As a result, installations work as expected without any errors.

Jira:RHEL-4711

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.

Jira:RHELDOCS-20471[1]

Installation fails due to busy partitions

A race condition in the storage subsystem causes the installation to fail when writing the partition table to disk. The system displays the following error message:

```
Partition(s) have been written, but we have been unable to inform the kernel of the change.
```

This error occurs because the partitions are reported as busy and the changes cannot be synchronized. To work around this problem, restart the installation.

Jira:RHEL-158237

11.14.2. Security

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.
Workaround: You can scan and remediate the system after the kickstart installation. This will fix the service-related issues.

Jira:RHELPLAN-44202[1]

11.14.3. File systems and storage

The **blk-availability** systemd service deactivates complex device stacks

In **systemd**, the default block deactivation code does not always handle complex stacks of virtual block devices correctly. In some configurations, virtual devices might not be removed during the shutdown, which causes error messages to be logged.
Workaround: Deactivate complex block device stacks by executing the following command:

```
# systemctl enable --now blk-availability.service
```

As a result, complex virtual device stacks are correctly deactivated during shutdown and do not produce error messages.

Jira:RHELPLAN-99108[1]

11.14.4. SSSD

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[1]

SSSD retrieves incomplete list of members if the group size exceeds 1500 members

During the integration of SSSD with Active Directory, SSSD retrieves incomplete group member lists when the group size exceeds 1500 members. This issue occurs because Active Directory's MaxValRange policy, which restricts the number of members retrievable in a single query, is set to 1500 by default.
Workaround: Change the MaxValRange setting in Active Directory to accommodate larger group sizes.

Jira:RHELDOCS-19603[1]

11.14.5. Supportability

Timeout when running sos report on IBM Power Systems, Little Endian

When running the **sos report** command on IBM Power Systems, Little Endian with hundreds or thousands of CPUs, the processor plugin reaches its default timeout of 300 seconds when collecting huge content of the **/sys/devices/system/cpu** directory. As a workaround, increase the plugin's timeout accordingly:

- For one-time setting, run:

```
# sos report -k processor.timeout=1800
```

- For a permanent change, edit the **[plugin_options]** section of the **/etc/sos/sos.conf** file:

```
[plugin_options]
# Specify any plugin options and their values here. These options take the form
# plugin_name.option_name = value
#rpm.rpmva = off
processor.timeout = 1800
```

The example value is set to 1800. The particular timeout value highly depends on a specific system. To set the plugin's timeout appropriately, you can first estimate the time needed to collect the one plugin with no timeout by running the following command:

```
# time sos report -o processor -k processor.timeout=0 --batch --build
```

Jira:RHELPLAN-51452[1]

11.14.6. Containers

Running systemd within an older container image does not work

Running systemd within an older container image, for example, **centos:7**, does not work:

```
$ podman run --rm -ti centos:7 /usr/lib/systemd/systemd
 Storing signatures
 Failed to mount cgroup at /sys/fs/cgroup/systemd: Operation not permitted
 [!!!!!!] Failed to mount API filesystems, freezing.
```

Workaround: Use the following commands:

```
# mkdir /sys/fs/cgroup/systemd
# mount none -t cgroup -o none,name=systemd /sys/fs/cgroup/systemd
# podman run --runtime /usr/bin/crun --
annotation=run.oci.systemd.force_cgroup_v1=/sys/fs/cgroup --rm -ti centos:7
/usr/lib/systemd/systemd
```

Jira:RHELPLAN-96940[1]

CHAPTER 12. AVAILABLE BPF FEATURES

A complete list of the Berkeley Packet Filter (BPF) features that are available in this version of Red Hat Enterprise Linux 9 is provided in this chapter. The tables include the lists of:

- System configuration and other options
- Available program types and supported helpers
- Available map types

This chapter contains automatically generated output of the **bpftool feature** command.

Table 12.1. System configuration and other options

Option	Value
unprivileged_bpf_disabled	2 (bpf() syscall restricted to privileged users, admin can change)
bpf_jit_enable	1 (enabled)
bpf_jit_harden	1 (enabled)
bpf_jit_kallsyms	1 (enabled)
bpf_jit_limit	528482304
CONFIG_BPF	y
CONFIG_BPF_SYSCALL	y
CONFIG_HAVE_EBPF_JIT	y
CONFIG_BPF_JIT	y
CONFIG_BPF_JIT_ALWAYS_ON	y
CONFIG_DEBUG_INFO_BTF	y
CONFIG_DEBUG_INFO_BTF_MODULES	y
CONFIG_CGROUPS	y
CONFIG_CGROUP_BPF	y
CONFIG_CGROUP_NET_CLASSID	y
CONFIG_SOCK_CGROUP_DATA	y

Option	Value
CONFIG_BPF_EVENTS	y
CONFIG_KPROBE_EVENTS	y
CONFIG_UPROBE_EVENTS	y
CONFIG_TRACING	y
CONFIG_FTRACE_SYSCALLS	y
CONFIG_FUNCTION_ERROR_INJECTION	y
CONFIG_BPF_KPROBE_OVERRIDE	n
CONFIG_NET	y
CONFIG_XDP_SOCKETS	y
CONFIG_LWTUNNEL_BPF	y
CONFIG_NET_ACT_BPF	m
CONFIG_NET_CLS_BPF	m
CONFIG_NET_CLS_ACT	y
CONFIG_NET_SCH_INGRESS	m
CONFIG_XFRM	y
CONFIG_IP_ROUTE_CLASSID	y
CONFIG_IPV6_SEG6_BPF	y
CONFIG_BPF_LIRC_MODE2	n
CONFIG_BPF_STREAM_PARSER	y
CONFIG_NETFILTER_XT_MATCH_BPF	m
CONFIG_BPFILTER	n
CONFIG_BPFILTER_UMH	n

Option	Value
CONFIG_TEST_BPF	m
CONFIG_HZ	1000
bpf() syscall	available
Large program size limit	available
Bounded loop support	available
ISA extension v2	available
ISA extension v3	available

Table 12.2. Available program types and supported helpers

Program type	Available helpers
socket_filter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
kprobe	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sched_cls	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sched_act	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
xdp	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_redirect, bpf_perf_event_output, bpf_csum_diff, bpf_get_current_task, bpf_get_numa_node_id, bpf_xdp_adjust_head, bpf_redirect_map, bpf_xdp_adjust_meta, bpf_xdp_adjust_tail, bpf_fib_lookup, bpf_get_current_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_strtol, bpf_strtoul, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_xdp_load_bytes, bpf_xdp_store_bytes, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
perf_event	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
cgroup_sock	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lwt_in	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_push_encap, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
lwt_out	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lwt_xmit	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_lwt_push_encap, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
sock_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_sock_map_update, bpf_getsockopt, bpf_sock_ops_cb_flags_set, bpf_sock_hash_update, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
sk_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_adjust_room, bpf_sk_redirect_map, bpf_sk_redirect_hash, bpf_get_current_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
cgroup_device	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
sk_msg	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_msg_redirect_hash, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
raw_tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sock_addr	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_getsockopt, bpf_bind, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
lwt_seg6local	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_seg6_store_bytes, bpf_lwt_seg6_adjust_srh, bpf_lwt_seg6_action, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
lirc_mode2	not supported
sk_reuseport	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_skb_load_bytes_relative, bpf_get_current_cgroup_id, bpf_sk_select_reuseport, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
flow_dissector	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sysctl	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
raw_tracepoint_writable	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
cgroup_sockopt	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
tracing	
struct_ops	
ext	
lsm	

Program type	Available helpers
sk_lookup	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete
syscall	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_get_socket_cookie, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_send_signal, bpf_skb_output, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_xdp_output, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_get_task_stack, bpf_d_path, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_sock_from_file, bpf_for_each_map_elem, bpf_snprintf, bpf_sys_bpf, bpf_btf_find_by_name_kind, bpf_sys_close, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_skc_to_unix_sock, bpf_kallsyms_lookup_name, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Program type	Available helpers
netfilter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_ktime_get_tai_ns, bpf_user_ringbuf_drain, bpf_cgrp_storage_get, bpf_cgrp_storage_delete

Table 12.3. Available map types

Map type	Available
hash	yes
array	yes
prog_array	yes
perf_event_array	yes
percpu_hash	yes
percpu_array	yes
stack_trace	yes
cgroup_array	yes
lru_hash	yes
lru_percpu_hash	yes
lpm_trie	yes
array_of_maps	yes
hash_of_maps	yes

Map type	Available
devmap	yes
sockmap	yes
cpumap	yes
xskmap	yes
sockhash	yes
cgroup_storage	yes
reuseport_sockarray	yes
percpu_cgroup_storage	yes
queue	yes
stack	yes
sk_storage	yes
devmap_hash	yes
struct_ops	yes
ringbuf	yes
inode_storage	yes
task_storage	yes
bloom_filter	yes
user_ringbuf	yes
cgrp_storage	yes
arena_map	yes

APPENDIX A. LIST OF TICKETS BY COMPONENT

Bugzilla and JIRA tickets are listed in this document for reference. The links lead to the release notes in this document that describe the tickets.

Component	Tickets
389-ds-base	Jira:RHEL-112727, Jira:RHEL-117748, Jira:RHEL-117782, Jira:RHEL-121170, Jira:RHEL-123231, Jira:RHEL-123258, Jira:RHEL-123893, Jira:RHEL-123897, Jira:RHEL-126552, Jira:RHEL-129559, Jira:RHEL-139825, Jira:RHEL-142980, Jira:RHEL-147212, Jira:RHEL-152338
NetworkManager	Jira:RHEL-113954, Jira:RHEL-115973, Jira:RHEL-122166, Jira:RHEL-122175, Jira:RHEL-24337, Jira:RHEL-5852, Jira:RHEL-24622, Jira:RHEL-17619, Jira:RHELPLAN-58745, Jira:RHEL-87994
NetworkManager-libreswan	Jira:RHEL-124258
Release Notes	Jira:RHELDOCS-21350, Jira:RHELDOCS-21587, Jira:RHELDOCS-19635, Jira:RHELDOCS-19072, Jira:RHELDOCS-18935, Jira:RHELDOCS-17520, Jira:RHELDOCS-16861, Jira:RHELDOCS-21505, Jira:RHELDOCS-21687, Jira:RHELDOCS-20337, Jira:RHELDOCS-19754, Jira:RHELDOCS-19889, Jira:RHELDOCS-20146, Jira:RHELDOCS-18158, Jira:RHELDOCS-17532, Jira:RHELDOCS-17508, Jira:RHELDOCS-19022, Jira:RHELDOCS-19284, Jira:RHELDOCS-18312, Jira:RHELDOCS-18480, Jira:RHELDOCS-19224, Jira:RHELDOCS-19028, Jira:RHELDOCS-19029, Jira:RHELDOCS-18959, Jira:RHELDOCS-19013, Jira:RHELDOCS-19012, Jira:RHELDOCS-19080, Jira:RHELDOCS-19050, Jira:RHELDOCS-19093, Jira:RHELDOCS-19149, Jira:RHELDOCS-19133, Jira:RHELDOCS-19171, Jira:RHELDOCS-19147, Jira:RHELDOCS-19139, Jira:RHELDOCS-19135, Jira:RHELDOCS-19137, Jira:RHELDOCS-19154, Jira:RHELDOCS-19143, Jira:RHELDOCS-19151, Jira:RHELDOCS-19115, Jira:RHELDOCS-18531, Jira:RHELDOCS-19193, Jira:RHELDOCS-20135, Jira:RHELDOCS-17958, Jira:RHELDOCS-16716, Jira:RHELDOCS-17974, Jira:RHELDOCS-22204, Jira:RHELDOCS-22205, Jira:RHELDOCS-17309, Jira:RHELDOCS-17545, Jira:RHELDOCS-17989, Jira:RHELDOCS-17702, Jira:RHELDOCS-17917, Jira:RHELDOCS-17102, Jira:RHELDOCS-16756, Jira:RHELDOCS-17518, Jira:RHELDOCS-16612, Jira:RHELDOCS-21742, Jira:RHELDOCS-21366, Jira:RHELDOCS-19852, Jira:RHELDOCS-18065, Jira:RHELDOCS-16979, Jira:RHELDOCS-19846, Jira:RHELDOCS-20196, Jira:RHELDOCS-19603, Jira:RHELDOCS-20471
aardvark-dns	Jira:RHEL-85839
adcli	Jira:RHEL-134945, Jira:RHEL-134948, Jira:RHEL-134950, Jira:RHEL-134951
aide	Jira:RHEL-1569, Jira:RHEL-83776

Component	Tickets
anaconda	Jira:RHEL-4737, Jira:RHEL-144834, Jira:RHEL-63237, Jira:RHEL-17205, Jira:RHEL-2250, Jira:RHEL-10216, Jira:RHELPLAN-168262, Jira:RHEL-80867, Jira:RHEL-14005, Jira:RHEL-9633, Jira:RHEL-4762, Jira:RHEL-4741, Jira:RHELPLAN-130370, Jira:RHELPLAN-53644, Jira:RHELPLAN-94811, Jira:RHEL-82566, Jira:RHEL-13837, Jira:RHELPLAN-110940, Jira:RHEL-4707, Jira:RHEL-4711
ansible-collection-microsoft-sql	Jira:RHEL-69311
ansible-collection-redhat-leapp	Jira:RHEL-117252
ansible-freeipa	Jira:RHEL-139144, Jira:RHEL-139257, Jira:RHEL-140607
bacula	Jira:RHEL-6856
bind	Jira:RHELPLAN-90604
boost	Jira:RHEL-116553
bootc-image-builder-container	Jira:RHEL-34807
buildah	Jira:RHEL-127908, Jira:RHEL-95964
ca-certificates	Jira:RHEL-54695
cepces	Jira:RHEL-121787
chrony	Jira:RHEL-112598
clevis	Jira:RHEL-132187
clevis-pin-tpm2	Jira:RHEL-68417
clevis-pin-trustee	Jira:RHEL-139790
cockpit	Jira:RHEL-112866
cockpit-machines	Jira:RHEL-31993
command-line-assistant	Jira:RHEL-129825

Component	Tickets
container-selinux	Jira:RHEL-112187
container-tools	Jira:RHEL-127908, Jira:RHEL-69742, Jira:RHEL-67859
cracklib	Jira:RHEL-5215
crash	Jira:RHEL-114658
createrepo_c	Jira:RHELPLAN-112860
crun	Jira:RHEL-127908
crypto-policies	Jira:RHEL-127829, Jira:RHEL-151499, Jira:RHEL-103793, Jira:RHEL-112697, Jira:RHEL-2735
cryptsetup	Jira:RHEL-100089
cyrus-sasl	Jira:RHELPLAN-94096
device-mapper-multipath	Jira:RHEL-118515, Jira:RHEL-133814, Jira:RHEL-135904, Jira:RHEL-141291, Jira:RHELPLAN-105944, Jira:RHELPLAN-99108
distribution	Jira:RHEL-96956, Jira:RHEL-139790, Jira:RHEL-117252, Jira:RHEL-120823, Jira:RHEL-96056, Jira:RHEL-68141, Jira:RHEL-6973, Jira:RHEL-22385
dnf	Jira:RHEL-76112, Jira:RHEL-94321, Jira:RHELPLAN-118420
dnf-plugins-core	Jira:RHEL-94014, Jira:RHEL-145372
edk2	Jira:RHEL-121983, Jira:RHELPLAN-69533, Jira:RHEL-82759, Jira:RHEL-68418
elfutils	Jira:RHEL-121664
fapolicyd	Jira:RHEL-94661, Jira:RHEL-118363, Jira:RHEL-141670, Jira:RHELPLAN-112355, Jira:RHEL-114562, Jira:RHEL-24345, Jira:RHEL-520
fips-provider-next	Jira:RHEL-96056
firewalld	Jira:RHEL-17708
frr	Jira:RHEL-125957

Component	Tickets
frr10	Jira:RHEL-125957
gcc	Jira:RHEL-105416
glibc	Jira:RHEL-1063, Jira:RHEL-41205, Jira:RHEL-61087, Jira:RHEL-109622, Jira:RHEL-111005, Jira:RHEL-112149, Jira:RHEL-137186, Jira:RHEL-141072, Jira:RHEL-49785, Jira:RHEL-140105, Jira:RHEL-54450, Jira:RHEL-150269, Jira:RHEL-153056
gnome-control-center	Jira:RHEL-68152
gnupg2	Jira:RHELPLAN-117566
gnutls	Jira:RHEL-125971, Jira:RHELPLAN-128129
golang	Jira:RHELPLAN-129104, Jira:RHELPLAN-123778
gtk3	Jira:RHEL-11924
haproxy	Jira:RHEL-74039
httpd	Jira:RHEL-129692
initscripts	Jira:RHEL-79783
ipa	Jira:RHEL-73399, Jira:RHEL-120954, Jira:RHEL-126515, Jira:RHEL-128238, Jira:RHEL-134542, Jira:RHEL-141446, Jira:RHEL-67913, Jira:RHELPLAN-121751, Jira:RHEL-151560, Jira:RHEL-4955, Jira:RHEL-12154, Jira:RHELPLAN-113281
iproute	Jira:RHEL-98272, Jira:RHEL-102012, Jira:RHEL-131661
java-25-openjdk	Jira:RHEL-128412
jmc-core	Jira:RHELPLAN-88788
kdump-anaconda-addon	Jira:RHEL-11196
kernel	Jira:RHELPLAN-153754, Jira:RHELPLAN-154595, Jira:RHELPLAN-108169, Jira:RHELPLAN-102815, Jira:RHELPLAN-102321, Jira:RHELPLAN-157294, Jira:RHELPLAN-147783, Jira:RHELPLAN-141042, Jira:RHELPLAN-135779, Jira:RHELPLAN-134771, Jira:RHELPLAN-96004, Jira:RHELPLAN-99859, Jira:RHELPLAN-114103, Jira:RHELPLAN-97394

Component	Tickets
kernel / Accelerators	Jira:RHEL-38583
kernel / Core	Jira:RHEL-25967
kernel / Crypto	Jira:RHEL-94929, Jira:RHEL-95629, Jira:RHEL-106910, Jira:RHEL-20145
kernel / Debugging-Tracing / EDAC-HERM	Jira:RHEL-45085
kernel / Debugging-Tracing / Perf	Jira:RHEL-45067, Jira:RHEL-47456, Jira:RHEL-74193, Jira:RHEL-95671, Jira:RHEL-95673, Jira:RHEL-106898, Jira:RHEL-124984
kernel / Debugging-Tracing / kexec - kdump	Jira:RHEL-104939
kernel / Debugging-Tracing / rtla	Jira:RHEL-113482
kernel / Desktop / Graphics	Jira:RHEL-124779
kernel / File Systems / GFS-GFS2	Jira:RHEL-7971, Jira:RHEL-129403
kernel / Networking	Jira:RHEL-80409, Jira:RHEL-100940, Jira:RHEL-100941, Jira:RHEL-130476, Jira:RHEL-88552, Jira:RHEL-88551
kernel / Networking / IPSec	Jira:RHEL-30141, Jira:RHEL-1015
kernel / Networking / NIC Drivers	Jira:RHEL-100057, Jira:RHEL-126034, Jira:RHEL-134986, Jira:RHEL-114873, Jira:RHEL-36283
kernel / Networking / Netfilter	Jira:RHEL-138511
kernel / Networking / Protocol / tcp	Jira:RHEL-115191
kernel / Networking / Protocol / udp	Jira:RHEL-138741
kernel / Networking / Wifi	Jira:RHEL-141399
kernel / Platform Enablement / ppc64	Jira:RHEL-14156, Jira:RHEL-28702, Jira:RHEL-15404

Component	Tickets
kernel / Storage	Jira:RHEL-137435
kernel / Storage / Multiple Devices (MD)	Jira:RHEL-30730
kernel / Storage / Storage Drivers	Jira:RHEL-9301, Jira:RHEL-10414, Jira:RHEL-109510, Jira:RHEL-8104, Jira:RHEL-25730, Jira:RHEL-8164
kernel / Virtualization	Jira:RHEL-1138
kernel / Virtualization / Hyper-V	Jira:RHEL-70228
kernel / Virtualization / KVM	Jira:RHEL-32892, Jira:RHEL-43214, Jira:RHEL-45585, Jira:RHEL-38957, Jira:RHEL-17331, Jira:RHEL-7212
kernel / Virtualization / Public Cloud Enablement	Jira:RHEL-81748
kernel / io_uring	Jira:RHEL-120699
kernel-rt	Jira:RHELPLAN-153123
kernel-rt / Other	Jira:RHEL-9318
kexec-tools	Jira:RHEL-33413, Jira:RHELPLAN-129876, Jira:RHELPLAN-115732
keylime	Jira:RHEL-111167, Jira:RHEL-118150, Jira:RHEL-11867, Jira:RHEL-1518
keylime-agent-rust	Jira:RHEL-118148
kmod	Jira:RHELPLAN-126922
kmod-kvdo	Jira:RHEL-8354
kpatch	Jira:RHEL-103845
krb5	Jira:RHEL-4888, Jira:RHELPLAN-114497, Jira:RHEL-4875
libabigail	Jira:RHEL-16629
libdnf	Jira:RHEL-81779, Jira:RHELPLAN-128381

Component	Tickets
libotr	Jira:RHELPLAN-122108
librepo	Jira:RHEL-62033
libsolv	Jira:RHEL-103995
libvirt	Jira:RHEL-7125, Jira:RHEL-108915, Jira:RHEL-114003, Jira:RHEL-118197
libvirt / General	Jira:RHEL-111840, Jira:RHEL-7043, Jira:RHEL-89415
libvirt / Storage	Jira:RHEL-140614
libxcrypt	Jira:RHELPLAN-106338
linux-sgx	Jira:RHEL-127046, Jira:RHEL-129059
llvm	Jira:RHEL-100898
lvm2	Jira:RHELPLAN-107107
maven	Jira:RHEL-127952
mysql	Jira:RHELPLAN-92864
mysql-8.4-module	Jira:RHEL-144470
net-snmp	Jira:RHEL-101614, Jira:RHEL-103557
nfs-utils	Jira:RHELPLAN-120807
nmstate	Jira:RHEL-110781, Jira:RHEL-110793, Jira:RHEL-141605
nodejs	Jira:RHEL-90821, Jira:RHEL-35990
nss	Jira:RHEL-127671
nvme-stas	Jira:RHELPLAN-58357
opencryptoki	Jira:RHEL-100059
openscap	Jira:RHEL-133976, Jira:RHELPLAN-145263
openslp	Jira:RHEL-6995

Component	Tickets
openssh	Jira:RHEL-108912, Jira:RHEL-118372, Jira:RHEL-119515, Jira:RHEL-45727, Jira:RHELPLAN-113842
openssl	Jira:RHELPLAN-148207, Jira:RHELPLAN-139207, Jira:RHELPLAN-113856, Jira:RHEL-40605, Jira:RHELPLAN-50959, Jira:RHELPLAN-48241
openwsman	Jira:RHEL-97643, Jira:RHEL-127516
osbuild-composer	Jira:RHEL-4649
oscap-anaconda-addon	Jira:RHEL-1824, Jira:RHELPLAN-44202
p11-kit	Jira:RHEL-91952, Jira:RHEL-139075
pam	Jira:RHEL-130875
pause-container	Jira:RHELPLAN-127619
pcs	Jira:RHEL-113763, Jira:RHEL-126842, Jira:RHEL-34781
pki-core	Jira:RHEL-129092, Jira:RHELPLAN-121754
podman	Jira:RHEL-3114, Jira:RHEL-126643, Jira:RHEL-127908, Jira:RHEL-157746, Jira:RHEL-88121, Jira:RHEL-70217, Jira:RHEL-32267, Jira:RHELPLAN-117005
postgresql	Jira:RHEL-90852
pqrpm	Jira:RHEL-112700
python-blivet	Jira:RHEL-122858, Jira:RHEL-158237
python3.11-lxml	Jira:RHELPLAN-143480
python3.14	Jira:RHEL-120823
qemu-kvm	Jira:RHEL-57677, Jira:RHELPLAN-114513, Jira:RHELPLAN-81033, Jira:RHELPLAN-75969, Jira:RHEL-81999, Jira:RHEL-62742, Jira:RHEL-66229, Jira:RHELPLAN-63771, Jira:RHELPLAN-150884, Jira:RHELPLAN-118495, Jira:RHELPLAN-99854
qemu-kvm / Devices	Jira:RHEL-1220

Component	Tickets
qemu-kvm / Devices / CPU Models	Jira:RHEL-17614
qemu-kvm / Devices / Machine Types	Jira:RHEL-104005
qemu-kvm / General	Jira:RHEL-73001, Jira:RHEL-73009
qemu-kvm / Live Migration	Jira:RHEL-97465, Jira:RHEL-7096
qemu-kvm / Networking	Jira:RHEL-21867, Jira:RHEL-333, Jira:RHEL-7336, Jira:RHEL-7337, Jira:RHEL-7335
rear	Jira:RHEL-56045
resource-agents	Jira:RHEL-118624, Jira:RHEL-32265
restore	Jira:RHELPLAN-94704
rhel-system-roles	Jira:RHEL-84891, Jira:RHEL-112772, Jira:RHEL-112805, Jira:RHEL-120325, Jira:RHEL-122958, Jira:RHEL-123018, Jira:RHEL-123028, Jira:RHEL-123040, Jira:RHEL-123041, Jira:RHEL-123044, Jira:RHEL-127973, Jira:RHEL-128436, Jira:RHEL-129416, Jira:RHEL-136599, Jira:RHEL-138058, Jira:RHEL-138279, Jira:RHEL-144496, Jira:RHEL-144592, Jira:RHEL-145215, Jira:RHEL-145220, Jira:RHEL-145248, Jira:RHEL-147823, Jira:RHEL-150782, Jira:RHEL-150789, Jira:RHEL-151438, Jira:RHELPLAN-95747, Jira:RHELPLAN-133165, Jira:RHEL-1172
rteval	Jira:RHEL-114928
ruby-4.0-module	Jira:RHEL-142278
runc	Jira:RHEL-124800
rust	Jira:RHEL-111847
rust-rpm-sequoia	Jira:RHEL-111478
samba	Jira:RHEL-114548
sblim-sfcb	Jira:RHEL-127515
scap-security-guide	Jira:RHEL-136121, Jira:RHEL-1800, Jira:RHELPLAN-107318
seabios	Jira:RHEL-7110

Component	Tickets
selinux-policy	Jira:RHEL-66119, Jira:RHEL-108982, Jira:RHEL-121165, Jira:RHEL-129879, Jira:RHEL-133898, Jira:RHEL-11792, Jira:RHELPLAN-115609
skopeo	Jira:RHEL-127908
snapm	Jira:RHEL-137377
sos	Jira:RHEL-121524, Jira:RHEL-142619, Jira:RHEL-140738, Jira:RHEL-121515, Jira:RHEL-121517, Jira:RHEL-121531, Jira:RHEL-121534, Jira:RHEL-142618, Jira:RHEL-112563, Jira:RHELPLAN-51452
sscg	Jira:RHEL-124447
stunnel	Jira:RHEL-52317
subscription-manager	Jira:RHEL-66122, Jira:RHEL-29178, Jira:RHELPLAN-146101
sudo	Jira:RHEL-128623
sysstat	Jira:RHEL-26275, Jira:RHEL-12009
systemd	Jira:RHEL-92781, Jira:RHELPLAN-100926, Jira:RHEL-6105
systemtap	Jira:RHEL-121662
tigervnc	Jira:RHELPLAN-114314
tog-pegasus	Jira:RHEL-127514
tpm2-tools	Jira:RHEL-94933
trustee-guest-components	Jira:RHEL-68141
tuned	Jira:RHELPLAN-129881
ubi9-container	Jira:RHEL-62749
unbound	Jira:RHEL-132717, Jira:RHELPLAN-117492
valgrind	Jira:RHEL-120965
vdo	Jira:RHEL-30525
virt-v2v	Jira:RHEL-13340

Component	Tickets
virtio-win	Jira:RHEL-11810, Jira:RHEL-1609, Jira:RHEL-869, Jira:RHEL-11366
virtio-win / distribution	Jira:RHEL-574
virtio-win / virtio-win-prewhql	Jira:RHEL-53962, Jira:RHEL-1084, Jira:RHEL-12118, Jira:RHEL-1212
volume_key	Jira:RHEL-113757
webkit2gtk3	Jira:RHEL-4157
xdp-tools	Jira:RHEL-119860

Component	Tickets
other	Jira:RHELDOCS-21216, Jira:RHELDOCS-21410, Jira:RHELDOCS-21467, Jira:RHELDOCS-20708, Jira:RHELDOCS-22067, Jira:RHELDOCS-21814, Jira:RHELDOCS-21815, Jira:RHELDOCS-21707, Jira:RHELDOCS-19756, Jira:RHELDOCS-21350, Jira:RHELDOCS-20258, Jira:RHELDOCS-20059, Jira:RHELDOCS-19635, Jira:RHELDOCS-18935, Jira:RHELDOCS-17752, Jira:RHELDOCS-17520, Jira:RHELDOCS-17040, Jira:RHEL-88550, Jira:RHELDOCS-16861, Jira:RHELPLAN-27737, Jira:RHELPLAN-27394, Jira:RHELDOCS-21153, Jira:RHELDOCS-22087, Jira:RHELDOCS-21687, Jira:RHELDOCS-19754, Jira:RHELDOCS-19455, Jira:RHEL-91106, Jira:RHELDOCS-19815, Jira:RHELDOCS-19716, Jira:RHELDOCS-19809, Jira:RHELDOCS-19810, Jira:RHELDOCS-19523, Jira:RHELDOCS-20146, Jira:RHELDOCS-20283, Jira:RHELDOCS-20519, Jira:RHELDOCS-20718, Jira:RHELDOCS-17532, Jira:RHELDOCS-17508, Jira:RHELDOCS-18699, Jira:RHELDOCS-19004, Jira:RHELDOCS-18312, Jira:RHELDOCS-18480, Jira:RHELDOCS-18701, Jira:RHELDOCS-18702, Jira:RHELDOCS-18703, Jira:RHELDOCS-19224, Jira:RHELDOCS-19028, Jira:RHELDOCS-19029, Jira:RHELDOCS-18592, Jira:RHELDOCS-18593, Jira:RHELDOCS-18803, Jira:RHELDOCS-18207, Jira:RHELDOCS-19013, Jira:RHELDOCS-19021, Jira:RHELDOCS-19012, Jira:RHELDOCS-19068, Jira:RHELDOCS-19069, Jira:RHELDOCS-19080, Jira:RHELDOCS-19050, Jira:RHELDOCS-19093, Jira:RHELDOCS-19115, Jira:RHELDOCS-19193, Jira:RHELDOCS-20135, Jira:RHELDOCS-17015, Jira:RHELDOCS-17135, Jira:RHELDOCS-17545, Jira:RHELDOCS-17038, Jira:RHELDOCS-17495, Jira:RHELDOCS-17462, Jira:RHELDOCS-18106, Jira:RHELDOCS-17782, Jira:RHELDOCS-16432, Jira:RHELDOCS-16393, Jira:RHELDOCS-17102, Jira:RHELPLAN-139805, Jira:RHELDOCS-16756, Jira:RHELPLAN-153267, Jira:RHELDOCS-16300, Jira:RHELDOCS-17518, Jira:RHELPLAN-131882, Jira:RHELPLAN-67314, Jira:RHELPLAN-110763, Jira:RHELPLAN-69554, Jira:RHELPLAN-113995, Jira:RHELPLAN-122745, Jira:RHELPLAN-99136, Jira:RHELPLAN-103232, Jira:RHELPLAN-60153, Jira:RHELPLAN-88246, Jira:RHELPLAN-100087, Jira:RHELPLAN-100639, Jira:RHELPLAN-113659, Jira:RHELPLAN-98983, Jira:RHELDOCS-16612, Jira:RHELDOCS-20464, Jira:RHELDOCS-18049, Jira:RHELDOCS-22157, Jira:RHELDOCS-21742, Jira:RHELDOCS-21325, Jira:RHELDOCS-19945, Jira:RHELDOCS-19728, Jira:RHELDOCS-19539, Jira:RHELDOCS-19734, Jira:RHELDOCS-19948, Jira:RHELDOCS-19496, Jira:RHELDOCS-18863, Jira:RHELDOCS-18064, Jira:RHELDOCS-16427, Jira:RHELDOCS-17719, Jira:RHELDOCS-18435, Jira:RHELPLAN-157225, Jira:RHELPLAN-145001, Jira:RHELPLAN-150080, Jira:RHELPLAN-154195, Jira:RHELPLAN-83423, Jira:RHELPLAN-109613, Jira:RHELPLAN-110191, Jira:RHELPLAN-117234, Jira:RHELPLAN-119001, Jira:RHELPLAN-119852, Jira:RHELPLAN-119655, Jira:RHELPLAN-112043, Jira:RHELPLAN-121205, Jira:RHELPLAN-121049, Jira:RHELPLAN-10061, Jira:RHELPLAN-96940, Jira:RHELDOCS-19603

APPENDIX B. REVISION HISTORY

0.0-0

Wed 20 May 2026, Valentina Ashirova (vaashiro@redhat.com)

- Release of the Red Hat Enterprise Linux 9.8 Release Notes.