Red Hat Enterprise Linux 9

9.6 Release Notes

Release Notes for Red Hat Enterprise Linux 9.6

Last Updated: 2025-05-20

Red Hat Enterprise Linux 9 9.6 Release Notes

Release Notes for Red Hat Enterprise Linux 9.6

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 9.6 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 5

CHAPTER 1. OVERVIEW 6
1.1. MAJOR CHANGES IN RHEL 9.6 6
Installer and image creation 6
RHEL for Edge 6
Security 6
Kernel 7
Dynamic programming languages, web and database servers 7
Compilers and development tools 7
Updated system toolchain 7
Updated performance tools and debuggers 7
Updated performance monitoring tools 8
Updated compiler toolsets 8
Red Hat Enterprise Linux system roles 8
RHEL in cloud environments 8
1.2. IN-PLACE UPGRADE 8
In-place upgrade from RHEL 8 to RHEL 9 8
In-place upgrade from RHEL 7 to RHEL 9 9
1.3. RED HAT CUSTOMER PORTAL LABS 9
1.4. ADDITIONAL RESOURCES 10

CHAPTER 2. DISTRIBUTION OF CONTENT IN RHEL 9 11
2.1. INSTALLATION 11
2.2. REPOSITORIES 11
2.3. APPLICATION STREAMS 12
2.4. PACKAGE MANAGEMENT WITH YUM/DNF 12

CHAPTER 3. NEW FEATURES 13
3.1. INSTALLER AND IMAGE CREATION 13
3.2. SECURITY 13
3.3. RHEL FOR EDGE 16
3.4. SOFTWARE MANAGEMENT 16
3.5. SHELLS AND COMMAND-LINE TOOLS 17
3.6. INFRASTRUCTURE SERVICES 18
3.7. NETWORKING 19
3.8. KERNEL 23
3.9. BOOT LOADER 26
3.10. FILE SYSTEMS AND STORAGE 27
3.11. HIGH AVAILABILITY AND CLUSTERS 28
3.12. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 29
3.13. COMPILERS AND DEVELOPMENT TOOLS 31
3.14. IDENTITY MANAGEMENT 38
3.15. SSSD 41
3.16. RED HAT ENTERPRISE LINUX SYSTEM ROLES 42
3.17. VIRTUALIZATION 45
3.18. RHEL IN CLOUD ENVIRONMENTS 47
3.19. SUPPORTABILITY 49
3.20. CONTAINERS 49
3.21. LIGHTSPEED 52

CHAPTER 4. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS 53

New kernel parameters 53
Removed kernel parameters 56
Changed kernel parameters 56
New sysctl parameters 57
Changed sysctl parameters 57

CHAPTER 5. BUG FIXES 59
5.1. SECURITY 59
5.2. SUBSCRIPTION MANAGEMENT 60
5.3. SOFTWARE MANAGEMENT 60
5.4. SHELLS AND COMMAND-LINE TOOLS 61
5.5. NETWORKING 61
5.6. FILE SYSTEMS AND STORAGE 63
5.7. HIGH AVAILABILITY AND CLUSTERS 64
5.8. COMPILERS AND DEVELOPMENT TOOLS 65
5.9. IDENTITY MANAGEMENT 66
5.10. RED HAT ENTERPRISE LINUX SYSTEM ROLES 70
5.11. VIRTUALIZATION 72
5.12. SUPPORTABILITY 75

CHAPTER 6. TECHNOLOGY PREVIEWS 76
6.1. INSTALLER AND IMAGE CREATION 76
6.2. SECURITY 77
6.3. RHEL FOR EDGE 79
6.4. SHELLS AND COMMAND-LINE TOOLS 79
6.5. INFRASTRUCTURE SERVICES 79
6.6. NETWORKING 79
6.7. KERNEL 81
6.8. FILE SYSTEMS AND STORAGE 82
6.9. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 83
6.10. COMPILERS AND DEVELOPMENT TOOLS 83
6.11. IDENTITY MANAGEMENT 84
6.12. DESKTOP 86
6.13. THE WEB CONSOLE 87
6.14. VIRTUALIZATION 87
6.15. RHEL IN CLOUD ENVIRONMENTS 88
6.16. CONTAINERS 88

CHAPTER 7. DEPRECATED FUNCTIONALITIES 90
7.1. INSTALLER AND IMAGE CREATION 90
7.2. SECURITY 91
7.3. SUBSCRIPTION MANAGEMENT 96
7.4. SOFTWARE MANAGEMENT 97
7.5. SHELLS AND COMMAND-LINE TOOLS 97
7.6. INFRASTRUCTURE SERVICES 98
7.7. NETWORKING 99
7.8. KERNEL 101
7.9. FILE SYSTEMS AND STORAGE 101
7.10. HIGH AVAILABILITY AND CLUSTERS 104
7.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 104
7.12. COMPILERS AND DEVELOPMENT TOOLS 104
7.13. IDENTITY MANAGEMENT 105
7.14. SSSD 106
7.15. DESKTOP 107

7.16. GRAPHICS INFRASTRUCTURES 110
7.17. RED HAT ENTERPRISE LINUX SYSTEM ROLES 111
7.18. VIRTUALIZATION 112
7.19. CONTAINERS 115
7.20. DEPRECATED PACKAGES 117

CHAPTER 8. KNOWN ISSUES 152
8.1. INSTALLER AND IMAGE CREATION 152
8.2. SECURITY 159
8.3. SOFTWARE MANAGEMENT 164
8.4. SHELLS AND COMMAND-LINE TOOLS 165
8.5. INFRASTRUCTURE SERVICES 167
8.6. NETWORKING 169
8.7. KERNEL 170
8.8. FILE SYSTEMS AND STORAGE 175
8.9. HIGH AVAILABILITY AND CLUSTERS 176
8.10. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS 177
8.11. IDENTITY MANAGEMENT 178
8.12. SSSD 181
8.13. DESKTOP 181
8.14. GRAPHICS INFRASTRUCTURES 182
8.15. THE WEB CONSOLE 183
8.16. RED HAT ENTERPRISE LINUX SYSTEM ROLES 183
8.17. VIRTUALIZATION 184
8.18. RHEL IN CLOUD ENVIRONMENTS 192
8.19. SUPPORTABILITY 194
8.20. CONTAINERS 195
8.21. LIGHTSPEED 196

CHAPTER 9. AVAILABLE BPF FEATURES 197

APPENDIX A. LIST OF TICKETS BY COMPONENT 216

APPENDIX B. REVISION HISTORY 226

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 9.6

Installer and image creation

Key highlights for RHEL installer:

- The newly created users will have administrative privileges by default, unless you deselect the option.
- You can now set the required time zone by using new options instead of the time zone map.
- The remote desktop protocol (RDP) for graphical remote access replaces VNC.

Key highlights for RHEL image builder:

- You can use RHEL image builder to create disk images with advanced partitioning.
- You can customize your blueprint to enable injecting a Kickstart files when building ISO images.
- Disk images, such as AWS or KVM, do not have a separate /**boot** partition.

For more information, see New features - Installer and image creation .

RHEL for Edge

Key highlights for RHEL for Edge:

- RHEL for Edge will no longer include the **dnsmasq** package by default.
- You can now add file system customizations to a blueprint when building the following image types:
- **simplified-installer**
- **edge-raw-image**
- **edge-ami**
- **edge-vsphere**
- You can now create FIPS compliant RHEL for Edge images.
- You can now use the FDO onboarding process, available as a Technology Preview, by storing and querying Owner Vouchers from the Sqlite or Postgresql databases.

For more information, see New features - RHEL for Edge .

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.

Kernel

This release brings key updates to kernel stability, performance, and features. A recent change impacting **MADV_RANDOM** performance related to **POSIX_FADV_NOREUSE** has been reverted to maintain expected application behavior.

The **eBPF** facility has been updated to align with Linux kernel version 6.12, and **TPM_TIS** has been rebased to upstream 6.7 for enhanced Lenovo hardware support. In addition to this, **kdump** is rebased to version 6.10.

NVMf-FC kdump now supports the IBM Power system for running **kexec-tools**.

For **cgroup v2**, the **/proc/cgroups** file is deprecated, with the **cgroup.stat** file now providing the definitive source for cgroup subsystem information.

For more information about the features introduced in this release and changes in the existing functionality, see New features - Kernel.

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

Compilers and development tools

Updated system toolchain

The following system toolchain components have been updated:

- **GCC 11.5**
- **Annobin 12.70**

Updated performance tools and debuggers

The following performance tools and debuggers have been updated in RHEL 9.5:

- **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 in RHEL 9.5:

- **PCP 6.2.2**
- **Grafana 10.2.6**

Updated compiler toolsets
The following compiler toolsets have been updated in RHEL 9.5:

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

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

Red Hat Enterprise Linux system roles
Notable new features in 9.6 RHEL system roles:

- With the new RHEL system role **aide**, you can detect unauthorized changes to files, directories, and system binaries.
- With the **systemd** RHEL system role you can now manage user units in addition to system units
- You can use the **ha_cluster** RHEL system role to export the **corosync** configuration of an existing cluster in a format that can be fed back to the role to create the same cluster.
- You can use the **podman** RHEL system role to manage the quadlet units of type **Pod**.
- The **metrics** RHEL system role now supports Valkey as an alternative to Redis.

For more information, see New features - Red Hat Enterprise Linux System Roles .

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 9.4 and 9.6 on the following architectures:
  - 64-bit Intel, AMD, and ARM
  - IBM POWER 9 (little endian) and later
  - IBM Z architectures, excluding z13

- From RHEL 8.10 to RHEL 9.4 and 9.6 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 .

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:

- Due to an issue with booting on the RHEL 9 kernel, you could upgrade an ARM machine to only RHEL 9.4. The issue is now fixed and ARM machines can be upgraded on all supported upgrade paths, namely from RHEL 8.10 to RHEL 9.4 and RHEL 9.6.
- Resource limitations are automatically adjusted when running the **leapp** utility to prevent various errors during the leapp execution. Systems with encrypted storage can be upgraded if the storage uses the LUKS2 format configured with the Clevis TPM 2.0 token.
- Implement a new solution to preserve Network Interface Card (NIC) names during the upgrade by using the net.naming-scheme argument in the kernel command line.
- Introduce configuring in-place upgrades on systems by using Red Hat Update Infrastructure (RHUI). For more information, see Using RHUI to configure an in-place upgrade .

In-place upgrade from RHEL 7 to RHEL 9

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

1.3. RED HAT CUSTOMER PORTAL LABS

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

- Registration Assistant
- Kickstart Generator
- Red Hat Product Certificates
- Red Hat CVE Checker
- Kernel Oops Analyzer
- Red Hat Code Browser
- VNC Configurator
- Red Hat OpenShift Container Platform Update Graph
- Red Hat Satellite Upgrade Helper
- JVM Options Configuration Tool

- Load Balancer Configuration Tool
- Red Hat OpenShift Data Foundation Supportability and Interoperability Checker
- Ansible Automation Platform Upgrade Assistant
- 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 Get Started page.

NOTE

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

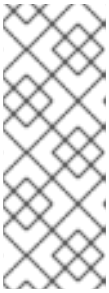
[1] Public release notes include links to access the original tracking tickets, but private release notes are not viewable so do not include links.

CHAPTER 2. DISTRIBUTION OF CONTENT IN RHEL 9

2.1. 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.

2.2. 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.

2.3. APPLICATION STREAMS

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

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

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

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

NOTE

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

Some additional Application Stream versions will be distributed as modules with a shorter life cycle in future minor RHEL 9 releases. Modules are collections of packages representing a logical unit: an application, a language stack, a database, or a set of tools. These packages are built, tested, and released together.

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

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

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

2.4. 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 3. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 9.6.

3.1. INSTALLER AND IMAGE CREATION

Added Kickstart support for CA certificates to enable encrypted DNS configuration during installation

Support for the **%certificate** section in the Kickstart file is added to enable the installation of CA certificates into the installer environment and the installed system. This simplifies the setup process and ensures that the encrypted DNS is operational after installation, reducing manual configuration and security gaps. The certificates are inlined in the Base64 ASCII format and imported through the **--dir** and **--filename** options. This enhancement facilitates encrypted DNS configuration as part of **Zero Trust Architecture** requirements. The encrypted DNS set up during installation ensures secure DNS resolution from the start, improving security and compliance in automated deployments.

Jira:RHEL-61430[1]

RHEL image builder supports creating disk images with advanced partitioning

With this enhancement, RHEL image builderl gained more options for customizing partitioning and creating disk images with advanced partitioning layout. You can create disk images with custom mountpoints, including custom mount options, LVM-based partitions and LVM-based SWAP to, for example, change the size of the / and the /**boot** directories by using a blueprint file.

Jira:RHELDOCS-19584[1]

bootc-image-builder now supports creating image mode disk images with advanced partitioning

With this enhancement, the **bootc-image-builder** tool gained more options for customizing partitioning and creating disk images with advanced partitioning layout. You can use the **bootc-image-builder** tool to create disk images of image-mode RHEL with custom mountpoints, including custom mount options, LVM-based partitions and LVM-based SWAP to, for example, change the size of the / and the /**boot** directories by using the **config.toml**.

Jira:RHELDOCS-19291[1]

The bootc image builder tool is generally available in RHEL

The **bootc image builder** tool, now is generally available in RHEL, 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]

3.2. SECURITY

pcsd now provides the --disable-polkit option

With this update, you can turn off loading the PolicyKit authorization framework by starting the **pcsd**

service with the **--disable-polkit** option. Running **pcsd** without **polkit** enables accessing PKCS #11 devices in limited environments such as the initial RAM disk. As a result, the Clevis decryption client can use a PKCS #11 device for automated unlocking LUKS-encrypted volumes at boot time.

Jira:RHEL-34856

ssh now provides a link with additional details about SSH login error messages

In case of an early error, the **ssh** command-line tool provides a link to the Red Hat Customer Portal page that contains additional details about common error messages and steps for resolving them. This helps troubleshoot SSH login problems when you use interactive mode.

Jira:RHEL-33809[1]

pkcs-tool now shows object URI

With this update, the **pkcs11-tool -L** and **pkcs11-tool -O** commands contain the **uri:** field in their outputs. You can use the URI information when configuring the **pkcs11** Clevis pin for automated unlocking LUKS-encrypted drives with PKCS #11 devices.

Jira:RHEL-53115

CBC ciphers can now be blocked in crypto-policies

With this update, **crypto-policies** uses the **openssl -CBC CipherString** directive. As a result, CBC cipher suites are disabled in OpenSSL if none of them are enabled in **crypto-policies**.

Jira:RHEL-76524[1]

nettle rebased to 3.10.1

The **nettle** library package has been rebased to upstream version 3.10.1. This version provides various bug fixes, optimizations and enhancements, most notably:

- Performance has been improved on 64-bit PowerPC architectures (SHA-256, AES decryption, and AES-GCM).
- DRBG-CTR-AES256, a new deterministic random bit generator, has been added.
- RSA-OAEP, an RSA encryption/decryption that uses a new OAEP padding scheme, has been added.
- SHAKE-128, an arbitrary length hash function of the SHA-3 family, has been added.
- Streaming API for SHAKE-128 and SHAKE-256 has been added.
- The MD5 assembly has been removed. This might incur a slight performance impact.

Jira:RHEL-52740[1]

Rsyslog rebased to 8.2412.0

The **rsyslog** packages have been rebased to upstream version 8.2412.0 in RHEL 9.6. Among other fixes and enhancements, you can bind a ruleset to the **imjournal** module. With this optimization, log messages can be filtered and processed at the input stage, which reduces the load on the main message queue. This minimizes resource utilization and ensures smoother handling of high-volume logs.

Jira:RHEL-65177

OpenSCAP rebased to 1.3.12

The OpenSCAP packages have been rebased to upstream version 1.3.12. This version provides bug fixes and various enhancements. For additional information, see the OpenSCAP release notes.

Jira:RHEL-88413

Clevis rebased to version 21 with support for PKCS #11

The **clevis** packages have been upgraded to version 21. This version contains many enhancements and bug fixes, notably:

- Added the **clevis-pin-pkcs11** subpackage which provides the **pkcs11** pin for unlocking LUKS-encrypted volumes using a PKCS #11 device (smart card).
- Added two checks to the **clevis-udisks2** subpackage.
- Added a fix that prevents "Address in use" errors.

Jira:RHEL-60257

New Keylime policy management tool

The new **keylime-policy** tool integrates all management tasks of Keylime runtime policies and measured boot policies and improves the performance of generating policies.

Jira:RHEL-75797

SELinux assigns a particular type to /dev/hfi1_0

With this update, the **hfi1_device_t** type is assigned to the **/dev/hfi1_0** device in the SELinux policy. As a result, SELinux can properly control access to the device.

Jira:RHEL-54996[1]

Additional services confined in the SELinux policy

This update adds additional rules to the SELinux policy that confine the following **systemd** services:

- **iio-sensor-proxy**
- **power-profiles-daemon**
- **switcheroo-control**
- **samba-bgqd**

As a result, these services no longer run with the **unconfined_service_t** SELinux label, which violated the CIS Server Level 2 benchmark "Ensure No Daemons are Unconfined by SELinux" rule, and run successfully in SELinux enforcing mode.

Jira:RHEL-17346, Jira:RHEL-24268, Jira:RHEL-53124, Jira:RHEL-61117

SCAP Security Guide rebased to 0.1.76

For additional information, see the SCAP Security Guide release notes.

Jira:RHEL-74240

Keylime requires HTTPS for revocation notifications

The Keylime components require the use of the more secure HTTPS protocol for revocation notification webhooks instead of HTTP. As a consequence, the Keylime verifier now requires the revocation notification webhook server CA certificate. You can add it to the **trusted_server_ca** configuration option or add it to the system trust store.

Jira:RHEL-78313

3.3. RHEL FOR EDGE

Support for deploying image mode for RHEL systems by using FDO

With this enhancement, now you can deploy an image mode for RHEL systems by using the FIDO Device Onboarding (FDO) process, available as a Technology Preview, to deliver the configuration to this system. Include a Kickstart file in an ISO build to configure any part of the installation process except the base image deployment. If you use an ISO with a **bootc** container base image, **bootc-image-builder** automatically installs **ostreecontainer**, the command to install the container image. You can still configure anything, except the **ostreecontainer** command.

Jira:RHELDOCS-19610[1]

RHEL 10 provides the greenboot package in version 0.15.8

The **greenboot** packages have been updated to version 0.15.8, which provides bug fixes and enhancements. Notable changes include:

- Fixed the **bootc** compatibility with **rpm-ostree** when **bootc** is available alongside **rpm-ostree**.
- General bug fix: If **bootc** is not available, rollback using **rpm-ostree**.

Jira:RHEL-80003

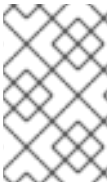
3.4. SOFTWARE MANAGEMENT

Image mode for RHEL users can now use dnf --transient to perform package transactions that reset on reboot

Previously, Image mode for RHEL users could transiently install, remove, and upgrade packages by running the **bootc usr-overlay** command to unlock the system and then make changes by running DNF commands. If you use **bootc usr-overlay**, when the system reboots, the **/usr** directory overlay disappears and all changes made to it will reset. Changes to other directories, including configuration in **/etc** and program state in **/var**, persist across reboots.

With this update, a new **--transient** flag and a new **persistence** configuration option have been added to DNF to improve the user experience on bootc systems. You can now skip the **bootc usr-overlay** step by using either of the following options:

- Use the **dnf --transient** command.
- Set the **persistence** option to **transient** in the **dnf.conf** file.



NOTE

Unlike when using **bootc usr-overlay**, **--transient** and **persistence=transient** ensure that the /**usr** directory remains read-only to other processes before, during, and after the transaction.

For example, to transiently install the **make** package, enter:

```
# dnf install --transient make
```

Jira:RHEL-70917

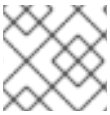
Improved error message when using DNF on a locked OSTree or bootc system

OSTree and bootc systems cannot be managed by DNF by default. Previously, a DNF error message did not say that this was an expected behavior and how you could change it. With this update, DNF detects whether it runs on a read-only OSTree or bootc system and informs you where to find more details about how to manage such systems with DNF.

Jira:RHEL-49670

DNF Automatic can now notify users about a failed update

With this update, a new **send_error_messages** boolean option has been added to the **[emitters]** section of the /**etc/dnf/automatic.conf** configuration file. As a result, if you set **send_error_messages** to **yes**, the DNF Automatic tool notifies you about failed automatic updates by using an emitter configured in the **emit_via** option.



NOTE

This feature is disabled by default.

Jira:RHEL-61882

3.5. SHELLS AND COMMAND-LINE TOOLS

ignoreduplicates option is now available

With this enhancement, the **ignoreduplicates** option is added in the **logrotate** configuration. The option ignores any duplicate file paths in the **logrotate** configuration, and is not enabled by default.

Jira:RHEL-5711[1]

maven-openjdk21 package is now available

RHEL supports running Maven with multiple Java versions, allowing users to select their preferred JDK. With this enhancement, a new **maven-openjdk21** package has been added to enable seamless execution of Maven with **OpenJDK 21**. The notable changes include the following:

- Expanded set of supported Java runtimes for Maven workflows.
- Improved flexibility for development and build environments.

Jira:RHEL-62175

openCryptoki rebased to version 3.24.0

The **openCryptoki** packages are rebased to version 3.24.0. Support has been added for the following:

- CCA token on non-IBM Z platforms (x86_64, ppc64)
- IBM Dilithium
- RSA-OAEP with SHA224, SHA384, and SHA512 on encrypt or decrypt.
- PKCS#11 v3.0 SHA3 mechanisms
- SHA-2 mechanisms
- SHA based key derivation mechanisms
- Protecting tokens with a token specific user group
- New libica AES-GCM API using the KMA instruction on z14 and later

Jira:RHEL-50064[1]

libva rebased to 2.22.0

The **libva** package is rebased to 2.22.0. Notable enhancement includes the following:

- Added VVC decode LibVA interface
- Support added for **linux-dmabuf**

Jira:RHEL-59629[1]

A new module stream maven 3.9 is available

A new update to the **maven 3.9** package is now available. In version 3.9, maven is not compatible with maven 2. The notable enhancement include the following:

- The **maven-openjdk21** package is now available. It enables seamless execution of Maven with the **OpenJDK 21** package. The **OpenJDK 21** package provides an expanded set of supported Java run times for Maven workflows, improving flexibility for development and build environments.

Jira:RHEL-73128

Multipath partner device is now supported

The **drmgr** is a utility for managing logical and physical hot plug capable resources. With this enhancement, **drmgr** supports hot plug addition and removal of a multipath drive.

Jira:RHEL-30880[1]

3.6. INFRASTRUCTURE SERVICES

Weak ciphers can be now disabled in CUPS configuration

Previously, when you disabled the weak cipher in the CUPS configurations, the configuration changes did not take effect. With this enhancement, if a user wants to disable a certain cryptographic algorithm via system policy, CUPS honors the system settings, if **SSLOptions NoSystem** is not in CUPS configuration files, and CUPS does not offer the system-wide disabled algorithm anymore.

As a result, to prevent possible breakage of existing configurations, the directive **SSLOptions NoSystem** is set in the **/etc/cups/cupsd.conf** and **/etc/cups/client.conf** files. If a user wants **cupsd** daemon or applications using **libcups** to follow system crypto policy, they can remove the mentioned **SSLOptions** directive from the respective configuration files:

- **/etc/cups/cupsd.conf**: if the **cupsd** daemon is expected to follow system crypto policy.
- **/etc/cups/client.conf**: if applications using **libcups** are expected to follow system crypto policy.

Jira:RHEL-68414[1]

3.7. NETWORKING

Added support for E825C interface

Added support for Ethernet functionality of the E825C network interface for Intel Granite Rapids-D platform to the **ice** driver.

Jira:RHEL-57827[1]

The i40e driver supports automatic reset behavior on MDD events

The Intel® Network Adapter Driver for PCIe* 40 Gigabit Ethernet can now reset problematic Single Root I/O Virtualization (SR-IOV) virtual functions (VFs) when it detects a malicious driver detection (MDD) event. You can activate this automatic reset behavior through the new **mdd-auto-reset-vf** option as in the following example command:

```
ethtool --set-priv-flags _ethX_ *mdd-auto-reset-vf* on
```

When the VF sends malformed packets classified as malicious, it can cause the Tx queue to freeze, which makes it unusable for several minutes. However, with **mdd-auto-reset-vf** enabled, a graceful VF reset automatically restores operational state when an MDD event occurs.

Jira:RHEL-54223[1]

NetworkManager now supports configuration of FEC encoding on NIC

With this enhancement, NetworkManager supports forward error correction (FEC) encoding support on the network interface controller (NIC). By disabling FEC encoding on NIC, you will have reduced overhead of redundant data transmission and lower latency of network traffic. Configure FEC settings on NIC by using the following steps:

1. Configure the FEC settings by using the **nmcli** utility:

   ```
   # nmcli con mod __<example_connection_name>__ ethtool.fec off
   ```

2. Bring the interface down to apply the ethtool FEC encoding setting:

   ```
   # nmcli con down __<example_connection_name>__
   ```

3. Bring the interface up to apply the ethtool FEC encoding setting:

   ```
   # nmcli con up __<example_connection_name>__
   ```

4. Use the **ethtool** utility to:

```
# ethtool --show-fec __<example_device_name>__
```

Jira:RHEL-24055

NetworkManager can automatically add routes to DNS servers

With the **ipv4.routed-dns** parameter, you can configure NetworkManager so that nameservers are reachable only through the correct network interface. Apart from **systemd-resolved** and **dnsmasq** backend DNS services in NetworkManager, other backend services do not support binding nameservers to the correct network interface. As a result, you can use NetworkManager to add an explicit route to the nameserver through the related network interface.

Jira:RHEL-45878

NetworkManager can set ipv4.dhcp-send-hostname`to `false by default

With this feature, you can set the **ipv4.dhcp-send-hostname** option in NetworkManager to **false** for all IPv4 connections. To disable this option by default, add the configuration snippet to the **/etc/NetworkManager/conf.d/99-no-hostname.conf** file as follows:

```
[connection]
match-device=type:ethernet
ipv4.dhcp-send-hostname=0
```

You can also set this option for IPv6.

Jira:RHEL-32685[1]

NetworkManager supports ip-ping-addresses and ip-ping-timeout properties for the connection setting

With this enhancement, you can add an IP address to the **ip-ping-addresses** and set a timeout with **ip-ping-timeout** settings. As a result, you can ensure that remote services, such as network file system (NFS), are mounted only after the target network is reachable.

Jira:RHEL-21160

nmstate supports the require-id-on-certificate setting on Libreswan configuration

With this enhancement, **libreswan**, an implementation of Internet Protocol Security (IPsec) specification, now supports the **require-id-on-certificate** setting for VPN configurations by using NetworkManager. With this feature, you can configure Subject Alternative Name (SAN) validation by using the **require-id-on-certificate** option. As a result, this implementation correctly enforces SAN validation based on the specified setting:

- No SAN validation is performed when set to **no**
- SAN are validated when set to **yes**

Jira:RHEL-58040[1]

NetworkManager DHCP Client supports IPv6-only preferred option for DHCPv4

With this enhancement, the IPv6-only preferred option for DHCPv4 is available for NetworkManager clients for the supported DHCP server. You can use this option in two ways: globally and locally. If enabled globally, this option allows and prioritizes only IPv6 addresses in dual networks that support

both IPv4 and IPv6. If enabled locally by setting the **ipv6.method disabled** option, IPv4 addresses assigned manually are prioritized over DHCP addresses.

Jira:RHEL-14370

xdp-tools rebased to version 1.5.1

The **xdp-tools** package has been upgraded to version 1.5.1, which provides multiple enhancements and bug fixes. Notable changes include:

- Added the **xdp-forward** utility that enables XDP-accelerated packet forwarding between supported network devices.
- Updated the **xdp-trafficgen** utility to support specifying User Datagram Protocol (UDP) packet sizes.
- Added a new option-based API for creating XDP sockets (XSK) and user memory (UMEM) objects.

Jira:RHEL-73054

wpa_supplicant was rebased to version 2.11

The **wpa_supplicant** utility has been upgraded to version 2.11, which provides multiple bug fixes and enhancements. Notable changes include:

- Removed incorrect Extensible Authentication Protocol (EAP) Session-Id length constraint.
- Added support for OpenSSL 3.0 API changes.
- The CONFIG_IEEE80211BE configuration option enabled for Extremely High Throughput (EHT) operation.
- Support for explicit Service Set Identifier (SSID) protection in 4-way handshake is disabled by default. You can enable it using the **ssid_protection=1** configuration option.

For more details, see the upstream changelog.

Jira:RHEL-58725

iproute2 rebased to version 6.11.0

The **iproute2** package has been upgraded to version 6.11.0, which provides multiple bug fixes and enhancements. Notable changes include:

- Added support for the **mst_enabled** parameter
- Added support for setting a Multiple Spanning Tree Instance (MSTI) for VLANs
- Added support for Multiple Spanning Tree (MST) states
- Fixed **libbpf** version check for ENABLE_BPF_SKSTORAGE_SUPPORT configuration option
- Added support for Berkeley Packet Filter (BPF) socket-local storage
- Removed support for unused and obsolete queueing disciplines (**qdiscs**) and classifiers
- Several NULL derefence fixes and code optimizations

For full extent, see the upstream article.

Jira:RHEL-62931

Bonding device supports IPsec HW offload with ESN

Previously, a bonding device did not support the IPSec Hardware **HW** offload feature with Extended Sequence Numbers (**ESN**). Consequently, setting up IPsec with HW offload and ESN failed on the bonding device. With this fix, you can setup IPsec HW offload with ESN on the bonding device, considering the bond ports already support this feature. As a result, the bonding device offloads IPsec traffic correctly.

Jira:RHEL-50630[1]

New "drop reasons" in the VXLAN implementation

In this update of the RHEL kernel, visibility patches were introduced which add new "drop reasons" in the Virtual eXtensible Local Area Networking (VXLAN) implementation. Visibility patches are important for troubleshooting problems, and thanks to these additions most of the dropped packets in VXLAN now have a reason attached to provide extra context.

Jira:RHEL-68063[1]

Network drivers for modems in RHEL are now fully supported

In the US, 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 may offer tools to unlock ModemManager, but they are not integrated in RHEL because they contain closed-source and private binaries.

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 full support:

- 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
- Qualcomm devices supported in upstream

Jira:RHELDOCS-16760[1]

nmstate now supports configuring IPvLAN

The **nmstate** API now supports configuring IPvLAN, a virtual network interface, that enhances network management and container networking.

IPvLAN supports the following modes:

- **l2**: IPvLAN receives and responds to ARP requests, which improves performance but has less control on the network traffic.

- **l3**: IPvLAN processes only layer 3 traffic and above. IPvLAN does not respond to ARP requests and you must manually configure the ARP table entries for the IPvLAN IP addresses on the relevant devices.
- **l3s**: IPvLAN processes the same way as in l3 mode, except that both egress and ingress traffic of a relevant device passes through the **netfilter** chain in the default namespace.
- **Private**: The **private** setting controls the isolation between the IPvLAN interface and other devices on the network.
- **Vepa**: When enabled, IPvLAN forwards traffic through a central switch, which improves the network management by reducing broadcast traffic.

In the following example, you can setup IPvLAN for **l3** mode:

```
---
interfaces:
  - name: ipvlan0
    type: ipvlan
    state: up
    ipvlan:
      base-iface: eth0
      mode: l3
      private: false
      vepa: false
```

Jira:RHEL-43438

3.8. KERNEL

Kernel version in RHEL 9.6

Red Hat Enterprise Linux 9.6 is distributed with the kernel version 5.14.0-503.11.1.

The eBPF facility has been rebased to Linux kernel version 6.12

Notable changes and enhancements include the following:

- BPF token, which supports delegating a subset of BPF functionality from privileged system-wide daemons to a trusted and unprivileged application.
- BPF arena, a sparse shared memory region between the BPF program and user space that makes pointers within the arena work seamlessly.
- **may_goto** instruction, which is a contract between the verifier and the program. The verifier allows the program to execute loops (provided that they run well) in most situations, but reserves the right to terminate it.
- BPF verifier support for static sub-program calls in spin lock critical sections.
- Support for attaching **kprobe** BPF programs in a session mode where the program is attached to both the function entry and return. The entry program can decide if the return program gets executed, and the programs can share a **u64** cookie value.
- The ability to specify and retrieve the BPF cookie for raw tracepoint programs to ease migration from classic to raw tracepoints.

- A new **bpf_wq** API has been introduced to provide a mechanism for deferring events.
- A number of new **kfuncs** (kernel functions callable from BPF programs) are added for calling crypto APIs, enabling/disabling preemption, generic bits iterators, and various VFS operations.
- Support declaring arrays of **kptr**, **bpf_rb_root**, and **bpf_list_head** from BPF programs.
- Support for detection of **kfuncs** for the running kernel and dumping compilable **kfunc** prototypes.
- Support for 64-bit BPF v4 CPU instructions for PowerPC.
- Support for resilient split BTF, which cuts down on duplication and makes BTF as compact as possible WRT BTF from modules.

Jira:RHEL-63880[1]

View the number of instances of each cgroup from cgroup.stat

For **cgroup v2**, the **cgroup.stat** control file is enhanced to show the number of instances of each cgroup subsystem in the unified hierarchy, including any dying ones.

The **/proc/cgroups** file used to show the number of cgroups for each cgroup subsystem is designed for **cgroup v1**. With **cgroup v2**, the information provided in **/proc/cgroups** is no longer applicable. This file is deprecated for **cgroup v2**.

Use the **cgroup.stat** file of the root cgroup to get the correct number of cgroup subsystems. This is the replacement of **/proc/cgroups** for **cgroup v2**.

Jira:RHEL-36267[1]

New option to disable idle states locally on CPUs during rtla-timerlat testing: deepest-idle-state

- The arguments for the **deepest-idle-state** are the number of the deepest allowed idle state. If -1 is the value in the argument, and disables idle states on all CPUs.
- In the **rtla-timerlat** instead of using **/dev/cpu_dma_latency** to disable the CPUs in the idle state globally, the **deepest-idle-state** option is added to set the deepest allowed idle state for CPUs where measurements are running.

As a result, you can save power and reflect the real-time workload during **rtls-timerlat** testing and use the **deepest-idle-state** instead of using the **/dev/cpu_dma_latency** to disable them globally.

Jira:RHEL-69522[1]

kpatch-dnf plugin is updated with improved kernel management

The kpatch-dnf plugin is updated with enhancements in filtering kernels for better management of kernel updates and patching. Administrators can selectively apply patches to specific kernel versions, reducing the risk of incompatible patching and improving overall system stability.

Jira:RHEL-77113[1]

Containerization of the rteval utility

With this update, you can run the **rteval** utility with all its runtime dependencies from a container image publicly available through the Quay.io container registry. This feature also enables you to, for example:

- Use the deployment flexibility, where older RHEL versions can get newer versions of **rteval**.
- Run multiple **rteval** instances on the same or multiple hosts.
- Allocate specific system resources to **rteval**, which ensures fine-grained control over resource usage.

Alternatively, you can use the dockerfile template to build your own container image with **rteval**. You can find this dockerfile and the README file with more information in the upstream repository.

Jira:RHEL-9909[1]

TPM_TIS rebased to upstream 6.7 for Lenovo hardware

This release introduces an updated version of the Trusted Platform Module (TPM) Integration Services (**TPM_TIS**) firmware to upstream version 6.7. This update addresses stability and security enhancements for RHEL 9.6.

Jira:RHEL-52747[1]

kdump is rebased to 6.10

This update incorporates the latest improvements, bug fixes, and features from the 6.10 kernel related to crash dumping.

Jira:RHEL-58641

Landlock, a new Linux Security Module (LSM) is released

RHEL 9.6 introduces Landlock, a new security feature that makes your containers safer. Landlock sets strict rules for processes like Podman to limit access to the file system through the kernel API, defining rules for themselves regardless of privilege level and allowing users to create hard limits over the accessible scope of the processes.

With Landlock, you can build programs that mitigate potential risks associated with misconfigured or maliciously targeted processes. This makes containers and the whole system more secure.

Jira:RHEL-8810

New integration testing to validate kdump procedures to prevent system failure

With this enhancement, you can check the log file for **kdump** procedures after any software or hardware updates to prevent system failure. After the analysis of the output log files, the configuration entries, such as **memory issues** or **blacklist of some drivers**, are corrected to validate the **kdump** procedures and generate the **vmcore**. This ensures that the **kdump** procedures are validated and corrected before a system crash after any software or hardware update.

Jira:RHEL-32060[1]

New timerlat-interval INTV_US and cyclictest-interval INTV_US options

With this enhancement, you can use the following new options of the **rteval** command to modify the base or periodic interval option in running **timerlat** or **cyclictest** threads:

- **timerlat-interval INTV_US**
- **cyclictest-interval INTV_US**

Note that if you do not use either of these options with **rteval**, the default value of 100 microseconds is applied.

Jira:RHEL-67423[1]

New option to disable idle states locally on latency testing with**cyclictest**

- The **cyclictest** tool sets **/dev/cpu_dma_latency** to 0 by default to avoid increased latency when waking up from idle, which disables idle states on all CPUs.
- The new **deepest-idle-state** option only disables idle states on CPUs which are selected for the testing. The argument specifies the deepest allowed idle state, setting it to **-1** disables all idle states on the measured CPUs.
- Tuning with the **cyclictest** is supposed to reflect the real-time workload testing, and thus using the **deepest-idle-state** instead of using the **/dev/cpu_dma_latency** to disable the CPU idle states reflects a use case where the real-time workload only disables idle states on the CPU where it is running.
- As a result, the **cyclictest** coverage of addressing all use cases is increased, and power consumption decreases.

Jira:RHEL-65487[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]

3.9. BOOT LOADER

GRUB Bootloader has been hardened in RHEL 9.6

This enhancement includes fixes for various security flaws discovered as part of a pro-active hardening effort in the GRUB2 code. This ongoing proactive fuzzing effort of the GRUB bootloader yielded several flaws and vulnerabilities, some of which were severe enough to be CVEs, such as the following:

- CVE-2024-45774 **grub2**: reader/jpeg: Heap out-of-bounds (OOB) Write during JPEG parsing
- CVE-2024-45775 **grub2**: commands/extcmd: Missing check for failed allocation
- CVE-2024-45776 **grub2**: grub-core/gettext: Integer overflow leads to Heap OOB Write and Read.
- CVE-2024-45781 **grub2**: fs/ufs: OOB write in the heap
- CVE-2024-45783 **grub2**: fs/hfs+: **refcount** can be decremented twice
- CVE-2025-0622 **grub2**: command/gpg: Use-after-free due to hooks not being removed on module unload
- CVE-2025-0624: **net**: OOB write in **grub_net_search_config_file()**

- CVE-2025-0677 **grub2**: UFS: Integer overflow may lead to heap based out-of-bounds write when handling symlinks
- CVE-2025-0690 **grub2**: read: Integer overflow may lead to out-of-bounds write

Many of these flaws are buffer or integer overflows where GRUB did not check the integrity or length of variables resulting in the possibility for heap out-of-bounds writes. These were found for a number of filesystems in different contexts. The most severe one, CVE-2025-0624 with a CVSS v3 score of 7.6, is also a potential buffer overflow involving a user-controlled environment variable during network boot. These flaws could lead to overwriting sensitive data up to malicious code execution, and thus bypassing Secure Boot.

All of these flaws and vulnerabilities have been fixed in RHEL 9.6.

Jira:RHELDOCS-20163[1]

3.10. FILE SYSTEMS AND STORAGE

EROFS file system is now 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[1]

snapm is now available in RHEL

Snapshot Manager (**snapm**) is a new component designed to assist in managing system state snapshots. You can use it to roll back updates or changes, and boot into previous system snapshots. Managing snapshots across multiple volumes and configuring boot entries for snapshot boot and snapshot rollback can often be complex and prone to errors. Snapshot Manager automates these common tasks and integrates seamlessly with Boom Boot Manager, simplifying the process. With this update, you can easily take snapshots of the system state, apply updates, and revert to the previous system state if necessary.

Jira:RHEL-59005[1]

NFS with TLS is fully supported

Network File System (NFS) with Transport Layer Security (TLS), introduced in RHEL 9.4 as a Technology Preview, is now fully supported. This feature enhances NFS security by enabling TLS for Remote Procedure Call (RPC) traffic, ensuring encrypted communication between clients and servers. For details, see Configuring an NFS server with TLS support.

Jira:RHEL-59704[1]

VFS mnt_idmap compile-time checking changes backported

This enhancement minimizes conflicts that might occur during the backporting of subsequent fixes or features. As a result, the risk of regressions with subsequent backports is reduced.

Jira:RHEL-33888[1]

CIFS client provides the ability to create special files under SMB shares

Common Internet File System (CIFS) client has the ability to create native Server Message Block (SMB), Network File System (NFS) or Windows Subsystem for Linux (WSL) symlinks. Use the new **symlink=default|none|native|unix|mfsymlinks|sfu|nfs|wsl** mount option to either completely disallow creating symlinks or to select what kind of symlinks will be created by the client. You can also create special files, such as character devices, block devices, pipes, and sockets, through NFS or WSL reparse points by using the **reparse=default|none|nfs|wsl** mount option. To create native Windows sockets that are supported by Windows applications on NT File System (NTFS) volumes, use the **nativesocket** mount option.

Jira:RHEL-76046[1]

3.11. HIGH AVAILABILITY AND CLUSTERS

Deleting multiple resources with a single pcs command

Before this update, the **pcs resource delete**, the **pcs resource remove**, the **pcs stonith delete** and the **pcs stonith remove** commands supported the removal of only one resource at a time. With this update, you can now delete multiple resources at once with a single command.

Jira:RHEL-61901

New pcs tag command option for displaying cluster resource tags in text, JSON, and command formats

The **pcs tag [config]** command now supports the **--output-format** option for the following use cases:

- Displaying the configured text in plain text format by specifying **--output-format=text**. This is the default value for this option.
- Displaying the commands created from the current cluster tags configuration by specifying **--output-format=cmd**. You can use these commands to re-create configured tags on a different system.
- Displaying the configured tags in JSON format by specifying **--output-format=json**, which is suitable for machine parsing.

Jira:RHEL-46284[1]

Support for exporting fencing level configuration in JSON format and as pcs commands

The **pcs stonith config** and the **pcs stonith level config** commands now support the **--output-format=** option to display the fencing level configuration in JSON format and as **pcs** commands.

- Specifying **--output-format=cmd** displays the **pcs** commands created from the current cluster configuration that configure fencing levels. You can use these commands to re-create configured fencing levels on a different system.
- Specifying **--output-format=json** displays the fencing level configuration in JSON format, which is suitable for machine parsing.

Jira:RHEL-16232

Removing Booth cluster tickets from the CIB after removal from the Booth configuration

After you remove a Booth cluster ticket by using the **pcs booth ticket remove** command, the state of the Booth ticket remains loaded in the Cluster Information Base (CIB). This is also the case after you remove a ticket from the Booth configuration on one site and pull the Booth configuration to another

site by using the **pcs booth pull** command. This might cause problems when you configure a ticket constraint, because a ticket constraint can be granted even after a ticket has been removed. As a consequence, the cluster might freeze or fence a node. As of RHEL 9.6, you can prevent this by removing a Booth ticket from the CIB with the **pcs booth ticket cleanup** command.

For information about removing a Booth ticket from the CIB, see Removing a Booth ticket.

Jira:RHEL-69040

3.12. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

A new module stream: mysql:8.4

MySQL 8.4 is now available as a new module stream, **mysql:8.4**. Notable enhancements over the previously available version 8.0 include:

- Enhancements to password management: Administrators can now enforce password expiration, lengths, strength, reuse policy, and other password-related settings.
- Authentication: The **caching_sha2_password** plugin is now the default and replaces the **mysql_native_password** plugin to increase the security.
- Backup Compatibility: The **mysqldump** utility now provides an **--output-as-version** option which enables logical backups to be compatible with older MySQL versions.
- **EXPLAIN**: This statement can now display results in JSON format.
- Deprecation and removal: The following features, which were previously deprecated have been removed:
  - The **mysqlpump** utility
  - The **mysql_native_password** authentication plugin
  - The **mysql_upgrade** utility

For more information about changes in MySQL 8.4, see Notable differences between MySQL 8.0 and MySQL 8.4.

For more information about MariaDB, see Using MariaDB.

To install the **mysql:8.4** stream, enter:

```
# dnf module install mysql:8.4
```

If you want to upgrade from MySQL 8.0, see Upgrading from MySQL 8.0 to MySQL 8.4 .

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

Jira:RHEL-68305[1]

ARGON2 password hashing is supported in PHP 8.3

PHP 8.3 is now available as the **php:8.3** module stream. With this enhancement, support for the **ARGON2I** and **ARGON2ID** password hashing algorithms, provided by the openssl extension, is now available.

Jira:RHEL-73907

nginx 1.26 module stream is now available

The **nginx 1.26** module stream includes various bug fixes and enhancements. Notable changes include:

- HTTP/2 support is now available on a per-server basis.
- Virtual servers can now be used with the stream module.
- Stream connections are now passed to listen sockets.
- Startup performance improvements are made for some complex configurations
- An instantiated service support is now available. The **nginx@.service** unit is an instantiated template service. An instance of this unit uses the **/etc/nginx/*<INSTANCE>*.conf** configuration file, where *INSTANCE* is replaced with the instance name. To allow multiple instances of the **nginx** server to run simultaneously, you must change the following configuration:
  - pid
  - access_log
  - error_log to pick non-conflicting paths, and listen to choose different ports.

You can check the example configuration file **/usr/share/doc/nginx/instance.conf** to understand how to make such changes.

Jira:RHEL-73508[1]

New php:8.3 module stream is now available

The RHEL 9.6 adds PHP 8.3 as a new **php:8.3** module stream. Notable enhancements include:

- Typed class constants
- Dynamic class constant fetch
- New **#[\Override]** attribute
- Deep-cloning of readonly properties

To install the **php:8.3** module stream, use the following command:

```
# dnf module install php:8.3
```

For more information, see the following resources:

- Switching to a later stream .
- Using the PHP scripting language.
- Red Hat Enterprise Linux Application Streams Life Cycle .

If you want to upgrade from the **php:8.2** stream, see Switching to a later stream .

Jira:RHEL-21448[1]

3.13. COMPILERS AND DEVELOPMENT TOOLS

LLVM Toolset updated to 19.1.7

LLVM Toolset has been updated to version 19.1.7.

Notable changes of the LLVM compiler:

- LLVM now uses debug records, a more efficient representation for debug information.

Notable updates of the Clang:

- C++14 sized deallocation is now enabled by default.
- C++17 support has been completed.
- Improvements to C++20 support, especially around modules, concepts, and Class Template Argument Deduction (CTAD) have been added.
- Improvements to C23, C2c, C23, and C2y support have been added.

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-57460

The llvm-doc package now contains only a reference to the upstream documentation.

In previous versions, the **llvm-doc** package contained the LLVM documentation in HTML format. With this update, the package provides only the **/usr/share/doc/llvm/html/index.html** file which contains a reference to the upstream documentation.

Jira:RHEL-68696

Clang and LLVM now support zstd for debug section compression

By default, Clang and LLVM tools use **Zlib** as the algorithm for debug section compression. With this enhancement, users can alternatively use the Zstandard (**zstd**) algorithm which can reach a higher compression rate than **Zlib**.

For example, if you want to use **zstd** compression when you compile a program with Clang, use the following command:

```
$ clang -Wa,-compress-debug-sections=zstd -Wl,--compress-debug-sections=zstd ...
```

Jira:RHEL-70328

Rust Toolset rebased to version 1.84.1

Rust Toolset has been updated to version 1.84.1. Notable enhancements since the previously available version 1.79.0 include:

- The new **LazyCell** and **LazyLock** types delay the initialization until the first use. These extend the earlier **OnceCell** and **OnceLock** types with the initialization function included in each instance.
- The new sort implementations in the standard library improve the runtime performance and compile times. They also try to detect cases where a comparator is not producing a total order, making that panic instead of returning unsorted data.
- Precise capturing for opaque return types have been added. The new **use<..>** syntax specifies the generic parameters and lifetimes used in an **impl Trait** return type.
- Many new features for **const** code have been added, for example:
  - Floating point support
  - **const** immediates for inline assembly
  - References to statics
  - Mutable reference and pointers
- Many new features for **unsafe** code have been added, for example:
  - Strict provenance APIs
  - **&raw** pointer syntax
  - Safely addressing statics
  - Declaring safe items in unsafe **extern** blocks
- The Cargo dependency resolver is now version aware. If a dependency crate specifies its minimum supported Rust version, Cargo uses this information when it resolves the dependency graph instead of using the latest **semver**-compatible crate version.

Compatibility notes:

- The WebAssembly System Interface (WASI) target is changed from **rust-std-static-wasm32-wasi** to **rust-std-static-wasm32-wasip1**. You can select the WASI target also by using the **--target wasm32-wasip1** parameter on the command line. For more information, see the Changes to Rust's WASI targets upstream blog post.
- The split panic hook and panic handler arguments **core::panic::PanicInfo** and **std::panic::PanicInfo** are now different types.
- **extern "C"** functions now abort on uncaught panics. Use **extern "C-unwind"** instead to allow unwinding across ABI boundaries.

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

Jira:RHEL-61964

PCP rebased to version 6.3.2

Performance Co-Pilot (PCP) has been updated to version 6.3.2. Notable changes over the previously available version 6.2.2 include:

- **pmdaopenmetrics**: Virtual Large Language Model (vLLM) metrics are now added by default.
- **pmdalinux**: Support for Hyper-V balloon metrics was added.
- **pmdalinux**: The networking and **hugepages** kernel metrics were updated.
- **pmdaamdgpu**: This new agent collects metrics from **libdrm** and **libdrm-amdgpu** libraries.
- **pmdabpftrace**: The start of this agent with many or slow **bpftrace** scripts was fixed.
- **pmdaproc**: This agent now collects new metrics from AMD GPUs from the Linux **fdinfo** interface.
- **pmdahacluster**: Metrics were updated to support new Pacemaker versions.
- **pmdastatsd**: A bug was fixed to avoid crashes under load.
- **pcp-htop**: AMD GPU metrics support was added.
- **pcp-htop**: Platform settings were fixed to enable screen tabs.
- **pcp-xsos**: This utility was added. For details see **pcp-xsos** provides a rapid summary of a system.
- **pmrep**: Numerous configuration file metric sets were updated.
- **pmlogconf**: Numerous configuration file auto records were updated.
- **libpcp** and **pmcd**: Several security-hardening improvements were added.
- **libpcp** and **pmlogger**: Support for the optional **zstd** compression of archives was added.

Jira:RHEL-58953

The glibc library contains improved IBM POWER10 optimizations

With this enhancement, hardware support for the IBM POWER10 platform has been improved in the **glibc** library. As a result, the performance of the **strcmp()** and **memchr()** APIs has been significantly improved on this platform.

Jira:RHEL-24740[1]

valgrind rebased to version 3.24.0

The **valgrind** suite has been updated to version 3.24.0. Notable enhancements include:

- The **--track-fds=yes** option now shows suppressible errors when using bad file descriptors, and the errors are written to the XML output. The warnings shown, if you do not use the option, are deprecated and will be removed in a future version.
- Error messages now support Ada name demangling.
- The **deflate-conversion** facility (z15/arch13) now supports the deflate compression call (DFLTCC) instruction on the IBM Z platform.
- On the IBM Z platform, **valgrind** now supports the instructions provided by the message security assist (MSA) facility and its 1-9 extensions.

- **Valgrind** now supports the following new Linux system calls:
  - **open_tree**
  - **move_mount**
  - **fsopen**
  - **fsconfig**
  - **fsmount**
  - **fspick**
  - **landlock_create_ruleset**
  - **landlock_add_rule**
  - **landlock_restrict_self**

Jira:RHEL-64070

libabigail rebased to version 2.6

The **libabigail** library has been updated to version 2.6. Notable changes include:

- Better support for Linux kernel module analysis by using the BPF Type Format (BTF) and Common Trace Format (CTF).
- Improved internal type comparison algorithms in the middle end.
- Improved logging in **abipkgdiff**, **abidw**, and **abilint** utilities
- Numerous bug fixes.

For further changes, see the upstream release notes.

Jira:RHEL-64069

SystemTap rebased to version 5.2

The **SystemTap** tracing and probing tool has been updated to version 5.2.

A notable enhancement is the full activation of **debuginfod-metadata** based probes, based on **elfutils** 0.192. With this feature, you can write a **systemtap** script to target a full range of versions of a given binary or library by searching a **debuginfod** server for all matching names.

Jira:RHEL-64066

elfutils rebased to version 0.192

The **elfutils** package has been updated to version 0.192. Notable improvements include:

- The **debuginfod** service can now perform a per-file signature verification to check the integrity by using the RPM Integrity Measurement Architecture (IMA) scheme from RHEL.
- A new **debuginfod** API was added to query server metadata, such as querying the build ID from a file name.

- **Debuginfod** server-side extraction of files from kernel **debuginfo** packages is now significantly faster
- The **dwfl_set_sysroot**, **dwfl_frame_unwound_source**, and **dwfl_unwound_source_str** functions were added to the **libdw** library.
- The **eu-stacktrace** utility is available as a Technology Preview. For details, see **eu-stacktrace** available as a Technology Preview.

Jira:RHEL-64067

The ld linker now detects if an application uses read, write, and execute permissions for a memory region

A memory region with read, write, and execute permissions at the same time is a potential point of attack because a buffer overflow can allow executable code to be injected into the memory and then executed.

With this enhancement, the **ld** linker detects whether an application uses a memory region with these 3 permissions and reports the following error for applications:

```
ld: error: <file_name> has a LOAD segment with RWX permissions
```

You can suppress the error by using **ld** with the **-no-error-rwx-segments** option. However, to prevent a potential risk in your application if the linker does report this error, modify your source code and change how you build your application so that the problem is eliminated.

Jira:RHEL-59802[1]

The ld linker now detects if an application uses an executable stack

A stack that is held in an executable region of memory is a potential point of attacks if, due to a buffer overrun, executable code is placed there.

With this enhancement, the **ld** linker detects whether an application is created with an executable stack and reports errors, such as the following:

```
error: creating an executable stack because of -z execstack command line option
error: <file>: is triggering the generation of an executable stack (because it has an executable
.note.GNU-stack section)
error: <file>: is triggering the generation of an executable stack because it does not have a
.note.GNU-stack section
```

You can suppress the error by using **ld** with the **-no-error-execstack** option. However, to prevent a potential risk in your application if **ld** reports the error, it is better to modify your source code and change the build machinery so that it does not use an executable stack.

Jira:RHEL-59801[1]

binutils now supports the arch15 extension of the IBM Z instruction set

With this enhancement, **binutils** supports the **arch15** extensions of CPUs on the IBM Z platform. Developers can now use the new features provided by the **arch15** extension in assembler source files or, when an updated compiler is available, also in compiled programs. This can result in smaller and faster programs.

Jira:RHEL-50068[1]

The boost-devel package provides BoostConfig.cmake and other official CMake scripts

This enhancement adds **BoostConfig.cmake** and other official CMake scripts to the **boost-devel** package. CMake uses these scripts in some cases to test if **boost** features exists. As a result, CMake projects that test for **boost** features work now more robustly.

Jira:RHEL-67177

Go Toolset rebased to version 1.23

Go Toolset has been updated to version 1.23. 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-62392[1]

glibc now supports the GB18030-2022 encoding standard

This enhancement updates the support of the GB18030 encoding standard in **glibc** from version 2005 to 2022. With version 2022, you can use 31 new transcoding relationships and the additional characters and code points introduced by this standard.

Jira:RHEL-56032[1]

3.14. IDENTITY MANAGEMENT

New tool to manage IdM ID range inconsistencies

With this update, Identity Management (IdM) provides the **ipa-idrange-fix** tool. You can use **ipa-idrange-fix** tool to analyze existing IdM ID ranges, identify users and groups outside these ranges, and propose to create new **ipa-local** ranges to include them.

The **ipa-idrange-fix** tool performs the following:

- Read and analyze existing ranges from LDAP.
- Search for users and groups outside of **ipa-local** ranges.
- Propose new **ipa-local** ranges to cover the identified users and groups.
- Prompt the user to apply the proposed changes.

By default, the tool excludes IDs below 1000 to prevent conflicts with system accounts. Red Hat strongly recommends creating a full system backup before applying any suggested changes.

For more information, see the **ipa-idrange-fix(1)** man page.

Jira:RHEL-45330

Kerberos now supports the Elliptic Curve Diffie-Hellman key agreement algorithm

The Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithm for PKINIT, as defined by RFC5349, is now supported. With this update, the **pkinit_dh_min_bits** setting in **krb5.conf`file can now be configured with `P-256**, **P-384**, or **P-521** to use ECDH by default.

Jira:RHEL-4902

ansible-freeipa rebased to 1.14.5

The **ansible-freeipa** package has been rebased from version 1.13.2 to version 1.14.5. Notable enhancements and bug fixes include:

- You can use **module_defaults** to define variables for multiple **ansible-freeipa** tasks
  The **freeipa.ansible_freeipa** collection now provides the **module_defaults** action group that

simplifies the use of **ansible-freeipa** modules. By using **module_defaults**, you can set default values to be applied to all modules of the collection used in a playbook. To do so, use the **action_group** named **freeipa.ansible_freeipa.modules**. For example:

```
- name: Test
  hosts: localhost
  module_defaults:
    group/freeipa.ansible_freeipa.modules:
      ipaadmin_password: Secret123
  tasks:
...
```

As a result, the playbook is more concise.

- Multiple IdM **sudo** rules can now be managed in a single Ansible task
  This enhancement adds the **sudorules** option to **ansible-freeipa**. By using **sudorules**, you can add, modify, and delete multiple Identity Management (IdM) **sudo** rules by using a single Ansible task. To do this, use the **sudorules** option of the **ipasudorule** module. As a result, you can define your **sudo** rules more easily, and execute them more efficiently.

  Using the **sudorules** option, you can specify multiple **sudo** rule parameters that apply to a particular **sudo** rule. This **sudo** rule is defined by the **name** variable, which is the only mandatory variable for the **sudorules** option.

- Removing external members by using the **ipagroup** module now works correctly
  Previously, attempting to ensure the absence of an external member from an IdM group by using the **ansible-freeipa ipagroup** module with the **externalmember** parameter did not remove the members from the group, even though Ansible presented the result of the task as **changed**. With this fix, using the **ipagroup** module with **externalmember** correctly ensures the absence of an external member from an IdM group. The fix also allows the use of either DOM\name or name@domain to identify AD users.

Jira:RHEL-67566

389-ds-base has been rebased to version 2.6.1

The **389-ds-base** package has been rebased to version 2.6.1. Notable bug fixes and enhancements over version 2.5.2 include:

- Log buffering for the error log
- An option to write the audit log in JSON format
- An option to defer updating group members when the group is updated
- An option to configure a number of PBKDF2 iterations
- The **logconv.py** log analyzer tool

Jira:RHEL-67195

openldap has been rebased to version 2.6.8

The **openldap** package has been updated to version 2.6.8. The update includes various enhancements and bug fixes, including:

- Handling of TLS connections has been improved.

- Kerberos **SASL** works with **STARTTLS** even when the Active Directory certificate is an Elliptic Curve Cryptography (ECC) certificate and **SASL_CBINDING** is set to **tls-endpoint**.

Jira:RHEL-71053

The new memberOfDeferredUpdate: on/off configuration attribute is now available in Directory Server

With this update, Directory Server introduces the new **memberOfDeferredUpdate** configuration attribute for the MemberOf plug-in. When set to **on**, the MemberOf plug-in defers the update of group members resulting in improved server responsiveness, especially if the group changes impact a large number of its members.

For details, see memberOfDeferredUpdate in the RHDS 12 Configuration and schema reference documentation.

Jira:RHEL-5151

Directory Server now provides buffering of the error, audit, and audit fail logs

Before this update, only the access and security logs had log buffering. With this update, Directory Server provides buffering of the error, audit, and audit fail logs. Use the following settings to configure log buffering:

- **nsslapd-errorlog-logbuffering** for the error log. Disabled by default.
- **nsslapd-auditlog-logbuffering** for the audit and audit fail log. Enabled by default.

For details, see nsslapd-errorlog-logbuffering and nsslapd-auditlog-logbuffering in the RHDS Configuration and schema reference documentation.

Jira:RHEL-78650

Directory Server now can update passwords with the CRYPT or CLEAR hashing algorithm after a successful bind

Before this update, Directory Server had a hardcoded list of hashing algorithms that were excluded from the password update during successful binds. Directory Server did not update user passwords that had the CRYPT or CLEAR hashing algorithm configured in the **passwordStorageScheme** attribute.

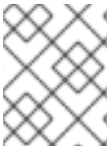
With this update, you can set the list of hashing algorithms that must be excluded from password updates by using the **nsslapd-scheme-list-no-upgrade-hash** configuration attribute. By default, **nsslapd-scheme-list-no-upgrade-hash** contains CRYPT and CLEAR for backward compatibility.

Jira:RHEL-62875

HSM is now fully supported in IdM

Hardware Security Modules (HSM) are now fully supported in Identity Management (IdM). You can store your key pairs and certificates for your IdM Cerificate Authority (CA) and Key Recovery Authority (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 IdM 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 Public-Key Cryptography Standard (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]

3.15. SSSD

New SSSD option: exop_force

You can use the **exop_force** option to force a password change even if no grace logins are left. Previously, SSSD did not attempt password changes if the LDAP server indicated that there were no grace logins remaining. Now, if you set **ldap_pwmodify_mode = exop_force** in the **[domain/...]** section of the **sssd.conf** file, SSSD tries to change the password even if no grace logins are left.

Jira:RHELDOCS-19863[1]

Support for group merging added in authselect

If you are using the **authselect** utility, you no longer need to manually edit the **nssswitch.conf** file to enable group merging. With this update, It is now integrated into **authselect** profiles, eliminating the need for manual changes.

Jira:RHELDOCS-19936[1]

Support for dynamic DoT updates in SSSD

SSSD now supports performing all dynamic DNS (dyndns) queries using DNS-over-TLS (DoT). You can securely update DNS records when IP addresses change, such as Identity Management (IdM) and Active Directory servers. To enable this functionality, you must install the **nsupdate** tool from the **bind9.18-utils** package.

You can use the following new options in the **sssd.conf** file to enable DoT and configure custom certificates for secure DNS updates:

- dyndns_dns_over_tls
- dyndns_tls_ca_cert
- dyndns_tls_cert

- dyndns_tls_key

For more details about these options, see the **sssd-ad(5)** and **sssd-ad(5)** man pages on your system.

Jira:RHELDOCS-20057[1]

3.16. RED HAT ENTERPRISE LINUX SYSTEM ROLES

New variable in the postfix RHEL system role: postfix_default_database_type

The **postfix** system role can determine the default database type used by **postfix** and export it as a variable **postfix_default_database_type**. As a result, you can set configuration parameters based on the default database type.

NOTE

Using **postfix_default_database_type** in a configuration parameter value is not supported on Ansible 2.9.

Jira:RHEL-69983

New variables in the microsoft.sql.server system role: mssql_tools_versions and mssql_tls_self_sign

The new **mssql-tools18** package brings functionality that is not backwards-compatible with the previous versions of the **mssql-tools** package. Therefore the following variables have been added to the **microsoft.sql.server** system role to adapt to the changes:

- **mssql_tools_versions** (list, defaults to version 18): Enables you to install different versions of **mssql-tools**.
- **mssql_tls_self_sign** (boolean): Specifies whether the certificates that you use are self-signed or not. Applicable when you also set the **mssql_tls_enable: true** variable.

IMPORTANT

When you use **mssql-tools18** with self-signed TLS certificates, you have to set **mssql_tls_self_sign: true** so that the role sets the **-C** flag in the **sqlcmd** command-line utility so that your certificates can be trusted.

As a result, you can use these configurations to install **mssql_tools** version 17; 18; or both in parallel.

For more details, see the resources in the **/usr/share/ansible/roles/microsoft.sql-server/** directory.

Jira:RHEL-68374

New RHEL system role: aide

You can use the new **aide** RHEL system role for detecting unauthorized changes to files, directories, and system binaries. With this role, you can accomplish, for example, the following tasks:

- Install the **aide** package on the managed node
- Generate the **/etc/aide.conf** file and template it out to the managed node

- Initialize the (Advanced Intrusion Detection Environment) AIDE database
- Run AIDE integrity checks on the managed node

IMPORTANT

The role does not explain how to create a suitable AIDE configuration.

As a result, you can manage AIDE at scale in an automated fashion to address your security, compliance or auditing needs.

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

Jira:RHEL-67244

New variable in the sudo RHEL system role: sudo_check_if_configured

The **sudo** RHEL system role now has the following variable:

- **sudo_check_if_configured** (boolean): Provides a semantic check of an already configured **sudoers** file in case the Ansible setup is not needed and is skipped.

As a result, you can use this setting to ensure the **sudo** role idempotence if Ansible intervention is not required.

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

Jira:RHEL-61596

The microsoft.sql.server system role enables AES 128-bit and AES 256-bit encryption for AD users

Since version 1.1.83, the **adutil** utility supports the Kerberos protocol with AES 128-bit and AES 256-bit encryption when creating and modifying an Active Directory (AD) user. With this update, the **microsoft.sql.server** system role automates enabling AES 128-bit and AES 256-bit encryption provided by the Kerberos protocol when creating or modifying AD users. As a result, manual post-configuration tasks are not necessary.

Jira:RHEL-67807

The systemd RHEL system role can manage user units in addition to system units

With this update, the **systemd** RHEL system role can now also manage user units. For each unit file or unit specified in **systemd_unit_files**, or **systemd_unit_file_templates**, or **systemd_started_units** etc., you can add a **user: name** if you want that file/unit to be managed for the given user. The default is **root** which is used for system units.

In order to get the units on the system managed by the role, including both system and user units, a new return variable has been added:

- **systemd_units_user** (dictionary): Each key is a name of a user given in one of the lists passed to the role, and **root** (even if **root** is not given). Each value is a dictionary of **systemd** units for that user, or system units for **root**.

IMPORTANT

The role does not create new users and it will return an error if you specify a non-existent user.

As a result, you can manage user units with the **systemd** RHEL system role.

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

Jira:RHEL-27760

Support for exporting corosync configuration of an existing cluster

The **ha_cluster** RHEL system role now supports exporting the **corosync** configuration of an existing cluster in a format that can be fed back to the role to recreate the same cluster. If you did not use the **ha_cluster** RHEL system role to create your cluster, or if you have lost the original playbook for the cluster, you can use this feature to build a new playbook for the cluster.

Jira:RHEL-70483

The podman RHEL system role can manage the quadlet units of type Pod

The **podman** utility of version 5 added support for **Pod** quadlet types. Consequently, the **podman** RHEL system role now enables you to also manage the quadlet units of type **Pod**.

For more details, see the upstream article.

Jira:RHEL-36014

New property added to the network RHEL system role network_connections variable: autoconnect_retries

There is no fine-grained control over the number of automatic retries to reconnect a network connection in the **network** RHEL system role. This limitation could be problematic for certain use cases where extending the retry process is critical, particularly in environments with unstable networks. The **autoconnect_retries** property added to the to the **network_connections** role variable configures how many times NetworkManager attempts to reconnect a network connection after an autoconnect failure. As a result, the **network** RHEL system role now allows configuring the number of automatic reconnection attempts after an autoconnect failure using the **autoconnect_retries** property in the **network_connections** variable. This enhancement provides greater control over network stability and performance, especially in environments with unstable networks.

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

Jira:RHEL-61599

New property added to the network RHEL system role network_connections variable: wait_ip

This update provides added support for the **wait_ip** property of the **ip** option in the **network_connections** role variable. The property specifies if the system should consider the network connection as activated only when a specific IP stack is configured. You can configure **wait_ip** with the following values:

- **any**: The system considers the connection activated once any IP stack is configured.
- **ipv4**: The system waits until IPv4 is configured.
- **ipv6**: The system waits until IPv6 is configured.

- **ipv4+ipv6**: The system waits until both IPv4 and IPv6 are configured.

As a result, the **network** RHEL system role now allows you to configure network connections based on specific IP stack configurations. This enables the connection to remain activated even if an IP address is not assigned, depending on the selected **wait_ip** setting.

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

Jira:RHEL-63026

The metrics RHEL system role now supports Valkey as an alternative to Redis

This update provides added support for the Valkey in-memory data structure store for the **metrics** RHEL system role. It is an alternative to Redis, which is no longer open source and is being removed from Linux distributions. Valkey is typically used as a high-performance caching layer. It stores data in memory, which accelerates applications by caching frequently accessed data. Additionally, you can use Valkey for other performance-critical operations, for example:

- Storing and retrieving user session data.
- Real-time communication between different application parts.
- Providing fast data access for analytics and monitoring.

Jira:RHEL-65748

New variable in the logging RHEL system role: logging_custom_templates

The following variable has been added to the **logging** RHEL system role:

- **logging_custom_templates**: A list of custom template definitions. You can use it with the **logging_outputs** variable when its option is **type: files** or **type: forwards**. You can specify this custom template for each output by setting the **template** option in a particular **logging_outputs** specification. Alternatively, you can set this custom template to be used by default for all files and forwards outputs by using the **logging_files_template_format** and **logging_forwards_template_format** global options.

As a result, you can format log entries differently than what the built-in defaults provide.

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

Jira:RHEL-61947

sshd RHEL system role validates commands and configurations

The **sshd** role uses the **quote** command when using the **command** or **shell** plugins to ensure you can use these commands safely. The role also validates certain user-supplied role variables passed to these plugins. This improves the security and robustness of using the role because, without validation, user-supplied variables that contain white space could split and not function correctly.

Jira:RHEL-73406

3.17. VIRTUALIZATION

KVM on IBM Z now supports more than one boot device

Guest operating systems running on KVM on IBM Z hosts can attempt booting from additional devices when the primary boot device is not bootable. This feature is supported for the following device types:

- **virtio-net**
- **virtio-blk**
- **virtio-scsi/cdrom**

To configure the order of the boot devices for the VM, use the **order** parameter on the **<boot>** line of their XML configuration. The VM will now attempt up to 8 devices for booting.

In addition, these devices now support the **loadparm** parameter for the **<boot>** line of their XML configuration. By using **loadparm**, it is possible to configure which boot entry the device uses when the guest operating system boots from the device.

Jira:RHEL-68440

Virtual machines supported in RHEL for Real Time

This update introduces full support for real-time virtualization in RHEL for Real Time. You can configure the host and guest operating systems to achieve low-latency and deterministic behavior for virtual machines (VMs). This makes real-time VMs suitable for applications that require real-time performance, such as industrial automation, telecommunications, and automotive systems.

Jira:RHELDOCS-20116[1]

Newly supported features for virtual machines on 64-bit ARM hosts

The following features are now supported for virtual machines on RHEL hosts that use the 64-bit ARM architecture, also known as aarch64:

- Migrating VMs between 64-bit ARM hosts. Note, however, that the migration currently only works when both hosts use the same CPU type and memory page size.
- The Trusted Platform Module (TPM) Interface Specification (TIS) hardware interface
- Non-volatile dual in-line memory module (NVDIMM) memory device
- The virtio-iommu device

Jira:RHELDOCS-19832[1]

virt-install now supports creating VMs with SEV-SNP

You can now use the **virt-install** utility to create a virtual machine (VM) that uses the AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) feature. To do so, use the **launchSecurity sev-snp,policy=0x30000** option.

Note that SEV-SNP is currently provided as a Technology Preview.

Jira:RHEL-62959

Support for VM live migration with shared virtiofs directory that provides write access to other parties

With this update, you can live migrate a virtual machine (VM) with a **virtiofs** shared directory, even if multiple other parties, such as the host and other VMs, have write access to that directory.

Jira:RHEL-29027

Virtualization support for IBM z17 processors

With this update, virtualization on RHEL adds support for the IBM z17 CPUs. As a result, virtual machines hosted on an IBM Z system with RHEL can now use new features that the z17 processors provide.

Jira:RHEL-33137[1]

Retrievable secrets are supported for Secure Execution on IBM Z

With this update, you can use generalized host-based secrets for cryptographic devices in Secure Execution virtual machines (VMs) on IBM Z. As a result, it is no longer needed to store secrets in an **initramfs** image when configuring Secure Execution, which simplifies creating a secure VM image. Note that this feature is currently only supported on IBM z17 processors.

Jira:RHEL-50754[1]

Virtualization support for Intel Xeon v6 processors

With this update, virtualization on RHEL 9 adds support for the Intel Xeon v6 processors, formerly known as Sierra Forest. As a result, virtual machines hosted on RHEL 9 can now use the **SierraForest** CPU model and utilize new features that the processors provide.

Jira:RHEL-15731[1], Jira:RHEL-15719

RHEL supports live migrating a VM with a Mellanox virtual function

With this update, you can perform live migration of a virtual machine (VM) with an attached virtual function (VF) of a Mellanox networking device.

However, this feature is currently only supported with a Mellanox CX-7 networking device with a specific firmware version. 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.

For more details and limitations, see: Live migrating a virtual machine with an attached Mellanox virtual function

Jira:RHELDOCS-19210[1]

3.18. RHEL IN CLOUD ENVIRONMENTS

Intel TDX in RHEL guests

The Intel Trust Domain Extension (TDX) feature is now fully supported in RHEL 9.5 and later when used as a guest operating system. If the host system supports TDX, you can deploy hardware-isolated RHEL 9 guests, called trust domains (TDs). This increases the isolation of the RHEL guest from the host, and makes it significantly more difficult for the host to access the data on the RHEL guest.

Jira:RHEL-70465[1]

Unified Kernel Image for RHEL is fully supported

Unified Kernel Image (UKI) for RHEL, which was introduced in RHEL 9.2 as a Technology Preview, is now fully supported. To use RHEL UKI, you must first install the **kernel-uki-virt** package. RHEL UKI can enhance SecureBoot protection in virtualized and cloud environments.

Jira:RHELDOCS-19839[1]

WSL images of RHEL 8 - 10 are available on the Customer Portal

RHEL 8, RHEL 9, and RHEL 10 images for the Windows Subsystem for Linux (WSL) can now be downloaded from the Red Hat Customer Portal. These images are available for all RHEL subscriptions, including no-cost developer subscriptions. By using the WSL images, you can create RHEL instances on your Windows system.

Note that the WSL images are provided as self-supported. As such, they are not supported by Red Hat, and are intended for application development purposes only.

In addition, the following issues are currently present in the RHEL guest operating system if you use a WSL image with a Windows WSL host:

- WSL instances of RHEL might work incorrectly in a graphical interface. Using a text user interface is recommended instead.
- To use podman, you must add the following lines to the **/etc/containers/containers.conf** file, in addition to the standard configuration steps:

```
[network]
firewall_driver="iptables"
```

- To use cloud-init, you must create the **/etc/cloud/cloud.cfg.d/99_wsl.cfg** file and add the following content to it, in addition to the standard configuration steps:

```
datasource_list: [WSL]
network: {config: disabled}
```

- It is not possible to set SELinux to enforcing mode.
- FIPS mode is not available in WSL instances of RHEL.

Jira:RHELDOCS-19876

RHEL on HPE can run up to 4096 vCPUs

With this feature, a RHEL virtual machine (VM) instance running with the RHEL KVM hypervisor on Hewlett Packard Enterprise Compute Scale-Up Server now supports up to 4096 virtual CPUs, 32 sockets, and 64 TB of memory to handle in-memory databases and other large compute intensive workloads.

Jira:RHEL-11043[1]

Enhanced automatic registration for eligible RHEL images

When purchasing certain eligible cloud marketplace subscriptions for RHEL 9.6 or later and for RHEL 10.0 or later, an improved version of the auto-registration function is available.

With the enhanced auto-registration, any RHEL instances on the eligible marketplaces will be automatically registered to Red Hat and automatically receive content updates from Red Hat Update Infrastructure (RHUI) after you establish a trusted connection between your Red Hat account and your account for the respective cloud platform, even if you did not have the trusted connection when you set launched the instance.

For additional details, see Understanding auto-registration.

Jira:RHELDOCS-19664[1]

3.19. SUPPORTABILITY

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]

The --api-url option is now available

With the **--api-url** option you can call another API as per requirement. For instance, 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]

3.20. CONTAINERS

Podman supports pushing and pulling images compressed with zstd:chunked

You can push images compressed with the **zstd:chunked** format to reduce the image size and use partial pulls.

Jira:RHEL-68240

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. The Buildah has been updated to version 1.39.0, Skopeo has been updated toversion 1.18.0. Podman v5.4 contains the following notable bug fixes and enhancements over the previous version:

- The **podman update** command now supports a wide variety of options related to healthchecks: the **--health-cmd** to define a new healthcheck and **--no-healthcheck** to disable an existing healthcheck. These options make it easier to add, modify, or disable healthchecks on running containers. For more information, see the **podman-update(5)** man page.
- The **--mount type=volume** option for the **podman run**, **podman create**, and **podman volume create** commands now supports a new option, **subpath=**, to make only a subset of the volume visible in the container.
- The **--userns=keep-id** option for the **podman run**, **podman create**, and **podman pod create** commands now supports a new option, **--userns=keep-id:size=**, to configure the size of the user namespace.
- The **podman kube play** command now supports Container Device Interface (CDI) devices.

- The **podman run**, **podman create**, and **podman pod create** commands now support a new option, **--hosts-file**, to define the base file used for **/etc/hosts** in the container.
- The **podman run**, **podman create**, and **podman pod create** commands now support a new option, **--no-hostname**, which disables the creation of **/etc/hostname** in the container.
- The **podman network create** command now supports a new option for bridge networks, **--opt mode=unmanaged**, which allows Podman to use an existing network bridge on the system without changes.
- The **--network** option for **podman run**, **podman create**, and **podman pod create** now accepts a new option for bridge networks, **host_interface_name**, which specifies a name for the network interface created outside the container.
- The **podman manifest rm** command now supports a new option, **--ignore**, to proceed successfully when removing manifests that do not exist.
- The **podman system prune** command now supports a new option, **--build**, to remove build containers leftover from prematurely terminated builds.
- Podman now passes container hostnames to Netavark, which uses them for any DHCP requests for the container.
- Packagers can now set the **BUILD_ORIGIN** environment variable when building podman from the Makefile. This provides information on who built the Podman binary, and this information is displayed in the **podman version** and **podman info** commands. Including this information can assist with bug reports by helping maintainers to identify the source and method of the build and installation.
- The **podman kube generate** and **podman kube play** commands can now create and run Kubernetes Job YAML.
- The **podman kube generate** command now includes information on the user namespaces for pods and containers in the generated YAML. The **podman kube play** command uses this information to duplicate the user namespace configuration when creating new pods based on the YAML.
- The **podman kube play** command now supports Kubernetes volumes of type image.
- The service name of **systemd** units generated by Quadlet can now be set with the **ServiceName** key in all supported Quadlet files.
- Quadlets can now disable their implicit dependency on **network-online.target** by using a new key, **DefaultDependencies**, supported by all Quadlet files.
- Quadlet **.container** and **.pod** files now support a new key, **AddHost**, to add hosts to the container or pod.
- The **PublishPort** key in Quadlet **.container** and **.pod** files can now accept variables in its value.
- Quadlet **.container** files now support two new keys, **CgroupsMode** and **StartWithPod**, to configure control groups for the container and whether the container will be started with the pod that it is part of.
- Quadlet **.container** files can now use the network of another container by specifying the **.container** file of the container to share within the Network key.

- Quadlet **.container** files can now mount images managed by **.image** files into the container by using the **Mount=type=image** key with an **.image** target.
- Quadlet **.pod** files now support six new keys, **DNS**, **DNSOption**, **DNSSearch**, **IP**, **IP6**, and **UserNS**, to configure **DNS**, static IPs, and user namespace settings for the pod.
- Quadlet **.image** files can now give an image multiple times by specifying the **ImageTag** key multiple times.
- Quadlets can now be placed in the **/run/containers/systemd** directory as well as existing directories, such as **$HOME/containers/systemd** and **/etc/containers/systemd/users**.
- Quadlet now properly handles subdirectories of a unit directory that is a symlink.
- The **podman manifest inspect** command now includes the manifest's annotations in its output.
- The **--add-host** option for **podman create**, **podman run**, and **podman pod create** now supports specifying multiple hostnames, semicolon-separated (for example **podman run --add-host test1;test2:192.168.1.1**).
- The **podman run** and **podman create** commands now support three new options for configuring healthcheck logging: **--health-log-destination** (specifies where logs are stored), **--health-max-log-count** (specifies how many healthchecks worth of logs are stored), and **--health-max-log-size** (specifies the maximum size of the healthcheck log).

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

Jira:RHEL-66763

Enhanced healthcheck output configuration is now available in Podman

Podman now offers enhanced configurability for healthcheck outputs on a per-container basis. Before this update, healthcheck outputs were limited to the five most recent executions, each capped at 500 characters, accessible only by using the **podman inspect** command. You can now adjust the amount of healthcheck output stored for each container, allowing for more comprehensive debugging information when needed. This feature is particularly beneficial for diagnosing intermittent healthcheck failures without disrupting the running service. Additionally, to address concerns about sensitive data and storage efficiency, you can opt to limit or disable healthcheck output storage for specific containers.

For more details, see the **podman-update** man page.

Jira:RHEL-60561[1]

Deploying a container image by using a single command is now available

You can deploy a container image into a RHEL cloud instance by using a signal command. The **system-reinstall-bootc** command installs performs the following actions:

- Pull the supplied image to set up SSH keys or access the system.
- Run the **bootc install to-existing-root** command with all the bind mounts and SSH keys configured.

Jira:RHELDOCS-19516[1]

Creating custom bootc images from scratch is now supported

You can create **bootc** images from scratch and fully control the contents of the image and tailor the

system environment to meet specific requirements. With the **bootc-base-imgectl** command, you can create custom **bootc** images based on an existing **bootc** base image. Bootc Image from Scratch are derived from container images and do not automatically receive updates from the default base image. To include such updates, you must incorporate them manually as part of your container pipeline. Additionally, you can use the **rechunk** subcommand in **bootc-base-imgectl** on any bootc container image to optimize or restructure the image as needed.

Jira:RHELDOCS-19825[1]

A new image build progressing bar available for bootc-image-builder

Previously, you could not check if an image build was progressing by looking into the logs. With this enhancement, you can check the progress of the image build that you created by using **bootc-image-builder**. You can revert to the previous behavior by using the **--progress=verbose** argument when building images.

Jira:RHELDOCS-20170[1]

The composefs filesystem is now available

The composefs read-only filesystem is now fully supported. This is generally intended only to be used by the bootc/ostree and podman projects at the current time. With composefs, you can use these projects to create and use read-only images, share file data between images, and validate images on runtime. As a result, you have a fully verified filesystem tree mounted, with opportunistic fine-grained sharing of identical files.

Jira:RHEL-18157[1]

3.21. LIGHTSPEED

The command-line assistant powered by RHEL Lightspeed is generally available in RHEL

The command-line assistant powered by RHEL Lightspeed is available within the RHEL command line. The generative AI that powers the assistant is trained on information from the RHEL product documentation and Red Hat Knowledgebase, and can help you to understand, configure, and troubleshoot your RHEL systems in a more accessible way, whether you are new to RHEL or already an experienced user.

Jira:RHELDOCS-20019[1]

The command line assistant supports using the systemd-creds as a password store manager

The command-line assistant powered by RHEL Lightspeed integrates command line assistant daemon (**clad**) by using the **systemd-creds**, a password store manager shipped with RHEL. This means that you can securely store your passwords by using databases such as PostgreSQL or MySQL as your history backend. As a result, you can use the tool for listing, showing, encrypting and decrypting unit credentials in a secure manner.

Jira:RHELDOCS-20024[1]

CHAPTER 4. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel distributed with Red Hat Enterprise Linux 9.6. These changes could include, for example, added or updated **proc** entries, **sysctl**, and **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

New kernel parameters

arm64.no32bit_el0=

[ARM64]

Unconditionally disable the execution of 32 bit applications.

con3215_drop=

[S390]

Format: y|n|Y|N|1|0

When set to true, drop data on the 3215 console when the console buffer is full. In this case the operator using a 3270 terminal emulator (for example x3270) does not have to enter the clear key for the console output to advance and the kernel to continue. This leads to a much faster boot time when a 3270 terminal emulator is active. If no 3270 terminal emulator is used, this parameter has no effect.

stress_hpt=

[PPC]

Limits the number of kernel HPT entries in the hash page table to increase the rate of hash page table faults on kernel addresses.

kvm.enable_virt_at_load=

[KVM,ARM64,LOONGARCH,MIPS,RISCV,X86]

If enabled, KVM will enable virtualization in hardware when KVM is loaded, and disable virtualization when KVM is unloaded (if KVM is built as a module).

If disabled, KVM will dynamically enable and disable virtualization on-demand when creating and destroying VMs, i.e. on the 0⇒1 and 1⇒0 transitions of the number of VMs.

Enabling virtualization at module lode avoids potential latency for creation of the 0⇒1 VM, as KVM serializes virtualization enabling across all online CPUs. The "cost" of enabling virtualization when KVM is loaded, is that doing so may interfere with using out-of-tree hypervisors that want to "own" virtualization hardware.

kvm-arm.wfe_trap_policy=

[KVM,ARM]

Control when to set WFE instruction trap for KVM VMs. Traps are allowed but not guaranteed by the CPU architecture.

trap: set WFE instruction trap

notrap: clear WFE instruction trap

kvm-arm.wfi_trap_policy=

[KVM,ARM]

Control when to set WFI instruction trap for KVM VMs. Traps are allowed but not guaranteed by the CPU architecture.

trap: set WFI instruction trap

notrap: clear WFI instruction trap

config_acs=

Format: <ACS flags>@<pci_dev>[; ...]

Specify one or more PCI devices (in the format specified above) optionally prepended with flags and separated by semicolons. The respective capabilities will be enabled, disabled or unchanged based on what is specified in flags.

ACS Flags is defined as follows:

bit-0
ACS Source Validation

bit-1
ACS Translation Blocking

bit-2
ACS P2P Request Redirect

bit-3
ACS P2P Completion Redirect

bit-4
ACS Upstream Forwarding

bit-5
ACS P2P Egress Control

bit-6
ACS Direct Translated P2P

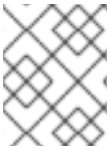
Each bit can be marked as:

0 – force disabled

1 – force enabled

x – unchanged

For example, pci=config_acs=10x would configure all devices that support ACS to enable P2P Request Redirect, disable Translation Blocking, and leave Source Validation unchanged from whatever power-up or firmware set it to.



NOTE

This may remove isolation between devices and may put more devices in an IOMMU group.

rcutree.nocb_nobypass_lim_per_jiffy=

[KNL]

On callback-offloaded (rcu_nocbs) CPUs, RCU reduces the lock contention that would otherwise be caused by callback floods through use of the →nocb_bypass list. However, in the common non-flooded case, RCU queues directly to the main →cblist in order to avoid the extra overhead of the →nocb_bypass list and its lock. But if there are too many callbacks queued during a single jiffy, RCU pre-queues the callbacks into the →nocb_bypass queue. The definition of "too many" is supplied by this kernel boot parameter.

rcutree.nohz_full_patience_delay=

[KNL]

On callback-offloaded (rcu_nocbs) CPUs, avoid disturbing RCU unless the grace period has reached the specified age in milliseconds. Defaults to zero. Large values will be capped at five seconds. All values will be rounded down to the nearest value representable by jiffies.

rcutree.rcu_divisor=

[KNL]

Set the shift-right count to use to compute the callback-invocation batch limit bl from the number of callbacks queued on this CPU. The result will be bounded below by the value of the rcutree.blimit kernel parameter. Every bl callbacks, the softirq handler will exit in order to allow the CPU to do other work.

Please note that this callback-invocation batch limit applies only to non-offloaded callback invocation. Offloaded callbacks are instead invoked in the context of an rcuoc kthread, which scheduler will preempt as it does any other task.

rcutree.enable_rcu_lazy=

[KNL]

To save power, batch RCU callbacks and flush after delay, memory pressure or callback list growing too big.

rcutree.rcu_normal_wake_from_gp=

[KNL]

Reduces a latency of synchronize_rcu() call. This approach maintains its own track of synchronize_rcu() callers, so it does not interact with regular callbacks because it does not use a call_rcu[_hurry]() path. Please note, this is for a normal grace period.

How to enable it:

echo 1 > /sys/module/rcutree/parameters/rcu_normal_wake_from_gp or pass a boot parameter "rcutree.rcu_normal_wake_from_gp=1"

Default is 0.

Removed kernel parameters

clocksource.max_cswd_read_retries=

[KNL]

Number of clocksource_watchdog() retries due to external delays before the clock will be marked unstable. Defaults to two retries, that is, three attempts to read the clock under test.

disable_cpu_apicid=

[X86,APIC,SMP]

Format: <int>

The number of initial APIC ID for the corresponding CPU to be disabled at boot, mostly used for the kdump 2nd kernel to disable BSP to wake up multiple CPUs without causing system reset or hang due to sending INIT from AP to BSP.

Changed kernel parameters

amd_iommu=

[HW,X86_64]

Pass parameters to the AMD IOMMU driver in the system.

Possible values are:

fullflush

Deprecated, equivalent to iommu.strict=1

off

do not initialize any AMD IOMMU found in the system

force_isolation

Force device isolation for all devices. The IOMMU driver is not allowed anymore to lift isolation requirements as needed. This option does not override iommu=pt

force_enable

Force enable the IOMMU on platforms known to be buggy with IOMMU enabled. Use this option with care.

pgtbl_v1

Use v1 page table for DMA-API (Default).

pgtbl_v2

Use v2 page table for DMA-API.

irtcachedis

Disable Interrupt Remapping Table (IRT) caching.

nohugepages

Limit page-sizes used for v1 page-tables to 4 KiB.

v2_pgsizes_only

Limit page-sizes used for v1 page-tables to 4KiB/2Mib/1GiB.

debug_guardpage_minorder=

[KNL]

When CONFIG_DEBUG_PAGEALLOC is set, this parameter allows control of the order of pages that will be intentionally kept free (and hence protected) by the buddy allocator. Bigger value increase the probability of catching random memory corruption, but reduce the amount of memory for normal system use. The maximum possible value is MAX_PAGE_ORDER/2. Setting this parameter to 1 or 2 should be enough to identify most random memory corruption problems caused by bugs in kernel or driver code when a CPU writes to (or reads from) a random memory location. Note that there exists a class of memory corruptions problems caused by buggy H/W or F/W or by drivers badly programming DMA (basically when memory is written at bus level and the CPU MMU is bypassed) which are not detectable by CONFIG_DEBUG_PAGEALLOC, hence this option will not help tracking down these problems.

page_reporting.page_reporting_order=

[KNL]

Minimal page reporting order.

Format: <integer>

Adjust the minimal page reporting order. The page reporting is disabled when it exceeds MAX_PAGE_ORDER.

preempt=

[KNL]

Select preemption mode if you have CONFIG_PREEMPT_DYNAMIC none - Limited to cond_resched() calls voluntary - Limited to cond_resched() and might_sleep() calls full - Any section that isn't explicitly preempt disabled can be preempted anytime. Tasks will also yield contended spinlocks (if the critical section isn't explicitly preempt disabled beyond the lock itself).

sched_thermal_decay_shift=

[Deprecated] [KNL, SMP]

Set a decay shift for scheduler thermal pressure signal. Thermal pressure signal follows the default decay period of other scheduler pelt.

usb-storage.delay_use=

[UMS]

The delay in seconds before a new device is scanned for Logical Units (default 1). Optionally the delay in milliseconds if the value has suffix with "ms". Example: delay_use=2567ms.

New sysctl parameters

skb_defer_max

Max size (in skbs) of the per-cpu list of skbs being freed by the cpu which allocated them. Used by TCP stack so far.

Default: 64

Changed sysctl parameters

overcommit_memory

This value contains a flag that enables memory overcommitment.

When this flag is 0, the kernel compares the userspace memory request size against total memory plus swap and rejects obvious overcommits.

When this flag is 1, the kernel pretends there is always enough memory until it actually runs out.

When this flag is 2, the kernel uses a "never overcommit" policy that attempts to prevent any overcommit of memory. Note that user_reserve_kbytes affects this policy.

This feature can be very useful because there are a lot of programs that malloc() huge amounts of memory "just-in-case" and don't use much of it.

The default value is 0.

See Documentation/mm/overcommit-accounting.rst and mm/util.c::__vm_enough_memory() for more information.

CHAPTER 5. BUG FIXES

This part describes bugs fixed in Red Hat Enterprise Linux 9.6 that have a significant impact on users.

5.1. SECURITY

shlibsign now works in FIPS mode

Before this update, the **shlibsign** program did not work in FIPS mode. Consequently, when you rebuilt an NSS library in FIPS mode, you had to leave FIPS mode to sign the library. The program has been fixed, and you can now use **shlibsign** in FIPS mode.

Jira:RHEL-58260

Audit now loads rules referencing /usr/lib/modules/

Prior to this update, when the **ProtectKernelModules** option was set to **true** for the **auditd.service**, the Audit subsystem did not load rules that reference files in the **/usr/lib/modules/** directory with the error message **Error sending add rule data request (No such file or directory)**. With this update, Audit loads also these rules, and you no longer have to reload the rules by using the **auditctl -R** or **augenrules --load** commands.

Jira:RHEL-59570[1]

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

When extracting certificates from the trust store, 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]

Rule to allow dac_override and dac_read_search for qemu-guest-agent added to the SELinux policy

Previously, the SELinux policy did not have rules to allow **qemu-guest-agent** the **dac_override** and **dac_read_search** capabilities. As a consequence, freezing and thawing virtual machine file systems did not work properly when the file system mount point DAC permission did not grant access to the user root. This update has added the missing rule to the policy. As a result, **fsfreeze**, which is an important **qemu-ga** command for creating consistent snapshots, works correctly.

Jira:RHEL-52476

OpenSSL cipher suites no longer enable cipher suites with disabled hashes or MACs

Previously, applying custom cryptographic policies could leave certain TLS 1.3 cipher suites enabled even if their hashes or MACs were disabled, because the OpenSSL TLS 1.3-specific **Ciphersuites** option values were controlled only by the **ciphers** option of the cryptographic policy. With this update, **crypto-policies** takes more algorithms into account when deciding whether to enable a cipher suite. As a result, OpenSSL on systems with custom cryptographic policies might refuse to negotiate some of the previously enabled TLS 1.3 cipher suites in better accordance with the system configuration.

Jira:RHEL-76528[1]

5.2. SUBSCRIPTION MANAGEMENT

RHEL web console Subscription Manager plugin now detects Insights data upload failures

Before this update, the **systemd** service manager automatically restarted **insights-client** service in the case of failure, which broke the built-in detection in the Subscription Manager plugin in the RHEL web console. This detection checked for the failed service state, which was correctly prevented. Consequently, the RHEL web console did not display any warning when an Insights data upload failed. With this update, the detection of the status of **insights-client** has been improved to account for the new status when an upload fails. As a result, Subscription Manager in the web console detects Insights data upload failures correctly.

Jira:RHEL-56159

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
```

Jira:RHELPLAN-137234[1]

5.3. SOFTWARE MANAGEMENT

dnf needs-restarting --reboothint now correctly reports whether a reboot is needed on systems with a real-time clock not running in UTC

Before this update, if you updated a package which required a system reboot to fully apply the update on a system with a real time clock not running in UTC, the **dnf needs-restarting --reboothint** command might not have reported that the reboot was needed. With this update, the **systemd** UnitsLoadStartTimestamp property is added as a preferred source of a boot time. As a result, **dnf needs-restarting --reboothint** is now more reliable outside of containers on systems with a real-time clock running in local time.

Jira:RHEL-14900

The repository metadata is now stored directly in the requested directory when using dnf reposync

Before this update, the **dnf reposync** command did not respect the **--norepopath** option for downloading a repository metadata. Consequently, this metadata was stored in a subdirectory named after the repository. With this update, the **dnf reposync** command now respects the **--norepopath** option, and the repository metadata is stored directly in the requested directory.

Jira:RHEL-40914

%patch N no longer applies a patch number 0

Before this update, when you used the **%patch N** syntax, where **N** is the number of a patch, the syntax also applied the patch number 0 (**Patch0**) in addition to the patch specified by **N**. With this update, the **%patch N** syntax has been fixed to only apply the patch number **N**.

IMPORTANT

If you use the **%patch** directive without a patch number specified, as a shorthand for **%patch 0**, **Patch0** is applied. However, a warning is printed that suggests you to use the explicit syntax, for example, **%patch 0** or **%patch -P 0** instead of **%patch** to apply the **zero-th** patch.

Jira:RHEL-6294

5.4. SHELLS AND COMMAND-LINE TOOLS

lparstat -E now displays correct values for busy and idle states

Previously, some values were not taken into account while calculating the idle ticks. As a consequence, the **lparstat -E** command displayed the busy and idle states under the **Normalized** and **Actual** sections, for example, **lparstat -E 4 4**. With this update, the calculation of the idle tick has been fixed. As a result, the **lparstat -E** utility now displays the correct values for busy and idle states.

Jira:RHEL-61089[1]

Traceroute now defaults to IPv6

Previously, traceroute defaulted to IPv4 addresses even when IPv6 addresses were available. With this enhancement, traceroute now defaults to IPv6 if available.

Jira:RHEL-59444

5.5. NETWORKING

Networking interface configuration persists after lldpad termination

Before this update, the networking interface configuration was removed when Link Layer Discovery Protocol Agent Daemon (**lldpad**) was terminated by **systemd** or manually. This update fixes the **lldpad** source-code so that the service does not reset interface configuration after termination.

Jira:RHEL-61874

RHEL displays the correct number of CPUs on a system of 512 CPUs

The **rps_default_mask** configuration setting controls the default Receive Packet Steering (**rps**) mechanism to direct incoming network packets towards specific CPUs. The **flow_limit_cpu_bitmap** parameter enables or disables flow control per CPU. With this fix, RHEL displays total CPUs along with its parameter values on the console correctly.

Jira:RHEL-61203

The netdev device attributes are removed from ethtool output

Due to changes in network device feature flags stored in the kernel, the following features will no longer appear in the output of the **ethtool -k** command:

- **tx-lockless**

- **netns-local**
- **fcoe-mtu**

Note that these flags were not features, but rather device attributes or properties that could not be changed by using the **ethtool -K** command in any driver.

Jira:RHEL-59091[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.

Jira:RHEL-69899

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]

5.6. FILE SYSTEMS AND STORAGE

multipathd no longer crashes because of errors encountered by the ontap prioritizer

Before this update, **multipathd** crashed when it was configured to use the ontap prioritizer on an unsupported path, because the prioritizer only works with NetApp storage arrays. This failure occurred due to a bug in the prioritizer's error logging code, which caused it to overflow the error message buffer. With this update, the error logging code has been fixed, and **multipathd** no longer crashes because of errors encountered by the ontap prioritizer.

Jira:RHEL-58920[1]

Native NVMe multipathing no longer causes a memory leak when enable_foreign is set to monitor natively multipathed NVMe devices

Before this update, enabling native NVMe multipathing caused a memory leak if the **enable_foreign** configuration parameter was set to monitor natively multipathed NVMe devices. With this update, the memory leak was fixed in **multipathd** monitoring code. As a result, **multipathd** can now monitor natively multipathed NVMe devices without increasing memory usage.

Jira:RHEL-73413[1]

RHEL installer now discovers and uses iSCSI devices as boot devices on aarch64

Previously, the absence of the **iscsi_ibft** kernel module in RHEL installers running on **aarch64** prevented the automatic discovery of iSCSI devices defined in firmware. As a result, these devices were not automatically visible nor selectable as boot devices in the installer during manual addition GUI.

This issue has been resolved by including the **iscsi_ibft** kernel module in newer **aarch64** builds of RHEL. As a result, the iSCSI devices are now automatically detected and available as boot options during installation.

Jira:RHEL-56135[1]

fstrim enabled by default on LUKS2 root in ostree-based new installations done by Anaconda

Previously, installing ostree-based systems, such as Image Mode, by using **ostreesetup** or **ostreecontainer** Kickstart commands with LUKS2 encryption enabled on the / (root) mount point resulted in systems where **fstrim** was not enabled. This could cause issues such as unresponsive systems or broken file chooser dialogs. With this fix, **fstrim** (discards) is now enabled by default in the LUKS2 metadata on newly installed systems.

To fix this issue in the existing installations, run the following command: .... **cryptsetup --allow-discards --persistent refresh <luks device>** .... **<luks device>** is the path to the root LUKS2 device.

Jira:RHEL-82430

Systems with NVMe over TCP controllers no longer crash because of a data transfer failure

Before this update, on 64-bit ARM architecture systems with NVMe over TCP storage controllers where optimal IO size is bigger than the PAGE_SIZE and an MD device uses a bitmap, the system could crash with the following error message:

> usercopy: Kernel memory exposure attempt detected from SLUB object 'kmalloc-512' (offset 440, size 24576)!

With this update, kernel checks that the final IO size does not exceed the bitmap length. As a result, the system no longer crashes.

Jira:RHEL-46615[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]

5.7. HIGH AVAILABILITY AND CLUSTERS

Resource constraints with expired rules no longer display

Before this update, the **pcs constraint location config resources** command displayed resource constraints with expired rules in the output. With this update, the command no longer displays constraints with expired rules if you do not specify the **--all** option.

Jira:RHEL-46293[1]

Status of a cloned resource running with only one instance now displays properly

Before this update, when you queried the status of the instances of a cluster resource clone with only one running instance, the **pcs status query** command displayed an error message. With this update, the command reports the resource status properly.

Jira:RHEL-55441

Successful recovery of an interrupted Pacemaker remote connection

Before this update, when network communication was interrupted between a Pacemaker remote node and the cluster node hosting its connection during the TLS handshake portion of the initial connection, the connection in some cases blocked and could not be recovered on another cluster node. With this update, the TLS handshake is asynchronous and a remote connection is successfully recovered elsewhere.

Jira:RHEL-34276

Cluster status of a disaster recovery site now displays correctly

Before this update, when you configured a disaster recovery recovery site and ran the **pcs dr status** command to display the status of the local and remote cluster sites, the command displayed an error instead of the cluster status. With this update, the cluster status of the local and remote sites displays correctly when you execute this command.

Jira:RHEL-61738

Cluster alerts now take immediate effect

Before this update, when you configured an alert in a Pacemaker cluster, the alert did not immediately take effect without a cluster restart. With this update, the cluster detects updates to cluster alerts immediately.

Jira:RHEL-55458

5.8. COMPILERS AND DEVELOPMENT TOOLS

The glibc getenv function provides a limited form of thread safety

The **glibc getenv** function is not thread safe. Previously, if an application still called the functions **getenv**, **setenv**, **unsetenv**, **putenv**, and **clearenv** at the same time, the application they could terminate unexpectedly or **getenv** could return incorrect values. With this bug fix, the **getenv** function provides a limited form of thread safety. As a result, applications no longer crash if they call the functions concurrently. Additionally, **getenv** returns only environment values that have been using **setenv** or which were present at the start of the program, and reports previously-set environment variables as unset only if there has been a potentially unordered **unsetenv** call.

This fix is not applicable if you directly modify the **environ** array.

Jira:RHEL-67692

The pcp package now sets the correct owner and group for the /var/lib/pcp/config/pmie/config.default file

Previously, if you installed the **pcp** package for the first time, the package installation process incorrectly set the ownership of the **/var/lib/pcp/config/pmie/config.default** file to **root:root**. As a consequence, the **pmie** service failed to start because the **pmieconf** utility, which is executed by this service, requires **pcp:pcp** ownership for this file. When the service failed to start, it logged the following error in the **/var/log/pcp/pmie/pmie_check.log** file:

```
Warning: no write access to pmieconf file "/var/lib/pcp/config/pmie/config.default", skip reconfiguration
```

With this update, the **pcp** package sets the correct ownership for the **/var/lib/pcp/config/pmie/config.default** file during the first installation and fixes it on existing installations. As a result, the **pmie** service starts correctly.

Jira:RHEL-59366

pcp-xsos provides a rapid summary of a system

The large number of configurable components in the Performance Co-Pilot (PCP) toolkit means that you often use several different tools to understand a system's performance. Many of these tools require additional processing time when you work with large, compressed time series data volumes. This enhancement adds the **pcp-xsos** utility to PCP. This utility can perform a fast, high-level analysis of an individual point in time from a PCP archive. As a result, **pcp-xsos** can help you gain insight into high level performance issues and also identify further targeted performance analysis tasks.

Jira:RHEL-30590[1]

iconv in-place conversions no longer result in corrupted output

The **iconv** utility can write the converted output to the same file. Previously, when you performed an in-place conversion and the source file exceeded a certain size, **iconv** overwrite the file before the processing was completed. Consequently, the file was corrupted. With this update, the utility creates a temporary file if the source and the output file are the same and overrides the source file after the conversion is complete. As a result, in-place conversions can no longer result in corrupted files.

Jira:RHEL-1915

Improvements in the glibc stub resolver and getaddrinfo() API calls

Previously, the **glibc** stub resolver and **getaddrinfo()** API calls could result in longer than expected delays in the following cases:

- The server was inaccessible.
- The server refused the query.
- The network packet with the query was lost.

With this update, the delays in failure cases are reduced and a new resolver option, **RES_STRICTERR**, was added. With this option, **getaddrinfo()** API calls report more DNS errors. Additionally, you can now use options with a **-** negative prefix in configuration files.

Jira:RHEL-50662[1]

The glibc exit function no longer crashes on simultaneous calls

Previously, multiple simultaneous calls to the **exit** function and calls to this function with simultaneous **<stdio.h>** stream operations were not synchronized. As a consequence, applications could terminate unexpectedly and data streams could be corrupted if a concurrent **exit** function call occurred in a multi-threaded application. With this update, **exit** now locks **<stdio.h>** streams when flushing them, and simultaneous calls to **exit** and **quick_exit** select one call to proceed. As a result, applications no longer crash in this scenario.

As a consequence of the fix, applications that perform a blocking read operation on a **<stdio.h>** stream, such as the **getchar** function, or that have a locked stream that uses the **flockfile** function cannot exit until the read operation returns or the lock is released. Such blocking is required by the POSIX standard.

Jira:RHEL-65358[1]

The implementation of POSIX thread condition variables in glibc to wake waiting threads has been improved

Previously, a defect in the POSIX thread condition variable implementation could allow a **pthread_signal()** API call to fail to wake a waiting thread. Consequently, a thread could wait indefinitely for a next signal or broadcast. With this bug fix, the implementation of POSIX thread condition variables now includes a sequence-relative algorithm to avoid the missed signal condition and to provide stronger guarantees that waiting threads are woken correctly.

Jira:RHEL-2419

The Boost.Asio no longer shows an exception when reusing a moved TCP socket

Previously, if an application used the **Boost.Asio** library and reused a moved TCP socket, the application failed with an **bad_executor** exception. This update fixes the issue, and the **Boost.Asio** library no longer fails in the described scenario.

Jira:RHEL-67973[1]

5.9. IDENTITY MANAGEMENT

Migrating an IdM deployment no longer results in duplicate HBAC rules

Previously, migrating from one Identity Management (IdM) deployment to another by using the **ipa-migrate** utility sometimes led to duplicate host-based access control (HBAC) rules on the destination server. Consequently, the "allow_all" and "allow_systemd-user" HBAC rules appeared twice when running the "ipa hbacrule-find" command on that server.

The problem has been fixed and migrating IdM deployments no longer results in duplicate HBAC rules.

Jira:RHEL-48104

Bypassing two-factor authentication using an expired token is no longer possible

Previously, it was possible to bypass two-factor authentication by creating an OTP token with a specific end-validity period.

In cases where two-factor authentication is enforced, a user without an OTP token could use their password to log in **once** and configure an OTP token. Subsequently, they would be required to use both their password and the OTP token for authentication. However, if a user created an OTP token with an expired end-validity date, IdM would incorrectly fall back to password-only authentication, effectively bypassing two-factor authentication. This was due to IdM not differentiating between non-existent and expired OTP tokens.

With this update, IdM now correctly differentiates between these scenarios. Consequently, two-factor authentication is now correctly enforced, preventing this bypass.

Jira:RHEL-4915

When starting an instance with a sub suffix, an incorrect error is no longer logged

Before this update, when starting an instance with a sub suffix, you could see the following incorrect message in the error log:

```
[time_stamp] - ERR - id2entry - Could not open id2entry err 0
[time_stamp] - ERR - dn2entry_ext - The dn "dc=example,dc=com" was in the entryrdn index, but it did not exist in id2entry of instance userRoot.
```

The root cause of the message was that during backend initialization, a subtree search was performed on the backend to determine if the subtree contained smart referrals. In addition, the issue had a minor performance impact on search operations for the first ten minutes after the server started.

With this update, the incorrect message is no longer logged and no performance impact occurs when the server starts.

Jira:RHEL-71218[1]

ldapsearch now respects the NETWORK_TIMEOUT setting as expected

Previously, an **ldapsearch** command ignored the timeout when the server was unreachable and, as a consequence, the search hung indefinitely instead of timing out. With this update, the logic error in TLS handling was fixed by adjusting connection retries and socket options.

As a consequence, the **ldapsearch** command no longer ignores the NETWORK_TIMEOUT setting and returns the following error when the timeout is reached:

```
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1).
```

Jira:RHEL-78297[1]

A race condition with paged result searches no longer closes the connection with a T3 error code

Previously, Directory Server did not use the proper thread protection when checking the connection's paged result data for a timeout event. As a consequence, the paged result timeout value changed

unexpectedly and triggered a false timeout when a new operation arrived. This caused a time out error and the connection was closed with the following **T3** error code:

The server closed the connection because the specified time limit for a paged result search has been exceeded.

With this update, the proper thread protection is used, and paged result searches no longer close the connection with a **T3** error code.

Jira:RHEL-76019[1]

Directory Server no longer fails when reindexing a VLV index with the sort attribute indexed with an extended matching rule

Before this update, a race condition was triggered during reindexing a virtual list views (VLV) index that had the sort attribute indexed with an extended matching rule. As a result, memory leaked and Directory Server failed. With this update, Directory Server serializes the VLV index key generation and no longer fails.

Jira:RHEL-67020

OpenLDAP library no longer fails when trying to free resources

Before this update, the OpenLDAP library tried to release memory by using the **SSL_CTX_free()** function in its destructor when an application had already cleaned up these resources by invoking the **OPENSSL_cleanup()** function, either directly or via the **atexit()** function. As a consequence, users experienced failures or undefined behavior when the invalid **SSL_CTX_free()** call tried to release already-cleaned-up SSL context resources.

With this update, a safe cleanup function has been added to skip SSL context cleanup in the OpenLDAP's destructor. As a result, the SSL context now leaks if not explicitly freed, ensuring a stable application shutdown.

Jira:RHEL-56502

High connection load no longer overloads a single thread in Directory Server

Before this update, even though Directory Server supports multiple listening threads, the first incoming connections were assigned to the same listener thread overloading it. As a result, some requests created high **wtime** and poor performance. With this update, Directory Server distributes the connection load across all listening threads.

Jira:RHEL-70252

VLV index cache now matches the VLV index as expected when using LMDB

Before this update, the virtual list views (VLV) index cache did not match the VLV index itself on instances with Lightning Memory-Mapped Database (LMDB), which caused the VLV index to return invalid values. With this update, the VLV index cache matches the VLV index, and the correct values are returned.

Jira:RHEL-64438[1]

The online backup no longer fails

Before this update, the online backup task could hang sporadically because of the incorrect lock order. With this update, the online backup works as expected and no longer fails.

Jira:RHEL-67005[1]

cleanAllRUV no longer blocks itself

Before this update, when you ran the **cleanAllRUV** task after a replica deletion from replication topology, the task was trying to update the replication configuration entry while the same task was purging the replication changelog of the old replica ID (**rid**). As a result, the server was unresponsive.

With this update, **cleanAllRUV** cleans up the replication configuration only after the changelog purging is complete.

Jira:RHEL-60135

Reindexing no longer fails when an entry RDN have the same value as the suffix DN

Before this update, if an entry's relative distinguished name (RDN) had the same value as the suffix distinguished name (DN) in the directory, then the **entryrdn** index got broken. As a result, Directory Server could perform slow search requests, get invalid results, and write alarming messages in the error log.

With this update, reindexing works as expected.

Jira:RHEL-74158[1]

The Account Policy plug-in now uses a proper flag for an update in a replication topology

Before this update, the Account Policy plugin did not use the proper flag for an update. As a result, in a replication topology, the Account Policy plugin updated the login history, but this update failed on a consumer server logging the following error message:

```
{{ERR - acct_update_login_history - Modify error 10 on entry
}}
```

With this update, the internal update succeeds and no errors are logged.

Jira:RHEL-74168[1]

On a supplier with LMDB, an offline import no longer generates duplicates of nsuniqueid

Before this update, an offline import of basic entries (with no replicated data) on a supplier with Lightning Memory-Mapped Database (LMDB) generated duplicates of the **nsuniqueid** operational attribute that must be unique. As a result, problems with replication occurred. With this update, the offline import no longer generates duplicates on the supplier.

Jira:RHEL-78344[1]

TLS 1.3 can now be used to connect to an LDAP server running in FIPS mode

Before this update, when you tried to explicitly set TLS 1.3 when connecting to an LDAP server in FIPS mode, the used TLS version still remained 1.2. As a result, an attempt to connect to the LDAP server by using TLS 1.3 failed. With this update, the upper limit of the TLS version in FIPS mode was changed to 1.3, and the attempt to connect to an LDAP server with TLS 1.3 no longer fails.

Jira:RHEL-78722

Directory Server backup no longer fails after the previous unsuccessful attempt

Before this update, if an initial backup attempt was unsuccessful, the next Directory Server backup failed

because backends stayed busy trying to complete the previous backup. As a result, the instance restart was required. With this update, Directory Server backup no longer fails after the previous unsuccessful attempt and the instance restart is no longer needed.

Jira:RHEL-61341

Failed replication between suppliers when using certificate-based authentication now has a more descriptive error message

Before this update, when a required CA certificate file was missing and a TLS connection setup was failing during replication between supplies, the error message was unclear to identify the problem. With this update, when a TLS setup error occurs, Directory Server logs more detailed error information. It now includes messages, such as **No such file or directory** for a missing certificate, making the problem solving easier.

Jira:RHEL-65662[1]

dsconf config replace can now handle multivalued attributes as expected

Before this update, the **dsconf config replace** command could set only one value for an attribute, such as **nsslapd-haproxy-trusted-ip**. With this release, you can set several values by using the following command:

```
# dsconf <instace_name> config replace nsslapd-haproxy-trusted-ip=<ip_address_1> nsslapd-haproxy-trusted-ip=<ip_address_2> nsslapd-haproxy-trusted-ip=<ip_address_3>
```

Jira:RHEL-67004

Directory Server now returns the correct set of entries when compound filters with OR (|) and NOT (!) operators are used

Before this update, when LDAP searches with OR (|) and NOT (**!**) operators were used, Directory Server did not return the correct set of entries. The reason was that Directory Server incorrectly evaluated access rights and entry matching and performed these steps in one phase. With this update, Directory Server performs access rights evaluation and entry matching in two separated phases and searches with compound filters with OR (|) and NOT (**!**) operators return the correct set of entries.

Jira:RHEL-65776[1]

Consumer status in a replication agreement on a supplier is displayed correctly after the Directory Server restart

Before this update, on a supplier in a replication topology, the status of the consumer in a replication agreement was reset during the Directory Server restart. As a result, the displayed consumer initialization time and the replication status were incorrect.

With this update, the replication agreement entry displays the correct status of the consumer and when it was initialized.

Jira:RHEL-67008

5.10. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The new sshd_allow_restart variable enables the sshd service to be restarted when needed

Before this update, the **sshd** RHEL system role was not restarting the **sshd** service on a managed node

when required. As a consequence, some changes related to configuration files from the`/etc/sysconfig/` directory and environment files were not applied. To fix the problem, the **sshd_allow_restart** (boolean, defaults to **true**) variable has been introduced to restart the **sshd** service on the managed node when necessary. As a result, the **sshd** RHEL system role now correctly applies all changes and ensures the **sshd** service actually uses those changes.

Jira:RHEL-73409

The podman RHEL system role no longer fails to process secrets when using the run_as_user variable

Before this update, the **podman** RHEL system role failed to process secrets that were specified for a particular user using the **run_as_user** variable due to missing user information. This caused errors when attempting to process secrets which have **run_as_user** set. The issue has been fixed, and the **podman** RHEL system role correctly handles secrets which are specified for a particular user using the **run_as_user** variable.

Jira:RHEL-73402

The firewall RHEL system role reports changed: True when there were changes applied

During playbook processing, the **firewall_lib.py** module from the **firewall** RHEL system role was replacing the **changed** message with **False** when using the **interface** variable in the playbook and a pre-existing networking interface on the managed node. As a consequence, **firewall** reported the **changed: False** message even when there had been changes done, and the contents from the **forward_port** variable were not saved as permanent. With this update, the **firewall** RHEL system role ensures the **changed** value is not reset to **False**. As a result, the role reports **changed: True** when there are changes, and **forward_port** contents are saved as persistent.

Jira:RHEL-65758

The certificate RHEL system role correctly reports an error when an issued certificate is missing the private key

When the private key of a certificate was removed, the **certmonger** utility on a managed node entered an infinite loop. Consequently, the **certificate** RHEL system role on the control node became unresponsive when re-issuing a certificate that had the private key deleted. With this update, the **certificate** RHEL system role stops processing and provides an error message with instructions for remedy. As a result, **certificate** no longer becomes unresponsive in the described scenario.

Jira:RHEL-13333[1]

The postgresql RHEL system role no longer fails to set the paths to a TLS certificate and private key

The **postgresql_cert_name** variable of the **postgresql** RHEL system role defines the base path to the TLS certificate and private key without suffix on the managed node. Before this update, the role did not define internal variables for the certificate and private key. As a consequence, if you set **postgresql_cert_name**, the Ansible task failed with the following error message:

> The task includes an option with an undefined variable. The error was: '__pg_server_crt' is undefined. '__pg_server_crt' is undefined

With this update, the role correctly defines these internal variables, and the task sets the paths to the certificate and private key in the PostgreSQL configuration files.

Jira:RHEL-62395

The network RHEL system role prioritizes permanent MAC address matching

When all of the following conditions were met:

- A network connection specified both an interface name and a media access control (MAC) address for configuring a parent and a virtual local area network (VLAN) connection.
- The physical interface had the same permanent and current MAC address.
- The networking configuration was applied multiple times.

The **network** RHEL system role compared the user-specified MAC address against either the permanent MAC or the current MAC address from the **sysfs** virtual filesystem. The role then treated a match with the current MAC as valid even if the interface name was different from what the user specified. As a consequence, the "no such interface exists" error occurred. With this update, the **link_info_find()** method prioritizes matching links by permanent MAC address when it is valid and available. If the permanent MAC is unavailable (None or "00:00:00:00:00:00"), the method falls back to matching the current MAC address. As a result, this change improves the robustness of MAC address matching by ensuring that permanent addresses are prioritized while maintaining a reliable fallback mechanism for interfaces with no permanent address.

Jira:RHEL-73404

The ansible-doc command provides the documentation again for the redhat.rhel_system_roles collection

Before this update, the **vpn** RHEL system role did not include documentation for the internal Ansible filter **vpn_ipaddr**. Consequently, using the **ansible-doc** command to list documentation for the **redhat.rhel_system_roles** collection would trigger an error. With this update the **vpn** RHEL system role includes the correct documentation in the correct format for the **vpn_ipaddr** filter. As a result, **ansible-doc** does not trigger any error and provides the correct documentation.

Jira:RHEL-61085

The storage RHEL system role correctly resizes logical volumes

The physical volume was not resized to its maximum size when using the **grow_to_fill** feature in the **storage** RHEL system role to automatically resize LVM physical volumes after resizing the underlying virtual disks. Consequently, not all of the storage free space was available when resizing existing or creating new additional logical volumes; and the **storage** RHEL system role failed. This update fixes the problem in the source code to ensure the role always resizes the physical volumes to their maximum size when using **grow_to_fill**.

Jira:RHEL-73244[1]

The storage RHEL system role now runs as expected on RHEL 10 managed nodes with VDO

Before this update, the **blivet** module required the **kmod-kvdo** package on RHEL 10 managed nodes using Virtual Data Optimizer (VDO). However, **kmod-kvdo** failed to install, and as a consequence caused even the **storage** RHEL system role to fail. The fix to this problem ensures that **kmod-kvdo** is not a required package for managed nodes with RHEL 10. As a result, **storage** no longer fails when managed nodes with RHEL 10 use VDO.

Jira:RHEL-82160[1]

5.11. VIRTUALIZATION

High-memory VMs now report their state correctly

Previously, live migrating a virtual machine (VM) that was using 1 TB of memory or more caused **libvirt** to report the state of the VM incorrectly. This problem has been fixed and the status of live-migrated VMs with high amounts of memory is now reported accurately by **libvirt**.

Jira:RHEL-28819[1]

Network boot for VMs now works correctly without an RNG device

Previously, when a virtual machine (VM) did not have an RNG device configured and its CPU model did not support the RDRAND feature, it was not possible to boot the VM from the network. With this update, the problem has been fixed, and VMs that do not support RDRAND can boot from the network even without an RNG device configured.

Note, however, that to increase security when booting from the network, adding an RNG device is highly encouraged for VMs that use a CPU model that does not support RDRAND.

Jira:RHEL-58631, Jira:RHEL-65725

vGPU live migration no longer reports excessive amount of dirty pages

Previously, when performing virtual machine (VM) live migration with an attached NVIDIA vGPU, an excessive amount of dirty pages could have been incorrectly reported during the migration. This problem could have increased the required VM downtime during the migration and the migration could have potentially failed.

With this update, the underlying problem has been fixed and the correct amount of dirty pages is reported during the migration, which can reduce the required VM downtime during vGPU live migration in some cases.

Jira:RHEL-64307[1]

vGPU live migration no longer fails if vGPU driver versions are different on source and destination hosts

Previously, virtual machine (VM) live migration with an attached NVIDIA vGPU would fail if driver versions on source and destination hosts were different.

With this update, the underlying code has been fixed and live migrating VMs with NVIDIA vGPUs now works correctly even if the driver versions are different on the source and destination host.

Jira:RHEL-33795[1]

Virtual machines no longer incorrectly report an AMD SRSO vulnerability

Previously, virtual machines (VMs) running on a RHEL 9 host with the AMD Zen 3 and 4 CPU architecture incorrectly reported a vulnerability to a Speculative Return Stack Overflow (SRSO) attack.

The problem was caused by a missing cpuid flag, which was fixed with this update. Any reports of an AMD SRSO vulnerability reported by a VM should be now treated as being correct.

Jira:RHEL-26152[1]

The installer 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 installer 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 installer 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 installer shows the expected system disk to install RHEL in the VM.

Jira:RHELPLAN-66975[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.

Jira:RHELPLAN-147926[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.

Jira:RHELPLAN-139536[1]

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.

Jira:RHELPLAN-119912[1]

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

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 card (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

5.12. 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

The sos now obfuscates proxy passwords in several places

Previously, the **sos** utility did not obfuscate passwords from proxy links. For example **HTTP_PROXY`and `HTTPS_PROXY** in the **/etc/environment** file. As a consequence, the **sos** utility could collect sosreports with customer proxy passwords unless cleaned up before submitting. This may pose a security concern. Several of those places were discovered and fixed to obfuscate the passwords.

Red Hat continually improves the sos utility to enhance obfuscation capabilities; however, the complete removal of sensitive information is not guaranteed. Users are responsible for reviewing and manually cleaning up any confidential data before sharing it with Red Hat.

Jira:RHEL-67712[1]

CHAPTER 6. 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.

6.1. 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]

A new rhel9/bootc-image-builder container image is generally available in RHEL

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]

6.2. SECURITY

Encrypted DNS in RHEL is available as a Technology Preview

You can enable encrypted DNS to secure DNS communication that uses DNS-over-TLS (DoT). Encrypted DNS (eDNS) encrypts all DNS traffic end-to-end, with no fallback to insecure protocols, and aligns with zero trust architecture (ZTA) principles.

To perform a new installation with eDNS, specify the DoT-enabled DNS server by using the kernel command line. This ensures encrypted DNS is active during the installation process, boot time, and on the installed system. If you require a custom CA certificate bundle, you can install it only by using the **%certificate** section in the Kickstart file. Currently, the custom CA bundle can be installed only through Kickstart installation.

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

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

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

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

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.

Jira:RHELPLAN-128129[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]

6.3. 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]

6.4. SHELLS AND COMMAND-LINE TOOLS

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.

Jira:RHEL-88550

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.

Jira:RHELPLAN-109991[1]

6.5. 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.

Jira:RHELPLAN-129881[1]

6.6. NETWORKING

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.

Jira:RHEL-88552[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.

Jira:RHEL-88551[1]

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 card.

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

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]

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.

Jira:RHELPLAN-102815[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_af

Marvell OcteonTX2 RVU Admin Function driver

rvu_nicpf

Marvell OcteonTX2 NIC Physical Function driver

rvu_nicvf

Marvell OcteonTX2 NIC Virtual Function driver

Jira:RHELPLAN-108169[1]

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

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

Jira:RHELPLAN-154595[1]

kTLS was updated to version 6.12

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

Jira:RHELPLAN-153754[1]

6.7. 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]

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

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

Jira:RHEL-38583[1]

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

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

Jira:RHELDOCS-19635[1]

6.8. FILE SYSTEMS AND STORAGE

NVMe-oF Discovery Service features available as a Technology Preview

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

Jira:RHELPLAN-102321[1]

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**).

Jira:RHELPLAN-58357[1]

NVMe/TCP using TLS is available as a Technology Preview

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

Jira:RHEL-9301[1]

6.9. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

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

A new module stream, **nodejs:22**, is now available as a Technology Preview. A future update will provide a Long Term Support (LTS) version of **Node.js 22**, which will be fully supported.

Node.js 22 included in RHEL 9.5 provides numerous new features, bug fixes, security fixes, and performance improvements over **Node.js 20** available since RHEL 9.3.

Notable changes include:

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

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

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

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

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

Jira:RHEL-35990

6.10. 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.

Jira:RHELPLAN-88788[1]

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]

eu-stacktrace available as a Technology Preview

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

Jira:RHELDOCS-19072[1]

6.11. IDENTITY MANAGEMENT

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

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

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

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

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

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

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

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

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

ACME available as a Technology Preview

The Automated Certificate Management Environment (ACME) service is now available in Identity Management (IdM) as a Technology Preview. ACME is a protocol for automated identifier validation and certificate issuance. Its goal is to improve security by reducing certificate lifetimes and avoiding manual processes from certificate lifecycle management.

In RHEL, the ACME service uses the Red Hat Certificate System (RHCS) PKI ACME responder. The RHCS ACME subsystem is automatically deployed on every certificate authority (CA) server in the IdM deployment, but it does not service requests until the administrator enables it. RHCS uses the **acmeIPAServerCert** profile when issuing ACME certificates. The validity period of issued certificates is 90 days. Enabling or disabling the ACME service affects the entire IdM deployment.

IMPORTANT

It is recommended to enable ACME only in an IdM deployment where all servers are running RHEL 8.4 or later. Earlier RHEL versions do not include the ACME service, which can cause problems in mixed-version deployments. For example, a CA server without ACME can cause client connections to fail, because it uses a different DNS Subject Alternative Name (SAN).

WARNING

Currently, RHCS does not remove expired certificates. Because ACME certificates expire after 90 days, the expired certificates can accumulate and this can affect performance.

- To enable ACME across the whole IdM deployment, use the **ipa-acme-manage enable** command:

```
# ipa-acme-manage enable
The ipa-acme-manage command was successful
```

- To disable ACME across the whole IdM deployment, use the **ipa-acme-manage disable** command:

```
# ipa-acme-manage disable
The ipa-acme-manage command was successful
```

- To check whether the ACME service is installed and if it is enabled or disabled, use the **ipa-acme-manage status** command:

```
# ipa-acme-manage status
ACME is enabled
The ipa-acme-manage command was successful
```

Jira:RHELPLAN-121754[1]

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]

6.12. 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 RDP. As a result, you can manage the server using graphical applications.

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

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

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

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 RDP. As a result, you can manage the server using graphical applications.

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

- The Firefox web browser

- Red Hat Subscription Manager (**subscription-manager-cockpit**)
- Firewall Configuration (**firewall-config**)
- Disk Usage Analyzer (**baobab**)

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

Jira:RHELPLAN-27737[1]

6.13. 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]

6.14. 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]

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]

New package: trustee-guest-components

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

Jira:RHEL-68141[1]

6.15. RHEL IN CLOUD ENVIRONMENTS

RHEL is available on Azure confidential VMs as a Technology Preview

With the updated RHEL kernel, you can create and run RHEL confidential virtual machines (VMs) on Microsoft Azure as a Technology Preview from RHEL 9.3. 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]

6.16. CONTAINERS

The podman-machine command is unsupported

The **podman-machine** command for managing virtual machines, is available only as a Technology Preview. Instead, run Podman directly from the command line.

Jira:RHELDOCS-16861[1]

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, bootloader, firmware, between others. There are no changes to existing container images. For more information, see Red Hat Ecosystem Catalog .

Jira:RHELDOCS-17803[1]

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

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

Jira:RHEL-32267

The podman artifact command is available as a Technology Preview

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

Jira:RHEL-70217

CHAPTER 7. 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 .

7.1. INSTALLER AND IMAGE CREATION

Deprecated Kickstart commands

The following Kickstart commands have been deprecated:

- **timezone --ntpservers**
- **timezone --nontp**
- **logging --level**
- **%packages --excludeWeakdeps**
- **%packages --instLangs**
- **%anaconda**
- **pwpolicy**
- **nvdimm**

Note that where only specific options are listed, the base command and its other options are still available and not deprecated. Using the deprecated commands in Kickstart files prints a warning in the logs. You can turn the deprecated command warnings into errors with the **inst.ksstrict** boot option.

Jira:RHELPLAN-60153[1]

The initial-setup package now has been deprecated

The **initial-setup** package has been deprecated in Red Hat Enterprise Linux 9.3 and will be removed in the next major RHEL release. As a replacement, use **gnome-initial-setup** for the graphical user interface.

Jira:RHELDOCS-16393[1]

The provider_hostip and provider_fedora_geoip values of the inst.geoloc boot option are deprecated

The **provider_hostip** and **provider_fedora_geoip** values that specified the GeoIP API for the **inst.geoloc=** boot option are deprecated. As a replacement, you can use the **geolocation_provider=URL** option to set the required geolocation in the installation program configuration file. You can still use the **inst.geoloc=0** option to disable the geolocation.

Jira:RHELPLAN-168262[1]

Capturing screenshots from the Anaconda GUI with a global hotkey is deprecated

Previously, users could capture screenshots of the Anaconda GUI by using a global hotkey. 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 future major RHEL releases.

Jira:RHELDOCS-17309[1]

Support for NVDIMM devices has been deprecated

Previously, the installation program allowed reconfiguring NVDIMM devices during installation. This support for NVDIMM devices during the Kickstart and GUI installation has been deprecated, and will be removed in the next major RHEL release. The NVDIMM devices in the sector mode will still be visible and usable in the installation program.

Jira:RHELDOCS-17702

Unable to load an updated driver from the driver update disc in the installation environment

A new version of a driver from the driver update disc might not load if the same driver from the installation initial ramdisk has already been loaded. As a consequence, an updated version of the driver cannot be applied to the installation environment.

Workaround: Use the **modprobe.blacklist=** kernel command line option together with the **inst.dd** option. For example, to ensure that an updated version of the **virtio_blk** driver from a driver update disc is loaded, use **modprobe.blacklist=virtio_blk** and then continue with the usual procedure to apply drivers from the driver update disk. As a result, the system can load an updated version of the driver and use it in the installation environment.

Jira:RHEL-4762

7.2. SECURITY

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

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

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

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

Jira:RHELDOCS-19815[1]

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, and EdDSA.

The SEED algorithm, which was created by the Korea Information Security Agency (KISA) and has been previously disabled upstream, is deprecated in the NSS cryptographic library.

Jira:RHELDOCS-19004[1]

pam_ssh_agent_auth is deprecated

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

Jira:RHELDOCS-18312[1]

compat-openssl11 is deprecated

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

Jira:RHELDOCS-18480[1]

SHA-1 is deprecated at SECLEVEL=2 in OpenSSL

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

Jira:RHELDOCS-18701[1]

OpenSSL Engines API is deprecated in Stunnel

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

Jira:RHELDOCS-18702[1]

OpenSSL Engines are deprecated

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

Jira:RHELDOCS-18703[1]

DSA is deprecated in GnuTLS

The Digital Signature Algorithm (DSA) is deprecated in the GnuTLS secure communications library and will be removed in a future major version of RHEL. DSA was previously deprecated by the National Institute of Standards and Technology (NIST), and is not considered secure. You can use ECDSA instead to ensure compatibility with future versions.

Jira:RHELDOCS-19224[1]

scap-workbench is deprecated

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

Jira:RHELDOCS-19028[1]

oscap-anaconda-addon is deprecated

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

Jira:RHELDOCS-19029[1]

SHA-1 is deprecated for cryptographic purposes

The usage of the SHA-1 message digest for cryptographic purposes has been deprecated in RHEL 9. The digest produced by SHA-1 is not considered secure because of many documented successful attacks based on finding hash collisions. The RHEL core crypto components no longer create signatures using SHA-1 by default. Applications in RHEL 9 have been updated to avoid using SHA-1 in security-relevant use cases.

Among the exceptions, the HMAC-SHA1 message authentication code and the Universal Unique Identifier (UUID) values can still be created using SHA-1 because these use cases do not currently pose security risks. SHA-1 also can be used in limited cases connected with important interoperability and compatibility concerns, such as Kerberos and WPA-2. See the List of RHEL applications using cryptography that is not compliant with FIPS 140-3 section in the RHEL 9 Security hardening document for more details.

If your scenario requires the use of SHA-1 for verifying existing or third-party cryptographic signatures, you can enable it by entering the following command:

```
# update-crypto-policies --set DEFAULT:SHA1
```

Alternatively, you can switch the system-wide crypto policies to the **LEGACY** policy. Note that **LEGACY** also enables many other algorithms that are not secure.

Jira:RHELPLAN-110763[1]

fapolicyd.rules is deprecated

The **/etc/fapolicyd/rules.d/** directory for files containing allow and deny execution rules replaces the **/etc/fapolicyd/fapolicyd.rules** file. The **fagenrules** script now merges all component rule files in this directory to the **/etc/fapolicyd/compiled.rules** file. Rules in **/etc/fapolicyd/fapolicyd.trust** are still processed by the **fapolicyd** framework but only for ensuring backward compatibility.

Jira:RHELPLAN-112355[1]

SCP is deprecated in RHEL 9

The secure copy protocol (SCP) is deprecated because it has known security vulnerabilities. The SCP API remains available for the RHEL 9 lifecycle but using it reduces system security.

- In the **scp** utility, SCP is replaced by the SSH File Transfer Protocol (SFTP) by default.
- The OpenSSH suite does not use SCP in RHEL 9.
- SCP is deprecated in the **libssh** library.

Jira:RHELPLAN-99136[1]

OpenSSL requires padding for RSA encryption in FIPS mode

OpenSSL no longer supports RSA encryption without padding in FIPS mode. RSA encryption without padding is uncommon and is rarely used. Note that key encapsulation with RSA (RSASVE) does not use padding but is still supported.

Jira:RHELPLAN-148207[1]

OpenSSL 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.

Jira:RHELPLAN-94096[1]

/etc/system-fips is now deprecated

Support for indicating FIPS mode through the **/etc/system-fips** file has been removed, and the file will not be included in future versions of RHEL. To install RHEL in FIPS mode, add the **fips=1** parameter to the kernel command line during the system installation. You can check whether RHEL operates in FIPS mode by displaying the **/proc/sys/crypto/fips_enabled** file.

Jira:RHELPLAN-103232[1]

libcrypt.so.1 is now deprecated

The **libcrypt.so.1** library is now deprecated, and it might be removed in a future version of RHEL.

Jira:RHELPLAN-106338[1]

7.3. 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.

Jira:RHELPLAN-146101[1]

7.4. SOFTWARE MANAGEMENT

The numberless %patch syntax has been deprecated

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

Jira:RHELDOCS-19810[1]

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]

7.5. 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/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.

Jira:RHELPLAN-94704[1]

The SQLite database backend in Bacula has been deprecated

The Bacula backup system supported multiple database backends: PostgreSQL, MySQL, and SQLite. The SQLite backend has been deprecated and will become unsupported in a later release of RHEL. As a replacement, migrate to one of the other backends (PostgreSQL or MySQL) and do not use the SQLite backend in new deployments.

Jira:RHEL-6856

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

Jira:RHELDOCS-18049[1]

cgroupsv1 is now deprecated in RHEL 9

The **cgroups** is a kernel subsystem used for process tracking, system resource allocation and partitioning. Systemd service manager supports booting in the cgroups **v1** mode as well as in cgroups **v2** mode. In Red Hat Enterprise Linux 9, the default mode is **v2**. In Red Hat Enterprise Linux 10, systemd will not support booting in the cgroups **v1** mode and only cgroups **v2** mode will be available.

Jira:RHELDOCS-17545[1]

7.6. 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]

7.7. NETWORKING

ipset has been deprecated

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

Jira:RHELDOCS-20146[1]

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.

Jira:RHELPLAN-69554[1]

NetworkManager connection profiles in ifcfg format are deprecated

In RHEL 9.0 and later, connection profiles in **ifcfg** format are deprecated. The next major RHEL release will remove the support for this format. However, in RHEL 9, NetworkManager still processes and updates existing profiles in this format if you modify them.

By default, NetworkManager now stores connection profiles in keyfile format in the **/etc/NetworkManager/system-connections/** directory. Unlike the **ifcfg** format, the keyfile format supports all connection settings that NetworkManager provides. For further details about the keyfile format and how to migrate profiles, see NetworkManager connection profiles in keyfile format .

Jira:RHELPLAN-58745[1]

The iptables back end in firewalld is deprecated

In RHEL 9, the **iptables** framework is deprecated. As a consequence, the **iptables** back end and the **direct interface** in **firewalld** are also deprecated. Instead of the **direct interface** you can use the native features in **firewalld** to configure the required rules.

Jira:RHELPLAN-122745[1]

The firewalld lockdown feature is deprecated.

The lockdown feature in **firewalld** is deprecated because it cannot prevent processes that are running as **root** from adding themselves to the allow list. The lockdown feature may be removed in a future major RHEL release.

Jira:RHEL-17708

The connection.master, connection.slave-type, and connection.autoconnect-slaves properties are deprecated

Red Hat is committed to using conscious language. For details about this initiative, see Making open source more inclusive. 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]

7.8. 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 .

Jira:RHELPLAN-113659[1]

The **kexec_load** system call for **kexec-tools** has been deprecated

The **kexec_load** system call, which loads the second kernel, will not be supported in future RHEL releases. The **kexec_file_load** system call replaces **kexec_load** and is now the default system call on all architectures.

For more information, see Is kexec_load supported in RHEL9? .

Jira:RHELPLAN-129876[1]

7.9. FILE SYSTEMS AND STORAGE

Support for the block translation table driver has been deprecated

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

Jira:RHELDOCS-19716[1]

The **nvme_core.multipath** parameter is deprecated

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

Jira:RHELDOCS-19809[1]

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.

Jira:RHELPLAN-107107[1]

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

7.10. HIGH AVAILABILITY AND CLUSTERS

Deprecated high availability features

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

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

Jira:RHEL-34781

Resilient Storage Add-On has been deprecated

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

Jira:RHELDOCS-19022[1]

7.11. DYNAMIC PROGRAMMING LANGUAGES, WEB AND DATABASE SERVERS

libdb has been deprecated

RHEL 9 currently provide Berkeley DB (**libdb**) version 5.3.28, which is distributed under the LGPLv2 license. The upstream Berkeley DB version 6 is available under the AGPLv3 license, which is more restrictive.

The **libdb** package is deprecated as of RHEL 9 and might not be available in future major RHEL releases.

In addition, cryptographic algorithms have been removed from **libdb** in RHEL 9 and multiple **libdb** dependencies have been removed from RHEL 9.

Users of **libdb** are advised to migrate to a different key-value database. For more information, see the following Red Hat Knowledgebase articles:

- How to migrate from libdb to a different key-value database
- Available replacements for the deprecated Berkeley DB (libdb) in RHEL

Jira:RHELPLAN-67314[1], Bugzilla:1974657, Jira:RHELPLAN-80695

7.12. 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.

Jira:RHELPLAN-129104[1]

Some PKCS1 v1.5 modes are now deprecated in Go's FIPS mode

Some **PKCS1** v1.5 modes are not approved in **FIPS-140-3** for encryption and are disabled. They will no longer work in Go's FIPS mode.

Jira:RHELPLAN-123778[1]

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]

7.13. 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]

SHA-1 in OpenDNSSec is now deprecated

OpenDNSSec supports exporting Digital Signatures and authentication records using the **SHA-1** algorithm. The use of the **SHA-1** algorithm is no longer supported. With the RHEL 9 release, **SHA-1** in OpenDNSSec is deprecated and it might be removed in a future minor release. Additionally, OpenDNSSec support is limited to its integration with Red Hat Identity Management. OpenDNSSec is not supported standalone.

Jira:RHELPLAN-88246[1]

The 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

7.14. SSSD

The ad_allow_remote_domain_local_groups option has been deprecated

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

Jira:RHELDOCS-19455[1]

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]

7.15. DESKTOP

Firefox and Thunderbird Flatpak images have been deprecated

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

Jira:RHEL-91106[1]

Evince has been deprecated

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

Jira:RHELDOCS-19889[1]

power-profile-daemon is deprecated

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

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

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

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

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

Jira:RHEL-68152

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]

7.16. 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]

The Intel vGPU feature has been removed

Previously, as a Technology Preview, it was possible to divide a physical Intel GPU device into multiple virtual devices referred to as **mediated devices**. These mediated devices could then be assigned to multiple virtual machines (VMs) as virtual GPUs. As a result, these VMs shared the performance of a single physical Intel GPU, however only selected Intel GPUs were compatible with this feature.

Since RHEL 9.3, the Intel vGPU feature has been removed entirely.

Jira:RHELPLAN-157294[1]

7.17. RED HAT ENTERPRISE LINUX SYSTEM ROLES

The sshd variable deprecated and replaced by sshd_config

To unify coding standards across the RHEL system roles, the **sshd** variable has been replaced by the **sshd_config** variable. The **sshd** variable is now deprecated and may be removed from the **sshd** Ansible role in a future major version of RHEL.

Jira:RHEL-73408

The mssql_accept_microsoft_odbc_driver_17_for_sql_server_eula variable has been deprecated

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

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

Jira:RHEL-69311

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.

Jira:RHELPLAN-95747[1]

7.18. 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

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]

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

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]

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]

SecureBoot image verification using SHA1-based signatures is deprecated

Performing SecureBoot image verification using SHA1-based signatures on UEFI (PE/COFF) executables has become deprecated. Instead, Red Hat recommends using signatures based on the SHA-2 algorithm, or later.

Jira:RHELPLAN-69533[1]

The virtual floppy driver has become deprecated

The **isa-fdc** driver, which controls virtual floppy disk devices, is now deprecated, and will become unsupported in a future release of RHEL. Therefore, to ensure forward compatibility with migrated virtual machines (VMs), Red Hat discourages using floppy disk devices in VMs hosted on RHEL 9.6.

Jira:RHELPLAN-81033[1]

qcow2-v2 image format is deprecated

With RHEL 9.6, 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 9.6 Image Builder cannot create disk images in the qcow2-v2 format.

Instead of qcow2-v2, Red Hat strongly recommends using qcow2-v3. To convert a qcow2-v2 image to a later format version, use the **qemu-img amend** command.

Jira:RHELPLAN-75969[1]

Legacy CPU models are now deprecated

A significant number of CPU models have become deprecated and will become unsupported for use in virtual machines (VMs) in a future major release of RHEL. The deprecated models are as follows:

- For Intel: models before Intel Xeon 55xx and 75xx Processor families (also known as Nehalem)
- For AMD: models before AMD Opteron G4
- For IBM Z: models before IBM z14

To check whether your VM is using a deprecated CPU model, use the **virsh dominfo** utility, and look for a line similar to the following in the **Messages** section:

```
tainted: use of deprecated configuration settings
deprecated configuration: CPU model 'i486'
```

Jira:RHELPLAN-114513[1]

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]

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

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]

7.19. CONTAINERS

The rsyslog container image has been deprecated

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

Jira:RHELDOCS-19523[1]

The runc container runtime has been deprecated

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

Jira:RHEL-69742

The podman-tests package has been deprecated

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

Jira:RHEL-67859

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.

Jira:RHELPLAN-117005[1]

rhel9/pause has been deprecated

The **rhel9/pause** container image has been deprecated.

Jira:RHELPLAN-127619[1]

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]

7.20. 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
- bacula-client
- bacula-common
- bacula-console
- bacula-director
- bacula-libs
- bacula-libs-sql
- bacula-logwatch
- bacula-storage
- bind9.18-libs
- bitmap-fangsongti-fonts
- bnx2
- bnx2fc
- bnx2i
- bogofilter
- Box2D
- brasero-nautilus
- cairomm
- cheese
- cheese-libs
- clucene-contribs-lib
- clucene-core
- clutter
- clutter-gst3
- clutter-gtk

- cnic
- cockpit-composer
- cogl
- compat-hesiod
- compat-locales-sap
- compat-locales-sap-common
- compat-openssl11
- compat-paratype-pt-sans-fonts-f33-f34
- compat-sap-c++-12
- compat-sap-c++-13
- containernetworking-plugins
- containers-common-extra
- culmus-aharoni-clm-fonts
- culmus-caladings-clm-fonts
- culmus-david-clm-fonts
- culmus-drugulin-clm-fonts
- culmus-ellinia-clm-fonts
- culmus-fonts-common
- culmus-frank-ruehl-clm-fonts
- culmus-hadasim-clm-fonts
- culmus-miriam-clm-fonts
- culmus-miriam-mono-clm-fonts
- culmus-nachlieli-clm-fonts
- culmus-simple-clm-fonts
- culmus-stamashkenaz-clm-fonts
- culmus-stamsefarad-clm-fonts
- culmus-yehuda-clm-fonts
- curl-minimal
- daxio

- dbus-glib
- dbus-glib-devel
- devhelp
- devhelp-libs
- dhcp-client
- dhcp-common
- dhcp-relay
- dhcp-server
- dotnet-apphost-pack-6.0
- dotnet-apphost-pack-7.0
- dotnet-hostfxr-6.0
- dotnet-hostfxr-7.0
- dotnet-runtime-6.0
- dotnet-runtime-7.0
- dotnet-sdk-6.0
- dotnet-sdk-7.0
- dotnet-targeting-pack-6.0
- dotnet-targeting-pack-7.0
- dotnet-templates-6.0
- dotnet-templates-7.0
- double-conversion
- efs-utils
- enchant
- enchant-devel
- eog
- evince
- evince-libs
- evince-nautilus
- evince-previewer

- evince-thumbnailer
- evolution
- evolution-bogofilter
- evolution-data-server-ui
- evolution-data-server-ui-devel
- evolution-devel
- evolution-ews
- evolution-ews-langpacks
- evolution-help
- evolution-langpacks
- evolution-mapi
- evolution-mapi-langpacks
- evolution-pst
- evolution-spamassassin
- festival
- festival-data
- festvox-slt-arctic-hts
- firefox
- firefox
- firefox-x11
- flite
- flite-devel
- fltk
- flute
- firewire-core
- fontawesome-fonts
- gc
- gcr-base
- gdisk

- gedit
- gedit-plugin-bookmarks
- gedit-plugin-bracketcompletion
- gedit-plugin-codecomment
- gedit-plugin-colorpicker
- gedit-plugin-colorschemer
- gedit-plugin-commander
- gedit-plugin-drawspaces
- gedit-plugin-findinfiles
- gedit-plugin-joinlines
- gedit-plugin-multiedit
- gedit-plugin-sessionsaver
- gedit-plugin-smartspaces
- gedit-plugin-synctex
- gedit-plugin-terminal
- gedit-plugin-textsize
- gedit-plugin-translate
- gedit-plugin-wordcompletion
- gedit-plugins
- gedit-plugins-data
- 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
- java-1.8.0-openjdk
- java-1.8.0-openjdk-demo
- java-1.8.0-openjdk-devel
- java-1.8.0-openjdk-headless
- java-1.8.0-openjdk-javadoc
- java-1.8.0-openjdk-javadoc-zip
- java-1.8.0-openjdk-src
- java-11-openjdk
- java-11-openjdk-demo
- java-11-openjdk-devel

- java-11-openjdk-headless
- java-11-openjdk-javadoc
- java-11-openjdk-javadoc-zip
- java-11-openjdk-jmods
- java-11-openjdk-src
- java-11-openjdk-static-libs
- java-17-openjdk
- java-17-openjdk-demo
- java-17-openjdk-devel
- java-17-openjdk-headless
- java-17-openjdk-javadoc
- java-17-openjdk-javadoc-zip
- java-17-openjdk-jmods
- java-17-openjdk-src
- java-17-openjdk-static-libs
- jboss-jaxrs-2.0-api
- jboss-logging
- jboss-logging-tools
- jdeparser
- jigawatts
- jigawatts-javadoc
- julietaula-montserrat-fonts
- kacst-art-fonts
- kacst-book-fonts
- kacst-decorative-fonts
- kacst-digital-fonts
- kacst-farsi-fonts
- kacst-fonts-common
- kacst-letter-fonts

- kacst-naskh-fonts
- kacst-office-fonts
- kacst-one-fonts
- kacst-pen-fonts
- kacst-poster-fonts
- kacst-qurn-fonts
- kacst-screen-fonts
- kacst-title-fonts
- kacst-titlel-fonts
- khmer-os-battambang-fonts
- khmer-os-bokor-fonts
- khmer-os-content-fonts
- khmer-os-fasthand-fonts
- khmer-os-freehand-fonts
- khmer-os-handwritten-fonts
- khmer-os-metal-chrieng-fonts
- khmer-os-muol-fonts
- khmer-os-muol-fonts-all
- khmer-os-muol-pali-fonts
- khmer-os-siemreap-fonts
- kmod-kvdo
- lasso
- libabw
- libadwaita-qt5
- libbase
- libblockdev-kbd
- libcanberra-gtk2
- libcdio-paranoia
- libcdio-paranoia-devel

- libcdr
- libcmis
- libdazzle
- libdb
- libdb-devel
- libdb-utils
- libdmx
- libepubgen
- libetonyek
- libexttextcat
- libfonts
- libformula
- libfreehand
- libgdata
- libgdata-devel
- libgnomekbd
- libiscsi
- libiscsi-utils
- liblangtag
- liblangtag-data
- liblayout
- libloader
- libmatchbox
- libmspub
- libmwaw
- libnsl2
- libnumbertext
- libodfgen
- liborcus

- libotr
- libpagemaker
- libpmem
- libpmem-debug
- libpmem-devel
- libpmem2
- libpmem2-debug
- libpmem2-devel
- libpmemblk
- libpmemblk-debug
- libpmemblk-devel
- libpmemlog
- libpmemlog-debug
- libpmemlog-devel
- libpmemobj
- libpmemobj++-devel
- libpmemobj++-doc
- libpmemobj-debug
- libpmemobj-devel
- libpmempool
- libpmempool-debug
- libpmempool-devel
- libpng15
- libpst-libs
- libqxp
- LibRaw
- libreoffice
- libreoffice-base
- libreoffice-calc

- libreoffice-core
- libreoffice-data
- libreoffice-draw
- libreoffice-emailmerge
- libreoffice-filters
- libreoffice-gdb-debug-support
- libreoffice-graphicfilter
- libreoffice-gtk3
- libreoffice-help-ar
- libreoffice-help-bg
- libreoffice-help-bn
- libreoffice-help-ca
- libreoffice-help-cs
- libreoffice-help-da
- libreoffice-help-de
- libreoffice-help-dz
- libreoffice-help-el
- libreoffice-help-en
- libreoffice-help-eo
- libreoffice-help-es
- libreoffice-help-et
- libreoffice-help-eu
- libreoffice-help-fi
- libreoffice-help-fr
- libreoffice-help-gl
- libreoffice-help-gu
- libreoffice-help-he
- libreoffice-help-hi
- libreoffice-help-hr

- libreoffice-help-hu
- libreoffice-help-id
- libreoffice-help-it
- libreoffice-help-ja
- libreoffice-help-ko
- libreoffice-help-lt
- libreoffice-help-lv
- libreoffice-help-nb
- libreoffice-help-nl
- libreoffice-help-nn
- libreoffice-help-pl
- libreoffice-help-pt-BR
- libreoffice-help-pt-PT
- libreoffice-help-ro
- libreoffice-help-ru
- libreoffice-help-si
- libreoffice-help-sk
- libreoffice-help-sl
- libreoffice-help-sv
- libreoffice-help-ta
- libreoffice-help-tr
- libreoffice-help-uk
- libreoffice-help-zh-Hans
- libreoffice-help-zh-Hant
- libreoffice-impress
- libreoffice-langpack-af
- libreoffice-langpack-ar
- libreoffice-langpack-as
- libreoffice-langpack-bg

- libreoffice-langpack-bn
- libreoffice-langpack-br
- libreoffice-langpack-ca
- libreoffice-langpack-cs
- libreoffice-langpack-cy
- libreoffice-langpack-da
- libreoffice-langpack-de
- libreoffice-langpack-dz
- libreoffice-langpack-el
- libreoffice-langpack-en
- libreoffice-langpack-eo
- libreoffice-langpack-es
- libreoffice-langpack-et
- libreoffice-langpack-eu
- libreoffice-langpack-fa
- libreoffice-langpack-fi
- libreoffice-langpack-fr
- libreoffice-langpack-fy
- libreoffice-langpack-ga
- libreoffice-langpack-gl
- libreoffice-langpack-gu
- libreoffice-langpack-he
- libreoffice-langpack-hi
- libreoffice-langpack-hr
- libreoffice-langpack-hu
- libreoffice-langpack-id
- libreoffice-langpack-it
- libreoffice-langpack-ja
- libreoffice-langpack-kk

- libreoffice-langpack-kn
- libreoffice-langpack-ko
- libreoffice-langpack-lt
- libreoffice-langpack-lv
- libreoffice-langpack-mai
- libreoffice-langpack-ml
- libreoffice-langpack-mr
- libreoffice-langpack-nb
- libreoffice-langpack-nl
- libreoffice-langpack-nn
- libreoffice-langpack-nr
- libreoffice-langpack-nso
- libreoffice-langpack-or
- libreoffice-langpack-pa
- libreoffice-langpack-pl
- libreoffice-langpack-pt-BR
- libreoffice-langpack-pt-PT
- libreoffice-langpack-ro
- libreoffice-langpack-ru
- libreoffice-langpack-si
- libreoffice-langpack-sk
- libreoffice-langpack-sl
- libreoffice-langpack-sr
- libreoffice-langpack-ss
- libreoffice-langpack-st
- libreoffice-langpack-sv
- libreoffice-langpack-ta
- libreoffice-langpack-te
- libreoffice-langpack-th

- libreoffice-langpack-tn
- libreoffice-langpack-tr
- libreoffice-langpack-ts
- libreoffice-langpack-uk
- libreoffice-langpack-ve
- libreoffice-langpack-xh
- libreoffice-langpack-zh-Hans
- libreoffice-langpack-zh-Hant
- libreoffice-langpack-zu
- libreoffice-math
- libreoffice-ogltrans
- libreoffice-opensymbol-fonts
- libreoffice-pdfimport
- libreoffice-pyuno
- libreoffice-sdk
- libreoffice-sdk-doc
- libreoffice-ure
- libreoffice-ure-common
- libreoffice-voikko
- libreoffice-wiki-publisher
- libreoffice-writer
- libreoffice-x11
- libreoffice-xsltfilter
- libreofficekit
- libreport
- libreport-anaconda
- libreport-cli
- libreport-filesystem
- libreport-gtk

- libreport-plugin-bugzilla
- libreport-plugin-reportuploader
- libreport-rhel-anaconda-bugzilla
- libreport-web
- librepository
- librevenge
- librevenge-gdb
- libserializer
- libsigc++20
- libsigsegv
- libsmbios
- libsoup
- libsoup-devel
- libstaroffice
- libstemmer
- libstoragemgmt-smis-plugin
- libteam
- libuser
- libuser-devel
- libvisio
- libvisual
- 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-libreport
- 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
- satyr
- scap-workbench
- sendmail
- sendmail-cf
- sendmail-doc

- setxkbmap
- sgabios
- sgabios-bin
- sil-scheherazade-fonts
- spamassassin
- speech-tools-libs
- suitesparse
- sushi
- team
- teamd
- texlive-xdvi
- thai-scalable-fonts-common
- thai-scalable-garuda-fonts
- thai-scalable-kinnari-fonts
- thai-scalable-loma-fonts
- thai-scalable-norasi-fonts
- thai-scalable-purisa-fonts
- thai-scalable-sawasdee-fonts
- thai-scalable-tlwgmono-fonts
- thai-scalable-tlwgtypewriter-fonts
- thai-scalable-tlwgtypist-fonts
- thai-scalable-tlwgtypo-fonts
- thai-scalable-umpush-fonts
- thunderbird
- tigervnc
- tigervnc-icons
- tigervnc-license
- tigervnc-selinux
- tigervnc-server

- tigervnc-server-minimal
- tigervnc-server-module
- totem-pl-parser
- tracer-common
- ucs-miscfixed-fonts
- usb_modeswitch
- usb_modeswitch-data
- usbredir-server
- usermode-gtk
- webkit2gtk3
- webkit2gtk3-devel
- webkit2gtk3-jsc
- webkit2gtk3-jsc-devel
- wpebackend-fdo
- wpebackend-fdo-devel
- xmlrpc-c
- xmlsec1-gcrypt
- xmlsec1-gcrypt-devel
- xmlsec1-gnutls
- xmlsec1-gnutls-devel
- xorg-x11-drivers
- xorg-x11-drv-dummy
- xorg-x11-drv-evdev
- xorg-x11-drv-fbdev
- xorg-x11-drv-libinput
- xorg-x11-drv-v4l
- xorg-x11-drv-vmware
- xorg-x11-drv-wacom
- xorg-x11-drv-wacom-serial-support

- xorg-x11-server-common
- xorg-x11-server-utils
- xorg-x11-server-Xdmx
- xorg-x11-server-Xephyr
- xorg-x11-server-Xnest
- xorg-x11-server-Xorg
- xorg-x11-server-Xvfb
- xorg-x11-utils
- xorg-x11-xbitmaps
- xorg-x11-xinit
- xorg-x11-xinit-session
- xsane
- xsane-common
- xxhash
- xxhash-libs
- yajl
- yelp
- yelp-libs
- yp-tools
- ypbind
- ypserv
- zhongyi-song-fonts

CHAPTER 8. KNOWN ISSUES

This part describes known issues in Red Hat Enterprise Linux 9.6.

8.1. INSTALLER AND IMAGE CREATION

The auth and authconfig Kickstart commands require the AppStream repository

The **authselect-compat** package is required by the **auth** and **authconfig** Kickstart commands during installation. Without this package, the installation fails if **auth** or **authconfig** are used. However, by design, the **authselect-compat** package is only available in the AppStream repository.

Workaround: Verify that the BaseOS and AppStream repositories are available to the installation program or use the **authselect** Kickstart command during installation.

Jira:RHELPLAN-10061[1]

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.

Workaround: Do not run Anaconda on the production system. Instead, run Anaconda in a temporary virtual machine to keep the SELinux policy unchanged on a production system. Running anaconda as part of the system installation process such as installing from **boot.iso** or **dvd.iso** is not affected by this issue.

Jira:RHELPLAN-110940[1]

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 installer fails to detect the **Local Media** installation source (only *Red Hat CDN* is detected).

This issue occurs because the default boot option **inst.stage2=** attempts to search for **iso9660** image format. However, a third party tool might create an ISO image with a different format.

Workaround: Use either of the following solution:

- When booting the installation, click the **Tab** key to edit the kernel command line, and change the boot option **inst.stage2=** to **inst.repo=**.

- To create a bootable USB device on Windows, use Fedora Media Writer.
- When using a third party tool such as Rufus to create a bootable USB device, first regenerate the RHEL ISO image on a Linux system, and then use the third party tool to create a bootable USB device.

For more information on the steps involved in performing any of the specified workaround, see, Installation media is not auto-detected during the installation of RHEL 8.3 .

Jira:RHELPLAN-53644[1]

The USB CD-ROM drive is not available as an installation source in Anaconda

Installation fails when the USB CD-ROM drive is the source for it and the Kickstart **ignoredisk --only-use=** command is specified. In this case, Anaconda cannot find and use this source disk.

Workaround: Use the **harddrive --partition=sdX --dir=**/ command to install from USB CD-ROM drive. As a result, the installation does not fail.

Jira:RHEL-4707

Hard drive partitioned installations with iso9660 filesystem fails

You cannot install RHEL on systems where the hard drive is partitioned with the **iso9660** filesystem. This is due to the updated installation code that is set to ignore any hard disk containing a **iso9660** file system partition. This happens even when RHEL is installed without using a DVD.

Workaround: Add the following script in the Kickstart file to format the disc before the installation starts.

Note: Before performing the workaround, backup the data available on the disk. The **wipefs** command formats all the existing data from the disk.

```
%pre
wipefs -a /dev/sda
%end
```

As a result, installations work as expected without any errors.

Jira:RHEL-4711

Anaconda fails to verify existence of an administrator user account

While installing RHEL using a graphical user interface, Anaconda fails to verify if the administrator account has been created. As a consequence, users might install a system without any administrator user account.

Workaround: Ensure you configure an administrator user account or the root password is set and the root account is unlocked. As a result, users can perform administrative tasks on the installed system.

Jira:RHELPLAN-110191[1]

New XFS features prevent booting of PowerNV IBM POWER systems with firmware older than version 5.10

PowerNV IBM POWER systems use a Linux kernel for firmware, and use Petitboot as a replacement for GRUB. This results in the firmware kernel mounting /**boot** and Petitboot reading the GRUB config and booting RHEL.

The RHEL 9 kernel introduces **bigtime=1** and **inobtcount=1** features to the XFS filesystem, which kernels with firmware older than version 5.10 do not understand.

Workaround: You can use another filesystem for /**boot**, for example ext4.

Jira:RHELPLAN-94811[1]

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 installer 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.
```

Workaround:

- 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.

Workaround: Do one of the following:

- Delete all connections using the **nmcli** utility except one connection you want to use. For example:
  a. List all connection profiles:

     ```
     # nmcli connection show
     ```

  b. Delete the connection profiles that you do not require:

     ```
     # nmcli connection delete <connection_name>
     ```

     Replace <connection_name> with the name of the connection you want to delete.
- Disable the auto connect network feature in Anaconda if no specific **ip=** or Kickstart network configuration is set.
  a. In the Anaconda GUI, navigate to **Network & Host Name**
  b. Select a network device to disable.

c. Click **Configure**.

d. On the **General** tab, clear the **Connect automatically with priority** checkbox.

e. Click **Save**.

Jira:RHELPLAN-130370[1]

Kickstart installations fail to configure the network connection

Anaconda performs the Kickstart network configuration only through the NetworkManager API. Anaconda processes the network configuration after the **%pre** Kickstart section. As a consequence, some tasks from the Kickstart **%pre** section are blocked. For example, downloading packages from the **%pre** section fails due to unavailability of the network configuration.

Workaround:

- Configure the network, for example using the **nmcli** tool, as a part of the **%pre** script.
- Use the installer boot options to configure the network for the **%pre** script.

As a result, it is possible to use the network for tasks in the **%pre** section and the Kickstart installation process completes.

Jira:RHELPLAN-150080[1]

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**.

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>
```

Workaround: Include the respective package with the service file in Kickstart's **%packages** section. As a result, RHEL installation completes, enabling expected services during installation.

Jira:RHEL-9633[1]

Unable to build ISOs from a signed container

Trying to build an ISO disk image from a GPG or a simple signed container results in an error, similar to the following:

```
manifest - failed
Failed
Error: cannot run osbuild: running osbuild failed: exit status 1
2024/04/23 10:56:48 error: cannot run osbuild: running osbuild failed: exit status 1
```

This happens because the system fails to get the image source signatures.

Workaround: You can either remove the signature from the container image or build a derived container image. For example, to remove the signature, you can run the following command:

```
 $ sudo skopeo copy --remove-signatures containers-storage:registry.redhat.io/rhel9/rhel-bootc:9.4
containers-storage:registry.redhat.io/rhel9/rhel-bootc:9.4
$ sudo podman run \
      --rm \
      -it \
      --privileged \
      --pull=newer \
      --security-opt label=type:unconfined_t \
      -v /var/lib/containers/storage:/var/lib/containers/storage \
      -v ~/images/iso:/output \
      quay.io/centos-bootc/bootc-image-builder \
      --type iso --local \
      registry.redhat.io/rhel9/rhel-bootc:9.4
```

To build a derived container image, and avoid adding a simple GPG signatures to it, see the Signing container images product documentation.

Jira:RHEL-34807

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**.

Workaround: 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 may cause reboot loop

Accessing a file system in the **rescue** mode triggers SELinux to autorelabel the file system on the next boot, which continues until SELinux runs in the **permissive** mode. Consequently, the system might go into an infinite loop of reboots after exiting the **rescue** mode as it cannot delete the **/.autorelabel** file.

Workaround: Switch to the **permissive** mode by adding **enforcing=0** to the kernel command line on the next boot. The system displays a warning message as a preventive measure that informs about the possibility of this issue when accessing the file system in the **rescue** mode.

Jira:RHEL-14005

Hostname resolution fails with encrypted DNS and custom CA in boot options

While using the **inst.repo=** or **inst.stage2=** boot options in the kernel command line along with a remote installation URL, an encrypted DNS, and a custom CA certificate in the kickstart file, the installer attempts to download the **install.img** stage2 image before processing the kickstart file. Consequently, the hostname resolution fails, leading to display of some errors before successfully fetching the stage2 image.

Workaround: Define the installation source in the kickstart file instead of the kernel command line.

Jira:RHEL-80867

Bonding device with LACP takes longer to become operational, causing subscription failures

When configuring a bonding device with LACP by using both kernel command-line boot options and a Kickstart file, the connection is created during the **initramfs** stage but reactivated in Anaconda. As a

consequence, it causes a temporary disruption that leads to system subscription failure via the **rhsm** Kickstart command.

Workaround: Add **--no-activate** to the Kickstart network configuration to keep the network operational. As a result, the system subscription completes successfully.

Jira:RHELDOCS-19852[1]

The services Kickstart command fails to disable the firewalld service

A bug in Anaconda prevents the **services --disabled=firewalld** command from disabling the **firewalld** service in Kickstart.

Workaround: Use the **firewall --disabled** command instead. As a result, the **firewalld** service is disabled properly.

Jira:RHEL-82566

Installer ignores the BOOTIF boot argument and activates all network devices

During installation, the installer does not consider the **BOOTIF=<MAC>** boot argument when determining which network devices to activate. As a result, all network interfaces are activated even if only one is specified.

Workaround: If the desired interface name is known, use the **ip=<DEVICE_NAME>:dhcp** kernel command line option to activate only the intended network device.

Jira:RHEL-78272[1]

Kickstart installation fails with an unknown disk error when 'ignoredisk' command precedes 'iscsi' command

Installing RHEL by using the kickstart method fails if the **ignoredisk** command is placed before the **iscsi** command. This issue occurs because the **iscsi** command attaches the specified iSCSI device during command parsing, while the **ignoredisk** command resolves device specifications simultaneously. If the **ignoredisk** command references an iSCSI device name before it is attached by the **iscsi** command, the installation fails with an "unknown disk" error.

Workaround: Ensure that the **iscsi** command is placed before the **ignoredisk** command in the Kickstart file to reference the iSCSI disk and enable successful installation.

Jira:RHEL-13837

Installer fails if /boot partition is not created when using ostreecontainer

When using the **ostreecontainer** Kickstart command to install a bootable container, the installation fails if the **/boot** partition is not created. This issue occurs because the installer requires a dedicated **/boot** partition to proceed with the container deployment.

Workaround: Ensure that a **/boot** partition is defined in the Kickstart file or manually created during the installation process.

Jira:RHEL-66155

Anaconda may not work correctly on s390x and ppc64le architectures

Image mode for RHEL supports **pp64le** and **s390x** architectures besides the already supported **x86_64** and ARM architectures. However, Anaconda may not function correctly on s390x and ppc64le architectures.

Jira:RHELDOCS-19496[1]

8.2. SECURITY

OpenSSL does not detect if a PKCS #11 token supports the creation of raw RSA or RSA-PSS signatures

The TLS 1.3 protocol requires support for RSA-PSS signatures. If a PKCS #11 token does not support raw RSA or RSA-PSS signatures, server applications that use the OpenSSL library fail to work with an RSA key if the key is held by the PKCS #11 token. As a result, TLS communication fails in the described scenario.

Workaround: Configure servers and clients to use TLS version 1.2 as the highest TLS protocol version available.

Jira:RHELPLAN-50959[1]

OpenSSL incorrectly handles PKCS #11 tokens that does not support raw RSA or RSA-PSS signatures

The **OpenSSL** library does not detect key-related capabilities of PKCS #11 tokens. Consequently, establishing a TLS connection fails when a signature is created with a token that does not support raw RSA or RSA-PSS signatures.

Workaround: Add the following lines after the **.include** line at the end of the **crypto_policy** section in the **/etc/pki/tls/openssl.cnf** file:

```
SignatureAlgorithms =
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384
MaxProtocol = TLSv1.2
```

As a result, a TLS connection can be established in the described scenario.

Jira:RHELPLAN-48241[1]

With a specific syntax, scp empties files copied to themselves

The **scp** utility changed from the Secure copy protocol (SCP) to the more secure SSH file transfer protocol (SFTP). Consequently, copying a file from a location to the same location erases the file content. The problem affects the following syntax:

scp localhost:/myfile localhost:/myfile

Workaround: Do not copy files to a destination that is the same as the source location using this syntax.

The problem has been fixed for the following syntaxes:

- **scp /myfile localhost:/myfile**
- **scp localhost:~/myfile ~/myfile**

Jira:RHELPLAN-113842[1]

The OSCAP Anaconda add-on does not fetch tailored profiles in the graphical installation

The OSCAP Anaconda add-on does not provide an option to select or deselect tailoring of security profiles in the RHEL graphical installation. Starting from RHEL 8.8, the add-on does not take tailoring into account by default when installing from archives or RPM packages. Consequently, the installation displays the following error message instead of fetching an OSCAP tailored profile:

```
There was an unexpected problem with the supplied content.
```

Workaround: You must specify paths in the **%addon org_fedora_oscap** section of your Kickstart file, for example:

```
xccdf-path = /usr/share/xml/scap/sc_tailoring/ds-combined.xml
tailoring-path = /usr/share/xml/scap/sc_tailoring/tailoring-xccdf.xml
```

As a result, you can use the graphical installation for OSCAP tailored profiles only with the corresponding Kickstart specifications.

Jira:RHEL-1824

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:

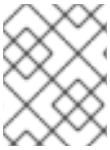
   ```
   # cd /usr/share/scap-security-guide/ansible
   ```

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.

Workaround: 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**.

Workaround: Remove the backslash from the malformed policy file manually by entering the following command: **sed -i 's/^\\//g' <malformed_file_name>**.

Jira:RHEL-11867[1]

Keylime agent rejects requests from the verifier after update

When the API version number of the Keylime agent (**keylime-agent-rust**) has been updated, the agent rejects requests that use a different version. As a consequence, if a Keylime agent is added to a verifier and then updated, the verifier tries to contact the agent using the old API version. The agent rejects this request and fails the attestation.

Workaround: Update the verifier (**keylime-verifier**) before updating the agent (**keylime-agent-rust**). As a result, when the agents are updated, the verifier detects the API change and updates its stored data accordingly.

Jira:RHEL-1518[1]

Missing files in trustdb cause denials for fapolicyd

When **fapolicyd** is installed with the Ansible DISA STIG profile, a race condition causes the **trustdb** database to be out of sync with the **rpmdb** database. As a consequence, missing files in **trustdb** cause denials on the system.

Workaround: Restart **fapolicyd** or run the Ansible DISA STIG profile again.

Jira:RHEL-24345[1]

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 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**.

Jira:RHELPLAN-115609[1]

SSH timeout rules in STIG profiles configure incorrect options

An update of OpenSSH affected the rules in the following Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) profiles:

- DISA STIG for RHEL 9 (**xccdf_org.ssgproject.content_profile_stig**)
- DISA STIG with GUI for RHEL 9 (**xccdf_org.ssgproject.content_profile_stig_gui**)

In each of these profiles, the following two rules are affected:

```
Title: Set SSH Client Alive Count Max to zero
CCE Identifier: CCE-90271-8
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0

Title: Set SSH Idle Timeout Interval
CCE Identifier: CCE-90811-1
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout
```

When applied to SSH servers, each of these rules configures an option (**ClientAliveCountMax** and **ClientAliveInterval**) that no longer behaves as previously. As a consequence, OpenSSH no longer disconnects idle SSH users when it reaches the timeout configured by these rules.

Workaround: These rules have been temporarily removed from the DISA STIG for RHEL 9 and DISA STIG with GUI for RHEL 9 profiles until a solution is developed.

Jira:RHELPLAN-107318[1]

GnuPG incorrectly allows using SHA-1 signatures even if disallowed by crypto-policies

The GNU Privacy Guard (GnuPG) cryptographic software can create and verify signatures that use the SHA-1 algorithm regardless of the settings defined by the system-wide cryptographic policies. Consequently, you can use SHA-1 for cryptographic purposes in the **DEFAULT** cryptographic policy, which is not consistent with the system-wide deprecation of this insecure algorithm for signatures.

Workaround: Do not use GnuPG options that involve SHA-1. As a result, you will prevent GnuPG from lowering the default system security by using the insecure SHA-1 signatures.

Jira:RHELPLAN-117566[1]

OpenSCAP memory-consumption problems

On systems with limited memory, the OpenSCAP scanner might stop prematurely or it might not generate the results files. To work around this problem, you can customize the scanning profile to deselect rules that involve recursion over the entire / file system:

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

Workaround: See the related Knowledgebase article.

Jira:RHELPLAN-145263[1]

Remediating service-related rules during kickstart installations might fail

During a kickstart installation, the OpenSCAP utility sometimes incorrectly shows that a service **enable** or **disable** state remediation is not needed. Consequently, OpenSCAP might set the services on the installed system to a non-compliant state.

Workaround: You can scan and remediate the system after the kickstart installation. This will fix the service-related issues.

Jira:RHELPLAN-44202[1]

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 with 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.

Workaround: Perform 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 with 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

8.3. 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.
```

Workaround: Restart the installation process.

Jira:RHELPLAN-118420[1]

Running createrepo_c on local repositories generates duplicate repodata files

When you run the **createrepo_c** command on local repositories, it generates duplicate copies of **repodata** files, one of the copies is compressed and one is not.

Workaround: There is no workaround available, however, you can safely ignore the duplicate files. The **createrepo_c** command generates duplicate copies because of requirements and differences in other tools relying on repositories created by using **createrepo_c**.

Jira:RHELPLAN-112860[1]

8.4. SHELLS AND COMMAND-LINE TOOLS

Renaming network interfaces using ifcfg files fails

On RHEL 9, the **initscripts** package is not installed by default. Consequently, renaming network interfaces using **ifcfg** files fails.

Workaround: To solve this problem, Red Hat recommends that you use **udev** rules or link files to rename interfaces. For further details, see Consistent network interface device naming and the **systemd.link(5)** man page.

If you cannot use one of the recommended solutions, install the **initscripts** package.

Jira:RHELPLAN-100926[1]

The chkconfig package is not installed by default in RHEL 9

The **chkconfig** package, which updates and queries runlevel information for system services, is not installed by default in RHEL 9.

To manage services, use the **systemctl** commands or install the **chkconfig** package manually.

For more information about **systemd**, see Introduction to systemd. For instructions on how to use the **systemctl** utility, see Managing system services with systemctl.

Jira:RHELPLAN-112043[1]

Setting the console keymap requires the libxkbcommon library on your minimal install

In RHEL 9, certain **systemd** library dependencies have been converted from dynamic linking to dynamic loading, so that your system opens and uses the libraries at runtime when they are available. With this change, a functionality that depends on such libraries is not available unless you install the necessary library. This also affects setting the keyboard layout on systems with a minimal install. As a result, the **localectl --no-convert set-x11-keymap gb** command fails.

Workaround: Install the **libxkbcommon** library:

```
# dnf install libxkbcommon
```

Jira:RHEL-6105

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.

Workaround: You can calculate the **%vmeff** value manually from the **/proc/vmstat** file. For details, see Why the **sar(1)** tool reports **%vmeff** values beyond 100 % in RHEL 8 and RHEL 9?

Jira:RHEL-12009

The Service Location Protocol (SLP) is vulnerable to an attack through UDP

The OpenSLP provides a dynamic configuration mechanism for applications in local area networks, such as printers and file servers. However, SLP is vulnerable to a reflective denial of service amplification attack through UDP on systems connected to the internet. SLP allows an unauthenticated attacker to register new services without limits set by the SLP implementation. By using UDP and spoofing the source address, an attacker can request the service list, creating a Denial of Service on the spoofed address.

To prevent external attackers from accessing the SLP service, disable SLP on all systems running on untrusted networks, such as those directly connected to the internet.

Workaround: Configure firewalls to block or filter traffic on UDP and TCP port 427.

Jira:RHEL-6995[1]

The ReaR rescue image on UEFI systems with Secure Boot enabled fails to boot with the default settings

ReaR image creation by using the **rear mkrescue** or **rear mkbackup** command fails with the following message:

```
grub2-mkstandalone may fail to make a bootable EFI image of GRUB2 (no /usr/*/grub*/x86_64-efi/moddep.lst file)
(...)
grub2-mkstandalone: error: /usr/lib/grub/x86_64-efi/modinfo.sh doesn't exist. Please specify --target or --directory.
```

The missing files are part of the **grub2-efi-x64-modules** package. If you install this package, the rescue image is created successfully without any errors. When the **UEFI** Secure Boot is enabled, the rescue image is not bootable because it uses a boot loader that is not signed.

Workaround: Add the following variables to the **/etc/rear/local.conf** or **/etc/rear/site.conf** ReaR configuration file):

```
UEFI_BOOTLOADER=/boot/efi/EFI/redhat/grubx64.efi
SECURE_BOOT_BOOTLOADER=/boot/efi/EFI/redhat/shimx64.efi
```

With the suggested workaround, the image can be produced successfully even on systems without the **grub2-efi-x64-modules** package, and it is bootable on systems with Secure Boot enabled. In addition, during the system recovery, the bootloader of the recovered system is set to the **EFI** shim bootloader.

For more information about **UEFI**, **Secure Boot**, and **shim bootloader**, see the UEFI: what happens when booting the system Knowledge Base article.

Jira:RHELDOCS-18064[1]

The %util column produced by sar and iostat utilities is invalid

When you collect system usage statistics by using the **sar** or **iostat** utilities, the **%util** column produced by **sar** or **iostat** might contain invalid data.

Jira:RHEL-26275[1]

The lsb-release binary is not available in RHEL 9

The information in **/etc/os-release** was previously available by calling the **lsb-release** binary. This binary was included in the **redhat-lsb package**, which was removed in RHEL 9. Now, you can display information about the operating system, such as the distribution, version, code name, and associated metadata, by reading the **/etc/os-release** file. This file is provided by Red Hat and any changes to it will be overwritten with each update of the **redhat-release** package. The format of the file is **KEY=VALUE**, and you can safely source the data for a shell script.

Jira:RHELDOCS-16427[1]

NetworkManager-wait-online.service fails to start on Azure VMs with Accelerated Networking

When you launch a Red Hat Enterprise Linux VM of Azure platform with the Accelerated Networking feature, also known as Single Root Input Output Virtualization (SR-IOV), multiple network interface cards may have the same MAC address. Consequently, the VM may fail to acquire an IP address from a DHCP server and NetworkManager-wait-online.service` may fail to start at boot time.

Workaround: Do not install the **initscripts-rename-device** package so that existing devices will not rename to existing device names.

Jira:RHEL-79783[1]

8.5. INFRASTRUCTURE SERVICES

The DBD::MySQL driver can fail to establish TLS-encrypted connections to MySQL 8 servers that have caching_sha2_password enabled

The **perl-DBD-MySQL** package is incorrectly linked against the **libmariadb** library. Consequently, Perl applications fail to establish a connection if all of the following conditions are met:

- The application connects to a MySQL 8 server.
- The **caching_sha2_password** option is enabled in the MySQL server configuration.
- The connection uses the **DBI→connect with mysql_ssl=1** option.

Workaround: See the corresponding solution in the Red Hat Knowledgebase.

Jira:RHEL-77083

Both bind and unbound disable validation of SHA-1-based signatures

The **bind** and **unbound** components disable validation support of all RSA/SHA1 (algorithm number 5) and RSASHA1-NSEC3-SHA1 (algorithm number 7) signatures, and the SHA-1 usage for signatures is restricted in the DEFAULT system-wide cryptographic policy.

As a result, certain DNSSEC records signed with the SHA-1, RSA/SHA1, and RSASHA1-NSEC3-SHA1 digest algorithms fail to verify in Red Hat Enterprise Linux 9 and the affected domain names become vulnerable.

To work around this problem, upgrade to a different signature algorithm, such as RSA/SHA-256 or elliptic curve keys.

For more information and a list of top-level domains that are affected and vulnerable, see the DNSSEC records signed with RSASHA1 fail to verify solution.

Jira:RHELPLAN-117492[1]

named fails to start if the same writable zone file is used in multiple zones

BIND does not allow the same writable zone file in multiple zones. Consequently, if a configuration includes multiple zones which share a path to a file that can be modified by the **named** service, **named** fails to start.

Workaround: Use the **in-view** clause to share one zone between multiple views and make sure to use different paths for different zones. For example, include the view names in the path.

Note that writable zone files are typically used in zones with allowed dynamic updates, secondary zones, or zones maintained by DNSSEC.

Jira:RHELPLAN-90604[1]

libotr is not compliant with FIPS

The **libotr** library and toolkit for off-the-record (OTR) messaging provides end-to-end encryption for instant messaging conversations. However, the **libotr** library does not conform to the Federal Information Processing Standards (FIPS) due to its use of the **gcry_pk_sign()** and **gcry_pk_verify()** functions. As a result, you cannot use the **libotr** library in FIPS mode.

Jira:RHELPLAN-122108[1]

Using the incorrect Perl database driver for MariaDB and MySQL can lead to unexpected results

The MariaDB database is a fork of MySQL. Over time, these services developed independently and are no longer fully compatible. These differences also affect the Perl database drivers. Consequently, if you use the **DBD::mysql** driver in a Perl application to connect to a MariaDB database, or the **DBD::MariaDB** driver to connect to a MySQL database, operations can lead to unexpected results. For example, the driver can return incorrect data from read operations. To avoid such problems, use the Perl driver in your application that matches the database service.

Red Hat only supports the following scenarios:

- The Perl **DBD::MariaDB** driver with a MariaDB database
- The Perl **DBD::mysql** driver with a MySQL database

Note that RHEL 8 contained only the **DBD::mysql** driver. If you plan to upgrade to RHEL 9 and then to RHEL 10 and your application uses a MariaDB database, install the **perl-DBD-MariaDB** package after the upgrade and modify your application to use the **DBD::MariaDB** driver.

For further details, see the Red Hat Knowledgebase solution Support of MariaDB/MySQL cross-database connection from Perl db drivers.

Jira:RHELDOCS-19728[1]

VMware vCenter cannot correctly remove a SATA disk from a running RHEL VM

When using the VMWare vCenter interface to remove a SATA disk from a running RHEL 9 guest on the VMware ESXi hypervisor, the disk currently does not get removed fully. It stops being functional and disappears from the guest in the vCenter inteface, but the SCSI interface still detects the disk as attached in the guest.

Jira:RHEL-79914[1]

8.6. NETWORKING

kTLS does not support offloading of TLS 1.3 to NICs

Kernel Transport Layer Security (kTLS) does not support offloading of TLS 1.3 to NICs. Consequently, software encryption is used with TLS 1.3 even when the NICs support TLS offload.

Workaround: Disable TLS 1.3 if offload is required. As a result, you can offload only TLS 1.2. When TLS 1.3 is in use, there is lower performance, since TLS 1.3 cannot be offloaded.

Jira:RHELPLAN-96004[1]

Failure to update the session key causes the connection to break

Kernel Transport Layer Security (kTLS) protocol does not support updating the session key, which is used by the symmetric cipher. Consequently, the user cannot update the key, which causes a connection break.

Workaround: Disable kTLS. As a result, with the workaround, it is possible to successfully update the session key.

Jira:RHELPLAN-99859[1]

The kernel can panic if you reduce the number of SR-IOV VFs at runtime

If all of the following conditions apply, the Linux kernel can panic:

- The host has Input-Output Memory Management Unit (IOMMU) enabled.
- A network driver uses a page pool.
- You reduce the number of Single Root I/O Virtualization (SR-IOV) Virtual Functions (VFs) of the network interface that uses this driver.

Workaround: Do not reduce the number of VFs at runtime. Reboot the machine to reset the number of VFs of all interfaces to 0. Afterwards, you can set a new number of VFs because increasing the number does not cause the kernel panic.

Jira:RHEL-76845[1]

The **initscripts** package is not installed by default

By default, the **initscripts** package is not installed. As a consequence, the **ifup** and **ifdown** utilities are not available.

Workaround: As an alternative, use the **nmcli connection up** and **nmcli connection down** commands to enable and disable connections. If the suggested alternative does not work for you, report the problem and install the **NetworkManager-initscripts-updown** package, which provides a NetworkManager solution for the **ifup** and **ifdown** utilities.

Jira:RHELPLAN-121205[1]

The **iwl7260-firmware** causes Wi-Fi issues on Intel Wi-Fi 6 AX200, AX210, and Lenovo ThinkPad P1 Gen 4

If you update the **iwl7260-firmware** or **iwl7260-wifi** driver to the version provided with RHEL 9.1 or later, the hardware may enter in an incorrect state and report its status incorrectly. Consequently, Intel Wi-Fi 6 cards may fail to function properly and display the following error message:

```
kernel: iwlwifi 0000:09:00.0: Failed to start RT ucode: -110
kernel: iwlwifi 0000:09:00.0: WRT: Collecting data: ini trigger 13 fired (delay=0ms)
kernel: iwlwifi 0000:09:00.0: Failed to run INIT ucode: -110
```

Workaround: An unconfirmed workaround is to power off the system completely and then power it back on. Do not perform a reboot.

Jira:RHELPLAN-134771[1]

Issues in DPLL stability during PF resets

The Digital Phase-Locked Loop (DPLL) system experienced several issues, including uninitialized mutex usage and incorrect handling of pin phase adjustments, particularly during Physical Function (PF) resets. These issues led to unstable management of DPLL and pin configurations, causing inconsistent data states and connection mismanagement.

Workaround: To resolve this, mutexes were properly initialized, and mechanisms for updating pin phase adjustments, DPLL data, and connection states during PF resets were corrected. As a result, the DPLL system now performs reliably during resets, with accurate phase adjustments and consistent connection states, improving the overall stability of clock synchronization.

Jira:RHEL-36283[1]

8.7. 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
```

Workaround: To avoid this problem, use one of the following approaches:

- Use the appropriate build configuration or environment options to create 4k and 64k page size compatible binaries.
- Build any user space packages that use **jemalloc** after booting into the final 64k kernel and runtime environment.

For example, you can build the **fd-find** tool, which also uses **jemalloc**, with the **cargo** Rust package manager. In the final 64k environment, trigger a new build of all dependencies to resolve the mismatch in the page size by entering the **cargo** command:

```
# cargo install fd-find --force
```

Jira:RHELPLAN-147783[1]

Upgrading to the latest real-time kernel with dnf does not install multiple kernel versions in parallel

Installing the latest real-time kernel with the **dnf** package manager requires resolving package dependencies to retain the new and current kernel versions simultaneously. By default, **dnf** removes the older **kernel-rt** package during the upgrade.

Workaround: Add the current **kernel-rt** package to the **installonlypkgs** option in the **/etc/yum.conf** configuration file, for example, **installonlypkgs=kernel-rt**.

The **installonlypkgs** option appends **kernel-rt** to the default list used by **dnf**. Packages listed in **installonlypkgs** directive are not removed automatically and therefore support multiple kernel versions to install simultaneously.

Note that having multiple kernels installed is a way to have a fallback option when working with a new kernel version.

Jira:RHELPLAN-153123[1]

The Delay Accounting functionality does not display the SWAPIN and IO% statistics columns by default

The **Delayed Accounting** functionality, unlike early versions, is disabled by default. Consequently, the **iotop** application does not show the **SWAPIN** and **IO%** statistics columns and displays the following warning:

```
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN and IO%
```

The **Delay Accounting** functionality, using the **taskstats** interface, provides the delay statistics for all tasks or threads that belong to a thread group. Delays in task execution occur when they wait for a kernel resource to become available, for example, a task waiting for a free CPU to run on. The statistics help in setting a task's CPU priority, I/O priority, and **rss** limit values appropriately.

Workaround: You can enable the **delayacct** boot option either at run time or boot.

- To enable **delayacct** at run time, enter:

  ```
  echo 1 > /proc/sys/kernel/task_delayacct
  ```

  Note that this command enables the feature system wide, but only for the tasks that you start after running this command.

- To enable **delayacct** permanently at boot, use one of the following procedures:
  - Edit the **/etc/sysctl.conf** file to override the default parameters:
    a. Add the following entry to the **/etc/sysctl.conf** file:

```
kernel.task_delayacct = 1
```

For more information, see How to set sysctl variables on Red Hat Enterprise Linux .

b. Reboot the system for changes to take effect.

- Add the **delayacct** option to the kernel command line.
  For more information, see Configuring kernel command-line parameters.

As a result, the **iotop** application displays the **SWAPIN** and **IO%** statistics columns.

Jira:RHELPLAN-135779[1]

Hardware certification of the real-time kernel on systems with large core-counts might require passing the skew-tick=1 boot parameter

Large or moderate sized systems with numerous sockets and large core-counts can experience latency spikes due to lock contentions on **xtime_lock**, which is used in the timekeeping system. As a consequence, latency spikes and delays in hardware certifications might occur on multiprocessing systems.

Workaround: You can offset the timer tick per CPU to start at a different time by adding the **skew_tick=1** boot parameter.

To avoid lock conflicts, enable **skew_tick=1**:

1. Enable the **skew_tick=1** parameter with **grubby**.

```
# grubby --update-kernel=ALL --args="skew_tick=1"
```

2. Reboot for changes to take effect.
3. Verify the new settings by displaying the kernel parameters you pass during boot.

```
cat /proc/cmdline
```

Note that enabling **skew_tick=1** causes a significant increase in power consumption and, therefore, it must be enabled only if you are running latency sensitive real-time workloads.

Jira:RHEL-9318[1]

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.

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
```

Jira:RHELPLAN-115732[1]

weak-modules from kmod fails to work with module inter-dependencies

The **weak-modules** script provided by the **kmod** package determines which modules are kABI-compatible with installed kernels. However, while checking modules' kernel compatibility, **weak-modules** processes modules symbol dependencies from higher to lower release of the kernel for which they were built. As a consequence, modules with inter-dependencies built against different kernel releases might be interpreted as non-compatible, and therefore the **weak-modules** script fails to work in this scenario.

Workaround: Build or put the extra modules against the latest stock kernel before you install the new kernel.

Jira:RHELPLAN-126922[1]

The Intel® i40e adapter permanently fails on IBM Power10

When the **i40e** adapter encounters an I/O error on IBM Power10 systems, the Enhanced I/O Error Handling (EEH) kernel services trigger the network driver's reset and recovery. However, EEH repeatedly reports I/O errors until the **i40e** driver reaches the predefined maximum of EEH freezes. As a consequence, EEH causes the device to fail permanently.

Jira:RHEL-15404[1]

dkms provides an incorrect warning on program failure with correctly compiled drivers on 64-bit ARM CPUs

The Dynamic Kernel Module Support (**dkms**) utility does not recognize that the kernel headers for 64-bit ARM CPUs work for both the kernels with 4 kilobytes and 64 kilobytes page sizes. As a result, when the kernel update is performed and the **kernel-64k-devel** package is not installed, **dkms** provides an incorrect warning on why the program failed on correctly compiled drivers.

Workaround: Install the **kernel-headers** package, which contains header files for both types of ARM CPU architectures and is not specific to **dkms** and its requirements.

Jira:RHEL-25967[1]

Kernel panic is encountered on IBM Power systems (ppc64le) when io_uring is enabled

In some cases,**ppc64le** systems encounter a kernel panic when using the **io_uring** kernel parameter due to intensive input-output operations. As a consequence, **ppc64le** stops working and requires a system restart. The data might get lost during the crash.

Workaround: Disable the **io_uring** feature by adding the following kernel parameter at boot time:

module.builtin=io_uring=0

Jira:RHEL-28702[1]

kdump fails to start with UKI

When you install the **kernel-uki-virt** and **kernel-modules-core** packages to enable Unified Kernel Image (UKI) on a confidential VM in Azure, the **kdump** service fails to start. Consequently, **kdump** does not work on the VM.

Workaround: Disable the SELinux policy and reboot the VM. As a result, the **kdump** service is running.

Jira:RHEL-66119[1]

8.8. 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.

Jira:RHELPLAN-105944[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.

Workaround: Deactivate complex block device stacks by executing the following command:

```
# systemctl enable --now blk-availability.service
```

As a result, complex virtual device stacks are correctly deactivated during shutdown and do not produce error messages.

Jira:RHELPLAN-99108[1]

Disabling quota accounting is no longer possible for an XFS filesystem mounted with quotas enabled

Starting with RHEL 9.2, it is no longer possible to disable quota accounting on an XFS filesystem which has been mounted with quotas enabled.

Workaround: Disable quota accounting by remounting the filesystem, with the quota option removed.

Jira:RHELPLAN-145001[1]

udev rule change for NVMe devices

There is a udev rule change for NVMe devices that adds **OPTIONS="string_escape=replace"** parameter. This leads to a disk by-id naming change for some vendors, if the serial number of your device has leading whitespace.

Jira:RHELPLAN-154195[1]

NVMe/FC devices cannot be reliably used in a Kickstart file

NVMe/FC devices can be unavailable during parsing or execution of pre-scripts of the Kickstart file, which can cause the Kickstart installation to fail.

Workaround: Update the boot argument to **inst.wait_for_disks=30**. This option causes a delay of 30 seconds, and should provide enough time for the NVMe/FC device to connect. With this workaround along with the NVMe/FC devices connecting in time, the Kickstart installation proceeds without issues.

Jira:RHEL-8164[1]

Kernel panic while using the qedi driver

While using the **qedi** iSCSI driver, the kernel panics after OS 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.

Workaround: Remove the **vdo** package and its dependencies prior to 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**.

Workaround: DisableLink Layer Discovery Protocol (LLDP) and then enable it for interfaces that can be set on the **vdsm** configuration level. For more information, https://access.redhat.com/solutions/6963195.

Jira:RHEL-8104[1]

System fails to boot when iommu is enabled

By enabling the Input-Output Memory Management Unit (IOMMU) on AMD platforms when the BNX2I adapter is in use, a system fails to boot with the Direct Memory Access Remapping (DMAR) timeout errors.

Workaround: Disable the IOMMU before booting by using the kernel command-line option, **iommu=off**. As a result, the system boots without any errors.

Jira:RHEL-25730[1]

8.9. 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]

8.10. 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.

Jira:RHELPLAN-143480[1]

The --ssl-fips-mode option in MySQL and MariaDB does not change FIPS mode

The **--ssl-fips-mode** option in **MySQL** and **MariaDB** in RHEL works differently than in upstream.

In RHEL 9, if you use **--ssl-fips-mode** as an argument for the **mysqld** or **mariadbd** daemon, or if you use **ssl-fips-mode** in the **MySQL** or **MariaDB** server configuration files, **--ssl-fips-mode** does not change FIPS mode for these database servers.

Instead:

- If you set **--ssl-fips-mode** to **ON**, the **mysqld** or **mariadbd** server daemon does not start.
- If you set **--ssl-fips-mode** to **OFF** on a FIPS-enabled system, the **mysqld** or **mariadbd** server daemons still run in FIPS mode.

This is expected because FIPS mode should be enabled or disabled for the whole RHEL system, not for specific components.

Therefore, do not use the **--ssl-fips-mode** option in **MySQL** or **MariaDB** in RHEL. Instead, ensure FIPS mode is enabled on the whole RHEL system:

- Preferably, install RHEL with FIPS mode enabled. Enabling FIPS mode during the installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place. For information about installing RHEL in FIPS mode, see 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 .

Jira:RHELPLAN-92864[1]

Git fails to clone or fetch from repositories with potentially unsafe ownership

To prevent remote code execution and mitigate CVE-2024-32004, stricter ownership checks have been introduced in **Git** for cloning local repositories. With this update, **Git** treats local repositories with potentially unsafe ownership as dubious.

As a consequence, if you attempt to clone from a repository locally hosted through **git-daemon** and you are not the owner of the repository, **Git** returns a security alert about dubious ownership and fails to clone or fetch from the repository.

Workaround: Explicitly mark the repository as safe by executing the following command:

```
git config --global --add safe.directory /path/to/repository
```

Jira:RHELDOCS-18435[1]

8.11. 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.

Workaround: Enable support for the SHA-1 algorithm on your RHEL 9 systems with the following command:

```
# update-crypto-policies --set DEFAULT:SHA1
```

Jira:RHELPLAN-114497[1]

The PKINIT authentication of a user fails if a RHEL 9 Kerberos agent communicates with a non-RHEL-9, non-AD Kerberos agent

If a RHEL 9 Kerberos agent, either a client or Kerberos Distribution Center (KDC), interacts with a non-RHEL-9 Kerberos agent that is not an Active Directory (AD) agent, the PKINIT authentication of the user fails.

Workaround: Perform one of the following actions:

- Set the RHEL 9 agent's crypto-policy to **DEFAULT:SHA1** to allow the verification of SHA-1 signatures:

  ```
  # update-crypto-policies --set DEFAULT:SHA1
  ```

- Update the non-RHEL-9 and non-AD agent to ensure it does not sign CMS data using the SHA-1 algorithm. For this, update your Kerberos client or KDC packages to the versions that use SHA-256 instead of SHA-1:
  - CentOS 9 Stream: krb5-1.19.1-15
  - RHEL 8.7: krb5-1.18.2-17
  - RHEL 7.9: krb5-1.15.1-53
  - Fedora Rawhide/36: krb5-1.19.2-7

- Fedora 35/34: krb5-1.19.2-3

As a result, the PKINIT authentication of the user works correctly.

Note that for other operating systems, it is the krb5-1.20 release that ensures that the agent signs CMS data with SHA-256 instead of SHA-1.

See also 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
```

Jira:RHELPLAN-113281[1]

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.

Workaround: 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

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]

Installing a RHEL 7 IdM client with a RHEL 9.2 and later IdM server in FIPS mode fails due to EMS enforcement

The TLS **Extended Master Secret** (EMS) extension (RFC 7627) is now mandatory for TLS 1.2 connections on FIPS-enabled RHEL 9.2 and later systems. This is in accordance with FIPS-140-3 requirements. However, the **openssl** version available in RHEL 7.9 and lower does not support EMS. In consequence, installing a RHEL 7 Identity Management (IdM) client with a FIPS-enabled IdM server running on RHEL 9.2 and later fails.

Workaround: If upgrading the host to RHEL 8 before installing an IdM client on it is not an option, remove the requirement for EMS usage on the RHEL 9 server by applying a NO-ENFORCE-EMS subpolicy on top of the FIPS crypto policy:

```
# update-crypto-policies --set FIPS:NO-ENFORCE-EMS
```

Note that this removal goes against the FIPS 140-3 requirements. As a result, you can establish and accept TLS 1.2 connections that do not use EMS, and the installation of a RHEL 7 IdM client succeeds.

Jira:RHEL-4955

Heimdal client fails to authenticate a user using PKINIT against RHEL 9 KDC

By default, a Heimdal Kerberos client initiates the PKINIT authentication of an IdM user by using Modular Exponential (MODP) Diffie-Hellman Group 2 for Internet Key Exchange (IKE). However, the MIT Kerberos Distribution Center (KDC) on RHEL 9 only supports MODP Group 14 and 16.

Consequently, the pre-autentication request fails with the **krb5_get_init_creds: PREAUTH_FAILED** error on the Heimdal client and **Key parameters not accepted** on the RHEL MIT KDC.

Workaround: Ensure that the Heimdal client uses MODP Group 14. Set the **pkinit_dh_min_bits** parameter in the **libdefaults** section of the client configuration file to 1759:

```
[libdefaults]
pkinit_dh_min_bits = 1759
```

As a result, the Heimdal client completes the PKINIT pre-authentication against the RHEL MIT KDC.

Jira:RHELDOCS-19846[1]

8.12. 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 retrieves incomplete list of members if the group size exceeds 1500 members

During the integration of SSSD with Active Directory, SSSD retrieves incomplete group member lists when the group size exceeds 1500 members. This issue occurs because Active Directory's MaxValRange policy, which restricts the number of members retrievable in a single query, is set to 1500 by default.

Workaround: Change the MaxValRange setting in Active Directory to accommodate larger group sizes.

Jira:RHELDOCS-19603[1]

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.

Workaround: 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.

Jira:RHELPLAN-44204[1]

8.13. 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.

Workaround: Manually enable the **vncserver** service after the system upgrade:

```
# systemctl enable --now vncserver@:port-number
```

As a result, VNC is now enabled and starts after every system boot as expected.

Jira:RHELPLAN-114314[1]

User Creation screen is unresponsive

When installing RHEL using a graphical user interface, the User Creation screen is unresponsive. As a consequence, creating users during installation is more difficult.

Workaround: Use one of the following solutions to create users:

- Run the installation in VNC mode and resize the VNC window.
- Create users after completing the installation process.

Jira:RHEL-11924[1]

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

8.14. 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]

8.15. 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]

8.16. 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.

Workaround: Unmask the **firewalld.service**:

```
systemctl unmask firewalld.service
```

Jira:RHELPLAN-133165[1]

Unable to register systems with environment names

The **rhc** system role fails to register the system when specifying environment names in **rhc_environment**.

Workaround: Use environment IDs instead of environment names while registering.

Jira:RHEL-1172

Running Microsoft SQL Server 2022 in high-availability mode as an SELinux-confined application does not work

Microsoft SQL Server 2022 on RHEL 9.4 and later supports running as an SELinux-confined application. However, due to a limitation in Microsoft SQL Server, running the service as an SELinux-confined application does not work in high-availability mode.

Workaround: You can run Microsoft SQL Server as an unconfined application if you require the service to be high available.

Note that this limitation also impacts installing Microsoft SQL Server when you use the **mssql** RHEL System Role to install this service.

Jira:RHELDOCS-17719[1]

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]

8.17. 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.

Workaround: Install **qemu-kvm-block-curl** and **qemu-kvm-block-ssh** on the host to enable https and ssh protocol support. Alternatively, use a different connection protocol or a different installation source.

Jira:RHELPLAN-99854[1]

Using NVIDIA drivers in virtual machines disables Wayland

Currently, NVIDIA drivers are not compatible with the Wayland graphical session. As a consequence, RHEL guest operating systems that use NVIDIA drivers automatically disable Wayland and load an Xorg session instead. This primarily occurs in the following scenarios:

- When you pass through an NVIDIA GPU device to a RHEL virtual machine (VM)
- When you assign an NVIDIA vGPU mediated device to a RHEL VM

There is currently no workaround for this issue.

Jira:RHELPLAN-117234[1]

The Milan VM CPU type is sometimes not available on AMD Milan systems

On certain AMD Milan systems, the Enhanced REP MOVSB (**erms**) and Fast Short REP MOVSB (**fsrm**) feature flags are disabled in the BIOS by default. Consequently, the **Milan** CPU type might not be available on these systems. In addition, VM live migration between Milan hosts with different feature flag settings might fail.

Workaround: Manually turn on **erms** and **fsrm** in the BIOS of your host.

Jira:RHELPLAN-119655[1]

A hostdev interface with failover settings cannot be hot-plugged after being hot-unplugged

After removing a **hostdev** network interface with failover configuration from a running virtual machine (VM), the interface currently cannot be re-attached to the same running VM. There is currently no workaround for this issue.

Jira:RHEL-7337

Live post-copy migration of VMs with failover VFs fails

Currently, attempting to post-copy migrate a running virtual machine (VM) fails if the VM uses a device with the virtual function (VF) failover capability enabled.

Workaround: Use the standard migration type, rather than post-copy migration.

Jira:RHEL-7335

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.

Jira:RHELPLAN-97394[1]

Windows VM fails to get IP address after network interface reset

Sometimes, Windows virtual machines fail to get an IP address after an automatic network interface reset. As a consequence, the VM fails to connect to the network.

Workaround: Disable and re-enable the network adapter driver in the Windows Device Manager.

Jira:RHEL-11366

Windows Server 2016 VMs sometimes stops working after hot-plugging a vCPU

Currently, assigning a vCPU to a running virtual machine (VM) with a Windows Server 2016 guest operating system might cause a variety of problems, such as the VM terminating unexpectedly, becoming unresponsive, or rebooting. There is currently no workaround for this issue.

Jira:RHELPLAN-63771[1]

Redundant error messages on VMs with NVIDIA passthrough devices

When using an Intel host machine with a RHEL 9.2 and later operating system, virtual machines (VMs) with a passed through NVDIA GPU device frequently log the following error message:

```
Spurious APIC interrupt (vector 0xFF) on CPU#2, should never happen.
```

However, this error message does not impact the functionality of the VM and can be ignored. For details, see the Red Hat KnoweldgeBase .

Jira:RHELPLAN-141042[1]

Restarting the OVS service on a host might block network connectivity on its running VMs

When the Open vSwitch (OVS) service restarts or crashes on a host, virtual machines (VMs) that are running on this host cannot recover the state of the networking device. As a consequence, VMs might be completely unable to receive packets.

This problem only affects systems that use the packed virtqueue format in their **virtio** networking stack.

Workaround: Use the **packed=off** parameter in the **virtio** networking device definition to disable packed virtqueue. With packed virtqueue disabled, the state of the networking device can, in some situations, be recovered from RAM.

Jira:RHEL-333

Recovering an interrupted post-copy VM migration might fail

If a post-copy migration of a virtual machine (VM) is interrupted and then immediately resumed on the same incoming port, the migration might fail with the following error: **Address already in use**

Workaround: Wait at least 10 seconds before resuming the post-copy migration or switch to another port for migration recovery.

Jira:RHEL-7096

NUMA node mapping not working correctly on AMD EPYC CPUs

QEMU does not handle NUMA node mapping on AMD EPYC CPUs correctly. As a result, the performance of virtual machines (VMs) with these CPUs might be negatively impacted if using a NUMA node configuration. In addition, the VMs display a warning similar to the following during boot.

```
sched: CPU #4's llc-sibling CPU #3 is not on the same node! [node: 1 != 0]. Ignoring dependency.
WARNING: CPU: 4 PID: 0 at arch/x86/kernel/smpboot.c:415 topology_sane.isra.0+0x6b/0x80
```

Workaround: Do not use AMD EPYC CPUs for NUMA node configurations.

Jira:RHELPLAN-150884[1]

PCIe ATS devices do not work on Windows VMs

When you configure a PCIe Address Translation Services (ATS) device in the XML configuration of virtual machine (VM) with a Windows guest operating system, the guest does not enable the ATS device after booting the VM. This is because Windows currently does not support ATS on **virtio** devices.

For more information, see the Red Hat KnowledgeBase .

Jira:RHELPLAN-118495[1]

virsh blkiotune --weight command fails to set the correct cgroup I/O controller value

Currently, using the **virsh blkiotune --weight** command to set the VM weight does not work as expected. The command fails to set the correct **io.bfq.weight** value in the cgroup I/O controller interface file. There is no workaround at this time.

Jira:RHELPLAN-83423[1]

Starting a VM with an NVIDIA A16 GPU sometimes causes the host GPU to stop working

Currently, if you start a VM that uses an NVIDIA A16 GPU passthrough device, the NVIDIA A16 GPU physical device on the host system in some cases stops working.

To work around the problem, reboot the hypervisor and set the **reset_method** for the GPU device to **bus**:

```
# echo bus > /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
# cat /sys/bus/pci/devices/<DEVICE-PCI-ADDRESS>/reset_method
bus
```

For details, see the Red Hat Knowledgebase .

Jira:RHEL-7212[1]

Windows VMs might become unresponsive due to storage errors

On virtual machines (VMs) that use Windows guest operating systems, the system in some cases becomes unresponsive when under high I/O load. When this happens, the system logs a **viostor Reset to device, \Device\RaidPort3, was issued** error. There is currently no workaround for this issue.

Jira:RHEL-1609[1]

Windows 10 VMs with certain PCI devices might become unresponsive on boot

Currently, a virtual machine (VM) that uses a Windows 10 guest operating system might become unresponsive during boot if a **virtio-win-scsi** PCI device with a local disk back end is attached to the VM.

Workaround: Boot the VM with the **multi_queue** option enabled.

Jira:RHEL-1084[1]

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** blue-screen error.

Jira:RHEL-935[1]

The virtio balloon driver sometimes does not work on Windows 10 and Windows 11 VMs

Under certain circumstances, the **virtio-balloon** driver does not work correctly on virtual machines (VMs) that use a Windows 10 or Windows 11 guest operating system. As a consequence, such VMs might not use their assigned memory efficiently.

Jira:RHEL-12118

The virtio file system has suboptimal performance in Windows VMs

Currently, when a virtio file system (virtiofs) is configured on a virtual machine (VM) that uses a Windows guest operating system, the performance of virtiofs in the VM is significantly worse than in VMs that use Linux guests. There is currently no workaround for this issue.

Jira:RHEL-1212[1]

Hot-unplugging a storage device on Windows VMs might fail

On virtual machines (VMs) that use a Windows guest operating system, removing a storage device when

the VM is running (also known as a device hot-unplug) in some cases fails. As a consequence, the storage device remains attached to the VM and the disk manager service might become unresponsive. There is currently no workaround for this issue.

Jira:RHEL-869

Hot plugging CPUs to a Windows VM might cause a system failure

When hot plugging the maximum number of CPUs to a Windows virtual machine (VM) with huge pages enabled, the guest operating system might crash with the following *Stop error*:

```
PROCESSOR_START_TIMEOUT
```

There is currently no workaround for this issue.

Jira:RHEL-1220

Updating virtio drivers on Windows VMs might fail

When updating the KVM paravirtualized (**virtio**) drivers on a Windows virtual machine (VM), the update might cause the mouse to stop working and the newly installed drivers might not be signed. This problem occurs when updating the **virtio** drivers by installing from the **virtio-win-guest-tools** package, which is a part of the **virtio-win.iso** file.

Workaround: Update the **virtio** drivers by using Windows Device Manager.

Jira:RHEL-574[1]

TX queue size cannot be changed in VMs that use vhost-kernel

Currently, you cannot set up TX queue size on KVM virtual machines (VMs) that use **vhost-kernel** as a back end for the **virtio** network driver. As a consequence, you can use only the default value of 256 for the TX queue, which might prevent you from optimizing your VM network throughput. There is currently no workaround for this issue.

Jira:RHEL-1138[1]

VMs incorrectly report the vulnerable status for spec_rstack_overflow parameter on the AMD EPYC model

When you boot a host, it does not detect any vulnerabilities in the **spec_rstack_overflow** parameter. After querying the parameter for logs, it displays the message:

```
# cat /sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow
Mitigation: Safe RET
```

After booting a VM on the same host, the VM detects a vulnerability in the **spec_rstack_overflow** parameter. And when you query the parameter for logs, it displays the message:

```
# cat /sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow
Vulnerable: Safe RET, no microcode
```

However, this is a false warning message, and you can ignore the status of the **/sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow** file inside the VM.

Jira:RHEL-17614[1]

Link status shows up on VM, even when status is down of e1000e or igb model interface

Before booting the VM, set the status of Ethernet link **down** for the **e1000** or **igb** model network interface. Despite this, after the VM boots, the network interface keeps the **up** status, because when you set the status of Ethernet link **down** and then stop and re-start the VM, it is automatically set back to **up**. Consequently, the correct state of network interface is not maintained.

Workaround: Set the network interface status to **down** inside the VM by using command:

```
# ip link set dev eth0 down
```

Alternatively, you can try to remove and add this network interface again while the VM is running.

Jira:RHEL-21867

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.

Workaround: Use fewer than 128 core per vCPU.

Jira:RHELDOCS-18863[1]

Windows VM with VBS and IOMMU device fails to boot

When you boot a Windows VM with Virtualization Based Security (VBS) enabled and an Input-Output Memory Management Unit (IOMMU) device by using the **qemu-kvm** utility, the booting sequence only shows the boot screen, resulting in an incomplete booting process.

Workaround: Ensure the VM domain XML is configured as below:

```
<features>
  <ioapic driver='qemu'/>
</features>
<devices>
<iommu model='intel'>
   <driver intremap='on' eim='off' aw_bits='48'/>
   <alias name='iommu0'/>
</iommu>
```

```
<memballoon model='virtio'>
  <alias name='balloon0'/>
  <address type='pci' domain='0x0000' bus='0x03' slot='0x00' function='0x0'/>
  <driver iommu='on' ats='on'/>
</memballoon>
</devices>
```

Otherwise, the Windows VM cannot boot.

Jira:RHEL-45585[1]

The **--migrate-disks-detect-zeroes** option might not work for VM migration

Currently, when migrating virtual machines (VMs) on RHEL 10, the **--migrate-disks-detect-zeroes** option might not work and the migration might proceed without zeroed block detection on the specified disk. This problem is caused by a bug in QEMU where mirroring jobs had been relying on punching holes, which results in a sparse destination file.

Jira:RHEL-82906

A virtual machine with a large amount of bootable data disks might fail to start

If you attempt to start a virtual machine (VM) with a large amount of bootable data disks, the VM might fail to boot with this error: **Something has gone seriously wrong: import_mok_state() failed: Volume Full**

Workaround: Decrease the number of bootable data disks and use one system disk. To ensure the system disk is first in the boot order, add **boot order=1** to the device definition of the system disk in the XML configuration. For example:

```
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/path/to/disk.qcow2'/>
  <target dev='vda' bus='virtio'/>
  <boot order='1'/>
</disk>
```

Set boot order only for the system disk.

Jira:RHEL-68418

VMs sending discard I/O requests might pause when **discard_granularity** is not configured

The host kernel fails misaligned discard I/O requests and QEMU uses the **werror=** ***policy*** parameter to respond to such failures. When **werror** is set to **stop**: **werror=stop**, a failed discard request causes the virtual machine (VM) to pause. This is usually undesirable because there is no way to correct this situation and resume the VM again.

Workaround: Ensure that the **discard_granularity** parameter on **virtio-blk** and **virtio-scsi** disks is set and matches the host's **/sys/block/*<blkdev>*/queue/discard_granularity** value. This makes the VM aware of the alignment constraints and ensures discard requests will be properly aligned, so they do not fail.

Jira:RHEL-86032[1]

Windows 2025 VM slows down if assigned with a large number of vCPU

When assigned with 32 or more vCPUs, Windows Server 2025 virtual machines (VMs) slow down on a Red Hat Enterprise Linux host. Consequently, a Windows VM may boot slowly or be stuck during boot when the VM is configured with a large number of vCPUs.

Workaround: You can use the workaround at your own risk. Boot VM with small number of vCPUs to disable plaformclock on Windows Server. In command prompt with administrator privileges, run:

```
bcdedit /set useplatformclock no
```

Then, shut down the VM and reconfigure it with the desired large number of vCPUs. Also make sure that the **hv-time** option is enabled before starting the large VM again.

Jira:RHEL-62742[1]

Too many open files in a virtiofs shared directory can crash the vrtiofsd process

When accessing a **virtiofs** shared directory with a large amount of open files from a virtual machine (VM), the operation might fail with the following error: **Too many open files** and the **virtiofsd** process might crash.

Workaround: Try any of the following steps:

- Run **virtiofsd** as root and use the **--inode-file-handles=mandatory** command-line option.
- Use the **--cache=never** command-line option.
- Increase the number of file descriptors **virtiofsd** is permitted to use with the **--rlimit-nofile** command-line option.

Jira:RHEL-87161[1]

VMs with large memory cannot boot on SEV-SNP host with AMD Genoa CPUs

Currently, virtual machines (VMs) cannot boot on hosts that use a 4th Generation AMD EPYC processor (also known as Genoa) and have the AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) feature enabled. Instead of booting, a kernel panic occurs in the VM.

Jira:RHEL-32892[1]

Installing the VirtIO-Win bundle cannot be canceled

Currently, if you start the installation of **virtio-win** drivers from the VirtIO-Win installer bundle in a Windows guest operating system, clicking the **Cancel** button during the installation does not correctly abort it. The installer wizard interface displays a "Setup Failed" screen, but the drivers are installed and the IP address of the guest is reset.

Jira:RHEL-53962, Jira:RHEL-53965

Windows VM running on Sapphire Rapids CPU with hypervisor launch type set to auto might fail to boot when restarted

If you set the hypervisor launch type to **auto** in a Windows virtual machine (VM) running on a Sapphire Rapids CPU, the VM might fail to boot when it is restarted. For example, you can set the hypervisor launch type to **auto** by using the **bcdedit /set hypervisorlaunchtype Auto** command.

Workaround: Do not set the hypervisor launch type to **auto** in the Windows VM.

Jira:RHEL-67699

Hot-plugging vCPUs and memory to Windows guests with VBS does not work

Currently, Windows Virtualization-based Security (VBS) is not compatible with hot-plugging CPU and memory resources. As a consequence, attempting to attach memory or vCPUs to a running Windows virtual machine (VM) with VBS enabled only adds the resources to the VM after the guest system is restarted.

Jira:RHEL-66229, Jira:RHELDOCS-19066

8.18. 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

Jira:RHELPLAN-114103[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.

Workaround: See the VMware Knowledge Base.

Jira:RHELPLAN-106947[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.

Jira:RHELPLAN-120807[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.

Workaround: Edit the **/etc/fstab** file on the machine and add extra timeout options to the **/boot** and **/boot/efi** mount points. For example:

```
UUID=e43ead51-b364-419e-92fc-b1f363f19e49 /boot xfs defaults,x-systemd.device-timeout=600,x-systemd.mount-timeout=600 0 0

UUID=7B77-95E7 /boot/efi vfat defaults,uid=0,gid=0,umask=077,shortname=winnt,x-systemd.device-timeout=600,x-systemd.mount-timeout=600 0 2
```

Jira:RHELDOCS-16979[1]

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]

Memory hot-plug possible on VMware when the memory size does not align with memory block size

Currently, it is possible to attempt hot-plugging memory to a RHEL 9 guest on VMware hypervisor even if the memory size of the attached memory dpes not align with the size of the individual memory blocks. However, attaching memory in this manner always fails with a **Block size unaligned hotplug range** error.

Workaround: Only hot-plug memory that is divisible by the configured memory block size on the guest. To obtain the memory block size, use the **lsmem** command. For further information, see The Red Hat KnowledgeBase.

Jira:RHEL-81748[1]

Nested VM with KVM virtualization and OVMF fails to boot on Azure or Hyper-V when using AMD EPYC processor

A nested VM with Open Virtual Machine Firmware (OVMF) fails to boot when run on a RHEL VM with KVM virtualization enabled in the Azure cloud or Hyper-V using the AMD EPYC processor. The VM fails to boot up with following log message:

```
Code=qemu-kvm: ../hw/core/cpu-sysemu.c:76  Aborted (core dumped) .
```

Workaround: Try booting without using the AMD EPYC processor.

Jira:RHEL-29919[1]

BIOS or UEFI supported Hyper-V Windows Server 2016 VM fails to boot if a host uses the AMD EPYC CPU processor

With the Hyper-V enabled setting, Hyper-V Windows Server 2016 VM fails to boot on the AMD EPYC CPU host.

Workaround: Check for the following log message:

```
kvm: Booting SMP Windows KVM VM with !XSAVES && XSAVEC.
If it fails to boot try disabling XSAVEC in the VM config.
```

And try adding **xsavec=off** to **-cpu cmdline** to boot Hyper-V Windows Server 2016 VM.

Jira:RHEL-38957[1]

kdump fails to complete on the Azure Confidential VMs

When you experience a kernel crash on a Red Hat Enterprise Linux VM on the Azure Confidential VM instances, in this case DCv5 and ECv5 series, the **kdump** process may not complete and the VM becomes unresponsive. As a result, after a forced reboot, there is a **vmcore-incomplete** file.

Jira:RHEL-70228[1]

8.19. 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]

8.20. CONTAINERS

Running systemd within an older container image does not work

Running systemd within an older container image, for example, **centos:7**, does not work:

```
$ podman run --rm -ti centos:7 /usr/lib/systemd/systemd
 Storing signatures
 Failed to mount cgroup at /sys/fs/cgroup/systemd: Operation not permitted
 [!!!!!!] Failed to mount API filesystems, freezing.
```

Workaround: Use the following commands:

```
# mkdir /sys/fs/cgroup/systemd
# mount none -t cgroup -o none,name=systemd /sys/fs/cgroup/systemd
# podman run --runtime /usr/bin/crun --annotation=run.oci.systemd.force_cgroup_v1=/sys/fs/cgroup -
-rm -ti centos:7 /usr/lib/systemd/systemd
```

Jira:RHELPLAN-96940[1]

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.

Workaround: 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

RHEL images on Azure marked as LVM require default layout resizing

When using **system-reinstall-bootc** or **bootc install** on Azure, RHEL images marked as LVM will require resizing the default layout.

Workaround: Use RHEL images labeled as RAW. This does not require resizing the default layout.

Jira:RHELDOCS-19945[1]

FIPS bootc image creation fails on FIPS enabled host

Building a disk image on a host by using Podman with enabled the FIPS mode fails with the exit code 3 because of the update-crypto-policies package:

```
# Enable the FIPS crypto policy
# crypto-policies-scripts is not installed by default in RHEL-10
RUN dnf install -y crypto-policies-scripts && update-crypto-policies --no-reload --set FIPS
```

Workaround: Build the bootc image with FIPS mode disabled.

Jira:RHELDOCS-19539

Insufficient disk space can cause deployment failure

Deploying a bootc container image on a package mode system without enough free disk space can result in installation errors and prevent the system from booting. Ensure adequate disk space is available for the image to install and adjust the provision logical volume before deployment.

Jira:RHELDOCS-19948[1]

8.21. LIGHTSPEED

Configuration file changes are not applied immediately

When making changes in the **etc/xdg/command-line-assistant/config.toml** configuration file, it takes around 30 to 60 seconds for the command line assistant daemon to recognize the changes, instead of applying the changes immediately. The command line assistant is also missing the **reload** functionality.

Workaround: Follow the steps:

1. Make the changes that you need to the **config.toml** configuration file.
2. Run the following command:

```
# systemctl restart clad
```

Jira:RHELDOCS-19734[1]

CHAPTER 9. 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 9.1. 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 9.2. 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 9.3. Available map types

Map type	Available
hash	yes
array	yes
prog_array	yes
perf_event_array	yes
percpu_hash	yes
percpu_array	yes
stack_trace	yes
cgroup_array	yes
lru_hash	yes
lru_percpu_hash	yes
lpm_trie	yes
array_of_maps	yes
hash_of_maps	yes

Map type	Available
devmap	yes
sockmap	yes
cpumap	yes
xskmap	yes
sockhash	yes
cgroup_storage	yes
reuseport_sockarray	yes
percpu_cgroup_storage	yes
queue	yes
stack	yes
sk_storage	yes
devmap_hash	yes
struct_ops	yes
ringbuf	yes
inode_storage	yes
task_storage	yes
bloom_filter	yes
user_ringbuf	yes
cgrp_storage	yes
arena_map	yes

APPENDIX A. LIST OF TICKETS BY COMPONENT

Bugzilla and JIRA tickets are listed in this document for reference. The links lead to the release notes in this document that describe the tickets.

Component	Tickets
389-ds-base	Jira:RHEL-67195, Jira:RHEL-5151, Jira:RHEL-78650, Jira:RHEL-62875, Jira:RHEL-71218, Jira:RHEL-76019, Jira:RHEL-67020, Jira:RHEL-70252, Jira:RHEL-64438, Jira:RHEL-67005, Jira:RHEL-60135, Jira:RHEL-74158, Jira:RHEL-74168, Jira:RHEL-78344, Jira:RHEL-78722, Jira:RHEL-61341, Jira:RHEL-65662, Jira:RHEL-67004, Jira:RHEL-65776, Jira:RHEL-67008
NetworkManager	Jira:RHEL-24055, Jira:RHEL-45878, Jira:RHEL-32685, Jira:RHEL-21160, Jira:RHEL-14370, Jira:RHEL-69899, Jira:RHEL-24337, Jira:RHEL-5852, Jira:RHEL-24622, Jira:RHELPLAN-58745, Jira:RHEL-17619
NetworkManager-libreswan	Jira:RHEL-58040
Release Notes	Jira:RHELDOCS-19863, Jira:RHELDOCS-16760, Jira:RHELDOCS-19839, Jira:RHELDOCS-20163, Jira:RHELDOCS-20170, Jira:RHELDOCS-18935, Jira:RHELDOCS-16861, Jira:RHELDOCS-17520, Jira:RHELDOCS-17803, Jira:RHELDOCS-19072, Jira:RHELDOCS-19635, Jira:RHELDOCS-19889, Jira:RHELDOCS-20146, Jira:RHELDOCS-18158, Jira:RHELDOCS-17532, Jira:RHELDOCS-17508, Jira:RHELDOCS-19022, Jira:RHELDOCS-19284, Jira:RHELDOCS-18312, Jira:RHELDOCS-18480, Jira:RHELDOCS-19224, Jira:RHELDOCS-19028, Jira:RHELDOCS-19029, Jira:RHELDOCS-18959, Jira:RHELDOCS-19013, Jira:RHELDOCS-19012, Jira:RHELDOCS-19080, Jira:RHELDOCS-19050, Jira:RHELDOCS-19093, Jira:RHELDOCS-19149, Jira:RHELDOCS-19133, Jira:RHELDOCS-19171, Jira:RHELDOCS-19147, Jira:RHELDOCS-19139, Jira:RHELDOCS-19135, Jira:RHELDOCS-19137, Jira:RHELDOCS-19154, Jira:RHELDOCS-19143, Jira:RHELDOCS-19151, Jira:RHELDOCS-19115, Jira:RHELDOCS-18531, Jira:RHELDOCS-20135, 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-19603, Jira:RHELDOCS-16979, Jira:RHELDOCS-19846
anaconda	Jira:RHEL-61430, Jira:RHEL-10216, Jira:RHEL-2250, Jira:RHEL-17205, Jira:RHELPLAN-168262, Jira:RHELPLAN-110940, Jira:RHELPLAN-53644, Jira:RHEL-4707, Jira:RHEL-4711, Jira:RHELPLAN-94811, Jira:RHEL-4741, Jira:RHELPLAN-130370, Jira:RHEL-4762, Jira:RHEL-4737, Jira:RHEL-9633, Jira:RHEL-14005, Jira:RHEL-80867, Jira:RHEL-82566, Jira:RHEL-78272, Jira:RHEL-13837, Jira:RHEL-66155

Component	Tickets
ansible-collection-microsoft-sql	Jira:RHEL-68374, Jira:RHEL-67807, Jira:RHEL-69311
ansible-freeipa	Jira:RHEL-67566
audit	Jira:RHEL-59570
bacula	Jira:RHEL-6856
bind	Jira:RHELPLAN-90604
binutils	Jira:RHEL-59802, Jira:RHEL-59801, Jira:RHEL-50068
boost	Jira:RHEL-67177, Jira:RHEL-67973
bootc-image-builder-container	Jira:RHEL-34807
ca-certificates	Jira:RHEL-54695
clevis	Jira:RHEL-60257
cockpit-machines	Jira:RHEL-31993
container-tools	Jira:RHEL-68240, Jira:RHEL-66763, Jira:RHEL-69742, Jira:RHEL-67859
createrepo_c	Jira:RHELPLAN-112860
crypto-policies	Jira:RHEL-76524, Jira:RHEL-76528, Jira:RHEL-2735
cups	Jira:RHEL-68414
cyrus-sasl	Jira:RHELPLAN-94096
device-mapper-multipath	Jira:RHEL-58920, Jira:RHEL-73413, Jira:RHELPLAN-105944, Jira:RHELPLAN-99108, Jira:RHELPLAN-66975
distribution	Jira:RHEL-59005, Jira:RHEL-6973, Jira:RHEL-18157, Jira:RHEL-68141, Jira:RHEL-22385
dnf	Jira:RHEL-70917, Jira:RHEL-49670, Jira:RHEL-61882, Jira:RHELPLAN-118420
dnf-plugins-core	Jira:RHEL-14900, Jira:RHEL-40914

Component	Tickets
edk2	Jira:RHEL-58631, Jira:RHELPLAN-69533, Jira:RHEL-68418
elfutils	Jira:RHEL-64067
fapolicyd	Jira:RHELPLAN-112355, Jira:RHEL-24345, Jira:RHEL-520
firewalld	Jira:RHEL-17708
gimp	Jira:RHELPLAN-109991
glibc	Jira:RHEL-67692, Jira:RHEL-24740, Jira:RHEL-1915, Jira:RHEL-50662, Jira:RHEL-65358, Jira:RHEL-56032, Jira:RHEL-2419
gnome-control-center	Jira:RHEL-68152
gnupg2	Jira:RHELPLAN-117566
gnutls	Jira:RHELPLAN-128129
golang	Jira:RHEL-62392, Jira:RHELPLAN-129104, Jira:RHELPLAN-123778
greenboot	Jira:RHEL-80003
gtk3	Jira:RHEL-11924
initscripts	Jira:RHEL-79783
ipa	Jira:RHEL-45330, Jira:RHEL-48104, Jira:RHEL-4915, Jira:RHEL-67913, Jira:RHELPLAN-113281, Jira:RHEL-12154, Jira:RHEL-4955
iproute	Jira:RHEL-62931
jmc-core	Jira:RHELPLAN-88788
kdump-anaconda-addon	Jira:RHEL-11196
kernel	Bugzilla:2177256, Jira:RHELPLAN-102815, Jira:RHELPLAN-102321, Jira:RHELPLAN-108169, Jira:RHELPLAN-154595, Jira:RHELPLAN-153754, Jira:RHELPLAN-157294, Jira:RHELPLAN-147783, Jira:RHELPLAN-96004, Jira:RHELPLAN-99859, Jira:RHELPLAN-135779, Jira:RHELPLAN-114103, Jira:RHELPLAN-97394, Jira:RHELPLAN-134771, Jira:RHELPLAN-141042
kernel / Accelerators	Jira:RHEL-38583
kernel / BPF	Jira:RHEL-63880

Component	Tickets
kernel / Core	Jira:RHEL-25967
kernel / Core / Control Groups	Jira:RHEL-36267
kernel / Crypto	Jira:RHEL-20145
kernel / Debugging-Tracing / kexec - kdump	Jira:RHEL-58641, Jira:RHEL-66119
kernel / Debugging-Tracing / rtla	Jira:RHEL-69522
kernel / File Systems	Jira:RHEL-33888
kernel / File Systems / CIFS	Jira:RHEL-76046
kernel / File Systems / NFS	Jira:RHEL-59704
kernel / Networking	Jira:RHEL-68063, Jira:RHEL-61203, Jira:RHEL-59091, Jira:RHEL-88552, Jira:RHEL-88551, Jira:RHEL-76845
kernel / Networking / Bonding	Jira:RHEL-50630
kernel / Networking / IPSec	Jira:RHEL-30141, Jira:RHEL-1015
kernel / Networking / NIC Drivers	Jira:RHEL-57827, Jira:RHEL-54223, Jira:RHEL-9897, Jira:RHEL-36283
kernel / Platform Enablement / NVMe	Jira:RHEL-9301, Jira:RHEL-8171, Jira:RHEL-8164
kernel / Platform Enablement / ppc64	Jira:RHEL-15404, Jira:RHEL-28702
kernel / Security	Jira:RHEL-8810
kernel / Security / TPM	Jira:RHEL-52747
kernel / Storage / Multiple Devices (MD)	Jira:RHEL-46615, Jira:RHEL-30730
kernel / Storage / Storage Drivers	Jira:RHEL-56135, Jira:RHEL-8466, Jira:RHEL-8104, Jira:RHEL-25730

Component	Tickets
kernel / Virtualization	Jira:RHEL-1138
kernel / Virtualization / Hyper-V	Jira:RHEL-29919, Jira:RHEL-70228
kernel / Virtualization / KVM	Jira:RHEL-50754, Jira:RHEL-26152, Jira:RHEL-7212, Jira:RHEL-10019, Jira:RHEL-17331, Jira:RHEL-45585, Jira:RHEL-32892, Jira:RHEL-38957
kernel / Virtualization / Public Cloud Enablement	Jira:RHEL-70465, Jira:RHEL-81748
kernel-rt	Jira:RHELPLAN-153123
kernel-rt / Other	Jira:RHEL-9318
kexec-tools	Jira:RHEL-32060, Jira:RHELPLAN-129876, Jira:RHEL-11471, Jira:RHELPLAN-115732
keylime	Jira:RHEL-75797, Jira:RHEL-78313, Jira:RHEL-11867, Jira:RHEL-1518
kmod	Jira:RHELPLAN-126922
kmod-kvdo	Jira:RHEL-8354
kpatch	Jira:RHEL-77113
krb5	Jira:RHEL-4902, Jira:RHELPLAN-114497, Jira:RHEL-4875, Jira:RHEL-4888
libabigail	Jira:RHEL-64069, Jira:RHEL-16629
libotr	Jira:RHELPLAN-122108
libva	Jira:RHEL-59629
libvirt	Jira:RHEL-28819, Jira:RHELPLAN-139536, Jira:RHELPLAN-119912
libvirt / General	Jira:RHEL-7043
libxcrypt	Jira:RHELPLAN-106338
lldpad	Jira:RHEL-61874
llvm	Jira:RHEL-57460, Jira:RHEL-68696, Jira:RHEL-70328

Component	Tickets
logrotate	Jira:RHEL-5711
lvm2	Jira:RHELPLAN-107107
maven	Jira:RHEL-62175, Jira:RHEL-73128
mysql	Jira:RHEL-68305, Jira:RHELPLAN-92864
nettle	Jira:RHEL-52740
nfs-utils	Jira:RHELPLAN-120807
nginx	Jira:RHEL-73508
nmstate	Jira:RHEL-43438
nodejs	Jira:RHEL-35990
nss	Jira:RHEL-58260
nvme-stas	Jira:RHELPLAN-58357
open-vm-tools	Jira:RHELPLAN-106947
opencryptoki	Jira:RHEL-50064
openldap	Jira:RHEL-71053, Jira:RHEL-78297, Jira:RHEL-56502
opensc	Jira:RHEL-53115
openscap	Jira:RHEL-88413, Jira:RHELPLAN-145263
openslp	Jira:RHEL-6995
openssh	Jira:RHEL-33809, Jira:RHELPLAN-113842, Jira:RHEL-45727
openssl	Jira:RHELPLAN-148207, Jira:RHELPLAN-50959, Jira:RHELPLAN-48241, Jira:RHEL-40605
osbuild-composer	Jira:RHEL-4649
oscap-anaconda-addon	Jira:RHEL-1824, Jira:RHELPLAN-44202
p11-kit	Jira:RHEL-58899

Component	Tickets
pacemaker	Jira:RHEL-34276, Jira:RHEL-55458
pause-container	Jira:RHELPLAN-127619
pcp	Jira:RHEL-58953, Jira:RHEL-59366, Jira:RHEL-30590
pcs	Jira:RHEL-61901, Jira:RHEL-46284, Jira:RHEL-16232, Jira:RHEL-69040, Jira:RHEL-46293, Jira:RHEL-55441, Jira:RHEL-61738, Jira:RHEL-34781
pcsc-lite	Jira:RHEL-34856
perl-DBD-MySQL	Jira:RHEL-77083
php	Jira:RHEL-73907, Jira:RHEL-21448
pki-core	Jira:RHELPLAN-121754
podman	Jira:RHEL-60561, Jira:RHEL-32267, Jira:RHEL-70217, Jira:RHELPLAN-117005
powerpc-utils	Jira:RHEL-61089, Jira:RHEL-30880
python-blivet	Jira:RHEL-82430
python3.11-lxml	Jira:RHELPLAN-143480
qemu-kvm	Jira:RHEL-68440, Jira:RHELPLAN-81033, Jira:RHELPLAN-75969, Jira:RHELPLAN-114513, Jira:RHELPLAN-99854, Jira:RHELPLAN-63771, Jira:RHELPLAN-150884, Jira:RHELPLAN-118495, Jira:RHEL-7478, Jira:RHEL-82906, Jira:RHEL-86032, Jira:RHEL-62742, Jira:RHEL-67699, Jira:RHEL-66229
qemu-kvm / Devices	Jira:RHEL-1220
qemu-kvm / Devices / CPU Models	Jira:RHEL-15731, Jira:RHEL-17614
qemu-kvm / Devices / Machine Types	Jira:RHEL-11043
qemu-kvm / Graphics	Jira:RHEL-7135
qemu-kvm / Live Migration	Jira:RHEL-64307, Jira:RHEL-33795, Jira:RHEL-7096

Component	Tickets
qemu-kvm / Networking	Jira:RHEL-7337, Jira:RHEL-7335, Jira:RHEL-7336, Jira:RHEL-333, Jira:RHEL-21867
realtime-tests	Jira:RHEL-65487
resource-agents	Jira:RHEL-32265
restore	Jira:RHELPLAN-94704
rhel-bootc-container	Jira:RHEL-33208
rhel-system-roles	Jira:RHEL-73408, Jira:RHEL-69983, Jira:RHEL-67244, Jira:RHEL-61596, Jira:RHEL-27760, Jira:RHEL-70483, Jira:RHEL-36014, Jira:RHEL-61599, Jira:RHEL-63026, Jira:RHEL-65748, Jira:RHEL-61947, Jira:RHEL-73409, Jira:RHEL-73406, Jira:RHEL-73402, Jira:RHEL-65758, Jira:RHEL-13333, Jira:RHEL-62395, Jira:RHEL-73404, Jira:RHEL-61085, Jira:RHEL-73244, Jira:RHEL-82160, Jira:RHELPLAN-95747, Jira:RHELPLAN-133165, Jira:RHEL-1172
rpm	Jira:RHEL-6294
rsyslog	Jira:RHEL-65177
rteval	Jira:RHEL-9909, Jira:RHEL-67423
rust	Jira:RHEL-61964
scap-security-guide	Jira:RHEL-74240, Jira:RHEL-1800, Jira:RHELPLAN-107318
seabios	Jira:RHEL-7110
selinux-policy	Jira:RHEL-54996, Jira:RHEL-17346, Jira:RHEL-52476, Jira:RHEL-11792, Jira:RHELPLAN-115609, Jira:RHEL-28814
sos	Jira:RHEL-24523, Jira:RHEL-30893, Jira:RHEL-35945, Jira:RHEL-22389, Jira:RHEL-67712, Bugzilla:1869561
sssd	Jira:RHELPLAN-44204
stunnel	Jira:RHEL-52317
subscription-manager	Jira:RHEL-29178, Jira:RHELPLAN-146101, Jira:RHELPLAN-137234
subscription-manager-cockpit	Jira:RHEL-56159

Component	Tickets
sysstat	Jira:RHEL-12009, Jira:RHEL-26275
systemd	Jira:RHELPLAN-100926, Jira:RHEL-6105
systemtap	Jira:RHEL-64066
tigervnc	Jira:RHELPLAN-114314
traceroute	Jira:RHEL-59444
trustee-guest-components	Jira:RHEL-68141
tuned	Jira:RHELPLAN-129881, Jira:RHEL-79914
unbound	Jira:RHELPLAN-117492
valgrind	Jira:RHEL-64070
vdo	Jira:RHEL-30525
virt-manager / Common	Jira:RHEL-62959
virt-v2v	Jira:RHELPLAN-147926
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-1084, Jira:RHEL-935, Jira:RHEL-12118, Jira:RHEL-1212, Jira:RHEL-53962
virtiofsd	Jira:RHEL-29027, Jira:RHEL-87161
webkit2gtk3	Jira:RHEL-4157
wpa_supplicant	Jira:RHEL-58725
xdp-tools	Jira:RHEL-73054, Jira:RHEL-3382

Component	Tickets
other	Jira:RHELDOCS-19863, Jira:RHELDOCS-19936, Jira:RHELDOCS-20057, Jira:RHELDOCS-18451, Jira:RHELDOCS-20116, Jira:RHELDOCS-19610, Jira:RHELDOCS-19876, Jira:RHELDOCS-19832, Jira:RHELDOCS-20019, Jira:RHELDOCS-20024, Jira:RHELDOCS-19516, Jira:RHELDOCS-19825, Jira:RHELDOCS-19584, Jira:RHELDOCS-19210, Jira:RHELDOCS-19291, Jira:RHELDOCS-20170, Jira:RHELDOCS-17040, Jira:RHEL-88550, Jira:RHELDOCS-20059, 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-19664, Jira:RHELDOCS-19635, Jira:RHELDOCS-19455, Jira:RHEL-91106, Jira:RHELDOCS-19815, Jira:RHELDOCS-19716, Jira:RHELDOCS-19809, Jira:RHELDOCS-19810, Jira:RHELDOCS-19523, Jira:RHELDOCS-20146, Jira:RHELDOCS-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, Jira:RHELPLAN-67314, Jira:RHELPLAN-110763, Jira:RHELPLAN-69554, Jira:RHELPLAN-113995, Jira:RHELDOCS-20135, Jira:RHELPLAN-122745, Jira:RHELPLAN-99136, Jira:RHELPLAN-103232, Jira:RHELPLAN-60153, Jira:RHELPLAN-88246, Jira:RHELPLAN-100087, Jira:RHELPLAN-100639, Jira:RHELPLAN-113659, Jira:RHELPLAN-98983, Jira: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, Jira:RHELPLAN-10061, Bugzilla:1697896, Jira:RHELPLAN-110191, Jira:RHELPLAN-96940, Jira:RHELPLAN-117234, Jira:RHELPLAN-119001, Jira:RHELPLAN-119852, Jira:RHELPLAN-119655, Jira:RHELPLAN-112043, Jira:RHELPLAN-121205, Jira:RHELPLAN-121049, Jira:RHELPLAN-109613, Jira:RHELPLAN-145001, Jira:RHELDOCS-19603, Jira:RHELDOCS-18064, Jira:RHELDOCS-16427, Jira:RHELPLAN-150080, Jira:RHELPLAN-154195, Jira:RHELPLAN-83423, Jira:RHELDOCS-17719, Jira:RHELDOCS-17720, Jira:RHELDOCS-19945, Jira:RHELDOCS-18720, Jira:RHELDOCS-18435, Jira:RHELDOCS-18863, Jira:RHELDOCS-19728, Jira:RHELDOCS-19539, Jira:RHELDOCS-19734, Jira:RHELDOCS-19948, Jira:RHELDOCS-19496

APPENDIX B. REVISION HISTORY

0.0-0

Tue 20 May 2025, Gabriela Fialová (gfialova@redhat.com)

- Release of the Red Hat Enterprise Linux 9.6 Release Notes.