Red Hat Enterprise Linux 9

9.5 Release Notes

Release Notes for Red Hat Enterprise Linux 9.5

Last Updated: 2025-06-11

Red Hat Enterprise Linux 9 9.5 Release Notes

Release Notes for Red Hat Enterprise Linux 9.5

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 9.5 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 appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting feedback through Jira (account required)

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

CHAPTER 1. OVERVIEW

1.1. MAJOR CHANGES IN RHEL 9.5

Security

With the new **sudo RHEL system role**, you can consistently manage sudo configuration at scale across your RHEL systems.

The **OpenSSL** TLS toolkit is upgraded to version 3.2.2. OpenSSL now supports certificate compression extension (RFC 8879) and Brainpool curves have been added to the TLS 1.3 protocol (RFC 8734).

The **ca-certificates** program now provides trusted CA roots in the OpenSSL directory format.

The **crypto-policies** packages have been updated to extend its control to algorithm selection in Java.

The **SELinux** policy now provides a boolean that allows QEMU Guest Agent to execute confined commands.

The **NSS** cryptographic toolkit packages have been rebased to upstream version 3.101.

See New features - Security for more information.

Dynamic programming languages, web and database servers

Later versions of the following Application Streams are now available:

- **Apache HTTP Server 2.4.62**
- **Node.js 22**

See New features - 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**
- **Annobin 12.70**

Updated performance tools and debuggers

The following performance tools and debuggers have been updated:

- **GDB 14.2**
- **Valgrind 3.23.0**
- **SystemTap 5.1**
- **elfutils 0.191**
- **libabigail 2.5**

Updated performance monitoring tools

The following performance monitoring tools have been updated:

- **PCP 6.2.2**

- **Grafana 10.2.6**

Updated compiler toolsets
The following compiler toolsets have been updated:

- **GCC Toolset 14** (new)
- **LLVM Toolset 18.1.8**
- **Rust Toolset 1.79.0**
- **Go Toolset 1.22**

See New features - Compilers and development tools for more information.

The web console

With the new **File browser** provided by the **cockpit-files** package, you can manage files and directories in the RHEL web console.

See New features - The web console for more information.

RHEL in cloud environments

You can now use the OpenTelemetry framework to collect telemetry data, such as logs, metrics, and traces, from RHEL cloud instances, and to send the data to external analytics services, such as AWS CloudWatch.

See New features - RHEL in cloud environments for more information.

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 9.5 on the following architectures:
  - 64-bit Intel and AMD
  - IBM POWER 9 (little endian) and later
  - IBM Z architectures, excluding z13
- From RHEL 8.8 to RHEL 9.2, and RHEL 8.10 to RHEL 9.4 on the following architectures:
  - 64-bit Intel, AMD, and ARM
  - IBM POWER 9 (little endian) and later
  - IBM Z architectures, excluding z13
- From RHEL 8.6 to RHEL 9.0 and RHEL 8.8 to RHEL 9.2 on systems with SAP HANA

For more information, see Supported in-place upgrade paths for Red Hat Enterprise Linux .

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

If you are upgrading to RHEL 9.2 with SAP HANA, ensure that the system is certified for SAP before the upgrade. For instructions on performing an in-place upgrade on systems with SAP environments, see How to in-place upgrade SAP environments from RHEL 8 to RHEL 9 .

Notable enhancements include:

- Properly close file descriptors for executed shell commands to prevent the common **Too many opened files** error.
- Introduce in-place upgrade for systems with the Satellite Server version 6.16.
- Target the **GA** channel repositories by default unless a different channel is specified by using the **--channel** leapp option.
- Update the default kernel command line during the upgrade process so that kernels installed later automatically contain expected parameters.

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 Upgrading from RHEL 7 to RHEL 8 .

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
- VNC Configurator
- Red Hat Satellite Upgrade Helper
- JVM Options Configuration Tool
- Load Balancer Configuration Tool
- Ceph Placement Groups (PGs) per Pool Calculator
- Yum Repository Configuration Helper
- Red Hat Out of Memory Analyzer

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.

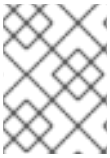
The Package manifest document provides a **package listing** for RHEL 9, including licenses and application compatibility levels.

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 .

The **Red Hat Insights** service, which enables you to proactively identify, examine, and resolve known technical issues, is available with all RHEL subscriptions. For instructions on how to install the Red Hat Insights client and register your system to the service, see the Red Hat Insights page.



NOTE

Release notes include a reference to their tracking ticket. If the ticket is not public, the reference is not linked.[1]

[1] Release notes include a reference to their tracking ticket. If the ticket is not public, the reference is not linked.

CHAPTER 2. ARCHITECTURES

Red Hat Enterprise Linux 9.5 is distributed with the kernel version 5.14.0-503.11.1, 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)

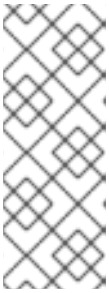
Make sure you purchase the appropriate subscription for each architecture. For more information, see Get Started with Red Hat Enterprise Linux - additional architectures .

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 might 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 9.5.

4.1. INSTALLER AND IMAGE CREATION

Minimal RHEL installation now installs only the s390utils-core package

In RHEL 8.4 and later, the **s390utils-base** package is split into an **s390utils-core** package and an auxiliary **s390utils-base** package. As a result, setting the RHEL installation to **minimal-environment** installs only the necessary **s390utils-core** package and not the auxiliary **s390utils-base** package. If you want to use the **s390utils-base** package with a minimal RHEL installation, you must manually install the package after completing the RHEL installation or explicitly install **s390utils-base** using a Kickstart file.

Bugzilla:1932480[1]

4.2. SECURITY

NSS rebased to 3.101

The NSS cryptographic toolkit packages have been rebased to upstream version 3.101, which provides many bug fixes and enhancements. The most notable changes are the following:

- DTLS 1.3 protocol is now supported (RFC 9147).
- PBMAC1 support has been added to PKCS#12 (RFC 9579).
- The X25519Kyber768Draft00 hybrid post-quantum key agreement has experimental support (**draft-tls-westerbaan-xyber768d00**).
- **lib::pkix** is the default validator in RHEL 10.
- RSA certificates with keys shorter than 2048 bits stop working, in accordance with the system-wide cryptographic policy (breaking fix).

Jira:RHEL-46840[1]

Libreswan accepts IPv6 SAN extensions

Previously, IPsec connection failed when setting up certificate-based authentication with a certificate that contained a subjectAltName (SAN) extension with an IPv6 address. With this update, the **pluto** daemon has been modified to accept IPv6 SAN and IPv4. As a result, IPsec connection is now correctly established with IPv6 address embedded in the certificate as an ID.

Jira:RHEL-32720[1]

Custom key sizes in ssh-keygen

You can now configure the size of keys generated by the **/usr/libexec/openssh/sshd-keygen** script by setting environment variables **SSH_RSA_BITS** and **SSH_ECDSA_BITS** in the **/etc/sysconfig/sshd** environment file.

Jira:RHEL-26454[1]

fips-mode-setup checks for use of Argon2 KDF in open LUKS volumes before enabling FIPS mode

The **fips-mode-setup** system management command now detects key derivation functions (KDF) used in currently open LUKS volumes, and aborts if it detects usage of Argon2 KDF. This is because Argon2 KDF is not FIPS-compatible, so preventing its use helps ensure FIPS compliance. As a result, switching into FIPS mode on a system with open LUKS volumes that use Argon2 as a KDF is blocked until those volumes are closed or converted to a different KDF.

Jira:RHEL-39026

New SELinux boolean to allow QEMU Guest Agent executing confined commands

Previously, commands that were supposed to run in a confined context through the QEMU Guest Agent daemon program, such as **mount**, failed with an Access Vector Cache (AVC) denial. To be able to run these commands, the **guest-agent** must run in the **virt_qemu_ga_unconfined_t** domain.

Therefore, this update adds the SELinux policy boolean **virt_qemu_ga_run_unconfined** that allows **guest-agent** to make the transition to **virt_qemu_ga_unconfined_t** for executables located in any of the following directories:

- **/etc/qemu-ga/fsfreeze-hook.d/**
- **/usr/libexec/qemu-ga/fsfreeze-hook.d/**
- **/var/run/qemu-ga/fsfreeze-hook.d/**

In addition, the necessary rules for transitions for the **qemu-ga** daemon have been added to the SELinux policy boolean.

As a result, you can now run confined commands through the QEMU Guest Agent without AVC denials by enabling the **virt_qemu_ga_run_unconfined** boolean.

Jira:RHEL-31211

OpenSSL rebased to 3.2.2

The OpenSSL packages have been rebased to upstream version 3.2.2. This update brings various enhancements and bug fixes, most notably the following:

- The **openssl req** command with the **-extensions** option no longer mishandles extensions when creating certificate signing requests (CSR). Previously, the command fetched, parsed, and checked the name of the configuration file section for consistency but the name was not used for adding extensions to the created CSR file. With this fix, the extension is added to the generated CSR. As a side effect of this change, if the section specifies an extension incompatible with its use in the CSR, the command might fail with an error such as **error:11000080:X509 V3 routines:X509V3_EXT_nconf_int:error in extension:crypto/x509/v3_conf.c:48:section=server_cert, name=authorityKeyIdentifier, value=keyid, issuer:always**.
- The default X.500 distinguished name (DN) formatting has been changed to use the UTF-8 formatter. This also causes the removal of space characters around the equal sign (**=**) that separates DN element types from their values.
- Certificate compression extension (RFC 8879) is now supported.
- The QUIC protocol can now be used on the client side as a Technology Preview.

- The Argon2d, Argon2i, and Argon2id key derivation functions (KDF) are supported.
- Brainpool curves have been added to the TLS 1.3 protocol (RFC 8734) but Brainpool curves remain disabled in all supported system-wide cryptographic policies.

Jira:RHEL-26271

crypto-policies provide algorithm selection in Java

The **crypto-policies** packages have been updated to extend its control to algorithm selection in Java. This is caused by the evolution of the Java cryptographic agility configuration and **crypto-policies** needing to catch up to provide a better mapping for a more consistent system-wide configuration. Specifically, the update has the following changes:

- DTLS 1.0 is now controlled by the **protocol** option, is disabled by default, and can be reenabled by using the **protocol@java-tls = DTLS1.0+** scoped directive.
- The **anon** and **NULL** ciphersuites are now controlled by **cipher@java-tls = NULL** and disabled by default.
- The list of signature algorithms is now controlled by the **sign@java-tls** scoped directive and aligned to the system-wide defaults.
- The list of signature algorithms is now controlled by the **sign** option and aligned to the system-wide defaults. If necessary, you can re-enable the use of desired algorithms specifically with Java with a **sign@java-tls = <algorithm1>+ <algorithm2>+** scoped directive.
- Elliptic curve (EC) keys smaller than 256 bits are disabled unconditionally to align with upstream guidance.

As a result, the list of cryptographic algorithms allowed for use with Java by default better matches system-wide defaults. For information on interoperability see the **/etc/crypto-policies/back-ends/java.config** file and configure your active cryptographic policy accordingly.

Jira:RHEL-45620[1]

The selinux-policy git repository for CentOS Stream 10 is now publicly accessible

CentOS Stream contributors now can participate in the development of the SELinux policy by contributing to the **c10s** branch of the **fedora-selinux/selinux-policy** git repository.

Jira:RHEL-22960

clevis rebased to version 20

The **clevis** packages have been upgraded to version 20. The most notable enhancements and fixes include the following:

- Increased security by fixing potential problems reported by static analyzer tools in the **clevis luks** command, **udisks2** integration, and the Shamir's Secret Sharing (SSS) thresholding scheme.
- Password generation now uses the **jose** utility instead of **pwmake**. This ensures enough entropy for passwords generated during the Clevis binding step.

Jira:RHEL-29282

ca-certificates provide trusted CA roots in the OpenSSL directory format

This update populates the **/etc/pki/ca-trust/extracted/pem/directory-hash/** directory with trusted CA root certificates. As a consequence, lookups and validations are faster when OpenSSL is configured to load certificates from this directory, for example, by setting the **SSL_CERT_DIR** environment variable to **/etc/pki/ca-trust/extracted/pem/directory-hash/**.

Jira:RHEL-21094[1]

The nbdkit service is confined by SELinux

The **nbdkit-selinux** subpackage adds new rules to the SELinux policy, and as a result, **nbdkit** is confined in SELinux. Therefore, the systems that run **nbdkit** are more resilient against privilege escalation attacks.

Jira:RHEL-5174

libreswan rebased to 4.15

The **libreswan** packages have been rebased to upstream version 4.15. This version provides substantial improvements over the previous version 4.9 that was provided in previous releases.

- Removed a dependency on **libxz** through **libsystemd**.
- In IKEv1, default proposals have been set to **aes-sha1** for Encapsulating Security Payload (ESP) and **sha1** for Authentication Header (AH).
- IKEv1 rejects ESP proposals that combine Authenticated Encryption with Associated Data (AEAD) and non-empty INTEG.
- IKEv1 rejects exchange when a connection has no proposals.
- IKEv1 has now a more limited default cryptosuite:

```
IKE={AES_CBC,3DES_CBC}-{HMAC_SHA2_256,HMAC_SHA2_512HMAC_SHA1}-
{MODP2048,MODP1536,DH19,DH31}
ESP={AES_CBC,3DES_CBC}-
{HMAC_SHA1_96,HMAC_SHA2_512_256,HMAC_SHA2_256_128}-
{AES_GCM_16_128,AES_GCM_16_256}
AH=HMAC_SHA1_96+HMAC_SHA2_512_256+HMAC_SHA2_256_128
```

- Failures of the **libcap-ng** library are no longer unrecoverable.
- TFC padding is now set for AEAD algorithms in the **pluto** utility.

Jira:RHEL-50006[1]

jose rebased to version 14

The **jose** package has been upgraded to upstream version 14. **jose** is a C-language implementation of the Javascript Object Signing and Encryption (JOSE) standards. The most important enhancements and fixes include the following:

- Improved bound checks for the **len** function for the **oct** JWK Type in OpenSSL.
- The protected JSON Web Encryption (JWE) headers no longer contain **zip**.
- **jose** avoids potential denial of service (DoS) attacks by using high decompression chunks.

Jira:RHEL-38079

Four RHEL services removed from SELinux permissive mode

The following SELinux domains for RHEL services have been removed from SELinux permissive mode:

- **afterburn_t**
- **bootupd_t**
- **mptcpd_t**
- **rshim_t**

Previously, these services from packages recently added to RHEL 9 were temporarily set to SELinux permissive mode, which allows gathering information about additional denials while the rest of the system is in SELinux enforcing mode. This temporary setting has now been removed, and as a result, these services now run in SELinux enforcing mode.

Jira:RHEL-22173

The bootupd service is SELinux confined

The **bootupd** service supports updating the boot loader, and therefore needs to be confined. This update to the SELinux policy adds additional rules, and as a result, the **bootupd** service runs in the **bootupd_t** SELinux domain.

Jira:RHEL-22172

4.3. RHEL FOR EDGE

Support available to file system customization for the simplified-installer and raw image types

With this enhancement, now you can add file system customizations to a blueprint when building the following image types:

- **simplified-installer**
- **edge-raw-image**
- **edge-ami**
- **edge-vsphere**

With some additional exceptions for OSTree systems, you can choose arbitrary directory names at the /**root** level of the file system, for example: /**local**,/***mypartition***, /**$PARTITION**.

In logical volumes, these changes are made on top of the LVM partitioning system. The following directories are supported: /**var**,/**var**/**log**, and /**var**/**lib**/**containers** on a separate logical volume.

Jira:RHELDOCS-17515[1]

4.4. SHELLS AND COMMAND-LINE TOOLS

The default value for the DefaultLimitCore systemd configuration option is now set to unlimited:unlimited

Previously, the default value for the **DefaultLimitCore systemd** configuration option was set to **0:infinity**. As a result, all processes started by **systemd** had a soft process limit for core files set to **0**, and no core files were created by default. However, the process adjusted the limit as required.

With this update, the default value for **DefaultLimitCore** is set to **unlimited:unlimited**. As a result, the core file size is not limited by default. The default size of the crash dumps in the **/etc/systemd/coredump.conf systemd-coredump** component configuration file is **1GiB**. Note that you can gather crash dumps for sporadic crashes, but ensure that the use of disk space by crash dumps remains conservative.

NOTE

The crash dumps stored by **systemd-coredump** are removed after 14 days if not used.

Jira:RHEL-15501

openCryptoki rebased to version 3.23.0

The **openCryptoki** packages are updated to version 3.23.0, which provides multiple bug fixes and enhancements. Notable changes include:

- **EP11**: Added support for FIPS-session mode
- Various updates are available for protection against RSA timing attacks

Jira:RHEL-23673[1]

librtas rebased to version 2.0.6

The **librtas** package is updated to version 2.0.6. With this update, you can use the lockdown-compatible ABI provided by the kernel.

Jira:RHEL-10566[1]

4.5. INFRASTRUCTURE SERVICES

The BIND 9.18 is now supported in RHEL

BIND 9.18 has been added in RHEL 9.5 in the new **bind9.18** package. The notable feature enhancements include the following:

- Added support for DNS over TLS (DoT) and DNS over HTTPS (DoH) in the **named** daemon
- Added support for both incoming and outgoing zone transfers over TLS
- Improved support for OpenSSL 3.0 interfaces
- New configuration options for tuning TCP and UDP send and receive buffers
- Various improvements to the **dig** utility

Jira:RHEL-14898[1]

intel-lpmd package is now available

Intel Low Power Model Daemon is a Linux daemon, which optimizes active idle power. It selects a set of most power efficient CPUs based on configuration file or CPU topology. Based on the system utilization and other information, it puts the system into Low Power Mode by activating the power efficient CPUs and disabling the rest. The system can be restored from Low Power Mode by activating all CPUs.

It is supported on Intel CPUs featuring hybrid architecture such as Performance-cores and Efficient-cores, which includes Meteor Lake CPUs, and both desktop and mobile.

intel-lpmd has the following advantages:

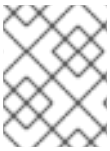
- Improved power efficiency: **intel-lpmd** intelligently distributes workloads between P-cores and E-cores.
- Longer battery life: **intel-lpmd** reduces power consumption during idle periods.

The daemon is not enabled by default. To ensure it starts on boot, run the following command: .Enable the **intel-lpmd** service:

```
# sudo systemctl enable intel_lpmd.service
```

Start the service:

```
# sudo systemctl start intel_lpmd.service
```



NOTE

By default, you must enable **intel-lpmd** if you are required to meet certain product energy efficiency policies.

Jira:RHELDOCS-18391[1]

4.6. NETWORKING

NetworkManager now supports the leftsubnet parameter for IPsec VPNs

With this update, NetworkManager supports the **leftsubnet** parameter to define the private subnet behind the local participant used to configure subnet-to-subnet scenarios in Internet Protocol Security (IPsec) VPNs.

Jira:RHEL-26776

nmstate now supports the congestion window clamp (cwnd) option

With this update, you can use the **cwnd** option of the **nmstate** utility to set a maximum limit on the TCP congestion window size. This way you can control the maximum amount of unacknowledged data expressed as a number of packets that can be in transit over the network at any given time. The following example YAML file sets the **cwnd** option:

```
---
interfaces:
  - name: eth1
    type: ethernet
```

```
    state: up
    ipv4:
      address:
        - ip: 192.0.2.251
          prefix-length: 24
      dhcp: false
      enabled: true

routes:
  config:
    - destination: 198.51.100.0/24
      metric: 150
      next-hop-address: 192.0.2.1
      next-hop-interface: eth1
      table-id: 254
      cwnd: 20
```

Jira:RHEL-19409

The NetworkManager-libreswan plugin supports the rightcert option

You can use the **rightcert** option when configuring Libreswan connections through NetworkManager. With this option, you can authenticate the "right" side participant of the IPsec (Internet Protocol Security) connection using a certificate.

Jira:RHEL-30370

The nmstate utility now supports the rightcert option

You can use the **rightcert** option when configuring Libreswan connections through the **nmstate** utility. With this option, you can authenticate the "right" side participant of the IPsec (Internet Protocol Security) connection using the certificate. The following example YAML file sets the **rightcert** option:

```
---
interfaces:
- name: hosta_conn
  type: ipsec
  ipv4:
    enabled: true
    dhcp: true
  libreswan:
    left: 192.0.2.1
    leftid: '%fromcert'
    leftrsasigkey: '%cert'
    leftmodecfgclient: false
    leftcert: leftcert.example.com
    right: 192.0.2.2
    rightid: '%fromcert'
    rightrsasigkey: '%cert'
    rightcert: rightcert.example.com
    rightsubnet: 192.0.2.2/32
```

Jira:RHEL-28898

nmstate now supports the leftsubnet option

You can define entire subnets for IPsec (Internet Protocol Security) connections when configuring

Libreswan connections through the **nmstate** utility by using the **leftsubnet** option. This ensures secure communication between different network segments. The following example YAML file sets the **leftsubnet** option:

```
interfaces:
- name: hosta
  type: ipsec
  ipv4:
    enabled: true
    dhcp: true
  libreswan:
    left: 192.0.2.246
    leftid: _<hosta.example.org>_
    leftcert: _<hosta.example.org>_
    leftsubnet: 192.0.4.0/24
    leftmodecfgclient: no
    right: 192.0.2.157
    rightid: _<hostb.example.org>_
    rightsubnet: 192.0.3.0/24
    ikev2: insist
```

Note that the IPsec technology requires a peer-to-peer configuration, including another server with appropriate IP addresses and IPsec settings.

Jira:RHEL-26755

NetworkManager supports connecting to IPsec VPNs that use IPv6 addressing

Previously, NetworkManager supported only IPv4 addressing when using the **NetworkManager-libreswan** plugin to connect to Internet Protocol Security (IPsec) VPN. With this update, you can connect to IPsec VPNs that use IPv6 addressing.

Jira:RHEL-21875

You can use both firewalld and nftables services simultaneously

The **firewalld** and **nftables systemd** services are available to use simultaneously. Previously, users could enable only one of these services at a time. With this enhancement, these **systemd** services no longer conflict with each other.

Jira:RHEL-17002[1]

4.7. KERNEL

Kernel version in RHEL 9.5

Red Hat Enterprise Linux 9.5 is distributed with the kernel version 5.14.0-503.11.1.

The eBPF facility has been rebased to Linux kernel version 6.8

Notable changes and enhancements include:

- Support exceptions allowing asserting conditions in BPF programs that should never be true but are hard for the verifier to infer.
- Improved working with per-cpu objects such as support for local per-cpu kptr and support for allocating and storing per-cpu objects in maps.

- Support for BPF v4 CPU instructions for **arm32** and **s390x**.
- Several new open-coded iterators for task, task_vma, css, and css_task.
- New **kfunc** that acquires the associated cgroup of a task within a specific cgroup v1 hierarchy.
- Support for BPF link_info for uprobe multi-link along with **bpftool** integration.
- Several improvements and bug fixes in the BPF verifier allowing more precise program verification and improving the BPF program developer experience.
- Verifier improvement which prevents the creation of infinite loops by combining tail calls and fentry/fexit programs.
- Change in BPF verifier logic to validate global subprograms lazily instead of unconditionally before the main program, so they can be guarded using BPF CO-RE techniques.
- Add the ability to pin the BPF timer to the current CPU.
- Support UID or GID options when mounting **bpffs**.

Jira:RHEL-23644[1]

rteval now supports relative CPU lists for loads

With this enhancement, the **--loads-cpulist** now accepts relative CPU lists as arguments. The syntax is the same for the default measurement CPU list when using the parameter **--measurement-cpulist**.

Jira:RHEL-25206[1]

A support for 420xx devices is added to QAT

With this update, QAT supports 420xx devices. It includes a new device driver that supports updates to the firmware loader and other capabilities. Compared to 4xxx devices, the 420xx devices now have more acceleration engines, 16 service engines, and 1 administrative engine, and support the wireless cipher algorithms **ZUC** and **Snow 3G**.

Jira:RHEL-17715[1]

Introducing noswap option when mounting TMPFS filesystem

TMPFS is an in-memory filesystem largely utilized for quickly sharing information across multiple processes. Starting with version 2.2, **glibc** expects a **tmpfs** filesystem to be mounted at **dev/shm** to support POSIX shared memory. This mount point is necessary for **shm_open** and **shm_unlink** subroutines to function correctly. TMPFS blocks can be swapped out when there is a memory shortage, which poses a problem for certain performance- or privacy-critical workloads.

Passing the new **noswap** mount option when mounting a TMPFS filesystem disables swap for that particular mount point of TMPFS.

Jira:RHEL-31975[1]

Kernel module is now updated to version 6.8

Kernel module is now updated to version 6.8, which includes the following features:

- Improved Hardware Support: Expanded compatibility for the latest processors, GPUs, and peripherals.

- Security Enhancements: Integration of critical security patches and mitigations to address recent vulnerabilities.
- Performance Optimizations: Enhanced scheduling, memory management, and I/O performance for improved workload efficiency.

Jira:RHEL-28063[1]

Introducing rteval container for real-time performance testing

The **rteval** container provides tools and methods for accurately measuring system latencies. With this feature, users can measure the real-time performance of their systems. It evaluates the configuration of the Linux kernel for optimal real-time performance to analyze performance based on specific application needs.

Note that no specific tuning guidelines are provided in the RHEL 9.5 release, and support is limited to customers with a Real-Time subscription.

Jira:RHELDOCS-19122[1]

NVMf-FC kdump is now supported on the IBM Power

NVMf-FC kdump now supports the IBM Power system for running **kexec-tools**. This allows the capture of system memory dumps over a fiber channel network using the NVMe storage devices for high-speed and low-latency access to storage for crash dump data.

Jira:RHEL-11471[1]

4.8. BOOT LOADER

UEFI variable filesystem (efivarfs) now supports analyzing persistent EFI variable space

With this update, you can now analyze the space used by persistent EFI variable storage on systems booted in UEFI mode. Using the utilities **df** and **du**, you can calculate the total space used by UEFI variables, such as EFI boot variables and the UEFI Secure Boot databases.

This prevents space exhaustion and enables better management of UEFI-related configuration, including Secure Boot and boot order settings.

Jira:RHELDOCS-19280[1]

4.9. FILE SYSTEMS AND STORAGE

File system quotas for tmpfs file system are supported

With this update, system administrators can implement file system quotas to limit the space or memory users can consume on a **tmpfs** file system, preventing memory exhaustion.

Jira:RHEL-7768[1]

NVMe TP 8006 in-band authentication with NVMe/TCP is supported

NVMe TP 8006 in-band authentication for NVMe over Fabrics (NVMe-oF) was introduced in RHEL 9.2 as a Technology Preview, which is fully supported. This feature provides DH-HMAC-CHAP in-band authentication protocol for NVMe-oF, which is defined in the NVMe Technical Proposal 8006. For

details, see the **dhchap-secret** and **dhchap-ctrl-secret** option descriptions in the **nvme-connect(1)** man page.

Jira:RHEL-61452

cryptsetup rebased to version 2.7

The **cryptsetup** package has been rebased to version 2.7. It contains improvements for the **libcryptsetup** package to support Linux Unified Key Setup (LUKS) encrypted devices in the **kdump** enabled systems.

Jira:RHEL-32377[1]

Dax feature is supported for Ext4 and XFS

The direct access (dax) feature for the Ext4 and XFS file systems, previously available as a Technology Preview, is fully supported. DAX enables an application to map persistent memory directly into its address space, enhancing performance. For more information, see Creating a file system DAX namespace on an NVDIMM.

Jira:RHELDOCS-19196[1]

EROFS file system is supported

EROFS is a lightweight generic read-only file system suitable for various read-only use cases, such as embedded devices or containers. It provides deduplication and transparent compression as options for scenarios that require them.

For more information, see the erofs documentation.

Jira:RHELDOCS-18451

nvme-cli and cryptsetup are now available for Opal automation on NVMe SEDs

NVMe Self-Encrypting Drives (SED) support the Opal storage specification of hardware encryption technology to secure data stored in the drive. Previously, Opal support for NVMe SEDs required manual interaction to manage passwords to access the data.

With this update, you can use **nvme-cli** and **cryptsetup** to automate encryption management and drive unlocking.

Run the following commands to use NVMe SED options on NVMe SSD:

- To discover SED Opal locking features:

```
# nvme sed discover /dev/nvme0n1
Locking Features:
 Locking Supported: Yes
 Locking Feature Enabled: No
 Locked: No
```

- To initialize an SED Opal device for locking:

```
# nvme sed initialize /dev/nvme0n1
New Password:
Re-enter New Password:
# nvme sed discover /dev/nvme0n1
```

```
Locking Features:
 Locking Supported: Yes
 Locking Feature Enabled: Yes
 Locked: No
```

- To lock a SED Opal device:

```
# nvme sed lock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
 Locking Supported: Yes
 Locking Feature Enabled: Yes
 Locked: Yes
```

- To unlock a SED Opal device:

```
# nvme sed unlock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
 Locking Supported: Yes
 Locking Feature Enabled: Yes
 Locked: No
```

- To change the SED Opal device password:

```
# nvme sed password /dev/nvme0n1
Password:
New Password:
Re-enter New Password:
```

- To revert an SED Opal device from locking:

```
# nvme sed lock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
        Locking Supported:         Yes
        Locking Feature Enabled:   Yes
        Locked:                    Yes
# nvme sed unlock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
        Locking Supported:         Yes
        Locking Feature Enabled:   Yes
        Locked:                    No
# nvme sed revert /dev/nvme0n1
```

- To reset an SED Opal device to disable locking with destructive revert:

```
# nvme sed lock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
        Locking Supported:       Yes
        Locking Feature Enabled: Yes
        Locked: Yes
```

```
# nvme sed revert -e /dev/nvme0n1
Destructive revert erases drive data. Continue (y/n)? y
   Are you sure (y/n)? y
   Password:
   # nvme sed discover /dev/nvme0n1
   Locking Features:
      Locking Supported:       Yes
      Locking Feature Enabled: No
      Locked:                  No
```

Note: Use **nvme sed revert** without the **-e** parameter to avoid erasing data on the NVMe disk.

The device may be either an NVMe character device such as /**dev**/**nvme0**, an NVMe block device such as /**dev**/**nvme0n1**, or an **mctp** address in the form **mctp:<net>,<eid>[:ctrl-id]**.

Example command to use an NVMe OPAL device on RHEL 10 with nvme-cli:

- Initialize, lock, and unlock an NVMe disk, and verify that data on the disk remains unchanged after unlocking:

```
# mount /dev/nvme0n1p1 /mnt/
# dd if=/dev/urandom of=/mnt/test.file bs=1M count=1024
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 3.65616 s, 294 MB/s
# md5sum /mnt/test.file
57edc80dab5bf803d0944e281bf2e9dd  /mnt/test.file
# umount /dev/nvme0n1p1
# nvme sed discover /dev/nvme0n1
Locking Features:
 Locking Supported:         Yes
 Locking Feature Enabled:   No
 Locked:                    No
# nvme sed initialize /dev/nvme0n1
New Password:
Re-enter New Password:
# nvme sed lock /dev/nvme0n1
# nvme sed discover /dev/nvme0n1
Locking Features:
 Locking Supported:         Yes
 Locking Feature Enabled:   Yes
 Locked:                    Yes
# mount /dev/nvme0n1p1 /mnt/
mount: /mnt: can't read superblock on /dev/nvme0n1p1.
       dmesg[8] may have more information after a failed mount system call.
# nvme sed unlock /dev/nvme0n1
# mount /dev/nvme0n1p1 /mnt/
# md5sum /mnt/test.file
57edc80dab5bf803d0944e281bf2e9dd  /mnt/test.file
# umount /dev/nvme0n1p1
# nvme sed discover /dev/nvme0n1
Locking Features:
   Locking Supported:         Yes
   Locking Feature Enabled:   Yes
   Locked:                    No
# nvme sed revert /dev/nvme0n1
```

```
Password:
# nvme sed discover /dev/nvme0n1
Locking Features:
   Locking Supported:        Yes
   Locking Feature Enabled:  No
   Locked:                   No
```

Jira:RHEL-18186

4.10. HIGH AVAILABILITY AND CLUSTERS

New pcs status wait command

The **pcs** command-line interface now provides a **pcs status wait** command. This command ensures that Pacemaker has completed any actions required by changes to the Cluster Information Base (CIB) and does not need to take any further actions in order to make the actual cluster state match the requested cluster state.

Jira:RHEL-25854

pcs support for new commands to query the status of a resource in a cluster

The **pcs** command-line interface now provides **pcs status query resource** commands to query various attributes of a single resource in a cluster. These commands query:

- the existence of the resource
- the type of the resource
- the state of the resource
- various information about the members of a collective resource
- on which nodes the resource is running

You can use these commands for pcs-based scripting since there is no need to parse plain text outputs.

Jira:RHEL-21051

New pcs resource defaults and pcs resource op defaults option for displaying configuration in text, JSON, and command formats

The **pcs resource defaults** and **pcs resource op defaults** commands and their aliases **pcs stonith defaults** and **pcs stonith op defaults** now provide the **--output-format** option.

- Specifying **--output-format=text** displays the configured resource defaults or operation defaults in plain text format, which is the default value for this option.
- Specifying **--output-format=cmd** displays the **pcs resource defaults** or **pcs resource op defaults** commands created from the current cluster defaults configuration. You can use these commands to re-create configured resource defaults or resource operation defaults on a different system.
- Specifying **--output-format=json** displays the configured resource defaults or resource operation defaults in JSON format, which is suitable for machine parsing.

Jira:RHEL-16231

New Pacemaker option to leave a panicked node shut down without rebooting automatically

You can now set the **PCMK_panic_action** variable in the **/etc/sysconfig/pacemaker** configuration file to **off** or **sync-off**. When you set this variable to **off** or **sync-off**, a node remains shut down after a panic condition instead of rebooting automatically.

Jira:RHEL-39057

Support for new pcsd Web UI features

The **pcsd** Web UI now supports the following features:

- When you set the **placement-strategy** cluster property to **default**, the **pcsd** Web UI displays a warning near the utilization attributes for nodes and resources. This warning notes that the utilization has no effect due to **placement-strategy** configuration.
- The **pscd** Web UI supports dark mode, which you can set through the user menu in the masthead.

Jira:RHEL-21895, Jira:RHEL-7726

4.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

Increased performance of the Python interpreter

All supported versions of Python in RHEL 9 are now compiled with GCC's **-O3** optimization flag, which is the default in upstream. As a result, you can observe increased performance of your Python applications and the interpreter itself.

Jira:RHEL-49615[1], Jira:RHEL-49635, Jira:RHEL-49637

httpd rebased to 2.4.62

The **httpd** package has been updated to version 2.4.62 that includes various bug fixes, security fixes, and new features. Notable feature include :

- The following directives have been added:
  - **CGIScriptTimeout** directive is added in the **mod_cgi** module .
  - **AliasPreservePath** directive in the **mod_alias** module to map the full path after alias in a location.
  - **RedirectRelative** directive in **mod_alias** to allow relative redirect targets to be issued as-is.
  - **DeflateAlterETag** directive in the **mod_deflate** module to control the modification of **ETag**. The **NoChange** parameter mimics 2.2.x behavior.
- An optional third argument for the **ProxyRemote** server is added in the **mod_proxy** module which configures basic authentication credentials to pass to the remote proxy.
- **LDAPConnectionPoolTTL** directive now accepts negative values to allow reusing the connections of any age. Previously, an error was encountered in the **mod_ldap** module when you parsed the configuration file with a negative value.

- You can now use the **-T** option to allow truncating the subsequent rotated log files without the initial log file being truncated in the rotatelogs binary.

Jira:RHEL-14668

mod_md rebased to version 2.4.26

The **mod_md** module has been updated to version 2.4.26. Notable changes over the previous version include:

- The following directives have been added:
  - **MDCheckInterval** to control the number of server checks for detected revocations.
  - **MDMatchNames all|servernames** to allow more control over how the MDomains are matched to the VirtualHosts.
  - **MDChallengeDns01Version** . When you set the value of this directive to **2**, it provides the command with the challenge value on the **teardown** invocation. By default, in version 1, only the **setup** invocation gets this parameter.
- For Managed Domain in **manual mode**, the **mod_md_verification** module now checks if all used **ServerName** and **ServerAlias** reports a warning instead of an error (AH10040).
- You can now configure the **MDChallengeDns01** directive for individual domains.

Jira:RHEL-25075[1]

PostgreSQL 16 now provides the pgvector extension

The **postgresql:16** module stream is now distributed with the **pgvector** extension. With the **pgvector** extension, you can store and query high-dimensional vector embeddings directly within PostgreSQL databases and perform a vector similarity search. Vector embeddings are numerical representations of data that are often used in machine learning and AI applications to capture the semantic meaning of text, images, or other data types.

Jira:RHEL-34669

A new db_converter tool to convert a libdb database to the GDBM format

The deprecated Berkeley DB (**libdb**) now provides the **db_converter** tool for converting a **lidbd** database to the GNU dbm (GDBM) database format. The **db_converter** tool is distributed in the **libdb-utils** subpackage.

For more information about alternatives to **libdb**, see the Red Hat Knowledgebase article Available replacements for the deprecated Berkeley DB (libdb) in RHEL.

Jira:RHEL-35607

A new nodejs:22 module stream is fully supported

A new module stream, **nodejs:22**, previously available as a Technology Preview, is fully supported with the release of the RHEA-2024:11235 advisory. The **nodejs:22** module stream now provides **Node.js 22.11**, which is a Long Term Support (LTS) version.

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, execute the **node --run <script-in-package.json>** command.

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

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

If you want to upgrade from the **nodejs:20** 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-67327

4.12. COMPILERS AND DEVELOPMENT TOOLS

System GCC rebased to version 11.5

The system version of GCC in RHEL 9 has been updated to version 11.5. This update provides numerous bug fixes.

Jira:RHEL-35635

A new tunable for glibc is available to improve performance by placing dynamic objects closer together

Previously, the dynamic loader of **glibc** placed dynamic objects randomly throughout the available address space to enhance security. Consequently, objects were often too far apart, which led to inefficient calls between them.

With this update, you can now place objects closer together, specifically, in the first 2 GB of address space, by setting the following tunable:

```
export GLIBC_TUNABLES=glibc.cpu.prefer_map_32bit_exec=1
```

Setting this tunable might result in improved performance for some applications at the expense of a small reduction in address space layout randomization (ASLR).

Jira:RHEL-20172[1]

glibc now supports dynamic linking of Intel APX-enabled functions

An incompatible dynamic linker trampoline was identified as a potential source of incompatibilities for Intel Advanced Performance Extensions (APX) applications. As a workaround, it was possible to use the **BIND_NOW** executable or use only the standard calling convention. With this update, the dynamic linker of **glibc** preserves APX-related registers.

NOTE

Because of this change, additional space is needed beyond the top of the stack. Users who strictly limit this space might need to adjust or evaluate the stack limits.

Jira:RHEL-25046[1]

Optimization of AMD Zen 3 and Zen 4 performance in glibc

Previously, AMD Zen 3 and Zen 4 processors sometimes used the Enhanced Repeat Move String (ERMS) version of the **memcpy** and **memmove** library routines regardless of the most optimal choice. With this update to **glibc**, AMD Zen 3 and Zen 4 processors use the most optimal versions of **memcpy** and **memmove**.

Jira:RHEL-25531[1]

System version of GDB rebased to version 14.2 and GDB removed from GCC Toolset

GDB has been updated to version 14.2. Starting with RHEL 9.5, GDB is transitioning into a rolling Application Stream with its system version rebased in minor releases of RHEL. Therefore, GDB is not included in GCC Toolset 14 in RHEL 9.

The following paragraphs list notable changes in GDB 14.2 since GDB 12.1.

General:

- The **info breakpoints** command now displays enabled breakpoint locations of disabled breakpoints as in the **y-** state.
- Added support for debug sections compressed with Zstandard (**ELFCOMPRESS_ZSTD**) for ELF.
- The Text User Interface (TUI) no longer styles the source and assembly code highlighted by the current position indicator by default. To re-enable styling, use the new command **set style tui-current-position**.
- A new **$_inferior_thread_count** convenience variable contains the number of live threads in the current inferior.
- For breakpoints with multiple code locations, GDB now prints the code location using the **<breakpoint_number>.<location_number>** syntax.
- When a breakpoint is hit, GDB now sets the **$_hit_bpnum** and **$_hit_locno** convenience variables to the hit breakpoint number and code location number. You can now disable the last hit breakpoint by using the **disable $_hit_bpnum** command, or disable only the specific breakpoint code location by using the **disable $_hit_bpnum.$_hit_locno** command.
- Added support for the **NO_COLOR** environment variable.

- Added support for integer types larger than 64 bits.
- You can use new commands for multi-target feature configuration to configure remote target feature sets (see the **set remote <name>-packet** and **show remote <name>-packet** in Commands).
- Added support for the Debugger Adapter Protocol.
- You can now use the new **inferior** keyword to make breakpoints inferior-specific (see **break** or **watch** in Commands).
- You can now use the new **$_shell()** convenience function to run a shell command during expression evaluation.

Changes to existing commands:

- **break**, **watch**
  - Using the **thread** or **task** keywords multiple times with the **break** and **watch** commands now results in an error instead of using the thread or task ID of the last instance of the keyword.
  - Using more than one of the **thread**, **task**, and **inferior** keywords in the same **break** or **watch** command is now invalid.
- **printf**, **dprintf**
  - The **printf** and **dprintf** commands now accept the **%V** output format, which formats an expression the same way as the **print** command. You can also modify the output format by using additional print options in brackets **[...]** following the command, for example: **printf "%V[-array-indexes on]", <array>**.
- **list**
  - You can now use the **.** argument to print the location around the point of execution in the current frame, or around the beginning of the **main()** function if the inferior has not started yet.
  - Attempting to list more source lines in a file than are available now issues a warning, referring the user to the **.** argument.
- **document user-defined**
  - It is now possible to document user-defined aliases.

New commands:

- **set print nibbles [on|off]** (default: **off**), **show print nibbles** - controls whether the **print/t** command displays binary values in groups of four bits (nibbles).
- **set debug infcall [on|off]** (default: **off**), **show debug infcall** - prints additional debug messages about inferior function calls.
- **set debug solib [on|off]** (default: **off**), **show debug solib** - prints additional debug messages about shared library handling.
- **set print characters <LIMIT>**, **show print characters**, **print -characters <LIMIT>** - controls how many characters of a string are printed.

- **set debug breakpoint [on|off]** (default: **off**), **show debug breakpoint** - prints additional debug messages about breakpoint insertion and removal.
- **maintenance print record-instruction [N]** - prints the recorded information for a given instruction.
- **maintenance info frame-unwinders** - lists the frame unwinders currently in effect in the order of priority (highest first).
- **maintenance wait-for-index-cache** - waits until all pending writes to the index cache are completed.
- **info main** - prints information on the main symbol to identify an entry point into the program.
- **set tui mouse-events [on|off]** (default: **on**), **show tui mouse-events** - controls whether mouse click events are sent to the TUI and Python extensions (when **on**), or the terminal (when **off**).

Machine Interface (MI) changes:

- MI version 1 has been removed.
- MI now reports **no-history** when reverse execution history is exhausted.
- The **thread** and **task** breakpoint fields are no longer reported twice in the output of the **-break-insert** command.
- Thread-specific breakpoints can no longer be created on non-existent thread IDs.
- The **--simple-values** argument to the **-stack-list-arguments**, **-stack-list-locals**, **-stack-list-variables**, and **-var-list-children** commands now considers reference types as simple if the target is simple.
- The **-break-insert** command now accepts a new **-g thread-group-id** option to create inferior-specific breakpoints.
- Breakpoint-created notifications and the output of the **-break-insert** command can now include an optional **inferior** field for the main breakpoint and each breakpoint location.
- The asynchronous record stating the **breakpoint-hit** stopped reason now contains an optional field **locno** giving the code location number in case of a multi-location breakpoint.

Changes in the GDB Python API:

- Events
  - A new **gdb.ThreadExitedEvent** event.
  - A new **gdb.executable_changed** event registry, which emits the **ExecutableChangedEvent** objects that have **progspace** and **reload** attributes.
  - New **gdb.events.new_progspace** and **gdb.events.free_progspace** event registries, which emit the **NewProgpspaceEvent** and **FreeProgspaceEvent** event types. Both of these event types have a single attribute **progspace** to specify the **gdb.Progspace** program space that is being added to or removed from GDB.
- The **gdb.unwinder.Unwinder** class
  - The **name** attribute is now read-only.

    - The name argument of the **__init__** function must be of the **str** type, otherwise a **TypeError** is raised.
    - The **enabled** attribute now accepts only the **bool** type.
- The **gdb.PendingFrame** class
    - New methods: **name**, **is_valid**, **pc**, **language**, **find_sal**, **block**, and **function**, which mirror similar methods of the **gdb.Frame** class.
    - The **frame-id** argument of the **create_unwind_info** function can now be either an integer or a **gdb.Value** object for the **pc**, **sp**, and **special** attributes.
- A new **gdb.unwinder.FrameId** class, which can be passed to the **gdb.PendingFrame.create_unwind_info** function.
- The **gdb.disassembler.DisassemblerResult** class can no longer be sub-classed.
- The **gdb.disassembler** module now includes styling support.
- A new **gdb.execute_mi(COMMAND, [ARG]...)** function, which invokes a GDB/MI command and returns result as a Python dictionary.
- A new **gdb.block_signals()** function, which returns a context manager that blocks any signals that GDB needs to handle.
- A new **gdb.Thread** subclass of the **threading.Thread** class, which calls the **gdb.block_signals** function in its **start** method.
- The **gdb.parse_and_eval** function has a new **global_context** parameter to restrict parsing on global symbols.
- The **gdb.Inferior** class
    - A new **arguments** attribute, which holds the command-line arguments to the inferior, if known.
    - A new **main_name** attribute, which holds the name of the inferior's **main** function, if known.
    - New **clear_env**, **set_env**, and **unset_env** methods, which can modify the inferior's environment before it is started.
- The **gdb.Value** class
    - A new **assign** method to assign a value of an object.
    - A new **to_array** method to convert an array-like value to an array.
- The **gdb.Progspace** class
    - A new **objfile_for_address** method, which returns the **gdb.Objfile** object that covers a given address (if exists).
    - A new **symbol_file** attribute holding the **gdb.Objfile** object that corresponds to the **Progspace.filename** variable (or **None** if the filename is **None**).
    - A new **executable_filename** attribute, which holds the string with a filename that is set by the **exec-file** or **file** commands, or **None** if no executable file is set.

- The **gdb.Breakpoint** class
  - A new **inferior** attribute, which contains the inferior ID (an integer) for breakpoints that are inferior-specific, or **None** if no such breakpoints are set.
- The **gdb.Type** class
  - New **is_array_like** and **is_string_like** methods, which reflect whether a type might be array- or string-like regardless of the type's actual type code.
- A new **gdb.ValuePrinter** class, which can be used as the base class for the result of applying a pretty-printer.
- A newly implemented **gdb.LazyString.__str__** method.
- The **gdb.Frame** class
  - A new **static_link** method, which returns the outer frame of a nested function frame.
  - A new **gdb.Frame.language** method that returns the name of the frame's language.
- The **gdb.Command** class
  - GDB now reformats the doc string for the **gdb.Command** class and the **gdb.Parameter** sub-classes to remove unnecessary leading whitespace from each line before using the string as the help output.
- The **gdb.Objfile** class
  - A new **is_file** attribute.
- A new **gdb.format_address(ADDRESS, PROGSPACE, ARCHITECTURE)** function, which uses the same format as when printing address, symbol, and offset information from the disassembler.
- A new **gdb.current_language** function, which returns the name of the current language.
- A new Python API for wrapping GDB's disassembler, including **gdb.disassembler.register_disassembler(DISASSEMBLER, ARCH)**, **gdb.disassembler.Disassembler**, **gdb.disassembler.DisassembleInfo**, **gdb.disassembler.builtin_disassemble(INFO, MEMORY_SOURCE)**, and **gdb.disassembler.DisassemblerResult**.
- A new **gdb.print_options** function, which returns a dictionary of the prevailing print options, in the form accepted by the **gdb.Value.format_string** function.
- The **gdb.Value.format_string** function
  - **gdb.Value.format_string** now uses the format provided by the **print** command if it is called during a **print** or other similar operation.
  - **gdb.Value.format_string** now accepts the **summary** keyword.
- A new **gdb.BreakpointLocation** Python type.
- The **gdb.register_window_type** method now restricts the set of acceptable window names.

Architecture-specific changes:

- AMD and Intel 64-bit architectures
  - Added support for disassembler styling using the **libopcodes** library, which is now used by default. You can modify how the disassembler output is styled by using the **set style disassembler *** commands. To use the Python Pygments styling instead, use the new **maintenance set libopcodes-styling off** command.
- The 64-bit ARM architecture
  - Added support for dumping memory tag data for the Memory Tagging Extension (MTE).
  - Added support for the Scalable Matrix Extension 1 and 2 (SME/SME2). Some features are still considered experimental or alpha, for example, manual function calls with ZA state or tracking Scalable Vector Graphics (SVG) changes based on DWARF.
  - Added support for Thread Local Storage (TLS) variables.
  - Added support for hardware watchpoints.
- The 64-bit IBM Z architecture
  - Record and replay support for the new **arch14** instructions on IBM Z targets, except for the specialized-function-assist instruction **NNPA**.
- IBM Power Systems, Little Endian
  - Added base enablement support for POWER11.

For more details about rolling Application Streams, see the Red Hat Enterprise Linux Application Streams Life Cycle.

Jira:RHEL-36211, Jira:RHEL-10550, Jira:RHEL-39555

elfutils rebased to version 0.191

The **elfutils** package has been updated to version 0.191. Notable improvements include:

- Changes in the **libdw** library:
  - The **dwarf_addrdie** function now supports binaries lacking a **debug_aranges** section.
  - Support for DWARF package files has been improved.
  - A new **dwarf_cu_dwp_section_info** function has been added.
- Caching eviction logic in the **debuginfod** server has been enhanced to improve retention of small, frequent, or slow files, such as **vdso.debug**.
- The **eu-srcfiles** utility can now fetch the source files of a DWARF/ELF file and place them into a **zip** archive.

Jira:RHEL-29194

SystemTap rebased to version 5.1

The **SystemTap** tracing and probing tool has been updated to version 5.1. Notable changes include:

- An experimental **--build-as=USER** flag to reduce privileges during script compilation.

- Improved support for probing processes running in containers, identified by host PID.
- New probes for userspace hardware breakpoints and watchpoints.
- Support for the **--remote** operation of **--runtime=bpf** mode.
- Improved robustness of kernel-user transport.

Jira:RHEL-29528

valgrind rebased to version 3.23.0

The **Valgrind** suite has been updated to version 3.23.0. Notable enhancements include:

- The **--track-fds=yes** option now warns against double closing of file descriptors, generates suppressible errors, and supports XML output.
- The **--show-error-list=no|yes** option now accepts a new value, **all**, to also print the suppressed errors.
- On the 64-bit IBM Z architecture, **Valgrind** now supports neural network processing assist (NNPA) facility vector instructions: **VCNF**, **VCLFNH**, **VCFN**, **VCLFNL**, **VCRNF**, and **NNPA** (z16/arch14).
- On the 64-bit ARM architecture, **Valgrind** now supports **dotprod** instructions (**sdot**/**udot**).
- On the AMD and Intel 64-bit architectures, **Valgrind** now provides more accurate instruction support for the x86_64-v3 microarchitecture.
- **Valgrind** now provides wrappers for the **wcpncpy**, **memccpy**, **strlcat**, and **strlcpy** functions that can detect memory overlap.
- **Valgrind** now supports the following Linux syscalls: **mlock2**, **fchmodat2**, and **pidfd_getfd**.

Jira:RHEL-29534, Jira:RHEL-10551

libabigail rebased to version 2.5

The **libabigail** library has been updated to version 2.5. Notable changes include:

- Improved suppression specification for strict conversions of flexible array data members.
- Added support for pointer-to-member types in C++ binaries.
- Improved **weak** mode of the **abicompat** tool.
- A new **abidb** tool to manage the ABI of operating systems.
- Numerous bug fixes.

Jira:RHEL-30013, Jira:RHEL-7325, Jira:RHEL-7332

New GCC Toolset 14

GCC Toolset 14 is a compiler toolset that provides recent versions of development tools. It is available as an Application Stream in the form of a Software Collection in the AppStream repository.

The following tools and versions are provided by GCC Toolset 14:

- GCC 14.2
- **binutils** 2.41
- **annobin** 12.70
- **dwz** 0.14

Note that the system version of GDB has been rebased and GDB is no longer included in GCC Toolset .

To install GCC Toolset 14, enter the following command as root:

```
# dnf install gcc-toolset-14
```

To run a tool from GCC Toolset 14:

```
$ scl enable gcc-toolset-14 <tool>
```

To run a shell session where tool versions from GCC Toolset 14 override system versions of these tools:

```
$ scl enable gcc-toolset-14 bash
```

GCC Toolset 14 components are also available in the **gcc-toolset-14-toolchain** container image.

For more information, see GCC Toolset 14 and Using GCC Toolset.

Jira:RHEL-29758[1], Jira:RHEL-29852

GCC Toolset 14: GCC rebased to version 14.2

In GCC Toolset 14, the GNU Compiler Collection (GCC) has been updated to version 14.2.

Notable changes include:

- Optimization and diagnostic improvements
- A new **-fhardened** umbrella option, which enables a set of hardening flags
- A new **-fharden-control-flow-redundancy** option to detect attacks that transfer control into the middle of functions
- A new **strub** type attribute to control stack scrubbing properties of functions and variables
- A new **-finline-stringops** option to force inline expansion of certain **mem*** functions
- Support for new OpenMP 5.1, 5.2, and 6.0 features
- Several new C23 features
- Multiple new C++23 and C++26 features
- Several resolved C++ defect reports
- New and improved experimental support for C++20, C++23, and C++26 in the C++ library
- Support for new CPUs in the 64-bit ARM architecture

- Multiple new instruction set architecture (ISA) extensions in the 64-bit Intel architecture, for example: AVX10.1, AVX-VNNI-INT16, SHA512, and SM4
- New warnings in the GCC's static analyzer
- Certain warnings changed to errors; for details, see Porting to GCC 14
- Various bug fixes

For more information about changes in GCC 14, see the upstream GCC release notes.

Jira:RHEL-29853[1]

GCC Toolset 14: annobin rebased to version 12.70

In GCC Toolset 14, **annobin** has been updated to version 12.70. The updated set of the **annobin** tools for testing binaries provides various bug fixes, introduces new tests, and updates the tools to build and work with newer versions of the GCC, Clang, LLVM, and Go compilers. With the enhanced tools, you can detect new issues in programs that are built in a non-standard way.

Jira:RHEL-29850[1]

GCC Toolset 14: binutils rebased to version 2.41

RHEL 9.5 is distributed with GCC Toolset 14 **binutils** version 2.41. New features include:

- **binutils** tools support architecture extensions in the 64-bit Intel and ARM architectures.
- The linker now accepts the **--remap-inputs <PATTERN>=<FILE>** command-line option to replace any input file that matches **<PATTERN>** with **<FILE>**. In addition, you can use the **--remap-inputs-file=<FILE>** option to specify a file containing any number of these remapping directives.
- For ELF targets, you can use the linker command-line option **--print-map-locals** to include local symbols in a linker map.
- For most ELF-based targets, you can use the **--enable-linker-version** option to insert the version of the linker as a string into the **.comment** section.
- The linker script syntax has a new command for output sections, **ASCIZ "<string>"**, which inserts a zero-terminated string at the current location.
- You can use the new **-z nosectionheader** linker command-line option to omit ELF section header.

Jira:RHEL-29851[1]

GCC Toolset 13: GCC supports AMD Zen 5

The GCC Toolset 13 version of GCC adds support for the AMD Zen 5 processor microarchitecture. To enable the support, use the **-march=znver5** command-line option.

Jira:RHEL-36523[1]

LLVM Toolset updated to 18.1.8

LLVM Toolset has been updated to version 18.1.8.

Notable LLVM updates:

- The constant expression variants of the following instructions have been removed: **and**, **or**, **lshr**, **ashr**, **zext**, **sext**, **fptrunc**, **fpext**, **fptoui**, **fptosi**, **uitofp**, **sitofp**.
- The **llvm.exp10** intrinsic has been added.
- The **code_model** attribute for global variables has been added.
- The backend for the AArch64, AMDGPU, PowerPC, RISC-V, SystemZ and x86 architectures has been improved.
- LLVM tools have been improved.

Notable Clang enhancements:

- C++20 feature support:
  - Clang no longer performs One Definition Rule (ODR) checks for declarations in the global module fragment. To enable more strict behavior, use the **-Xclang -fno-skip-odr-check-in-gmf** option.
- C++23 feature support:
  - A new diagnostic flag **-Wc++23-lambda-attributes** has been added to warn about the use of attributes on lambdas.
- C++2c feature support:
  - Clang now allows using the _ character as a placeholder variable name multiple times in the same scope.
  - Attributes now expect unevaluated strings in attribute parameters that are string literals.
  - The deprecated arithmetic conversion on enumerations from C++26 has been removed.
  - The specification of template parameter initialization has been improved.
- For a complete list of changes, see the upstream release notes for Clang .

ABI changes in Clang:

- Following the SystemV ABI for x86_64, the **__int128** arguments are no longer split between a register and a stack slot.
- For more information, see the list of ABI changes in Clang .

Notable backwards incompatible changes:

- A bug fix in the reversed argument order for templated operators breaks code in C++20 that was previously accepted in C++17.
- The **GCC_INSTALL_PREFIX** CMake variable (which sets the default **--gcc-toolchain=**) is deprecated and will be removed. Specify the **--gcc-install-dir=** or **--gcc-triple=** option in a configuration file instead.
- The default extension name for precompiled headers (PCH) generation (**-c -xc-header** and **-c -xc++-header**) is now **.pch** instead of **.gch**.

- When **-include a.h** probes the **a.h.gch** file, the include now ignores **a.h.gch** if it is not a Clang PCH file or a directory containing any Clang PCH file.
- A bug that caused **__has_cpp_attribute** and **__has_c_attribute** to return incorrect values for certain C++-11-style attributes has been fixed.
- A bug in finding a matching **operator!=** while adding a reversed **operator==** has been fixed.
- The name mangling rules for function templates have been changed to accept that functions can be overloaded on their template parameter lists or requires-clauses.
- The **-Wenum-constexpr-conversion** warning is now enabled by default on system headers and macros. It will be turned into a hard (non-downgradable) error in the next Clang release.
- A path to the imported modules for C++20 named modules can no longer be hard-coded. You must specify all the dependent modules from the command line.
- It is no longer possible to import modules by using **import <module>**; Clang uses explicitly-built modules.
- For more details, see the list of potentially breaking changes.

For more information, see the LLVM release notes and Clang release notes.

LLVM Toolset is a rolling Application Stream, and only the latest version is supported. For more information, see the Red Hat Enterprise Linux Application Streams Life Cycle document.

Jira:RHEL-28687

Rust Toolset rebased to version 1.79.0

Rust Toolset has been updated to version 1.79.0. Notable enhancements since the previously available version 1.75.0 include:

- A new **offset_of!** macro
- Support for C-string literals
- Support for inline **const** expressions
- Support for bounds in associated type position
- Improved automatic temporary lifetime extension
- Debug assertions for **unsafe** preconditions

Rust Toolset is a rolling Application Stream, and only the latest version is supported. For more information, see the Red Hat Enterprise Linux Application Streams Life Cycle document.

Jira:RHEL-30070

Go Toolset rebased to version 1.23

Go Toolset has been updated to version 1.23 with the release of the RHSA-2025:3773 advisory.

Notable enhancements include:

- The **for-range** loop accepts iterator functions of the following types:

    - **func(func() bool)**
    - **func(func(K) bool)**
    - **func(func(K, V) bool)**
      Calls of the iterator argument function create the iteration values for the **for-range** loop. For reference links, see the upstream release notes.

- The Go Toolchain can collect usage and breakage statistics to help the Go team to understand how the Go Toolchain is used and working. By default, Go Telemetry does not upload telemetry data and stores it only locally. For further information, see the upstream Go Telemetry documentation.
- The **go vet** sub-command includes the **stdversion** analyzer which flags references to symbols that are too new for the version of Go you use in the referring file.
- The **cmd** and **cgo** features support the **-ldflags** option to pass flags to the C linker. The **go** command uses this flag automatically to avoid **argument list too long** errors when you use a very large **CGO_LDFLAGS** environment variable.
- The **trace** utility tolerates partially broken traces and attempts to recover the trace data. This is especially useful in case of crashes, because you can get the trace leading up to the crash.
- The traceback printed by the runtime after an unhandled panic or other fatal error carries indentation to distinguish the stack trace of the **goroutine** from the first **goroutine**.
- The compiler build time overhead of using profile-guided optimization was reduced to single-digit percentage.
- The new **-bindnow** linker flag enables immediate function binding when building a dynamically-linked ELF binary.
- The //**go:linkname** linker directive no longer refer to internal symbols in the standard library and the runtime that are not marked with //**go:linkname** on their definition.
- If a program no longer refers to a **Timer** or **Ticker**, garbage collection cleans them up immediately even if their **Stop** method has not been called. The timer channel associated with a **Timer** or **Ticker** is now unbuffered with capacity 0. This ensures that, every time a **Reset** or **Stop** method is called, no stale values are not sent or received after the call.
- The new **unique** package provides facilities for canonicalizing values, such as **interning** or **hash-consing**.
- The new **iter** package provides the basic definitions to work with user-defined iterators.
- The **slices** and **maps** packages introduce several new functions that work with iterators.
- The new **structs** package provides types for struct fields that modify properties of the containing struct type, such as memory layout.
- Minor changes are made in the following packages:
    - **archive/tar**
    - **crypto/tls**
    - **crypto/x509**

- **database/sql**
- **debug/elf**
- **encoding/binary**
- **go/ast**
- **go/types**
- **math/rand/v2**
- **net**
- **net/http**
- **net/http/httptest**
- **net/netips**
- **path/filepath**
- **reflect**
- **runtime/debug**
- **runtime/pprof**
- **runtime/trace**
- **slices**
- **sync**
- **sync/atomic**
- **syscall**
- **testing/fstest**
- **text/template**
- **time**
- **unicode/utf16**

For more information, see the upstream release notes.

Go Toolset is a rolling Application Stream, and Red Hat supports only the latest version. For more information, see the Red Hat Enterprise Linux Application Streams Life Cycle document.

Jira:RHEL-83437[1]

Go Toolset rebased to version 1.22

Go Toolset has been updated to version 1.22.

Notable enhancements include:

- Variables in for loops are now created per iteration, preventing accidental sharing bugs. Additionally, for loops can now range over integers.
- Commands in workspaces can now use a vendor directory for the dependencies of the workspace.
- The **go get** command no longer supports the legacy **GOPATH** mode. This change does not affect the **go build** and **go test** commands.
- The **vet** tool has been updated to match the new behavior of the for loops.
- CPU performance has been improved by keeping type-based garbage collection metadata nearer to each heap object.
- Go now provides improved inlining optimizations and better profile-guided optimization support for higher performance.
- A new **math/rand/v2** package is available.
- Go now provides enhanced HTTP routing patterns with support for methods and wildcards.

For more information, see the Go upstream release notes.

Go Toolset is a rolling Application Stream, and only the latest version is supported. For more information, see the Red Hat Enterprise Linux Application Streams Life Cycle document.

Jira:RHEL-29527[1]

PCP rebased to version 6.2.2

Performance Co-Pilot (PCP) has been updated to version 6.2.2. Notable changes over the previously available version 6.2.0 include:

New tools and agents

- **pcp2openmetrics**: a new tool to push PCP metrics in Open Metrics format to remote end points
- **pcp-geolocate**: a new tool to report latitude and longitude metric labels
- **pmcheck**: a new tool to interrogate and control PCP components
- **pmdauwsgi**: a new PCP agent that exports instrumentation from uWSGI servers

Enhanced tools

- **pmdalinux**: added new kernel metrics (hugepages, filesystems, TCP, softnet, virtual machine balloon)
- **pmdalibvirt**: added support for metric labels, added new balloon, vCPU, and domain info metrics
- **pmdabpf**: improved eBPF networking metrics for use with the **pcp-atop** utility

Jira:RHEL-30198

Grafana rebased to version 10.2.6

The **Grafana** platform has been updated to version 10.2.6.

Notable enhancements include:

- Support for zooming in on the y axis of time series and candlestick visualizations by holding shift while clicking and dragging.
- Streamlined data source selection when creating a dashboard.
- Updated User Interface, including updates to navigation and the command palette.
- Various improvements to transformations, including the new unary operation mode for the **Add field from calculation** transformation.
- Various improvements to dashboards and data visualizations, including a redesigned empty dashboard and dashboard panel.
- New geomap and canvas panels.

Other changes:

- Various improvements to users, access, authentication, authorization, and security.
- Alerting improvements along with new alerting features.
- Public dashboards now available.

For a complete list of changes since the previously available **Grafana** version 9.2, see the upstream documentation.

Jira:RHEL-31246[1]

Red Hat build of OpenJDK 17 is now the default Java implementation in RHEL 9

The default RHEL 9 Java implementation is being changed from OpenJDK 11, which has reached its End Of Life (EOL), to OpenJDK 17. After this update, the **java-17-openjdk** packages, which provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit, will also provide the **java** and **java-devel** packages. For more information, see the OpenJDK documentation.

Existing packages in RHEL 9 that call **java**/**bin** or **java-openjdk**/**bin** directly will be immediately able to use OpenJDK 17.

Existing packages in RHEL 9 that require the **java** or **java-devel** packages directly, namely **tomcat** and **systemtap-runtime-java**, will pull the appropriate dependency automatically.

Ant, Maven, and packages that are using Java indirectly through the **javapackages-tools** package will be fully transitioned in an asynchronous update shortly after the general availability of RHEL 9.5.

If you need to install OpenJDK for the first time or if the default package is not installed through a dependency chain, use DNF:

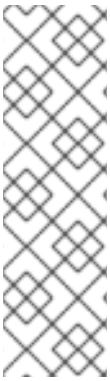
```
# dnf install java-17-openjdk-devel
```

For more information, see Installing multiple minor versions of Red Hat build of OpenJDK on RHEL by using yum.

IMPORTANT

The current **java-11-openjdk** packages in RHEL 9 will not receive any further updates. However, Red Hat will provide Extended Life Cycle support (ELS) phase 1 with updates for Red Hat build of OpenJDK 11 until October 31, 2027. See Red Hat build of OpenJDK 11 Extended Lifecycle Support (ELS-1) Availability for details.

For information specific to the OpenJDK ELS program and the OpenJDK lifecycle, see the OpenJDK Life Cycle and Support Policy .



NOTE

If you have the **alternatives** command set to **manual** mode for **java** and related components, OpenJDK 11 will still be used after the update. To use OpenJDK 17 in this case, change the **alternatives** setting to **auto**, for example:

```
# alternatives --auto java
# alternatives --auto javac
```

Use the **alternatives --list** command to verify the settings.

Jira:RHEL-56094[1]

4.13. IDENTITY MANAGEMENT

python-jwcrypto rebased to version 1.5.6

The **python-jwcrypto** package has been updated to version 1.5.6. This version includes a security fix to an issue where an attacker could cause a denial of service attack by passing in a malicious JWE Token with a high compression ratio.

Jira:RHELDOCS-18197[1]

ansible-freeipa rebased to 1.13.2

The **ansible-freeipa** package has been rebased from version 1.12.1 to 1.13.2. Notable enhancements include:

- You can create an inventory of Identity Management (IdM) servers for **ansible-freeipa** playbooks dynamically. The **freeipa** plugin gathers data about the IdM servers in the domain, and selects only those that have a specified IdM server role assigned. For example, if you want to search the logs of all IdM DNS servers in the domain to detect possible issues, the plugin ensures that all IdM replicas with the DNS server role are detected and automatically added to the managed nodes.
- The **ansible-freeipa** package requires the **ansible-core** package version 2.14 minimum. Both **ansible-core** 2.14 and the latest version of **ansible-freeipa** are available in the Appstream repository. For this reason, no manual update of **ansible-core** is required.
- You can more efficiently run **ansible-freeipa** playbooks that use a single Ansible task to add, modify, and delete multiple Identity Management (IdM) users, user groups, hosts, and services. Previously, each entry in a list of users had its dedicated API call. With this enhancement, several API calls are combined into one API call within a task. The same applies to lists of user groups, hosts and services.

As a result, the speed of adding, modifying, and deleting these IdM objects by using the **ipauser**, **ipagroup**, **ipahost** and **ipaservice** modules is increased. The biggest benefit can be seen when the client context is used.

- **ansible-freeipa** additionally provides the roles and modules as an Ansible collection in the **ansible-freeipa-collection** subpackage. To use the new collection:

  1. Install the **ansible-freeipa-collection** subpackage.

  2. Add the **freeipa.ansible_freeipa** prefix to the names of roles and modules. Use the fully-qualified names to follow Ansible recommendations. For example, to refer to the **ipahbacrule** module, use **freeipa.ansible_freeipa.ipahbacrule**.

  You can simplify the use of the modules that are part of the **freeipa.ansible_freeipa** collection by applying **module_defaults**.

Jira:RHEL-35565

ipa rebased to version 4.12.0

The **ipa** package has been updated from version 4.11 to 4.12.0. Notable changes include:

- You can enforce LDAP authentication to fail for a user that does not provide an OTP token.
- You can enroll an Identity Management (IdM) client using a trusted Active Directory user.
- Documentation for identity mapping in FreeIPA is now available.
- The **python-dns** package has been rebased to version 2.6.1-1.el10.
- The **ansible-freeipa** package has been rebased from version 1.12.1 to 1.13.2.

For more information, see the FreeIPA and ansible-freeipa upstream release notes.

Jira:RHEL-39140

certmonger rebased to version 0.79.20

The **certmonger** package has been rebased to version 0.79.20. The update includes various bug fixes and enhancements, most notably:

- Enhanced handling of new certificates in the internal token and improved the removal process on renewal.
- Removed restrictions on tokens for **CKM_RSA_X_509** cryptographic mechanism.
- Fixed the documentation for the **getcert add-scep-ca**, **--ca-cert**, and **--ra-cert** options.
- Renamed the D-Bus service and configuration files to match canonical name.
- Added missing **.TP** tags in the **getcert-resubmit** man page.
- Migrated to the SPDX license format.
- Included owner and permissions information in the **getcert list** output.
- Removed the requirement for an NSS database in the **cm_certread_n_parse** function.
- Added translations using Webplate for Simplified Chinese, Georgian, and Russian.

Jira:RHEL-12493

389-ds-base rebased to version 2.5.2

The **389-ds-base** package has been updated to version 2.5.2. Notable bug fixes and enhancements over version 2.4.5 include:

- https://www.port389.org/docs/389ds/releases/release-2-5-2.html

Jira:RHEL-31777

Improved MIT krb5 TCP connection timeout handling

Previously, TCP connections timed out after 10 seconds. With this update, MIT **krb5** TCP connection handling has been modified to no longer use a default timeout. The **request_timeout** setting now limits the total request duration rather than the duration of individual TCP connections. This change addresses integration issues with SSSD, especially for two-factor authentication use cases. As a result, users experience more consistent handling of TCP connections, as the **request_timeout** setting now effectively controls the global request maximum duration.

Jira:RHEL-17132[1]

4.14. SSSD

samba rebased to version 4.20.2

The **samba** packages have been upgraded to upstream version 4.20.2, which provides bug fixes and enhancements over the previous version. The most notable changes are:

- The **smbacls** utility can now save and restore discretionary access control list (DACL) entries. This feature mimics the functionality of the Windows **icacls.exe** utility.
- Samba now supports conditional access control entries (ACEs).
- Samba no longer reads currently logged on users from the **/var/run/utmp** file. This feature was removed from the **NetWkstaGetInfo** level 102 and **NetWkstaEnumUsers** level 0 and 1 functions because **/var/run/utmp** uses a time format that is not year 2038 safe.

Note that the server message block version 1 (SMB1) protocol has been deprecated since Samba 4.11 and will be removed in a future release.

Back up the database files before starting Samba. When the **smbd**, **nmbd**, or **winbind** services start, Samba automatically updates its **tdb** database files. Red Hat does not support downgrading **tdb** database files.

After updating Samba, use the **testparm** utility to verify the **/etc/samba/smb.conf** file.

Jira:RHEL-33645[1]

New SSSD option: failover_primary_timeout

You can use the **failover_primary_timeout** option to specify the time interval in seconds for the **sssd** service to attempt reconnecting to the primary IdM server after switching to a backup server. The default value is 31 seconds. Previously, if the primary server was unavailable, SSSD would automatically switch to a backup server after the fixed timeout of 31 seconds.

Jira:RHEL-17659[1]

4.15. DESKTOP

GNOME Online Accounts can restrict which features providers can use

You can use the new **goa.conf** file in the system configuration directory, usually named **/etc/goa.conf**, to limit what features each provider can use.

In the **goa.conf** file, the group name defines the provider type, and the keys define boolean switches to disable the individual features. If you do not set any key or section for a feature, the feature is enabled.

For example, to disable the mail feature for Google accounts, use the following setting:

```
[google]
mail=false
```

You can use the **all** special section name to cover every provider. The value in the specific provider has precedence, if it exists and contains a valid boolean value. Note that some combinations of disabled features can lead to incomplete or invalid accounts being read by the GOA users, such as the Evolution application. Always test the changes first. Restart the GNOME Online Accounts for the changed configuration to take effect.

Jira:RHEL-40831

4.16. THE WEB CONSOLE

New package: cockpit-files

The **cockpit-files** package provides the File manager page in the RHEL web console. With the File manager, you can perform the following actions:

- Browse files and directories on file systems you can access
- Sort files and directories by various criteria
- Filter displayed files by a sub-string
- Copy, move, delete, and rename files and directories
- Create directories
- Upload files
- Bookmark file paths
- Use keyboard shortcuts for the actions

Jira:RHELDOCS-16362[1]

4.17. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Support for new ha_cluster system role features

The **ha_cluster** system role now supports the following features:

- Configuring utilization attributes for node and primitive resources.

- Configuring node addresses and SBD options by using the **ha_cluster_node_options** variable. If both **ha_cluster_node_options** and **ha_cluster** variables are defined, their values are merged, with values from **ha_cluster_node_options** having precedence.
- Configuring access control lists (ACLs).
- Configuring Pacemaker alerts to take an external action when a cluster event such as node failure or resource starting or stopping occurs.
- Easy installation of agents for cloud environments by setting the **ha_cluster_install_cloud_agents** variable to **true**.

Jira:RHEL-30111, Jira:RHEL-17271, Jira:RHEL-27186, Jira:RHEL-33532

Support for configuring GFS2 file systems by using RHEL system roles

Red Hat Enterprise Linux 9.5 supports the configuration and management of the Red Hat Global File System 2 (GFS2) by using the **gfs2** RHEL system role. The role creates GFS2 file systems in a Pacemaker cluster managed with the **pcs** command-line interface.

Previously, setting up GFS2 file systems in a supported configuration required you to follow a long series of steps to configure the storage and cluster resources. The **gfs2** role simplifies the process. Using the role, you can specify only the minimum information needed to configure GFS2 file systems in a RHEL high availability cluster.

The gfs2 role performs the following tasks:

- Installing the packages necessary for configuring a GFS2 file system in a Red Hat high availability cluster
- Setting up the **dlm** and **lvmlockd** cluster resources
- Creating the LVM volume groups and logical volumes required by the GFS2 file system
- Creating the GFS2 file system and cluster resources with the necessary resource constraints

Jira:RHELDOCS-18629[1]

New sudo RHEL system role

sudo is a critical part of RHEL system configuration. With the new **sudo** RHEL system role, you can consistently manage sudo configuration at scale across your RHEL systems.

Jira:RHEL-37549

The storage RHEL system role can now manage Stratis pools

With this enhancement, you can use the **storage** RHEL system role to complete the following tasks:

- Create a new encrypted and unencrypted Stratis pool
- Add new volumes to the existing Stratis pool
- Add new disks to the Stratis pool

For details on how to manage Stratis pools and other related information, see the resources in the **/usr/share/doc/rhel-system-roles/storage/** directory.

Jira:RHEL-31854

New variables in the journald RHEL system role: journald_rate_limit_interval_sec and journald_rate_limit_burst

The following two variables have been added to the **journald** RHEL system role:

- **journald_rate_limit_interval_sec** (integer, defaults to 30): Configures a time interval in seconds, within which only the **journald_rate_limit_burst** log messages are handled. The **journald_rate_limit_interval_sec** variable corresponds to the **RateLimitIntervalSec** setting in the **journald.conf** file.

- **journald_rate_limit_burst** (integer, defaults to 10 000): Configures the upper limit of log messages, which are handled within the time defined by **journald_rate_limit_interval_sec**. The **journald_rate_limit_burst** variable corresponds to the **RateLimitBurst** setting in the **journald.conf** file.

As a result, you can use these settings to tune the performance of the **journald** service to handle applications that log many messages in a short period of time.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/journald/** directory.

Jira:RHEL-30170

New variables in the podman RHEL system role: podman_registry_username and podman_registry_password

The **podman** RHEL system role now enables you to specify the container image registry credentials either globally or on a per-specification basis. For that purpose, you must configure both role variables:

- **podman_registry_username** (string, defaults to unset): Configures the username for authentication with the container image registry. You must also set the **podman_registry_password** variable. You can override **podman_registry_username** on a per-specification basis with the **registry_username** variable. Each operation involving credentials would then be performed according to the detailed rules and protocols defined in that specification.

- **podman_registry_password** (string, defaults to unset): Configures the password for authentication with the container image registry. You must also set the **podman_registry_username** variable. You can override **podman_registry_password** on a per-specification basis with the **registry_password** variable. Each operation involving credentials would then be performed according to the detailed rules and protocols defined in that specification. For security, encrypt the password using the Ansible Vault feature.

As a result, you can use the **podman** RHEL system role to manage containers with images, whose registries require authentication for access.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/podman/** directory.

Jira:RHEL-30185

New variable in the postfix RHEL system role: postfix_files

The **postfix** RHEL system role now enables you to configure extra files for the Postfix mail transfer agent. For that purpose, you can use the following role variable:

postfix_files

Defines a list of files to be placed in the **/etc/postfix/** directory that can be converted into Postfix Lookup Tables if needed. This variable enables you to configure Simple Authentication and Security Layer (SASL) credentials, and similar. For security, encrypt files that contain credentials and other secrets using the Ansible Vault feature.

As a result, you can use the **postfix** RHEL system role to create these extra files and integrate them in your Postfix configuration.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/postfix/** directory.

Jira:RHEL-46854

The snapshot RHEL system role now supports managing snapshots of LVM thin pools

With thin provisioning, you can use the **snapshot** RHEL system role to manage snapshots of LVM thin pools. These thin snapshots are space-efficient and only grow as data is written or modified after the snapshot is taken. The role automatically detects if the specified volume is scheduled for a thin pool. The added feature could be useful in environments where you need to take frequent snapshots without consuming much physical storage.

Jira:RHEL-48227

New option in the logging RHEL system role: reopen_on_truncate

The **files** input type of the **logging_inputs** variable now supports the following option:

reopen_on_truncate (boolean, defaults to false)

Configures the **rsyslog** service to re-open the input log file if it was truncated, such as during log rotation. The **reopen_on_truncate** role option corresponds to the **reopenOnTruncate** parameter for **rsyslog**.

As a result, you can configure **rsyslog** in an automated fashion through the **logging** RHEL system role to re-open an input log file if it was truncated.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/logging/** directory.

Jira:RHEL-46590[1]

New variable in the logging RHEL system role: logging_custom_config_files

You can provide custom logging configuration files by using the following variable for the **logging** RHEL system role:

logging_custom_config_files (list)

Configures a list of configuration files to copy to the default logging configuration directory. For example, for the **rsyslog** service it is the **/etc/rsyslog.d/** directory. This assumes the default logging configuration loads and processes the configuration files in that directory. The default **rsyslog** configuration has a directive such as **$IncludeConfig /etc/rsyslog.d/*.conf**.

As a result, you can use customized configurations not provided by the **logging** RHEL system role.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/logging/** directory.

Jira:RHEL-40273

The logging RHEL system role can set ownership and permissions for rsyslog files and directories

The **files** output type of the **logging_outputs** variable now supports the following options:

- **mode** (raw, defaults to null): Configures the **FileCreateMode** parameter associated with the **omfile** module in the **rsyslog** service.
- **owner** (string, defaults to null): Configures the **fileOwner** or **fileOwnerNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **fileOwnerNum**. Otherwise, it sets **fileOwner**.
- **group** (string, defaults to null): Configures the **fileGroup** or **fileGroupNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **fileGroupNum**. Otherwise, it sets **fileGroup**.
- **dir_mode** (defaults to null): Configures the **DirCreateMode** parameter associated with the **omfile** module in **rsyslog**.
- **dir_owner** (defaults to null): Configures the **dirOwner** or **dirOwnerNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **dirOwnerNum**. Otherwise, it sets **dirOwner**.
- **dir_group** (defaults to null): Configures the **dirGroup** or **dirGroupNum** parameter associated with the **omfile** module in **rsyslog**. If the value is an integer, it sets **dirGroupNum**. Otherwise, it sets **dirGroup**.

As a result, you can set ownership and permissions for files and directories created by **rsyslog**.

Note that the file or directory properties are the same as the corresponding variables in the Ansible **file** module.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/logging/** directory. Alternatively, review the output of the **ansible-doc file** command.

Jira:RHEL-34935[1]

Using the storage RHEL system role creates fingerprints on managed nodes

If not already present, **storage** creates a unique identifier (fingerprint) every time you run this role. The fingerprint has the form of the **# system_role:storage** string written to the **/etc/fstab** file on your managed nodes. As a result, you can track which nodes are managed by **storage**.

Jira:RHEL-30888

New variables in the podman RHEL system role: podman_registry_certificates and podman_validate_certs

The following two variables have been added to the **podman** RHEL system role:

- **podman_registry_certificates** (list of dictionary elements): Enables you to manage TLS certificates and keys used to connect to the specified container image registry.
- **podman_validate_certs** (boolean, defaults to null): Controls whether pulling images from container image registries will validate TLS certificates or not. The default null value means that it is used whatever the default configured by the **containers.podman.podman_image** module is. You can override the **podman_validate_certs** variable on a per-specification basis with the **validate_certs** variable.

As a result, you can use the **podman** RHEL system role to configure TLS settings for connecting to container image registries.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/podman/** directory. Alternatively, you can review the **containers-certs(5)** manual page.

Jira:RHEL-33547

New variable in the podman RHEL system role: podman_credential_files

Some operations need to pull container images from registries in an automated or unattended way and cannot use the **podman_registry_username** and **podman_registry_password** variables.

Therefore, the **podman** RHEL system role now accepts the **containers-auth.json** file to authenticate against container image registries. For that purpose, you can use the following role variable:

podman_credential_files (list of dictionary elements)

Each dictionary element in the list defines a file with user credentials for authentication to private container image registries. For security, encrypt these credentials using the Ansible Vault feature. You can specify file name, mode, owner, group of the file, and can specify the contents in different ways. See the role documentation for more details.

As a result, you can input container image registry credentials for automated and unattended operations.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/podman/** directory. Alternatively, you can review the **containers-auth.json(5)** and **containers-registries.conf(5)** manual pages.

Jira:RHEL-30183

The nbde_client RHEL system role now enables you to skip running certain configurations

With the **nbde_client** RHEL system role you can now disable the following mechanisms:

- Initial ramdisk
- NetworkManager flush module
- Dracut flush module

The **clevis-luks-askpass** utility unlocks some storage volumes late in the boot process after the NetworkManager service puts the operating system on the network. Therefore, no configuration changes to the mentioned mechanisms are necessary.

As a result, you can disable the mentioned configurations from being run to support advanced networking setups, or volume decryption to occur late in the boot process.

Jira:RHEL-45717

The ssh RHEL system role now recognizes the ObscureKeystrokeTiming and ChannelTimeout configuration options

The **ssh** RHEL system role has been updated to reflect addition of the following configuration options in the OpenSSH utility suite:

- **ObscureKeystrokeTiming** (yes|no|interval specifier, defaults to 20): Configures whether the **ssh** utility should obscure the inter-keystroke timings from passive observers of network traffic.

- **ChannelTimeout**: Configures whether and how quickly the **ssh** utility should close inactive channels.

When using the **ssh** RHEL system role, you can use the new options such as in this example play:

```
---
- name: Non-exclusive sshd configuration
  hosts: managed-node-01.example.com
  tasks:
    - name: Configure ssh to obscure keystroke timing and set 5m session timeout
      ansible.builtin.include_role:
        name: rhel-system-roles.ssh
      vars:
        ssh_ObscureKeystrokeTiming: "interval:80"
        ssh_ChannelTimeout: "session=5m"
```

Jira:RHEL-40180

The src parameter was added to the network RHEL system role

The **src** parameter to the **route** sub-option of the **ip** option for the **network_connections** variable has been added. This parameter specifies the source IP address for a route. Typically, it is useful for the multi-WAN connections. These setups ensure that a machine has multiple public IP addresses, and outbound traffic uses a specific IP address tied to a particular network interface. As a result, support for the **src** parameter provides better control over traffic routing by ensuring a more robust and flexible network configuration capability in the described scenarios.

For more details, see the resources in the **/usr/share/doc/rhel-system-roles/network/** directory.

Jira:RHEL-3252

The storage RHEL system role can now resize LVM physical volumes

If the size of a block device has changed and you use this device in an LVM, you can adjust the LVM physical volume as well. With this enhancement, you can use the **storage** RHEL system role to resize LVM physical volumes to match the size of the underlying block devices after you resized it. To enable automatic resizing, set **grow_to_fill: true** on the pool in your playbook.

Jira:RHEL-14862

4.18. VIRTUALIZATION

New features for 64-bit ARM hosts

The following virtualization features have now become fully supported on the 64-bit ARM architecture:

- 4 KiB memory page size virtual machines (VMs) on 4kiB memory page size hosts. Note that hosts and guests with different page sizes are still not supported. The only supported page size combinations are 4 KiB/4 KiB and 64 KiB/64 KiB.
- The **virtiofs** feature for sharing files between the host and the VM
- Guest error RAS recovery (Reliability, Availability, Serviceability)
- The **pvpanic** event logging device
- The **virtio-mem** feature for dynamic memory assignment

As a result, VMs hosted on RHEL 9 running on an 64-bit ARM system will be able to use these features.

Jira:RHEL-43234[1]

RHEL supports live migrating VMs with attached NVIDIA vGPUs

With this update, you can now live migrate a running virtual machine with attached vGPUs to another KVM host. Currently, this is only possible with NVIDIA GPUs.

This functionality is available only with certain NVIDIA Virtual GPU Software Driver versions. Refer to the relevant NVIDIA vGPU documentation for more details.

Jira:RHELDOCS-16572[1]

nbdkit rebased to version 1.38

The **nbdkit** package has been rebased to upstream version 1.38, which provides various bug fixes and enhancements. The most notable changes are the following:

- Block size advertising has been enhanced and a new read-only filter has been added.
- The Python and OCaml bindings support more features of the server API.
- Internal struct integrity checks have been added to make the server more robust.

For a complete list of changes, see the upstream release notes.

Jira:RHEL-31884

Adjustable packet loss prevention added for the NetKVM driver

This update adds the **MinRxBufferPercent** parameter for the NetKVM driver, which you can use to reduce the risk of received packet loss in Windows virtual machines. The default value of **MinRxBufferPercent** is 0, and setting a higher value, up to 100, improves the prevention of packet loss, but might increase CPU consumption during high network traffic.

Jira:RHEL-19627

4.19. RHEL IN CLOUD ENVIRONMENTS

OpenTelemetry Collector is available for RHEL on AWS

While running RHEL on Amazon Web Services (AWS), you can now use the OpenTelemetry (OTel) framework to collect and send telemetry data, for example, logs. You can maintain and debug the RHEL cloud instances by using the OTel framework. With this update, RHEL includes the OTel Collector service, which you can use to manage logs. The OTel Collector gathers, processes, transforms, and exports logs to and from various formats and external back ends.

You can also use the OTel Collector to aggregate the collected data and generate metrics useful for analytics services. For example, you can configure OTel Collector to send data to Amazon Web Services (AWS) CloudWatch, which enhances the scope and accuracy of data obtained by CloudWatch from RHEL instances.

For details, see Configuring the OpenTelemetry Collector for RHEL on public cloud platforms.

Jira:RHELDOCS-18125[1]

awscli2 is generally available for RHEL on AWS

With the **awscli2** utility, you can now use Amazon Web Services (AWS) APIs from a RHEL instance to deploy new infrastructure offerings, and manage existing deployments. Note that installing **awscli2** from a Red Hat Enterprise Linux repository ensures that **awscli2** is installed from a trusted source and receives automatic updates. As a result, you can gather information regarding cloud deployment services, manage infrastructure resources, and refer to built-in documentation provided with **awscli2**.

Jira:RHEL-14523[1]

Log collection on Azure is now disabled by default

Previously, the Windows Azure Linux Agent (WALA) in Microsoft Azure collected debugging logs on virtual machines (VMs) by default. However, these agent logs might contain confidential information. To improve data security, WALA is now disabled by default, and does not collect any data on the VM. To re-enable log collection, do the following:

1. Edit the **/etc/waagent.conf** file.
2. Set the **Logs.Collect** parameter value to **y**.

Jira:RHEL-7273[1]

4.20. SUPPORTABILITY

The --api-url option is now available

With the **--api-url** option you can call another API according to the requirements. For example, the API for an OCP cluster. Example: **sos collect --cluster-type=ocp --cluster-option ocp.api-url=_<API_URL> --alloptions**.

Jira:RHEL-24523

The new --skip-cleaning-files option is now available

The **--skip-cleaning-files** option for the **sos report** command allows you to skip cleaning selected files. The option supports globs and wildcards. Example: **sos report -o host --batch --clean --skip-cleaning-files 'hostname'**.

Jira:RHEL-30893[1]

The plugin option names now use only hyphens instead of underscores

To ensure consistency across **sos** global options, the plugin option names now use only hyphens instead of underscores For example, the networking plugin **namespace_pattern** option is now **namespace-pattern** and must be specified by using the **--plugin-option networking.namespace-pattern=<pattern>** syntax.

Jira:RHELDOCS-18655[1]

4.21. CONTAINERS

Image mode for RHEL now supports FIPS mode

With this enhancement, you can enable the FIPS mode when building a bootc image to configure the system to use only FIPS-approved modules. You can use **bootc-image-builder**, which requires enabling

the FIPS crypto policy in the Containerfile configuration, or use the RHEL Anaconda installation, that additionally to enabling FIPS mode in the Containerfile, also requires adding the **fips=1** kernel argument when booting the system installation. See Installing the system with FIPS mode enabled for more details.

The following is a Containerfile with instructions to enable the **fips=1** kernel argument:

```
FROM registry.redhat.io/rhel9/rhel-bootc:latest#
# Enable fips=1 kernel argument:
https://containers.github.io/bootc/building/kernel-arguments.html
COPY 01-fips.toml /usr/lib/bootc/kargs.d/
# Install and enable the FIPS crypto policy
RUN dnf install -y crypto-policies-scripts && update-crypto-policies --no-reload --set FIPS
```

Jira:RHELDOCS-18585[1]

Image mode for RHEL now supports logically bound app images

With this enhancement, you have support for container images that are lifecycle bound to the base bootc image. This helps unite different operational processes for applications and operating systems and the app images are referenced from the base image as image files or an equivalent. As a result, you can manage multiple container images for system installations, for example, for a disconnected installation, the system must all be mirrored, not just one.

Jira:RHELDOCS-18666[1]

Podman and Buildah support adding OCI artifacts to image indexes

With this update, you can create artifact manifests and add them to image indexes.

The **buildah manifest add** command now supports the following options:

- the **--artifact** option to create artifact manifests
- the **--artifact-type**, **--artifact-config-type**, **--artifact-layer-type**, **--artifact-exclude-titles**, and **--subject** options to adjust the contents of the artifact manifests it creates.

The **buildah manifest annotate** command now supports the following options:

- the **--index** option to set annotations on the index itself instead of a one of the entries in the image index
- the **--subject** option for setting the subject field of an image index.

The **buildah manifest create** command now supports the **--annotation** option to add annotations to the new image index.

Jira:RHEL-33572

Option is available to disable Podman health check event

This enhancement adds a new **healthcheck_events** option in the **containers.conf** configuration file under the **[engine]** section to disable the generation of **health_status** events. Set **healthcheck_events=false** to disable logging health check events.

Jira:RHEL-34603

Runtime resource changes in Podman are persistent

The updates of container configuration by using the **podman update** command are persistent. Note that this enhancement is for both SQLite and BoltDB database backends.

Jira:RHEL-33567

Building multi-architecture images is fully supported

The **podman farm build** command that creates multi-architecture container images s now fully supported.

A farm is a group of machines that have a UNIX Podman socket running in them. The nodes in the farm can have different machines of various architectures. The **podman farm build** command is faster than the **podman build --arch --platform** command.

You can use **podman farm build** to perform the following actions:

- Build an image on all nodes in a farm.
- Bundle an image on all nodes in a farm up into a manifest list.
- Run the **podman build** command on all the farm nodes.
- Push the images to the registry specified by using the **--tag** option.
- Locally create a manifest list.
- Push the manifest list to the registry.

The manifest list contains one image per native architecture type present in the farm.

Jira:RHEL-34609

Quadlets for pods in Podman are available

Beginning with Podman v5.0, you can use Quadlet to automatically generate a **systemd** service file from a pod description.

Jira:RHEL-33574

The Podman v2.0 RESTful API has been updated

The new fields has been added to the **libpod/images/json** endpoint:

- The **isManifest** boolean field to determine if the target is a manifest or not. The **libpod** endpoint returns both images and manifest lists.
- The **os** and **arch** fields for image listing.

Jira:RHEL-34612

Kubernetes YAML now supports a data volume container as an init container

A list of images to automatically mount as volumes can now be specified in Kubernetes YAML by using the **"io.podman.annotations.kube.image.automount/$ctrname"** annotation. Image-based mounts using **podman run --mount type=image,source=<image>,dst=<path>,subpath=<path>** now support a new option, **subpath**, to mount only part of the image into the container.

Jira:RHEL-34605

The Container Tools packages have been updated

The updated Container Tools RPM meta-package, which contains the Podman, Buildah, Skopeo, **crun**, and **runc** tools, is now available. Podman v5.0 contains the following notable bug fixes and enhancements over the previous version:

- The **podman manifest add** command now supports a new **--artifact** option to add OCI artifacts to a manifest list.
- The **podman create**, **podman run**, and **podman push** commands now support the **--retry** and **--retry-delay** options to configure retries for pushing and pulling images.
- The **podman run** and **podman exec** commands now support the **--preserve-fd** option to pass a list of file descriptors into the container. It is an alternative to **--preserve-fds**, which passes a specific number of file descriptors.
- Quadlet now supports templated units.
- The **podman kube play** command can now create image-based volumes by using the **volume.podman.io/image** annotation.
- Containers created with the **podman kube play** command can now include volumes from other containers by using a new annotation, **io.podman.annotations.volumes-from**.
- Pods created with the **podman kube play** command can now set user namespace options by using the **io.podman.annotations.userns annotation** in the pod definition.
- The **--gpus** option to **podman create** and **podman run** is now compatible with Nvidia GPUs.
- The **--mount** option to **podman create** and **podman run** supports a new mount option, **no-dereference**, to mount a symlink instead of its de-referenced target into a container.
- Podman now supports the new **--config** global option to point to a Docker configuration where registry login credentials can be sourced.
- The **podman ps --format** command now supports the new **.Label** format specifier.
- The **uidmapping** and **gidmapping** options to the **podman run --userns=auto** option can now map to host IDs by prefixing host IDs with the @ symbol.
- Quadlet now supports systemd-style drop-in directories.
- Quadlet now supports creating pods by using the new **.pod** unit files.
- Quadlet now supports two new keys, **Entrypoint** and **StopTimeout**, in **.container** files.
- Quadlet now supports specifying the **Ulimit** key multiple times in **.container** files to set more than one **ulimit** on a container.
- Quadlet now supports setting the **Notify** key to **healthy** in **.container** files, to only notify that a container has started when its health check begins passing.
- The output of the **podman inspect** command for containers has changed. The **Entrypoint** field changes from a string to an array of strings and **StopSignal** from an integer to a string.

- The **podman inspect** command for containers now returns nil for health checks when inspecting containers without health checks.
- It is no longer possible to create new BoltDB databases. Attempting to do so results in an error. All new Podman installations now use the SQLite database backend. Existing BoltDB databases remain usable.
- Support for CNI networking is gated by a build tag and is not enabled by default.
- Podman now prints warnings when used on **cgroups v1** systems. Support for **cgroups v1** is deprecated and will be removed in a future release. You can set the **PODMAN_IGNORE_CGROUPSV1_WARNING** environment variable to suppress warnings.
- Network statistics sent over the Docker-compatible API are now per-interface, and not aggregated, which improves Docker compatibility.
- The default tool for rootless networking has been changed from **slirp4netns** to **pasta** for improved performance. As a result, networks named **pasta** are no longer supported.
- Using multiple filters with the List Images REST API now combines the filters with AND instead of OR, improving Docker compatibility.
- The parsing for several Podman CLI options which accept arrays has been changed to no longer accept string-delimited lists, and instead to require the option to be passed multiple times. These options are:
    - The **--annotation** option to **podman manifest annotate** and **podman manifest add**
    - The **--configmap**, **--log-opt**, and **--annotation** options to **podman kube play**
- The **--pubkeysfile** option to **podman image trust set**
    - The **--encryption-key** and **--decryption-key** options to **podman create**, **podman run**, **podman push** and **podman pull**
    - The **--env-file** option to **podman exec**, the **--bkio-weight-device**, **--device-read-bps**, **--device-write-bps**, **--device-read-iops**, **--device-write-iops**, **--device**, **--label-file**, **--chrootdirs**, **--log-opt**, **--env-file** options to **podman create** and **podman run**
    - The **--hooks-dir** and **--module** global options
- The **podman system reset** command no longer waits for running containers to stop, and instead immediately sends the **SIGKILL** signal.
- The **podman network inspect** command now includes running containers that use the network in its output.
- The **podman compose** command is now supported on other architectures in addition to AMD and Intel 64-bit architectures (x86-64-v2) and the 64-bit ARM architecture (ARMv8.0-A)..
- The **--no-trunc** option to the **podman kube play** and **podman kube generate** commands has been deprecated. Podman now complies to the Kubernetes specification for annotation size, which removes the need for this option.
- Connections from the **podman system connection** command and farms from the **podman farm** command are now written to a new configuration file called **podman-connections.conf** file. As a result, Podman no longer writes to the **containers.conf** file. Podman still respects existing connections from **containers.conf**.

- Most **podman farm** subcommands no longer need to connect to the machines in the farm to run.
- The **podman create** and **podman run** commands no longer require specifying an entrypoint on the command line when the container image does not define one. In this case, an empty command is passed to the OCI runtime, and the resulting behavior is runtime-specific.
- A new API endpoint, **/libpod/images/$name/resolve**, has been added to resolve a potential short name to a list of fully-qualified image references Podman, which you can use to pull the image.

For more information about notable changes, see upstream release notes.

Jira:RHEL-32714

The --compat-volumes option is available for Podman and Buildah

You can use the new **--compat-volumes** option with the **buildah build**, **podman build**, and **podman farm build** commands. This option triggers special handling for the contents of directories marked using the **VOLUME** instruction such that their contents can subsequently only be modified by **ADD** and **COPY** instructions. Any changes made in those locations by **RUN** Instructions will be discarded. Previously, this behavior was the default, but it is now disabled by default.

Jira:RHEL-52239

A new rhel10-beta/rteval container image

The real-time **registry.redhat.io/rhel10-beta/rteval** container image is now available in the Red Hat Container Registry to run latency analysis on either a standalone RHEL installation. With **rhel10-beta/rteval** container image, you can perform latency testing within a containerized setup to determine if such a solution is viable for your real-time workloads or to compare results against a bare metal run of **rteval**. To use this feature, subscribe to RHEL with real-time support. No tuning guidelines are provided.

Jira:RHELDOCS-18522[1]

The containers.conf file is now read-only

The system connections and farm information stored in the **containers.conf** file is 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.

You can still manually edit the **containers.conf** file if needed. System connections that were added by Podman v4.0 remain unchanged after the upgrade to Podman v5.0.

Jira:RHEL-40637

macvlan and ipvlan network interface names are configurable in containers.conf

To specify **macvlan** and **ipvlan** networks, you can adjust the name of the network interface created inside containers by using the new **interface_name** field in the **containers.conf** configuration file.

Jira:RHELDOCS-18769[1]

bootc-image-builder now supports defining and injecting custom Kickstart files to ISO builds

With this enhancement, now you can define a Kickstart by setting users, customize partitioning, inject key, and inject the Kickstart file to an ISO build to configure the installation process. The resulting disk image creates a self-contained installer that automates and deploys devices, disconnected systems, edge devices, between others. As a result, it is much easier to create customized media with **bootc-image-builder**.

Jira:RHELDOCS-18734[1]

Support to building GCP images by using bootc-image-builder

By using the **bootc-image-builder** tool you can now generate **.gce** disk images and provision the instances on the Google Compute Engine (GCE) platform.

Jira:RHELDOCS-18472[1]

Support to creating and deploying VMDK with bootc-image-builder

With this enhancement, now you can create a Virtual Machine Disk (VMDK) from a bootc image, by using the **bootc-image-builder** tool, and deploy VMDK images to VMware vSphere.

Jira:RHELDOCS-18398[1]

The podman pod inspect command now provides a JSON array regardless of the number of pods

Previously, the **podman pod inspect** command omitted the JSON array when inspecting a single pod. With this update, the **podman pod inspect** command now produces a JSON array in the output regardless of the number of pods inspected.

Jira:RHELDOCS-18770[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 9.5. 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

numa_cma=<node>:nn[MG][,<node>:nn[MG]]

[KNL,CMA]

Sets the size of kernel numa memory area for contiguous memory allocations. It will reserve CMA area for the specified node.

With numa CMA enabled, DMA users on node nid will first try to allocate buffer from the numa area which is located in node nid, if the allocation fails, they will fallback to the global default memory area.

reg_file_data_sampling=

[x86]

Controls mitigation for Register File Data Sampling (RFDS) vulnerability. RFDS is a CPU vulnerability which might allow userspace to infer kernel data values previously stored in floating point registers, vector registers, or integer registers. RFDS only affects Intel Atom processors.

Values:

- **on** :: Turns ON the mitigation
- **off** :: Turns OFF the mitigation

This parameter overrides the compile time default set by CONFIG_MITIGATION_RFDS. Mitigation cannot be disabled when other VERW based mitigations (such as MDS) are enabled. To disable RFDS mitigation all VERW based mitigations need to be disabled.

For details see: **Documentation/admin-guide/hw-vuln/reg-file-data-sampling.rst**

locktorture.acq_writer_lim=

[KNL]

Set the time limit in jiffies for a lock acquisition. Acquisitions exceeding this limit will result in a splat once they do complete.

locktorture.bind_readers=

[KNL]

Specify the list of CPUs to which the readers are to be bound.

locktorture.bind_writers=

[KNL]

Specify the list of CPUs to which the writers are to be bound.

locktorture.call_rcu_chains=

[KNL]

Specify the number of self-propagating **call_rcu()** chains to set up. These are used to ensure that there is a high probability of an RCU grace period in progress at any given time. Defaults to 0, which disables these **call_rcu()** chains.

locktorture.long_hold=

[KNL]

Specify the duration in milliseconds for the occasional long-duration lock hold time. Defaults to 100 milliseconds. Select **0** to disable.

locktorture.nested_locks=

[KNL]

Specify the maximum lock nesting depth that locktorture is to exercise, up to a limit of **8** (MAX_NESTED_LOCKS). Specify **zero** to disable. Note that this parameter is ineffective on types of locks that do not support nested acquisition.

workqueue.default_affinity_scope=

Select the default affinity scope to use for unbound work queues. Can be one of "cpu", "smt", "cache", "numa" and "system". Default is "cache". For more information, see the Affinity Scopes section in **Documentation/core-api/workqueue.rst**.

This can be changed after boot by writing to the matching **/sys/module/workqueue/parameters** file. All work queues with the "default" affinity scope will be updated accordingly.

locktorture.rt_boost=

[KNL]

Do periodic testing of real-time lock priority boosting. Select **0** to disable, **1** to boost only rt_mutex, and **2** to boost unconditionally. Defaults to **2**, which might seem to be an odd choice, but which should be harmless for non-real-time spinlocks, due to their disabling of preemption. Note that non-realtime mutexes disable boosting.

locktorture.writer_fifo=

[KNL]

Run the write-side locktorture kthreads at **sched_set_fifo()** real-time priority.

locktorture.rt_boost_factor=

[KNL]

Number that determines how often and for how long priority boosting is exercised. This is scaled down by the number of writers, so that the number of boosts per unit time remains roughly constant as the number of writers increases. However, the duration of each boost increases with the number of writers.

microcode.force_minrev=

[X86]

Format: <bool>

Enable or disable the microcode minimal revision enforcement for the runtime microcode loader.

module.async_probe=<bool>

[KNL]

When set to true, modules will use async probing by default. To enable or disable async probing for a specific module, use the module specific control that is documented under **<module>.async_probe**. When both **module.async_probe** and **<module>.async_probe** are specified, **<module>.async_probe** takes precedence for the specific module.

module.enable_dups_trace

[KNL]

When **CONFIG_MODULE_DEBUG_AUTOLOAD_DUPS** is set, this means that duplicate **request_module()** calls will trigger a **WARN_ON()** instead of a **pr_warn()**. Note that if **MODULE_DEBUG_AUTOLOAD_DUPS_TRACE** is set, **WARN_ON()** will always be issued and this option does nothing.

nfs.delay_retrans=

[NFS]

Specifies the number of times the NFSv4 client retries the request before returning an EAGAIN error, after a reply of NFS4ERR_DELAY from the server. Only applies if the softerr mount option is enabled, and the specified value is **>= 0**.

rcutree.do_rcu_barrier=

[KNL]

Request a call to **rcu_barrier()**. This is throttled so that userspace tests can safely hammer on the sysfs variable if they so choose. If triggered before the RCU grace-period machinery is fully active, this will error out with EAGAIN.

rcuscale.minruntime=

[KNL]

Set the minimum test run time in seconds. This does not affect the data-collection interval, but instead allows better measurement of things such as CPU consumption.

rcuscale.writer_holdoff_jiffies=

[KNL]

Additional write-side holdoff between grace periods, but in jiffies. The default of zero says no holdoff.

rcupdate.rcu_cpu_stall_notifiers=

[KNL]

Provide RCU CPU stall notifiers, but see the warnings in the RCU_CPU_STALL_NOTIFIER Kconfig option's help text. TL;DR: You almost certainly do not want rcupdate.rcu_cpu_stall_notifiers.

rcupdate.rcu_task_lazy_lim=

[KNL]

Number of callbacks on a given CPU that will cancel laziness on that CPU. Use **-1** to disable cancellation of laziness, but be advised that doing so increases the danger of OOM due to callback flooding.

rcupdate.rcu_tasks_lazy_ms= ++

[KNL]

Set timeout in milliseconds RCU Tasks asynchronous callback batching for **call_rcu_tasks()**. A negative value will take the default. A value of zero will disable batching. Batching is always disabled for **synchronize_rcu_tasks()**.

rcupdate.rcu_tasks_rude_lazy_ms=

[KNL]

Set timeout in milliseconds RCU Tasks Rude asynchronous callback batching for **call_rcu_tasks_rude()**. A negative value will take the default. A value of zero will disable batching. Batching is always disabled for **synchronize_rcu_tasks_rude()**.

rcupdate.rcu_tasks_trace_lazy_ms=

[KNL]

Set timeout in milliseconds RCU Tasks Trace asynchronous callback batching for call_rcu_tasks_trace(). A negative value will take the default. A value of zero will disable batching. Batching is always disabled for synchronize_rcu_tasks_trace().

spectre_bhi=

[X86]

Control mitigation of Branch History Injection (BHI) vulnerability. This setting affects the deployment of the HW BHI control and the SW BHB clearing sequence.

Values:

on

(default) Enable the HW or SW mitigation as needed.

off

Disable the mitigation.

unwind_debug

[X86-64]

Enable unwinder debug output. This can be useful for debugging certain unwinder error conditions, including corrupt stacks and bad or missing unwinder metadata.

workqueue.cpu_intensive_thresh_us=

Per-cpu work items which run for longer than this threshold are automatically considered CPU intensive and excluded from concurrency management to prevent them from noticeably delaying other per-cpu work items. Default is **10000** (10ms).

If **CONFIG_WQ_CPU_INTENSIVE_REPORT** is set, the kernel will report the work functions which violate this threshold repeatedly. They are likely good candidates for using WQ_UNBOUND work queues instead.

workqueue.cpu_intensive_warning_thresh=<uint> If **CONFIG_WQ_CPU_INTENSIVE_REPORT** is set, the kernel will report the work functions which violate the **intensive_threshold_us** repeatedly. To prevent spurious warnings, start printing only after a work function has violated this threshold number of times.

The default is 4 times. **0** disables the warning.

workqueue.default_affinity_scope=

Select the default affinity scope to use for unbound work queues. Can be one of "cpu", "smt", "cache", "numa" and "system". Default is "cache". For more information, see the Affinity Scopes section in Documentation/core-api/workqueue.rst.

This can be changed after boot by writing to the matching **/sys/module/workqueue/parameters** file. All work queues with the "default" affinity scope will be updated accordingly.

xen_msr_safe=

[X86,XEN]

Format: <bool>

Select whether to always use non-faulting (safe) MSR access functions when running as Xen PV guest. The default value is controlled by **CONFIG_XEN_PV_MSR_SAFE**.

Updated kernel parameters

clearcpuid=

X[,X...] [X86]

Disable CPUID feature X for the kernel. See numbers X.

Note the Linux-specific bits are not necessarily stable over kernel options, but the vendor-specific ones should be. X can also be a string as appearing in the flags: line in /proc/cpuinfo which does not have the above instability issue. However, not all features have names in /proc/cpuinfo. Note that using this option will taint your kernel.

Also note that user programs calling CPUID directly or using the feature without checking anything will still see it. This just prevents it from being used by the kernel or shown in **/proc/cpuinfo**. Also note the kernel might malfunction if you disable some critical bits.

cma_pernuma=nn[MG]

[KNL,CMA]

Sets the size of kernel per-numa memory area for contiguous memory allocations. A value of **0** disables per-numa CMA altogether. And If this option is not specified, the default value is **0**. With per-numa CMA enabled, DMA users on node nid will first try to allocate buffer from the pernuma area which is located in node nid, if the allocation fails, they will fallback to the global default memory area.

csdlock_debug=

[KNL]

Enable debug add-ons of cross-CPU function call handling. When switched on, additional debug data is printed to the console in case a hanging CPU is detected, and that CPU is pinged again to try to resolve the hang situation. **The default value of this option depends on the CSD_LOCK_WAIT_DEBUG_DEFAULT Kconfig option.**

<module>.async_probe[=<bool>]

[KNL]

If no <bool> value is specified or if the value specified is not a valid <bool>, enable asynchronous probe on this module. Otherwise, enable or disable asynchronous probe on this module as indicated by the <bool> value. See also: module.async_probe

earlycon=

[KNL]

Output early console device and options.

When used with no options, the early console is determined by stdout-path property in device tree's chosen node or the ACPI SPCR table if supported by the platform.

cdns,<addr>[,options] Start an early, polled-mode console on a Cadence (xuartps) serial port at the specified address. Only supported option is baud rate. If baud rate is not specified, the serial port must already be setup and configured.

uart[8250],io,<addr>[,options[,uartclk]]uart[8250],mmio,<addr>[,options[,uartclk]]uart[8250],mmio32,<addr>[,options[,uartclk]]uart[8250],mmio32be,<addr>[,options[,uartclk]]uart[8250],0x<addr>[,options]

Start an early, polled-mode console on the 8250/16550 UART at the specified I/O port or MMIO address. MMIO inter-register address stride is either 8-bit (mmio) or 32-bit (mmio32 or mmio32be). If none of [io|mmio|mmio32|mmio32be], **<addr>** is assumed to be equivalent to 'mmio'. 'options' are specified in the same format described for "console=ttyS<n>"; **if unspecified, the h/w is not initialized. 'uartclk' is the uart clock frequency; if unspecified, it is set to 'BASE_BAUD' * 16.**

earlyprintk=

[X86,SH,ARM,M68k,S390]

earlyprintk=vga earlyprintk=sclp earlyprintk=xen earlyprintk=serial[,ttySn[,baudrate]] earlyprintk=serial[,0x...[,baudrate]] earlyprintk=ttySn[,baudrate] earlyprintk=dbgp[debugController#] earlyprintk=pciserial[,force],bus:device.function[,baudrate] earlyprintk=xdbc[xhciController#]

earlyprintk is useful when the kernel crashes before the normal console is initialized. It is not enabled by default because it has some cosmetic problems.

Append ",keep" to not disable it when the real console takes over.

Only one of vga, efi, serial, or USB debug port can be used at a time.

Currently only ttyS0 and ttyS1 might be specified by name. Other I/O ports might be explicitly specified on some architectures (x86 and arm at least) by replacing ttySn with an I/O port address, such as: earlyprintk=serial,0x1008,115200 You can find the port for a given device in /proc/tty/driver/serial: 2: uart:ST16650V2 port:00001008 irq:18.

Interaction with the standard serial driver is not very good.

The VGA and EFI output is eventually overwritten by the real console.

The xen option can only be used in Xen domains.

The sclp output can only be used on s390.

The optional "force" to "pciserial" enables use of a PCI device even when its classcode is not of the UART class.

iommu.strict=

[ARM64, X86, S390]

Configure TLB invalidation behaviour.

Format: { "0" | "1" }

0 - Lazy mode

Request that DMA unmap operations use deferred invalidation of hardware TLBs, for increased throughput at the cost of reduced device isolation. Will fall back to strict mode if not supported by the relevant IOMMU driver.

1 - Strict mode

DMA unmap operations invalidate IOMMU hardware TLBs synchronously.

unset

Use value of CONFIG_IOMMU_DEFAULT_DMA_{LAZY,STRICT}.

NOTE

On x86, strict mode specified via one of the legacy driver-specific options takes precedence.

mem_encrypt=

[x86_64]

AMD Secure Memory Encryption (SME) control.

Valid arguments: on, off

Default: off

mem_encrypt=on: Activate SME mem_encrypt=off: Do not activate SME

mitigations=

[X86,PPC,S390,ARM64]

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

Value: off

Disable all optional CPU mitigations. This improves system performance, but it might also expose users to several CPU vulnerabilities. Equivalent to: if nokaslr then kpti=0 [ARM64] gather_data_sampling=off [X86] kvm.nx_huge_pages=off [X86] l1tf=off [X86] mds=off [X86] mmio_stale_data=off [X86] no_entry_flush [PPC] no_uaccess_flush [PPC] nobp=0 [S390] nopti [X86,PPC] nospectre_bhb [ARM64] nospectre_v1 [X86,PPC] nospectre_v2 [X86,PPC,S390,ARM64] **reg_file_data_sampling=off [X86]** retbleed=off [X86] **spec_rstack_overflow=off [X86]** spec_store_bypass_disable=off [X86,PPC] **spectre_bhi=off [X86]** spectre_v2_user=off [X86] srbds=off [X86,INTEL] ssbd=force-off [ARM64] tsx_async_abort=off [X86]

nosmap

[PPC]

Disable SMAP (Supervisor Mode Access Prevention) even if it is supported by processor.

nosmep

[PPC64s]

Disable SMEP (Supervisor Mode Execution Prevention) even if it is supported by processor.

nox2apic

[x86_64,APIC]

Do not enable x2APIC mode.

NOTE

This parameter will be ignored on systems with the **LEGACY_XAPIC_DISABLED** bit set in the **IA32_XAPIC_DISABLE_STATUS MSR**.

panic_print=

Bitmask for printing system info when panic happens. User can chose combination of the following bits:

- bit 0: print all tasks info
- bit 1: print system memory info
- bit 2: print timer info
- bit 3: print locks info if CONFIG_LOCKDEP is on
- bit 4: print ftrace buffer
- bit 5: print all printk messages in buffer
- **bit 6: print all CPUs backtrace (if available in the arch)**

IMPORTANT

This option might print a *lot* of lines, so there are risks of losing older messages in the log. Use this option carefully, you might consider setting up a bigger log buffer with "log_buf_len" along with this.

pcie_aspm=

[PCIE]

Forcibly enable or ignore PCIe Active State Power Management.

Value:

off

Do not touch ASPM configuration at all. Leave any configuration done by firmware unchanged.

force

Enable ASPM even on devices that claim not to support it.

WARNING

Forcing ASPM on might cause system lockups.

s390_iommu=

[HW,S390]

Set s390 IOTLB flushing mode.

Value:

strict

with strict flushing every unmap operation will result in an IOTLB flush.

Default

is lazy flushing before reuse, which is faster.

Deprecated

equivalent to iommu.strict=1.

spectre_v2=

[x86]

Control mitigation of Spectre variant 2 (indirect branch speculation) vulnerability. The default operation protects the kernel from user space attacks.

Value:

on

unconditionally enable, implies spectre_v2_user=on.

off

unconditionally disable, implies spectre_v2_user=off.

auto

kernel detects whether your CPU model is vulnerable.

Selecting 'on' will, and 'auto' might, choose a mitigation method at run time according to the CPU, the available microcode, **the setting of theCONFIG_MITIGATION_RETPOLINE configuration option, and the compiler with which the kernel was built.**

usbcore.quirks=

[USB]

A list of quirk entries to augment the built-in USB core quirk list. List entries are separated by commas. Each entry has the form **VendorID:ProductID:Flags**. The IDs are 4-digit hex numbers and Flags is a set of letters. Each letter will change the built-in quirk; setting it if it is clear and clearing it if it is set. The

letters have the following meanings:

- a = USB_QUIRK_STRING_FETCH_255 (string descriptors must not be fetched by using a 255-byte read);
- b = USB_QUIRK_RESET_RESUME (device cannot resume correctly so reset it instead);
- c = USB_QUIRK_NO_SET_INTF (device cannot handle Set-Interface requests);
- d = USB_QUIRK_CONFIG_INTF_STRINGS (device cannot handle its Configuration or Interface strings);
- e = USB_QUIRK_RESET (device cannot be reset (e.g morph devices), do not use reset);
- f = USB_QUIRK_HONOR_BNUMINTERFACES (device has more interface descriptions than the **bNumInterfaces** count, and cannot handle talking to these interfaces);
- g = USB_QUIRK_DELAY_INIT (device needs a pause during initialization, after we read the device descriptor);
- h = USB_QUIRK_LINEAR_UFRAME_INTR_BINTERVAL (For high speed and super speed interrupt endpoints, the USB 2.0 and USB 3.0 spec require the interval in microframes (1 microframe = 125 microseconds) to be calculated as interval = 2 ^ (bInterval-1). Devices with this quirk report their bInterval as the result of this calculation instead of the exponent variable used in the calculation);
- i = USB_QUIRK_DEVICE_QUALIFIER (device cannot handle device_qualifier descriptor requests);
- j = USB_QUIRK_IGNORE_REMOTE_WAKEUP (device generates spurious wakeup, ignore remote wakeup capability);
- k = USB_QUIRK_NO_LPM (device cannot handle Link Power Management);
- l = USB_QUIRK_LINEAR_FRAME_INTR_BINTERVAL (Device reports its bInterval as linear frames instead of the USB 2.0 calculation);
- m = USB_QUIRK_DISCONNECT_SUSPEND (Device needs to be disconnected before suspend to prevent spurious wakeup);
- n = USB_QUIRK_DELAY_CTRL_MSG (Device needs a pause after every control message);
- o = USB_QUIRK_HUB_SLOW_RESET (Hub needs extra delay after resetting its port);
- **p = USB_QUIRK_SHORT_SET_ADDRESS_REQ_TIMEOUT (Reduce timeout of the SET_ADDRESS request from 5000 ms to 500 ms);**

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

Removed kernel parameters

- [BUGS=X86] **noclflush**:: Do not use the CLFLUSH instruction.
- **Workqueue.disable_numa**
- [X86] **noexec**
- [BUGS=X86-32] **nosep**:: Disables x86 SYSENTER/SYSEXIT support.

- [X86] **nordrand**:: Disable kernel use of the RDRAND.
- **thermal.nocrt**

New sysctl parameters

oops_limit

Number of kernel oopses after which the kernel should panic when **panic_on_oops** is not set. Setting this to **0** disables checking the count. Setting this to **1** has the same effect as setting **panic_on_oops=1**. The default value is **10000**.

warn_limit

Number of kernel warnings after which the kernel should panic when **panic_on_warn** is not set. Setting this to **0** disables checking the warning count. Setting this to **1** has the same effect as setting **panic_on_warn=1**. The default value is **0**.

kexec_load_limit_panic

This parameter specifies a limit to the number of times the syscalls **kexec_load** and **kexec_file_load** can be called with a crash image. It can only be set with a more restrictive value than the current one.

Value:

-1
: Unlimited calls to kexec. This is the default setting.

N
: Number of calls left.

kexec_load_limit_reboot

Similar functionality as **kexec_load_limit_panic**, but for a normal image.

numa_balancing_promote_rate_limit_MBps

Too high promotion or demotion throughput between different memory types might hurt application latency. You can use this parameter to rate-limit the promotion throughput. The per-node maximum promotion throughput in MB/s is limited to be no more than the set value.

Set this parameter to less than 1/10 of the PMEM node write bandwidth.

Updated sysctl parameters

kexec_load_disabled

A toggle indicating if the syscalls`kexec_load` and `kexec_file_load` have been disabled. This value defaults to 0 (false: `kexec_*load` enabled), but can be set to 1 (true: `kexec_*load` disabled).

Once true, kexec can no longer be used, and the toggle cannot be set back to **false**. This allows a kexec image to be loaded before disabling the syscall allowing a system to set up (and later use) an image without it being altered. Generally used together with the `modules_disabled`_ sysctl.

panic_print

Bitmask for printing system info when panic happens. User can chose combination of the following bits:

- bit 0 print all tasks info

- bit 1 print system memory info
- bit 2 print timer info
- bit 3 print locks info if **CONFIG_LOCKDEP** is on
- bit 4 print ftrace buffer
- **bit 5 print all printk messages in buffer**
- **bit 6 print all CPUs backtrace (if available in the arch)**

sched_energy_aware

Enables or disables Energy Aware Scheduling (EAS). EAS starts automatically on platforms where it can run (that is, platforms with asymmetric CPU topologies and having an Energy Model available). If your platform happens to meet the requirements for EAS but you do not want to use it, change this value to **0**. **On Non-EAS platforms, write operation fails and read doesn't return anything.**

CHAPTER 6. DEVICE DRIVERS

6.1. NEW DRIVERS

Table 6.1. Cryptographic drivers

Description	Name	Limited to architectures
IAA Compression Accelerator Crypto Driver	iaa_crypto	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	intel_qat	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_4xxx	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_c3xxx	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_c3xxxvf	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_c62x	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_c62xvf	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_dh895xcc	AMD and Intel 64-bit architectures
Intel® QuickAssist Technology - 0.6.0	qat_dh895xccvf	AMD and Intel 64-bit architectures

Table 6.2. Network drivers

Description	Name	Limited to architectures
	bcm-phy-ptp	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	mt7925-common	64-bit ARM architecture, AMD and Intel 64-bit architectures
	mt7925e	64-bit ARM architecture, AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
	mt792x-lib	64-bit ARM architecture, AMD and Intel 64-bit architectures
CAN bus driver for Bosch M_CAN controller on PCI bus	m_can_pci	IBM Power Systems, AMD and Intel 64-bit architectures
CAN bus driver for Bosch M_CAN controller	m_can	IBM Power Systems, AMD and Intel 64-bit architectures
CAN driver for 8 devices USB2CAN interfaces	usb_8dev	IBM Power Systems, AMD and Intel 64-bit architectures
CAN driver for EMS Dr. Thomas Wuensche CAN/USB interfaces	ems_usb	IBM Power Systems, AMD and Intel 64-bit architectures
CAN driver for Kvaser CAN/USB devices	kvaser_usb	IBM Power Systems, AMD and Intel 64-bit architectures
CAN driver for PEAK-System USB adapters	peak_usb	IBM Power Systems, AMD and Intel 64-bit architectures
Intel® Infrastructure Data Path Function Linux Driver	idpf	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Marvell 88Q2XXX 100/1000BASE-T1 Automotive Ethernet PHY driver	marvell-88q2xxx	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Marvell Octeon EndPoint NIC Driver	octeon_ep	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Microchip 251x/25625 CAN driver	mcp251x	AMD and Intel 64-bit architectures
Microchip MCP251xFD Family CAN controller driver	mcp251xfd	AMD and Intel 64-bit architectures
NXP imx8 DWMAC Specific Glue layer	dwmac-imx	64-bit ARM architecture
	bcm-phy-ptp	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
Realtek 802.11ax wireless 8852C driver	rtw89_8852c	64-bit ARM architecture, AMD and Intel 64-bit architectures
Realtek 802.11ax wireless 8852CE driver	rtw89_8852ce	64-bit ARM architecture, AMD and Intel 64-bit architectures
serial line CAN interface	slcan	IBM Power Systems, AMD and Intel 64-bit architectures
Socket-CAN driver for PEAK PCAN PCIe/M.2 FD family cards	peak_pciefd	IBM Power Systems, AMD and Intel 64-bit architectures
	bcm-phy-ptp	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	mt7925-common	64-bit ARM architecture, AMD and Intel 64-bit architectures
	mt7925e	64-bit ARM architecture, AMD and Intel 64-bit architectures
	mt792x-lib	64-bit ARM architecture, AMD and Intel 64-bit architectures

Table 6.3. Platform drivers

Description	Name	Limited to architectures
AMD HSMP Platform Interface Driver - 2.0	amd_hsmp	AMD and Intel 64-bit architectures
AMD Platform Management Framework Driver	amd-pmf	AMD and Intel 64-bit architectures
Intel TPMI enumeration module	intel_vsec_tpmi	AMD and Intel 64-bit architectures
Intel TPMI SST Driver	isst_tpmi	AMD and Intel 64-bit architectures
Intel TPMI UFS Driver	intel-uncore-frequency-tpmi	AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
Intel Uncore Frequency Common Module	intel-uncore-frequency-common	AMD and Intel 64-bit architectures
Intel Uncore Frequency Limits Driver	intel-uncore-frequency	AMD and Intel 64-bit architectures
Intel WMI Thunderbolt force power driver	intel-wmi-thunderbolt	AMD and Intel 64-bit architectures
Mellanox PMC driver	mlxbf-pmc	64-bit ARM architecture
	intel-hid	AMD and Intel 64-bit architectures
	isst_tpmi_core	AMD and Intel 64-bit architectures

Table 6.4. Graphics drivers and miscellaneous drivers

Description	Name	Limited to architectures
AMD XCP Platform Devices	amdxcp	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
DRM execution context	drm_exec	
Range suballocator helper	drm_suballoc_helper	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	regmap-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	regmap-raw-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	regmap-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
	regmap-raw-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	regmap-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
	regmap-raw-ram	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Arm FF-A interface driver	ffa-module	64-bit ARM architecture
NVIDIA BlueField-3 GPIO Driver	gpio-mlxbf3	64-bit ARM architecture
I/O Address Space Management for passthrough devices	iommufd	
CS42L43 Core Driver	cs42l43	AMD and Intel 64-bit architectures
CS42L43 SoundWire Driver	cs42l43-sdw	AMD and Intel 64-bit architectures
MEI GSC Proxy	mei_gsc_proxy	AMD and Intel 64-bit architectures
	pwrseq_emmc	64-bit ARM architecture
	pwrseq_simple	64-bit ARM architecture
SDHCI platform driver for Synopsys DWC MSHC	sdhci-of-dwcmshc	64-bit ARM architecture
	arm_cspmu_module	64-bit ARM architecture
NVIDIA pinctrl driver	pinctrl-mlxbf3	64-bit ARM architecture
NXP i.MX93 power domain driver	imx93-pd	64-bit ARM architecture
Intel RAPL TPMI Driver	intel_rapl_tpmi	AMD and Intel 64-bit architectures

Description	Name	Limited to architectures
Mellanox BlueField power driver	pwr-mlxbf	64-bit ARM architecture
NXP i.MX93 src driver	imx93-src	64-bit ARM architecture
Provide Trusted Security Module attestation reports via configfs	tsm	AMD and Intel 64-bit architectures

6.2. UPDATED DRIVERS

Table 6.5. Storage driver updates

Description	Name	Current version	Limited to architectures
Broadcom MegaRAID SAS Driver	megaraid_sas	07.727.03.00-rc1	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Driver for Microchip Smart Family Controller	smartpqi	2.1.24-046	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
Emulex LightPulse Fibre Channel SCSI driver	lpfc	0:14.2.0.16	64-bit ARM architecture, IBM Power Systems, AMD and Intel 64-bit architectures
MPI3 Storage Controller Device Driver	mpi3mr	8.5.0.0.50	

CHAPTER 7. 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 7.1. 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 7.2. 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 7.3. 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

CHAPTER 8. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 9.5 that have a significant impact on users.

8.1. INSTALLER AND IMAGE CREATION

The Kickstart installations now applies the dhcpclass option correctly

The application of the Kickstart configuration is moved from NetworkManager to Anaconda by using the NetworkManager API. Previously, Anaconda handled only commands specified in the **%pre** section. During installation, this change had caused omission of the **dhcpclass** option in the Kickstart network command, which led to incorrect application of network configuration. With this update, the handling of the **dhcpclass** option in Anaconda by using the NetworkManager API has been corrected. As a result, the **dhcpclass** option defined in Kickstart configurations is now properly applied during the installation process.

Jira:RHEL-30406

Improved installer stability during virtual network devices configuration

Previously, the installation program could crash when creating a VLAN network device over an existing virtual network device (for example, Team or Bond) in the GUI. This occurred when the underlying device's state changed during the configuration update to the user interface for the new device state.

With this update, the process of refreshing the state of networking in GUI optimized to handle changes in the virtual device state. As a result, the installation program no longer crashes due to changes regarding virtual network devices configured in GUI.

Jira:RHEL-20891

The rhc system role no longer fails on the registered systems when rhc_auth contains activation keys

Previously, a failure occurred when you executed playbook files on the registered systems with the activation key specified in the **rhc_auth** parameter. This issue has been resolved. It is now possible to execute playbook files on the already registered systems, even when activation keys are provided in the **rhc_auth** parameter.

Bugzilla:2186218

Stale network link configuration files no longer cause rendering your operating system unbootable

Previously, the RHEL installer created stale **/etc/systemd/network/** link configuration files during the installation. The outdated configuration files interfere with the intended network settings. This leads to an unbootable system if the boot is from NVMe over TCP. With this fix, users no longer need to manually remove, **/etc/systemd/network/10-anaconda-ifname-nbft*.link** files and regenerate the **initramfs** by running the **dracut -f** command.

Jira:RHEL-30149

8.2. SECURITY

Non-constant time code paths removed from OpenSSL EC signatures

Previously, OpenSSL used non-constant time code paths for Elliptic Curve Digital Signature Algorithm

(ECDSA) signatures. This could have exposed the signature operations to attacks similar to the Minerva attack and potentially reveal the private key. This update removes non-constant time code paths in OpenSSL EC signatures, and as a result, this vulnerability is no longer present.

Jira:RHEL-38514

SELinux policy correctly labels npm

Previously, the **npm** service executable was labeled with the generic **lib_t** SELinux type. As a consequence, **npm** could not be executed. In this update, the **npm** executable has been explicitly labeled in the SELinux policy with the **bin_t** type. As a result, the **npm** service starts successfully and runs in the **unconfined_service_t** domain.

Jira:RHEL-36587

SELinux policy adds rules for sysadm_r users to define input/output log directory through sudo

Previously, the SELinux policy did not contain rules to allow confined administrators to run any command to specify the input/output log directory by using **sudo** when the **iolog_dir** option was defined in the **sudo** configuration. As a consequence, confined administrators in the **sysadm_r** role could not run commands by using **sudo** with the **iolog_dir** option. This update adds a rule to the SELinux policy, and as a result, **sysadm_r** users can run commands by using **sudo** with **iolog_dir**.

Jira:RHEL-16104

Audit rules for /proc are now correctly loaded during the boot

Before this update, the system failed to load Audit watch rules for the /**proc** directory during the boot phase. Consequently, the administrator had to load the rules manually later, and the rules were not applied during the boot. The bug has been fixed, and the system now loads the Audit rules related to /**proc** during the boot phase.

Jira:RHEL-5197

Audit in the immutable mode no longer prevents auditd from starting

Previously, if the Audit system was set to the immutable mode by adding the **-e 2** rule, the **augenrules** command exited with a return code of 1 instead of 0 when restarting the **auditd** service or running the **augenrules --load** command. Consequently, the system interprets the return code of 1 as an error, and this prevents it from starting **auditd** at boot. With this update, **augenrules** exits with a zero return code when Audit is set to the immutable mode, and the system can correctly start **auditd** in this scenario.

Jira:RHEL-40110

IPsec ondemand connections no longer fail to establish

Previously, when an IPsec connection with the **ondemand** option was set up by using the TCP protocol, the connection failed to establish. With this update, the new Libreswan package makes sure that the initial IKE negotiation completes over TCP. As a result, Libreswan successfully establishes the connection even in TCP mode of IKE negotiation.

Jira:RHEL-51879[1]

update-ca-trust extract no longer fails to extract certificates with long names

When extracting certificates from the truststore, the **trust** tool internally derives the file name from the certificates' object label. For long enough labels, the resulting path might previously have exceeded the

system's maximum file name length. As a consequence, the **trust** tool failed to create a file with a name that exceeded the maximum file name length of a system. With this update, the derived name is always truncated to within 255 characters. As a result, file creation does not fail when the object label of a certificate is too long.

Jira:RHEL-58899[1]

8.3. SUBSCRIPTION MANAGEMENT

subscription-manager no longer retains nonessential text in the terminal

Starting with RHEL 9.1, **subscription-manager** displays progress information while processing any operation. Previously, for some languages, typically non-Latin, progress messages did not clean up after the operation finished. With this update, all the messages are cleaned up properly when the operation finishes.

If you have disabled the progress messages before, you can re-enable them by entering the following command:

```
# subscription-manager config --rhsm.progress_messages=1
```

Bugzilla:2136694[1]

8.4. SOFTWARE MANAGEMENT

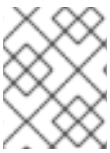
The dnf autoremove command behavior is now consistent with the man page documentation and the command now considers the package installation reason

Previously, when you removed unnecessary packages by using the **dnf autoremove** command, installed packages marked as **installonly** were removed. However, the **dnf(8)** man page documentation contained information that **installonly** packages were excluded from the **dnf autoremove** operations.

With this update, the following fixes were provided:

- The **dnf(8)** man page documentation now conveys that **installonly** packages are not excluded from **dnf autoremove**.
- DNF now correctly infers a package installation reason from the installation history if multiple **installonly** packages are included in the **dnf autoremove** operation.

As a result, the **dnf autoremove** command behavior is now consistent with the man page documentation and the command now considers the package installation reason.



NOTE

If **dnf autoremove** insists on removing the required packages, mark these packages as **dnf mark install *<package>***.

Jira:RHEL-15902

The dnf-automatic systemd service no longer fails to apply security updates

Previously, when you used the **dnf-automatic-install systemd** service to only apply security fixes, the automatic upgrade of the **samba-client-libs** package failed. With this update, **dnf-automatic** applies

security updates the same way as the DNF tool. As a result, the **dnf-automatic** service no longer fails to apply security updates.

Jira:RHEL-21874

dnf remove --duplicates no longer exits with nonzero exit code and error message

Previously, if you ran the **dnf remove --duplicates** command when no duplicate packages were present on the system, **dnf** exited with non-zero exit code and the **No duplicated packages found for removal.** error on standard error output (**stderr**). With this update, **dnf** now exits with **0** and does not write anything on **stderr**. Note that the same issue was also fixed for the **dnf remove --oldinstallonly** command when no older versions of **installonly** packages are installed.

Jira:RHEL-6424

dnf remove-n now removes only packages with the matching RPM names

Previously, if you had installed some package and another package that has the name of the former package in the RPM Provides directive, a first invocation of the **dnf remove-n** command removed the former package. A repeated invocation of the command removed the latter package.

With this update, the **dnf remove-n** command removes only packages with matching RPM names and does not consider the RPM Provides. As a result, only one invocation of **dnf remove-n** is now sufficient to remove all matching packages.

Jira:RHEL-38470

dnf reinstall now respects a cost of the repositories when reinstalling a package

Previously, if you reinstalled a package available in multiple repositories, the package was not reinstalled from a repository with the lowest cost. With this update, the DNF tool supplies packages from all repositories to a dependency solver if the packages have the equal **name-epoch-version-release-architecture** identifier. As a result, the **dnf reinstall** command now respects the cost of the repositories.

Jira:RHEL-25005

dnf-system-upgrade now points to its documentation by using a secure HTTPS link

Previously, the **dnf-system-upgrade** service documentation used the insecure HTTP link to access its documentation. With this update, the URL now uses the secure HTTPS schema.

Jira:RHEL-13053[1]

dnf history rollback now correctly executes during a repeated rollback of an RPM transaction that includes installation and upgrade of the same package

Previously, when you performed a repeated rollback on an RPM transaction that included installation and upgrade of the same package, the **dnf history rollback** command attempted to perform a bogus transaction. This transaction failed instead of doing nothing because the rollback to the latest transaction had nothing to roll back.

With this update, calculating a difference between the two same-version RPM transactions is now fixed in the **libdnf** library. As a result, **dnf history rollback** that points to the currently latest RPM transaction now correctly results in the **Nothing to do.** output.

Jira:RHEL-17494

microdnf no longer fails to reinstall packages that conflict with an RPM symbol they provide

Previously, when you reinstalled a package with the **microdnf** package manager, the RPM transaction failed. With this update, **libdnf** creates an RPM transaction where the package being reinstalled provides an RPM symbol that the package also conflicts with. As a result, **microdnf** can now reinstall packages that conflict with an RPM symbol they provide.

Jira:RHEL-1454[1]

Interpreting the Anaconda Kickstart script no longer hangs when you install the system

Previously, when you installed the system with the Anaconda Kickstart script, interpreting this script randomly hung. With this update, the **libdnf** memory management allows applying a query after increasing the number of available packages. As a result, system installation does not hang because the **libdnf** library does not throw an exception after enabling a repository.

Jira:RHEL-27657[1]

DNF(8) now includes information about dnf makecache --timer not trying further mirrors if the first mirror fails

Previously, the information that the **dnf makecache --timer** command does not try further mirrors in a repository mirrorlist if the first mirror failed was not included in the DNF(8) man page. With this update, the documentation was updated to include this information.

Jira:RHEL-1342

8.5. SHELLS AND COMMAND-LINE TOOLS

The pkla-compact binary is executed when the polkit is called on the logind-session-monitor event

Previously, re-verification of the authorizations for polkit actions was triggered by any **logind-session-monitor** event for all users, for example, login, logout, session state change. Additionally, each **CheckAuthorization** request executed the **polkit-pkla-compat** binary to check for legacy **.pkla** configuration files even if no such files are present on the system, which causes CPU usage to increase by the polkit daemon.

Currently, only the **logind-session** changes that are relevant for the polkit actions are reflected. If the session's state changes, the polkit objects associated with the session trigger re-verification (**CheckAuthorization**). You must restart (**log out to login screen and re-login** or **reboot**) the GNOME shell for a successful update.

The **polkit-pkla-compat** binary is now a soft dependency. As a result, you can reduce the CPU intensity by uninstalling the **polkit-pkla-compat** binary only if there are no **.pkla** files present in **/etc/polkit-1/localauthority**, **/etc/polkit-1/localauthority.conf.d**, **/var/lib/polkit-1/localauthority** and their specific sub directories.

Jira:RHEL-39063[1]

Improved dovecot stability for missing sieve scripts

Previously, **dovecot** did not properly track optional sieve scripts. As a result, if the hash group for the path of the missing script matched that of another script, the LDA process could crash during the email delivery.

With this fix, dovecot no longer crashes when handling missing optional scripts, as the comparison and handling of these scripts have been corrected.

Jira:RHEL-37160[1]

The print-config option in nvram command does not result in segmentation fault

Previously, when the **nvram** command was run with the **print-config** option, it resulted in segmentation fault. The segmentation fault occurred because the code tried to access memory beyond the limit of the data present in the **varlen** index. The **varlen** index is the length of the string provided by the user.

This update adds a condition to check whether the length of data is greater than the **varlen** index. It prevents accessing memory beyond the limit and therefore preventing segmentation faults.

Jira:RHEL-23624[1]

The nvram --nvram-size command does not result in segmentation fault

Previously, when the **nvram-size** command exceeded the default size value, a segmentation fault was encountered.

```
nvram: WARNING: expected 268435456 bytes, but only read 15360!
```

With this fix, now a check condition for **nvram-size** is added to avoid the infinite while loop and prevent the segmentation fault.

Jira:RHEL-23619[1]

ReaR now interprets square brackets enclosing IPv6 addresses in URLs as expected

Previously, square brackets in **OUTPUT_URL** and **BACKUP_URL** were not interpreted correctly. Specifying an IPv6 address instead of a hostname requires enclosing the address in square brackets, for example, [::1] for localhost. Since the brackets were not interpreted correctly, using an IPv6 address in a **sshfs:**// or **nfs:**// URL was not possible.

As a consequence, if the user used a **sshfs:**// or **nfs:**// scheme in the **BACKUP_URL** or **OUTPUT_URL** with an IPv6 address enclosed in square brackets, ReaR aborted prematurely with an error message, for example:

```
ERROR: Invalid scheme '' in BACKUP_URL
```

With this update, ReaR is now fixed to not interpret square brackets as shell metacharacters when parsing **sshfs:**// and **nfs:**// URLs. Now, you can use IPv6 addresses enclosed in brackets in **BACKUP_URL** and **OUTPUT_URL** that use the **sshfs:**// or **nfs:**// scheme . For example:

```
OUTPUT_URL=nfs://[2001:db8:ca2:6::101]/root/REAR
```

Before this fix was implemented, it was possible to work around the bug by using quoting and backslash characters, for example:

```
OUTPUT_URL="nfs://\[2001:db8:ca2:6::101\]/root/REAR"
```

Note: If you have been using the workaround, remove the backslash characters after applying the update.

Jira:RHEL-40565

8.6. NETWORKING

CPU usage rises negligibly when NetworkManager processes large regularly updated routing tables

Previously, when external routing daemons updated big IPv6 tables of more than thousands of routes, NetworkManager increased its CPU usage to almost 100%. This could slow down the overall system performance and network configuration. The problem has been fixed by updating the NetworkManager source code to ignore the changes to routes for routing protocols other than a small set of protocols. As a result, the CPU usage rises negligibly in the previously described circumstances.

Jira:RHEL-26195[1]

The value for ipv6.ip6-privacy no longer changes between connection activations

Originally, when the global default value was not set for the **ipv6.ip6-privacy** parameter, its value reverted to the value from the **/proc/sys/net/ipv6/conf/default/use_tempaddr** file. A recent change to the NetworkManager source code caused it to incorrectly fall back to the value read from the **/proc/sys/net/ipv6/conf/IFNAME/use_tempaddr** file instead. As a consequence, IPv6 address generation changed, and the value for **ipv6.ip6-privacy** could change between connection activations. The problem has been fixed by reverting back to the original behavior. As a result, the value for **ipv6.ip6-privacy** does not change anymore between connection activations.

Jira:RHEL-31182

The xdp-loader features command now works as expected

The **xdp-loader** utility was compiled against the previous version of **libbpf**. As a consequence, **xdp-loader features** failed with an error:

```
Cannot display features, because xdp-loader was compiled against an old version of libbpf without support for querying features.
```

The utility is now compiled against the correct **libbpf** version. As a result, the command now works as expected.

Jira:RHEL-3382

Mellanox ConnectX-5 adapter works in the DMFS mode

Previously, while using the Ethernet switch device driver model (**switchdev**) mode, the **mlx5** driver failed if configured in the device managed flow steering (**DMFS**) mode on the **ConnectX-5** adapter. Consequently, the following error message appeared:

```
mlx5_core 0000:5e:00.0: mlx5_cmd_out_err:780:(pid 980895): DELETE_FLOW_TABLE_ENTRY(0x938) op_mod(0x0) failed, status bad resource(0x5), syndrome (0xabe70a), err(-22)
```

As a result, when you update the firmware version of the **ConnectX-5** adapter to 16.35.3006 or later, the error message will not appear.

Jira:RHEL-9897[1]

NetworkManager can mitigate the impact of CVE-2024-3661 (TunnelVision) in VPN connection profiles

VPN connections rely on routes to redirect traffic through a tunnel. However, if a DHCP server uses the classless static route option (121) to add routes to a client's routing table, and the routes propagated by the DHCP server overlap with the VPN, traffic can be transmitted through the physical interface instead

of the VPN. CVE-2024-3661 describes this vulnerability, which is also know as TunnelVision. As a consequence, an attacker can access traffic that the user expects to be protected by the VPN.

On RHEL, this problem affects LibreSwan IPSec and WireGuard VPN connections. Only LibreSwan IPSec connections with profiles in which both the **ipsec-interface** and **vt-interface** properties are undefined or set to **no** are not affected.

The CVE-2024-3661 document describes steps to mitigate the impact of TunnelVision by configuring VPN connection profiles to place the VPN routes in a dedicated routing table with a high priority. The steps work for both LibreSwan IPSec and WireGuard connections. However, to apply the mitigation steps to a LibreSwan IPSec connection profile, you must use NetworkManager 1.48.10-5 or later. On RHEL 9.5, this version is provided by the RHSA-2025:0377 advisory.

Jira:RHEL-73167[1]

8.7. KERNEL

eBPF programs in Linux Falcon Sensor caused a kernel panic on load

Previously, **eBPF** programs used by the Linux Falcon Sensor in user-mode caused kernel panics. As a consequence, some of the kernels of RHEL v9.4 were affected when loading such programs.

With this update, the issue is fixed, and **eBPF** programs run normally on the RHEL v9.5 kernels.

Jira:RHEL-34937[1]

RHEL previously failed to recognize NVMe disks when VMD was enabled

When you reset or reattached a driver, the Volume Management Device (VMD) domain previously did not soft-reset. Consequently, the hardware could not properly detect and enumerate its devices. With this update, the operating system with VMD enabled now correctly recognizes NVMe disks, especially when resetting a server or working with a VM machine.

Bugzilla:2128610[1]

8.8. FILE SYSTEMS AND STORAGE

multipathd now displays a message instead of being unresponsive

Previously, on executing the **multipathd show maps topology** command or any other command without any multipath devices, the command used to hang and timeout without any other response. With this update, the **multipathd** command now displays **ok** where there is no output to return without hanging and timing out.

Jira:RHEL-44569[1]

multipath now correctly associates the paths with native multipathd NVMe devices

Previously, the **multipath** command displayed native **multipathd** NVMe devices with namespace 1, as the first defined namespace in their path, instead of displaying the correct path. With this fix, **multipath** now correctly matches the paths to the native **multipathd** NVMe devices while listing them. As a result, while using **multipath** to view native **multipathd** NVMe devices, you can see the correct paths, where the namespace ID of the path matches the namespace ID of NVMe devices.

Jira:RHEL-28068[1]

Modification in flush_on_last_del parameter of multipathd resolves service hanging issue

Previously, **multipathd** could hang while trying to automatically remove an unused multipath device whose last path was deleted. In this case, the multipath device was set to queue IO when there were no usable paths

With this fix, by disabling queuing, **multipathd** now automatically removes multipath devices. If queueing is not disabled on a device, **multipathd** will not attempt for the automatic removal. To accomplish this, you can set the following options along with **yes** or **no** for the **flush_on_last_del** parameter:

- **always**: When set to **always** or **yes**, **multipathd** always disables queueing when the last path has been deleted.
- **unused**: This is the default option. When set to **unused** or **no**, **multipathd** disables queueing when the last path has been deleted and the device is unused.
- **never**: When set to **never**, **multipathd** never disables queueing when the last path has been deleted.

As a result, **multipathd** no longer becomes unresponsive while trying to automatically remove unused multipath devices of which the last known path is invalid.

Jira:RHEL-30272[1]

System boots correctly when adding a NVMe-FC device as a mount point in /etc/fstab

Previously, due to a known issue in the **nvme-cli nvmf-autoconnect systemd** services, systems failed to boot while adding the Non-volatile Memory Express over Fibre Channel (NVMe-FC) devices as a mount point in the **/etc/fstab** file. Consequently, the system entered into an emergency mode. With this update, a system boots without any issue when mounting an NVMe-FC device.

Jira:RHEL-8171[1]

LUNs are now visible during the operating system installation

Previously, the system was not using the authentication information from firmware sources, specifically in cases involving iSCSI hardware offload with CHAP (Challenge-Handshake Authentication Protocol) authentication stored in the iSCSI iBFT (Boot Firmware Table). As a consequence, the iSCSI login failed during installation.

With the fix in the **udisks2-2.9.4-9.el9** firmware authentication, this issue is now resolved and LUNs are visible during the installation and initial boot.

Bugzilla:2213769[1]

8.9. HIGH AVAILABILITY AND CLUSTERS

pcs output no longer wrapped when piped to the grep utility

Previously, when the **pcs** output was piped to another process, the output width always defaulted to 80 characters. This made it difficult to use the **grep** utility to look for specific lines in the output. With this change, **pcs** does not wrap its output when piped to **grep**.

Jira:RHEL-36514

pcsd processes now consistently stop correctly and promptly

Previously, the creation method for **pcsd** processes sometimes caused a deadlock during process termination. The processes were then terminated only after a **systemd** timeout. This fix changes the process creation method and there is no longer a deadlock when the processes are stopped. As a result, **pcsd** consistently stops correctly within a short time.

Jira:RHEL-28749

pcs validation of SBD options

Previously, when you enabled SBD with the **pcs stonith sbd enable** command and specified values for SBD options that are not valid, it resulted in SBD misconfiguration. The **pcs** command-line interface has been updated to validate the values for SBD options. When the values are not valid, **pcs** reports the error and does not create or update an SBD configuration.

Jira:RHEL-17962

Ability to remove Booth configuration from a Booth arbitrator node

Previously, running the **pcs booth destroy** command to remove Booth configuration from a Booth arbitrator node yielded an error. This happened because the command did not remove Booth configuration from nodes that are not part of the cluster. It is now possible to remove Booth configuration from Booth arbitrators.

Jira:RHEL-7737

pcs no longer validates fencing topology with fencing levels greater than 9

The Pacemaker cluster resource manager ignores fencing topology levels greater than 9. Configuring levels greater than 9 might lead to failed fencing. With this update, you can configure fencing levels with values of only 1 to 9 in the **pcs** command-line interface and fencing topology works correctly.

Jira:RHEL-2977

The CIB manager no longer increases in size indefinitely with each request from an asynchronous client

Previously, when the CIB manager received a request from an asynchronous client, it leaked a small amount of memory. This caused the CIB manager process gradually to grow in size. With this fix, the relevant memory is freed for asynchronous clients and the CIB manager process does not grow in size indefinitely.

Jira:RHEL-40117

The crm_node -i command now correctly parses a node ID

Previously, the **crm_node -i** and the equivalent **crm_node --*cluster-id*** commands would sometimes show a "Node is not known to cluster" message instead of the local node's cluster ID as expected. With this fix, node IDs are properly parsed and the command works as intended.

Jira:RHEL-47249

8.10. COMPILERS AND DEVELOPMENT TOOLS

GCC Toolset 13: GCC now compiles code correctly on IBM POWER9, Little Endian with vectorization enabled

Previously, when compiling code on IBM POWER9, Little Endian with vectorization enabled, the GCC compiler generated incorrect code. The Register Transfer Language (RTL) pattern in the expander has been fixed, and the code now compiles correctly.

Jira:RHEL-45190[1]

glibc dynamic linker prevents reentrant malloc calls made by applications using TLS access from custom malloc implementations

Some applications provide a custom **malloc** dynamic memory allocation implementation that uses global-dynamic thread-local storage (TLS) instead of initial-exec TLS. Before this update, applications with bundled **malloc** calls that use global-dynamic TLS could experience reentrant calls into the application's **malloc** subsystem. As a consequence, the application **malloc** call crashed due to stack exhaustion or unexpected state of internal data structures. With this update, the **glibc** dynamic linker detects TLS access from custom **malloc** implementations. If a TLS access during a **malloc** call is detected, further calls during TLS processing are skipped, and reentrant **malloc** calls are prevented.

Jira:RHEL-39992

TLS data is no longer overwritten by calls to dlopen() from an ELF constructor

Previously, the **glibc** dynamic linker did not track the initialization status of thread-local storage (TLS) correctly in certain cases where the **dlopen()** function was invoked from an ELF constructor. Consequently, TLS data was reverted to its original value after it had been modified by the application. With this update, the dynamic linker uses a separate flag to track TLS initialization for each shared object. As a result, TLS data is no longer unexpectedly overwritten by calls to the **dlopen()** function from an ELF constructor.

Jira:RHEL-36148

Perftools no longer fail to process LTO debug information

Previously, the Binary File Descriptor (BFD) library from the **binutils** collection, which is used by performance tools to read debug information from binary files, was unable to handle debug information generated by the GCC compiler with the Link Time Optimization (LTO) enabled. As a consequence, perftools displayed error messages and failed to run correctly when examining files that contained LTO debug information. The BFD library has been updated to handle debug information generated during compilation with LTO enabled, and the affected perftools successfully process such debug information.

Jira:RHEL-43758[1]

8.11. IDENTITY MANAGEMENT

The ipa-replica-manage command no longer resets the nsslapd-ignore-time-skew setting during forced replication

Previously, the **ipa-replica-manage force-sync** command reset the **nsslapd-ignore-time-skew** setting to **off**, regardless of the configured value. With this update, the **nsslapd-ignore-time-skew** setting is no longer overwritten during forced replication.

Jira:RHEL-52300[1]

The ipa idrange-add command now warns that Directory Server must be restarted on all IdM servers

Previously, the **ipa idrange-add** command did not warn the administrator that they must restart the Directory Server (DS) service on all IdM servers after creating a new range. As a consequence, the

administrator sometimes created a new user or group with a UID or GID belonging to the new range without restarting the DS service. The addition resulted in the new user or group not having an SID assigned. With this update, a warning that DS needs to be restarted on all IdM servers is added to the command output.

Jira:RHELDOCS-18201[1]

certmonger now correctly renews KDC certificates on hidden replicas

Previously, when the certificate was about to expire, **certmonger** failed to renew the KDC certificate on hidden replicas. This happened because the renewal process only considered non-hidden replicas as active KDCs. With this update, the hidden replicas are treated as active KDCs, and **certmonger** renews the KDC certificate successfully on these servers.

Jira:RHEL-39477[1]

AD administrators can now deploy IdM replicas

Previously, during the installation of a RHEL Identity Management (IdM) replica, checking if the provided Kerberos principal had the required privilege did not extend to checking user ID overrides. Consequently, a replica connection check failed while trying to deploy a replica using the credentials of an AD administrator that had an ID override with the needed privilege.

With this update, a check if there is an ID override for the principal that has the needed privileges has been added. As a result, you can now deploy a replica using the credentials of an AD administrator that is configured to act as an IdM administrator.

Note that this fix also applies to **ansible-freeipa**.

Jira:RHEL-26261

Directory Server no longer ignores nsslapd-idletimeout

Previously, if a connection was open by a non Directory Manager user, Directory Server could ignore the **nsslapd-idletimeout** value and did not close the connection after the specified amount of time. With this update, Directory Server closes connection as expected after reaching the configured idle time.

Jira:RHEL-17511[1]

Search operations now return large groups faster

Previously, if searches of large static groups used a filter that contained **equality** matching components with the **uniquemember** attribute, for example, **'(uniquemember=uid=foo,ou=people,<suffix>)'**, such searches were slow and CPU-intensive. With this update, during search filter evaluation, Directory Server uses an internal structure where the member distinguished names (DNs) are sorted, which makes searches of large groups faster and less CPU-intensive.

Jira:RHEL-49454[1]

One-level scoped search no longer fails to return sub-suffixes

Previously, when you ran the **ldapsearch** command with the **-s** option set to **one**, the search result did not contain sub-suffixes of the entry specified in the **-b** option. With this update, the one-level scoped search successfully returns immediate children of the entry.

Jira:RHEL-49458

The Referential Integrity plug-in no longer leads to the server failure

Previously, when you used the Referential Integrity plug-in with the deferred check, the thread that processed the check could access the released data structure at shutdown leading to server failure. With this update, the plug-in no longer releases the data structure until the deferred checking thread stops and no failure occurs.

Jira:RHEL-5108

The dscreate ds-root command now accepts a relative path

Previously, when you tried to create an instance as a non-root user and provided a **bin_dir** argument value that contained a relative path, the relative path was written to the **defaults.inf** file causing the instance creation failure. With this update, when you provide a relative path as the **bin_dir** argument value, the instance is now created successfully.

Jira:RHEL-5115

Offline import of LDIF files now runs correctly

Previously, before an offline import the cache autotuning operation was not triggered. As a result, the import operation was slow when performed by the **ldif2db** script. With this update, Directory Server triggers the cache autotuning before the **ldif2db** operation increasing the import performance.

Jira:RHEL-5131

The dsconf schema matchingrules list command now displays the new inchainMatch matching rule

Previously, the **dsconf** utility did not display the supported **inchainMatch** matching rule in the list of matching rules because **inchainMatch** was registered without matching syntax. With this update, the syntax for the **inchainMatch** is defined, and when you run the **dsconf schema matchingrules list** command, the **inchainMatch** is displayed in the list.

Jira:RHEL-33087

8.12. SSSD

Integration between shadow-utils and sss_cache for local user caching is disabled

In RHEL 9, the SSSD implicit **files** provider domain, which retrieves user information from local files such as **/etc/shadow** and group information from **/etc/groups**, was disabled by default. However, the integration in **shadow-utils** was not fully disabled, which resulted in calls to **sss_cache** when adding or deleting local users. The unnecessary cache updates caused performance issues for some users. With this update, the **shadow-utils** integration with **sss_cache** is fully disabled, and the performance issues caused by unnecessary cache updates no longer occur.

Jira:RHEL-56352, Jira:RHELPLAN-100639

8.13. THE WEB CONSOLE

cockpit-machines now correctly removes USB host devices

The **cockpit-machines** add-on did not correctly handle removals of USB host devices from running virtual machines. Consequently, when you clicked **Remove** in the RHEL web console, instead of successful removal, you saw the following error message:

> Danger alert: Host device could not be removed

With this update, USB host device removals have been fixed, and you can correctly remove a USB host device from a virtual machine through the RHEL web console.

Jira:RHEL-31082

8.14. RED HAT ENTERPRISE LINUX SYSTEM ROLES

Implementation of multiple sets of key-value pairs of node attributes is now consistent with other cluster configuration components

The **ha_cluster** RHEL system role supports only one set of key-value pairs for each configuration item. Previously, when you configured multiple sets of node attributes, the sets were merged into a single set. With this update, the role uses only the first set you define and ignores the other sets. This behavior is now consistent with how the role implements multiple sets of key-value pairs for other configuration components that use a key-value pair structure.

Jira:RHEL-33076

No property conflicts between the NetworkManager service and the NetworkManager plugin

Previously, the **network** RHEL system role did not request user consent to restart the **NetworkManager** service when updates were available to networking packages, particularly, due to wireless interface changes. Consequently, this led to potential conflicts between the **NetworkManager** service and the **NetworkManager** plugin. Alternatively, the **NetworkManager** plugin was failing to run correctly. The problem has been fixed by making the **network** RHEL system role ask user for their consent to restart the **NetworkManager** service. As a result, there are no property conflicts between the **NetworkManager** service and the **NetworkManager** plugin in the described scenario.

Jira:RHEL-32872

GRUB2 on RHEL 9 and RHEL 10 Beta UEFI managed nodes correctly prompts for a password

Previously, the **bootloader** RHEL system role incorrectly placed the password information in the **/boot/efi/EFI/redhat/user.cfg** file on managed nodes that ran RHEL 9 and RHEL 10 Beta with UEFI Secure Boot feature. The correct location was the **/boot/grub2/user.cfg** file. Consequently, when you rebooted the managed node to modify any boot loader entry, GRUB2 did not prompt you for a password. This update fixes the problem by setting the path for **user.cfg** to **/boot/grub2/** in the source code. When you reboot the OS on a UEFI Secure Boot managed node to modify any boot loader entry, GRUB2 prompts you to input your password.

Jira:RHEL-39996

You cannot set the name parameter for the imuxsock input type

Previously, the **logging** RHEL system role incorrectly set a name parameter for the **imuxsock** input type. As a consequence, this input type did not support the **name** parameter and the **rsyslog** utility on the managed node printed this error **...parameter 'name' not known — typo in config file?...**. This update fixes the **logging** RHEL system role to ensure that the **name** parameter is not associated with the **imuxsock** input type.

Jira:RHEL-35561

Running the storage RHEL system role on a system with a pre-existing Stratis pool works as expected

Previously, the **storage** RHEL system role could not process the existing devices and device formats.

This caused the role to fail on systems with a pre-existing Stratis pool, when checking if Stratis format conformed to the configuration specified by the playbook. Consequently, the playbook failed with an error, however the Stratis pool itself was not damaged or changed. This update makes the **storage** RHEL system role work correctly with Stratis devices and other formats without labelling support. As a result, running a playbook on a system with a pre-existing Stratis pool no longer fails.

Jira:RHEL-29874[1]

Removing Quadlet-defined networks using podman works irrespective of a custom NetworkName directive

When removing networks, the **podman** RHEL system role was using the "systemd- + name of the Quadlet file" syntax for the network name. Consequently, if the Quadlet file had a different **NetworkName** directive in it, the removal would fail. With this update, the **podman** source code has been updated to use "the Quadlet file name + the **NetworkName** directive from that file" as a name of the network to remove. As a result, removal of networks defined by Quadlet files using the **podman** RHEL system role works both with and without a custom **NetworkName** directive in the Quadlet file.

Jira:RHEL-40761

The storage RHEL system role is idempotent again

The **storage** RHEL system role in some cases incorrectly calculated sizes of existing devices. Consequently, running the same playbook again without changes caused the role to attempt resizing the device that already had the correct size, instead of passing without errors. With this update, the size calculation was fixed. As a result, the role now correctly identifies that the device already has the size specified by the playbook and does not try to resize it.

Jira:RHEL-25777

The network units in the Quadlet unit files are now properly cleaned up

The **podman** RHEL system role was not correctly managing the network units defined under the **[Network]** section in the Quadlet unit files. Consequently, the network units were not stopped and disabled and subsequent runs would fail due to those units not being cleaned up properly. With this update, **podman** manages the **[Network]** units, including stopping and removing. As a result, the **[Network]** units in the Quadlet unit files are properly cleaned up.

Jira:RHEL-50102

The podman RHEL system role creates new secrets if necessary

The **podman** RHEL system role incorrectly did not check whether a secret with the same name already existed if you used the **skip_existing: true** option of the **podman_secrets** role variable. Consequently, the role did not create any new secret if using that option. This update fixes the **podman** RHEL system role to check for existing secrets if you use **skip_existing: true**. As a result, the role properly creates new secrets if they do not exist. Conversely, it does not create a secret of the same name if you use **skip_existing: true**.

Jira:RHEL-39438

The linger feature can be canceled for the correct users

When processing the instruction list of configuration items from kube files or Quadlet files, the **podman** RHEL system role was incorrectly using the user ID associated with the entire list. It did not use the user ID associated with the list item to compile the linger file name. Consequently, the linger file was not

created and therefore the **podman** RHEL system role could not cancel the linger feature for the actual user if necessary. With this update, **podman** uses the correct username to construct the linger file name. As a result, the linger feature can be canceled for the correct users.

Jira:RHEL-32382

The podman RHEL system role can set the ownership of the host directory again

Previously, the **podman** RHEL system role was using the **become** keyword with the user when setting the ownership of the host directory. As a consequence, the role could not properly set the ownership. With this update, the **podman** RHEL system role does not use **become** with the ordinary user. Instead, it uses the **root** user. As a result, **podman** can set the ownership of the host directory.

As a complement to this bug fix, the following role variables have been added to the **podman** RHEL system role:

- **podman_subuid_info** (dictionary): Exposes information used by the role from the **/etc/subuid** file. This information is needed to properly set the owner information for host directories.
- **podman_subgid_info** (dictionary): Exposes information used by the role from the **/etc/subgid** file. This information is needed to properly set the group information for host directories.

For more details about the newly added variables, see the resources in the **/usr/share/doc/rhel-system-roles/podman/** directory.

Jira:RHEL-32464

The podman RHEL system role now correctly searches for subgid values

Subordinate group IDs (**subgid**) is a range of group ID values assigned to non-root users. By using these values, you can run processes with different group IDs inside a container compared to the host system. Previously, the **podman** RHEL system role was incorrectly searching in the **subgid** values using the group name instead of using the user name. Consequently, the difference between the user name and the group name made **podman** fail to look up the **subgid** values. This update fixes **podman** to correctly search for **subgid** values and the problem no longer occurs in this scenario.

Jira:RHEL-56626

The sshd RHEL system role can configure the second sshd service correctly

Running the **sshd** RHEL system role to configure the second **sshd** service on your managed nodes caused an error if you did not specify the **sshd_config_file** role variable. Consequently, your playbook would fail and the **sshd** service would not be configured correctly. To fix the problem, deriving of the main configuration file has been improved. Also, the documentation resources in the **/usr/share/doc/rhel-system-roles/sshd/** directory have been made clearer to avoid this problem. As a result, configuring the second **sshd** service as described in the above scenario works as expected.

Jira:RHEL-29309

The bootloader RHEL system role generates the missing /etc/default/grub configuration file if necessary

Previously, the **bootloader** RHEL system role expected the **/etc/default/grub** configuration file to be present. In some cases, for example on OSTtree systems, **/etc/default/grub** can be missing. As a consequence, the role failed unexpectedly. With this update, the role generates the missing file with default parameters if necessary.

Jira:RHEL-26714

The cockpit RHEL system role installs all cockpit-related packages that match a wildcard pattern

Previously, the **dnf** module used through the **cockpit** RHEL system role did not install all **cockpit**-related packages. As a consequence, some requested packages were not installed. With this update, the source code of the **cockpit** RHEL system role was changed to use the **dnf** module directly with an asterisk wildcard package name and a list of packages to exclude. As a result, the role correctly installs all requested packages that match the wildcard pattern.

Jira:RHEL-41090

8.15. VIRTUALIZATION

Virtual machines with a large amount of vCPUs and virtual disks no longer fail

Previously, assigning a large amount of vCPUs and virtual disks to a RHEL virtual machine (VM) might have caused the VM to fail to boot. With this update, the problem has been fixed and virtual machines work normally in these cases.

Jira:RHEL-32990[1]

Using NBD to migrate a VM storage over a TLS connection works correctly

Previously, when migrating a virtual machine (VM) and its storage device by using the Network Block Device (NBD) protocol over a TLS connection, a data race in the TLS handshake might have made the migration appear to be successful. However, it could have caused the QEMU process on the destination VM to become unresponsive to further interactions.

With this update, the problem has been fixed and using the NBD protocol over a TLS connection for a VM migration works correctly.

Jira:RHEL-33440

The installation program shows the expected system disk to install RHEL on VM

Previously, when installing RHEL on a VM using **virtio-scsi** devices, it was possible that these devices did not appear in the installation program because of a **device-mapper-multipath** bug. Consequently, during installation, if some devices had a serial set and some did not, the **multipath** command was claiming all the devices that had a serial. Due to this, the installation program was unable to find the expected system disk to install RHEL in the VM.

With this update, **multipath** correctly sets the devices with no serial as having no World Wide Identifier (WWID) and ignores them. On installation, **multipath** only claims devices that **multipathd** uses to bind a multipath device, and the installation program shows the expected system disk to install RHEL in the VM.

Bugzilla:1926147[1]

Windows guests boot more reliably after a v2v conversion on hosts with AMD EPYC CPUs

After using the **virt-v2v** utility to convert a virtual machine (VM) that uses Windows 11 or a Windows Server 2022 as the guest OS, the VM previously failed to boot. This occurred on hosts that use AMD EPYC series CPUs. Now, the underlying code has been fixed and VMs boot as expected in the described circumstances.

Bugzilla:2168082[1]

nodedev-dumpxml lists attributes correctly for certain mediated devices

Before this update, the **nodedev-dumpxml** utility did not list attributes correctly for mediated devices that were created using the **nodedev-create** command. This has been fixed, and **nodedev-dumpxml** now displays the attributes of the affected mediated devices properly.

Bugzilla:2143158

virtiofs devices can now be attached after restarting virtqemud or libvirtd

Previously, restarting the **virtqemud** or **libvirtd** services prevented **virtiofs** storage devices from being attached to virtual machines (VMs) on your host. This bug has been fixed, and you can now attach **virtiofs** devices in the described scenario as expected.

Bugzilla:2078693

blob resources now work correctly for virtio-gpu on IBM Z

Previously, the **virtio-gpu** device was incompatible with **blob** memory resources on IBM Z systems. As a consequence, if you configured a virtual machine (VM) with **virtio-gpu** on an IBM Z host to use **blob** resources, the VM did not have any graphical output.

With this update, **virtio** devices have an optional **blob** attribute. Setting **blob** to **on** enables the use of **blob** resources in the device. This prevents the described problem in **virtio-gpu** devices, and can also accelerate the display path by reducing or eliminating copying of pixel data between the guest and host. Note that **blob** resource support requires QEMU version 6.1 or later.

Jira:RHEL-7135

Resuming a postcopy VM migration now works correctly.

Previously, when performing a postcopy migration of a virtual machine (VM), if a proxy network failure occurred during the RECOVER phase of the migration, the VM became unresponsive and the migration could not be resumed. Instead, the recovery command displayed the following error:

```
error: Requested operation is not valid: QEMU reports migration is still running
```

With this update, this problem has been fixed and poscopy migrations now resume correctly in the described circumstances.

Jira:RHEL-7115

Reinstalling virtio-win drivers no longer causes DNS configuration to reset on the guest

In virtual machines (VMs) that use a Windows guest operating system, reinstalling or upgrading **virtio-win** drivers for the network interface controller (NIC) previously caused DNS settings in the guest to reset. As a consequence, your Windows guest in some cases lost network connectivity.

With this update, the described problem has been fixed. As a result, if you reinstall or upgrade from the latest version of **virtio-win**, the problem no longer occurs. Note, however, that upgrading from a prior version of **virtio-win** will not fix the problem, and DNS resets might still occur in your Windows guests.

Jira:RHEL-1860[1]

VNC viewer correctly initializes a VM display after live migration of ramfb

This update enhances the **ramfb** framebuffer device, which you can configure as a primary display for a virtual machine (VM). Previously, **ramfb** was unable to migrate, which resulted in VMs that use **ramfb**

showing a blank screen after live migration. Now, **ramfb** is compatible with live migration. As a result, you see the VM desktop display when the migration completes.

Jira:RHEL-7478

Setting static IP in a RHEL virtual machine on a VMware host now works correctly

Previously, when using RHEL as a guest operating system of a virtual machine (VM) on a VMware host, the DatasourceOVF function did not work correctly. As a consequence, if you used the **cloud-init** utility to set the VM's network to static IP and then rebooted the VM, the VM's network was changed to DHCP. This problem has been fixed, and VMs now set static IP as expected in the described scenario.

Jira:RHEL-12122

8.16. SUPPORTABILITY

The sos clean on an existing archive no longer fails

Previously, an existing archive could not be cleaned by running **sos clean** due to a regression in the **sos** code that incorrectly detected the root directory of a tarball and prevented it from cleaning data. As a consequence, **sos clean** running on an existing sosreport tarball does not clean anything within the tarball. This update adds an implementation of a proper detection of the root directory in the reordered tarball content. As a result, **sos clean** performs sensitive data obfuscation on an existing sosreport tarball correctly.

Jira:RHEL-35945

The sos stops collecting user's .ssh configuration

Previously, the **sos** utility collected the **.ssh** configuration by default from a user. As a consequence, this action caused a broken system for users that are mounted by using automount utility. With this update, the **sos** utility no longer collects the **.ssh** configuration.

Jira:RHEL-22389

8.17. CONTAINERS

Netavark no longer fails resolving DNS TCP queries

Previously, when you ran a container in a Podman network, some domain names would not resolve even though they worked on the host system or in a container not using the Podman network. With this update, Netavark supports TCP DNS queries and the problem is fixed.

Jira:RHEL-52246

CHAPTER 9. 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.

9.1. INSTALLER AND IMAGE CREATION

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]

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]

Boot loader installation and configuration via 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 via the **bootupd**/**bootupctl** tool contained within the container image, even without an explicit boot loader configuration in Kickstart.

Jira:RHEL-17205[1]

The bootc image builder tool is available as a Technology Preview

The **bootc image builder** tool, now available as a Technology Preview, works as a container to easily create and deploy compatible disk images from the **bootc** container inputs. After running your container image with **bootc image builder**, you can generate images for the architecture that you need. Then, you can deploy the resulting image on VMs, clouds, or servers. You can easily update the images with the bootc, instead of having to regenerate the content with **bootc image builder** every time a new update is required.

Jira:RHELDOCS-17468[1]

A new rhel9/bootc-image-builder container image is available as a Technology Preview

The rhel9/bootc-image-builder container image for image mode for RHEL includes a minimal version of image builder that converts bootable container images, for example rhel-bootc, to different disk image formats, such as QCOW2, AMI, VMDK, ISO, and others.

Jira:RHELDOCS-17733[1]

9.2. SECURITY

gnutls now uses kTLS as a 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.

Bugzilla:2108532[1]

OpenSSL clients can use the QUIC protocol as a 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]

The io_uring interface is available as a 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]

9.3. RHEL FOR EDGE

FDO now provides storing and querying Owner Vouchers from a SQL backend as a Technology Preview

With this Technology Preview, FDO **manufacturer-server**, **onboarding-server**, and **rendezvous-server** are available for storing and querying Owner Vouchers from a SQL backend. As a result, you can select a

SQL datastore in the FDO servers options, along with credentials and other parameters, to store the Owner Vouchers.

Jira:RHELDOCS-17752[1]

9.4. SHELLS AND COMMAND-LINE TOOLS

GIMP available as a Technology Preview in RHEL 9

GNU Image Manipulation Program (GIMP) 2.99.8 is now available in RHEL 9 as a Technology Preview. The **gimp** package version 2.99.8 is a pre-release version with a set of improvements, but a limited set of features and no guarantee for stability. As soon as the official GIMP 3 is released, it will be introduced into RHEL 9 as an update of this pre-release version.

In RHEL 9, you can install **gimp** easily as an RPM package.

Bugzilla:2047161[1]

9.5. INFRASTRUCTURE SERVICES

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.

Bugzilla:2113900

9.6. 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]

WireGuard VPN is available as a Technology Preview

WireGuard, which Red Hat provides as an unsupported Technology Preview, is a high-performance VPN solution that runs in the Linux kernel. It uses modern cryptography and is easier to configure than other VPN solutions. Additionally, the small code-basis of WireGuard reduces the surface for attacks and, therefore, improves the security.

For further details, see Setting up a WireGuard VPN.

Bugzilla:1613522[1]

kTLS available as a Technology Preview

RHEL provides kernel Transport Layer Security (KTLS) 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.

Bugzilla:1570255[1]

The systemd-resolved service is available as a Technology Preview

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

Note that **systemd-resolved** is an unsupported Technology Preview.

Bugzilla:2020529

The PRP and HSR protocols are now available as a Technology Preview

This update adds the **hsr** kernel module that 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 zero-loss redundancy in Ethernet networks.

Bugzilla:2177256[1]

NetworkManager and the Nmstate API support MACsec hardware offload

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

Offloading IPsec encapsulation to a NIC is now available as a 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.

Bugzilla:2178699[1]

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 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.

Bugzilla:2023416[1]

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_nicpf

Marvell OcteonTX2 NIC Physical Function driver

rvu_nicvf

Marvell OcteonTX2 NIC Virtual Function driver

rvu_nicvf

Marvell OcteonTX2 RVU Admin Function driver

Bugzilla:2040643[1]

Network drivers for modems in RHEL are available as Technology Preview

Device manufacturers support Federal Communications Commission (FCC) locking as the default setting. FCC provides a lock to bind WWAN drivers to a specific system where WWAN drivers provide a channel to communicate with modems. Based on the modem PCI ID, manufacturers integrate unlocking tools on Red Hat Enterprise Linux for ModemManager. However, a modem remains unusable if not unlocked previously even if the WWAN driver is compatible and functional. Red Hat Enterprise Linux provides the drivers for the following modems with limited functionality as a Technology Preview:

- Qualcomm MHI WWAM MBIM - Telit FN990Axx
- Intel IPC over Shared Memory (IOSM) - Intel XMM 7360 LTE Advanced
- Mediatek t7xx (WWAN) - Fibocom FM350GL
- Intel IPC over Shared Memory (IOSM) - Fibocom L860GL modem

Jira:RHELDOCS-16760[1], Jira:RHEL-6564, Bugzilla:2110561, Bugzilla:2123542, Bugzilla:2222914

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.

Bugzilla:2186375[1]

kTLS rebased to version 6.3

The kernel Transport Layer Security (KTLS) functionality is a Technology Preview. In RHEL 9.3, kTLS was rebased to the 6.3 upstream version, and notable changes include:

- Added the support for 256-bit keys with TX device offload
- Delivered various bug fixes

Bugzilla:2183538[1]

Soft-RoCE available as a Technology Preview

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) is a network protocol that implements RDMA over Ethernet. Soft-RoCE is the software implementation of RoCE which maintains two protocol versions, RoCE v1 and RoCE v2. The Soft-RoCE driver, **rdma_rxe**, is available as an unsupported Technology Preview in RHEL 9.

Note that Soft-RoCE is deprecated since RHEL 9.5 and will be removed in RHEL 10.

9.7. KERNEL

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]

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]

9.8. FILE SYSTEMS AND STORAGE

NVMe-oF Discovery Service features are now fully supported

The NVMe-oF Discovery Service features, defined in the NVMexpress.org Technical Proposals (TP) 8013 and 8014 was introduced in Red Hat Enterprise Linux 9.0 as a Technology Preview, is now fully supported. 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.

Bugzilla:2021672[1]

nvme-stas package 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**).

Bugzilla:1893841[1]

9.9. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

9.10. COMPILERS AND DEVELOPMENT TOOLS

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.

Bugzilla:1980981

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]

9.11. IDENTITY MANAGEMENT

DNSSEC available as Technology Preview in IdM

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.

Bugzilla:2084180

HSM support is available as a Technology Preview

Hardware Security Module (HSM) support is now available in Identity Management (IdM) as a Technology Preview. You can store your key pairs and certificates for your IdM CA and KRA on an HSM. This adds physical security to the private key material.

IdM relies on the networking features of the HSM to share the keys between machines to create replicas. The HSM provides additional security without visibly affecting most IPA operations. When using low-level tooling the certificates and keys are handled differently but this is seamless for most users.

NOTE

Migration of an existing CA or KRA to an HSM-based setup is not supported. You need to reinstall the CA or KRA with keys on the HSM.

You need the following:

- A supported HSM
- The HSM PKCS #11 library
- An available slot, token, and the token password

To install a CA or KRA with keys stored on an HSM, you must specify the token name and the path to the PKCS #11 library. For example:

```
ipa-server-install -r EXAMPLE.TEST -U --setup-dns --allow-zone-overlap --no-forwarders -N --auto-reverse --random-serial-numbers —token-name=HSM-TOKEN --token-library-path=/opt/nfast/toolkits/pkcs11/libcknfast.so --setup-kra
```

Jira:RHELDOCS-17465[1]

LMDB database type is available in Directory Server as a Technology Preview

The Lightning Memory-Mapped Database (LMDB) is available in Directory Server as an unsupported Technology Preview.

Currently, you can use only the command line to migrate or install instances with LMDB.

To migrate existing instances from Berkeley Database (BDB) to LMDB, use the **dsctl *instance_name* dblib bdb2mdb** command that sets the **nsslapd-backend-implement** parameter value to **mdb**. Note that this command does not clean up the old data. You can revert the database type by changing **nsslapd-backend-implement** back to **bdb**. For more details, see Migrating the database type from BDB to LMDB on an existing DS instance.

Important

Before migrating existing instances from BDB to LMDB, backup your databases. For more details, see Backing up Directory Server.

To create a new instance with the LMDB, you can use either of the following methods:

- In the interactive installer, set **mdb** in the **Choose whether mdb or bdb is used**line. For more details, see Creating an instance using the interactive installer .
- In the **.inf** file, set **db_lib = mdb** in the **[slapd]** section. For more details, see Creating a **.inf** file for a Directory Server instance installation.

Directory Server stores LMDB settings under the **cn=mdb,cn=config,cn=ldbm database,cn=plugins,cn=config** entry that includes with the following new configuration parameters:

- **nsslapd-mdb-max-size** sets the database maximum size in bytes.
  Important: Make sure that **nsslapd-mdb-max-size** is high enough to store all intended data. However, the parameter size must not be too high to impact the performance because the database file is memory-mapped.
- **nsslapd-mdb-max-readers** sets the maximum number of read operations that can be opened at the same time. Directory Server autotunes this setting.
- **nsslapd-mdb-max-dbs** sets the maximum number of named database instances that can be included within the memory-mapped database file.

Along with the new LMDB settings, you can still use the **nsslapd-db-home-directory** database configuration parameter.

In case of mixed implementations, you can have BDB and LMDB replicas in your replication topology.

Jira:RHELDOCS-19061[1]

ACME supports automatically removing expired certificates as a Technology Preview

The Automated Certificate Management Environment (ACME) service in Identity Management (IdM) adds an automatic mechanism to purge expired certificates from the certificate authority (CA) as a Technology Preview. As a result, ACME can now automatically remove expired certificates at specified intervals.

With this enhancement, ACME can now automatically remove expired certificates at specified intervals.

Removing expired certificates is disabled by default. To enable it, enter:

```
# ipa-acme-manage pruning --enable --cron "0 0 1 * *"
```

This removes expired certificates on the first day of every month at midnight.

NOTE

Expired certificates are removed after their retention period. By default, this is 30 days after expiry.

For more details, see the **ipa-acme-manage(1)** man page.

Jira:RHELPLAN-145900

IdM-to-IdM migration is available as a Technology Preview

IdM-to-IdM migration is available in Identity Management as a Technology Preview. You can use a new **ipa-migrate** command to migrate all IdM-specific data, such as SUDO rules, HBAC, DNA ranges, hosts, services, and more, to another IdM server. This can be useful, for example, when moving IdM from a development or staging environment into a production one or when migrating IdM data between two production servers.

Jira:RHELDOCS-18408[1]

9.12. 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 VNC. 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.

Certain applications, such as LibreOffice, only provide a command-line interface, and their graphical interface is disabled.

Jira:RHELPLAN-27394[1]

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 VNC. 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.

Certain applications, such as LibreOffice, only provide a command-line interface, and their graphical interface is disabled.

Jira:RHELPLAN-27737[1]

9.13. THE WEB CONSOLE

The RHEL web console can now manage WireGuard connections

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]

9.14. VIRTUALIZATION

Creating nested virtual machines

Nested KVM virtualization is provided as a Technology Preview for KVM virtual machines (VMs) running on Intel, AMD64, and IBM Z 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]

AMD SEV, SEV-ES, and SEV-SNP for KVM virtual machines

As a Technology Preview, RHEL 9 provides the Secure Encrypted Virtualization (SEV) feature for AMD EPYC host machines that use the KVM hypervisor. If enabled on a virtual machine (VM), SEV encrypts the VM's memory to protect the VM from access by the host. This increases the security of the VM.

In addition, the enhanced Encrypted State version of SEV (SEV-ES) is also provided as Technology Preview. SEV-ES encrypts all CPU register contents when a VM stops running. This prevents the host from modifying the VM's CPU registers or reading any information from them.

RHEL 9.5 and later also provides the Secure Nested Paging (SEV-SNP) feature as Technology Preview. SNP enhances SEV and SEV-ES by improving its memory integrity protection, which helps prevent hypervisor-based attacks, such as data replay or memory re-mapping.

Note that SEV and SEV-ES work only on the 2nd generation of AMD EPYC CPUs (codenamed Rome) or later. Similarly, SEV-SNP works only on 4rd generation AMD EPYC CPUs (codenamed Genoa) or later. Also note that RHEL 9 includes SEV, SEV-ES, and SEV-SNP encryption, but not the SEV, SEV-ES, and SEV-SNP security attestation and live migration.

Jira:RHELPLAN-65217[1]

Intel TDX in RHEL guests

As a Technology Preview, the Intel Trust Domain Extension (TDX) feature can now be used in RHEL 9.2 and later guest operating systems. If the host system supports TDX, you can deploy hardware-isolated RHEL 9 virtual machines (VMs), called trust domains (TDs). Note, however, that TDX currently does not work with **kdump**, and enabling TDX will cause **kdump** to fail on the VM.

Bugzilla:1955275[1]

A unified kernel image of RHEL is now available as a Technology Preview

As a Technology Preview, you can now obtain the RHEL kernel as a unified kernel image (UKI) for virtual machines (VMs). A unified kernel image combines the kernel, initramfs, and kernel command line into a single signed binary file.

UKIs can be used in virtualized and cloud environments, especially in confidential VMs where strong SecureBoot capabilities are required. The UKI is available as a **kernel-uki-virt** package in RHEL 9 repositories.

Currently, the RHEL UKI can only be used in a UEFI boot configuration.

Bugzilla:2142102[1]

CPU clusters on 64-bit ARM

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]

Live migrating a VM with a Mellanox virtual function is now available as a Technology Preview

As a Technology Preview, you can now live migrate a virtual machine (VM) with an attached virtual function (VF) of a Mellanox networking device.

This feature is currently available only on a Mellanox CX-7 networking device. The VF on the Mellanox CX-7 networking device uses a new **mlx5_vfio_pci** driver, which adds functionality that is necessary for the live migration, and **libvirt** binds the new driver to the VF automatically.

Jira:RHEL-13007[1]

9.15. RHEL IN CLOUD ENVIRONMENTS

RHEL is now available on Azure confidential VMs as a Technology Preview

With the updated RHEL kernel, you can now create and run RHEL confidential virtual machines (VMs) on Microsoft Azure as a Technology Preview. The newly added unified kernel image (UKI) now enables booting encrypted confidential VM images on Azure. The UKI is available as a **kernel-uki-virt** package in RHEL 9 repositories.

Currently, the RHEL UKI can only be used in a UEFI boot configuration.

Jira:RHELPLAN-139800[1]

9.16. CONTAINERS

composefs filesystem is available as a Technology Preview

The key technologies **composefs** uses are:

- OverlayFS as the kernel interface
- Enhanced Read-Only File System (EROFS) for a mountable metadata tree
- The **fs-verity** feature (optional) from the lower filesystem

Key advantages of **composefs**:

- Separation between metadata and data. **composefs** does not store any persistent data. The underlying metadata and data files are stored in a valid lower Linux filesystem such as **ext4**, **xfs**, **btrfs**, and so on.
- Mounting multiple **composefs** with a shared storage.
- Data files are shared in the page cache to enable multiple container images to share their memory.
- Support **fs-verity** validation of the content files.

Jira:RHEL-52237

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]

A new rhel9/rhel-bootc container image is available as a Technology Preview

The **rhel9/rhel-bootc** container image is now available in the Red Hat Container Registry as a Technology Preview. With the RHEL bootable container images, you can build, test, and deploy an operating system exactly as a container. The RHEL bootable container images differ from the existing application Universal Base Images (UBI) thanks to the following enhancements: RHEL bootable container images contain additional components necessary to boot, such as, kernel, initrd, boot loader, firmware, between others. There are no changes to existing container images. For more information, see Red Hat Ecosystem Catalog .

Jira:RHELDOCS-17803[1]

Pushing and pulling images compressed with zstd:chunked is available as a Technology Preview

The **zstd:chunked** compression is now available as a Technology Preview.

Jira:RHEL-32267

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. 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.

Bugzilla:1899167[1]

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.

Bugzilla:1979521

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.

Bugzilla:2127473

Capturing screenshots from the Anaconda GUI with a global hot key is deprecated

Previously, users could capture screenshots of the Anaconda GUI by using a global hot key. This meant that users could extract the screenshots manually from the installation environment for any further usage. This functionality has been deprecated.

Jira:RHELDOCS-17166[1]

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 the future major RHEL release.

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

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 RAM disk has already been loaded. As a consequence, an updated version of the driver cannot be applied to the installation environment.

As a 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

10.2. 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.

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, SHB-DSA, ML-DSA, and FN-DSA.

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]

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.

Bugzilla:2054740

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]

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.

Bugzilla:2168665

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]

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.

Bugzilla:1995600[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.

Bugzilla:2034569

10.3. 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

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.

Bugzilla:2163716

10.4. 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. SHELLS AND COMMAND-LINE TOOLS

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 or low levels for a host or interface are reached.

Jira:RHELDOCS-18959[1]

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.

Bugzilla:1997366[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

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]

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 running ReaR. For example, run the **export TMPDIR=...** statement and then run the **rear** command in the same shell session or script.

Jira:RHELDOCS-18049[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 and 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. INFRASTRUCTURE SERVICES

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]

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]

10.7. 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

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.

Bugzilla:1935544[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 .

Bugzilla:1894877[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.

Bugzilla:2089200

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 might 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]

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]

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.

Bugzilla:2013884[1]

The rdma_rxe Soft-RoCE driver is deprecated

Software Remote Direct Memory Access over Converged Ethernet (Soft-RoCE), also known as RXE, is a feature that emulates Remote Direct Memory Access (RDMA). Since RHEL 9.3, the Soft-RoCE feature is available as a Technology Preview. Furthermore, this feature has been deprecated and will be removed in RHEL 10.

Jira:RHELDOCS-19774[1]

10.8. KERNEL

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 .

Bugzilla:2058153

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? .

Bugzilla:2113873[1]

10.9. 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]

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.

Bugzilla:2038183

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]

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 the event 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

10.10. HIGH AVAILABILITY AND CLUSTERS

Deprecated high availability features

The following features have been deprecated in 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 specific maintenance support lifecycles.

Jira:RHELDOCS-19022[1]

10.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

libdb has been deprecated

RHEL 8 and 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

Bugzilla:1927780[1], Bugzilla:1974657, Jira:RHELPLAN-80695

10.12. COMPILERS AND DEVELOPMENT TOOLS

Redis will be replaced with Valkey in Grafana, PCP, and grafana-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]

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.

Bugzilla:2111072

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.

Bugzilla:2092016[1]

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]

10.13. 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]

BDB backend is deprecated in 389-ds-base

The **libdb** library that implements the Berkeley Database (BDB) version used by **389-ds-base** is deprecated in RHEL 9.0. As a result, Directory Server deprecated the BDB backend. Support for BDB will be removed in the future major version of Directory Server.

As a replacement, Directory Server can now create instances with Lightning Memory-Mapped Database (LMDB) available as a Technology Preview.

Jira:RHELDOCS-19064[1]

OpenSSL deprecates MD2, MD4, MDC2, Whirlpool, Blowfish, CAST, DES, IDEA, RC2, RC4, RC5, SEED, and PBKDF1

The OpenSSL project has deprecated a set of cryptographic algorithms because they are insecure, uncommonly used, or both. Red Hat also discourages the use of those algorithms, and RHEL 9 provides them for migrating encrypted data to use new algorithms. Users must not depend on those algorithms for the security of their systems.

The implementations of the following algorithms have been moved to the legacy provider in OpenSSL: MD2, MD4, MDC2, Whirlpool, Blowfish, CAST, DES, IDEA, RC2, RC4, RC5, SEED, and PBKDF1.

See the **/etc/pki/tls/openssl.cnf** configuration file for instructions on how to load the legacy provider and enable support for the deprecated algorithms.

Bugzilla:1975836

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

10.14. 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]

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]

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:SSSD-6596

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:SSSD-6601

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]

10.15. 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 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 is removed

The Eye of GNOME (**eog**) image viewer application is removed in RHEL 10.

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]

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]

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]

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]

Evince is deprecated

The Evince has been deprecated and will be removed in a future major release.

Jira:RHELDOCS-19141[1]

The GNOME Terminal is deprecated

The GNOME Terminal has been deprecated and will be removed in a future major release.

Jira:RHELDOCS-19156[1]

10.16. 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]

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]

10.17. 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]

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.

Bugzilla:1999770

10.18. 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

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.

Bugzilla:1935497[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.

Bugzilla:1965079

QCOW2-v2 image format is deprecated

With RHEL 9, 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 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.

Bugzilla:1951814

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]

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]

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'
```

Bugzilla:2060839

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]

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]

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.

Bugzilla:2206599[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

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 also removed support for using these versions as a guest operating system in this update.

- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

Jira:RHEL-11810

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]

10.19. 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]

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.

Bugzilla:2069279[1]

rhel9/pause has been deprecated

The **rhel9/pause** container image has been deprecated.

Bugzilla:2106816

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 via 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 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]

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 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]

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

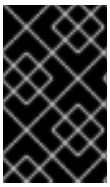
The **rhel9/openssl** container image has been deprecated.

Jira:RHELDOCS-18106[1]

10.20. 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
- 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
- babl
- 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
- 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
- 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
- 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
- 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
- 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
- jboss-jaxrs-2.0-api
- jboss-logging
- jboss-logging-tools
- jdeparser
- 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
- 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
- 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

- librepository
- librevenge
- librevenge-gdb
- libserializer
- libsigc++20
- libsigsegv
- libsmbios
- libsoup
- libsoup-devel
- libstaroffice
- libstemmer
- libstoragemgmt-smis-plugin
- libteam
- libuser
- libuser-devel
- libvisio
- libvisual
- 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
- 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-utils
- openal-soft
- openchange
- openscap-devel
- openscap-python3
- openslp-server
- 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-netifaces
- python3-nispor
- python3-py
- python3-pycdlib
- python3-pycurl
- 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
- runc
- saab-fonts
- sac
- scap-workbench
- sendmail
- sendmail-cf
- sendmail-doc
- setxkbmap
- sgabios
- sgabios-bin
- sil-scheherazade-fonts
- spamassassin
- speech-tools-libs

- suitesparse
- sushi
- team
- teamd
- 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
- tracer-common
- ucs-miscfixed-fonts
- usb_modeswitch
- usb_modeswitch-data
- usbredir-server

- webkit2gtk3
- webkit2gtk3-devel
- webkit2gtk3-jsc
- webkit2gtk3-jsc-devel
- wpebackend-fdo
- wpebackend-fdo-devel
- 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
- yelp
- yelp-libs
- yp-tools
- ypbind
- ypserv
- zhongyi-song-fonts

CHAPTER 11. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 9.5.

11.1. INSTALLER AND IMAGE CREATION

The auth and authconfig Kickstart commands require the AppStream repository

The **authselect-compat** package is required by the **auth** and **authconfig** Kickstart commands during installation. Without this package, the installation fails if **auth** or **authconfig** are used. However, by design, the **authselect-compat** package is only available in the AppStream repository.

To work around this problem, verify that the BaseOS and AppStream repositories are available to the installation program or use the **authselect** Kickstart command during installation.

Bugzilla:1640697[1]

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.

Bugzilla:1697896[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.

To work around this problem, 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.

Bugzilla:2050140

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.

As a 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 .

Bugzilla:1877697[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.

To work around this problem, use the **harddrive --partition=sdX --dir=**/ command to install from USB CD-ROM drive. As a result, the installation does not fail.

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.

To work around this problem, 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

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.

To work around this problem, 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.

Bugzilla:2047713

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.

To work around this problem, you can use another filesystem for **/boot**, for example ext4.

Bugzilla:1997832[1]

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 is aborted with the following error:

```
The command 'mount --bind /mnt/sysimage/data /mnt/sysroot/data' exited with the code 32.
```

To work around this issue:

- Use an automatic partitioning scheme and do not add any mount points manually.
- Manually assign mount points only inside **/var** directory. For example, **/var/*my-mount-point***), and 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.

As a 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**.

Bugzilla:2115783[1]

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.

To work around this problem:

- 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.

Bugzilla:2173992

Images built with the stig profile remediation fails 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

Driver disk menu fails to display user inputs on the console

When you start RHEL installation using the **inst.dd** option on the kernel command line with a driver disk, the console fails to display the user input. Consequently, it appears that the application does not respond to the user input and stops responding, but displays the output which is confusing for users. However, this behavior does not affect the functionality, and user input gets registered after pressing **Enter**.

As a workaround, to see the expected results, ignore the absence of user inputs in the console and press **Enter** when you finish adding inputs.

Jira:RHEL-4737

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>
```

To work around this problem, include the given 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]

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. To work around this issue, 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-beta/rhel-bootc:9.4 containers-storage:registry.redhat.io/rhel9-beta/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-beta/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

bootc-image-builder does not support building images from private registries

Currently, you cannot build base disk images which come from private registries by using **bootc-image-builder**. To work around this issue, copy the private registry into your localhost, then build the image with the following arguments:

- **--local**

- **localhost/<image name>:tag** as the image

For example, to build your image:

```
sudo podman run \
--rm \
-it \
--privileged \
--pull=newer \
--security-opt label=type:unconfined_t \
-v ./config.toml:/config.toml \
-v ./output:/output \
-v /var/lib/containers/storage:/var/lib/containers/storage \
registry.redhat.io/rhel9/bootc-image-builder:latest
--type qcow2 \
--local \
quay.io/<namespace>/<image>:<tag>
```

Jira:RHELDOCS-18720[1]

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.

As a work around, 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

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.

As a 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

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. To work around this problem, use the **firewall --disabled** command instead. As a result, the **firewalld** service is disabled properly.

Jira:RHEL-82566

11.2. 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.

To work around this problem, configure servers and clients to use TLS version 1.2 as the highest TLS protocol version available.

Bugzilla:1681178[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.

To work around the problem, 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.

Bugzilla:1685470[1]

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

To work around this problem, 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**

Bugzilla:2056884

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.
```

To work around this problem, 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

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

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. To work around this problem, use just one certificate instead of multiple certificates.

Jira:RHELPLAN-157225[1]

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**. To work around the problem, 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. To work around this problem, 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]

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. To work around this problem, restart **fapolicyd** or run the Ansible DISA STIG profile again.

Jira:RHEL-24345[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]

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 by using the **openssl** CA tool. The X.509 v1 format does not meet current web requirements.

Jira:RHEL-40605

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

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**.

Bugzilla:2064274

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. As a 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.

Bugzilla:2038978

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.

To work around this problem, 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.

Bugzilla:2070722

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**

For more details and more workarounds, see the related Knowledgebase article.

Bugzilla:2161499

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 noncompliant state. As a workaround, you can scan and remediate the system after the Kickstart installation. This will fix the service-related issues.

Jira:RHELPLAN-44202[1]

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]

Missing rules in the SELinux policy block permissions to SQL databases

Missing permission rules from the SELinux policy block connections to SQL databases. Consequently, the FIDO Device Onboard (FDO) services **fdo-manufacturing-server.service**, **fdo-owner-onboarding-server.service**, and **fdo-rendezvous-server.service** cannot connect to FDO databases, such as PostgreSQL and SQLite. Therefore, the system cannot start the FDO by using the supported databases for credentials and other parameters, such as storing ownership vouchers.

You can work around this problem by performing the following steps:

1. Create a new file named **local_fdo_update.cil** and enter the missing SELinux policy rules:

```
(allow fdo_t etc_t (file (write)))
(allow fdo_t fdo_conf_t (file (append create rename setattr unlink write )))
(allow fdo_t fdo_var_lib_t (dir (add_name remove_name write )))
(allow fdo_t fdo_var_lib_t (file (create setattr unlink write )))
(allow fdo_t krb5_keytab_t (dir (search)))
(allow fdo_t postgresql_port_t (tcp_socket (name_connect)))
(allow fdo_t sssd_t (unix_stream_socket (connectto)))
(allow fdo_t sssd_var_run_t (sock_file (write)))
```

2. Install the policy module package:

```
# semodule -i local_fdo_update.cil
```

As a consequence, FDO can connect to the PostgreSQL database and also fix problems related to SQLite permissions over **/var/lib/fdo/**, where the SQLite database files are expected to be located.

Jira:RHEL-28814

OpenSSH in RHEL 9.0-9.3 is not compatible with OpenSSL 3.2.2

The **openssh** packages provided by RHEL 9.0, 9.1, 9.2, and 9.3 strictly check for the OpenSSL version. Consequently, if you upgrade the **openssl** packages to version 3.2.2 and higher and you keep the **openssh** packages in version 8.7p1-34.el9_3.3 or earlier, the **sshd** service fails to start with an **OpenSSL version mismatch** error message.

To work around this problem, upgrade the **openssh** packages to version 8.7p1-38.el9 and later. See the sshd not working, OpenSSL version mismatch solution (Red Hat Knowledgebase) for more information.

Jira:RHELDOCS-19626

11.3. SOFTWARE MANAGEMENT

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.
```

To work around this problem, restart the installation process.

Bugzilla:2073510

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. 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**.

Bugzilla:2056318

11.4. SHELLS AND COMMAND-LINE TOOLS

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.

Bugzilla:2053598[1]

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.

To work around this problem, install the **libxkbcommon** library:

```
# dnf install libxkbcommon
```

Jira:RHEL-6105

The %vmeff metric from the sysstat 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. To work around this problem, 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. Alternatively, to work around this problem, configure firewalls to block or filter traffic on UDP and TCP port 427.

Jira:RHEL-6995[1]

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.

To work around this problem, 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 boot loader of the recovered system is set to the **EFI** shim boot loader.

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]

11.5. INFRASTRUCTURE SERVICES

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.

Bugzilla:2070495

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. To work around this problem, 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.

Bugzilla:1984982

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.

Bugzilla:2086562

11.6. NETWORKING

Bluetooth device does not work properly after resuming from the suspend mode

When your system suspends or resumes, the **RTL8852BE** Wi-Fi card does not function properly. Consequently, you will notice either audio interruptions during the resume process or audio does not work properly after resuming from the suspend mode. As a workaround, you need to update RHEL Wi-Fi driver.

Jira:RHEL-24414[1]

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. To work around this problem, 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.

Bugzilla:2000616[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. To work around this problem, disable kTLS. As a result, with the workaround, it is possible to successfully update the session key.

Bugzilla:2013650[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. 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.

Bugzilla:2018112[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. 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.

Bugzilla:2082303

The iwl7260-firmware breaks Wi-Fi on Intel Wi-Fi 6 AX200, AX210, and Lenovo ThinkPad P1 Gen 4

After updating the **iwl7260-firmware** or **iwl7260-wifi** driver to the version provided by RHEL 9.1 and later, the hardware gets into an incorrect internal state. reports its state incorrectly. Consequently, Intel Wifi 6 cards might not work and display the 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
```

An unconfirmed workaround is to power off the system and back on again. Do not reboot.

Bugzilla:2129288[1]

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.

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. 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
```

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
```

Bugzilla:2167783[1]

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.

As a 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.

Bugzilla:2181571[1]

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.

As a 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.

Bugzilla:2132480[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. As a 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]

The kdump mechanism fails to capture the vmcore file on LUKS-encrypted targets

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.

As a workaround, query the **Recommended crashkernel value** and gradually increase the memory size to an appropriate value. The **Recommended crashkernel value** can serve as reference to set the required memory size.

1. Print the estimate 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 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
```

Bugzilla:2064708

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.

To work around the problem, build or put the extra modules against the latest stock kernel before you install the new kernel.

Bugzilla:2103605[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 stops responding. As a consequence, EEH causes the device to fail permanently.

Jira:RHEL-15404[1]

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 KB and 64 KB 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. To work around this problem, 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]

11.8. 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.

Bugzilla:2033080[1]

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. To work around this problem, 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.

Bugzilla:2011699[1]

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.

To work around this issue, disable quota accounting by remounting the filesystem, with the quota option removed.

Bugzilla:2160619[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.

Bugzilla:2185048

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. To work around this issue, 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]

Kernel panic while using the qedi driver

While using the **qedi** iSCSI driver, the kernel panics after the operating system boots. To work around this issue, disable the **kfence** runtime memory error detector feature by adding **kfence.sample_interval=0** to the kernel boot command line.

Jira:RHEL-8466[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. To work around this issue, remove the **vdo** package and its dependencies before attempting to update.

Jira:RHEL-8354

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 aborted with an error, for example, **[qedf_eh_abort:xxxx]:1: Aborting io_req=ff5d85a9dcf3xxxx**.

To work around this problem, 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. To work around this problem, 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]

RHEL installation program does not automatically discover or use iSCSI devices as boot devices on aarch64

The absence of the **iscsi_ibft** kernel module in RHEL installation program running on aarch64 prevents automatic discovery of iSCSI devices defined in firmware. These devices are not automatically visible in the installation program nor selectable as boot devices when added manually by using the GUI. As a workaround, add the "inst.nonibftiscsiboot" parameter to the kernel command line when booting the installation program and then manually attach iSCSI devices through the GUI. As a result, the installation program can recognize the attached iSCSI devices as bootable and installation completes as expected.

For more information, see KCS solution.

Jira:RHEL-56135[1]

11.9. 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]

11.10. 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.

Bugzilla:2157708

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 Installing the system in FIPS mode.
- Alternatively, you can switch FIPS mode for the entire RHEL system by following the procedure in Switching the system to FIPS mode .

Bugzilla:1991500

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.

To work around this problem, explicitly mark the repository as safe by executing the following command:

```
git config --global --add safe.directory /path/to/repository
```

Jira:RHELDOCS-18435[1]

11.11. 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.

To work around the problem, enable support for the SHA-1 algorithm on your RHEL 9 systems with the following command:

```
# update-crypto-policies --set DEFAULT:SHA1
```

Bugzilla:2060798

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. To work around the problem, 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 The DEFAULT:SHA1 subpolicy has to be set on RHEL 9 clients for PKINIT to work against AD KDCs.

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
```

Bugzilla:2057471

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.

To work around this problem, 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:RHEL-4889

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]

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. To work around this problem, see the following Knowledgebase article: Migrated IdM users unable to log in due to mismatching domain SIDs.

Jira:RHELPLAN-109613[1]

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.

If upgrading the host to RHEL 8 before installing an IdM client on it is not an option, work around the problem by removing 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

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]

dsconf config replace cannot handle multivalued attributes

Currently, the **dsconf config replace** command cannot set several values to a multivalued attribute, such as **nsslapd-haproxy-trusted-ip**.

To work around this issue, use the **ldapmodify** utility. For example, if you want to set several trusted IP addresses, run the following command:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x << EOF

dn: cn=config
changetype: modify
add: nsslapd-haproxy-trusted-ip
nsslapd-haproxy-trusted-ip: 192.168.0.1
nsslapd-haproxy-trusted-ip: 192.168.0.2
nsslapd-haproxy-trusted-ip: 192.168.0.3
EOF
```

Jira:RHEL-67004

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.

To work around this problem, change the MaxValRange setting in Active Directory to accommodate larger group sizes.

Jira:RHELDOCS-19603

11.12. 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 registers the DNS names properly

Previously, if the DNS was set up incorrectly, SSSD always failed the first attempt to register the DNS name. To work around the problem, this update provides a new parameter **dns_resolver_use_search_list**. Set **dns_resolver_use_search_list = false** to avoid using the DNS search list.

Bugzilla:1608496[1]

11.13. 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.

To work around the problem, 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.

Bugzilla:2060308

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.

To work around this problem, 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]

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

11.14. 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]

11.15. 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]

11.16. 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. To work around this problem, unmask the **firewalld.service**:

```
systemctl unmask firewalld.service
```

Bugzilla:2123859

Unable to register systems with environment names

The **rhc** system role fails to register the system when specifying environment names in **rhc_environment**. As a workaround, use environment IDs instead of environment names while registering.

Jira:RHEL-1172

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. To work around this problem, 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]

The mssql RHEL System Role cannot configure Microsoft SQL Server with AD integration

The Microsoft SQL Server service does not provide the **adutil** tool that the service requires for the integration with Active Directory (AD). Consequently, you cannot use the **mssql** RHEL System Role to configure this scenario on a RHEL 9 managed node. No workaround is available, and you can use the RHEL System Role only to configure Microsoft SQL Server without AD integration on RHEL 9.

Jira:RHELDOCS-17720[1]

11.17. 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.

To work around this problem, 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.

Bugzilla:2014229

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]

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. To work around these problems, manually turn on **erms** and **fsrm** in the BIOS of your host.

Bugzilla:2077767[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. To work around the problem, use the standard migration type, rather than post-copy migration.

Jira:RHEL-7335

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

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.

Bugzilla:2005173[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. To work around this problem, disable and re-enable the network adapter driver in the Windows Device Manager.

Jira:RHEL-11366

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.

Bugzilla:1915715

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 .

Bugzilla:2149989[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.

To work around this problem, 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**

To work around this problem, 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
```

To work around this issue, do not use AMD EPYC CPUs for NUMA node configurations.

Bugzilla:2176010

NFS failure during VM migration causes migration failure and source VM coredump

Currently, if the NFS service or server is shut down during virtual machine (VM) migration, the source virtual machine's QEMU is unable to reconnect to the NFS server when it starts running again. As a result, the migration fails and a coredump is initiated on the source VM. Currently, there is no workaround available.

Bugzilla:2058982

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 .

Bugzilla:2073872

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.

Bugzilla:1970830

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. To work around the problem, boot the VM with the **multi_queue** option enabled.

Jira:RHEL-1084[1]

Windows 11 VMs with a memory balloon device set might close unexpectedly during reboot

Currently, rebooting virtual machines (VMs) that use a Windows 11 guest operating system and a memory balloon device in some cases fails with a **DRIVER POWER STAT FAILURE** stop error. There is currently no workaround for this issue.

Jira:RHEL-935[1]

The virtio balloon driver sometimes does not work on Windows 10 VMs

Under certain circumstances, the virtio-balloon driver does not work correctly on virtual machines (VMs) that use a Windows 10 guest operating system. As a consequence, such VMs might not use their assigned memory efficiently. There is currently no workaround for this issue.

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.

To work around this problem, update the **virtio** drivers by using Windows Device Manager.

Jira:RHEL-574[1]

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]

Virtual machines incorrectly report an AMD SRSO vulnerability

RHEL 9.4 virtual machines (VMs) running on a RHEL 9 host with the AMD Zen 3 and 4 CPU architecture incorrectly report a vulnerability to a Speculative Return Stack Overflow (SRSO) attack:

```
# lscpu | grep rstack

Vulnerability Spec rstack overflow: Vulnerable: Safe RET, no microcode
```

The problem is caused by a missing **cpuid** flag and the vulnerability is in fact fully mitigated in VMs under the following conditions:

- You have the updated **linux-firmware** package on the host as described here: cve-2023-20569.
- The host kernel has the mitigation enabled, which is the default behavior. If the mitigation is enabled, **Safe RET** is displayed in the **lscpu** command output on the host.

Jira:RHEL-26152[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. As a 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

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

Kdump fails on virtual machines with AMD SEV-SNP

Currently, kdump fails on RHEL 9 virtual machines (VMs) that use the AMD Secure Encrypted Virtualization (SEV) with the Secure Nested Paging (SNP) feature. There is currently no workaround for this issue.

Jira:RHEL-10019[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. To work around this issue, use fewer than 128 core per vCPU.

Jira:RHELDOCS-18863[1]

11.18. RHEL IN CLOUD ENVIRONMENTS

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. Reboot the VM

Bugzilla:2059545[1]

Customizing RHEL 9 guests on ESXi sometimes causes networking problems

Currently, customizing a RHEL 9 guest operating system in the VMware ESXi hypervisor does not work correctly with NetworkManager key files. As a consequence, if the guest is using such a key file, it will have incorrect network settings, such as the IP address or the gateway.

For details and workaround instructions, see the VMware Knowledge Base.

Bugzilla:2037657[1]

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.

Bugzilla:2081114[1]

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.

To work around the problem, 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]

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]

11.19. 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
```

Bugzilla:1869561[1]

11.20. CONTAINERS

Podman and bootc do not share the same registry login process

Podman and **bootc** use different registry login processes when pulling images. As a consequence, if you login to an image by using Podman, logging to a registry for **bootc** will not work on that image. When you install an image mode for RHEL system, and login to registry.redhat.io by using the following command:

```
# podman login registry.redhat.io <username_password>
```

And then you attempt to switch to the **registry.redhat.io/rhel9/rhel-bootc** image with the following command:

```
# bootc switch registry.redhat.io/rhel9/rhel-bootc:9.4
```

You should be able to see the following message:

```
Queued for next boot: registry.redhat.io/rhel9/rhel-bootc:9.4
```

However, an error is displayed:

```
ERROR Switching: Pulling: Creating importer: Failed to invoke skopeo proxy method OpenImage:
remote error: unable to retrieve auth token: invalid username/password: unauthorized: Please login to
the Red Hat Registry using your Customer Portal credentials. Further instructions can be found here:
https://access.redhat.com/RegistryAuthentication
```

To work around this issue, follow the steps Configuring container pull secrets to use authenticated registries with **bootc**.

Jira:RHELDOCS-18471[1]

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.
```

To work around this problem, 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]

Root filesystem are not expanded by default

When you use a base container image, that does not include **cloud-init** to create an AMI or QCOW2 container image by using **bootc-image-builder**, the root filesystem size is not expanded dynamically on boot to the full size of the provisioned virtual disk.

To work around this issue, apply one of the following available options:

- Include **cloud-init** in the image.
- Include custom logic in the container image to expand the root filesystem, for example:

```
/usr/bin/growpart /dev/vda 4
unshare -m bin/sh -c 'mount -o remount,rw /sysroot && xfs_growfs /sysroot'
```

- Include a custom logic to use the additional space for secondary filesystems, for example, **/var/lib/containers**.

NOTE

By default, the physical root storage is mounted at the /**sysroot** partition.

Jira:RHEL-33208

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-31777, Jira:RHEL-17511, Jira:RHEL-49454, Jira:RHEL-49458, Jira:RHEL-5108, Jira:RHEL-5115, Jira:RHEL-5131, Jira:RHEL-33087, Jira:RHEL-67004
NetworkManager	Jira:RHEL-26195, Jira:RHEL-31182, Jira:RHEL-24337, Jira:RHEL-5852, Jira:RHEL-24622, Bugzilla:1894877, Jira:RHEL-17619
NetworkManager-libreswan	Jira:RHEL-26776, Jira:RHEL-30370, Jira:RHEL-21875
Release Notes	Jira:RHELDOCS-18629, Jira:RHELDOCS-19280, Jira:RHELDOCS-19196, Jira:RHELDOCS-18935, Jira:RHELDOCS-19061, Jira:RHELDOCS-16861, Jira:RHELDOCS-16760, Jira:RHELDOCS-17520, Jira:RHELDOCS-17803, Jira:RHELDOCS-18158, Jira:RHELDOCS-17532, Jira:RHELDOCS-17508, Jira:RHELDOCS-19022, Jira:RHELDOCS-18531, Jira:RHELDOCS-19284, Jira:RHELDOCS-18312, Jira:RHELDOCS-18480, Jira:RHELDOCS-19224, Jira:RHELDOCS-19028, Jira:RHELDOCS-19029, Jira:RHELDOCS-19064, 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-16756, Jira:RHELDOCS-16612, Jira:RHELDOCS-17102, Jira:RHELDOCS-17166, Jira:RHELDOCS-17309, Jira:RHELDOCS-17545, Jira:RHELDOCS-17518, Jira:RHELDOCS-17989, Jira:RHELDOCS-17702, Jira:RHELDOCS-17917, Jira:RHELDOCS-19193, Jira:RHELDOCS-16979
WALinuxAgent	Jira:RHEL-7273
anaconda	Jira:RHEL-30406, Jira:RHEL-20891, Jira:RHEL-10216, Jira:RHEL-2250, Jira:RHEL-17205, Bugzilla:2127473, Bugzilla:2050140, Bugzilla:1877697, Jira:RHEL-4707, Jira:RHEL-4711, Bugzilla:1997832, Jira:RHEL-4741, Bugzilla:2115783, Jira:RHEL-4762, Jira:RHEL-4737, Jira:RHEL-9633, Jira:RHEL-30149, Jira:RHEL-14005
ansible-freeipa	Jira:RHEL-35565
audit	Jira:RHEL-5197, Jira:RHEL-40110
bacula	Jira:RHEL-6856
bind	Jira:RHEL-14898, Bugzilla:1984982

Component	Tickets
binutils	Jira:RHEL-43758
bootc-image-builder-container	Jira:RHEL-34807
ca-certificates	Jira:RHEL-21094, Jira:RHEL-54695
certmonger	Jira:RHEL-12493
clevis	Jira:RHEL-29282
cloud-init	Jira:RHEL-12122
cockpit-machines	Jira:RHEL-31082, Jira:RHEL-31993
container-tools	Jira:RHEL-33572, Jira:RHEL-33574, Jira:RHEL-32714
createrepo_c	Bugzilla:2056318
crypto-policies	Jira:RHEL-39026, Jira:RHEL-45620, Jira:RHEL-2735
cryptsetup	Jira:RHEL-32377
cyrus-sasl	Bugzilla:1995600
device-mapper-multipath	Jira:RHEL-44569, Jira:RHEL-28068, Jira:RHEL-30272, Bugzilla:2033080, Bugzilla:2011699, Bugzilla:1926147
distribution	Jira:RHEL-29758, Jira:RHEL-29853, Jira:RHEL-29850, Jira:RHEL-29851, Jira:RHEL-14523, Jira:RHEL-6973, Jira:RHEL-22385
dnf	Jira:RHEL-15902, Jira:RHEL-21874, Jira:RHEL-6424, Jira:RHEL-38470, Jira:RHEL-25005, Jira:RHEL-1342, Bugzilla:2073510
dnf-plugins-core	Jira:RHEL-13053
dovecot	Jira:RHEL-37160
edk2	Bugzilla:1935497
elfutils	Jira:RHEL-29194
fapolicyd	Bugzilla:2054740, Jira:RHEL-24345, Jira:RHEL-520
firewalld	Jira:RHEL-17002, Jira:RHEL-17708

Component	Tickets
gcc	Jira:RHEL-35635
gcc-toolset-13-gcc	Jira:RHEL-36523, Jira:RHEL-45190
gdb	Jira:RHEL-36211
gimp	Bugzilla:2047161
glibc	Jira:RHEL-20172, Jira:RHEL-25046, Jira:RHEL-25531, Jira:RHEL-39992, Jira:RHEL-36148
gnome-online-accounts	Jira:RHEL-40831
gnupg2	Bugzilla:2070722
gnutls	Bugzilla:2108532
golang	Jira:RHEL-29527, Bugzilla:2111072, Bugzilla:2092016
grafana	Jira:RHEL-31246
gtk3	Jira:RHEL-11924
httpd	Jira:RHEL-14668
ipa	Jira:RHEL-39140, Jira:RHEL-52300, Jira:RHEL-39477, Jira:RHEL-26261, Bugzilla:2084180, Bugzilla:2057471, Jira:RHEL-12154, Jira:RHEL-4955
jmc-core	Bugzilla:1980981
jose	Jira:RHEL-38079
kdump-anaconda-addon	Jira:RHEL-11196
kernel	Bugzilla:1613522, Bugzilla:1570255, Bugzilla:2177256, Bugzilla:2178699, Bugzilla:2023416, Bugzilla:2021672, Bugzilla:1955275, Bugzilla:2142102, Bugzilla:2040643, Bugzilla:2186375, Bugzilla:2183538, Bugzilla:2206599, Bugzilla:2167783, Bugzilla:2000616, Bugzilla:2013650, Bugzilla:2132480, Bugzilla:2059545, Bugzilla:2005173, Bugzilla:2128610, Bugzilla:2129288, Bugzilla:2013884, Bugzilla:2149989
kernel / BPF	Jira:RHEL-23644, Jira:RHEL-34937
kernel / Crypto	Jira:RHEL-17715, Jira:RHEL-20145

Component	Tickets
kernel / File Systems	Jira:RHEL-7768
kernel / Kernel-Core	Jira:RHEL-25967
kernel / Memory Management	Jira:RHEL-31975
kernel / Networking / IPSec	Jira:RHEL-30141, Jira:RHEL-1015
kernel / Networking / NIC Drivers	Jira:RHEL-9897, Jira:RHEL-36283
kernel / Networking / Wifi	Jira:RHEL-24414
kernel / Other	Jira:RHEL-28063
kernel / Platform Enablement / NVMe	Jira:RHEL-8171, Jira:RHEL-8164
kernel / Platform Enablement / ppc64	Jira:RHEL-15404
kernel / Storage / Multiple Devices (MD)	Jira:RHEL-30730
kernel / Storage / Storage Drivers	Jira:RHEL-61452, Jira:RHEL-8466, Jira:RHEL-8104, Jira:RHEL-25730, Jira:RHEL-56135
kernel / Virtualization	Jira:RHEL-43234, Jira:RHEL-1138
kernel / Virtualization / KVM	Jira:RHEL-13007, Jira:RHEL-7212, Jira:RHEL-26152, Jira:RHEL-10019, Jira:RHEL-17331
kernel-rt	Bugzilla:2181571
kernel-rt / Other	Jira:RHEL-9318
kexec-tools	Bugzilla:2113873, Jira:RHEL-11471, Bugzilla:2064708
keylime	Jira:RHEL-11867, Jira:RHEL-1518
kmod	Bugzilla:2103605
kmod-kvdo	Jira:RHEL-8354

Component	Tickets
krb5	Jira:RHEL-17132, Bugzilla:2060798, Jira:RHEL-4875, Jira:RHEL-4889, Jira:RHEL-4888
libabigail	Jira:RHEL-30013, Jira:RHEL-16629
libdb	Jira:RHEL-35607
libdnf	Jira:RHEL-17494, Jira:RHEL-1454, Jira:RHEL-27657
libotr	Bugzilla:2086562
libreswan	Jira:RHEL-32720, Jira:RHEL-50006, Jira:RHEL-51879
librtas	Jira:RHEL-10566
libvirt	Bugzilla:2143158, Bugzilla:2078693
libvirt / General	Jira:RHEL-7043
libxcrypt	Bugzilla:2034569
llvm-toolset	Jira:RHEL-28687
lvm2	Bugzilla:2038183
mod_md	Jira:RHEL-25075
mysql	Bugzilla:1991500
nbdkit	Jira:RHEL-31884
nfs-utils	Bugzilla:2081114
nmstate	Jira:RHEL-19409, Jira:RHEL-28898, Jira:RHEL-26755
nodejs	Jira:RHEL-67327
nss	Jira:RHEL-46840
nvme-stas	Bugzilla:1893841
open-vm-tools	Bugzilla:2037657
opencryptoki	Jira:RHEL-23673

Component	Tickets
openscap	Bugzilla:2161499
openslp	Jira:RHEL-6995
openssh	Jira:RHEL-26454, Bugzilla:2056884, Jira:RHEL-45727
openssl	Jira:RHEL-26271, Jira:RHEL-38514, Bugzilla:2168665, Bugzilla:1975836, Bugzilla:1681178, Bugzilla:1685470, Jira:RHEL-40605
osbuild-composer	Jira:RHEL-4649
oscap-anaconda-addon	Jira:RHEL-1824, Jira:RHELPLAN-44202
p11-kit	Jira:RHEL-58899
pacemaker	Jira:RHEL-39057, Jira:RHEL-40117, Jira:RHEL-47249
pause-container	Bugzilla:2106816
pcp	Jira:RHEL-30198
pcs	Jira:RHEL-25854, Jira:RHEL-21051, Jira:RHEL-16231, Jira:RHEL-21895, Jira:RHEL-36514, Jira:RHEL-28749, Jira:RHEL-17962, Jira:RHEL-7737, Jira:RHEL-2977, Jira:RHEL-34781
pki-core	Jira:RHELPLAN-145900
podman	Jira:RHEL-34603, Jira:RHEL-33567, Jira:RHEL-34609, Jira:RHEL-34612, Jira:RHEL-34605, Jira:RHEL-52239, Jira:RHEL-52237, Jira:RHEL-40637, Jira:RHEL-52246, Jira:RHEL-32267, Bugzilla:2069279
polkit	Jira:RHEL-39063
postgresql	Jira:RHEL-34669
powerpc-utils	Jira:RHEL-23624, Jira:RHEL-23619
python3.11-lxml	Bugzilla:2157708
python3.12	Jira:RHEL-49615
qemu-kvm	Jira:RHEL-32990, Bugzilla:1965079, Bugzilla:1951814, Bugzilla:2060839, Bugzilla:2014229, Bugzilla:1915715, Bugzilla:2176010, Bugzilla:2058982, Bugzilla:2073872, Jira:RHEL-7478

Component	Tickets
qemu-kvm / Devices	Jira:RHEL-1220
qemu-kvm / Devices / CPU Models	Jira:RHEL-17614
qemu-kvm / Graphics	Jira:RHEL-7135
qemu-kvm / Live Migration	Jira:RHEL-7096, Jira:RHEL-7115
qemu-kvm / Networking	Jira:RHEL-7337, Jira:RHEL-7335, Jira:RHEL-7336, Jira:RHEL-333, Jira:RHEL-21867
qemu-kvm / Storage / NBD	Jira:RHEL-33440
rear	Jira:RHEL-40565
resource-agents	Jira:RHEL-32265
restore	Bugzilla:1997366
rhel-bootc-container	Jira:RHEL-33208
rhel-system-roles	Jira:RHEL-30111, Jira:RHEL-37549, Jira:RHEL-31854, Jira:RHEL-30170, Jira:RHEL-30185, Jira:RHEL-46854, Jira:RHEL-48227, Jira:RHEL-46590, Jira:RHEL-40273, Jira:RHEL-34935, Jira:RHEL-30888, Jira:RHEL-33547, Jira:RHEL-30183, Jira:RHEL-45717, Jira:RHEL-40180, Jira:RHEL-3252, Jira:RHEL-14862, Jira:RHEL-33076, Jira:RHEL-32872, Jira:RHEL-39996, Jira:RHEL-35561, Jira:RHEL-29874, Jira:RHEL-40761, Jira:RHEL-25777, Jira:RHEL-50102, Jira:RHEL-39438, Jira:RHEL-32382, Jira:RHEL-32464, Jira:RHEL-56626, Jira:RHEL-29309, Jira:RHEL-26714, Jira:RHEL-41090, Bugzilla:1999770, Bugzilla:2123859, Jira:RHEL-1172, Bugzilla:2186218
rteval	Jira:RHEL-25206
rust	Jira:RHEL-30070
s390utils	Bugzilla:1932480
samba	Jira:RHEL-33645
scap-security-guide	Jira:RHEL-1800, Bugzilla:2038978
seabios	Jira:RHEL-7110

Component	Tickets
selinux-policy	Jira:RHEL-31211, Jira:RHEL-22960, Jira:RHEL-5174, Jira:RHEL-22173, Jira:RHEL-22172, Jira:RHEL-36587, Jira:RHEL-16104, Jira:RHEL-11792, Bugzilla:2064274, Jira:RHEL-28814
shadow-utils	Jira:RHEL-56352
sos	Jira:RHEL-24523, Jira:RHEL-30893, Jira:RHEL-35945, Jira:RHEL-22389, Bugzilla:1869561
sssd	Jira:RHEL-17659, Bugzilla:1608496
stunnel	Jira:RHEL-52317
subscription-manager	Jira:RHEL-29178, Bugzilla:2163716, Bugzilla:2136694
sysstat	Jira:RHEL-12009, Jira:RHEL-26275
systemd	Jira:RHEL-15501, Bugzilla:2018112, Jira:RHEL-6105
systemtap	Jira:RHEL-29528
tigervnc	Bugzilla:2060308
tuned	Bugzilla:2113900
udisks2	Bugzilla:2213769
unbound	Bugzilla:2070495
valgrind	Jira:RHEL-29534
vdo	Jira:RHEL-30525
virt-v2v	Bugzilla:2168082
virtio-win	Jira:RHEL-11810, Jira:RHEL-11366, Jira:RHEL-1609, Jira:RHEL-869
virtio-win / distribution	Jira:RHEL-1860, Jira:RHEL-574
virtio-win / virtio-win-prewhql	Jira:RHEL-19627, Jira:RHEL-1084, Jira:RHEL-935, Jira:RHEL-12118, Jira:RHEL-1212
webkit2gtk3	Jira:RHEL-4157

Component	Tickets
xdp-tools	Jira:RHEL-3382
other	Jira:RHELDOCS-18197, Jira:RHELDOCS-18125, Jira:RHELDOCS-16362, Jira:RHELDOCS-19280, Jira:RHELDOCS-18585, Jira:RHELDOCS-18666, Jira:RHELDOCS-18522, Jira:RHELDOCS-18769, Jira:RHELDOCS-16572, Jira:RHELDOCS-18734, Jira:RHELDOCS-18472, Jira:RHELDOCS-18398, Jira:RHELDOCS-18471, Jira:RHELDOCS-17515, Jira:RHELDOCS-19196, Jira:RHELDOCS-18201, Jira:RHELDOCS-18770, Jira:RHELDOCS-17040, Bugzilla:2020529, Jira:RHELPLAN-27394, Jira:RHELPLAN-27737, Jira:RHELDOCS-18935, Jira:RHELDOCS-17465, Jira:RHELDOCS-16861, Jira:RHELDOCS-17520, Jira:RHELDOCS-17752, Jira:RHELDOCS-17803, Jira:RHELDOCS-17468, Jira:RHELDOCS-17733, Jira:RHELDOCS-18408, Jira:RHELDOCS-17532, Jira:RHELDOCS-17508, 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, Bugzilla:1927780, Jira:RHELPLAN-110763, Bugzilla:1935544, Bugzilla:2089200, Jira:RHELPLAN-99136, Jira:RHELPLAN-103232, Bugzilla:1899167, Bugzilla:1979521, Jira:RHELPLAN-100087, Jira:RHELPLAN-100639, Bugzilla:2058153, Jira:RHELPLAN-113995, Jira:RHELPLAN-98983, Jira:RHELPLAN-131882, Jira:RHELPLAN-139805, Jira:RHELDOCS-16756, Jira:RHELPLAN-153267, Jira:RHELDOCS-16300, Jira:RHELDOCS-16432, Jira:RHELDOCS-16393, Jira:RHELDOCS-16612, Jira:RHELDOCS-17102, Jira:RHELDOCS-17015, Jira:RHELDOCS-18049, Jira:RHELDOCS-17135, Jira:RHELDOCS-17545, Jira:RHELDOCS-17038, Jira:RHELDOCS-17495, Jira:RHELDOCS-17518, Jira:RHELDOCS-17462, Jira:RHELDOCS-18106, Jira:RHELDOCS-17782, Jira:RHELDOCS-19193, Jira:RHELPLAN-157225, Bugzilla:1640697, Bugzilla:1697896, Bugzilla:2047713, Jira:RHELPLAN-96940, Jira:RHELPLAN-117234, Jira:RHELPLAN-119001, Jira:RHELPLAN-119852, Bugzilla:2077767, Bugzilla:2053598, Bugzilla:2082303, Jira:RHELPLAN-121049, Jira:RHELPLAN-109613, Bugzilla:2160619, Jira:RHELDOCS-18064, Jira:RHELDOCS-16427, Bugzilla:2173992, Bugzilla:2185048, Bugzilla:1970830, Jira:RHELDOCS-17719, Jira:RHELDOCS-17720, Jira:RHELDOCS-18720, Jira:RHELDOCS-18435

APPENDIX B. REVISION HISTORY

0.1-3

Tue May 20 2025, Gabriela Fialová (gfialova@redhat.com)

- Removed Bug Fix BZ-2094673 (IdM)

0.1-2

Mon May 12 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated the Customer Portal labs section

0.1-1

Tue April 22 2025, Marc Muehlfeld (mmuehlfeld@redhat.com)

- Added an Enhancement RHEL-83437 (Dynamic programming languages, web and database servers)

0.1-0

Thu March 20 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated a New Feature in RHEL-35565 (IdM)

0.0-9

Tue March 18 2025, Gabriela Fialová (gfialova@redhat.com)

- Added a Known Issue in RHEL-82566 (Installer)

0.0-8

Tue March 11 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated a Deprecated functionality in RHEL-30730 (Filesystems and storage)

0.0-7

Thu March 6 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated a Technology Preview in RHELPLAN-145900 (IdM)

0.0-6

Thu February 27 2025, Marc Muehlfeld (mmuehlfeld@redhat.com)

- Added a Technology Preview in RHELDOCS-19773 (Networking)
- Added a Deprecated Functionality in RHELDOCS-19774 (Networking)
- Removed an enhancement about composefs, as it remains a Technology Preview (Containers)

0.0-5

Mon February 24 2025, Gabriela Fialová (gfialova@redhat.com)

- Added a Known Issue in RHELDOCS-19626 (Security)

- Updated a Feature in RHELDOCS-18125 (RHEL in cloud environments)

0.0-4

Wed February 19 2025, Gabriela Fialová (gfialova@redhat.com)

- Added a New Feature in RHELDOCS-18391 (Infrastructure services)

0.0-6

Thu Feb 06 2025, Gabriela Fialová (gfialova@redhat.com)

- Added an Enhancement RHELDOCS-18451 (Filesystems)

0.0-5

Thu Jan 30 2025, Gabriela Fialová (gfialova@redhat.com)

- Added an Known Issue RHELDOCS-19603 (IdM SSSD)

0.0-4

Wed Jan 22 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated links in a Technology Preview RHELDOCS-19061 (IdM DS)
- Added an Known Issue RHELDOCS-18863 (Virtualization)
- Updated an Enhancement RHEL-45620 (Security)
- Corrected typos throughout the document.

0.0-3

Mon Jan 20 2025, Gabriela Fialová (gfialova@redhat.com)

- Added an Known Issue RHEL-13837 (Installer)

0.0-2

Thu January 16 2025, Marc Muehlfeld (mmuehlfeld@redhat.com), Gabriela Fialová (gfialova@redhat.com)

- Added a Bug Fix RHEL-73167 (Networking)
- Added a Removed Functionality RHELDOCS-19141 (Desktop)
- Added a Removed Functionality RHELDOCS-19156 (Desktop)

0.0-1

Thu January 9 2025, Gabriela Fialová (gfialova@redhat.com)

- Updated an Enhancement RHEL-7768 (Filesystems and storage)

0.0-0

Wed November 13 2024, Gabriela Fialová (gfialova@redhat.com)

- Release of the Red Hat Enterprise Linux 9.5 Release Notes.